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

January 15, 2010/15 janvier 2010

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

Commercial Litigation: Website Injunction Denied

In *Belron Canada Inc. v. TCG International Inc.*, the British Columbia Court of Appeal ruled on a lower court decision denying the plaintiff Belron's application for an interim injunction, which would have restrained the Defendant TCG from operating the website windshields.com "in relation to the Canadian automobile glass repair or replacement business" (para. 1). The website was geared towards referring consumers to glass dealers in the U.S., Quebec and (as had been proposed by TCG) throughout Canada. Belron's position in the underlying litigation was that the use of the website breached a 2005 contact between the parties, whereby Belron had purchased TCG's Canadian assets, which included clauses of non-competition, non-solicitation and non-interference. TCG had made the website operative in 2007.

In her decision the motion judge held that Belron had made out a strong *prima facie* case of breach. However, on the latter two requirements for granting an injunction, she held that there was insufficient evidence of either irreparable harm to Belron's substantial market presence in Canada; moreover, as to this kind of web-based business initiative, the balance of convenience favoured TCG:

> At this time, the Website is the only one of its kind in Quebec and there is no Website like it operating in the rest of Canada. There are, however, several other companies that operate websites along the same lines as the Website in the United States. The defendants argue that any impediment to the Website's expansion across Canada at this vital early juncture would provide a great opportunity for competitors who wish to establish a market presence ahead of TCG. As the internet is not limited by geography, there is, in theory, nothing standing in the way of those American-based companies from entering the Canadian marketplace before the Expiration Date. TCG's timing of being the first such business to exploit the market in Quebec and potentially throughout the rest of Canada, is a reasonable business advantage (at para. 17).

On the appeal, Belron argued that once a judge has determined that there is a strong *prima facie* case of a breach of a negative covenant, there is no basis in law for her to consider irreparable harm or balance of convenience. The Court of Appeal was not convinced by this argument, holding that while "in most commercial cases involving sophisticated and solvent litigants in which a strong prima facie case is made out that there has been or will be breach of a negative covenant, an interim injunction will be granted," the law would not be well-served by formulating a rule to this effect. Each motion for an injunction should consider all of the three-part test, as the motions judge had in this case. The appeal was dismissed.

Common Law Defence to Defamation

In *Grant v. Torstar Corp.*, the Supreme Court of Canada decided that it was necessary to create a new common law defence to defamation claims. The respondent had aired a story investigating the

development of a golf course, and the story had included the views of some local residents who felt that the plaintiff was exerting political influence behind the scenes to obtain approval. The plaintiff sued, and the issue was whether a new common law defence should be made available to journalists. The Court held that this should be the case, to adequately protect the interest of freedom of expression. It would apply where: the publication was on a matter of public interest, and the publisher was diligent in trying to verify the allegation, having regard to: the seriousness of the allegation; the public importance of the matter; the urgency of the matter; the status and reliability of the source; whether the plaintiff's side of the story was sought and accurately reported; and whether the inclusion of the defamatory statement was justifiable.

> 96 A second preliminary question is what the new defence should be called. In arguments before us, the defence was referred to as the responsible journalism test. This has the value of capturing the essence of the defence in succinct style. However, the traditional media are rapidly being complemented by new ways of communicating on matters of public interest, many of them online, which do not involve journalists. These new disseminators of news and information should, absent good reasons for exclusion, be subject to the same laws as established media outlets. I agree with Lord Hoffmann that the new defence is "available to anyone who publishes material of public interest in any medium": *Jameel*, at para. 54.
>
> 97 A review of recent defamation case law suggests that many actions now concern blog postings and other online media which are potentially both more ephemeral and more ubiquitous than traditional print media. While established journalistic standards provide a useful guide by which to evaluate the conduct of journalists and non-journalists alike, the applicable standards will necessarily evolve to keep pace with the norms of new communications media. For this reason, it is more accurate to refer to the new defence as responsible communication on matters of public interest.

