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

June 14, 2007/14 juin 2007

IT.Can NEWSLETTER/BULLETIN

Canadian IT Law Association

www.it-can.ca

Part 1 of this newsletter is prepared by Professors 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 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

Computer Law & Customs Tariff: Classification of Musical Digital Interface (MIDI)

The Federal Court of Appeal, Ottawa has delivered its judgment in *Jam Industries Ltd. v. Canada (Border Services Agency)*. In this case, the President of the Canada Border Services Agency (CBSA) refused a request by the appellant to classify some goods under tariff item no. 9948.00.00. The latter is a concessionary tariff which eliminates or reduces duties that are otherwise payable for goods that are therein covered. The President's decision was upheld by the Canadian International Trade Tribunal (CITT), a decision which the appellant further appealed to the Federal Court of Appeal in the present proceeding. The goods in issue in the present appeal are 29 models of key board synthesizers, digital pianos and digital organs (the keyboard goods), 13 models of non-keyboard synthesizers (collectively with the keyboard goods, musical instruments) and four expansion boards for synthesizers. Tariff item no 9948.00.00 refers inter alia to "articles for use in automatic data processing machines and units thereof, magnetic or optical readers, machines for transcribing data onto data media in coded form and machines for processing such data" as well as "parts and accessories for the foregoing". Under s.2(1) of *Customs Tariff*, the phrase "for use in" when associated with a tariff item or goods classified thereto means that "the goods must be wrought or incorporated into or attached to, other goods referred to in that tariff item" (¶6). The CBSA classified the goods in question into three different tariff items and none of them was classified under tariff item no. 9948.00.00. The CITT found on evidence that the musical instruments were midi-enabled. MIDI (musical digital interface) is a protocol through which musical information can be transferred in a digital form between devices that incorporate the interface. For the transfer to happen there has to be some connection between the devices. Under the MIDI protocol, CITT found that musical instruments were connected with the computer, such that the computer and the instruments were enabled to perform tasks which they could not perform independently. Consequently, it found that "[t]hrough the connection of the MIDI-enabled instrument to the computer; it is the instrument's functions that are expanded or improved and not those of the computer" (¶11). CITT also found that the musical instrument was for use with computer and not "for use in" a computer and therefore fall outside tariff no. 9948.00.00. With regard to the expansion board, the CITT concluded that they did not fall within the concessionary items because they were parts and accessories of a musical instrument and not for use in parts of or accessories of computers.

In this appeal the appellant argues that there was an error of law when CITT departed from its original jurisprudence and found that the functional connection test for the purpose of tariff 9948.00.00 decision is that the tariff item must enhance the functionality of the host (i.e. the computer) and not that of the item attached to the host, which here refers to the musical instrument. The court held that the standard of review here is reasonableness. It concluded that the lone fact that CITT departed from its own jurisprudence regarding the application of the phrase "for use in" "does not prove that the decision in issue here is unreasonable, and does not give rise to a distinct ground of judicial intervention"

(¶20). In dismissing the appeal with costs the court observed that pursuant to the Supreme Court decision in *Domtar. v. Quebec* administrative tribunals in Canada have the authority to err in their arrears of expertise. As such, lack of consistency or unanimity is the price to pay for the freedom of decision making and independence of the tribunal members.

