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

October 19, 2011/19 octobre 2011

IT.Can NEWSLETTER/BULLETIN

Canadian IT Law Association

www.it-can.ca

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

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

Part 1

Hyperlinking Not "Publication" for Defamation Purposes: SCC

In *Crookes v. Newton*, a case previously reported on in previous issues of this newsletter, the Supreme Court of Canada has upheld lower court findings that inserting hyperlinks to allegedly defamatory material does not constitute the element of publication in defamation law. The plaintiff Crookes, a B.C. businessperson and member of the Green Party, alleged that he had been defamed by hyperlinks inserted into an article (portentously entitled "Free Speech in Canada") posted on a website owned and operated by the defendant, Newton. One of the links was "shallow," directing users to a page containing various articles, while the other was "deep" and took the user directly to the article. Crookes sued Newton in defamation, arguing that by using the hyperlinks or by refusing to remove them when notified of the allegedly defamatory content of the underlying articles, Newton had become a "publisher" of the articles and was liable. Both the trial judge and a majority of the B.C. Court of Appeal dismissed the action, accepting Newton's argument that the hyperlinks were analogous to a footnote or library listing and thus constituting publication.

For a majority of the Supreme Court of Canada, Justice Abella upheld the lower court findings that inserting the hyperlinks was not publication. After an overview of the historically broad nature of what acts may constitute publication, Abella J. noted modern trends toward the finding that a passive act regarding a defamatory statement, such as a simple reference to it, would not by itself qualify as publication:

> A reference to other content is fundamentally different from other acts involved in publication. Referencing on its own does not involve exerting *control* over the content. Communicating something is very different from merely communicating that something exists or where it exists. The former involves dissemination of the content, and suggests control over both the content and whether the content will reach an audience at all, while the latter does not. Even where the goal of the person referring to a defamatory publication is to expand that publication's audience, his or her participation is merely ancillary to that of the initial publisher: with or without the reference, the allegedly defamatory information has already been made available to the public by the initial publisher or publishers' acts. These features of references distinguish them from acts in the publication process like creating or posting the defamatory publication, and from repetition (para. 26).

Hyperlinks, then, were essentially references to other content, over which the linker had no control and in the development/creation of which he/she had no role. Even though the hyperlink made for easy facilitation the transfer of information, it was still a referral and not a communication of the defamatory content. The hyperlink is content neutral, and requires action by a third party before they can gain access to the information.

Abella J. remarked that such an interpretation of the publication rule not only accorded with U.S. trends to immunize the facilitator of communications from liability, but was more consonant with post-*Charter* defamation jurisprudence which sought to balance the traditional interest of defamation law in protecting reputation with "the foundational

role of freedom of expression in the development of democratic institutions and values" (para. 32). She noted the primary role of the Internet in disseminating information, and observed at para. 36:

> The Internet cannot, in short, provide access to information without hyperlinks. Limiting their usefulness by subjecting them to the traditional publication rule would have the effect of seriously restricting the flow of information and, as a result, freedom of expression. The potential "chill" in how the Internet functions could be devastating, since primary article authors would unlikely want to risk liability for linking to another article over whose changeable content they have no control. Given the core significance of the role of hyperlinking to the Internet, we risk impairing its whole functioning. Strict application of the publication rule in these circumstances would be like trying to fit a square archaic peg into the hexagonal hole of modernity.

Making a reference to defamatory material, "without more," was not publication: "Only when a hyperlinker presents content from the hyperlinked material in a way that actually repeats the defamatory content, should that content be considered to be "published" by the hyperlinker" (para. 42). In the instant case, nothing on Newton's page itself was defamatory, nor was there any opinion expressed at all about Crookes, despite the use of the hyperlinks. The appeal was dismissed.

In a concurring opinion, McLachlin C.J. and Fish J. agreed substantially with the reasons of the majority, but would have reformulated the test for where a hyperlinker could "publish" defamatory material: "if the text indicates *adoption or endorsement of the content of the hyperlinked text*. If the text communicates agreement with the content linked to, then the hyperlinker should be liable for the defamatory content" (para. 48). Deschamps J. concurred in the result but disagreed with the other two approaches. She would have found that the "deep link" article was indeed published as Newton had made a deliberate decision to be a conduit to that information, but that there was insufficient evidence that anyone had actually read the article via the hyperlink, resulting in there being no finding of publication.