The Court also concluded later in its judgment that it was particularly important to maintain the "repetition rule" (that it was not a defence to claim one was merely repeating another person's libel, not originating it ,"in the age of the internet, when defamatory material can spread from one website to another at great speed" (para 119).

Privacy: The "Right to Forget"?

Media outlets have recently been reporting on legal developments regarding the ability of individuals to legally compel the deletion of online information about themselves—or, what is being colloquially described as the "right to forget." In Germany, for example, lawyers for convicted murderer Wolfgang Erle have sent Wikipedia a cease and desist letter for continuing to list Erle as the murderer of actor Walter Sedlmayr. This was on the basis that German law requires that after serving 15 years of his sentence Erle was no longer a "public figure" and his name and likeness could not be used in association with the Sedlmayr murder. His continued identification as the murderer on the English version of Wikipedia, the letter said, was unlawful and was interfering with his attempts to reintegrate into Germany society. In France, the government is considering a "right to forget" law, which would "force online and mobile firms to dispose of e-mails and text messages after an agreed length of time or on the request of the individual concerned."

Truncating Breathalyser Readings

R. v. MacLeod considered the appropriate method of understanding breathalyzer readings for determining whether a third reading is required. Normally operators are required to obtain two breath samples. However, if the two samples vary by more than 20mg, then the "Recommended Standards of Procedures of the Canadian Society of Forensic Science Alcohol Test Committee" indicate that this should be taken to show that there is a problem with one of the samples, and therefore a third sample should be taken. In *MacLeod*, the accused's two readings were 137 mg and 114 mg. Since these differ by 23 mg, he argued that a third sample ought to have been taken: since it was not, the readings should not be considered reliable.

A police officer and an expert called for the Crown testified that in the circumstances, no third reading was required. In their practice, readings were "truncated" before being compared to see whether they differed by more than 20 mg. In this case that meant that the reading of 114 mg was taken to be 110 mg and the reading of 137 mg was taken to be 130 mg. In that event they did not differ by more than 20 mg and no third sample was required. The expert witness, a forensic toxicologist for the Centre of Forensic Science in Sault Ste. Marie, was accepted as an expert in issues relating to the functioning and operation of the Intoxilyzer 5000C.

The expert testified earlier designed instruments had not provided a third digit at all, and so that could only then have been estimated by the technician. The Intoxilizer allows for a third digit, but the expert testified that it related to calibrating the instrument and conducting blank testing, in order to show that the instrument was clearing alcohol correctly. However, he testified, breath samples vary in quality, so that the third digit loses meaningfulness when it comes to actual breath testing. He testified that the practice of truncating the reading to eliminate the third digit provided a more conservative estimate of an accused's blood alcohol level, and therefore was fairer, in addition to serving to avoid needless third tests. He also testified that the Alcohol Testing Committee guidelines meant a greater than 20mg difference in truncated blood alcohol readings.

The trial judge concluded that it had been shown that the practice of truncating readings both had a scientific basis and operated fairly to an accused, and accordingly that no third reading was required. In that event the readings were admissible and the accused was convicted.

U.S. Cases of Interest: Injunctive Take-down Order Can't Be Enforced

In *Blockowicz v. Williams*, Chief Judge James Holderman of the U.S. Dist. Ct. for Illinois (Eastern Division) denied a motion by the successful plaintiffs in a defamation case for the enforcement of a permanent injunction requiring the removal of the defamatory postings. The plaintiffs were unable to compel the defendants to comply with the injunction, and thus approached the third-party website providers on whose sites the defamatory remarks were posted to assist. All but one, ripoffreport.com, co-operated and removed the remarks. The plaintiffs brought a motion to have the court compel Xcentric Ventures, the operators of ripoffreport.com, to comply, but Xcentric argued that the court had no authority under the Federal Rules of Civil Procedure to make such an order. The court considered Rule 65(d), which provides that injunctions bind not only named parties, "but also nonparties who act with the named party." The Rule has been interpreted as requiring that such nonparties must be "acting in concert or legally identified (i.e. acting in the capacity of an agent, employee, officer etc.) with the enjoined party" (p. 4). The plaintiffs argued that Xcentric's service agreement with the defendants, which constituted an "ongoing promise" on Xcentric's part to "publish or remove the defamatory statements in exchange for indemnification and an exclusive copyright license to those statements" amounted to acting in concert or participation (p. 5). However, Chief Judge Holderman found that there was no evidence that Xcentric intended to "protect defamers and aid them in circumventing court orders," nor that Xcentric and the defendants had even been in contact since the issuing of the injunction (p. 6). Accordingly, Xcentric's "tenuous connection" with the defendants was insufficient to ground an order for compliance with the injunction.

