WORLD INTERNET LAW REPORT

Volume 3, Issue 12 December 2002

Monthly News & Comment on Internet Law and Regulation from Around the World

HIGHLIGHTS

NEWS

A COURT IN CANADA has ruled that publication of material on the Internet is equivalent to publication in a newspaper for the purposes of assessing whether the material is libelous (Page 3)

THE COUNCIL OF EUROPE has approved the final, definitive text of an international agreement combating race hate on the Internet. The agreement takes the form of an additional protocol to the CoE's 2001 Cybercrime Convention. (Page 5)

THE FRENCH GOVERNMENT has officially announced the implementation of the EC Electronic Communications Directive's provisions regarding e-commerce and personal data into domestic law (Page 6)

THE FRENCH DATA PROTECTION AUTHORITY has filed judicial complaints against five companies for alleged violation of national privacy laws linked to spamming (Page 7)

THE ACT ON ELECTRONIC SIGNATURES entered into force in Slovakia on May 1, 2002 (the "Act"). However, it was not possible to use electronic signatures fully in practice since further implementing regulations were required. These regulations were recently issued by the National Security Office, the governmental body in charge of electronic signature issues. (Page 10)

IN HUNGARY A recent case involving employment-related data protection issues has once again shed light on the dubious interpretation of the regulation of e-mail monitoring in the workplace (Page 9)

CASES

THE CANADIAN INTERNET REGISTRATION AUTHORITY (CIRA) has released the first decision in respect of a ".ca" domain name dispute under the CIRA Domain Name Dispute Resolution Policy (CDRP). *Report by Ian R. Hay of Blake, Cassels & Graydon LLP, Toronto.* (Page 15)

IN THE UNITED STATES The Supreme Court of Virginia has affirmed a decision granting comity to another state court's out-of-state discovery order regarding content on an Internet chat room. The case involved an action brought in the Superior Court of the State of California for the County of Los Angeles, in which Nam Tai Electronics alleged that a certain unknown individual had posted "false, defamatory, and otherwise unlawful messages" in an online chat room discussing the company's publicly traded stock. *Report by David Brownlie, Potter Group Legal Services, Chicago.* (Page 16)

COMMENTARY

UNITED KINGDOM: Adequacy of Cyber-Criminal Investigations: Is 'Big Brother' in Cyberspace? *By Cadgas Evrim Ergun, Cakmak Law Office.*

Cybercriminal investigations require international regulations as the Internet allows cybercrimes to be committed regardless of conventional state-borders. However, there is also strong criticism that cybercrime is being used by governments as a device to restrict personal privacy of electronic communications by citizens and that the legal response is disproportionate to the offence. (Page 19)

ITALY: Alternative Dispute Resolution: Online Arbitration and Mediation in Italy and the European Union in Comparison with the United States *by Alessandro del Ninno, of Studio Legale Tonucci* (Page 22)

IN THIS REPORT

NEWS

CASES

COMMENTARY

Submissions by Authors: The editors of *World Internet Law Report* invite readers to submit for publication articles that address issues arising out of the regulation of the Internet and e-commerce, either on a national or transnational level. Articles with an appeal to an international audience are most welcomed. Prospective authors should contact Nichola Dawson, World Internet Law Report, c/o BNA International Inc, Heron House, 10 Dean Farrar Street, London SW1H 0DX; tel. (+44) (0)20 7559 4807; fax (+44) (0)20 7233 2313; or e-mail: nicholad@bna.com.

WORLD INTERNET LAW REPORT

WORLD INTERNET LAW REPORT is published monthly by BNA International Inc., a subsidiary of The Bureau of National Affairs, Inc., Washington, D.C., U.S.A. Administrative headquarters: Heron House, 10 Dean Farrar Street London SW1H 0DX, England. Tel. (+44) (0)20-7559 4801; Fax (+44) (0)20-7222-5550; E-mail marketing@bnai.com. In the U.S. call toll-free on: 1-800-727-3116. Subscription price: U.S. and Canada U.S.$925/U.K. and rest of world £550. Additional copies of this publication are available to existing subscribers at half price when they are sent in the same envelope as a standard subscription.

Website: *www.worldtaxandlaw.com* *ISSN 1468-4438*

Publishing Director: **Deborah Hicks** ***Editorial Director:*** **Joel Kolko** ***Editor:*** **Nichola Dawson** ***Production Manager:*** **Nitesh Vaghadia**

Correspondents: *Canada:* Peter Menyasz; *France:* Arthur Rogers

News From Around the World

AUSTRALIA

Measures Introduced to Protect Consumers from Internet Dumping

The Minister for Communications, Information Technology and the Arts, Senator Richard Alston, has announced a package of measures to safeguard consumers against unexpected high telephone bills and "Internet dumping".

The package of measures has been developed following the release of draft regulations for public comment in May 2002.

The measures respond to ongoing consumer concerns about the practice of "Internet dumping". This practice occurs when, without the users knowledge or consent, Internet dialler software transfers users from their current Internet service provider (ISP), which they have usually accessed using an untimed local call, to a premium rate telephone number. Most content services of this kind are accessed in Australia through the 190 premium rate number range.

The package has also been developed to address concerns that children are gaining access through Internet diallers to sexually explicit Internet content, and in the process incurring unexpected high bills on their parents' telephone account.

The government is also responding to consumer concerns about the potential for unexpected high bills from other content services provided on the 190 number range or through 0011 (international) numbers.

An important part of the safeguard package are regulations which will give the Australian Communications Authority (ACA) a broad range of flexible powers to regulate the supply of premium rate services.

This package of measures also aims to limit exposure of telephone customers to unexpected high bills and give the ACA flexible powers to put in place other service provider rules. Most importantly, consumers will be informed so they can take proactive measures to protect themselves against unexpected high bills and Internet dumping.

Further information is available from the ACA website at *www.aca.gov.au*

AUSTRALIA

Online Censorship Legislation Criticised by Civil Liberties Watchdog

Electronic Frontiers Australia (EFA) has deemed the Federal Government's online censorship programme an expensive failure and expressed the view that the legislation is ineffective and should be repealed.

Under the new legislation, 'The Co-Regulatory Scheme for Internet Content Regulation', members of the public are permitted to complain to the Australian Broadcasting Authority (ABA), about prohibited material displayed on the Internet. As the regulatory body in this field, the ABA is then allowed to insist that any offensive material is taken down, provided it is hosted on an Australian server.

The criticism from EFA comes in response to a recent paper issued by the Department of Communications, Information Technology and the Arts which praised the success of the legislation and celebrated its effectiveness in regulating online content and protecting users (particularly minors) from offensive material.

EFA has said that the government has no evidence to support the claim made in the paper and that the government has made no effort to make publicly available any information on successful prosecutions resulting from the monitoring scheme.

The pressure group has also put forward the suggestion that much of the prohibited content reported to ABA is still online or accessible. EFA went on to charge the ABA with time wasting by spending the majority of its Internet censorship efforts investigating content on foreign-hosted websites over which is has no authority or control.

Reports have estimated that the censorship scheme costs AU$2.7 million per year.

The government is reported to be considering EFA's submission in the context of the current review of the legislation and has said that it will consider EFA's views along with everyone else's.

CANADA

Ontario Court Rules Internet Publication is Equivalent to a Newspaper

OTTAWA—Publication of material on the Internet is equivalent to publication in a newspaper for the purposes of assessing whether the material is libelous, according to the Ontario Court of Appeal.

Ontario's Libel and Slander Act in part defines a newspaper as a "paper" containing certain information for public distribution, and the word "paper" is broad enough to mean a newspaper published on the Internet, Justice Robert Armstrong wrote on behalf of the three-member panel in rejecting an appeal of a lower

court's finding that a writer was not entitled to sue a magazine for libel because he failed to provide adequate notice of the suit.

> "The purpose and scheme of the notice provision in the Libel and Slander Act are to extend its benefits to those who are sued in respect of a libel in a newspaper, irrespective of the method or technique of publication. To use the words of (the lower court judge), 'a newspaper is no less a newspaper because it appears in an online version' ", the ruling said.

If the conclusion that the word paper should be considered broadly is incorrect, and the term should be given a more restrictive meaning, then the requirements of the Act for notice within six weeks after the alleged libel would not apply, it said. But that result would clearly be "absurd", because it would mean that an action against a newspaper would be barred, but not an action against an online publication, it said.

The case involved a negative review by freelance writer Allan Weiss of a novel by science fiction writer Robert Sawyer in Realms Magazine, which was published in Realms' December 3, 1997 issue. Sawyer took strong exception to the review and e-mailed a letter of complaint to the magazine alleging that Weiss was in a conflict of interest because of a prior personal dispute between the two and other negative comments. Weiss alleged that the letter was libelous and that it had been published on the magazine's Internet site, while Sawyer argued that the letter never appeared on the site.

An Ontario Court of Justice ruling found that the libel action could not be heard because Weiss did not provide notice as required in the Libel and Slander Act. Weiss' lawyer argued before the original and appellate courts that the notice requirement only applied if the letter was published in print form. The Court of Appeal ruling found that Weiss was entitled to continue a portion of his action related to the faxes of the alleged libelous letter to local newspapers and to the original e-mail of the letter to Realms Magazine. Because any republication of a libel is a new libel, and because the faxes were not published by the newspapers, they were not subject to a notice requirement, Weiss is entitled to continue his libel action related to them, if he chooses to do so, the ruling said.

The e-mail transmission, meanwhile, was not mentioned in the original court ruling, but was raised as an issue in the appeal, it said. Since the e-mail was received by the magazine's editors, it represents a separate publication of the alleged libelous material, it said.

"As in the case of the faxes, no notice is required in regard to the e-mail transmission. The plaintiff therefore is entitled to continue his action in regard to the e-mail transmission if he chooses to do so", it said.

The ruling is available on the Internet at *www.ontariocourts.on.ca/decisions/2002/september/weissC37351.htm.*

(*Allan Weiss v. Robert Sawyer, Ontario Court of Appeal*, File #C37351, judgment rendered Sept. 19, 2002)

CANADA

Independent ISPs Warn Market Domination Will Lead to Higher Prices

The strategy by Canada's largest cable companies to drive independent ISPs out of business spells trouble for Canadian Internet users, who will be bound as a result to experience large price increases in their high speed Internet services coupled with increasingly poor customer service.

This is the view expressed by a sub-group of the Canadian Association of Internet Providers (CAIP) in a recent submission to the Canadian Radio-television and Telecommunications Commission (CRTC). The sub-group, known as the Independent Members of CAIP (IMCAIP), also plans to take its message to parliamentarians over the next few months.

> "The cable industry has made it quite clear that, if all goes according to its plans, independent ISPs will soon be extinct", said Jay Thomson, President of CAIP, on behalf of IMCAIP. "Canadians know … how they felt about cable TV prices and service before the cable companies faced competition from satellite TV services. They better start preparing themselves for a repeat of those days with their Internet services if the cable companies succeed in driving out competition from independent ISPs."

Mr. Thomson was referring to a statement made some months ago by the head of the cable industry's lobby group that cable's new low-priced "Cable Lite" service is intended to "put dial-up [Internet services] on the shelf along with the eight-track cartridge". As IMCAIP makes clear in its CRTC submission, the cable companies are marketing their "Cable Lite" services at prices designed to cannibalise the dial-up market served by independent ISPs while preventing independent ISPs from offering the same type of "lite" service, or any competitive cable high speed service for that matter. IMCAIP also raises similar concerns about the telephone companies' new ADSL "lite" services.

The IMCAIP submission asks the CRTC to prevent the incumbent cable and telephone companies from continuing to price their high speed services at anti-competitive levels and to force them to make their "lite" services available to third-party ISPs at competitive rates.

A copy of the submission is available at *www.caip.ca/issues/infrastr/Cable_Access/PartVII_20021112_application.pdf*

CHINA

External Organisations Permitted to Register a Country Domain Name

The development of the Internet within China is set to receive a boost in December 2002, as CNNIC (www.cnnic.net.cn/e-index.shtml) the authority responsible for administering and managing the .cn domain, opens its doors to businesses outside of China.

Until now, only entities with Chinese ownership or a physical address within China have been eligible to apply for .cn domain names. This is set to change in December 2002, with the introduction of liberal rules enabling non-Chinese based companies to register within the .cn domain. CNNIC is expecting a rush of foreign businesses, as well as brand owners, eager to secure their presence in China by registering .cn domain names – particularly given China's recent accession to the World Trade Organisation.

NeuStar (www.neustar.com.cn) the administrator of .us and .biz, is overseeing the appointment of .cn registrars outside China on behalf of CNNIC. Although details of the appointed registrars have not yet been published, NeuStar is due to release this information shortly. Non-Chinese businesses will then be able to register .cn domain names on a "first come, first served" basis. Businesses with a current or potential interest in China are advised to register their brand and company names within .cn to ensure they do not miss out.

Dora Chow and Simon Moran, CMS Cameron McKenna; e-mail: dora.chow@cmck.com; simon.moran@cmck

EUROPEAN UNION

Council of Europe Passes Measure To Combat Race Hate on Internet

STRASBOURG—Ministers representing the 44 member nations of Council of Europe (CoE) approved on November 7, 2002, a final, definitive text of an international agreement combating race hate on the Internet.

The agreement takes the form of an additional protocol[1] to the CoE's 2001 Cybercrime Convention (*see WILR, Vol. 3, issue 1, January 2002*).

Parties to the protocol are required to outlaw racist and xenophobic material and content that amounts to Holocaust denial. They are also obliged to offer cross-border co-operation in investigations and prosecutions.

The main Convention's 34 signatories include the United States, Canada, and Japan. The three nations have observer status at the CoE and participate in drafting CoE treaties.

Specialists from the U.S. Department of Justice and its Canadian counterpart were involved in drafting both the Convention and the new protocol.

The protocol is scheduled to be opened for signature at a ceremony during the January 27–31, 2003 session of the CoE Parliamentary Assembly. The Convention was opened for signature on November 23, 2001, but will not come into force until five states have completed ratification.