Anonymity and Facebook

The applicant in *A.B. (Litigation Guardian) v. Bragg Communications Inc.* became aware of a fake Facebook profile which included her photograph and various identifying information, and which allegedly included scandalous sexual commentary of a private and intimate nature. The applicant wanted to bring a defamation action against whomever had made the posting, and applied for an order requiring the respondent to disclose the identity of the persons who used the IP address from which the posting had been made. That part of the litigation has been largely uncontroversial. However, in addition the applicant sought an order which would allow her to proceed using only a pseudonym. She also sought a partial publication ban of the information contained in the fake Facebook profile. The Chambers Judge had granted the disclosure order but refused the anonymity request and the publication ban. The Court of Appeal upheld that decision: see the IT.Can newsletter of March 9, 2011.

The matter is now proceeding to the Supreme Court of Canada, where her application in the ultimate issue is opposed by two media organizations, the Halifax Herald and Global Television. As a preliminary matter the applicant had sought an order 1) allowing her to bring her application for leave to appeal by using pseudonyms, and 2) prohibiting publication of the words used in the Facebook profile until final disposition of the matter: those applications were granted in May 2011. The Court has now granted the application for leave to appeal itself. In addition the anonymization order and publication ban granted earlier were continued.

Computers and Searches

The Ontario Court of Appeal has handed down a significant decision on the permissible scope of searches of a computer with its judgment in *R. v. Jones*. The accused was being investigated for fraud, and in connection with that investigation the police had obtained a warrant and were conducting a search of his computer. In particular they were looking for emails connected to communications in pursuit of the fraud, and images relating to a computer-generated forged invoice. In the course of executing that warrant, a police officer discovered

images of child pornography on the computer. The officer then sought advice from a Crown attorney as to whether he could, without seeking a further warrant, continue to search the computer for child pornography. He was advised that he could do so, and examined further files, including the video files that he would not have accessed had the search been confined to evidence of fraud. As a result of that further search the officer discovered 57 images and 31 videos of child pornography. The accused was therefore also charged with possession of child pornography.

The trial judge found that the search for both the images and video files violated the accused`s section 8 right. Calling the advice that was given to the police "reckless and cavalier", the trial judge had excluded the evidence. The Ontario Court of Appeal agreed with the trial judge in part: they concluded that the police did not have the authority to search for the child pornography without a further warrant, and that the search for and seizure of the video files was a violation of section 8. However, they also disagreed in part, and particularly about the ultimate result: they concluded that the search of the image files was *not* a section 8 violation, and they reconsidered the section 24(2) analysis with regard to the video files and decided not to exclude that evidence. Their reasoning led them to look at the proper scope of the search under the warrant, the "plain view" doctrine, and section 489 of the *Criminal Code* which permits a person executing a warrant to seize things not mentioned in the warrant in some circumstances.

The Court of Appeal acknowledged that a search of a computer engaged a significant privacy interest on the part of the accused, quoting Justice Fish in *R. v. Morelli*: "[i]t is difficult to imagine a search more intrusive, extensive, or invasive of one's privacy than the search and seizure of a personal computer." On that basis, they agreed with the accused that police ought not to be given free rein to examine a computer at will for any purpose simply because they were entitled to examine it for one purpose.

However, they also acknowledged that the Crown was correct in pointing to a number of practical concerns in limiting the scope of a search:

(a) the difficulty in narrowing the field of search, given the realities of developing technology and the recognized ability of individuals to conceal information by storing it in different fashions, and by manipulating and reorganizing it so that a simple viewing of folder names and file lists or extensions may not provide an accurate reflection of the information stored in them;

(b) the fact that a warrant is issued (often very early) at the investigatory stage, and it is not practical at that stage to be precise about what could be relevant evidence;

(c) the fact that investigators, when making out grounds for a warrant, may not have the advance knowledge of what they will be examining or how they may be able to access the information stored on the computer, given the fast-paced nature of developing technology; and

(d) the difficulty that judicial officers face in assessing the suitability of technological search parameters that may be put forward in a wide variety of personal electronic device seizures. (para 39).