Videolink Evidence in Criminal Trials

The Alberta Provincial Court considered the use of testimony by way of video link from Australia with its decision in *R. v. D'Entremont*. The accused was charged with failure to obey a yield before entering a highway. One of the Crown's witnesses had been rendered a paraplegic in the motor vehicle accident which ensued. She now lived in a long-term medical facility near her home town of Wollongong Australia. The trial judge described the prospect of her traveling to Alberta for the trial as "for practical purposes, all but impossible" (para 6). Accordingly, the Crown applied under section 714.2 to have her evidence received from Australia. Section 714.2 of the *Code* says:

(1) A court shall receive evidence given by a witness outside Canada by means of technology that permits the witness to testify in the virtual presence of the parties and the court unless one of the parties satisfies the court that the reception of such testimony would be contrary to the principles of fundamental justice.

The accused objected to the testimony being received in this way. He argued that that there was a great advantage to seeing a witness "live". He also argued that cross-examination would be made more difficult by the delays inherent in closed circuit television transmissions, and that this hindrance to cross-examination made the order sought contrary to the principles of fundamental justice.

The trial judge rejected the accused's argument and granted the order. He reviewed the rationale for having created section 714.2, as discussed in previous case law. He noted that the section created a presumption that evidence from outside Canada would be received in this fashion, unless it was shown that doing so would be contrary to the principles of fundamental justice. This contrasted with section 714.1, which gives a judge discretion to grant such an order, depending on a number of factors, in the case of a witness who was in another province.

In creating this presumption, the trial judge held, Parliament must be taken to have understood the various relevant factors. These included the importance of cross-examination, the need to see to it that witnesses do not have access to materials they should not during breaks, the necessity (or lack thereof) for a judge to observe a witness in person to assess credibility, the possibility of uncooperative or perjuring witnesses, and so on. He concluded that the technological sophistication of the videoconference equipment was sufficient to presumptively guarantee fairness.

Note as well that the judge referred with approval to guidelines laid down in a previous case, *R. v. Heynen*, 2000 YTTC 502 (no hyperlink available) to the use of such technology:

Use of Video:

i) Delays: Some slight delays can exist between receiving the picture and accompanying sound. All parties involved should be instructed not to speak over the delay and to wait before speaking to ensure that the witness has finished speaking and has had a full opportunity to hear any transmission.

ii) Movement: Picture quality seems to deteriorate with movement. All parties should keep their movements to a minimum to avoid reducing the quality of the picture transmission.

iii) Exhibits: Arrangements must be made for someone to have and manage all relevant exhibits that the witness may need.

iv) Clerk: An appropriate person in the place where the witness appears must be available to administer an oath. It is also advisable that the person be a court clerk and be familiar with the clerk services required. Other officials, although well meaning, may not, as one did in this case, act in a appropriate manner. It is especially important to have a clerk to take charge of the exhibits and to control a number of matters, including the needs of a witness and the ability to retrieve a witness after a short adjournment.

v) Preliminary Matters: Extra care should be taken to introduce everyone who will be involved and visible to the witness on video.

vi) Equipment: The clerk in the courtroom needs to be familiar with the use of the equipment if a technician is not available. Clear instructions need to be given when the audio and picture transmission to a witness are shut off.