In adopting the protocol text, the CoE Committee of Ministers did not act on demands from the Parliamentary Assembly for changes to the final draft. In September 2002, the Assembly claimed that the protocol had been weakened, under pressure in particular from the United States.

Parliamentarians complained that the text fails to establish an offense of "unlawful hosting" – and allows parties to enter a reservation allowing them to opt out of the obligation to impose penal sanctions or to set up other efficient remedies.

Assembly members feared for the effectiveness of the agreement if the United States declines to co-operate, given that 2,500 of the 4,000 racist sites currently identified are hosted in the USA. (DoJ officials had argued in negotiations on the original Convention that the federal government could not make commitments on issues of criminal law for which individual states are responsible).

A report from the Assembly's Legal Affairs Committee has acknowledged that case law in the U.S. Supreme Court had held that hate speech is punishable only if there is an imminent threat to a specific person. The same report pointed to U.S. constitutional protection for freedom of speech.

The Assembly, a consultative body that consists of delegations from national parliaments, has no powers to amend draft treaties.

Peter Csonka, a senior official in the CoE directorate for criminal justice affairs, told WILR: "Ministers adopted the final draft without making any alterations".

A CoE statement explained that the protocol aims:

> "to harmonise substantive criminal law in the fight against racism and xenophobia on the Internet, and to improve international co-operation in this area, while respecting the right to freedom of expression enshrined, more than 50 years ago, in the [CoE] European Convention on Human Rights".
>
> "All the offenses recognised by the protocol must be committed 'intentionally' for criminal liability to apply", the statement continued. "A service-provider will not be held criminally liable for having served as a conduit for, or having hosted, a website or newsroom containing such material, unless the intentional nature of the dissemination of racist and xenophobic material can be established under domestic law in each given case."

1 Additional Protocol to the Convention on Cybercrime concerning the criminalisation of acts of a racist or xenophobic nature committed through computer systems. Further background, with a links to the texts of the Convention and the protocol can be found at: *www.coe.int* - Theme files/All files.

EUROPEAN UNION

Commission Plans to Introduce Minimum Quality Standards for Websites Providing Health Advice

Industry and Information Society Commissioner Erkki Liikanen, is rumoured to be contemplating the introduction of a common E.U. standard that would reinforce consumer protection in connection with healthcare and pharmaceutical websites.

The Commission is said to mainly criticise medical websites for providing incomplete or inaccurate information, failing to disclose the credentials of their sources and failing to specify which information is editorial and which is based on sponsors. No details about the forthcoming legislation have yet been disclosed.

It is likely that the European Commission will seek to strengthen transparency on the purpose of medical sites, to enforce strict privacy criteria for the treatment of personal data and recommend effective monitoring of medical websites in Member States.

Christopher Kuner, Hunton & Williams, Brussels; e-mail: ckuner@hunton.com

EUROPEAN UNION

Current Status of .eu Domain Names

The .eu domain is to be introduced pursuant to Regulation (EC) No. 733/2002, which was adopted by the European Parliament and the Council in April 2002. The .eu domain will become the first continent specific domain to be made available for registration, allowing European individuals and companies to create a truly European identity on the Internet. Given the saturation of .com registrations and the fact that the majority of these are registered to U.S. entities, .eu will be an important tool in tackling what is perceived by some as U.S. cyberspace hegemony. Demand will be high and preparation is the key to successfully registering key brands under .eu.

Registrations will commence with a sunrise period during which intellectual property owners will be given the opportunity to pre-register .eu domain names based on trademark rights. Following the sunrise period, registrations will open up on a first come, first served basis to organisations established within the European Union or E.U. citizens. Alpha 2 country codes will not be allowed for registration under .eu (*e.g.* .fr.eu, .de.eu). A domain name disputes procedure will also be made available to tackle illegitimate registrations, particularly those that infringe prior existing intellectual property rights.

At this stage no dates have been determined as to when registrations under .eu will commence, however we anticipate that this will be during the summer of 2003. Prior to this though, a number of procedural steps have to be completed.

First, pursuant to a call by the European Commission for organisations to run the .eu registry, a non- profit organisation should be chosen in February 2003 to:

> "organise, administer and manage the .eu TLD in the general interest and on the basis of principles of quality efficiency, reliability and accessibility". (Article 4 (2) (a) of Regulation (EC) No 733/2002).

The registry cannot itself act as a registrar and will be responsible for the accreditation of private sector registrars who will handle domain name applications.

The decision of the Commission on the selection of the registry, after consultation with Member States, is expected to be announced in February 2003, with a contract to be signed between the Commission and the registry in April 2003. Subsequent to this, the following steps should be completed by the second quarter of 2003:

- Formulation and adoption of the public policy rules and public policy principles on registration by the Commission in consultation with Member States, and the registry.
- Formulation and adoption of the registration policy by the Commission in consultation with Member States, and the registry.
- Proposal of a blacklist of geographical and/or geopolitical names by E.U. Member States which will either be disallowed from registration, or restricted to registration under an appropriate second level domain. Intellectual property owners will be given 30 days to object.
- Notification of the designated registry to the Internet Corporation of Assigned Names and Numbers (ICANN), and start of the delegation process by ICANN.
- Adoption of the procedure for accreditation of registrars by the .eu registry.

A number of registration companies are beginning to offer pre registrations for .eu domain names despite the fact that the registry has not yet been chosen, and the registration policy has not been formulated. These companies should be treated with caution and any pre-payments for .eu domain names to these companies should be avoided.

David Taylor, Lovells, Paris; e-mail: drd@lovells.com

FRANCE

Government to Implement Electronic Communications Directive Provisions on E-Commerce and Personal Data

The French Government has officially announced the implementation of the EC Electronic Communications Directive's provisions regarding e-commerce and personal data into domestic law. According to the French government, the purpose is to ensure the transparency of transactions for the benefit of the consumers

by providing them with information. The next legal step will address the security of electronic exchanges to encourage e-commerce development.

In addition, this bill – which will be proposed before December 31, 2002 – will not be limited to e&#30;commerce rules – but may also define the legal framework concerning "spamming" by e-mail. On that matter, the French Government tends to favour an opt-in system for e-mail marketing based on the prior consent of the web user to receive advertising by e-mail. Therefore, France will follow the European Commission position. However, it is worth noting that the legal framework regarding electronic communication is included in this bill, and not in the bill currently before the French Parliament, which deals with data protection – notably, with the overdue implementation of the E.U. general Data Protection Directive into French law.

Alexandre Menais, Lovells, Paris

FRANCE

French Data Protection Authority Releases Report on Spamming and Files Complaints for Alleged Violation of National Privacy Laws

On November 21, 2002, the French Data Protection Authority (the "CNIL")[1] released a report on spamming and named five companies it believes have criminally infringed French law on data protection. Their records have been transmitted to the Paris Court's Criminal Prosecution Office,[2] which will then decide whether or not to prosecute the companies.

The CNIL is an independent public body, which has been in charge of data protection in France since 1978. It follows up the proper implementation of the data protection rules in France. Therefore, it issues recommendations and reports; and it receives and manages the formalities required before any automated data processing takes place. It also notifies infringers and has the power to refer cases to a Criminal Prosecution Office.[3]

The Internet brought new and wide-ranging opportunities to collect and process data. This created new challenges to the implementation of very protective French rules applicable to personal data processing. As a consequence, the CNIL has kept a close eye on the technical evolutions arising from the Internet. Since 1997, it has released numerous reports and recommendations on the interpretation of the existing rules to this new medium. In particular, it stressed the requirement for systematic prior information of the data subject before any collection of data can take place. This was especially relevant in the area of unsolicited commercial communications *via* e-mails, a.k.a. "spamming".

Since an e-mail address relates either directly (john.doe@lw.com) or indirectly (webmaster@lw.com) to an individual, it constitutes personal data. The CNIL defines spamming as sending large amounts of unsolicited e-mail to recipients with which the sender (i) had no prior contact and whose address it collected irregularly[4] or (ii) had a prior contact but for a different purpose.[5]

In this respect, a European Directive recently entered into force, which provides that

> "The use of […] electronic mail for the purposes of direct marketing may only be allowed in respect of subscribers who have given their prior consent". However, "where a natural or legal person obtains from its customers their electronic contact details for electronic mail, in the context of the sale of a product or a service, […] *(it)* may use these electronic contact details for direct marketing of its own similar products or services provided that customers clearly and distinctly are given the opportunity to object […]".[6] This system has been referred to as "soft opt-in".

Currently, French law[7] provides for an "opt-out" system with respect to marketing means, *i.e.* consumers may receive unsolicited e-mails until they oppose (expressly excluding automated telephone calls and faxes, for which "opt-in" is required). However, a much-anticipated draft "Digital Economy Bill" was unveiled on November 25, 2002,[8] which would require the prior consent of the recipient, along with the same exception as Section 13 (2) of the said Directive. The draft Bill, which derives from a previous "Information Society Bill", is expected to become an Act by mid-2003.

Spamming carries no specific sanction under French law. However, it comprises a number of acts (collecting, mass-sending, transferring addresses), which may infringe data protection or other regulations.

In order to assess and fight against spamming, the CNIL opened an e-mail account in July 2002 (spam@cnil.fr). All spammed Internet users were asked to forward the spams they received to this account. In the space of three months, over 325,000 e-mails were sent and reviewed.

With a view to informing both individuals and companies, the CNIL adopted a three-tier attitude:

- it published the result of its analysis of the forwarded e-mails;
- it publicised its decision to expose some particularly significant spammers; and finally
- it released a toolkit about spamming and how it should be handled.

In the first-ever assessment of spamming in France by a public body, the CNIL analysed the content and features of the messages it had received. It emerged that 85 percent of all spams were English-written, 8 percent Asian-written and 7 percent French-written. The advertised services were mostly porn-related, financial products, medical products, tourism and online casinos.

Criminal Sanctions Applicable to the Targeted Spammers

As an exemplary sanction, the CNIL has taken five resolutions to transmit the information it had gathered

in relation to the five companies to the Paris Court's Criminal Prosecution Office. The latter will in turn decide to open (or not) criminal proceedings in relation thereto. Four out of five of the targeted companies are French: Alliance Bureautique Service (ABS) (e-mail addresses extraction software); Suniles (tourism); le Top 50 du "X" (porn websites); and BV Communication (dating). The fifth one is Great-Meds.com (online sale of medicines, presumably, U.S.-based).

These companies could face heavy criminal sanctions on the basis of the misdemeanours constituted by absence of prior declaration, unfair data collection and failing to provide the recipients of the e-mails with the opportunity to oppose the data processing.

Section 226–16 of the French Criminal Code provides that

> "to carry out, or to cause to be carried out, the automated processing of personal data without having observed, prior to the operation, the *preliminary formalities* laid down by law, is punished by three years' imprisonment and a fine of EUR45,000, even where committed through negligence". [Emphasis added]

The CNIL noticed that none of the spammers had complied with the prior formalities requirement before they started collecting personal data and using it to spam.

Section 226–18 of the same Code in turn provides that

"the *collection of data by fraudulent, unfair or unlawful means*, or the *processing* of personal data *despite the opposition* of the data subject, where this objection is based on legitimate grounds, is punished by five years' imprisonment and a fine of EUR300,000". [Emphasis added]

As such, collecting e-mail addresses without the knowledge or the authorisation of the natural person – or data subject – to whom they relate, constitutes collection of personal data by unfair means. The CNIL was informed that, usually, either the spams do not provide recipients with the opportunity to oppose to the processing, or the address they provide serves as a confirmation of the validity of the recipient's address. Therefore, in the present case, the CNIL considered that the spam recipients were not granted the right to oppose.

It is worth noting that under French law, where specifically provided, legal persons may incur criminal liability, with fines increased five-fold and additional sanctions such as, *inter alia*, winding-up or prohibition to practice a professional activity. All misdemeanours cited in this study extend their sanctions to legal persons.

Other Sanctions Applicable to Spamming

The CNIL has identified criminal offenses relevant to spamming, although they did not fit with the facts it had analysed.

First, hacking computers in order to get e-mail addresses or to send spams carries heavy sanctions in France. Section 323–1 of the French Criminal Code prohibits unauthorised access to automated data processing systems (computers). Fraudulently accessing or remaining within all or part of a computer bears sanctions of one year's imprisonment and a fine of EUR15,000.

Secondly, attacks to computer systems, such as "mail bombing"[9] falls under Section 323–2 of the French Criminal Code, which prohibits obstructing or interfering with the functioning of a computer, with three years' imprisonment and a fine of EUR45,000. Here again, legal persons may incur heavy criminal liability.

As concerns civil remedies, the CNIL pointed out the possibility to terminate an Internet service agreement where a user was identified as a spammer. This is possible on the basis of breach of terms of conditions and/or of the customs that apply online (Netiquette).[10]

The CNIL did not mention other sanctions in relation to data protection, despite a previous thorough analysis, mainly based on Directive 95/46/EC.[11] In particular, compliance with the purpose of the processing is mandatory. Section 226–21 of the French Criminal Code sanctions diverting personal data from its proper purpose by five years' imprisonment and a fine of EUR300,000. This Section covers the purpose of legitimate personal data files, where the processing goes beyond what had been declared to the CNIL. This is in line with Section 13(2) of the 2002/58/EC Directive and with the wide definition of spamming usually provided by the CNIL.

Moreover, as concerns transfers and assignments of data files, Section 226–22 of the said Code sanctions bringing personal data to the knowledge of a third party who has no authority to receive it without prior authorisation of the concerned person by one year's imprisonment and a fine of EUR15,000.

It is to be noted that the application of French criminal law to foreign natural and legal persons is an issue. Since spamming is not criminally sanctioned as such, attaching criminal liability to the sender's offence (data processing, hacking, *etc.*) may not be straightforward under French law, because of confined, connecting factors. In this respect, Section 113–7 of the French Criminal Code provides that "French criminal law is applicable to any felony, as well as to *any misdemeanour punished by imprisonment*, committed by a French or *foreign national* outside the territory of the French Republic, where the *victim is a French national* at the time the offence took place".

