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

June 15, 2009/15 juin 2009

IT.Can NEWSLETTER/BULLETIN

Canadian IT Law Association

www.it-can.ca

Part 1 of this newsletter is prepared by Professors Robert Currie, Chidi Oguamanam and Stephen Coughlan of the Law and Technology Institute of Dalhousie Law School. Part 2 of this newsletter is prepared by Professors Pierre Trudel and France Abran of the L.R. Wilson Chair in Information Technology and Electronic Commerce Law, Université de Montréal.

Les auteurs de la première partie du présent bulletin sont les professeurs Robert Currie, Chidi Oguamanam et Stephen Coughlan de l'Institut de droit et de technologie de la Faculté de droit de l'Université de Dalhousie. Les professeurs Pierre Trudel et France Abran de le Chaire en droit des technologies de l'information et du commerce électronique L.R. Wilson de la Faculté de droit de l'Université de Montréal ont rédigé la seconde partie du présent bulletin.

Part 1

Admissibility of Traffic Camera Images

The British Columbia Provincial Court considered the rules governing the admissibility of images obtained from a traffic camera in *R. v. Eged* (May 28, 2009, no electronic citation available). The accused was charged with having driven through a red light, and the evidence against him consisted of a photograph taken by a traffic camera, introduced by way of certificate evidence in accordance with the British Columbia *Motor Vehicle Act*. In particular the accused argued that the evidence did not comply with the proper provisions of the *Act*, and that he could not be convicted when the license plate number was not legible in the photograph.

The *Act* contained, in section 82, provisions relating to the admission by certificate of evidence, including evidence which had been converted to electronic format. The evidence in the case had be admitted under that section, and the trial judge found that having been admitted, the certificates established the accused's guilt unless he showed evidence to the contrary. The accused produced no evidence to the contrary, but argued that compliance with section 82 was not sufficient. He argued that as section 82.1 contained provisions which were specific to the admission of electronic images obtained through a traffic camera, the certificates were only admissible if that particular provision was relied upon. The trial judge, however, rejected this argument, and held that it was sufficient for the Crown to tender documents pursuant to s. 82 despite the availability of a more specific provision. The trial judge did not accept the argument that this approach rendered the more specific provision redundant.

The accused also argued that he could not be convicted when the photograph was not clear enough to allow the license plate to be read. An enforcement officer had studied the captured image in the photo with a magnifying glass, had read its license number, and had prepared the certificate based on that reading. The accused argued that the illegibility of the licence plate could not be saved by an Enforcement Officer's certification. The trial judge, however, concluded that the statutory scheme did not require that the judge hearing the dispute must personally be able to read the photograph and make out the licence plate and the jurisdiction. Rather, the statutory scheme calls for an enforcement officer to be in a position to sign and complete a certificate stating that she has determined the licence plate number and that it was issued in the particular jurisdiction. That occurred in this case, and therefore the evidence was sufficient for the accused to be convicted.

Covert Video Surveillance by Private Investigator

The Privacy Commissioner of Canada received a complaint from a woman who (along with her daughter) was videotaped in a public place during a covert video surveillance operation on the woman's sister. The covert surveillance was being conducted by the sister's insurance company in connection with a claim arising out of a motor vehicle accident. The complainant also became aware that there was a surveillance report concerning her sister which reported her and her daughter's activities, including her license plate number, as well as videos and photographs which she had not consented to.

The woman filed a complaint against the private investigation firm that the insurance company had hired.

The Privacy Commissioner discovered that the private investigation firm had not intended to capture information about the complainant, and that this information had been obtained inadvertently as a result of the investigation into the sister. The firm conceded that they had no policy to deal with private information collected accidentally concerning third parties, but defended their actions as not violating the *Personal Information Protection and Electronic Documents Act* (PIPEDA). In particular they claimed "that the circumstances of the complainant's case fell outside the scope of the *Act*; that the *Act* allows collection of information of an individual without his or her consent if the collection is reasonable for an investigation of a breach of agreement or a contravention of laws (paragraph 7(1)(b)), and; that it was not reasonable to expect to obtain the consent of all parties whose information was inadvertently caught on videotape during an investigation." In addition the private investigator did not wish to have to blur the images of individuals accidentally recorded during video surveillance.