2ième partie

Ordonnance visant à empêcher la diffusion de message sur Internet rejetée

L'entreprise Béton St-Hubert requiert une ordonnance du tribunal tendant à interdire au défendeur de diffuser, publier, reproduire ou faire circuler directement ou indirectement sur un site Internet ou sur tout médium des propos diffamatoires concernant la sécurité de son établissement ou la pollution environnementale causée elle.

Compte tenu de la preuve disponible, le tribunal conclut que la demanderesse n'a pas établi son droit à l'ordonnance de sauvegarde qu'elle recherche. Selon les enseignements de la Cour d'appel, la valeur accordée à la liberté d'expression, particulièrement en matière d'intérêt public, limite l'injonction aux seuls cas exceptionnels où il peut être démontré qu'elle est justifiée en raison des propos déjà prononcés clairement diffamatoires et impossibles à justifier et de la prévisibilité d'une nouvelle atteinte à des droits protégés en l'absence d'ordonnance. Les préoccupations soulevées par le défendeur dans les annonces (sécurité d'un site industriel et les questions de pollution environnementale), peuvent être considérées, si elles sont véridiques, comme étant d'intérêt public. Et le Tribunal ne peut conclure que ces propos sont clairement diffamatoires et impossibles à justifier, ni de la prévisibilité des prochains propos.

- *Béton St-Hubert c. Entreprises Kijiji Canada inc.*, 009 QCCS 5676 (CanLII), 30 novembre 2009.

Les blogueurs sont tenus à des devoirs de « communication responsable »

Dans sa décision *Grant v. Torstar,* la Cour suprême du Canada reconnaît qu' « Étant donné les atteintes à la réputation qu'une fausse déclaration peut causer, la presse et ceux qui œuvrent dans la communication sur des questions d'intérêt public, comme les blogueurs, doivent faire preuve de prudence. » (par. 62). Elle observe qu'« Un examen de la jurisprudence récente relative à la diffamation permet de constater que de nombreux recours concernent désormais des articles de blogue ainsi que d'autres médias en ligne dont la portée est susceptible d'être à la fois plus éphémère et plus répandue que celle de la presse écrite. Même si les normes journalistiques établies constituent un guide utile pour évaluer la conduite tant des journalistes que des non-journalistes, les normes applicables évolueront forcément pour suivre l'évolution des nouveaux médias. Il est donc plus juste de désigner ce nouveau moyen sous le nom de défense de communication responsable concernant des questions d'intérêt public. ». (par 97).

Ainsi, s'agissant de l'exigence de prendre les mesures afin de s'assurer de l'exactitude des affirmations, la Cour affirme que : (…) il ne faut pas que l'exigence légale de la vérification de l'exactitude empêche la diffusion en temps utile de nouvelles importantes. Il ne faut pas non plus que la course au « scoop » à laquelle prendrait part un journaliste (ou un blogueur) serve d'excuse à la diffusion irresponsable d'allégations diffamatoires. Il s'agit de décider si la nécessité d'informer le public commandait que le défendeur procède à la communication au moment où il l'a fait. Ce facteur, comme d'autres, s'examine à la lumière de ce que le défendeur savait ou devait savoir au moment de la diffusion. Si un délai raisonnable lui avait permis de découvrir la vérité et de corriger les erreurs diffamatoires sans nuire à l'actualité de la nouvelle, le facteur favoriserait le demandeur. » (par. 113)

- *Grant v. Torstar Corp*, 2009 CSC 61 (CanLII), 22 décembre 2009.

