IRIS
Legal Observations
of the European Audiovisual Observatory
OBSERVATOIRE EUROPÉEN DE L'AUDIOVISUEL
EUROPEAN AUDIOVISUAL OBSERVATORY
EUROPÄISCHE AUDIOVISUELLE INFORMATIONSSTELLE

IRIS 2014-10/24

LU-Luxembourg:Ratification of the Council of Europe Convention on Cybercrime

On 18 July 2014, the Grand Duchy of Luxembourg formally ratified and implemented the Council of Europe Convention on Cybercrime, as well as its Additional Protocol concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems. As the Grand Duchy was one of the last members of the Council of Europe that had signed (in 2003), but not ratified the Convention and its Protocol, the Chambre des députés (parliamentary assembly) had become subject to pressure from a number of international organisations.

Luxembourg had already introduced, before the increasing importance of the Internet, provisions in its criminal law concerning attacks on information systems. Therefore, the majority of the provisions included in the Convention covering substantive aspects had already been transposed by the Luxembourgish legislator and did not need to be amended. This concerns, for example, the offences foreseen by the Convention in relation to child pornography: Article 383ter of the Luxemburgish Criminal Code already established, amongst others, an extensive provision according to which it is a criminal offence to store or transmit an image of a pornographic nature of a minor with a view to disseminating the images by any means.

Similarly, the aim of the Additional Protocol to the Convention, to harmonise "substantive criminal law in the fight against racism and xenophobia on the Internet" and to improve "international co-operation in this area" had already been reached in Luxembourg: the national Criminal Code covers these crimes; for instance, Article 3 of the Protocol relating to the dissemination of racist and xenophobic material through computer systems corresponds to article 457-1 of the Criminal Code. This provision proscribes incitement to hatred and violence against a person or a group via any written, spoken or pictorial means based on one of the elements included in article 454 of the Criminal Code. Article 454 even goes beyond the list contained in Article 2 of the Protocol, as it includes not only race, colour, descent, national or ethnic origin and religion, but also attacks on individuals or groups on the grounds of their sexual orientation, their gender, their disabilities, as well as their age.

However, the ratifying law aims at filling some gaps in the national substantive law, taking into consideration national case law. This especially concerns criminal provisions in view of data protection breaches. The law of 18 July 2014 modifies a number of provisions in the Criminal Code and the Code of Criminal Procedure. For example, Article 496 of the Criminal Code now also explicitly includes electronic keys and passwords amongst the objects that the perpetrator of the offence may aim at obtaining, as it was not possible under the previous situation to criminalise the act of "phishing" a password or "stealing" other persons' "online identities" if they were using their real names.

Most importantly, procedural rules were adapted in order to reflect the requirements of the Convention. In order to satisfy Title 2 of the Convention relating to expedited preservation of stored computer data, as one of the key amendments, Article 24-1, point 1 of the Code of Criminal Procedure introduces a "quick freeze procedure". According to this procedure, it will be possible to track and localise the origin or the destination of traffic data without the obligation of immediately opening a preliminary investigation. This will be possible by requiring that the providers, on specific notice, store whatever data is available on a specific user or account and keep it available for possible later formal requests by the competent authority to hand over the data. In that way, useful information that is likely to be lost or modified can be kept available on request by the investigating judge or the general public prosecutor for a 90 day-period. Finally, necessary amendments resulting from the above mentioned changes are also introduced in the data protection law for the electronic communications sector.

• *Loi du 18 juillet 2014 portant 1) approbation de la Convention du Conseil de l'Europe sur la cybercriminalité ouverte à la signature à Budapest le 23 novembre 2001, 2) approbation du Protocole additionnel à la Convention sur la cybercriminalité, relatif à l'incrimination d'actes de nature raciste et xénophobe commis par le biais de systèmes informatiques, fait à Strasbourg le 28 janvier 2003, 3) modification du Code pénal, 4) modification du Code d'instruction criminelle, 5) modification de la loi modifiée du 30 mai 2005 concernant la protection de la vie privée dans le secteur des communications électroniques, Mémorial A - N°157, 12 août 2014, page 2406* (Act of 18 July 2014 on the Council of Europe Convention on Cybercrime, the Additional Protocol, and other amendments, Memorial A - N°157, 12 August 2014, p. 2406)
http://merlin.obs.coe.int/redirect.php?id=17260
FR

Mark D. Cole & Jenny Metzdorf

University of Luxembourg, Luxembourg

OBSERVATOIRE EUROPÉEN DE L'AUDIOVISUEL
EUROPEAN AUDIOVISUAL OBSERVATORY
EUROPÄISCHE AUDIOVISUELLE INFORMATIONSSTELLE

IRIS
Legal Observations
of the European Audiovisual Observatory