



EUROPE

EU – New European e-privacy rules

On 18 December 2009, the new EU Directive 2009/136 on privacy and electronic communication was published in the EU Official Journal. The Directive modifies the existing E-Privacy Directive 2002/58 of 12 July 2002. It entered into force on 19 December 2009 and the EU Member States have to transpose it into national law by 25 May 2011.

(more on page 2)

Contents

EUROPE	1
• New European e-privacy rules	1
• Article 29 Data Protection Working Party finds that Andorra and Israel have an adequate level of protection of personal data	3
• EU ratifies the WIPO Copyright Treaty and the WIPO Performances and Phonograms Treaty	3
BELGIUM	4
• Act on games of chance amended in order to restrict online gambling	4
• New Act on payment services modifies the rules on electronic payment services	4
• Supreme Court finds that the confidentiality of communications applies to both the existence and the content of an e-mail	5
• Court of Appeal of Brussels asks preliminary question to the European Court of Justice in the Sabam v. Scarlet case	5
• Court of Appeal of Brussels finds that using a competitor's trade name or trademark in meta tags infringes the Fair Trade Practices Act	6
• Court of Appeal of Liège finds that the E-Commerce Act entitles only public authorities to enjoin a hosting provider to disclose personal data of its registered users	6
• Court of Appeal of Brussels finds that the license agreement of the Crossroads Bank for Entreprises for the re-use of its public sector information violates database law	7
• Court of Appeal of Brussels finds that the administrator of an online discussion forum can be held liable for publishing or preserving unlawful videos and articles	7
• Criminal Court of Brussels finds that online publications can qualify as a press delict and that purely technical webmasters cannot be held liable for a press delict if the website editor can be identified	8
• Criminal Court of Brussels finds that online publications can qualify as a press delict and that the person responsible for a website can be held liable for racist and xenophobic content on his website	8
• Court of First Instance of Brussels qualifies online defamation as a press delict	9
THE NETHERLANDS	9
• Court of Appeal of Amsterdam finds letter of objection sent by e-mail admissible under certain circumstances	9
• Court of Rotterdam partially annuls record spam fine	10
• OPTA publishes new assessment framework for compliance with Telecommunications Act	10

Data security breach notification

The most important new rule is the obligation to notify breaches of the security of personal data. However, this is not a general obligation; it only applies to providers of publicly available electronic communications services, such as telecommunication companies and internet service providers. A recital in the Directive provides, however, that the interest of users in being notified is not limited to the electronic communications sector and that therefore explicit, mandatory notification requirements applicable to all sectors should be introduced at EU level as a matter of priority.

A 'personal data breach' is broadly defined as 'a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed in connection with the provision of a publicly available electronic communications service in the Community'.

In the case of a personal data breach, the competent national authority must always be notified, regardless of whether or not there is a risk for the individual users concerned. The individual users themselves must be notified of the breach only if the breach is 'likely to adversely affect' their personal data or privacy. This is the case where the breach could result in, for example, identity theft or fraud, physical harm, significant humiliation or damage to reputation. In addition, the individual users do not have to be notified if the provider has demonstrated to the satisfaction of the competent national authority that it has implemented appropriate technological protection measures that render the data concerned unintelligible to any person who is not authorised to access it.

If the provider decides not to notify the individual users but the competent national authority is of the opinion that the breach is likely to have adverse effects for the users, then the authority may require the provider to notify the users. The competent national authority may also adopt guidelines and issue instructions concerning the circumstances in which providers are required to notify personal data breaches, the format of such notification and the manner in which the notification is to be made. They are also able to audit whether or not providers comply with their notification obligations and to impose appropriate sanctions in the event of a failure to do so.

Providers also have to maintain an inventory of personal data breaches comprising the facts surrounding the breach, its effects and the remedial action taken.

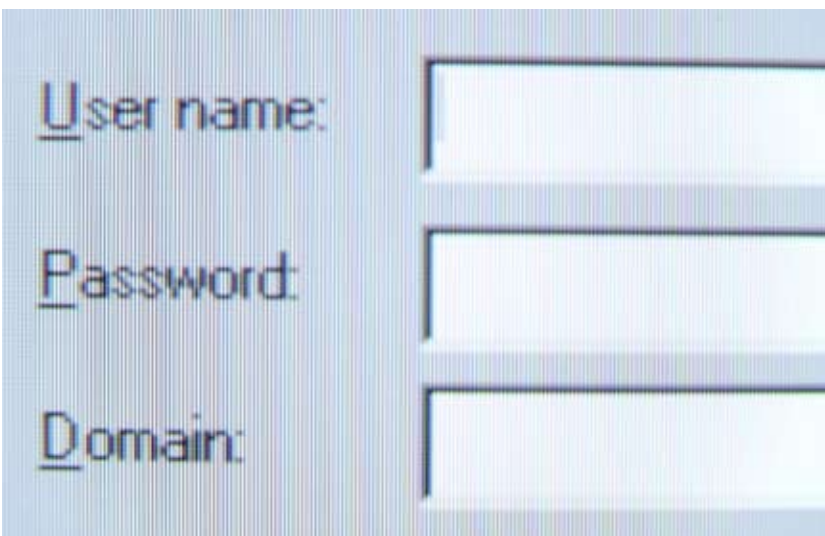
In its notification to the individual users, a provider must at a minimum describe the nature of the personal data breach and the contact points where more information can be obtained, as well as recommending measures to mitigate the possible adverse effects of the breach. The notification to the competent authority must also describe the consequences of the breach and the measures proposed or taken by the provider to address the breach.