The Privacy Commission concluded that the complaint was well-founded. They noted that paragraph 7(1)(b) allows an organization to collect personal information without the knowledge or consent of the individual only if it is reasonable to expect that the collection with the knowledge or consent of the individual would compromise the availability or the accuracy of the information and the collection is reasonable for purposes related to investigating a breach of an agreement or a contravention of the laws of Canada or a province. That provision would permit private investigation firms to conduct video surveillance in certain situations and of certain people. However, in this particular instance the private investigation firm conceded that the information concerning the complainant and her daughter was not relevant to the investigation and had been collected inadvertently, and so it did not fall within the exception. The firm had also refused to blur the complainant and her daughter's faces in the images they had obtained, and had refused to comply with the Commission's recommendation that they depersonalize similar information in future cases. Accordingly the complaint was well-founded.

Covert Video Surveillance – Privacy Commissioner's Guidelines

The Privacy Commissioner of Canada has issued guidelines for the use of covert video surveillance. These guidelines are a companion to previously issued guidelines on overt video surveillance in the private sector.

The guidelines note the common misconception that when covert video surveillance occurs in a public place, no privacy-related obligations arise. The Commission notes that any collection of personal information taking place in the course of commercial activity by an organization subject to PIPEDA must comply with the Act, regardless of the location where the collection takes place.

In deciding whether the collection, without consent, of information by way of covert video surveillance will be in compliance with PIPEDA, the Commission recommended that organizations consider a number of factors. First, there must be a demonstrable need for collecting that information, which would require that the organization has a strong basis to support the use of covert video surveillance as a means of collecting personal information. There must be a legitimate business purpose and objective, and a strong likelihood that collecting the personal information will help the organization achieve that objective. Second, the organization must balance the need for the information against the individual's loss of privacy, to be certain that the loss of privacy is proportional to the benefit gained: it will not be enough simply that covert video surveillance offers the greatest benefit to the organization. Finally, the organization should consider the use of less intrusive means first.

The Commission also discussed the general rule that consent is required for the collection of personal information. They concluded that implied consent might sometimes be found: for example "an individual can be considered to have implicitly consented to the collection of their personal information through video surveillance if that

individual has initiated formal legal action against the organization and the organization is collecting the information for the purpose of defending itself against the legal action." However, often covert video surveillance will take place without consent. In such cases, compliance with paragraph 7(1)(b) would be necessary, which requires that "collection with the knowledge and consent of the individual would compromise the availability or accuracy of the information; and the collection is reasonable for purposes related to investigating a breach of an agreement or a contravention of the laws of Canada or a province." This exception might allow the collection of information about a third party without his or her consent, if collection of that information is relevant to the investigation. However, often information about third parties will not be relevant, and so such information should be deleted or depersonalized as quickly as possible. This would involve the use of blurring technology when required.

The Commission also recommended that organizations have a policy on the use of covert video surveillance dealing with the purposes for which it can be undertaken, who can authorize it, how information will be stored, and so on, as well as a practice of documenting use, including a description of alternative measures taken, who viewed the surveillance and what it was used for, how the images were disposed of, and other questions. In addition the Commission recommended best practices for using private investigation firms. These included a number of specific recommendations, including:

- confirmation that the private investigation firm constitutes an "investigative body" as described in PIPEDA "Regulations Specifying Investigative Bodies";
- an acknowledgement by the hiring organization that it has authority under PIPEDA to collect from and disclose to the private investigation firm the personal information of the individual under investigation;
- confirmation by the private investigation firm that it will collect personal information in a manner consistent with all applicable legislation, including PIPEDA;
- confirmation that the private investigation firm provides adequate training to its investigators on the obligation to protect individuals' privacy rights and the appropriate use of the technical equipment used in surveillance;
- a provision prohibiting the use of a subcontractor unless previously agreed to in writing, and unless the subcontractor agrees to all service agreement requirements;
- a provision allowing the hiring company to conduct an audit.

Domain Name Disputes

"forsale.ca": Reverse Domain Name Hijacking

In *Globe Media International Corporation v. Bonfire Development Inc.*, a 3-member CIRA panel (Josefo, Macramalla and Lametti, Chair) heard a dispute regarding the domain name forsale.ca—and issued "what appears to be the first ever case of reverse domain name hijacking involving a .ca domain" (L. Benetton, "Panel makes finding of reverse domain name hijacking", *The Lawyers' Weekly,* Vol. 29, No. 5 (5 June 2009)). The Complainant ("Globe") is Canadian corporation with offices in Toronto, Ontario, which registered the trademark WWW. FOR-SALE.CA on 21 January 2005. The Registrant ("Bonfire") is a Canadian corporation with offices in Calgary, Alberta. Bonfire purchased the domain name for $30,000 from one Tom Brown on 12 January 2009; Brown had registered the domain name after it expired on 3 January 2009. Both Brown and Bonfire had ignored Globe's requests to purchase the domain name.