The accused had argued that the warrant was too broad and invalid because it did not limit the types of files that could be accessed or the relevant time frame within which the police were entitled to examine the dated files on the computer. The Crown, in response, pointed to the lack of any such explicit limitations as support for their claim that the police were therefore entitled to search the entire hard drive. The Court of Appeal rejected both positions. In their view, specific limits on the types of files or dates of files were not needed, but their absence did not mean that the police had an unlimited search power under the warrant. Rather, there was a limit on the search power in the warrant, which was created by the offence with regard to which the warrant had been issued. Police were entitled to search the computer in any way necessary to find the evidence of the fraud they were investigating: however, when their focus shifted and they began examining files to find child pornography, they were acting outside the warrant and unlawfully. The court held:

> [42] I do not accept that the right to examine the entire contents of a computer for evidence of one crime (fraud, in this

> case) carries with it the untrammelled right to rummage through the entire computer contents in search of evidence of another crime (possession of child pornography, in this case) without restraint – even where, as here, the warrant may properly authorize unlimited access to the computer's files and folders in order to accomplish its search objectives. A computer search pursuant to a warrant must be related to the legitimate targets respecting which the police have established reasonable and probable grounds, as articulated in the warrant.

The court accepted the analogy for these purposes between a computer and a physical space, holding that there was "no reason in principle why the state should be any more entitled to roam around through the contents of a person's computer in an indiscriminate fashion than it would be to do so in a person's home without further authorization" (para 49). They also noted that typically when the police are searching a computer they have already seized it, and so there is no urgency to the search: obtaining a new warrant is therefore practical. Accordingly the warrant did not authorize the police to search for the child pornography, and none of that evidence (neither the image files nor the videos) had been found lawfully based purely on the warrant.

However, the Court of Appeal held that both the "plain view" doctrine applied to searches of computer files. The plain view doctrine requires that the officer must be lawfully in the place where the search is being conducted; that the nature of the evidence is immediately apparent as constituting a criminal offence, and; that the evidence was discovered inadvertently. Further, the plain view doctrine confers a seizure power but not a search power, and so it is applicable to those items that are visible but does not permit a further search to find other evidence of other crimes. The fact that the date is digitally contained on a computer, they held, did not defeat the plain view doctrine. Rather, when a file is opened on a computer using the appropriate software, they held, that image is then in plain view and can be seized on that basis. Applying that doctrine, the court concluded that the child pornography image files were admissible as having been in plain view and discovered in the course of the search for evidence of fraud.

Similarly, section 489 of the *Criminal Code* permits a police officer who is lawfully in a place executing a warrant to seize things not mentioned in the warrant if there are reasonable grounds to believe they will afford evidence of a crime. That provision also allowed the seizure of the image files.

However, the Court held, neither of these rationales applied to the video files. Those files were not accidentally discovered, but rather were only found because of a deliberate search of the sort which is not permitted under the plain view doctrine. The Court of Appeal held that to permit the plain view doctrine to apply in that circumstance would invite overseizure by the police, which they observed was "a risk to which electronic media searches are particularly susceptible and something the court must guard against" (para 67). Similarly section 489 did not apply, because the officer did not come across the video files in the course of his search for evidence of fraud. Accordingly the search for and seizure of the video files was not authorized by any law and violated the accused's section 8 right.

However, the Court of Appeal concluded that the evidence ought not to be excluded under section 24(2). In differing from the trial judge's assessment on that point, they rejected her harsh view of the advice given to the police that they did have the power to search for evidence not mentioned in the warrant. The law around searches of computers had been difficult to assess at the time the advice had been given, they said, and although it turned out to be wrong it was not at the time negligent, reckless or in wilful disregard of the respondent's Charter rights. That factor weighed heavily in their decision to allow the evidence to be admitted.