Cookies, spyware, malware and viruses

Third parties may wish to store information on the equipment of a user or gain access to information already stored on the equipment, via cookies, spyware, malware or viruses. The existing E-Privacy Directive already contained rules on this issue, but these rules have now been modified in three ways.

Originally the scope of the rules was limited to the situation in which the accessing and storing of information on the user's equipment took place by means of *electronic communications networks*. It was unclear whether these rules also applied to the situation in which the cookies, spyware, malware or viruses were installed on the user's equipment by means of software on external data carriers (such as cd-roms or USB sticks) or downloads. In order to bring this situation also within the scope of the rules, the words 'the use of electronic communication networks to' have now been deleted.

As a second modification, the user's right of 'refusal' of such storage or access has been replaced by a right of 'consent'. Whether this change in terminology will make a difference, is doubtful, as a recital in the Directive still uses the word 'refusal'. Importantly, the same recital provides that, where it is technically possible



and effective, a provider may imply a user's consent from the settings of the user's browser or another application. This is a pragmatic solution to avoid that one cannot visit websites without each time being presented with a pop-up window asking for consent.

Under the previous rules, a provider was exempted from the obligation to offer a user information and a right of refusal if the sole purpose of the storage or access was *carrying out* or *facilitating* a communication over an electronic communications network. An example of *carrying out* a communication is transmitting an IP address to a service provider, because otherwise access to the internet is technically impossible. An example of *facilitating* is transmitting information on the user's preferred language to visit a certain website stored in a cookie. Now, as the third modification, the new rules delete the exemption for facilitating.

Spam

In the main, individuals do not have the means to initiate legal proceedings against senders of unsolicited electronic communications (spam) or the damage that they suffered does not suffice for them to initiate legal proceedings. The new rules aim to provide a more effective enforcement of anti-spam rules against spammers. Under the new rules, other natural or legal persons having a legitimate interest in the cessation or prohibition of the infringements of anti-spam rules are also entitled to initiate legal proceedings against spammers. These are, for instance, electronic communications service providers that wish to protect their legitimate business interests or trade unions that represent the interests of spammed members.

In addition, Member States may lay down specific penalties for electronic communications service providers which by their negligence contribute to infringement of anti-spam rules.

Stronger enforcement

The new Directive also provides stronger enforcement mechanisms. For instance, Member States have to grant competent national authorities the power to order the cessation of infringements of the e-privacy rules. (FDE)

The Directive can be found on <http://eur-lex.europa.eu>

EU – Article 29 Data Protection Working Party finds that Andorra and Israel have an adequate level of protection of personal data

On 1 December 2009, the Article 29 Data Protection Working Party issued two opinions in which it found that Andorra and Israel have an adequate level of protection of personal data. As both countries are now considered to offer an adequate level of protection, the transfer of personal data from the EU to them is no longer prohibited.

Despite an adequate level of protection being considered in place now, the Article 29 Working Party included in its opinions a few suggestions for improving the national Data Protection Acts, as both countries are currently in the process of adopting a new one.

Israel was advised to extend data protection to manual databases and to extend the application of the proportionality principle to data processing carried out by the private sector. Moreover, Israel needs an interpretation of the exemptions in international data transfers online as envisaged in the EU Data Protection Directive.

Andorra was recommended to explicitly include in its Data Protection Act that in case of automated individual decisions, the individual (the data subject) has the right to know the logic involved in the decision (even though this is already customary practice). (TS)

The opinions can be found on http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2009/wp165_en.pdf (Israel) and http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2009/wp166_en.pdf (Andorra)

EU – EU ratifies the WIPO Copyright Treaty and the WIPO Performances and Phonograms Treaty

On 14 December 2009, the EU and its Member States ratified the WIPO Copyright Treaty ('WCT') and the WIPO Performances and Phonograms Treaty ('WPPT'). Both treaties aim at bringing the protection of copyright and related rights into line with modern technologies, especially the internet.

The WCT explicitly states that computer programmes are literary works eligible for copyright protection. The WCT contains a few provisions granting rights to authors of literary and artistic works. The authors have the exclusive right to distribution and to authorise commercial rental and any public communication. Footnotes to the treaty Articles specify that the provisions fully apply in the digital environment, in particular to the use of works in digital form.

For example, the storage of a protected work in digital form in an electronic medium constitutes a reproduction.