The Panel first considered whether the domain name was "confusingly similar" to Globe's mark under 4.1(a) of the CIRA Policy. It easily ruled that, shorn of the non-distinctive elements "www", ".ca" and the hyphen, "the domain name and the trade-mark are identical in appearance, sound and in the ideas suggested" and thus was confusingly similar (para. 24). The Panel then assessed whether the domain name had been registered "in bad faith" per the criteria in 3.7 of the Policy. It took note of the fact that Bonfire or related parties had been found in the past to be engaged in cyber-squatting, of which it disapproved. However, as to whether Bonfire was cyber-squatting in this particular case, the Panel

answered in the negative. It held that the domain name was:

> a generic term over which the Complainant in this particular case cannot claim exclusivity. This is so despite being the owner of a trade-mark registration that is confusing with the domain name. The term "for sale" is clearly and obviously a commonly used term by businesses and members of the public to say the least, and is one over which the Complainant would be hard pressed to assert a monopoly (para. 27).

While descriptive or generic domain names could still be found to have been registered in bad faith, forsale.ca was "so clearly generic that its registration cannot be seen as being registered in bad faith" (para. 29). Accordingly, the Panel ruled that the registration was not made in bad faith.

For completeness, the Panel also assessed whether Bonfire had a "legitimate interest" in the domain name, which it pointed out is an inquiry which "tries to find some more or less objective or ascertainable link between the Registrant and the domain name in question, aside from mere registration and which is legitimate" (para. 32). The Panel ruled that Globe had not provided sufficient evidence to indicate that Bonfire had no legitimate interest, as it was required to do under the Policy. The domain name was generic, and the fact that it had not yet been used for a commercial or other purpose was irrelevant. Accordingly, the Panel held that Bonfire had a legitimate interest, and that the Complaint overall was dismissed.

In the most interesting development, Bonfire requested that the Panel make a ruling against Globe for the practice of "reverse domain name hijacking." This formally comes under 4.6 of the Policy, which provides that the Panel can award costs against a Complainant where the Complaint was brought "for the purpose of attempting, unfairly and without colour of right, to cancel, or obtain a transfer of any Registration which is the subject of the Proceeding." The phrase "reverse domain name hijacking" refers, *inter alia*, to the practice of registering a mark and using the rights in the mark to attempt to wrest a domain name from its legitimate owner. The Panel noted that to support such a finding, it would have to rule that the Complaint itself was brought in bad faith.

The Panel stated that while typically the presence of a confusing trademark was sufficient to defeat claims of reverse domain name hijacking, it should also consider the conduct of the Complainant and the nature of the domain name. It noted that Globe had previously registered a number of domain names which reflected well-known trademarks (such as versace.ca and mentos.ca) and had registered trademarks containing the corresponding domain names. It thus concluded that Globe was engaged in reverse domain name hijacking, in a paragraph worth setting out in its entirety:

> The Panel concludes that the Complainant sought to register these trade-marks in an attempt to legitimize the corresponding and previously registered domain name registrations. This constitutes a serious and profound abuse of the trade-mark regime and its intended purpose to serve the public. This, when coupled with the initiation of proceedings under the Policy in connection with a clearly generic domain name, represents an alarming pattern of behaviour on the part of the Complainant. Under the circumstances, the foregoing negates any possible argument of colour of right. The mere fact of having a registered trade-mark in this case is insufficient to establish a colour of right on the part of the Complainant given its egregious conduct. For lack of a better term, the Complainant appears to have engaged in filching (para. 41).

The Panel expressed its willingness to order against Globe the up to $5,000 in costs provided for in 4.6 of the Policy, noting that this was the first imposition of such an extraordinary remedy but "the extraordinary behaviour of the Complainant cannot be tolerated or endorsed by the Panel, and merits a ruling on costs" (para. 43). It directed Bonfire to make submissions as to costs, including legal fees paid and disbursements, prior to the order being made.