Immigration Law: Reliability of Internet Documents

The Federal Court in Ottawa has delivered its judgment in *Jalil v. Canada (Minister of Citizenship and Immigration)*. In this case the applicant, a Pakistani citizen, was granted refugee status in Canada in 1977. That same year, he applied for permanent residence status. After seven years, he applied to court to compel Citizenship and Immigration Canada (CIC) to make a decision on his pending application for permanent residence. In 2005, CIC rendered a decision denying the applicant's application on the ground that he was inadmissible pursuant to the *Immigration and Refugee Protection Act*. The applicant was found to belong to an organization in Pakistan, Quami Movement (MQM-A), that was engaged in terrorism. Upon an application for a judicial review of the CIC decision by the applicant, the court allowed a judicial review and ordered a re-determination of the applicant's permanent residence application. A different immigration officer examined the application. She based her decision on three key documents which she also made available to the applicant. The first document was entitled *Muttahida Quomi Mhaz, Terrorist Group of Pakistan* (MQM). It was obtained from the website of South Asia Terrorism Portal (SATP), an organization. The second document was titled *Muttahida Quami Movement-Altaf* (MQM-A). It was obtained from the website of Jane's Insurgency and Terrorism. The last document was a report generated by Amnesty International entitled, *Human Rights Crisis in Karachi*. In discrediting these documents, the applicant counsel relied *inter alia* on two documents from two experts, one from Dr. Gowher Rizvi, Director of Ash Institute for Democratic Governance and Innovation. Another was an affidavit from Dr. Lisa Given, Associate Professor in the School of Library and Information Services, Faculty of Education, University of Alberta. Dr. Given's affidavit focuses on the "use of internet sources and the criteria that librarians use to assess internet documents". She assessed the three documents. She doubted the reliability of the document from the SATP website because references were not provided in support of the claims made. On the documents from Jane's website, she found that it was not attributed to any author and there was no reference in support of the claims made notwithstanding that the document ended with "©2004 Jane's Information Group Paul Burton". Overall, she concluded "that the reliability of all the documents is reduced because of the lack of source evidence, the use of phrases like "suspected" and "accused of", the lack of authorship and/or other background details such as how the information was [sic] complied and the mixing of reference to MQM-A and MQM" (¶7). In regard to the Amnesty International document, she concluded it was difficult to assess its quality because it lacked independently corroborated evidence.

In her decision, the Officer placed limited reliance on the two documents from the internet but placed greater reliance on the Amnesty International document. The court upheld Dr Given's impression of the website information and faulted immigration officers' reliance on the two internet documents and found that since they could not be attributed to authors and had no references, they could probably have been a duplication of each other. On the other hand, contrary to Dr. Given's affidavit evidence, the court found the Amnesty International report concluded with an explanation of how the information in the report was generated. It also held that based on Amnesty International's reputation and explanation on how the report was made, the officer's reliance on the report was reasonable. However, the court noted that reputation alone is not conclusive of credibility of a document emanating from Amnesty International. It also found that the decision by the officer to give more weight to documentary evidence other than the statement of an unbiased expert is valid. The court held that "[it] is well established that an administrative decision-maker is entitled to prefer documentary evidence over the applicant's evidence although the decision-maker must explain in clear and unmistakable terms why it preferred the documentary evidence" (¶26).

On all other bases upon which the officer came to the conclusion that the applicant was inadmissible, the court held that they were consistent with the Supreme authorities, especially in *Suresh* and *Mugesera*. Accordingly, it dismissed the application for judicial review.

Patents and Trademarks – Amended Regulations for Small Entities

A variety of regulations, specifically the *Patent Rules*, the *Trade-marks Regulations* (1996), the *Industrial Design Regulations*, the *Integrated Circuit Topography Regulations* and the *Copyright Regulations*, have been amended to provide greater incentives to entities employing 50 or fewer employees to make use of less expensive intellectual property protection schemes. These organizations (which along with universities are now designated as "small entities") have been permitted since 1985 to pay reduced fees, amounting to savings of up to $3,000 over the life of a patent. However, since a Federal Court decision in 2003, organizations taking advantage of that scheme have also been exposed to an increased risk that they would lose their patent protection. The new amendments are intended to reduce or eliminate that risk.