Internet Evidence Struck from Affidavit

In *Rosetim Investments Inc. v. BCE Inc.*, Justice Richards of the Saskatchewan Court of Appeal heard a motion for leave to appeal an interlocutory decision striking certain paragraphs and exhibits from affidavits. The underlying action was for an oppression remedy against BCE for failure to pay appropriate dividend levels, but the plaintiffs wished to add a claim under the Saskatchewan *Securities Act*, and filed affidavits in support. One of the affiants, DeMaria, was an articled clerk for plaintiffs' counsel,

and in it he referred to "various materials which he downloaded from websites such as 'Thomson Research', 'Investext' and 'Thor Wealth Management Group'. These are annexed to the affidavit as Exhibits A to F inclusive and comprise many hundreds of pages" (para. 7). Another affidavit was sworn by Haigh, a proposed representative plaintiff. His affidavit included a printout of the history of BCE's stock price, taken from the BCE website, as well as various reports from the RBC "Capital Markets" website. The case management judge below had struck the paragraphs and exhibits from the DeMaria affidavit, ruling as follows:

> As pointed out by Justice Popescul, in order to be admissible, internet material must be established to be reliable. There is nothing in the DeMaria affidavit which suggests the reports come from an official website or that the information can be verified. The objectivity of the organization posting the material cannot be assessed by me based upon the information before me. Furthermore, it is unlikely that Mr. DeMaria, as an articling student, is able of his own knowledge to prove the contents of the analysts' reports nor does he state the grounds for his belief as required by Rule 319. Accordingly, I find that paragraphs 2, 3, 4, 5, 6 and 7 offend Rule 319 of *The Queen's Bench Rules* and those paragraphs and the exhibits referred to in them are not admissible.

He struck the RBC material from the Haigh affidavit on similar grounds, but allowed the material regarding the BCE share price as the defendant BCE did not contest its accuracy. Justice Richards resisted the plaintiffs' argument that this was a precedent-setting "internet law" case, finding the judge's rulings to be a straightforward application of the rules around affidavit content, and denied leave to appeal.

U.K.: LinkedIn Contacts Must Be Disclosed

In a 2008 decision which has just come to our attention (*Hays Specialist Recruitment (Holdings) Ltd. v. Ions*), Justice David Richards of the UK High Court of Justice (Chancery Division) presided over a pre-action disclosure motion regarding an individual's list of business contacts on the LinkedIn professional social network. The proposed action was by Hays, an employee recruitment company, versus Ions, who had worked for Hays as a mid-level employee for 6.5 years. Several weeks before resigning, Ions set up his own recruitment firm and Hays was prepared to allege that he used confidential information regarding Hays's clients in violation of his employment contract. Specifically, after Ions departed the company examined his computer and found indications that he had invited at least two Hays clients (and possibly more) to join his network on LinkedIn. It alleged he had copied and used confidential client information to do this, in violation of his employment contract, and sought disclosure of his entire LinkedIn profile and all associated information.

Ions argued that Hays had encouraged him to use LinkedIn while he was employed there, that the uploading of client contact info to the site was with Hays' consent, and that once uploaded and accessible by his other contacts it was thereafter not confidential. Justice Richards found that the essential factual point was that the information was accessible to Ions once he left Hays and began with his own firm. "Even if he uploaded [the contact information] with authority, it is difficult to imagine that the authority was not limited to using them in the performance of his duties as an employee of Hays." Even if the information was not confidential, the evidence suggested that this had been Ions' purpose all along. This was enough to order disclosure of the e-mail traffic between Ions LinkedIn account and Hays' network, as well as all documents stemming from his use of certain LinkedIn contacts and evidence of any business with those contacts which resulted.