This Section gives so-called "universal competence" to the French criminal Courts, in circumstances where a French national falls victim to acts performed abroad. No reciprocity is required, *i.e.* regulation of spamming in the country of the sender is not a requirement for French criminal law to apply. Pursuant to this Section, foreign companies, such as Great-Meds.com, could face criminal exposure if any individual adversely affected by their activities is a French national.

Toolkit Against Spamming

The CNIL announced its decision to close its "spam-box" and to set up a toolkit against spamming. It is intended to provide both legal and technical advice to

prevent and fight against spamming. The CNIL has relied upon the assistance of French ISPs, consumer associations and distance-sellers to provide up-to-date and efficient information to Internet users and providers alike and help to make the initiative a success.

1 *Commission Nationale de l'Informatique et des Libertés*, set up by Act 78-17 January 6, 1978.
2 *Procureur de la République de Paris*.
3 Since 1978, the CNIL has referred only 25 cases to Criminal Prosecution Offices. A Bill implementing Directive 95/46/EC under French law provides the CNIL with more direct power to impose administrative sanctions, including fines. It should become an Act in 2003.
4 For example, in websites, chat-rooms, mailing lists or forums.
5 Though this second case, which is part of the CNIL's usual definition of spam, is not mentioned in the instant report.
6 Section 13 (1) and (2) of Directive 2002/58/EC of the European Parliament and of the Council of July 12, 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications). This Directive should be implemented in all Member States by October 31, 2003.
7 Ordinance n° 2001-741, JO n° 196, August 25, 2001 n° 13645, which inserted Section L. 121-20-5 of the French Consumer Code.
8 Text available, in French, at *www.lesechos.fr/evenement/pjl_eco_numerique.pdf*. More information, in French, at *www.premier-ministre.gouv.fr/fr/p.cfm?ref=36713&d=1*.
9 Lyon Civil Court of First Instance, February 20, 2001, Paris Criminal Court of First Instance, May 24, 2002.
10 Rochefort sur Mer Civil Court of First Instance, February 28, 2001, Paris Civil Court of First Instance, January 15, 2002.
11 "Le publipostage électronique et la protection des données personnelles" (electronic mass mailing and personal data protection), report by Ms. Alvergnat, October 14, 1999.

Laurent Szuskin and Fabien Lesort, Latham & Watkins, Paris; e-mail: laurent.szuskin@lw.com and fabien.lesort@lw.com

HUNGARY

Opinion Issued on E-Mail Monitoring, Internet Use in the Workplace

A recent case involving employment-related data protection issues has once again shed light on the dubious interpretation of the regulation of e-mail monitoring in the workplace.

The Hungarian Labour Code ("Labour Code") provides that an employer may only ask for information and personal data from an employee if it does not infringe their personal rights and it is relevant in respect of their employment. An earlier opinion published by the Parliamentary Data Protection Commissioner ("Data Protection Commissioner") provides some initial guidance on how these general provisions of the Labour Code could be interpreted in the case of e-mail monitoring by employers.

Different Approaches

According to the Data Protection Commissioner, a different approach should be applied between e-mail addresses accessed solely by the employee (for example, *a.person@companyname.hu*) and e-mail addresses used for the purposes of the employer (for example, *info@companyname.hu*). The latter may be monitored and freely accessed by the employer. The former, however, which are considered to be personalised e-mail addresses, cannot be monitored or accessed by the employer (similar to phone conversations and personal letters) without obtaining the consent of the employee.

The Data Protection Commissioner also states that data relating to the habits of an employee's Internet usage (*i.e.*, frequency of usage, type of websites, *etc.*) will constitute personal data. If Internet usage is prohibited for non-professional purposes (*i.e.*, outside the scope of the work), an employee's Internet usage may be monitored by the employer. An employee's attention must be drawn, in advance, to the rules on Internet usage in the workplace. In other cases, monitoring the employee's Internet usage constitutes unlawful processing of personal data.

This opinion of the Data Protection Commissioner is criticised and disputed among experts, as there are many aspects of the opinion, which do not reflect reality. However, it is important to note that the opinion of the Data Protection Commissioner is not binding on courts or other authorities. In any event, there are no published precedents in this respect, and, as such, this opinion may still strongly influence the daily practice of Hungarian employers.

By Andras Lendavi, Linklaters, Budapest; e-mail: andras-lendavi@linklaters.com.

ITALY

Implementing Legislation for the Electronic Signatures Directive is Enacted

Italy has recently enacted Legislative Decree No. 10 of January 23, 2002 (the "Decree") to implement the Directive 1999/93/EC on a community framework for electronic signatures (the "Directive").

Italy already had a detailed set of rules governing electronic signatures and electronic documents as set out in Presidential Decree No. 445 of December 28, 2000. As a result, the implementation of the Directive resulted in certain overlaps between the existing domestic framework and the E.U. requirements for electronic signatures. The Decree has partially amended the existing legislation and created new provisions as required.

Italian law already provided for a "digital signature" system based on asymmetric keys and authorised certification service providers. However, the Decree introduced a distinction between advanced electronic signatures and electronic signatures (the latter are also known as "light" signatures).

The Decree defines the electronic signature as data in electronic form which are attached to or logically associated with other electronic data and which serve as a method of authentication. A document signed with a "light" signature satisfies the legal requirements of being

in written form and can be admitted as evidence according to a fair evaluation which considers the security and quality aspects thereto. As set out in the Directive, the advanced signature is obtained through a procedure that guarantees the identification of the signatory uniquely and links the latter to the signature itself.

The Decree specifies that the document undersigned with an electronic signature cannot be denied legal effectiveness and admissibility as evidence in legal proceedings solely on the grounds that it is in electronic form, or not based upon a qualified certificate issued by an accredited certification service provider or not created by a secure signature-creation device.

The provision of certification services by entities located in Italy or in any other E.U. State is not subject to a prior authorisation. A certification service provider intending to release qualified certificates is required to send a notice to the Innovation and Technology Department, at the Italian Ministry Council, before beginning its activity. The certification service provider is liable for damages to any entity who reasonably relies on that certificate as regards the accuracy and the completeness of the information therein.

Finally, a regulation is due to be adopted to implement the provisions of the Decree and the Directive. It is also expected that the regulation will clarify issues relating to specific requirements for certification service providers. The first draft of the regulation was approved by the Italian Ministry Council on August 2, 2002 and the final version is yet to be published.

Daniela De Pasquale, Gianni, Origoni, Grippo & Partners, Milan; e-mail: d.depasquale@gop.it

THE NETHERLANDS

Court Fails to Provide Clear Guidance to ISPs on Unlawful Content

On November 7, 2002, the Amsterdam Court of Appeal confirmed the judgment handed down by the Amsterdam District Court on April 25, 2002 by dismissing the appeal of XS4ALL in the so-called Radikal case against Deutsche Bahn German Railways company.

XS4ALL lodged an appeal, because in their opinion the judgment of April 25, 2002 provided no guidance as to how providers should deal with complaints about allegedly unlawful content. The Court has upheld the judgment, which required Internet Service Provider XS4ALL to block information on a subscriber's website and to disclose the subscriber's name and address. The disputed website contained two articles from the radical-left magazine Radikal in which instructions were given to disrupt the German Railways in protest against the transport of nuclear waste by rail.

Reference is made to the Scientology versus XS4ALL case of June 9, 1999 in which the Court decided that providers must take action if they are informed of material infringing copyright or other rights on their servers, when there are no reasonable grounds for doubting the correctness of the notice. However, the Scientology case dealt with copyright infringement while the Radikal case deals with unlawful expressions of another nature.

According to the Court, XS4ALL knew or should reasonably have known, after the notification by Deutsche Bahn that the information in question was unlawful. In this particular case the Court considered the displayed information obviously unlawful because visitors to the website are urged to carry out instructions to sabotage the German Railways. In other words, the articles incite people to commit a criminal offence. Furthermore the Court considered that even though the sabotage mentioned in the articles is not aimed at causing accidents, it cannot be ruled out that accidents will happen as a result of it and that persons will be in danger. Therefore, XS4ALL should have removed this information immediately. As the Scientology case has already shown, ISP's should take action when subscribers commit unlawful acts. The Court stated in the Radikal case that an ISP is not obliged to remove or block the information upon first notice

> "... for example in the case of information which is *allegedly offensive* or *allegedly breaches copyright* ...".[1]

In such cases the ISP must request more detailed information from the complainant and the subscriber.

However, the Court has again failed to provide clear guidance as to when certain information is indisputably unlawful, consequently failing to make clear when a provider is obliged to infringe the privacy and freedom of speech of its subscribers [ENMV].

The decision of the Amsterdam Court of Appeal can be found on www.rechtspraak.nl under LJN number AF0091

1 Consideration 4.9 of the Amsterdam Court of Appeal judgment (November 7, 2002).

Eva Visser, Stibbe, Amsterdam

SLOVAK REPUBLIC

New Regulations Enable Full Use Of Electronic Signatures In Practice

The Act on Electronic Signatures entered into force in Slovakia on May 1, 2002 (the "Act"). However, it was not possible to use electronic signatures fully in practice since further implementing regulations were required.

These regulations were recently issued by the National Security Office, the governmental body in charge of electronic signature issues, and are in force as of October 1, 2002. They lay down in detail the conditions for the practical operation of electronic signatures, such as: the form and the process of creating a guaranteed electronic signature; signature schemes, algorithms,

and the parameters of these algorithms which are necessary to create guaranteed electronic signatures; and the procedure for using electronic signatures in commercial and administrative relations.

An electronic signature is defined in the Act as "information attached or otherwise linked to an electronic document". This information consists of a "private" key which, when used with its connected "public" key, allows the document to be verified. In practice, this means that the recipient of the document may verify the authenticity and inviolability of the electronic document with a publicly available certificate. This certificate contains:

- the name of the person who will use the signature;
- the date of issuance;
- the date of expiry of the signature; and
- the public code for the person who will use the signature. The public code thus fulfils the same role as a notary public does for the verification of documents in written form.

An electronic signature is considered as equal to a hand-written signature for both private transactions and communications with governmental authorities.

Two Levels Of Security

Electronic signatures and certificates are issued in Slovakia by certification authorities and have two levels of security—a so-called "common electronic signature" and a "guaranteed electronic signature". A common electronic signature is issued by a Certification Authority and has no "time seal" attached to it. A guaranteed electronic signature is issued by an Accredited Certification Authority and has a "time seal", which is an attachment which enables the recipient to identify the exact date and time of its execution. For communications with governmental authorities, a guaranteed electronic signature is required.

It is foreseen that, in the relatively near future, further reforms will be made to admit electronic signatures in civil, criminal and administrative proceedings, and that electronic filing with courts and other governmental authorities, including tax authorities, should be enabled.

The National Security Office oversees the activities of Certification Authorities and Accredited Certification Authorities. A (non-accredited) Certification Authority does not need a licence to perform its role; it merely notifies the National Security Office that it has started operating. An Accredited Certification Authority does require a licence, which will be issued by the National Security Office. So far no such licences have been issued, but at least three bodies have recently filed applications with the Office.

Marie-Helene Cote, Linklaters, Bratislava; e-mail: marie-helene.cote@linklaters.com

SWEDEN

New Rules for Country Domain Name to be Introduced

New rules for registering.se domain names are set to simplify the registration procedure, making it less complex and removing the need for prior assessment of applications.

Under the new system, which is set to come into force in April 2003, anyone will be permitted to register under the Swedish top-level domain "se".

Domain names will be assigned by the registrar on a "first come, first served" basis.

A provision for dispute resolution proceedings will also be provided for under the new system, whereby a domain name can be deregistered if the holder lacks a right or justified interest in the domain name and if the domain name is registered in bad faith.

SWITZERLAND

Basel E-Banking Group Asks for Feedback on New Paper Identifying Key Risk Issues

A working group established by the Basel Committee on Banking Supervision has announced that it would like to receive comments on a new paper highlighting the risks and responsibilities in cross-border electronic banking.

In October, the Basel Committee's Electronic Banking Group released *Management and Supervision of Cross-Border Electronic Banking Activities*, a 17-page paper that identifies risk management responsibilities in cross-border electronic banking and the need for effective home country supervision.

The EBG wants comment from bankers on specific principles set out in the new paper and on the roles of home country banking supervisors, said Hugh Kelly, special advisor for global banking at the Office of the Controller of the Currency and the OCC's representative to the EBG.

He said the paper should encourage bankers to ask key questions about their operations before they use the Internet to offer products and services in other countries.

Assess Risk First, Paper Says

The first portion of the EBG paper calls on banks, before they offer products and services in other countries through the Internet, to assess the risks – such as regulatory requirements of and local business practices in particular nations – and to establish an effective risk management programme for those activities.

As part of that effort, the EBG paper also urges bankers to give potential customers in other countries plenty of specific information about the bank

> "Before engaging in cross-border e-banking transactions with foreign customers, a bank should ensure that adequate information is disclosed on its website to allow potential customers to make a determination of the bank's identity, home country, and whether it has the relevant regulatory license(s) before they establish the relationship," the paper said.

Supervisory Roles Spelled Out

The second portion of the EBG paper spells out the roles for home country supervisors and promotes co-operation between banking supervisors. According to Kelly, the EBG wants to encourage supervisors to assert authority when needed – for example, in making licensing decisions – while minimising regulatory burden on bankers.

Among other points, the paper encourages bankers – as part of the initial due diligence effort – to consider consulting with supervisors in other nations on issues that might arise in connection with certain activities.

Kelly said the EBG wants the paper to spark an ongoing dialogue on risk and how to manage it.