Prior to the Federal Court of Appeal decision in *Dutch Industries Ltd. v. The Commissioner of Patents, Barton No-Till Disk Inc. and Flexi-Coil Ltd. (Dutch Industries)* the Canadian Intellectual Property Office (CIPO) permitted patent holders who were found to have mistakenly registered under the small entity regime to "top-up" their payments and thereby preserve their patent protection. In *Dutch Industries* it was determined that CIPO did not have the authority to accept such payments. The result of that decision was that anyone who had registered a patent under the small entities regime now faced the risk of losing patent protection in the event of a successful challenge. One result of that change was that small entities now account for only 11 percent of patent applications received by CIPO, as opposed to 22 percent in 2000.

A provision was earlier enacted providing the possibility of retroactive relief for patent holders who, prior to February 1 2006, had incorrectly paid the small entity fees. These new amendments make a number of adjustments, most notably providing a means for entities which in future initially pay the wrong fees to correct this error and retain their patent protection. The regulations require that the patent holder had paid the small entity fee in good faith, and that a time be fixed for the payment of the difference in fees.

Privacy Commissioner – Annual Report

The Office of the Privacy Commissioner released its Annual Report for 2006, noting some trends in the number and types of complaints brought, and the sectors from which those issues originate. There was an increase in the number of *PIPEDA*-related inquiries in 2006, going from 5,685 in 2005 to 6,050 inquiries. The report notes that even with this 6.4% increase there has been an overall decline in inquiries since 2003, when there were 12,132 inquiries. The report speculates that the decline in inquiries is attributable to greater familiarity on the part of Canadian organizations and individuals with the terms of *PIPEDA*.

Although inquiries have declined, the number of complaints under *PIPEDA* increased from 400 in 2005 to 424 complaints in 2006. Within that overall increase, however, the Commission noted that the number of complaints against financial institutions, insurance companies and the transportation sector, which have been subject to *PIPEDA* since 2001 declined slightly. This was in contrast to sectors such as the retail and accommodation sectors, which have been subject to *PIPEDA* only since 2004 and which were the source of substantially more complaints than in previous years.

Of these complaints 309 were closed, compared to 401 in 2005. Only five percent of the complaints were deemed to be well-founded – that is, the Commissioner made a finding that an organization had failed to respect *PIPEDA* – compared to 21 percent which were ultimately found not to be well founded. However, 20 percent of the cases were resolved by an organization committing to take corrective action during the investigation, nearly double the number in 2005. Taking into account further cases which were resolved even before a

formal investigation was begun and those in which a settlement was negotiated, 51 percent of cases were closed without the need for a hearing. The percentage of settled cases dropped by 13 per cent compared to last year, but this category still constituted the largest portion of closed cases.

Self-reported data breaches by organizations increased by 41 per cent in 2006. The Commission suggested this increase was due to an increased awareness by the private sector of the responsibilities that come with maintaining customers' personal information.

The report also notes that preliminary letters of findings were introduced in 2006, by which letters were sent to complainants and respondents in cases of a likely contravention of *PIPEDA*. These letters contained specific recommendations and required the private sector organization to respond by a specified deadline. Twenty-six such letters were sent out in 2006, of which 21 resulted in the organization agreeing within the deadline to comply with the Commissioner's recommendations. The Commissioner referred the other five cases to litigation, which resulted in the organizations choosing to comply. The report notes that financial institutions and insurance companies each accounted for roughly one-quarter of the letters sent, speculating that this was due to the generally large size of financial and insurance organizations and the significant amount of personal information they collect. Typically these letters recommended fine-tuning of existing privacy policies and procedures, rather than dealing with a complete absence of procedures. In contrast nine letters were sent to organizations which had only become subject to *PIPEDA* in 2004, and these recommendations generally involved setting up privacy policies and procedures such as designating a privacy officer, training staff, and developing information for customers.

The report also noted that the average time it took to deal with a complaint in 2006 rose by five months to a period of 16 months. The Commission attributed this delay partly to the increased complexity of some investigations and partly to delays caused by the new process of sending preliminary letters of findings, but suggested that most of the increase was due to staff shortages.