2ième partie

Choix du support ou d'une technologie lors d'une demande d'accès à un document

L'Association professionnelle des ingénieurs du gouvernement du Québec (la demanderesse) a formulé une demande d'accès au Directeur général des élections du Québec (l'organisme) afin d'obtenir une copie informatique intégrale des rapports financiers des différents partis politiques pour les années 2008 et 2009. L'organisme a accepté de rendre accessibles ces rapports en format « papier » mais refuse de communiquer la version informatisée en invoquant les articles 126 et 488 de la *Loi électorale*. Le procureur de l'organisme réfère à ces articles pour démontrer que l'intention du législateur est de limiter l'accès à certaines informations sensibles lorsque celles-ci sont disponibles sous la forme informatisée. Selon lui, l'adresse des donateurs ne doit pas être divulguée afin de respecter l'esprit et l'intention du législateur. La demanderesse présente une demande de révision à la Commission d'accès à l'information. La question au cœur du débat est la suivante : lorsque les renseignements réclamés sont détenus par un organisme sur plusieurs documents de formes distinctes, la partie demanderesse peut-elle exiger l'obtention des informations dans le format de son choix ? En d'autres termes, est-ce qu'il appartient à l'organisme de rendre accessible un document sous la forme qu'il privilégie ou si cette option est plutôt réservée à la partie demanderesse ?

Dans sa décision, la CAI accueille la demande de révision et ordonne à l'organisme de communiquer les rapports financiers sous forme numérique. Pour la CAI, un premier élément de réponse se trouve à l'article 1 de la *Loi sur l'accès* qui précise que celle-ci s'applique quelle que soit la forme du document réclamé; le choix semble être offert au demandeur. Ensuite, selon l'article 10 de la *Loi sur l'accès*, la partie qui exerce son droit d'accès peut obtenir une copie du document sauf si, notamment, sa reproduction soulève des difficultés pratiques sérieuses en raison de sa forme. En l'absence d'un tel scénario, la Loi n'accorde pas cette discrétion à l'organisme. Or aucune preuve n'a été faite selon laquelle la divulgation du document soulèverait des difficultés pratiques sérieuses. L'article 488 de la *Loi électorale*, sur lequel s'appuie l'organisme pour justifier la non-divulgation de l'adresse des donateurs, ne vise que la situation où il rendrait accessible cette information sur son site Internet. Selon la Commission, cet article ne vise pas la situation où l'information se retrouve sur un support informatique. Ce serait ajouter à la Loi que de conclure de la sorte. Au surplus, l'article 126 de la *Loi électorale* prévoit que certains renseignements contenus dans les rapports financiers des partis politiques (nom et adresse du donateur ainsi que le montant de sa contribution) ont un caractère public. Il s'agit d'une exception à la règle générale de la protection des renseignements personnels. Enfin, selon la CAI, un troisième élément de réponse se retrouve à l'article 23 de la *Loi concernant le cadre juridique des technologies de l'information* qui prévoit que le choix d'un support ou d'une technologie tient compte de la demande de la personne qui exerce son droit d'accès sauf si ce choix soulève des difficultés pratiques sérieuses. Encore une fois, le législateur semble davantage offrir le choix à la partie demanderesse en l'absence de difficultés importantes qui doivent être démontrées par l'organisme. Dans le présent dossier, cette preuve n'a pas été faite. La CAI conclut que « La Loi sur l'accès n'oblige pas l'organisme à créer un support numérique ou technologique et à y transférer les données. Toutefois, lorsque ce document existe sur un support technologique, et c'est le cas en l'espèce, la partie demanderesse peut l'exiger si aucun motif légal n'est invoqué pour en restreindre l'accès. »

- *Association professionnelle des ingénieurs du gouvernement du Québec (APIGQ) c. Québec (Directeur général des élections)*, 2011 QCCAI 223 (CanLII), 3 octobre 2011.

Rapport quinquennal de la Commission d'accès à l'information (CAI)

Le Rapport quinquennal 2011 de la Commission d'accès à l'information intitulé *Technologie et vie privée : à l'heure des choix de société* a été déposé le 29 septembre dernier à l'Assemblée nationale. Comme le soulignait le président de la CAI, « en 2002, au moment de la publication du dernier

rapport quinquennal de la Commission, Facebook, YouTube, Twitter, Google Street View et WikiLeaks n'existaient pas encore! » Ce rapport insiste ainsi sur la nécessité d'adopter des mécanismes visant à mieux informer les individus des enjeux inhérents aux environnements électroniques. Il met également de l'avant des problématiques visant l'accès aux documents des organismes publics.