The WPPT grants rights to performers and producers of phonograms. Performers have the right to demand to be identified as the performer and the exclusive right to authorise broadcasting and communication to the public of unfixed performances. Both performers and producers of phonograms have the exclusive rights of reproduction, distribution, authorising commercial rental and making protected content available online. Moreover, they are entitled to remuneration for broadcasting and communication to the public. These rights fully apply in the digital environment as well.

Both treaties also contain provisions requiring implementation measures. The Contracting Parties may, for example, provide for limitations of or exceptions to the rights granted to authors, performers and producers of phonograms. Implementation of the most suitable measures for enforcement is also left to the Contracting Parties.



In order to ensure a uniform application of both treaties by the Member States of the EU, the European Copyright Directive was issued right after signature of the treaties in 1996. The provisions of the Directive had to be transposed by 22 December 2002 at the latest. As a consequence, all national legislation is already in line with the two treaties. The treaties will enter into force with respect to the EU and its Member States on 14 March 2010. (TS)

The WCT can be found on http://www.wipo.int/export/sites/www/treaties/en/ip/wct/pdf/trtdocs_wo033.pdf and the WPPT on http://www.wipo.int/export/sites/www/treaties/en/ip/wppt/pdf/trtdocs_wo034.pdf

BELGIUM

BE – Act on games of chance amended in order to restrict online gambling

On 1 February 2010, the new Act of 10 January 2010 amending the Act of 7 May 1999 on games of chance was published in the Official Journal. The 1999 Act provides that, in principle, the exploitation of a gambling establishment is prohibited, unless such establishment has obtained a license from the Gambling Commission.

However, due to the emergence of a vast number of gambling websites which in turn lead to excessive gambling activity, the Belgian government had proposed a new Act aiming at regulating the activities of online gambling websites. One of the main changes made by the new Act is that it also brings online games of chance within the scope of the Act. As a result, international providers of online gambling websites which direct their activities towards the Belgian market have to comply with the Belgian Act on games of chance and must obtain a license to provide such games. One of the conditions to meet to obtain such a license is that the provider of the online game of chance must also provide the same game in the 'real world'. Therefore, providers of games of chance which limit their gambling services to internet gambling will not obtain a license from the Gambling Commission.

Another novelty is that, when the public prosecutor does not prosecute a violation of the Act, the Gambling Commission is entitled to impose administrative fines instead. (LDA)

The Act can be found on <http://www.belgiumlex.be>

BE – New Act on payment services modifies the rules on electronic payment services

On 15 January 2010, the new Act of 10 December 2009 on payment services was published in the Official Journal. It will enter into force on 1 April 2010. It transposes into Belgian law EU Directive 2007/64 which aims at coordinating national provisions regarding the access of new payment service providers to the market on the one hand, and information requirements and respective rights and obligations of payments services users and providers on the other hand. The Act covers all aspects of payment services and thus includes services provided electronically.

The Act consists of two parts: the first part specifies the information to be given to the payment service user, and the second part

contains the provisions on the rights and obligations of all parties with regard to the supply and use of payment services.

With respect to electronic payment services, the Act repeals the former Act of 17 July 2002 on transactions executed by means of instruments for the transfer of electronic financial means, and introduces the following specific provisions:

- in case of unauthorised payment transactions, the payer's payment service provider must immediately refund the payer the amount of the unauthorised payment transaction after having been notified without undue delay by the payer of the unauthorised or incorrectly executed payment. The payer can only be held liable for unauthorised payment transactions in case of fraudulent use or gross negligence;
- in case of non-execution or defective execution of the payment or use of an incorrect unique identifier, the payment service provider will be liable to the payer for correct execution of the payment transaction, unless it can prove to the payer and to the payee's payment service provider that the payee's payment service provider received the amount of the payment transaction;
- payment systems and payment service providers are permitted to process personal data when this is necessary to safeguard the prevention, investigation and detection of payment fraud. (LL)

The Act can be found on <http://www.belgiumlex.be>

BE – Supreme Court finds that the confidentiality of communications applies to both the existence and the content of an e-mail

In a judgement of 1 October 2009, the Supreme Court found that the confidentiality of electronic communications set forth in Article 124, 1° and 4° of the Electronic Communications Act of 13 June 2005 protects both the existence as well as the content of an e-mail.

The Court was requested by Schepens NV to annul a judgement of the Court of Appeal of Antwerp of 6 September 2007. In the legal proceedings before the Court of Appeal, the opposing party had invoked Article 124 as grounds to oppose to the use of the content of some e-mails in the proceedings. The Court of Appeal had decided that those e-mails indeed had to be excluded from the proceedings.

Schepens NV subsequently appealed to the Supreme Court, arguing that Article 124 only protects information relating to the transfer of

an e-mail message such as the names of the correspondents, the moment of sending and the duration and that the content itself of an e-mail is not protected by the confidentiality of electronic communications.

