[DE] Court Refuses to Open Main Proceedings on "Black Surfing"

IRIS 2010-9:1/18

Christian M. Bron
Institute of European Media Law (EMR), Saarbrücken/Brussels

In a decision of 3 August 2010, the Amtsgericht Wuppertal (Wuppertal District Court - AG) refused to open the main proceedings in a case concerning the unauthorised use of an unencrypted wireless network on the grounds of insufficient suspicion.

On two days in August 2008, the defendant had logged onto a third-party (unencrypted) wireless network without permission and without paying a fee.

In the AG's opinion, this did not constitute either the offence of unauthorised tapping under Article 89(1)(1) of the Telekommunikationsgesetz (Telecommunications Act - TKG) or unauthorised retrieval or acquisition of personal data under Articles 44 and 43(2)(3) of the Bundesdatenschutzgesetz (Federal Data Protection Act - BDSG). The AG therefore revised the opinion it had expressed in 2007 and, at the same time, opposed the view of the AG Zeven (Zeven District Court), which considered the unauthorised use of a WLAN to constitute unauthorised tapping under Articles 148 and 89 TKG (see IRIS 2010-3: 1/16).

The AG did not consider this to be a criminal act under Article 89(1)(1) TKG because the defendant's conduct did not represent "tapping" in the sense of the provision. Tapping should be understood as directly listening to something or making it audible for other people, as well as switching on a recording device. In any case, this required there to be some form of communication between other people, to which the perpetrator listened in as a third party. There must be a deliberate, purposeful receipt of third-party messages, which are deliberately and purposefully listened to by the culprit, in order for tapping to have taken place. In this case, the defendant did not deliberately and purposefully receive messages. By logging on to the unencrypted network, he had been able to share the use of the Internet connection. The necessary receipt of the IP address did not constitute tapping. The confidentiality of third-party communication was not affected by this act. Also, the defendant had also not listened in on a third-party exchange of data, since the IP address had been allocated to the defendant as the sole user of the Internet connection.

A punishable offence under Articles 44(1) and 43(2)(3) BDSG was ruled out because the defendant had not accessed or obtained any personal data. Personal data was any information on personal and factual conditions that was assigned to a natural person and not accessible to the public. However, IP data was not personal data in the sense of Article 3(1) BDSG, since the IP address was freely allocated to whichever computer was using the network. When it was received by the defendant, this data was therefore intended for him as the user.

Nor had a criminal offence been committed under Article 202b of the Strafgesetzbuch (Criminal Code) (interception of data) because the IP data received had been intended for the defendant as the user of the network.

Beschluss des AG Wuppertal (Az. 26 Ds-10 Js 1977/08-282/08)

http://medien-internet-und-recht.de/pdf/VT_MIR_2010_120.pdf

Decision of the Wuppertal District Court (case no. 26 Ds-10 Js 1977/08-282/08)