> "We know it's a complicated issue, but we think this paper will provide some added value and hopefully promote some dialogue on these issues," he said

Comments on the paper may be sent to national supervisory authorities and central banks and may also be sent to the Secretariat of the Basel Committee on Banking Supervision at the Bank for International Settlements, CH-4002 Basel, Switzerland. Comments may be submitted via e-mail *jean-philippe.svoronos@bis.org.*

The Electronic Banking Group's paper is available at the website of the Bank for International Settlements, *www.bis.org/publ/bcbs93.pdf*

UNITED KINGDOM

Content Regulator Takes First Action Under E-Commerce Directive

The U.K. premium rate services regulator ICSTIS has become the first U.K. content regulator to take action under the recently-implemented Electronic Commerce (EC Directive) Regulations 2002. In a move welcomed by the Department of Trade and Industry, the nominated U.K. co-ordinator for all e-commerce cases, ICSTIS has fined and barred two online sexual entertainment service providers, and reported both cases to the National Hi-Tech Crime Unit.

The two cases involved website content promoted by two different service providers, Spanish-based Greenock and German-based Premium Call GmbH. The promotional material repeatedly referred to sexual acts involving children, while the dialler software used to access both companies' websites at premium rate charges of £1.50 per minute downloaded automatically without users' knowledge and appeared to be deliberately designed to mislead users into running up huge phone bills.

ICSTIS imposed a fine of £75,000 on Greenock and a fine of £50,000 on Premium Call GmbH, while access to both services was barred for a period of two years. Both companies were also instructed to offer redress to complainants.

In emphasising its commitment to protecting U.K. consumers, ICSTIS Chairman Sir Peter North said:

"The use of premium rate charging as a way of paying for Internet and other content has considerable potential, but consumers have to be able to use the payment mechanism with confidence. All services depend on consumer trust, and all services suffer when that trust is abused. The sanctions imposed on Greenock and Premium Call GmbH reflect the serious consumer harm caused by their services and serve as a warning to others that we will not hesitate to take decisive action to protect U.K. consumers from such abuse."

Under the E-Commerce Directive, ICSTIS is permitted in "cases of urgency" involving matters of public policy (particularly the protection of minors and consumers) to take direct action against service providers based in other European Union Member States.

This was the basis on which action was taken against the offending Spanish and German websites. The action taken was similar to that followed by ICSTIS under the Emergency Procedure contained in its own Code of Practice.

In both cases, and in keeping with the Directive, ICSTIS' direct action was notified to the European Commission and the Department of Trade and Industry (DTI), who welcomed the move.

Further information about the adjudications against Greenock and Premium Call GmbH, along with details of ICSTIS and its work can be found online at *www.icstis.org.uk*

UNITED STATES

Congress Approves Legislation Granting Relief to Small Webcasters

The Senate and the House of representatives has approved an amended version of legislation (H.R. 5469) intended to grant small webcasters relief from paying large royalty payments to the recording industry for streaming copyrighted music online.

The bill was passed after Sen. Jesse Helms (R-N.C.) lifted his hold on the measure, placed at the request of religious broadcasters. Broadcasters were concerned that the original version of the bill would have set a precedent for making royalty payments to the recording industry.

Senate Judiciary Committee Chairman Patrick Leahy (D-Vt.) had been attempting to shepherd the bill through the Senate after it passed in the House in October 2002 (195 DER A-22, 10/8/02). The House version of the bill was a compromise resulting from intense negotiations between the recording industry and webcasters.

The new version of the bill, dubbed the "Small Webcaster Settlement Act of 2002", would allow the recording industry to negotiate individual or group agreements with small webcasters. Observers said, however, that the specific financial terms set out in the original bill would apply to these new agreements.

In the original bill, small webcasters were defined as those with gross revenues of less than $1 million from the period beginning November 1998 through to June 2002, and less than $500,000 in 2003.

Under the original bill, the payment period for royalties would have extended from October 28, 1998 to December 31, 2004. The rate from 1998 until the end of 2002 would have been eight percent of a webcaster's gross revenues during that period, or five percent of a webcaster's expenses, whichever was greater. The rate would have increased in 2003 and 2004, to 10 percent of the webcaster's first $250,000 in gross revenues and 12 percent of any revenues in excess of $250,000 during the year.

Recording Industry Supportive

The new Senate bill essentially authorises SoundExchange, which is the organisation charged by the recording industry to collect royalty payments, to reach agreements with small commercial and non-commercial webcasters.

"The recording industry did not seek nor propose this authorization", according to a statement released by the Recording Industry Association of America, which supported the compromise bill.

In a statement, Leahy said he expected the rates set forth in the original version of H.R. 5469 to be implemented so that small webcasters could calculate their royalty payments as a percentage of revenue.

"Those rates were the product of tough negotiations under congressional guidance and will likely continue to serve as the basis for any agreement negotiated under the amended legislation", he said.

Webcasters, represented in part by the Digital Media Association, called the compromise bill a win for everyone.

> "Today's congressional approval of the Small Webcaster Settlement Act is a victory for all consumers and all providers of Internet radio", said Jonathan Potter, executive director of DiMA.

Provisions of Bill

The compromise bill would delay back payments due by non-commercial webcasters, including colleges and universities, for six months until June 20, 2003.

Meanwhile, small commercial webcasters would have until December 15, 2002 to negotiate an agreement with the recording industry. The agreements would cover the period from October 28, 1998 through to December 31, 2004. Although the bill did not set a specific rate, royalty payments would have to be based on a percentage of revenue or expenses, or both, and include a minimum fee.

Small commercial webcasters were not defined in the new version of the bill. Instead, senators were comfortable in letting marketplace negotiations define who was small, Potter said that for those who qualified as small webcasters under the terms of the original bill, however, negotiation would be brief.

There could be tiered rates for other webcasters who had not yet reached agreement with the recording industry, Potter suggested. Large webcasters, such as Yahoo! or AOL, moreover, which were not specifically covered under the bill, would be likely to engage in marketplace negotiations, he added.

The bill also contained a provision explaining that no agreement entered into could be admissible as evidence or otherwise taken into account in any administrative, judicial, or other government proceeding as a precedent for royalty payments. The provisions of the bill could also not be taken into account by the U.S. Court of Appeals for the District of Columbia Circuit, which is reviewing a rate structure set by the librarian of Congress in July 2002.

SoundExchange Ready

John Simson, executive director of SoundExchange, said in a statement:

> "This legislation is a positive step forward for webcasters, artists, and record labels because it brings some long-awaited certainty to the marketplace. We are pleased that Congress found a way to implement the rates and terms for small webcasters that the House proposed last month.
>
> "We will work expeditiously toward putting those rates and terms into effect as Congress has requested.
>
> "On another important issue, we are pleased that revisions to the bill offered the opportunity for record companies and artists to extend a six-month stay of payments for non-commercial webcasters. This provides all parties time to address the unique circumstances of non-commercial webcasters and reach an appropriate arrangement.

"Looking to the future, we hope that the costly and uncertain roads of litigation and legislation will not be necessary. We urge webcasters, broadcasters, and others to meet us in good faith to find marketplace solutions, rather than fighting in court and other forums. It's now time for us all to work together to realise a vigorous digital media marketplace that recognises the value and contributions of artists and record companies."

UNITED STATES

House Passes Bill Against Accepting Payment for Illegal Internet Gambling Debts

A bill that would make it illegal to accept credit cards and other financial instruments for debts incurred through illegal Internet gambling (H.R. 556) was passed by the House of Representatives on October 1, 2002.

The bill was originally introduced by Reps. James A. Leach (R-Iowa), vice chairman of the Financial Services Committee, and John J. LaFalce (D-N.Y.), the committee's ranking member, and reported out of the committee in October 2001 by a vote of 34–18. The bill gained new momentum after the bill's sponsors reached an agreement with Rep. Robert W. Goodlatte (R-Va.), who had introduced competing legislation.

Moreover, because most Internet gambling is conducted by offshore operators, who are beyond the reach of U.S. law enforcement, the bill would enable state and federal attorneys general to request that injunctions be issued to any party, such as a financial institution or Internet service provider, to prevent this type of crime. Finally, the bill would allow federal banking regulators to create rules requiring financial institutions to use designated methods to block or filter Internet gambling transactions.

The bill would require the secretary of the Treasury, in consultation with the Federal Reserve and the Department of Justice, to promulgate regulations.

The measure enjoyed widespread support from law enforcement groups, Internet service providers, sports groups, and the financial services industry.

> "Internet gambling sites provide anonymous, isolated access for problem gamblers", said Financial Services Committee Chairman Michael G. Oxley (R-Ohio).

Lawmakers also argued that Internet gaming sites are unregulated, and also serve as a way for criminals to launder money and evade taxes.

> "Not only can the huge debts amassed through gambling on the Internet destroy lives and families, the U.S. Department of Justice and the FBI have testified before Congress that these offshore sites serve as major potential conduits for organized crime, money laundering, and terrorism", Leach said in a statement.

Controversial Provision

During debate of the bill, Rep. John Conyers Jr. (D-Mich.), ranking member of the Judiciary Committee, said one exemption in the bill essentially defeated its purpose, which was to stop Internet gambling. As he read it, the bill would exempt any lawful transaction with a business licensed or authorized by a state, including lotteries.

Leach said nothing in the bill was designed to overturn the Wire Act or any other law, and the provision in question only applied to intrastate transactions, not interstate.

> "This bill is an enforcement mechanism that stops the ability of interstate Internet gambling", he said.

Rep. Sue W. Kelly (R-N.Y.) clarified in a colloquy that the provision to exempt lawful transactions carried out with a business licensed or authorised by a state not be interpreted to expand the reach of gambling.

> "Some parties have raised concerns that this would be read broadly to allow the transmission of casino or lottery games in interstate commerce, for example over the Internet, simply because one state authorises its businesses to do so", she said.

Instead, the exemption was intended to recognise current law, which allows states jurisdiction over wholly intrastate activity, Kelly said. The bill would leave intact current interstate gambling prohibitions such as the Wire Act, federal prohibitions on lotteries, and the Gambling Ship Act, she said.

Companion legislation has not been introduced in the Senate. However, Sen. Jon L. Kyl (R-Ariz.) has introduced legislation in the past to expand the scope of the Wire Act, which prohibits gambling over telephone lines, to include the Internet.

CASE REPORTS

CANADA

FIRST DECISION UNDER THE CIRA DISPUTE RESOLUTION POLICY RELEASED

The Canadian Internet Registration Authority (CIRA) has released the first decision in respect of a ".ca" domain name dispute under the CIRA Domain Name Dispute Resolution Policy (CDRP). The decision, rendered on October 7, 2002, resulted from a proceeding administered by the British Columbia International Commercial Arbitration Centre, one of two dispute resolution service providers authorised by CIRA, and was rendered by a single-member panel.

This dispute involved the «redrobin.ca» domain name, registered by Greg Tieu. The complainant was Red Robin International, Inc., the owner of the registered Canadian trademark RED ROBIN. As the registrant provided no response to the complaint and did not otherwise participate in the proceeding, the decision of the panel was decided on the basis of the complaint alone. The panel concluded in this case that the domain name should be transferred to the complainant.

In order to succeed under the CDRP, a complainant must prove that the registrant's domain name is "confusingly similar" to the complainant's trademark or trade name ("Mark") and that the registrant has registered the domain name in "bad faith", and must provide some evidence that the registrant has no "legitimate interest" in the domain name. The CDRP defines a "confusingly similar" domain name as one that

> "so nearly resembles the Mark in appearance, sound or the ideas suggested by the Mark as to be likely to be mistaken for the Mark".

In its decision, the panel found that the domain name «redrobin.ca» was identical to the complainant's trademark, and was therefore confusingly similar.

The only evidence available to the panel that touched upon the issue of whether the registrant had a "legitimate interest" in the domain was a series of letters exchanged between the complainant and the registrant. The panel remarked that

> "the only reasonable inference from the statements of the Registrant in this correspondence is that, having been given the opportunity to explain the existence of a legitimate interest in the Domain Name, he has not done so."

The panel concluded on that basis that that there was no evidence in the record of any of the number of factors set out in the CDRP that would constitute a legitimate interest of the registrant.

On the final issue, the panel found on a number of grounds that the complainant established that the registration was obtained in "bad faith". The letters by the registrant to the complainant suggested that the registrant had not used the domain name, and that the registrant was offering to sell it to the complainant and implied that he would sell it to someone else if the complainant did not buy it. The evidence also demonstrated that the same registrant had previously registered the domain name «virginatlanticairlines.ca» and other domain names associated with well-known businesses. Finally, the registrant's rejection of offers to release him from liability and to reimburse him for the cost of registering the domain name in exchange for an immediate transfer of the domain name supported the position that the registrant's primary purpose was to sell the domain name for consideration in excess of his actual costs of registration.

On these grounds, the panel found the registration of «redrobin.ca» to have been obtained in bad faith, and concluded that the domain name should be transferred to the complainant.

CIRA took over control of registration of ".ca" domain names from the University of British Columbia in November 2000. The CDRP came into effect in June 2002, and is available at *www.cira.ca/en/cat_dpr_policy.html*. The decision discussed above is available online at *www.cira.ca/en/dpr-decisions/00001-redrobin.pdf*.

Ian R. Hay, Blake, Cassels & Graydon LLP, Toronto; e-mail: ian.hay@blakes.com

FRANCE

THE USE OF REGISTERED CORPORATE NAMES IN METATAGS

S.F.O.B. v. Notter GmbH

Paris Court of Appeal, March 13, 2002

A website including metatags using a registered corporate name may constitute an infringement of registered corporate names. In a summary judgment of the Paris Court of Appeal, the use of a distinctive sign other than an industrial property right was considered illicit. The defendant, Notter GmbH, had included in its metatags the registered corporate name of a direct competitor, the French company S.F.O.B, and was ordered to suppress the litigious metatags. Users of an Internet search engine could, by typing "sfob", automatically access the website of Notter GmbH. Since the scope of the companies' businesses was comparable and the French company was operating on the German market the Court considered that S.F.O.B and Notter GmbH were competitors. Consequently, the Court confirmed the lower Court's ruling on that point. However the Court of Appeal overruled the lower Court's rejection

of the claim for damages. The Court of Appeal held that the fact of using the registered corporate name of its competitor for personal purposes constituted sufficient grounds for allocating a provision for damages.

