Available online at www.sciencedirect.com

ScienceDirect

www.compseconline.com/publications/prodclaw.htm

Computer Law & Security Review

European national news

Nick Pantlin[*]

Herbert Smith Freehills LLP, London, United Kingdom

Keywords:
Internet
ISP/Internet service provider
Software
Data protection
IT/Information technology
Communications
European law/Europe

ABSTRACT

The regular article tracking developments at the national level in key European countries in the area of IT and communications – co-ordinated by Herbert Smith Freehills LLP and contributed to by firms across Europe. This column provides a concise alerting service of important national developments in key European countries. Part of its purpose is to compliment the Journal's feature articles and briefing notes by keeping readers abreast of what is currently happening "on the ground" at a national level in implementing EU level legislation and international conventions and treaties. Where an item of European National News is of particular significance, CLSR may also cover it in more detail in the current or a subsequent edition.

1. Belgium

1.1. *Belgian Criminal Code amended to protect minors against 'grooming' and 'cyberluring'*

In April 2014, the Belgian Parliament adopted two new acts,[1] which amend the Belgian Criminal Code ("**BCC**") by introducing two new Articles, Article 377*quater* and Article 433*bis*/1 and adding a new section titled 'Luring of minors on the internet with a view to committing a crime or a misdemeanour'.

Prior to the adoption of these new acts, minors could only be protected against solicitation for sexual purposes through information and communication technologies ("**ICT**") by invoking Articles 379 and 210*bis* of the BCC. These Articles concern respectively (i) inciting minors to fornication and (ii) forgery of informatics. Neither of these Articles, however, specifically addresses the use of ICT to commit the offences of child grooming and cyberluring. Moreover, they predate the appearance of, for example, social media sites and chat rooms, which are commonly used by perpetrators of sexual abuse of minors. Therefore, the introduction of two up-to-date, explicit provisions can be perceived as a step forward.

Even though both new acts protect the same interests, their scope of application differs to a significant extent. The new Article 377*quater* penalizes the proposal made by an adult, via ICT, to meet a minor who is under 16 year-old, for the purpose of committing any of the offences listed in the chapters 'Indecent assault and rape', 'Depravity of youth and prostitution' and 'Public indecency' of the BCC, to the extent that this proposal is followed by material acts leading to such a meeting. The perpetrator of such offence may be punished with a prison sentence from 1 to 5 years.

The new section titled 'Luring of Minors on the internet with a view to committing a crime or misdemeanour' on the

* Nick Pantlin, Herbert Smith Freehills, Exchange House, Primrose St, London EC2A 2HS (Tel.: +44 20 7374 8000).
E-mail address: Nick.Pantlin@hsf.com.
URL: http://www.herbertsmithfreehills.com

[1] Act of 10 April 2014 regarding the protection of minors against solicitation with the purpose of committing criminal offences of a sexual nature, Official Gazette 30 April 2014; Act of 30 April 2014 amending the Criminal Code with a view to protect children against cyberlurers, Official Gazette 30 April 2014.

http://dx.doi.org/10.1016/j.clsr.2014.07.013
0267-3649/

other hand stipulates in its new Article 433*bis*/1 that an adult, communicating via ICT with an apparent or presumable minor in order to facilitate the commission of a crime or offence against that minor will be subject to imprisonment between 3 months and 5 years if one of the following four conditions is fulfilled:

- the adult has concealed or lied about his or her identity, age or capacity;
- the adult has stressed the confidentiality of their conversations;
- the adult has offered or mentioned the prospect of a gift or any other advantage; or
- the adult has deceived the minor in any other way.

The preparatory documents of the parliament on the adoption of the 'Cyberluring Act' clarify that as to the application of Article 433*bis*/1, it is of no importance whether or not the communication that took place between the adult and the minor actually resulted in a proposition or meeting, whereas the applicability of Article 377*quater* requires material acts leading to a meeting. Therefore, it seems that Article 433*bis*/1 has a broader scope of application than the new Article 377*quater*.

These new provisions have already proved to be useful, as the police were recently able to arrest a man in his forties, who tried to arrange a meeting with a 15-year old girl.[2]

Cédric Lindenmann, Junior Associate (cedric.lindenmann@stibbe.com) and **Emilie Claes**, Trainee (emilie.claes@stibbe.com) from Stibbe, Brussels (Tel: +32 2533 53 51).

2. Denmark

2.1. *Amended data retention requirements under Danish law*

On 8 April 2014, the European Court of Justice declared the European Data Retention Directive (2006/24/EC) invalid. Subsequently, the Danish Ministry of Justice has issued an executive order of amendment (BEK nr. 660/2014) amending the Danish Retention Order.

Previously, Danish internet service providers were required to retain data regarding internet sessions, including the sender's and recipient's IP addresses, the transmission protocol, the sender's and receiver's port numbers, and the time of the start and end of the communication.

Now, the only data that internet service providers shall retain about a user's access to the internet are:

- the allocated user identity (e.g. username or customer number);
- the user identity and the telephone number which has been allocated to communications as a part of a public electronic communication network;
- the name and address of the subscriber or registered user to whom an IP address or user identity or telephone number had been allocated at the time of communication; and
- the time of the beginning and end of a communication.

An internet service provider providing wireless access to the internet must also retain data concerning the local network's geographical or physical location and the identity of the used communication equipment.

The executive order of amendment became effective as of 22 June 2014. However, to allow internet service providers time to adapt to the new regulation, the order provides for a transitional period whereby the previous provisions apply until 22 September 2014.

Lau Normann Jørgensen, Partner, LNJ@kromannreumert.com and **Julie Aaby Ryttov**, Assistant Attorney, jry@kromannreumert.com from Kromann Reumert, Copenhagen office, Denmark (Tel. +45 70 12 12 11)

3. France

No contribution for this issue.

Alexandra Neri, Partner, alexandra.neri@hsf.com and **Jean-Baptiste Thomas-Sertillanges**, Avocat, Jean-Baptiste.Thomas-Sertillanges@hsf.com, from the Paris Office of Herbert Smith Freehills LLP (Tel.: +33 1 53 57 78 57).

4. Germany

4.1. *German Federal Court of Justice – judgement on liability of the owner of a private WLAN*

On 8 January 2014, the German Federal Court of Justice (*Bundesgerichtshof*, hereinafter "**BGH**") ruled that a father as the owner of a private wireless local area network ("**WLAN**") cannot be held responsible for copyright infringements committed by his adult son if he did not have any knowledge of such infringements in the past (I ZR 169/12 – "*BearShare*").

There is generally a presumption that the owner of an internet access that was used to commit copyright infringements (e.g. by using illegal file sharing sites) is responsible for such infringements. However, the Court found that an exception to this general rule exists if the respondent can demonstrate that he made his connection available to his family and that a specific family member might have committed the infringement. The owner of the access might have to perform some investigations in that regard. However, in that case the claimant will then bear the full burden of proving that the respondent committed the infringement.

This might even be the case if the father had not instructed his adult son that the use of internet file sharing services might result in a copyright infringement and had not forbidden the use of such services as long as there had not been any third party infringement in the past. The court ruled that within families it is appropriate for the owner of an internet connection to allow family members over 18 years of age, who are responsible for their actions on their own, to use

[2] http://datanews.knack.be/ict/nieuws/veertiger-die-met-belgisch-tienermeisje-afsprak-via-facebook-aangehouden/article-4000698796763.htm.