2ième partie

La vidéosurveillance intelligente : promesses et défis

Publié conjointement par le Centre de recherche informatique de Montréal CRIM et Technopôle Défense et Sécurité, ce rapport de recherche dresse un portrait détaillé de la technologie de la vidéosurveillance intelligente destinée à la sécurité des personnes et des lieux. Il s'intéresse également au marché de la sécurité publique et civile et aux possibilités que ce dernier offre pour la vidéosurveillance intelligente.

- Valérie GOUAILLIER (CRIM) et Aude-Emmanuelle FLEURANT (Technopôle Défense et Sécurité), *La vidéosurveillance intelligente : promesses et défis : rapport de veille technologique et commerciale*, mars 2009.

Deux dispositions de la Loi HADOPI censurées par le Conseil constitutionnel – France

Le 10 juin 2009, le Conseil constitutionnel, gardien des droits et libertés constitutionnellement garantis, a rendu sa décision n° 2009-580 DC, à l'égard de la *Loi favorisant la diffusion et la protection de la création sur Internet*. Un groupe de parlementaires avait saisi le Conseil sur les articles 5, 10 et 11 de la loi. Le Conseil a jugé que deux articles de la loi contreviennent aux droits constitutionnels garantis.

L'article 5 de la loi crée la « Haute Autorité pour la diffusion des oeuvres et la protection des droits sur Internet » (HADOPI). La commission de protection des droits de cette Autorité a pour mission de mettre en oeuvre les nouveaux mécanismes d'avertissement et de sanction des titulaires d'accès à Internet qui auront manqué à l'obligation de surveillance de cet accès. L'article 11 de la loi définit cette obligation de surveillance. Le Conseil constitutionnel a jugé que plusieurs des dispositions de ces articles 5 et 11 n'étaient pas conformes à la Constitution : *« La liberté de communication et d'expression, énoncée à la Déclaration des droits de l'homme et du citoyen de 1789 [...] implique aujourd'hui, eu égard au développement généralisé d'Internet et à son importance pour la participation à la vie démocratique et à l'expression des idées et des opinions, la liberté d'accéder à ces services de communication au public en ligne. Or les articles 5 et 11 de la loi [confient] à la commission de protection des droits de la HADOPI des pouvoirs de sanction l'habilitant à restreindre ou à empêcher l'accès à Internet à des titulaires d'abonnement. Ces pouvoirs pouvaient donc conduire à restreindre l'exercice, par toute personne, de son droit de s'exprimer et de communiquer librement. Dans ces conditions, le législateur ne pouvait, quelles que soient les garanties encadrant le prononcé des sanctions, confier de tels pouvoirs à une autorité administrative dans le but de protéger les titulaires du droit d'auteur. De tels pouvoirs ne peuvent incomber qu'au juge. »*

Quant à l'article 10 de la loi, il *« confie au tribunal de grande instance le pouvoir d'ordonner les mesures nécessaires pour prévenir ou faire cesser une atteinte à un droit d'auteur ou un droit voisin.* Le Conseil constitutionnel a estimé que *le législateur n'a pas méconnu la liberté d'expression et de communication en confiant ce pouvoir au juge. Il appartiendra à la juridiction saisie de ne prononcer, dans le respect de cette liberté, que des mesures strictement nécessaires à la préservation des droits en cause. »*

Rappelons que l'élaboration de la loi HADOPI contre le téléchargement illégal, a été initiée par le chef de l'État qui avait parrainé les accords de l'Elysée le 23 novembre 2007. Ces accords entre les joueurs de l'industrie musicale et du cinéma, ainsi que les fournisseurs d'accès Internet, acceptaient de mettre en application des recommandations du rapport de Olivennes qui préconisait la «riposte graduée» contre le «piratage»: deux courriels d'avertissement à l'internaute, puis suspension de l'abonnement Internet en cas de récidive. Les avertissements et la suspension devaient être prononcés par la Haute autorité de diffusion des oeuvres et protection des droits sur Internet.

- Voir CONSEIL CONSTITUTIONNEL, Communiqué de presse et Décision n° 2009-580 DC du 10 juin 2009, *Loi favorisant la diffusion et la protection de la création sur Internet*.

- Estelle De Marco, « HADOPI – Analyse du nouveau mécanisme de prévention de la contrefaçon à la lumière des droits et libertés fondamentaux », *Juriscom.net*, 4 juin 2009.