Unreasonable Search – Use of a High Power Flashlight

The British Columbia Supreme Court has decided in *R. v. Grunwald* that the use of a high power flashlight in order to see through tinted windows constitutes an unreasonable search violating section 8 of the *Charter*. The accused was stopped at a police checkpoint at 11:00 p.m., in a location the police had chosen because there was enough overhead lighting to operate without flashlights. He was driving a pick up truck with a canopy over the rear cargo area, and the canopy had darkly tinted windows on all sides. While one officer asked the accused for his license and insurance, a second officer walked to the rear of the vehicle to check the license sticker. That second officer detected a smell of marijuana from the vehicle, but was unable to see through the tinted windows into the cargo area with his unaided eye. He therefore shone his flashlight into the cargo area and testified that in there he saw several garbage bags, one of which was open to reveal Ziploc bags containing marijuana bud. The accused was placed under arrest. At trial he argued that the police had violated his section 8 right by shining the flashlight into the cargo area.

The trial judge accepted that the accused had a reasonable expectation of privacy in the totality of the circumstances. The accused was present at the time of the search, had possession and control of the area searched, and both subjectively and objectively there was a reasonable expectation of privacy. The cargo area was concealed from view in normal conditions, and it was only through the use of a high power flashlight equivalent to a car's headlight that the police were able to see in. This was an intrusion of territorial privacy. The trial judge noted that in *R. v. Wong* the Supreme Court had held that individuals were entitled to protection against any means of technology through which police might intrude on privacy. Although the flashlight in this case was a low level of technology and not as intrusive or penetrating as something like an x-ray, the same principle applied. It was not like looking through clear glass: without using some device the officer would have been unable to see into the accused's private space. Accordingly the officer had engaged in a search, and since it was conducted without a warrant and was not incidental to the purpose of the vehicle stop it was an unreasonable search.

The trial judge concluded, however, that admission of the evidence would not be harmful to the reputation of the administration of justice, and declined to exclude it under s. 24(2).

2ième partie

Production en preuve de copies de sauvegarde d'un système informatique

Bouchard, pdg de l'entreprise SIDO, a été destitué de ses fonctions. Il prétend avoir été victime d'un complot et conteste sa destitution et son congédiement par un recours en oppression en vertu de la Loi canadienne sur les sociétés par actions. Lorsqu'il était pdg, les copies de sauvegarde ou copies miroir du système informatique de SIDO lui étaient confiées de façon préventive et à des fins conservatoires. SIDO revendique ces copies de sauvegarde et en demande la remise immédiate alléguant son droit de propriété et Bouchard riposte par une requête fondée sur les articles 2, 20, 46 et 402 C.p.c. et demande que les copies de sauvegarde soient confiées à un fiduciaire indépendant afin qu'elles soient conservées et que les parties puissent y avoir accès afin de procéder aux expertises appropriées.

Selon le tribunal, une copie de sauvegarde ou une copie miroir d'un disque dur est un ensemble de documents technologiques au sens de la *Loi concernant le cadre juridique des technologies de l'information*. Il serait donc entre les mains d'une partie et non d'un tiers, tel que visé par l'article 402 alinéa 1 C.p.c. Un document en possession d'une partie n'est pas un élément matériel de preuve prévu à l'alinéa 2 de l'article 402 C.p.c. et la procédure adéquate pour en obtenir communication est plutôt le *subpoena duces tecum*, à condition que l'on sache que le document existe. Ce que veut Bouchard, c'est conserver les copies de sauvegarde afin de procéder à une « expertise », soit explorer le contenu de toute la documentation afin de découvrir des éléments de preuve pertinents à sa demande.