En raison des multiples enjeux découlant de la protection des renseignements personnels à l'ère numérique, la CAI recommande de mieux encadrer l'information transmise aux personnes concernées tout en s'assurant qu'elles expriment un consentement libre et éclairé (par exemple: adopter des politiques de confidentialité simplifiées présentant, en termes clairs et compréhensibles, une vue d'ensemble de leurs engagements en matière de protection de renseignements personnels, utiliser des pictogrammes de protection informant les citoyens de leurs engagements en matière de protection de renseignements personnels, signaler la présence de mécanismes susceptibles d'identifier ou de localiser une personne physique lors de l'utilisation de leurs produits).

Selon la CAI, la protection des renseignements personnels des natifs du numérique nécessite que des actions soient entreprises en faveur de la sensibilisation, de l'éducation et de l'implication de l'ensemble des acteurs (par exemple: développer des programmes scolaires au primaire et au secondaire visant à éduquer les jeunes aux enjeux des TI et du Web 2.0, s'interroger sur la nécessité de modifier les lois pour interdire le profilage des jeunes dans les environnements électroniques).

La sécurité étant un principe fondamental en matière de protection des renseignements personnels, la CAI recommande que les organismes publics et les entreprises soient obligés de déclarer à la Commission toute faille de sécurité présentant un risque pour les renseignements personnels. Elle recommande aussi que soient déterminées les conditions et modalités de cette déclaration.

La Commission croit nécessaire qu'un responsable de l'accès et de la protection des renseignements personnels soit désigné pour assumer tout ou partie des fonctions conférées par la *Loi sur la protection dans le secteur privé*. Elle souligne l'importance qu'une personne réponde auprès du public et de la Commission de l'application de la *Loi sur la protection dans le secteur privé* et que cette personne contribue à établir dans l'entreprise une culture de protection des renseignements personnels.

La CAI croit que si l'accès à l'information gouvernementale a été le « fer de lance » de l'adoption de la *Loi sur l'accès,* il importe maintenant d'augmenter de façon substantielle la quantité des informations accessibles aux citoyens et de faciliter, dans le respect des droits de chacun, l'accès à cette information. Ainsi, la Commission propose d'adapter le régime d'accès à l'information à la réalité actuelle en ouvrant, sauf exceptions, l'ensemble des données gouvernementales à la consultation et à l'utilisation. D'autres recommandations contribuent à renforcer le régime d'accès à l'information, notamment celles qui abordent l'assujettissement de certains organismes à la *Loi sur l'accès* et la nécessité pour ceux-ci de respecter les délais prescrits pour justifier un refus d'accès.

De même, si la protection des renseignements personnels a été la « pierre d'assise » de l'adoption de la *Loi sur la protection dans le secteur privé*, il est essentiel, pour la CAI, de s'assurer que les recours mis à la disposition des citoyens peuvent être exercés adéquatement et que les entreprises soient représentées par un interlocuteur. En somme, « les recommandations contenues dans ce rapport invitent à s'arrêter sur les choix que nous avons faits et que nous voulons faire en tant que société en matière d'accès à l'information et de protection des renseignements personnels à l'ère numérique. »

- Commission d'accès à l'information, *Rapport quinquennal 2011 – Technologies et vie privée à l'heure des choix de société*, 2011.

Enjeux juridiques du Web 2.0 et milieu scolaire

L'utilisation des différents outils du Web 2.0 permet l'accès à un ensemble sans précédent de services de communication et à des informations de toute nature. Mais les activités d'échange, de recherche et de diffusion d'informations sur Internet comportent des écueils. Ces écueils ne sont pas pires que ceux qui sont associés à bien d'autres activités. À l'instar des

autres lieux de vie, Internet implique des risques que les enseignants, les écoles, les commissions scolaires, les étudiants et les parents doivent connaître et gérer.

Ce Guide expose comment gérer les risques lors de la mise en place d'applications de Web 2.0 dans le milieu scolaire québécois. Les outils analysés sont les réseaux sociaux, les sites de partage de contenu, les blogues, le micro-blogue (Twitter), les sites de notation de personnes, de services ou de produits, les sites wikis et les flux RSS. Ce Guide situe les responsabilités des participants et propose des politiques, des mesures et des précautions à mettre en place.