La protection de l'identité des personnes sur Internet

Ce n'est pas facile de protéger son identité sur le réseau des réseaux. Les éléments constituant l'identité et susceptibles d'être utilisés de façon frauduleuse sont de divers ordres: sexe, nom, prénom, lieu et date de naissance, noms et prénoms des parents, et dans certains pays le numéro d'assurance sociale, et même les données financières. L'édition de décembre du Bulletin *e-Veille* présente une revue des tendances au sujet de la protection de l'identité. Citant les travaux de l'Organisation de coopération et de développement économiques (OCDE), le

Bulletin rappelle qu'il s'avère difficile de donner une définition reconnue internationalement au vol de renseignements personnels relatifs à l'identité : « chaque pays le définit différemment. Certains pays le voient comme un crime grave en soi, alors que d'autres le perçoivent comme un délit non criminel ou encore, comme une étape préliminaire à un crime de plus grande envergure. Néanmoins, tous s'entendent généralement pour dire qu'on parle de « vol d'identité », ou plus précisément de vol de renseignements personnels, lorsqu'« un individu acquiert, transfert, possède ou utilise les renseignements personnels d'une personne morale ou physique sans être autorisé à le faire dans l'intention de commettre un crime ou une fraude ou en lien avec un crime ou une fraude ».

Au Canada, le projet de loi S-42 modifiant le Code criminel réfère au vol d'identité entendu comme étant un vol de renseignements personnels, alors que la fraude à l'identité ou l'usurpation d'identité « constitue l'usage trompeur subséquent des renseignements relatifs à l'identité d'une autre personne dans le cadre de diverses infractions (comme la supposition de personne, la fraude ou l'usage abusif des données de cartes de crédit) ».

Le Bulletin présente aussi une revue des initiatives prises dans plusieurs pays afin de prévenir le vol de renseignements personnels chez les jeunes. Le Canada n'est pas en reste. En effet, diverses initiatives ont été mises en place notamment par le Commissariat à la vie privée pour sensibiliser et informer les jeunes sur les risques de la navigation sur Internet et sur la protection de leurs renseignements personnels. Enfin, le Bulletin présente un dossier sur les travaux menés à l'OCDE sur le vol de renseignements personnels.

- Bulletin d'information *e-Veille*, Décembre 2009.

Nouveau cadre réglementaire pour les communications électroniques – Union européenne

Le 19 décembre 2009 est entré en vigueur le nouveau cadre réglementaire des communications électroniques pour l'Union européenne. Ces directives doivent être transposées par les États membres dans leur législation nationale avant le 25 mai 2011. Parmi les caractéristiques du nouveau cadre réglementaire, les auteurs soulignent les suivantes :

- La promotion de la concurrence, entre opérateurs de communications électroniques, basée sur le développement d'infrastructures/ réseaux propres à ces derniers alors que l'ancien cadre réglementaire privilégiait plutôt une concurrence basée sur les services offerts.
- La séparation fonctionnelle (filialisation) des opérateurs verticalement intégrés est instaurée comme moyen permettant de favoriser une concurrence effective sur les marchés de détail.
- Les textes instaurent une possibilité pour les autorités réglementaires nationales d'imposer des obligations ex ante aux opérateurs disposant d'une puissance significative de marché au niveau des marchés de détail. Auparavant, cette possibilité n'existait que pour les marchés de gros.
- Les textes énoncent le principe de la neutralité technologique en ce qui a trait au spectre radioélectrique.
- La mise en place d'un Organe des régulateurs européens de communications électroniques (ORECE) est prévu. Cette nouvelle instance européenne contribuera à assurer une concurrence équitable et une cohérence accrue de la réglementation sur les marchés des télécommunications.
- La protection du consommateur est renforcée par plusieurs dispositions, notamment une première qui permet à ce dernier de changer d'opérateur téléphonique (avec portabilité du numéro) en un jour ouvrable ; et une seconde qui renforce les obligations d'informations précontractuelles en matière de fourniture d'accès. Il y a obligation d'informer les consommateurs du niveau de qualité minimale que le prestataire s'engage à fournir. Les consommateurs devront également être mieux informés.
- Enfin, il y a un renforcement de la protection des données personnelles. Les fournisseurs de services de communications électroniques

accessibles au public seront tenus de notifier aux autorités nationales compétentes de même qu'aux personnes concernées toute violation des données à caractère personnel relatives à ces personnes. L'obligation de notification est contrôlée par les autorités nationales compétentes et les fournisseurs devront tenir à jour un inventaire des attaques subies et des mesures prises conséquemment.