However, the Court of Appeal, rendering a summary judgment, did not rule on the allegation that the metatags constituted an act of unfair competition and parasitism. The French company, suffering a fall in turnover of 69.94 percent, argued that this fall resulted from the litigious metatags and alleged that the litigious metatags were the proximate cause of an actual injury.

Liability for unfair competition and parasitism is based upon general principles of tort law as enunciated by case law. In order to establish a cause of action and bring a suit, a party injured by an act of unfair competition must prove:

- that an act of unfair competition has been committed, such as confusion with the products and services of the injured party or discrediting of the competitor;
- that such act was the proximate cause of an actual injury; and
- the amount of injury suffered.

On grounds of parasitism (similar to the common law remedy of "passing off"), persons or companies can be held liable where they have sought to benefit from the goodwill attached to another's product, in order to make a profit out of such goodwill.

The website owner must prove its goodwill and that a misrepresentation and a prejudice for her/him has resulted from such misrepresentation. The likelihood of confusion does not need to be demonstrated.

Concerning these two remedies it seems likely that the Courts will either find that a likelihood of confusion exists or that the German company sought to profit from the goodwill of the French company or even both. Here again the remaining issue will essentially be the evidence, which has to be supplied by the French company, proving that the litigious metatags were the proximate cause of its actual injury.

Other remedies are or may be available in respect of the unauthorised use of another party's registered or unregistered trademark, logo or other material in metatags or the hidden text of a website.

In the Distrimart case (March 13, 2002), the Paris Court of Appeal held that a metatag using the plaintiff's trademark constitutes an infringement of trademark on the grounds that this use created a likelihood of confusion. In addition, the reproduction of trademarks owned by Chanel in metatags located in the site of another company marketing luxury products was considered as an infringement by the Paris Court of Appeal (March 3, 2000).

A person infringes a registered trademark if she/he uses or reproduces a trademark for products or services identical to those listed in the registration. Trademark infringement also exists if there is a likelihood of confusion in the mind of the public, through:

- use of identical trademarks for products or services similar to those listed in the registration; or
- use of an imitated trademark for products or services identical or similar to those listed in the registration (Articles L-713-2 and L-713-3 of the French Intellectual property code).

According to French case law an infringement of trademark by using a third party's trademark would not be constituted if the three following requirements are fulfilled:

- the use of the trademark must be a necessary reference. Indispensable referencing is, for example, when a manufacturer of accessory products uses the trademark of the principal product for promotion purposes;
- the use must not create any likelihood of confusion on the part of consumers, regarding the origin of the products or services provided on the website; and
- the use of the trademark must not be the cause of any injury to the owner of the trademark.

The unauthorised use of a third party's trademark may also give rise to an action for unfair competition and or parasitism (see above).

Sabine Lipovetsky and Fabrice Perbost, Attornies at law, Kahn & Associés; e-mail: slipovetsky@kahnlaw.com and fperbost@kahnlaw.com

UNITED STATES

ISP ORDERED TO REVEAL SUBSCRIBER IDENTITY

America Online, Inc. v. Nam Tai Electronics, Inc. 2002 WL 31454120 (Va.)

The Supreme Court of Virginia has affirmed a decision granting comity to another state court's out-of-state discovery order regarding content on an Internet chat room. The case involved an action brought in the Superior Court of the State of California for the County of Los Angeles, in which Nam Tai Electronics alleged that a certain unknown individual had posted "false, defamatory, and otherwise unlawful messages" in an online chat room discussing the company's publicly traded stock.

In their search for the unknown individual, Nam Tai obtained a commission from the California court for out-of-state discovery to depose AOL's custodian of records. AOL filed a motion to quash the subpoena *duces tecum*, arguing that First Amendment protection applied to all claims made in the California complaint. Nam Tai contended that principles of comity, in which courts of one state or jurisdiction will give effect to laws and judicial decisions of another state or jurisdiction, required the Virginia court to give deference to the procedures used by the California court when it issued the commission.

The Court identified four principles that must be considered before granting comity to an order of a foreign court:

> "First, the foreign court must have personal and subject matter jurisdiction to enforce its order within its own judicatory domain. Second, the

procedural and substantive law applied by the foreign court must be reasonably comparable to that of Virginia. Third, the foreign court's order must not have been falsely or fraudulently obtained. And, fourth, enforcement of the foreign court's order must not be contrary to the public policy of Virginia, or prejudice the rights of Virginia or her citizens."

AOL argued that the California court lacked personal jurisdiction over any party other than Nam Tai. The court noted, however, that it is not uncommon for a plaintiff to use a "John Doe" pleading style to initiate a lawsuit with an unknown defendant. For purposes of comity, therefore, they need not be concerned with whether the California court will ultimately be able to assert personal jurisdiction on a particular person.

AOL also challenged the California court's application of California substantive law in ruling that First Amendment concerns did not apply. The Virginia court, however, refused to act as "surrogates for the appellate courts of that jurisdiction," stating that foreign courts are in a better position to determine the substantive law of their own jurisdiction, and a high degree of deference will be given to their judgment.

Finally, the court found that California's statutory cause of action in this case was reasonably comparable to Virginia law and not repugnant to public policy. The subpoena *duces tecum* was therefore upheld, requiring AOL to produce records sufficient to identify the unknown subscriber.

David Brownlie, Potter Group Legal Services, Chicago; e-mail: dbrownlie@pottergroup.com

UNITED STATES

■ WEBSITE HELD NOT "PUBLIC ACCOMMODATION" UNDER 1990 AMERICANS WITH DISABILITIES ACT

Access Now Inc. v. Southwest Airlines

U.S. District Court for the Southern District of Florida, October 18, 2002

A website designed in a manner that frustrated technological tools used by blind Internet users is not a place of public accommodation that must comply with the accessibility requirements of the 1990 Americans with Disabilities Act, the U.S. District Court for the Southern District of Florida has found.

In a case of first impression, Judge Patricia A. Seitz observed that an Internet website is qualitatively different to the physical places Congress specifically defined as "places of public accommodation" in the act.

> "Because the Internet website, southwest.com, does not exist in any particular geographical location, plaintiffs are unable to demonstrate that Southwest's website impedes their access to a specific physical, concrete space such as a particular airline ticket counter or travel agency", she wrote.

Access Now Inc., a non-profit advocacy group, sued Southwest Airlines Co., alleging that the company's website – which offered special deals and a convenient reservation system – violated the ADA because it did not allow for the proper operation of screen reader technology, thereby preventing blind Internet users from using the website's functions.

The ADA, 42 U.S.C. §§12101 *et seq.*, requires that operators of public accommodations remove barriers that prevent individuals with disabilities from taking advantage of the goods or services in question.

Examining the definitional section of the ADA, 42 U.S.C. §12181(7), and federal regulations interpreting the meaning of "place of public accommodation", the court said the plain language of these provisions required a place of public accommodation to be a physical concrete structure.

Definition of 'Places of Public Accommodation'

Section 12181(7) sets out 12 categories of places of public accommodation – including inns, restaurants, cincemas, schools, dry cleaners, parks, zoos, daycare centres, and health spas. These are all physical locations, the court observed.

Further, regulations promulgated by the attorney general define a "place of public accommodation" in terms of physical places

> "all or any portion of buildings, structures, sites, complexes, equipment, rolling stock or other conveyances, roads, walks, passageways, parking lots, or other real or personal property, including the site where the building, property, structure, or equipment is located". 28 C.F.R. § 36.104.
>
> "[T]o fall within the scope of the ADA as presently drafted, a public accommodation must be a physical, concrete structure", the court said. "To expand the ADA to cover 'virtual' spaces would be to create new rights without well-defined standards."

The court rejected the plaintiff's claim that a website is a place of "exhibition, display and a sales establishment", which arguably falls within the 12 categories described in the statute. The court used a device of statutory interpretation, *ejusdem generis*, which requires that

> "where general words follow a specific enumeration of persons or things, the general words should be limited to persons or things similar to those specifically enumerated".

The rule *ejusdem generis* cannot be used to create a place of public accommodation by pulling individual words out of their context, the court said.

No Nexus Between Website, Physical Place

The court also declined to follow a decision from the First Circuit, stating that the Eleventh Circuit had interpreted the ADA more narrowly and declined to expand

the definition of place of public accommodation into cyberspace.

In *Carparts Distribution Center Inc. v. Automotive Wholesalers Association of New England*, 37 F.3d 12 (1st Cir. 1994), the First Circuit held that the ADA definition of "public accommodation" is not limited to physical space, but includes health benefit plans.

However, the Eleventh Circuit – which encompasses Florida – adopted a narrower test in *Rendon v. Valleycrest Productions*, 294 F.3d 1279 (11th Cir. 2002). In *Rendon*, the court held that an automatic fast finger selection device used in a television game show was a "place of public accommodation" under the ADA because there was a nexus between the concrete premises of public accommodation – a television studio – and the challenged technological device.

Because an Internet website is not a means of accessing a concrete physical space such as a particular airline ticket counter or travel agency, it would not be a place of public accommodation under the *Rendon* rule, the court said.

Other Actions in the Pipeline

Phyllis F. Resnick, Vice President of Access Now, told WILR that Access Now intends to appeal the court's decision and that they expect to file more lawsuits with similar allegations against various Internet websites in the future.

Access Now had also filed complaints with similar allegations against Barnes & Noble and American Airlines. Barnes and Noble has settled with Access Now. American Airlines has filed a motion to dismiss that is presently awaiting hearing or decision (*Access Now Inc. v. American Airlines Inc.,* S.D. Fla., No. 02-CV-22076, *complaint filed* 16/07/02).

The plaintiffs were represented by Howard Ronald Behar and Steven Robert Reininger of Rasco, Reininger, Perez & Esquenazi, Coral Gables, Fla. The defendant was represented by Anne Marie Estevez, and Beth Hilary Storper Joseph of Morgan, Lewis & Bockius, Miami.

UNITED STATES

■ BUS SERVICE'S FAILURE TO CODE WEBSITE FOR DISABLED USERS HELD AS LIKELY VIOLATION OF ADA

Martin v. Metropolitan Atlanta Rapid Transit Authority

(N.D. Ga., No. 1:01-cv-3255-TWT, October 7, 2002)

Plaintiffs in a class action lawsuit are likely to succeed in demonstrating that a website containing route and schedule information for a municipal mass transit system is in violation of the 1990 Americans with Disabilities Act, according to a ruling of the U.S. District Court for the Northern District of Georgia. The defendants, the Metropolitan Atlanta Rapid Transit Authority (MARTA), represented to the court that it was working to make its website more accessible to disabled users –particularly blind users who cannot now use technological tools to read aloud text on the website.

District Judge Thomas W. Thrash Jr., without much discussion of the issue, said that the website's shortcomings in this regard most likely violated the ADA, and it directed the parties to come up with a remedial order that addresses those shortcomings.

Website Not Equally Accessible

Vincent Martin, who is blind, filed a class action lawsuit on behalf of himself and other disabled individuals, against MARTA, alleging MARTA's operation of its mass transit operation violated various provisions of the ADA. Among various of the other claims, Martin alleged that the MARTA website was designed in a manner that blind Internet users were unable to access the information at the site. The complaint alleged that MARTA violated the mandate of the ADA by failing to make

> "adequate communications capacity available, through accessible formats and technology, to enable users to obtain information and schedule service"; the court said, citing 49 C.F.R. §37.167(f).

The ADA, 42 U.S.C. §§12101, *et seq.*, requires that operators of public accommodations remove barriers that prevent individuals with disabilities from taking advantage of the goods or services in question.

Plaintiffs alleged MARTA failed to provide scheduling and routing information in an accessible format as required under 49 C.F.R. §37.160 – either through the phone, the mail or the Internet. Plaintiffs sought declaratory and injunctive relief against MARTA.

Blind Users Lacked Schedule Data

Agreeing, the court said schedule and route information was not equally accessible to disabled persons and those who are not disabled.

> "MARTA representatives also concede that the system's web page is not formatted in such a way as to be read by persons who are blind but who are capable of using text reader software for the visually impaired", said the court.

MARTA fell short in the implementation of its own rules and until the deficiencies are corrected, MARTA is in violation of the ADA, the court said.

Plaintiffs met their burden of showing that they were likely to succeed in proving that defendants failed to make available to individuals with disabilities adequate information concerning transportation services through accessible formats and technology.

Vincent Martin was represented by Georgia K. Lord of Decatur, Ga., and MARTA was represented by John R. Lowery of Pursley, Lowery & Meeks, Atlanta, Ga.

COMMENTARY

UNITED KINGDOM

Adequacy of Cyber-Criminal Investigations: Is 'Big Brother' in Cyberspace?

Cagdas Evrim Ergun, Cakmak Law Office, Ankara; e-mail: c.ergun@cakmak.gen.tr

Introduction

Cybercriminal investigations require international regulations, as the Internet allows cybercrimes to be committed regardless of conventional state-borders. Although there are no reliable statistics available on the full scale of the computer-related crime phenomenon, the number of illegal activities can be expected to grow as computer and network use increases.

Any definition of cybercrime would have to be as complex and fast changing as the technology through which the crimes are carried out. Different views exist on what constitutes cybercrime. However, it can be generally defined as actions directed against the confidentiality, integrity and availability of computer systems, networks and computer data, as well as the misuse of such systems, networks and data. The terms "cybercrime", "computer crime", "computer-related crime" and "high-tech crime" are often used interchangeably, and some authors prefer to use the term "misuse" instead of "crime", since in many cases abuses or misuses related to computers may not fit within the definition offered by traditional crime laws and legislation.