Lignes directrices pour la protection des enfants sur Internet – UIT

Des projets de lignes directrices pour la protection des enfants dans le cyberespace ont été présentés pour discussion le 18 mai à l'occasion de la Journée mondiale des télécommunications et de la société de l'information, dont le thème était cette année «Protection des enfants dans le cyberespace». Ces projets s'inscrivent dans le cadre de l'initiative COP (Child Online Protection) créée sous forme d'un réseau international de collaboration (composé d'institutions des Nations Unies et d'autres partenaires) dont le but est de promouvoir la protection en ligne des enfants dans le monde entier. L'initiative COP repose sur une approche multi-parties prenantes et sur la conviction que chacun - particuliers ou organisations, en ligne ou mobile, éducateur ou législateur, expert technique ou organisme du secteur privé - peut apporter sa contribution.

Puisque les enfants sont de véritables citoyens du numérique dans un univers en ligne ou les frontières semblent s'estomper, il est indispensable que toutes les parties prenantes, y compris les enfants eux-mêmes, réagissent à tout ce qui menace leur bien-être. Ils sont vivement encouragés à apprendre à utiliser les outils en ligne de façon sûre, y compris en installant des pare-feu et des logiciels antivirus et en apprenant à détecter des contenus inhabituels. Les projets de lignes directrices portent sur les droits en ligne des enfants, les contenus préjudiciables et illégaux, les brimades en ligne, les questions de respect de la vie privée et le commerce électronique. Ces lignes directrices postulent que la meilleure défense pour la protection des enfants était de leur faire prendre conscience des risques en ligne et de leur proposer des options et des solutions pour y remédier.

Les parents et les éducateurs devraient collaborer et se familiariser avec les sites Internet que consultent leurs enfants pour décider de ce qui est sûr et approprié en ligne. Les parents sont encouragés à s'informer pour améliorer la sécurité des enfants qui naviguent dans l'univers virtuel et sur Internet. Il est indispensable de connaître les possibilités s'offrant aux enfants en ligne, de même qu'il est essentiel que les parents s'intéressent aux activités de leurs enfants. Les parents doivent être éduqués, responsabilisés et déterminés à faire en sorte que leurs enfants vivent des expériences en ligne réellement bénéfiques; ils doivent parallèlement leur faire prendre de meilleures habitudes pour assurer leur sécurité en ligne.

Un projet de lignes directrices pour les décideurs a aussi été mis de l'avant. Puisque l'Internet est devenu un outil technique qui ouvre à ses principaux bénéficiaires – les enfants et les jeunes – des horizons et des possibilités presque infinis, il est indiqué dans les lignes directrices que les gouvernements ont l'obligation d'assurer la protection des mineurs aussi bien dans le monde réel que dans le monde virtuel. Les gouvernements et les décideurs ont pour mission essentielle de mettre en place un cadre durable à l'intérieur duquel une stratégie nationale et multinationale adaptée pourra être élaborée. Ainsi, l'industrie de l'Internet et les professionnels du secteur auront un rôle important à jouer, en particulier parce que, à la vitesse à laquelle la technologie évolue, un grand nombre de méthodes traditionnelles dans les domaines de l'activité législative ou de la prise de décisions ne sont plus adaptées.

Enfin, le projet de lignes directrices pour le secteur privé reflète le fait que dans plusieurs pays, le secteur privé assume la direction des opérations et adopte des méthodes volontaires d'autorégulation, reflétant sa détermination à réagir de manière responsable à l'utilisation que les enfants font des TIC et des communications en ligne. Il est dans l'intérêt de ce secteur de prendre des mesures et d'anticiper le changement, non seulement parce que c'est la chose à faire du point de vue moral mais aussi parce qu'à longue échéance, cette attitude contribuera à renforcer la confiance du public dans le support que constitue Internet.

- Tiré de : UIT, Communiqué de presse – Lignes directrices proposées pour l'initiative pour la protection en ligne des enfants (COP) – À l'intention des enfants, des parents, des

enseignants, des décideurs et du secteur privé, 20 mai 2009.