- Le cadre juridique mis en place vient renforcer la lutte contre le « pourriel» en introduisant la possibilité d'une action en justice contre les spammeurs. Les États membres doivent veiller à ce que ces actions en justice puissent être ouvertes aux personnes physiques et morales, et parmi celles-ci tout spécialement aux fournisseurs de services de communications électroniques. Cette approche se fonde sur le fait que ces fournisseurs de services consacrent des investissements substantiels à la lutte contre le pourriel et ils sont mieux placés pour identifier les polluposteurs. Des sanctions contre les fournisseurs de services de communications électroniques qui, par leur négligence, contribueraient à la prolifération du « spam » sont prévues.

- Thibault VERBIEST, Bertrand VANDEVELDE et Momchil MONOV, « Un nouveau cadre juridique européen pour les communications électroniques, » *Droit & Technologie*, 11 janvier 2010.

- Europa, *Réforme des télécommunications de l'UE: 12 mesures pour des droits du consommateur renforcés, un internet plus ouvert, un marché unique européen des télécommunications et des connexions internet à haut débit pour tous*, Communiqué de presse, Bruxelles, 20 novembre 2009.

La réforme comprend deux directives modifiant cinq directives datant de 2002 relatives aux télécommunications et un nouveau règlement :

- *Directive 2009/140/CE du Parlement européen et du Conseil du 25 novembre 2009 modifiant les directives 2002/21/CE relative à un cadre réglementaire commun pour les réseaux et services de communications électroniques, 2002/19/CE relative à l'accès aux réseaux de communications électroniques et aux ressources associées, ainsi qu'à leur interconnexion, et 2002/20/CE relative à l'autorisation des réseaux et services de communications électroniques* ;

- *Directive 2009/136/CE du Parlement européen et du Conseil du 25 novembre 2009 modifiant la directive 2002/22/CE concernant le service universel et les droits des utilisateurs au regard des réseaux et services de communications électroniques, la directive 2002/58/CE concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques et le règlement (CE) no 2006/2004 relatif à la coopération entre les autorités nationales chargées de veiller à l'application de la législation en matière de protection des consommateurs* ;

- *Règlement (CE) no 1211/2009 du Parlement européen et du Conseil du 25 novembre 2009 instituant l'Organe des régulateurs européens des communications électroniques (ORECE) ainsi que l'Office*.

Développement durable et aspects linguistiques du monde numérique – Forum des droits sur Internet – France

Dans le cadre de ses travaux sur les problématiques de développement durable et Internet, le Forum des droits sur l'Internet publie ses réflexions et ses recommandations sur les aspects linguistiques du monde numérique. Dans sa Recommandation « Internet et développement durable II : langues et internet », le Forum émet plusieurs propositions visant à améliorer le multilinguisme et l'accessibilité linguistique sur Internet et qui s'adressent particulièrement aux exploitants de sites internet, éditeurs de logiciels, fabricants de matériels ou encore aux pouvoirs publics.

Le Forum recommande de permettre l'utilisation de tous les caractères de la langue française pour les noms de domaine, afin de respecter notamment les patronymes français. Il considère, par ailleurs, que la

standardisation d'un clavier informatique facilitant la saisie de la langue française serait de nature à préserver ce patrimoine linguistique. Enfin, le Forum déconseille l'utilisation de pictogrammes pour matérialiser le choix de la langue sur un site Internet mais de l'écrire en toutes lettres dans la propre langue du lecteur.

- FORUM DES DROITS SUR INTERNET, *La langue et internet : Le Forum des droits sur l'internet publie une étude inédite*, 7 janvier 2010.
- FORUM DES DROITS SUR INTERNET, *Recommandation Internet et développement durable II : Langues et internet*, 22 décembre 2009.