As previously mentioned, this study deals primarily, but not exclusively, with the balance between increasing investigative powers of the governments and the respect for personal privacy of Internet users. In so doing, a particular consideration will be given to the Convention on Cybercrime of the Council of Europe (the Convention), since the essential discussions in political, social and commercial milieus concentrate on the matter of its compliance with human rights.

The topic is of interest mainly for two reasons. Firstly, the criminal use of the network is of significant importance, since its extent and risks are increasing considerably in parallel with the role of the Internet in our lives. Secondly, contemporary developments call into question the compliance of governments' cybercrime policies with human rights, among them, in particular, the respect of personal privacy. Privacy matters are particularly prominent when dealing with an electronic environment where the information can be transferred across national borders, or intercepted, and verification of who you are dealing with can be difficult.

Law Governing Cybercrime

Effective action against cybercrime is necessary at both national and international level. On a national level, comprehensive and internationally oriented answers to the new challenges of network security and computer crime are often still missing, and in most countries, reactions to computer crime focus on national law (especially criminal law), neglecting alternative preventive measures. Some countries have introduced criminal laws addressing illegal collection, storage, modification, disclosure or dissemination of personal data. Despite the efforts of international and supranational organisations, the various national laws worldwide show remarkable differences, especially with respect to the liability of intermediary service providers and content providers, and the coercive powers of investigative agencies (especially in relation to encrypted data and investigations in international networks).

On the international and supranational levels, the need to effectively combat computer-related crime has been broadly recognised and various organisations have been co-ordinating or attempting to harmonise relevant activities. The House of Lords Select Committee on Science and Technology, in its paper *Information Society*,[1] stated that:

> "[where] government intervention is needed, it is also clear that as much as possible should be agreed internationally". And, "there are issues here which must be resolved internationally, to ensure that the defence and law enforcement agencies of national governments are not emasculated by the growth of the Information Society".

For this purpose, considerable effort has been made by the G8 Justice and Home Affairs Ministries which adopted a set of principles and a 10-point action plan in December 1997, which was endorsed by the G8 Birmingham summit in May 1998 and is now implemented.

A more significant effort to combat cybercrime at international level has been conducted from within by the Council of Europe (CoE), which approved the Convention on Cybercrime in September 2001. The Convention is the first international treaty on crimes committed via the Internet and other computer networks, dealing particularly with the interception of communications, preservation and disclosure of traffic data, production orders, search and seizure of stored computer data, real-time collection of traffic data and interception of content data. It also contains a series of powers and procedures such as the search of computer networks and interception. Its main objective, set out in the preamble, is to pursue a common criminal policy aimed at the protection of society against cybercrime, especially by adopting appropriate legislation and fostering international co-operation. However, there are considerable criticisms from commercial interests and human rights

groups on both sides of the Atlantic are arguing that the Convention does not adequately protect privacy and individual rights and favours international policing agencies.

Threats to Personal Privacy of Cyber Users

"Freedom of speech and privacy are frequently conceived as rights or interests of the individual, and as rights or interests of the community as a whole." Electronic invasion of privacy should be considered in the same manner as physical invasion of privacy, since both raise the same legal issues. However, the existence of information technology transforms the nature of private and public space, making it possible for personal privacy to be invaded without physical entry into someone's home.

More than in any other transnational crime, the speed, mobility and flexibility of computer crime challenge the existing rules of criminal procedural law.

Approximation of procedural law powers will improve the protection of victims by ensuring that law enforcement agencies have the powers they need to investigate offences on their own territory, and will ensure that they are able to respond quickly and effectively to requests from other countries for co-operation. However, any new powers for law enforcement need to comply with the respect for personal privacy.

The Court of Justice has consistently held that such legislative provisions may not discriminate against persons to whom Community law gives the right to equal treatment or restrict the fundamental freedoms guaranteed by Community law.[2]

However, many parts of the Convention are not consistent with human rights, in particular the respect of personal privacy, since it undermines network security, reduces government accountability and improperly lengthens the reach of law enforcement. In the words of Judge Pettiti, of the European Court of Human Rights,

"the mission of the Council of Europe and of its organs is to prevent the establishment of systems and methods that would allow 'Big Brother' to become master of the citizen's private life".

The essential criticism of the Convention as regards personal privacy refers to the imbalance between the powers of law enforcement agencies and the rights of Internet users. In other words, the Convention gives significant powers to law enforcement agencies and does not provide checks and balances for Internet users. In the subsequent part of this article, consideration will be given to the factors that constitute the basis of that lack of balance.

Increasing Powers of Law Enforcement Authorities

Retention of Traffic Data

To investigate and prosecute crimes involving the use of the Internet, law enforcement authorities frequently use traffic data stored by service providers for billing purposes. Under the E.U. Personal Data Protection Directives, both the general purpose-limitation principles of Directive 95/46/EC and the more specific provisions of Directive 97/66/EC, traffic data must be erased or made anonymous immediately after the telecommunications service is provided, unless they are necessary for billing purposes. However, as stated in the EU Forum on Cybercrime in November 2001, law enforcement authorities consider the retention of a minimum amount of traffic data for a minimum period of time necessary to facilitate criminal investigations. Accordingly, the E.U. Data Protection Directives allow Member States to adopt legislative measures to restrict the scope of the obligation to erase traffic data when this constitutes a necessary measure for, amongst others, the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the telecommunications system.

The retention of traffic data beyond the requirements of billing purposes in order to facilitate criminal investigations is an improper invasion of the right to privacy guaranteed under Article 8 of the ECHR. Moreover, those data may not only be used for investigative purposes. It is also possible that they are used for other purposes such as the construction of a commercial profile. Where traffic data are to be preserved in specific cases there must be a demonstrable need, the period of retention must be as short as possible and the practice must be clearly regulated by law.

Any legislative measure that may provide for the retention of traffic data for law enforcement purposes needs to fulfill certain conditions. The proposed measures should be appropriate, necessary and proportionate, as required by Community law and international law (including Directive 97/66/EC and 95/46/EC, the European Convention for the Protection of Human Rights of November 4, 1950 and the Council of Europe Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data of January 28, 1981). However, some Member States are taking legal initiatives requiring or allowing service providers to store certain categories of traffic data, not needed for billing purposes, after the provision of the service but which are considered useful for criminal investigations. The scope and form of these initiatives varies considerably, but they are all based on the idea that more data should be available for law enforcement authorities than would be the case if service providers only process data which are strictly needed for the provision of the service.

Government Access to Encryption Keys

The Convention includes a certain number of provisions which allow law enforcement officials to access to many types of personal security information. Article 19.4 requires the signatory states to adopt such measures as to empower its competent authorities to order any person who has knowledge about the functioning of the computer system, to provide all necessary information to enable search and seizure. This is directly related to human rights concerns and issues for example under the ECHR (Article 6) such as a suspect's right to fair trial, right not to self-incriminate himself/herself, and right to silence.

In the United Kingdom, the Regulation of Investigatory Powers Act 2000 provides for such government access to encryption keys, and that should be considered as a significant risk to the privacy and human rights of Internet users. This is because, first, the U.K. Government has not shown these powers to be either necessary or effective in countering criminal misuse of the Internet, and most experts agree that they will not be ef-

fective against serious criminals. Moreover, other countries such as Germany have considered and rejected such measures as unnecessary, ineffective, and detrimental to the safety, security and privacy of honest citizens and businesses who make use of the Internet.

Secondly, these measures are indiscriminate and make no distinction between the keys and information owned by criminals and those owned by honest citizens. They are technically ineffective and easy to circumvent from a criminal perspective and yet create potential risks for honest citizens and businesses that are more than sufficient to undermine confidence in Internet use in the United Kingdom.

Secret Surveillance Systems and Interception of Communication

Secret surveillance and interception of telecommunications over the Internet or otherwise, is only acceptable within the limits and under the conditions laid down by Article 8 of the European Convention on Human Rights. The same applies – by analogy – to the development of infrastructures that are designed to facilitate interception activities where these are lawful in specific cases.

In the European Union, in accordance with the general principle of confidentiality of communications, interceptions are illegal unless they are authorised by law when necessary in specific cases for limited purposes. This follows from Article 8 of the European Convention of Human Rights, referred to in Article 6 of the TEU and more particularly from Directives 95/46/EC and 97/66/EC. All Member States have a legal framework in place to allow law enforcement to obtain judicial orders for the interception of communications on the public telecommunications network. This legislation, which has to be in line with Community law to the extent that it applies, contains safeguards protecting individuals' fundamental right to privacy. This includes measures such as limiting the use of interception to investigations of serious crimes, requiring that interception in individual investigations should be necessary and proportionate, or ensuring that the individual is informed about the interception as soon as it will no longer hamper the investigation.

The convention promotes the use of interception for only "serious offences to be determined by domestic law". Even this limitation serves little effect, for the definition of serious crime is left to domestic law, and some countries in the CoE have an extremely broad definition of serious crime for content interception purposes.

Privacy is not an absolute right, and does not oppose lawful interception of communications based on clear legal powers and subject to effective judicial control and adequate remedies for abuse. However, interception and processing of data with systems like Echelon, which automatically intercepts phone calls, e-mails and faxes, is not consistent with fundamental human rights guaranteed by all major international agreements and relevant national legislation.

Justification of Governments for Increasing Investigative Powers

So far, we have examined arguments supporting the idea that cybercrime is used by states as a device to restrict personal privacy of electronic communications. We will now consider the subject from the other, more controversial side, which considers increasing investigative powers of law enforcement agencies as proportionate to the offence caused by cybercrime.

First, it must be remembered that crime is an invasion of privacy as well. If governments do not increase investigative powers of law enforcement agencies, the personal privacy of citizens will be threatened, not by the criminal investigations, but by the crime itself. A cybercrime invades both the victim's privacy and the sense of security of a whole society. Although a citizen has a right to privacy, this right has to be balanced on occasion against the need for police officers to invade that privacy at a minor level, in order to prevent a major, criminal invasion of privacy.

Secondly, the Internet's global nature makes it almost impossible to combat cybercrime without effective investigative powers.

> "Cybercrime knows no boundaries. It is very difficult to prosecute, because data is so volatile that it can be deleted within seconds. If there are no quick measures to trace back communications and crime online, there will be no possibility of prosecuting them"

said Peter Csonka, deputy director of the CoE's economic crime division, which is co-ordinating the drafting process.

As a counter argument against the criticism of the Convention, it could be said that there are many procedural guarantees in the Convention, which enable any abuse to be forestalled. First, the introduction, use and application of the powers and procedures will be subject to the conditions and safeguards for which the domestic law of each Contracting Party provides. This is to ensure that human rights are honoured, as they are defined in the applicable international instruments, such as the European Convention on Human Rights. Secondly, every procedural method will be placed in the framework of existing guarantees, including the prior authorisation of a judge, according to the country's legal system. And lastly, Article 15.1 of the Convention requires the test of proportionality to be applied, taking account both of the nature and of the circumstances of the offence which is the object of the investigation.

Another argument used by governments is related to the changing features of the telecommunication. As stated in the Opinion 4/2001 on the Council of Europe's Draft Convention on Cybercrime, there will no longer be any need to store traffic data for billing purposes, since the price charged for a communication is becoming less and less dependent on distance and destination, and service providers move towards flat rate billing.

Law enforcement authorities fear that this will reduce potential material for criminal investigations and therefore advocate that service providers keep certain traffic data for at least a minimum period of time so that these data may be used for law enforcement purposes.

Conclusion

It is true that adequate investigative powers are necessary to allow the police to fulfil their tasks effectively.

However, these powers should be adequate, proportionate to the offence and consistent with fundamental human rights, such as privacy and freedom of expression as outlined in the European Convention on Human Rights, the Universal Declaration of Human Rights, and the International Covenant on Civil and Political Rights. These important international instruments should be taken into account by governments and regional and international organisations by adopting regulations on cybercrime. Any co-ordinated policy initiative at national, supranational or international level should therefore provide for the protection of personal data and privacy.

As Akdeniz, founder and director of Cyber-Rights & Cyber-Liberties (U.K.), pointed out, governments and supranational and international organisations should co-operate to respect fundamental human rights such as freedom of expression and privacy and should encourage rather than limit peoples' usage of the Internet through excessive regulation. They should carefully weigh the benefits of such steps in criminal investigations against the potential for compromising privacy, and find appropriate, balanced and proportionate solutions fully respecting the fundamental rights to privacy and data protection. This includes measures such as requiring judicial review, assuring against self-incrimination, ensuring data is gathered for specific reasons, using proportionate means on all occasions, and upholding data protection principles.

1 House of Lords, Select Committee on Science and Technology, Information Society: Agenda for action in the U.K. (1995-1996 H.L. 77).

2 Case C-274/96 Bickel & Franz (1998) ECR I-7637 para 17, Case C-186/87 Cowan (1989) ECR 195 para 19.

3 Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Official Journal L 281, 23/11/1995 p. 0031–0050.

4 Directive 97/66/EC concerning the processing of personal data and the protection of privacy in the telecommunications sector. Official Journal L 024, 30/01/1998 p. 0001–0008.

■ ITALY

Alternative Dispute Resolution: Online Arbitration and Mediation in Italy and the European Union in Comparison with the United States

Alessandro del Ninno, Studio Legale Tonucci, Rome; e-mail: adelninno@tonucci.it; www.tonucci.it

Introduction

Alternative Dispute Resolution and Online Dispute Resolution procedure, is a subject of great interest, because it arises at a very sensitive phase of the commercial relations between companies or between companies and consumers: that which jurists call the "pathological" phase of contractual relations, a pre-litigation phase that involves the need to regulate the claims of each party.

The arrival of new Communications and Information Technology has brought us into the Global Information Society in which we all now live. It has brought with it the need to revisit traditional legal instruments and institutions and the need to constantly adapt "traditional" rules and laws in line with technological progress and to the development of the Internet. This phenomenon has given rise to new situations and commercial relations on the one hand, but it has also made apparent on the other, the insufficiency – if not the total absence – of specific legal rules and fixed standards to regulate these new scenarios.