- *L'initiative pour la protection des enfants (COP)*
- *Child Online Protection Draft Guidelines*
- *Global Cybersecurity Agenda*

Recommandations de sénateurs pour renforcer les protections de la vie privée sur Internet – France

Partant de la prémisse que le droit à la vie privée est confronté à l'apparition de nouvelles «mémoires numériques », conséquence de nombreuses évolutions ayant pour effet principal ou incident d'augmenter la quantité de collectes de données permettant de suivre un individu dans l'espace et le temps, les sénateurs Yves Détraigne (Marne) et Anne-Marie Escoffier (Aveyron, RDSE) ont déposé un rapport d'information formulant quinze recommandations pour mieux garantir le droit à la vie privée à l'heure du numérique et renforcer ainsi la confiance des citoyens à l'égard de la société de l'information.

Le rapport identifie les facteurs qui portent des menaces globales pour la protection de la vie privée. Il mentionne la recherche d'une sécurité collective toujours plus infaillible, l'accélération des progrès technologiques (géolocalisation, Bluetooth, RFID, nanotechnologies), la tendance à l'exposition de soi et d'autrui sur Internet, au travers notamment des réseaux sociaux sont des facteurs porteurs de tendances constituant des nouveaux défis au regard du droit à la vie privée. Ils observent que le cadre juridique français sur la protection des données personnelles y apporte certaines réponses mais que les règles de droit paraissent relativement inadaptées aux enjeux de la mondialisation et aux spécificités d'Internet. En effet, d'une part, il existe des divergences d'interprétation concernant l'applicabilité du droit communautaire aux traitements de données effectuées par des entreprises situées en dehors de l'Union européenne, en particulier aux États-Unis, d'autre part, Internet pose des questions nouvelles au regard du droit à la vie privée, telles que sa conciliation avec la protection de la propriété intellectuelle, le statut de l'adresse IP, l'inflation de pratiques commerciales «anonymement intrusives », comme la publicité ciblée, ainsi que la difficulté pour les internautes à faire valoir leurs droits.

Au nombre des mesures préconisées, il y a l'imposition d'une redevance aux grands organismes, publics et privés qui traitent des données à caractère personnel; l'introduction dans la loi d'une précision afin de définir l'adresse IP comme une donnée personnelle ; la création d'une obligation de notifier les failles de sécurité informatique à la Commission nationale de l'informatique et des libertés (Cnil) et « compléter les grands principes de la reconnaissance d'un « droit à l'oubli ». Toutefois, le rapport reconnaît « la difficulté de trouver un équilibre entre le droit à l'oubli et la liberté d'expression et d'information» ce qui n'empêche pas les sénateurs de mettre de l'avant une règle en vertu de laquelle « les moteurs de recherche pourraient mettre à la disposition des utilisateurs identifiés des outils qui leur permettraient, même d'une manière imparfaite, de « nettoyer leur passé » en coupant certains liens issus du référencement.

- *La vie privée à l'heure des mémoires numériques. Pour une confiance renforcée entre citoyens et société de l'information*, Rapport d'information de M. Yves DÉTRAIGNE et Mme Anne-Marie ESCOFFIER, fait au nom de la commission des lois n° 441 (2008-2009) – 27 mai 2009.

Consultation publique sur l'Internet du futur – France

Le Gouvernement français a lancé une consultation publique sur l'Internet du futur en vue de recueillir l'avis de l'ensemble des acteurs concernés par ce thème : universitaires, chercheurs, grandes entreprises, PME, société civile... Cette consultation porte notamment sur l'identification des thématiques liées au concept d'Internet du futur (technologies du « cœur de réseau », réseaux d'accès, réseaux spontanés, Internet des objets, contenus, usages et services...), l'organisation de la recherche en France dans ce domaine, la coordination des plateformes d'expérimentation, l'organisation des pôles de compétitivité TICs sur cette thématique, la normalisation, les actions à mettre en œuvre pour

préparer l'industrie française à ces changements importants, etc.

Le ministère de l'Économie, de l'industrie et de l'emploi avait constitué en 2007 un groupe de réflexion sur l'Internet du futur présidé et co-présidé respectivement par l'Institut national de recherche en informatique et automatique (INRIA) et l'Institut Télécom. Ce groupe de réflexion composé d'experts reconnus au niveau international et appartenant à des organismes de recherche, des PME et des groupes industriels travaillant sur ces questions a rendu son rapport, à la mi-juin 2008. C'est à partir de cette base que l'on a souhaité lancer cette consultation publique afin de recueillir l'avis de l'ensemble des acteurs concernés par l'Internet du futur et de préparer un plan d'actions sur le sujet.