The Supreme Court found that Article 124 prohibits the interception and use of an e-mail without the prior consent of the sender thereto. According to the Court, one cannot become acquainted with the content of an e-mail without at the same time becoming acquainted with the existence of that e-mail. The Court therefore ruled that Article 124 equally protects the content of an e-mail and the information regarding the transfer of the e-mail. (SCO)

The case can be found on <http://jure.juridat.just.fgov.be>

BE – Court of Appeal of Brussels asks preliminary question to the European Court of Justice in the Sabam v. Scarlet case

In 2004, the Belgian Society of Authors, Composers and Publishers (Sabam) initiated legal proceedings against the internet service provider Tiscali Belgium, now Scarlet, before the Court of First Instance of Brussels, arguing that the ISP infringed Sabam members copyright by illegal music-file sharing over the ISP's peer-to-peer networks.

On 29 June 2007, the President of the Court held that Scarlet was indeed liable for the copyright infringements committed by its customers and ordered Scarlet to prevent its customers from illegally downloading copyright-protected music by installing a system to filter and block peer-to-peer files (see our previous ICT Law Newsletters No. 18 and 28).

Scarlet appealed this judgement. It argued that Article 87 §1 of the Copyright Act, which provides that a court can issue a cease-and-desist order to an intermediary service provider whose services are used by third parties for copyright infringement is not in conformity with the E-Copyright Directive 2001/29. Scarlet claimed that this Directive allows courts only to take *provisional* measures.

Sabam, on the other hand, argued that Article 87 §1 of the E-Copyright Act contains an unconditional obligation for courts to stop copyright infringements and that the E-Copyright Directive 2001/29 and the IP Enforcement Directive 2004/48 do not impact this obligation.

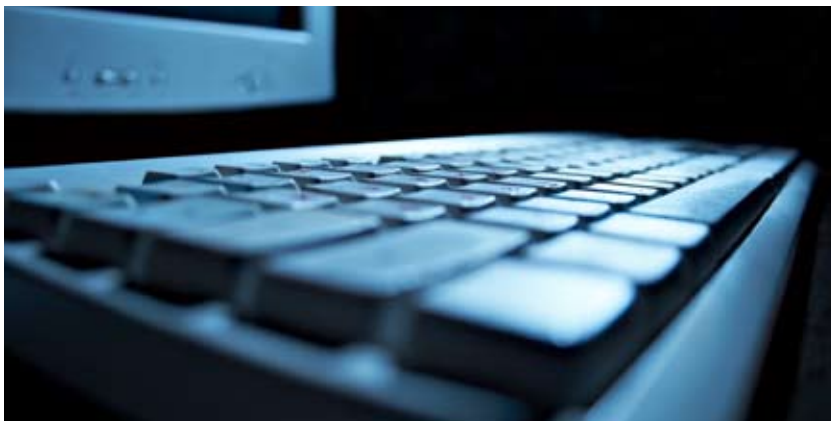
In its judgement of 28 January 2010, the Court of Appeal found that it is necessary to first ask the ECJ the preliminary question of

whether Directives 2001/29 and 2004/48, in combination with Directives 95/46, 2000/31 and 2002/58, allow a court to order an ISP to install such a preventative filter, and if so, whether the principle of proportionality is applicable when it is brought to rule on the efficiency and the dissuasive effect of the requested measure.

In the *Promusicae* case, the ECJ had already answered a preliminary question on Directives 2000/31, 2001/29, 2004/48 and 2002/58. The Court of Appeal, however, found that the circumstances in the *Promusicae* case were too different from this case to take the ECJ's judgement in the *Promusicae* case into account in the case now before it. According to the Court of Appeal, the infringement would be an *a priori* infringement of the privacy, whereas in the *Promusicae* case, the infringement was *a posteriori*. The Court also found that this case concerns the installation of a preventative system, whereas the *Promusicae* case was about revealing the identity and the addresses of people. As a result, the Court concluded that, given the difference in circumstances, it had to ask the ECJ for a new preliminary judgement, applied to the circumstances of this case. (EW)

BE – Court of Appeal of Brussels finds that using a competitor's trade name or trademark in meta tags infringes the Fair Trade Practices Act

In a judgement of 15 September 2009, the Court of Appeal of Brussels found that using a competitor's trade name or trademark in meta tags in order to direct users towards one's own website is an unfair trade practice.



Télé-Secours is a non-profit organisation which provides assistance at a distance to people who request its aid over the telephone. M.G. was the director of Group Elico, a company specialised in telephone security systems

and of Eurosoins, a company which gives aid and medical care to elderly people from a distance. M.G. decided to create the websites careassistance.org, careassistance.be and careassistance.com by means of which he would provide services similar to those of Télé-Secours. To attract customers, he used the words 'télésecours', 'telescours', 'télésecours', 'tele-secours', 'tele secours' and 'télé secours' as meta tags in the source code of his websites. Subsequently, Télé-Secours initiated cease-and-desist proceedings against M.G.

