[DE] BGH Finds WLAN Operator Liable

IRIS 2010-7:1/13

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

On 12 May 2010, the Bundesgerichtshof (Federal Supreme Court - BGH) granted an injunction to a music rights marketing company against the private operator of a WLAN under contributory negligence rules.

A piece of music, the rights to which were marketed by the plaintiff, had been shared on the Internet using the defendant's WLAN. The plaintiff claimed damages from the defendant and demanded an injunction as well as reimbursement of the cost of sending a cease-and-desist demand. The Landgericht Frankfurt/Main (Frankfurt/Main district court) had essentially upheld the plaintiff's application. On appeal, however, the Oberlandesgericht Frankfurt/Main (Frankfurt/Main appeal court) had ruled that the WLAN operator was not liable.

Ruling on a further appeal, the BGH agreed that the plaintiff had no civil law entitlement to damages for breach of copyright by the defendant, either as perpetrator or participant, since it had not been proved that the defendant had shared the music himself or deliberately helped a third party to do so. There was every reason to assume that the person to whom an IP address had been allocated would be responsible for an infringement committed from that address. However, in this case, this assumption had been credibly refuted by the defendant's claim that he had been on holiday when the offence was committed. Neither had he intentionally participated in an infringement by a third party.

However, under contributory negligence rules, the BGH found the WLAN owner liable for failing to prevent a protected work from being made available to the public (Art. 19a of the Urheberrechtsgesetz - Copyright Act). By operating a WLAN that was not sufficiently secure, the defendant had wilfully and, with sufficient causality, contributed to this infringement and failed to meet his duty of due diligence in this respect. Even private individuals - if only in their own interest to protect their data - could be expected to verify whether their WLAN was sufficiently secure to prevent its misuse by third parties standing outside. Although private WLAN operators could not be required to ensure that their network was always protected by the latest technology, when buying a WLAN router they could be expected to implement "security measures that are standard for private households in accordance with their purpose".

© European Audiovisual Observatory (Council of Europe) 2026

The defendant's WLAN router was secured using a 16-digit password according to the WPA encryption method. The BGH held that this system had been adequate in September 2006, when the offence was committed. However, the defendant had not changed the original password set by the manufacturer. One of the "minimum standards for private computer use" at the time had been to enter a personal, sufficiently secure password.

Limitations of liability on the basis of which - in order to protect a business model, for example - preventative duties of due diligence were disregarded or which could apply to hosting service providers under Art. 10 of the Telemediengesetz (Telemedia Act - TMG) did not apply in this case. The BGH did not examine the more obvious possibility of indemnity for access providers under Art. 8 TMG (or Art. 9 of the Teledienstegesetz - Teleservices Act - that applied when the offence was committed).

Urteil des BGH vom 12. Mai 2010 (Az. I ZR 121/08)

http://juris.bundesgerichtshof.de/cgi-bin/rechtsprechung/document.py?Gericht=bgh&Art=en&Datum=Aktuell&Sort=12288&nr=52202&pos=2&anz=638

BGH ruling of 12 May 2010 (case no. I ZR 121/08)

© European Audiovisual Observatory (Council of Europe) 2026

© European Audiovisual Observatory (Council of Europe) 2026