Ouverture du courriel d'un salarié par l'employeur – France

Dans un arrêt du 15 décembre 2009, la Cour de cassation n'a pas considéré que le fait d'ouvrir des courriels sur le poste de travail d'un salarié dont la lecture de certains révélaient leur nature privée faisait tomber la présomption de leur caractère professionnel. La décision concernait le congédiement d'un clerc de notaire pour faute grave suite à la découverte sur son ordinateur de courriels dénonçant le comportement et la gestion de son employeur auprès de tiers. La Cour de cassation a confirmé l'arrêt de la cour d'appel d'Angers qui avait jugé que le salarié avait outrepassé sa liberté d'expression, en jetant le discrédit sur son employeur en des termes excessifs et injurieux. Il avait ainsi manqué à ses obligations justifiant la rupture immédiate du contrat de travail. La Cour relève que les fichiers ouverts par l'employeur étaient intitulés « essais divers, essais divers B, essais divers B, essais divers restaurés ». Étant donné que le salarié ne les avait pas identifiés comme étant personnels, ils étaient présumés professionnels. Du coup, la Cour en conclut que l'employeur était en droit d'ouvrir les fichiers, même en l'absence de l'intéressé.

- Tiré de : « Ouverture de courriel de salarié : la Cour de cassation affine sa jurisprudence », *Legalis.net*, 8 janvier 2010.
- *Bruno B. c. Giraud et Migot*, Cour de cassation, Chambre sociale, Arrêt du 15 décembre 2009, *Legalis.net.*

Google Suggest se mérite une condamnation pour injure – France

L'association du nom d'une société avec le terme « arnaque » dans la barre de requête de Google grâce à la fonction Google Suggest constitue de la diffamation. Une décision de la cour d'appel de Paris rendue le 9 décembre 2009 de même qu'un jugement au fond du 4 décembre 2009 du Tribunal de Commerce de Paris ont condamné Google pour la suggestion « nom de l'entreprise – arnaque ». Les entreprises avaient fait constater que lorsqu'un internaute saisissait dans la barre de requêtes de Google leur nom, la suggestion associait leur nom avec le mot « arnaque » en premier.

Les entreprises plaignantes ont obtenu gain de cause puisque les juges ont considéré que l'association « arnarque » avec le nom de l'entité était injurieuse. De son côté, Google a fait valoir le caractère automatique du procédé activé par l'usager. Le moteur de recherche fonctionne sans intervention humaine et les résultats de recherche sont uniquement le résultat d'algorithmes appliqués à une base de données recensant les requêtes les plus fréquentes. Le tribunal écarte cet argument en estimant que le système comporte un certain contrôle humain puisque Google invite les internautes à signaler les suggestions indésirables. De plus, le moteur de recherche évite les propositions « qui pourraient offenser un plus grand nombre », notamment, les termes grossiers, de même que les mots incitant à la haine ou à la violence. Cela implique la possibilité d'un tri préalable entre les requêtes enregistrées dans la base de données. Dès lors qu'il reçoit une mise en demeure, Google ne peut plus ignorer le caractère litigieux de la suggestion.

Le Tribunal a également rejeté l'argument relatif à la liberté d'expression et d'information. Il a estimé que la seule utilité du service est d'éviter à l'internaute d'avoir à saisir sa requête. Au surplus, la suppression de l'expression litigieuse n'empêcherait pas les utilisateurs de disposer de toutes les références indexées par Google.

Google avait aussi fait valoir que sa responsabilité ne saurait être engagée en raison de l'absence de fixation préalable de la suggestion litigieuse. Le juge ne retient pas davantage cet argument en se contentant de rappeler le fonctionnement du système. En première instance, le tribunal avait été plus explicite en observant que le directeur de la publication « invoque à tort que le message litigieux n'aurait pas fait l'objet d'une fixation préalable à sa communication au public, alors qu'il a été admis au sein de la base de données au terme d'une sélection à laquelle la société Google affirme elle-même se livrer sur la base de critères qu'elle a prédéfinis, par un procédé qui pourrait s'apparenter à la modération a priori d'un forum de discussion, étant ajouté qu'à tout le moins après la première mise en demeure adressée par la société demanderesse le 17 février 2009, le maintien ou toute nouvelle admission de l'expression dans cette base de données ne pouvait que résulter d'un choix conscient ».