- Pierre Trudel et France Abran, *Guide pour gérer les aspects juridiques du Web 2.0 en milieu scolaire*, Juin 2011, Équipe de recherche: Cynthia Gaudette, François Joli-Coeur, Annie Lagueux, Geneviève Normand et Jean-François R. Ouellette.

Clause d'interdiction de vente sur Internet constitue une restriction illégale à la concurrence – CJUE

La Cour de justice de l'Union européenne (CJUE) a décidé qu'une clause d'un accord de distribution sélective interdisant la vente de produits de cosmétique sur Internet constitue une restriction illégale à la concurrence. La décision fait suite à un recours préjudiciel auprès de la CJUE afin de déterminer si une interdiction générale et absolue de vente en ligne constitue une restriction de la concurrence « par objet », si un tel accord peut bénéficier d'une exemption par catégorie, et dans le cas où celle-ci n'est pas applicable, s'il peut bénéficier d'une exemption individuelle. La Cour a conclu que l'exigence d'une vente de produits cosmétiques dans un espace physique en présence d'un pharmacien n'était pas justifiée à l'égard de médicaments qui ne sont pas vendus sur ordonnance médicale. Une telle prohibition limite radicalement la possibilité pour un distributeur agréé de vendre les produits à des clients situés hors de sa zone d'activité. La Cour a également considéré qu'un tel accord de distribution sélective ne peut bénéficier d'une exemption par catégorie car celle-ci ne peut s'appliquer à des accords verticaux ayant pour objet la restriction des ventes actives ou passives aux utilisateurs finals désireux d'acheter sur Internet et localisés en dehors de la zone des détaillants autorisés.

- *Pierre Fabre Dermo-Cosmétique c. Président de l'Autorité de la concurrence*, Cour de justice de l'Union européenne, Troisième chambre, Arrêt du 13 octobre 2011.
- « Pierre Fabre Dermo-Cosmétique : la CJUE invalide l'interdiction de vente sur internet », *Légalis.net,* 14 octobre 2011.

Conditions justifiant un monopole sur les jeux de hasard par Internet – CJUE

Dans son arrêt rendu le 15 septembre, la Cour rappelle qu'un monopole sur les jeux de hasard constitue une restriction à la libre prestation des services. Toutefois, une telle restriction peut être justifiée par des raisons impérieuses d'intérêt général telles que l'objectif d'assurer un niveau de protection particulièrement élevé des consommateurs.

La Cour rappelle notamment sa jurisprudence selon laquelle – afin d'être cohérente avec l'objectif de lutter contre la criminalité et celui de réduire les occasions de jeu – une réglementation nationale instituant un monopole, tout en permettant au titulaire du monopole de mener une politique d'expansion, doit véritablement reposer sur la constatation que les activités criminelles et frauduleuses liées aux jeux constituent un problème dans l'État membre concerné auquel une expansion des activités réglementées serait de nature à y remédier. La Cour souligne cependant que, le seul objectif de maximiser les recettes du Trésor public ne permet pas de justifier une telle restriction à la libre prestation de services.

Dans ce contexte, la Cour souligne également que, seule une publicité mesurée et strictement limitée à ce qui est nécessaire pour canaliser les consommateurs vers les réseaux de jeu contrôlés pourrait être admise. Une politique commerciale expansionniste, dont l'objectif est l'accroissement du marché global des activités des jeux, ne serait pas cohérente avec l'objectif de lutte contre les activités criminelles et frauduleuses.

Enfin, la Cour examine la question de savoir si les contrôles des opérateurs de jeux de hasard effectués dans d'autres États membres – comme en l'espèce ceux auxquels sont soumises les filiales maltaises en Malte – doivent être pris en compte par les autorités d'un autre État membre, en l'occurrence l'Autriche. Selon MM Dickinger et Ömer, ainsi que le gouvernement maltais, Malte aurait en effet développé un système régulateur des jeux de hasard sur Internet performant de nature à répondre à l'objectif de protection des joueurs contre les fraudes.