This is why the various national, supranational and international lawmakers have found it necessary to create a new, *ad hoc* legal framework with regard to the impact of ICT technologies on the contractual relationship. But it is precisely in the pathological phase of computerised commercial relations that the use of technology could assist businesses and consumers. This can be done by providing them with flexible online tools that are efficient and less costly for alternative dispute resolution. Data transmission procedures and telematic tools can overcome the fact that transactions often occur between parties from different countries, with different legal systems and national laws.

1. Characteristics of ODR Procedures and the Use of ADR Procedures on the Internet

Before analysing the current experiences of ODR (Online Dispute Resolution) schemes, which are a subspecies of the general category of ADR or Alternative Dispute Resolution, it is useful to provide some explanation of how these procedures work.

The online resolution of disputes is the easiest and most innovative means of resolving disputes arising from Internet transactions. But it is a tool that is increasingly used to resolve off-line disputes as well, for issues that are not necessarily related to the web. In fact, there is no reason why a good online dispute resolution service could not also apply to cases other than those arising from e-commerce.

ODR is a simple and practical method: it breaks down the barriers of time and space, and allows for dialogue between parties who are so far apart so as to render unfeasible, traditional "face to face" conciliation or arbitration.

In its short history, ODR has already had a significant impact on both the B2C market, business to consumer, as well as the B2B market, business to business. ODR measures are set to become increasingly important in the near future, particularly in the latter area. Consider

the case of web marketplaces. These are environments where businesses need to be guarantied a more time efficient means of resolving potential conflicts.

The first models for the development of online dispute resolution can be summarised as follows:

- *Assisted negotiation*: The two parties exchange monetary offers and counter-offers, according to an automated system provided by a provider of ODR services. In this system, however, there is no provision for third party intervention that would assist the parties to resolve their disputes.
- *Online conciliation or mediation*. The parties communicate with each other by e-mail or on dedicated chat lines in the presence of a third party, a conciliator who helps them to find an online agreement. This is the closest model to the traditional method of "face to face" conciliation.
- *Online arbitration*. The parties refer to an arbiter who not only assists them in arriving at an agreement but also issues a decision on the case at hand. All of this occurs after an exchange, via the Internet, of documentation related to the case. In short, conciliation is achieved online through online dialogue between the parties. Specifically, online arbitration will also involve an exchange of documentation and arbitrage reports between the parties.

It might be of interest to provide a more in-depth analysis of how these ODR models work in practice. The ODR scheme of "assisted negotiation" is defined in commercial practice as the "blind", "automatic" or "blind offer" model.

The blind or automatic model is a negotiation model between the two disputing parties: in the negotiation there is no intervention by a neutral third party, as the two parties are simply put in contact by specialised software. The system is defined as "blind" because the parties never see each other, right up until the end of the procedure. The amount of the offer is sent online to the other party to resolve the dispute, but they only know that the other party has improved its own offer.

The "blind offer" system is instigated by a request form which is completed and sent online. The "defendant" is contacted by the service provider, and can accept, offline as well, a mediation attempt. If it is accepted, the procedure starts.

The software for the procedure provides that, in the alternative, both the plaintiff and the defendant can exchange monetary offers and counter-offers to resolve the dispute. This may continue for 60 days, and within this time period, there is no limitation on the number of offers that can be exchanged between the parties.

Once the plaintiff has sent a claim for damages, the defendant responds with a counter-offer, to which the plaintiff replies with a new request. Each new offer must be improved by at least five percent (higher or lower, depending on which party is making the offer).

All the offers made are "blind" that is, the amounts are not known to the other party: each party is notified automatically, from time to time, that the other party has made a new offer that is better than the last (by at least five percent).

A settlement is reached if the plaintiff's claim comes within 30 percent of the defendants claim. This provision (the 30 percent) would have been pre-emptively accepted by the parties before the offers began.

In this model everything is based on software with fairly simple calculations and that notifies the parties of a new offer, without specifying the amount. The entire procedure is nonetheless facilitated by explanatory e-mails from the Provider to the parties.

This is obviously a model for resolving disputes of a monetary nature. The model is particularly well-suited to insurance disputes, that is, between the insured party and the insurance company. However, commercial and industry disputes in general could benefit from a similar method. It is also clear, at the same time, that there are limitations with respect to disputes involving more complex issues from those of a purely monetary nature.

The strength of this blind negotiation model lies in the fact that it overcomes one of the major obstacles to an agreement between the two parties: each party's fear of showing all its cards and of appearing weak in the other party's eyes.

The "calculator" software (instead of the presence of a "physical" conciliator) enables parties to communicate information without communicating directly between themselves or to discuss without actually openly negotiating.

The ODR model of "online conciliation or mediation" is one of these alternative mechanisms on the web that is based on a model defined as "open". The basic concept behind this model is completely different: even though it is online rather than in person, communication and direct exchanges between the two parties are preferred and the work of the online conciliator remains that of helping the parties to discuss openly and to find – by means of dialogue – a solution that will satisfy both parties.

This concept is closest to the traditional notion of non-virtual conciliation whereby conciliators use a series of techniques to convince the parties to collaborate and co-operate with one another, to try to overcome the parties' reservations and weaknesses. Moreover, an expert conciliator is knowledgeable in and will apply various psychological techniques to interpret the non-verbal language of the parties, their attitude, their feelings and their instinctive reactions. Obviously, reproducing this model online is very difficult, at least with the current state of information technology. In fact, the systems of online conciliation inspired by this open model are still greatly limited by the scant "inter-activeness" of currently available software. These systems primarily use e-mail or chat-room conferencing, while trying wherever possible to recreate the atmosphere of a typical settlement hearing within a virtual environment. Just as in a real arbitration hearing, the provider of conciliation services makes a virtual resolution room available to both parties and provides for a conciliator who is qualified as an expert.

On the basis of the open model, the provider's website contains a form to be completed to initiate the proceedings. On this form, the parties must provide their personal information as well as the nature and the mon-

etary amount of the issues in dispute. Following receipt of the completed form (obviously by e-mail), the provider will proceed to contact the other party. If the other party accepts, a conciliator is appointed and a line for confidential communication is created (that can only be accessed by the parties and the conciliator with respective passwords) where the entire procedure will take place.

Once virtual contact has been established between the parties and the conciliator, the procedure tends to follow the traditional pattern of a non-virtual settlement proceeding. The mediator must present himself and request that the parties do the same; after which each party will be requested to describe their own version of the facts. The conciliator may request clarifications from the parties and then may proceed to the next phase of identifying the issues in dispute, reviewing the nature of proposals and of discussions and then defining the agreement.

The system is set up in a way that enables the parties to choose what type of communication they would like to use: only with the conciliator (using the available "reply to message" command for all e-mails); with the conciliator and with the other party (using the command "reply to all"). Similar to traditional mediation, this system also enables the conciliator to "meet" separately with each party, to discuss in private the more sensitive and confidential aspects of the dispute.

Like more traditional settlement proceedings, the virtual system must guarantee the utmost reserve to the proceedings, ensuring the confidentiality of conversations between individual parties and the conciliator, and ensuring that there is no access to third parties.

This system provides clear advantages: the use of e-mail, in fact, enables fast communication between parties who cannot or do not wish to meet physically, without incurring excessive costs. The system also enables service providers to appoint expert mediators and to make preparations without concern for the distance or the cost of relocating.

The system does have certain disadvantages. Virtual communications – at least in their current state – are hardly very "expressive", especially with regard to emotions and non-verbal communications.

The first users in this area agree that the model is inadequate and that it is still absolutely necessary to make new efforts to improve the level of virtual communications. To be sure, some improvements will come with the greater diffusion of video and audio communication systems (web cam) which make it possible to communicate between the parties and conciliators even from afar.

2. The European Legal Framework in the Area of ADR procedures

The European Community has only recently addressed this issue from a legal perspective, with Directive 2000/31 on Electronic Commerce. Article 17 introduced the following normative principle:

Out-of-Court Dispute Settlement

1. Member States shall ensure that, in the event of disagreement between an information society service provider and the recipient of the service, their legislation does not hamper the use of out-of-court schemes, available under national laws for dispute settlement, including appropriate electronic means.

2. Member States shall encourage bodies responsible for the out-of-court settlement of, in particular, consumer disputes to operate in a way which provides adequate procedural guarantees for the parties concerned.

3. Member States shall encourage bodies responsible for out-of-court dispute settlement to inform the Commission of the significant decisions they take regarding information society services and to transmit any other information on the practices, usages or customs relating to electronic commerce.

Nonetheless, this Article, which includes both electronic commercial relations B2B as well as B2C, applies only to the alternative dispute resolution of e-commerce transactions between businesses and between businesses and consumers for the purpose of electronically provided services. It does not apply to transactions for the supply of goods to purchasers on the basis of prior contracts that were concluded online.

Moreover, there is another limitation arising from the fact that these provisions, upon a careful reading, apply to Member States unrestricted by already existing national legislation in the area of out-of-court settlement for e-commerce service transactions, taking into consideration "adequate electronic means" as well as the peculiarities of computerised commercial relations. This means that the E.U. Directive, far from introducing a new normative principle (for example, requiring Member States to create proper telematic procedures in their national legal systems, aimed at providing ODR services), merely requires that Member States work towards applying existing national ADR schemes and laws to the new e-commerce disputes, by means of "adequate electronic means".

The European Trans-National Network for Extra-Judicial Alternative Dispute Settlement Between Professionals and Consumers (EEJ-NET and FIN-NET Systems)

On May 5, 2000, the E.U. Commission officially launched the "European Extra-Judicial Network EEJ-NET". The system's experimental phase began on October 16, 2001, after the Commission had issued Recommendation 2001/310/CE on April 4, 2001, on the "Principles related to extra-judicial bodies involved in the voluntary settlement of consumer disputes." (all documents and forms can be downloaded from: *http://europa.eu.int/comm/consumers/policy/developments/acce_just/index_en.html*).

The extra-judicial European network (EEJ-NET) shall handle trans-border disputes between consumers and providers of goods and/or services, such as supply problems, defective products, or products and services that do not conform to their description. These issues are dealt with by a sole, national arbitration chamber (known as a "Clearing House"), which have been established in each Member State. This arbitration chamber, which is a point of national contact, assists unsatisfied consumers with information. It also provides recourse to the alternative dispute resolution system in the country

where the business from which the products or services were purchased is located.

The primary purpose of the national Clearing House is to act as a sole point of reference at the national level. This role has two distinct aspects:

National Level

To provide consumers of each country with a sole point of contact from which they can obtain information from available bodies for extra-judicial dispute resolution within their jurisdiction and to which they can address their claims.

Member States may also consider the possibility of incorporating other functions so that these extra-judicial bodies can further assist consumers at a national level.

European Level

In the event that a consumer files a claim following a transaction with a supplier from another Member State, the Clearing House of the consumer's country should be available to provide information and assistance. Information may be obtained between the Clearing House of the supplier's country. The Clearing House also provides assistance to the consumer in terms of the filing and the forwarding of the claim. Moreover, the Clearing House provides information of national nature to other Clearing Houses of Members States seeking to advise consumers from their country of the appropriate bodies to address their claims within a given jurisdiction.

The Clearing Houses are provided with a certain number of specific functions. In any event, the list is not exhaustive and as the network evolves it is possible that new functions and projects will emerge.

Most Member States have set up clearing houses (amongst others: Austria, Ireland, Luxembourg, Sweden, the United Kingdom, Portugal, France and Finland. For the related websites see: *www.eej-net.org.uk/Europe/ europe.html*), in many cases using their national European Consumer Centre (sometimes called a Euroguichet) as the most appropriate location for the service. Norway and Iceland are participating as well and the Commission is looking at ways to bring enlargement candidate countries into the network.

However, the above-mentioned procedure does not have to occur entirely online. The consumer can obtain forms (available in the consumer's own language) from the official website, with which to send in claims, and can choose his or her own arbiter from a list of lawyers specialised in Consumer Protection Law. The procedure will not be costly and will be expedited through the legal system. The consumer is not required to seek out legal assistance.

The EEJ-Net will complement and reinforce the recently launched Financial Services complaints Network (FIN-NET – *http://finnet.jrc.it/en*) for resolution of consumer complaints on financial services.

3. ODR in the U.S.: the role of the International Centre for Dispute Resolution of the AAA

The current situation on ADR and ODR procedures in the United States points out the important role played by the American Arbitration Association (AAA), whose rules and procedures have been changed or modified for the resolution of disputes via an electronic forum. By evaluating the perspective and experience provided through the process of international arbitration as handled by the International Centre for Dispute Resolution (ICDR) – which is the international division of the AAA – it is possible to stress the key differences between the European and the American approach to the matters concerned.

The approach followed in the United States to develop Online Dispute Resolution procedures is focused on B2B disputes for online vertical markets. With over 1.2 trillion dollars in business-to-business e-commerce made in 2000 (with projections of B2B transactions which shall be more than quintuple in 2005), the need for an efficient method to resolve potential disputes in the related market has become fundamental.

In fact, regardless of whether modern companies utilise and work predominantly with computer technology or not, disputes will still arise. These disputes need a speedy resolution and, in the end, it seems inevitable that companies will look for some kind of online dispute resolution procedure, whether or not their business are digitally integrated.

Consequently, AAA has implemented protocols and procedures (in particular the E-commerce Dispute Management Protocol and the Due Process Protocol for B2B: see *www.adr.org*) for dealing with B2B disputes for online vertical markets. Such procedures are based on some principles whose importance has been underlined by more than 100 senior executive properly interviewed by the AAA: integrity, security, cost and effectiveness of technology.

Moreover, the Association is actually strengthening its capacity to service B2B vertically integrated markets where tens of thousands of online supply chain purchases for a given industry will soon occur, and its ability to handle any case online.