- Ministère de l'Économie, de l'industrie et de l'emploi, *Consultation publique sur l'Internet du futur*.
- Ministère de l'enseignement supérieur et de la recherche, *Lancement d'une consultation publique sur l'Internet du futur*.

Utilisation d'une messagerie professionnelle pour critiquer un employeur assimilée à une faute grave – France

Dans un arrêt du 23 février 2009, la cour d'appel de Limoges a considéré que l'utilisation de sa messagerie professionnelle pour diffuser, à un nombre important de collègues, des informations dénigrantes à l'encontre de son employeur constitue une violation de l'obligation de loyauté à laquelle est tenu un employé et est assimilable à une faute grave justifiant un licenciement. Un conseiller commercial de la compagnie d'assurance GPA Vie avait envoyé des courriers électroniques, depuis sa messagerie professionnelle, à plusieurs centaines de salariés de la société pour les inciter à intenter une action en justice à l'encontre de leur employeur. Le contenu de certains de ces envois dénigrait la politique de gestion des sinistres suivie par GPA Vie. Certains destinataires de ces messages les avaient alors transférés à leur supérieur hiérarchique.

Lors de l'entretien préalable au licenciement de ce salarié, le contenu des courriers était au nombre des faits reprochés par la direction. L'employé avait alors saisi les tribunaux en alléguant que l'employeur avait porté atteinte à sa vie privée en accédant sans autorisation à sa messagerie. L'employeur prétendait, au contraire, que toute utilisation de son poste de travail par un salarié est supposée avoir une finalité professionnelle, y compris l'envoi de messages électroniques, à charge pour l'employé d'identifier les dossiers et courriers qu'il considère comme personnels.

Pour les juges de la Cour d'appel, le seul élément qui doit être pris en compte est la possibilité qu'avaient les destinataires des messages litigieux de les divulguer. Ils en déduisent que l'employeur n'a pas violé le secret des correspondances de son salarié. Ils n'ont donc pas accueilli les prétentions de l'employé au sujet d'une atteinte à sa vie privée. Ils ont par contre rappelé que si une utilisation personnelle de la messagerie professionnelle peut être tolérée, elle devient fautive « dès lors qu'elle est habituelle voire systématique ».

- Tiré de : Utilisation de sa messagerie professionnelle pour dénigrer son employeur : faute grave, *LEGALIS.NET*, 5 juin 2009.
- *François L. c. Generali Vie,* Cour d'appel de Limoges, Chambre sociale, Arrêt du 23 février 2009.

Un appel au boycott mène à une condamnation pour dénigrement – France

La société ASW avait appelé au boycott d'un concours de Miss Pole Dance co-organisé par son concurrent Ponthieu Invest. Le tribunal de commerce de Paris, dans une décision du 3 avril 2009 a jugé que ce comportement a jeté le discrédit sur l'événement et constitue une faute de dénigrement constitutif de concurrence déloyale.

ASW qui avait refusé de participer à cette manifestation a lancé une campagne de boycott sur son site Internet au moyen d'un communiqué que le tribunal a jugé dénigrant. Les magistrats ont estimé que son contenu dépassait de loin le droit d'exercice normal d'une critique professionnelle dans le cadre d'une concurrence même rude. Ainsi, le fait d'employer le terme « sulfureux » à

plusieurs reprises a été considéré comme jetant publiquement le discrédit sur cette manifestation. ASW a par ailleurs porté atteinte à la réputation de son concurrent direct et s'est attribué subtilement des qualités déniés à Ponthieu Invest. Les juges ont aussi décidé qu'il fallait porter à la connaissance du public la condamnation pour dénigrement. Ils ont donc ordonné à ASW de reproduire le dispositif du jugement précédé du titre « condamnation pour dénigrement » sur son site et dans trois publications pour une somme de 10 000 euros.

- Tiré de : Appel au boycott en ligne : condamnation pour dénigrement, *LEGALIS. NET,* 2 juin 2009.
- *Ponthieu Invest / ASW Inc.*, Tribunal de commerce de Paris, 15ème chambre, Jugement du 3 avril 2009.

À signaler

- Guylaine HENRI, Les conflits juridictionnels : le point de vue des acteurs, présenté à l'Institut canadien d'administration de la justice, 8 mai 2009, Commission d'accès à l'Information du Québec. L'auteure présente les conflits de compétence auxquels la Commission d'accès à l'information a été confrontée..