À cet égard, la Cour rappelle que, en l'absence d'harmonisation de la réglementation de ce secteur au niveau de l'Union, aucune obligation de reconnaissance mutuelle des autorisations délivrées par les autres États membres ne saurait exister en l'état actuel du droit de l'Union et que la seule circonstance qu'un État membre a choisi un système de protection différent de celui adopté par un autre État membre n'a aucune incidence sur l'appréciation de la nécessité et de la proportionnalité des dispositions prises en la matière.

- *Bezirksgericht Linz Jochen Dickinger, Franz Ömer*, arrêt de la Cour (quatrième chambre) du 15 septembre 2011 (demande de décision préjudicielle du Bezirksgericht Linz - Autriche) - procédure pénale contre Jochen Dickinger, Franz Ömer (Affaire C-347/09).

- *Un monopole des jeux de hasard par Internet ne peut être justifié que s'il poursuit de manière cohérente et systématique l'objectif de lutte contre les dangers liés à de tels jeux*, CJUE, Communiqué de presse no 91/11, 15 septembre 2011.

Ordonnance relative aux communications électroniques, encadrant les « cookies » et « pourriels » – France

L'ordonnance relative aux communications électroniques, encadrant « cookies » et « pourriels » et qui prévoit la mise en place d'un médiateur indépendant en cas de désaccord entre les opérateurs et leurs clients, est parue au Journal officiel, vendredi le 26 août 2011. Cette ordonnance transpose des directives européennes relatives au secteur des télécommunications. Le texte indique que *« tout fournisseur d'un service de communications électroniques (...) est tenu d'instituer un médiateur impartial et compétent auquel ses clients peuvent s'adresser en cas de différend relatif aux conditions de leur contrat ou à l'exécution* [de celui-ci] ». L'ordonnance dispose que *« Les modalités d'intervention du médiateur doivent être facilement accessibles, rapides, transparentes pour les deux parties et confidentielles »*.

Le texte renforce la protection de la vie privée et vise les spams. *Il prévoit qu'* « Est interdite la prospection directe au moyen de systèmes automatisés d'appel ou de communication, d'un télécopieur ou de courriers électroniques utilisant les coordonnées d'une personne physique, abonné ou utilisateur, qui n'a pas exprimé préalablement son consentement à recevoir des prospections directes par ce moyen. »

Les « cookies », ces petits fichiers qui suivent à la trace l'internaute et permettent de cibler très finement la publicité, sont également encadrés. L'article 38 impose aussi des obligations aux fournisseurs d'accès en matière de protection des données personnelles.

- *Ordonnance no 2011-1012 du 24 août 2011 relative aux communications électroniques*, Journal officiel, 26 août 2011 – Edition numéro 0197.

Pratiques de sites de réservation hotelière jugées trompeuses – France

Le recours portait sur les pratiques de deux sites de réservation de prestations de voyage. On leur reprochait des pratiques commerciales consistant à diffuser des informations de nature à induire en erreur les internautes sur la disponibilité réelle des chambres des hôtels en cause. En réponse à une requête, on pouvait par exemple lire sur expedia.fr : « Aucune chambre n'est disponible aux dates sélectionnées » ou sur hotels.com : « l'hôtel n'est pas disponible aux dates que vous avez choisies ». De telles affirmations laissaient croire que l'information avait une portée universelle et qu'elle signifiait que l'hôtel était complet alors qu'elle concernait

uniquement la disponibilité sur le site. Les sites ont changé leur formulation et précisent que les renseignements reflètent les informations qui sont traitées par leur système de réservation. Le tribunal a considéré que les modifications étaient conformes au code de la consommation. Mais à titre de sanctions pour les pratiques jugées trompeuses faisant l'objet du recours, le Tribunal de Grande Instance de Paris a pris acte de ces changements et a condamné ces sites de tourisme à verser des indemnités de plus de 500,000 euros au Syndicat national des hôteliers, restaurateurs, cafetiers et traiteurs et à deux hôtels.

- *Synhorcat et autres c. Expedia et autres*, Tribunal de commerce de Paris, 15ème chambre, Jugement du 4 octobre 2011, *Legalis,net*.