This new paradigm for conflict management will, on the one hand, allow for resolution and management of disputes at the comparable speed of the transaction but, on the other hand, will raise complex questions including those of procedural soundness.

The ICDR and the AAA actually offer a variety of options for ODR, but the main option for ODR in the United States, is considered to be the offer of hybrid solutions. In fact, the AAA has the ability to handle the entire case online or just the filing and exchange of documents, and then to conduct the hearings off-line. Parties can file any claim for any type of case through the Internet.

Another process called Online Assisted ADR (which is, to date, the most frequently used process with AAA) refers to a combination of both Internet access and online applications, incorporating the use of traditional methods such as document sharing and in-person-hearings. This seems to be a popular model that allows parties to adapt, depending on their personal preferences, technological capabilities and the complexity of the case.

Online ADR is yet another process that is accomplished exclusively online. A variety of resources could

be used, such as chat rooms, web-based meetings and document sharing. This model most likely fits with what otherwise might be handled as a "documents only" arbitration proceeding and is most suitable for low value or single-issue disputes.

In conclusion of this brief overview of the e-commerce services set up by the AAA in the field of online dispute resolution, we can summarise the main purposes of these procedures as follows:

- to facilitate B2B e-commerce integrity by assisting companies in avoiding disputes;
- to provide expertise to contain disputes; and
- to provide speedy and cost effective resolutions.

4. European and U.S. Approaches to ADR and ODR: the Key Differences

The key differences between the European and U.S. approaches may be summarised as follows:

- The European policy in this sector is focused on the Protection of Consumers. The above-mentioned activities in the development of an European Extra Judicial Network are designed to strengthen the legal instruments at the consumers' disposal, *i.e.*, by providing a policy which is increasingly angled towards consumers rather than one which favours the needs of e-commerce service providers.
- The European strategy in the field of Alternative Dispute Resolution does not focus on the development of online procedures, with the web-based technologies being only a small part of the proceedings and being limited to the possibility of downloading forms and documents from the Internet;
- Even the "traditional" part of the European ADR (which is not carried out online) is focused on B2C commercial relationship (as well as the related legal framework: see the E-commerce Directive 2000/31), and the development of proper alternative procedures for the resolution of B2B dispute is at this stage only a perspective to be further developed. B2B operators can only exploit indirect advantages from the EEJ-NET system, which is built on consumers' needs;
- The U.S. policy in the ADR and ODR sector on the other hand, is focused on the B2B market operators, and the related procedures have been developed to strengthen alternative "out-of-court dispute settlement" instruments for the providers of e-commerce services;
- The U.S. strategy aims to further strengthen the availability of online services in the field of ADRs, and the perspective is to turn the actual "traditional" ADRs into technologically integrated procedures to be provided completely online.

Perhaps the reason for such different approaches can be found in the European and American E-commerce markets themselves, the B2B e-commerce market in the United States being more developed than in Europe, where a considerable increase in the number of players and the scale of the budgets is anticipated from early 2005.

5. ADR and Online Related Services in the Member States: a Brief Overview

France

No online out-of-court disputes schemes currently exist in France.

In business-to-business transactions, it is possible to resort to out-of-court dispute settlement mechanisms, instead of going to court, if this has been provided for in the contract or if the parties in dispute agree to this mechanism.

However, these mechanisms are not specific to the settlement of disputes relating to online transactions. They apply to all disputes related to business-business transactions. Some of the out-of-court dispute settlement bodies propose online settlement services. Law firms can also offer arbitration schemes.

Germany

Out-of-court schemes are very rarely used in business-to-consumer transactions. Chambers of commerce (industry and trade) operate out-of-court dispute settlement schemes which are primarily used for business-to-business disputes. Some of these chambers also carry out arbitration for the settlement of consumer complaints.

The association for computer law provides out-of-court settlement schemes on the Internet (*www.cybercourt.org*) for both consumers and companies. There is one pilot scheme launched by the association which is carrying out an online court of arbitration.

Furthermore, law firms offer arbitration schemes in the business-to-business sector.

Apart from these general out-of-court schemes, there are no specific schemes for the settlement of disputes regarding information society services.

Spain

Regulation on out-of-court schemes exists but it is not focused on the settlement of disputes relating to online transactions.

The out-of-court settlement of disputes body in the framework of the 'FIN-NET' in Spain is *Banco de Espana*. The clearing house established in Spain in the framework of the 'EEJ-NET' is the Spanish Consumer.

Other Spanish alternative resolution bodies for business-to-consumer disputes not specific to information service providers can be found on the website of the Spanish Consumer Institute.

The Law on electronic commerce of June 27, 2002 (not yet published in the Official Journal) allows for contracting parties to submit their disputes to an arbitrator, including those involving standard contracts. It also allows the arbitration procedure to be carried out electronically.

The Law also adds that within one year after the adoption of the Law, the government will adopt a seal that will identify ISSPS which:

- comply with the codes of conduct adopted with the participation of consumer associations;
- adhere to the alternative dispute resolution systems; and
- have established notice and take down procedures of illicit material.

The Ministry of Economy has announced that it is working on a project to protect consumers when using new technologies. The project would include the creation of an arbitration court for e-commerce disputes. The arbitration court is expected to start operating in 2002.

United Kingdom

Trust UK is a non-profit organisation endorsed by the U.K. Government to enhance consumer confidence when buying online. Companies subscribing to a code of practice approved by Trust UK can use the trust UK hallmark on their website (see *www.trustuk.org.uk)*.

The "Which? Web Trader Scheme" has been set up in the United Kingdom under the umbrella of Trust UK to provide consumers with protection when purchasing online. It achieves this by ensuring that the participating traders provide consumers with a fair service. It also provides consumers with help if anything goes wrong.

Traders in the United Kingdom who agree to meet and abide by the Code of Practice may use the Web Trader logo on their website. Should customers complain about the services of Which? Web Traders these traders will be investigated and permission to display the logo may be withdrawn.

If the customers making the complaint is a subscriber to Which? Online, then, the scheme will provide legal help using lawyers from the Which? Legal Service.

Which? Web Trader has made arrangements with similar organisations in France, Belgium, Spain, Portugal, Italy and the Netherlands. Further details are available at *www.which.com/webtrader.*

Trusted Shops provides a money back guarantee to customers. The retailers subscribing to the scheme are obliged to comply with a number of obligations (see *www.trustedshops.com*).

Nominet, the U.K. Internet names organisation, has launched a revised Dispute Resolution Service (DRS) effective from September 24, 2001 (*www.nic.uk*). Nominet's DRS deals with disputes over U.K. domain names, using a similar system to that of the ICANN Uniform domain Name Dispute Resolution Policy. The DRS imposes on the complaint to prove that the disputed name is similar or identical to its registered or unregistered trademark and that the domain name holder has taken unfair advantage of these rights.

6. A brief overview of the Italian ADR Procedures

It must be pointed out that in Italy there are no specific laws about the so-called ADR related to online transaction, B2C or B2B. On the other hand, rules about arbitration and conciliation contained in the Law of December 29, 1993 No. 580 can be considered as the legal framework to refer to with regard to "traditional" out-of-court dispute settlement schemes.

With specific regard to the ADR related to the online transactions (B2C or B2B) or to disputes arising from Internet or e-commerce relationships, the Chamber of Commerce of Milan has recently introduced a new and interesting system (see section 7 below).

With regard to specific ADR procedures, it must be pointed out that in Italy, ADR has been set up in specific fields. For example, in the Telecommunications field, the Law of July 31, 1997 No. 247 has provided that the Italian Communications Authority institute its own arrangements to regulate out of court settlements of controversies that may arise between:

- telecommunication operators;
- users or categories of users and telecommunication operators.

For these controversies, identified by regulations introduced by the Italian Communication Authority, no recourse can be made to a court of law without a compulsory attempt at settlement being made, to then be concluded within thirty days from the day on which the petition was put to the Authority. For this purpose, the terms for appealing to courts of law are suspended until the term for the conclusion of the arbitration proceedings elapses.

With regard to controversies sub letter (a), a Regulation has been adopted with the Decision 148/01/CONS published in the Italian Official Journal of April 11, 2001 No. 85 "Regulation related to the resolution of disputes between Telecommunications operators". This particular ADR cannot in any case be carried out online.

With regard to controversies sub letter (b), a Regulation has been adopted with the Decision No. 182/02/CONS "Regulation related to the dispute resolution between Telecommunication Operators and users" (published in the Italian Official Journal of July 18, 2002 No. 167). This particular ADR also cannot be carried out online.

Furthermore, the law of July 30, 1998 No. 281 "Discipline of consumers' and users' rights" (published in the Italian Official Journal of August 14, 1998 No. 189) has introduced a specific ADR for consumers and users (also represented by the respective Associations), even if the alternative conciliation procedure (to be concluded within 60 days) cannot be carried out via the web.

Another ADR is that provided by the law of November 14, 1995 No. 481 "Provision for the regulation and the competition in the field of public utility services. Institution of the Authority for the regulation of public utility services". In common with the other ADRs, this alternative conciliation and arbitration procedure cannot be carried out via the web.

7. ODR Services in Italy: the Case of the Arbitration Chamber of Milan

With regard to Italy, this country has recently issued rules that provide for the government to adopt – among others – Directive 2000/31. Article 31 of Community Law 39/2002 outlines the principles and criteria for the receipt of the Electronic Commerce Directive. Paragraph 1, letter (m), provides that the future legislative decree (currently being prepared) should provide that

> " in the event of dissent between providers and receivers of information technology services, the out-of-court dispute settlement can also be adequately provided by electronic means". [emphasis added]

Clearly, our country has also followed in the footsteps of the European Community, and therefore the above considerations, about the limits of the new rules (see section 2 above) also apply to the pending national legal framework.

It is useful now to refer to concrete examples of ODR mechanisms that are already available to Italian users, by citing Italy's service of online dispute resolution of the Arbitration Chamber of Milan. (the website address for which is: *www.risolvionline.it).*

The ODR model of the Arbitration Chamber of Milan falls under the category of "online conciliation and mediation". This service enables the resolution of commercial disputes related to the Internet and e-commerce, and is targeted towards the resolution of disputes between both B2B and B2C. Lawyers may also send a request for settlement or participate in the settlement proceedings as the representative of a consumer or a business. There are no monetary limits: this service applies to all disputes, irrespective of their economic worth.

To summarise, the procedure is as follows:

- The parties that wish to bring a dispute to settlement complete and send the online application form for settlement.
- Upon receipt of the application, the manager of the service contacts the other party and invites the party to participate in the settlement by completing and sending (always via the web) the registration form for online dispute settlement proceedings. There is no obligation to submit to the settlement: if the party contacted by the manager does not accept to participate, the settlement proceedings will not take place.
- On the other hand, if the other party accepts to participate in the settlement proceedings, RisolviOnline assigns a conciliator to the case and fixes a date and time to start the settlement meeting, which will take place on a designated chat-line.
- At the date and time fixed by the manager, the parties and the conciliator will connect by web to the site *www.camera-arbitrale.com/conciliazione* and insert the settlement code, the password and the username assigned to them by RisolviOnline. The conciliator presides over the process, just as in a face-to-face conciliation.
- At the end of the meeting, if the result is positive the conciliator will send to each party, by mail, the meeting minutes of the online settlement that lust be printed in two copies to be signed and sent to RisolviOnline (by mail or by fax).
- The service collects the signed copies and sends them to the other party to ensure that both parties have a copy of the other's signed document. This last procedure is necessary to perfect the online agreement, to acquire the nature of a real binding contract applicable under the law to both parties.

The cost of this service by the Arbitration Chamber of Milan is proportional to the value of the dispute (and in any event offered freely until December 31, 2002). Even if payment is required to send the application, in the event that the other party refuses to participate in the settlement proceedings, the amount will be refunded in full by the banking services.

The first dispute handled by means of the ODR scheme outlined above, was resolved in June 2002.

Conclusion

It will be interesting to see if the online development of ADR will modify its methods, tools and goals. Certainly, the growth of online ADR is bound to be impressive. As electronic commerce grows, so will the need for new online tools for resolving e-commerce disputes. It appears as if mediation, much more so than arbitration, is well suited for diffusion on the web. Even today, arbitration requires a higher level of formality: it requires more signed documentation (even if electronic signatures could suffice) and more involved legal discussions. Mediation, on the other hand, favours informality.

One can likely assume that the development of online mediation will be more preferable for purely commercial disputes. It will be particularly well-suited for disputes of a purely monetary nature, for those involving insurance and in general for issues involving online users, for online financial trading, for e-commerce and for domain name disputes. Essentially, it will work best in areas that are already particularly equipped for a web marketplace, where businesses enter into contact in a fixed area for the purchase and sale of goods among themselves (in a vertical chain). It would seem that disputes that need a larger sphere for dialogue are certainly more apt for traditional "physical" mediation. One need only think of family, social, cultural and inter-ethnic disputes, to name but a few.

In sum, we can predict that online dispute resolution will have distinct and curious developments in the future:

- The apparently contradictory tendency to repress, in certain cases, the role of the third party (the model of "blind" negotiation), but also the discovery that the role of the conciliator can be mechanically assisted in mediating and obtaining compromises (the "open model of online mediation, especially with the prospect of further improvements in software). Perhaps the secret of the success of online dispute resolution lies in the combination of these two prospects.
- The tendency towards the *global*: e-commerce disputes occur between parties who are geographically distant, who have never seen each other, who have reached a deal between themselves and who have resolved their potential disputes without physically "meeting" each other. These parties do not need to know where their "jurisdiction" is located.
- The tendency towards the *local*: parties are in an environment (the Internet) that creates the context for business to take place and finds ways to resolve potential disputes. The Internet is the widest possible context, but it is an environment, and in this context, co-operative justice operates among participants: if you don't follow the rules and resolve disputes according to the established rules of practice within the environment in which you work, you will be excluded. From this viewpoint, these marketplaces are nothing more than the continuation of the story of the market itself.