- Tiré de : « Google Suggest : le moteur de recherche condamné pour injure », *Legalis.net*, 05/01/10.
- *Google Inc. c. Direct Energie*, Cour d'appel de Paris Pôle 1, 2ème chambre Arrêt du 09 décembre 2009, *Legalis.net*.
- *Direct Energie / Google Inc*, Tribunal de commerce de Paris Ordonnance de référé du 7 mai 2009.

La présence de fichiers de porno sur un poste de travail n'est pas en soi un motif suffisant de congédiement – France

Dans un arrêt rendu le 8 décembre 2009, la chambre sociale de la Cour de cassation a estimé que la seule conservation de photos à caractère pornographique et zoophilique sur le poste informatique d'un salarié, en l'absence de constatation d'un usage abusif affectant son travail, ne constituait pas un manquement aux obligations résultant de son contrat pouvant justifier son licenciement. La décision justifiant le congédiement de la Cour d'appel reposait sur l'argument suivant lequel les fichiers contenant des photos à caractère pornographique portant atteinte à la dignité humaine étaient enregistrés et conservés dans l'ordinateur du salarié et dans un fichier archive accessible par tout utilisateur. L'instance d'appel avait estimé que cela suffisait pour établir le détournement par le salarié du matériel mis à sa disposition en violation des notes de service de l'employeur et constituait un risque de favoriser un commerce illicite en portant atteinte à l'image de marque de l'employeur. La Cour de cassation ne souscrit pas à ces motifs et renvoie plutôt l'affaire au tribunal de première instance pour statuer sur les seules conséquences du licenciement.

- Tiré de : « Des fichiers porno sur le poste du salarié ne justifient pas son licenciement », *Legalis.net,* 6 janvier 2010.
- *Sergio G. c. Peugeot Citroën automobiles*, Cour de cassation, Chambre sociale, Arrêt du 8 décembre 2009, *Legalis.net.*

This newsletter is intended to keep members of IT.Can informed about Canadian legal developments as well as about international developments that may have an impact on Canada. It will also be a vehicle for the Executive and Board of Directors of the Association to keep you informed of Association news such as upcoming conferences.

If you have comments or suggestions about this newsletter, please contact Professors Robert Currie, Chidi Oguamanam and Stephen Coughlan at it.law@dal.ca if they relate to Part 1 or Pierre Trudel at pierre.trudel@umontreal.ca if they relate to Part 2.

Disclaimer: The IT.Can Newsletter is intended to provide readers with notice of certain new developments and issues of legal significance. It is not intended to be a complete statement of the law, nor is it intended to provide legal advice. No person should act or rely upon the information in the IT.Can Newsletter without seeking specific legal advice.

Le présent bulletin se veut un outil d'information à l'intention des membres d'IT.Can qui souhaitent être renseignés sur les développements du droit canadien et du droit international qui pourraient avoir une incidence sur le Canada. Le comité exécutif et le conseil d'administration de l'Association s'en serviront également pour vous tenir au courant des nouvelles concernant l'Association, telles que les conférences à venir.

Pour tous commentaires ou toutes suggestions concernant la première partie du présent bulletin, veuillez contacter les professeurs Robert Currie, Chidi Oguamanam et Stephen Coughlan à l'adresse électronique it.law@dal.ca ou en ce qui concerne la deuxième partie, veuillez contacter Pierre Trudel à pierre.trudel@umontreal.ca.

Avertissement : Le Bulletin IT.Can vise à informer les lecteurs au sujet de récents développements et de certaines questions à portée juridique. Il ne se veut pas un exposé complet de la loi et n'est pas destiné à donner des conseils juridiques. Nul ne devrait donner suite ou se fier aux renseignements figurant dans le Bulletin IT.Can sans avoir consulté au préalable un conseiller juridique.