Télé-Secours argued that using the meta tags was an unfair trade practice as set forth in the Fair Trade Practice Act of 14 July 1991 because it created confusion. The Court found that the use of meta tags results in the competitor's website appearing in a search engine's search results when searching online for Télé-Secours and that, in addition, a meta tag is invisible, which means that consumers cannot see the difference between the competitors. The Court also found that a meta tag is not a form of authorised comparative advertising because it does not show the objective difference between two products. Therefore, the Court agreed with Télé-Secours and ordered M.G. to cease and desist using the meta tags. (LL)

The case can be found on <http://jure.juridat.just.fgov.be>

BE – Court of Appeal of Liège finds that the E-Commerce Act entitles only public authorities to enjoin a hosting provider to disclose personal data of its registered users

On 22 October 2009, the Court of Appeal of Liège issued a judgement in which it found that Article 21 §2 of the E-Commerce Act of 11 March 2003 entitles only public authorities to enjoin a hosting provider to disclose personal data of its registered users.

Some anonymous registered users of the website of the consumer rights association Test-Aankoop / Test-Achats ('TA') had posted slanderous comments about a company on TA's website. The company had subsequently initiated summary proceedings before the President of the Commercial Court of Liège requesting TA to be ordered to communicate to the President and to its own lawyer the identification data of the users concerned that are in TA's possession, such as their IP address. The company based its request on Article 21 §2 of the E-Commerce Act. This Article provides that an ISP has to communicate to the judicial or administrative authorities, at their request,

all information that it may have and that can be useful for seeking and finding offences made through their intermediary.

TA defended itself by arguing that, in summary proceedings, the President of a Court is only entitled to take *provisional* measures and that the alleged slander had not been sufficiently proven.

However, the President did not agree with TA and found that communicating the identification data would not cause substantial and irreparable harm. Moreover, he found that such disclosure was authorised by Article 21 §2 of the E-Commerce Act as it would take place upon an order of the President, being a 'judicial authority'. He therefore ordered TA to communicate the identification data to the company, subject to a penalty of EUR 1,000 per day of delay.

In order to avoid having to pay a penalty, TA communicated the identification data to the company, but it also lodged an appeal before the Court of Appeal of Liège. The Court found that the President's reasoning was incorrect and ruled that, according to the precise wording of Article 21 §2 of the E-Commerce Act, this Article entitles only public authorities, such as police and public prosecutors, and not private parties such as the claiming company to enjoin a hosting provider to communicate identification data of its users. (NRO)

BE – Court of Appeal of Brussels finds that the license agreement of the Crossroads Bank for Enterprises for the re-use of its public sector information violates database law

The Crossroads Bank for Enterprises ('CBE') is the official public register that pools all identification data of enterprises established in Belgium, such as the data of the national register of legal entities, the VAT number, the data of the National Social Security Office.

Pursuant to the Act of 16 January 2003 on the creation of the CBE, the Act of 7 March 2007 transposing EU Directive 2003/98 on the re-use of public sector information, and the Royal Decree of 18 July 2008 on the commercial re-use of the public sector information of the CBE, the CBE has been entitled to draw up the terms and conditions of a license agreement for licensing parts of the public sector information in its possession for commercial re-use.

This license agreement provided that a licensee was obliged to point out any discrepancy between the licensee's own data and the CBE's data, and, in that case, to grant the

CBE a royalty-free right to use the licensee's data in order for the CBE to complete and/or correct the CBE's data. However, a maker of a database, Infobase, willing to make use of the CBE's data, disagreed with this requirement and other clauses, arguing that these provisions were not compliant with the Royal Decree of 18 July 2008 mentioned above and with the Database Act of 31 August 1998. On 8 April 2009, the President of the Brussels Court of First Instance dismissed Infobase's claim in its entirety but Infobase appealed that judgement.

On 19 November 2009, the Court of Appeal of Brussels found that, at first sight, this requirement constituted a repeated and systematic extraction and/or re-utilisation of insubstantial parts of the contents of the licensee's databases, the cumulative effect of which is to reconstitute and/or make available to the public (and thus to the licensee's competitors) all or a substantial part of the contents of the licensee's databases. The Court found that this seriously prejudiced the licensee's investment and it therefore ordered the CBE to refrain from using this clause in its license agreement, subject to a penalty of EUR 2,500 per day.

Infobase's other claims, such as the removal from the license agreement of the CBE's audit right and the prohibition on putting the public sector information also at the disposal of people other than its end-users, were rejected by the Court as, in its opinion, Infobase did not sufficiently demonstrate the necessity of the requested provisional measures. (NRO)

The case can be found on <http://jure.juridat.just.fgov.be>

BE – Court of Appeal of Brussels finds that the administrator of an online discussion forum can be held liable for publishing or preserving unlawful videos and articles

In a recently published judgement of 23 January 2009, the Brussels Court of Appeal convicted two administrators of the website www.assabyle.com for inciting hatred and violence against the Jewish people.