Le droit québécois, souligne le tribunal, est silencieux en matière de communication préalable d'éléments de preuve sur support électronique, ce qu'on appelle le *e-discovery*, ce qui est surprenant étant donné que le Québec a été la première juridiction à promulguer une loi concernant le cadre juridique des technologies de l'information. Les conditions de l'ordonnance Anton Piller ne sont pas réunies ici. En fait, la procédure de Bouchard a des allures de saisie avant jugement pour rechercher des éléments de preuve, ce qui est interdit. Mais il existe un intérêt à ce que le contenu d'un serveur soit conservé afin de démontrer qu'un document a déjà existé et qu'il a été détruit. Les pouvoirs du tribunal étant étendus en vertu du recours en oppression intenté en vertu de la Loi canadienne sur les sociétés par actions, il rend des ordonnances de sauvegarde des droits des parties. Il ordonne à Bouchard de remettre à SIDO les copies de sauvegarde, de ne pas les reproduire ni d'en conserver de duplicata. Il ordonne à SIDO de ne pas altérer de quelque façon que ce soit l'intégrité des copies de sauvegarde.

Commentez cet article au Blogue de IT.CAN

- *Bouchard c. Société industrielle de décolletage et d'outillage (SIDO) ltée*, Cour supérieure du Québec, 2007 QCCS 2272, 16 mai 2007.

Ordonnance pour cesser d'endommager et d'interférer le réseau de Bell

Pour fournir son service de téléphonie par voie IP, Vidéotron déconnecte les fils téléphoniques préexistants dans la résidence de l'ancien abonné du réseau de Bell et les relie à son réseau de câbles. Le déconnexion s'effectue de deux façons, selon que le filage intérieur est connecté par un protecteur ou qu'il soit par un « Network Interface Device » (NID). Dans un cas comme dans l'autre, les techniciens de Vidéotron ouvrent les couvercles des boîtiers pour déconnecter le filage de l'abonné du réseau de Bell afin de connecter l'abonné sur son propre réseau. Bell affirme que cela constitue une interférence dans les composantes de son réseau. Bell demande l'émission d'une ordonnance d'injonction interlocutoire contre Vidéotron avant le procès au fond sur son action en injonction permanente et en dommages par laquelle elle requiert qu'il soit ordonné à Vidéotron de cesser d'endommager et d'interférer avec son réseau jusqu'au jugement final.

Le tribunal rejette la requête en injonction interlocutoire. Il y a apparence de droit clair en ce qui concerne les droits de Bell sur le filage lui appartenant dans le NID. Mais le vrai problème ne se situe pas dans le NID mais au niveau des protecteurs;

le filage intérieur a été coupé à l'intérieur du 30 centimètres du point le plus près du protecteur, partie du filage dont Bell revendique la propriété mais n'a pas établi son droit. Le tribunal est satisfait de l'existence d'une question sérieuse à juger. La question est technique, complexe et se pose dans un milieu hautement réglementé par le CRTC.

Cependant, il n'y a pas de préjudice irréparable. Il n'y a pas de preuve que les actions de Vidéotron « empêchent irrémédiablement » Bell d'offrir les services qu'elle s'est contractuellement engagée à fournir à ses client ou que Bell aurait perdu des clients à cause de la façon dont les déconnexions auraient été effectuées. Bell est facilement en mesure de reconnecter les abonnés de Vidéotron à son réseau même si le filage intérieur de l'abonné est coupé. Bell est capable de quantifier ses dommages le cas échéant et Vidéotron est en mesure de répondre à toute condamnation en dommages s'il y a lieu. Le tribunal n'est pas convaincu que Bell subira un préjudice irréparable et sérieux si l'injonction interlocutoire n'est accordée, ni que le préjudice qu'elle pourrait subir ne pourra être compensé adéquatement par le jugement final.

- *Bell Canada c. Vidéotron ltée*, Cour supérieure, 2007 QCCS 2478, 24 mai 2007.

