[AT] Disclosure of IP Addresses under Security Police Act is Constitutional

IRIS 2012-10:1/5

Sebastian Schweda
Institute of European Media Law (EMR), Saarbrücken/Brussels

On 29 June 2012, the Austrian Verfassungsgerichtshof (Constitutional Court - VfGH) ruled that the disclosure of the owner of an IP address to the security authorities under Articles 53(3a)(2) and (3) of the Austrian Sicherheitspolizeigesetz (Security Police Act - SPG) did not breach either the secrecy of telecommunications or the right to data protection.

The plaintiff had given the impression on an Internet chat site that he was offering under-age children ("7-11 year olds, or even younger if required") for sex. The Vienna police authorities were informed and took immediate steps to ascertain, firstly, the IP address that had been used to send the message and then, from the Internet service provider, the plaintiff's name and address, since they believed the safety of minors was in immediate danger. The plaintiff initiated legal proceedings with the VfGH, claiming breaches of telecommunications secrecy under Article 10a of the Staatsgrundgesetz (Basic Law - StGG) and of the right to data protection under Article 1 of the Datenschutzgesetz 2000 (2000 Data Protection Act - DSG 2000) in conjunction with Article 8 of the European Convention on Human Rights (ECHR). In particular, he complained that no judicial warrant had been granted before the data had been accessed. Such a warrant was required for breaches of telecommunications secrecy according to Article 10a StGG.

However, the VfGH rejected the complaint. In its decision, it took the opportunity to state its general position on the scope of telecommunications secrecy. It considered that telecommunications secrecy covered "all content data" of a communication, but not "all telecommunications traffic". Under the SPG, the security authorities were entitled to investigate an IP address simply on the grounds of a message brought to their attention either by a communication partner or by an open Internet communication accessible to anyone. If the content of a communication was made known to the security authorities in this way, traffic data disclosed on this basis was not covered by telecommunications secrecy.

However, monitoring of Internet traffic or precautionary data storage were not authorised under Article 53(3a)(2) and (3) SPG. The VfGH therefore considered that this provision did not authorise the disclosure of content data and that, for

that reason, it did not constitute a breach of telecommunications privacy.

Although the right to data protection had been breached, this had taken place on a specific legal basis that was entirely reasonable, in view of the security authorities' remit to ward off dangerous attacks, which was in the public interest. Finally, Article 8 ECHR did not state that a judicial warrant was required for every intrusion.

The Oberste Gerichtshof (Supreme Court - OGH) had previously ruled that the disclosure of master data belonging to a (known) IP address by a provider did not constitute a breach of telecommunications secrecy if it formed part of a criminal investigation. It was irrelevant whether the provider itself, in order to issue information on master data, also had to process traffic data internally, as long as the "secret was not leaked" (see IRIS 2011-7/7).

Erkenntnis des österreichischen Verfassungsgerichtshofs vom 29. Juni 2012 (Az. B 1031/11-20)

http://www.vfgh.gv.at/cms/vfgh-site/attachments/7/9/2/CH0006/CMS1343980347887/ip_adresse_b1031-11.pdf

Decision of the Austrian Constitutional Court of 29 June 2012 (case no. B 1031/11-20)