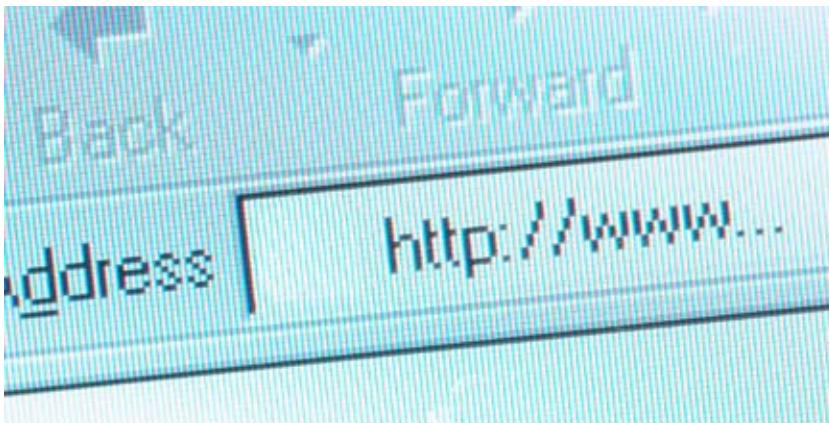
Both individuals were the administrators of the discussion forum on the website and were in charge of the daily management of this forum's content. On the forum, several articles and videos with a Zionist, racist and xenophobic content were available.

In March 2002, the Centre for Equal Opportunities and Opposition to Racism filed a criminal complaint against unidentified individuals. On 21 June 2006, the Criminal Court of

Brussels convicted the two administrators for anti-Semitism, negationism and incitement to hate. The Court of Appeal now confirmed this judgement.

The Court of Appeal found that by diffusing Zionist, racist and xenophobic articles and videos with full knowledge of the content thereof, the two administrators infringed the Anti-Racism and Anti-Xenophobia Act of 30 July 1981. According to the Court, a forum administrator is criminally liable if the administrator is the co-author or the accomplice of the internet user who posts an article or video on the administrator's online forum. The Court found that the administrator of an online discussion forum can be considered the author of a criminally infringing publication if the administrator:

- himself posts or diffuses the unlawful messages and acted as the author thereof;
- keeps the unlawful messages available on his forum with full knowledge of the content thereof; or
- modifies an existing message in such a way that makes it unlawful.



The Court found that the regime of exemption from liability set forth in the E-Commerce Act of 11 March 2003 only benefits intermediary service providers that merely transmit information. According to the Court, the Act does not provide such exemption regime for other intermediary service providers such as the administrators of online discussion forums.

Both administrators were ordered to pay a fine of EUR 2,000 or face imprisonment for one year. (SCO)

BE – Criminal Court of Brussels finds that online publications can qualify as a press delict and that purely technical webmasters cannot be held liable for a press delict if the website editor can be identified

In a recently published judgement of 23 June 2009, the Criminal Court of Brussels found that online publications can qualify as a press delict and that the related gradual liability regime set forth in Article 25 of the Constitution thus also applies to online publications. According to this gradual liability regime, a website editor is liable only if the author of the content concerned is not domiciled in Belgium. The Court also found that a webmaster who undertakes work of a purely technical nature is not liable for a press delict on the website if the website editor can be identified and is domiciled in Belgium.

In this case, two individuals were prosecuted for having published on a website a number of works of a discriminatory nature which had been written by an author who was not domiciled in Belgium. X was the person who had decided to publish these works online and Y was the webmaster who had only technically put the publication on the website. The website mentioned X as the responsible editor and Y as the webmaster.

In its judgement, the Court defined a press delict as an offence which *'has been committed by means of the press and which has been given a certain actual publicity and is an expression of opinion'*. The Court found that this publicity can also be given via the internet. The Court therefore applied Article 25 of the Constitution and found that X was liable for the publication of the discriminatory and xenophobic content, condemning him to one month's imprisonment. The Court also held that Y was not to be considered an editor of the website because of his purely technical role. (LL)

BE – Criminal Court of Brussels finds that online publications can qualify as a press delict and that the person responsible for a website can be held liable for racist and xenophobic content on his website

In a second judgement on the topic of press delicts, the Criminal Court of Brussels on 27 November 2009 again found that online publications can qualify as a press delict and that the person responsible for a website can be held liable for the content on that website when this content constitutes a press delict, so that that person's liability is subject to the

gradual liability regime for press delicts set forth in Article 25 of the Constitution.

The former chairwoman of the right-wing political party Front Nouveau de Belgique ('FNB') was accused of infringing the Anti-Racism Act of 30 July 1981 because some of her publications had incited hatred and racial discrimination. In this case, between 1 December 1997 and 1 June 1999 the FNB's party newspaper *Le Bastion* contained a number of articles of such discriminatory nature, some of which had been written by known authors, and others of which the author was unknown. The former chairwoman was the responsible editor for this newspaper at that time. Copies of the issues concerned had also been posted on the FNB's website, where they were accessible until 2003. As a result of these publications, the Center for Equality of Opportunities, the MRAX (Mouvement contre le Racisme, l'Antisémitisme et la Xénophobie) and the League for Human Rights filed a criminal complaint against the former chairwoman for acts of discrimination with regard to the articles of which the authors were unknown.