La sécurité des opérations bancaires par Internet

Partant du constat que les services bancaires en ligne sont désormais aussi complets que ceux qui sont proposés en succursale, les auteurs passent en revue les problématiques liées à la sécurité des transactions bancaires pour ensuite examiner les approches de solution aux défis posés par la sécurisation des services bancaires en ligne. Ils concluent que les initiatives juridiques et techniques mises en place en vue d'assurer une plus grande sécurité des transactions n'offrent pas de solutions parfaites. Ce serait le manque d'encadrement juridique des activités des autorités de certification qui laisserait planer un doute sur le réel degré de secret offert. Dans une seconde partie, l'étude passe en revue des modèles de mécanismes de supervision des autorités de certification pour ensuite traiter des responsabilités des certificateurs et des banques.

- Marc LACOURSIÈRE et Édith VÉZINA, « La sécurité des opérations bancaires par Internet », [2007] 41 *Revue juridique Thémis* 89-156.

Diffusion de l'image d'une personne sur Internet via "Google Street View"

La nouvelle fonction intégrée début juin dans l'outil Google Maps permettant de voir des rues à hauteur d'homme, soulève des craintes relativement à la vie privée. Aux États-Unis et au Canada anglophone, il est généralement admis qu'il est licite de prendre des images d'un lieu public comme une rue et de les diffuser. Par contre au Québec, la situation est différente. L'article 36 du *Code civil du Québec* dispose que peuvent être notamment considérés comme des atteintes à la vie privée d'une personne les actes suivants : « *[...]* 3° Capter ou utiliser son image ou sa voix lorsqu'elle se trouve dans des lieux privés; 4° Surveiller sa vie privée par quelque moyen que ce soit; 5° Utiliser son nom, son image, sa ressemblance ou sa voix à toute autre fin que l'information légitime du public. »

Avant la décision *Aubry c. Vice Versa* ([1998]1 RCS 191), il était généralement tenu pour acquis que, pour déterminer si la diffusion d'une image était fautive, il fallait établir qu'elle portait sur la vie privée d'une personne. Mais selon la décision Aubry, la diffusion de l'image est en soi fautive, sauf si on est en mesure d'établir un motif d'intérêt public. Il faut, à tout coup, démontrer un motif légitime de publier l'une ou l'autre de ces image. Le droit d'une personne de s'opposer à la diffusion de son image ne s'arrête plus aux confins de sa vie privée : il prévaut aussi longtemps que l'intérêt public à la publication n'a pas été démontré. Avec une telle règle, il est difficile de postuler que la captation et la diffusion d'images de personnes identifiables sur un site web, comme dans "Google Street View" est a priori licite.

Commentez cet article au Blogue de IT.CAN

Sur les enjeux juridiques du déploiement au Québec de "Google Street View" :

- Voir Paul JOURNET, *Google Street View au Québec*?, Technaute, 8 juin 2007.

Sur la diffusion de photos sur Internet au Québec :

- Voir *Société des casinos du Québec c. Boyer*, 2005 IIJCan 7808 (QC C.S.), 500-05-062084-007, 2 mars 2005. (Résumé dans *Bulletin IT.Can*, 14 avril 2005)

Sur les règles applicables en matière de protection de l'image diffusée sur Internet en France :

- Voir Philippe BELLOIR, *La protection de l'image publiée sur Internet–À propos de l'arrêt de la Cour d'appel de Lyon du 27 janvier 2005 FathiaX…c/SA Société G…*, Juriscom.net, 11 avril 2005.

Sur l'utilisation des caméras de surveillance dans les lieux publics :

- La CAI rappelle que tout projet d'utilisation de caméras de surveillance avec enregistrement doit respecter *Les règles d'utilisation de la vidéosurveillance avec enregistrement dans les lieux publics par les organismes publics*, 9 juin 2004.
- Voir aussi Laurent BILODEAU, *Rapport final d'enquête concernant l'installation de caméras de surveillance par le Service de police de la ville de Montréal*, 23 février 2005. (Résumé dans *Bulletin IT.Can,* 14 avril 2005).