The Court found that, even though she alleged having no knowledge whatsoever of managing online publications, she was liable because she was the responsible person for the content of the newspaper and the content of the FNB's website. The Court found that traditionally, a press delict is defined as '*an offence that implies the expression of a thought or opinion in a published or printed written work*' and that this definition also covers online publications. Therefore, the Court applied Article 25 of the Constitution, held the former chairwoman, in her capacity of editor of the newspaper and the website, liable for acting in a way that incites hatred and racial discrimination, and condemned her to six months of imprisonment suspended. (LL)

BE – Court of First Instance of Brussels qualifies online defamation as a press delict

On 15 October 2009, the Court of First Instance of Brussels issued a judgement in which it found that posting defamatory comments below an online video can be considered a press delict.

In May 2008, an NGO in support of the people of Palestine organised a march in the city of Nivelles. As this march was rather controversial, some highly-ranked officials including Mr. F. gave a speech in which they clarified their position as regards the march. In his speech, Mr. F. stated i.a. that: '*I am determinate to*

fight against all extremists, all Nazis, all fascists wherever they are and whenever they show themselves'. This speech was filmed and subsequently partially posted by Mr. R on the website of an organisation defending the rights of Jewish people (CCOJB). Moreover, Mr. R. also put a comment below the video fragment stating that the video shows that Mr. F. assimilates the current Israeli policy with the Nazi policy. In response to this video fragment and Mr. R's comment, a vast number of internet users posted very violent and hurtful comments addressed to Mr. F.

Mr. F. felt aggrieved over the misrepresentation of his opinion and initiated legal proceedings against Mr. R. and the CCOJB before the Court of First Instance of Brussels. In its judgement, the Court first assessed whether online defamatory comments could be considered a press delict as set forth in Article 25 of the Constitution. According to the Court, a press delict is to be defined as '*an offence that implies the expression of a thought or opinion in a published and printed written work*'. Although Article 25 of the Constitution provides that it applies to expressions in a '*printed written work*', the Court found that this term should be interpreted extensively in order to take into account technological evolution. Consequently, in the Court's opinion, a threatening or defamatory comment posted on a website is to be considered a press delict.

This reasoning led the Court to conclude that Mr. R.'s online posting of only parts of Mr. F.'s speech and the accompanying comments had created a flagrant misrepresentation of Mr. F.'s opinion. Moreover, the Court found that Mr. R.'s conclusion that Mr. F. assimilated the current Israeli policy with the Nazi policy was clearly defamatory and was to be considered a press delict. (LDA)

THE NETHERLANDS

NL – Court of Appeal of Amsterdam finds letter of objection sent by e-mail admissible under certain circumstances

On 17 December 2009, the Tax Division of the Amsterdam Court of Appeal ruled that a letter of objection sent by e-mail under certain circumstances may be considered admissible as a means of objection in administrative procedures. According to the law a letter of objection requires a signature in order to verify its authenticity.

In this case, however, the responsible civil servant had not given the plaintiff the opportunity to remedy the formal failure. Moreover, the

civil servant's answer explicitly stated the letter of objection would be dealt with, resulting in a decision.

The court ruled that under these circumstances there was apparently no doubt as to the authenticity of the letter of objection, so that it could be considered admissible. (TS)

The case can be found on <http://zoeken.rechtspraak.nl>, LJN BK 7701

NL – Court of Rotterdam partially annuls record spam fine

On 15 January 2010, the Court of Rotterdam ruled that the Dutch Independent Post and Telecommunications Authority ('OPTA') did not sufficiently prove that a party was involved in sending out vast quantities of spam. Following various complaints via www.spamklacht.nl (OPTA's website for spam complaints), OPTA imposed a record fine of a total of EUR 510,000 upon the owners of two firms called Abodata and Call Data.

The actual transmission of the spam messages was conducted by Call Data, which had a formal partnership with Abodata. However, OPTA regarded the recently bankrupted Abodata as the originator of the spam, which advertised job vacancies at Abodata's 'thuiswerkcentrale' ('work at home centre'). Interested parties could react to the advertisement by calling an expensive 0900-number. To generate high call revenues, callers were kept on the line as long as possible by telephone operators who were specially trained for that purpose.



Call Data was fined EUR 270,000 for its role in this scheme, but did not raise any objection to the decision. Abodata, being fined another EUR 240,000, did lodge a notice of objection with OPTA. However, OPTA dismissed the objection stating that the nature of the activities of Abodata and its partnership with Call Data constituted sufficient grounds to consider Abodata to be an offender.

Abodata then appealed to the Court of Rotterdam, arguing that it was not aware of the spam operation. Abodata only had an agreement with Call Data for the joint use of workspace, personnel and facilities, but not for direct marketing activities. When it became clear to Abodata that Call Data was sending out spam in its name, it ended the partnership. The Court of Rotterdam found that OPTA did not sufficiently demonstrate that Abodata's defence was untruthful. The court held that the story of Abodata was not necessarily implausible or unlikely and therefore annulled the fine.