Surveillance automatisée des réseaux P2P – France

Le Conseil d'Etat a annulé la décision du 18 octobre 2005 de la Cnil (Commission nationale de l'informatique et des libertés) qui refusait d'autoriser quatre sociétés de gestion collective du secteur musical (Sacem, SDRM, SCPP et SPPF) à mettre en place une collecte automatique des adresses IP des contrefacteurs pour surveiller les réseaux « peer to peer » et y constater les contrefaçons d'oeuvres musicales.

Le système soumis à la Cnil prévoyait deux phases. Après avoir identifié les internautes qui mettaient gratuitement en ligne moins de 50 fichiers musicaux, grâce à une sélection d'adresses IP résultant des requêtes sur les réseaux P2P, ceux-ci recevaient un message d'avertissement leur signalant les conséquences juridiques de la pratique de la contrefaçon. Les internautes ayant pendant cette première phase mis à disposition plus de 50 fichiers musicaux à des tiers étaient ensuite sélectionnés pour faire l'objet d'un contrôle renforcé pendant une période de quinze jours, consistant en une surveillance des intéressés qui une fois les preuves réunies, auraient pu faire l'objet de poursuites civiles ou pénales.

Un tel système consistait en un traitement automatisé portant sur des données relatives aux infractions et nécessitant l'autorisation préalable de la Cnil. La Cnil a refusé l'autorisation, entre autres sur le fait *« que l'envoi de messages de prévention passait par une identification des internautes via leur adresse IP par les fournisseurs d'accès servant de relais aux envois. Or, selon la Commission, les fournisseurs d'accès ne peuvent conserver les données de connexions des internautes à cette fin et leur identification n'est possible que dans le cadre d'une procédure judiciaire. Elle s'appuyait également sur le fait que la généralisation et l'importance de la collecte de données à caractère personnel envisagée n'étaient pas proportionnées à la finalité poursuivie, la recherche et la constatation de mise à disposition illégale d'œuvres musicales. La CNIL reprochait encore aux sociétés de s'être réservées la fixation du nombre d'infractions constatées au-delà duquel des actions seraient engagées et la révision unilatérale de ce seuil. »*

Le Conseil d'État a conclu, dans sa décision du 23 mai 2007, que la Cnil a entaché sa décision d'une erreur d'appréciation en estimant que les traitements envisagés conduisaient à une surveillance exhaustive et continue des fichiers des réseaux d'échanges et donc disproportionnée par rapport à la finalité poursuivie. Elle ne pouvait aussi légalement refuser d'accorder les autorisations au motif que les traitements reposaient uniquement sur des critères quantitatifs en l'absence de toute disposition législative en ce sens. Elle a également commis une erreur en estimant que les critères quantitatifs étaient dépourvus de pertinence eu égard à la finalité envisagée. Cependant le Conseil d'État approuve la Cnil qui avait réprouvé les envois de messages pédagogiques. La diffusion de ces messages n'avait pas pour but la mise à disposition d'informations à l'autorité judiciaire pour le besoin d'une poursuite pénale, condition prévue pour la conservation des données de connexion.

Commentez cet article au Blogue de IT.CAN

- Yann TESAR, *Le Conseil d'État s'oppose à la CNIL sur la surveillance des réseaux P2P par les sociétés de gestion collective*, Juriscom.net, 25 mai 2007.
- *Le Conseil d'État censure la Cnil sur le peer to peer*, Legalis.net, 24 mai 2007.
- *Sacem et autres/Cnil*, Conseil d'État, Section du contentieux, 23 mai 2007.

À signaler

- Nicolas SAMARCQ, *Le contrôle des messageries électroniques professionnelles*, LEXagone.com, 31 mai 2007.
- Aurélie TAIEB, *La liberté d'expression est-elle garantie sur Internet?*, Juriscom.net, 6 juin 2007.
- Forum des droits sur l'Internet, *Rapport de synthèse–Consultation publique des internautes*, 7 juin 2007.

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 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 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.