In the Netherlands, the prohibition on sending spam is laid down in article 11.7 of the Dutch Telecommunications Act. The legal concept of 'sender' is interpreted broadly and includes both the actual sender (e.g. a marketing company) and the material sender (i.e. the client). Both parties are obliged to comply with the prohibition. This judgement shows, however, that OPTA cannot simply identify a party as a material sender, but that it will need to provide sufficient proof, taking into account the defence of the alleged material sender. (WP)

The case can be found on: <http://zoeken.rechtspraak.nl>, LJN BK 9408

NL – OPTA publishes new assessment framework for compliance with Telecommunications Act

On 5 January 2010, the Dutch Independent Post and Telecommunications Authority (OPTA) published a new assessment framework for compliance with the provisions of the Telecommunications Act ('TA') regarding changes in and termination of contracts between providers and subscribers. According to the TA, providers of electronic communication services must announce every change in contract provisions at least four weeks in advance and enable the subscribers to terminate the contract free of charge.

OPTA monitors compliance with these provisions of the TA and is competent to take corrective measures if necessary. OPTA will use the so-called 'assessment framework' in executing its tasks. The main elements of this framework are:

- the right to terminate the contract applies in case of *every single* change in both written and non-written clauses, provided that it concerns changes to the detriment of the subscriber. Furthermore, there is no right to terminate if the change in contract provisions inevitably follows from changes in legislation or other government measures;

- unless explicitly provided for in the contract, price changes for inflation adjustment reasons are also to be considered as a change to the detriment of the subscriber resulting in a right to terminate;
- the subscriber should have at least four weeks in order to consider alternatives. The provider must enable the subscriber to compare the previous situation with the new one;
- every subscriber must be informed individually about the changes and the right to terminate their contract. Only if individual communication has proven to be impossible is information through general means of communication acceptable. The provider may also send individual short messages with a reference to further information on the website. The short message must however explicitly mention the right to terminate the contract;
- the provisions of the TA apply to both electronic communication and programme services. If both services are offered at the same time the right to terminate applies to both, unless based on the circumstances separate contracts can be concluded
- OPTA considers changes in television channels offered (when not being an extension) as a change to the detriment of the subscriber. The right to terminate does not apply if the disappearance of a channel results from its cancellation, the loss of broadcasting rights or a decision of the relevant programme council;
- the subscriber should be able to invoke his/her right to terminate the contract free of charge. By consequence all equipment owned by the subscriber does not have to be returned and if equipment has been given on loan, the provider must pay for its return. (TS)

The OPTA assessment framework can be found on <http://www.opta.nl/nl/actueel/alle-publicaties/publicatie/?id=3103>

Have contributed to this issue of the ICT Law Newsletter: Sofie Costermans, Laurens Dauwe, Frederic Debusseré, Lore Leitner, Wanne Pemmelaar, Reinout Rinzema, Nicolas Roland, Tim Sterkenburg, Erik Valgaeren, Christian van Seeters, Emmelie Wijckmans.

For more information

If you require further copies of this newsletter, or advice on any of the matters raised in it, please contact:

Amsterdam office

Reinout Rinzema, T +31 20 546 01 12, F +31 20 546 08 11, reinout.rinzema@stibbe.com

Brussels office

Erik Valgaeren, T +32 2 533 53 51, F +32 2 533 51 15, erik.valgaeren@stibbe.com

Amsterdam	Brussels	London	New York
Strawinskyalaan 2001	Central Plaza	Exchange House	489 Fifth Avenue
P.O. Box 75640	Loksumstraat 25 rue de Loxum	Primrose Street	32nd Floor
1070 AP Amsterdam	1000 Brussels	London EC2A 2ST	New York, NY 10017
The Netherlands	Belgium	United Kingdom	USA
T +31 20 546 06 06	T +32 2 533 52 11	T +44 20 7466 63 00	T +1 212 972 40 00
F +31 20 546 01 23	F +32 2 533 52 12	F +44 20 7466 63 11	F +1 212 972 49 29
info@stibbe.nl	info@stibbe.be	info@stibbe.co.uk	info@stibbeus.com

The ICT Law Newsletter is also available on our website www.stibbe.com

All rights reserved. Care has been taken to ensure that the content of this newsletter is as accurate as possible. However the accuracy and completeness of the information in this newsletter, largely based upon third party sources, cannot be guaranteed. The materials contained in this newsletter have been prepared and provided by Stibbe for information purposes only. They do not constitute legal or other professional advice and readers should not act upon the information contained in this newsletter without consulting legal counsel. Consultation of this newsletter will not create an attorney-client relationship between Stibbe and the reader. The newsletter may be used only for personal use and all other uses are prohibited.

Stibbe, Herbert Smith LLP and Gleiss Lutz are three independent firms which have a formal alliance.

© Stibbe 2010 Publisher: Erik Valgaeren, Stibbe, Central Plaza, Loksumstraat 25 rue de Loxum - BE-1000 Brussels