Grundrecht auf Freifunken: Warum der BGH offenes WLAN nicht verbieten kann*

Die anstehende BGH-Entscheidung zu offenen Funknetzen vor dem Hintergrund des BVerfG-Urteils zur Vorratsdatenspeicherung

Oliver García**

19. April 2010

Am 12. Mai 2010 will der I. Zivilsenat des Bundesgerichtshofs eine Entscheidung zur Haftung im Internet (Az. I ZR 121/08) verkünden. Es geht um die Frage, ob private Internetnutzer, die in ihrem Haushalt ein Funknetz (WLAN) betreiben, von Rechts wegen verpflichtet sind, dieses so zu konfigurieren, daß Außenstehende darüber nicht auf das Internet zugreifen und so anonym Rechtsverletzungen begehen können. Die Antwort auf diese Frage hat die bisherige Instanzrechtsprechung ausschließlich durch einen Griff in den zivilrechtlichen Werkzeugkasten der Störerhaftung und der Verkehrssicherungspflicht zu geben versucht, und zwar sowohl Gerichte, die – wie das OLG Düsseldorf[1] – eine Haftung des WLAN-Betreibers bejaht haben, als auch das OLG Frankfurt[2], das im konkreten, nun zum BGH gelangten Fall eine Haftung verneint hat.

Daß sich der BGH, Berichten von der mündlichen Verhandlung am 18. März 2010 zufolge, bemerkenswert behutsam an diese Frage "herantastet", mag daher rühren, daß der Fall noch eine weitere Ebene hat, die bisher kaum in den Blick genommen wurde. Nämlich eine verfassungsrechtliche Ebene, die durch eine zwischenzeitliche Entscheidung des Bundesverfassungsgerichts nochmals an Gewicht gewonnen hat.

Diskutiert wurde in der mündlichen Verhandlung die auch bislang im Mittelpunkt stehende Frage, ob offene Funknetze nicht eine Gefahrenquelle seien, die zum Mißbrauch durch Dritte einladen, obwohl sich dieser technisch problemlos vermeiden ließe. In der Tat erscheint es auf den ersten Blick einleuchtend, zum Schutze vor potentiellen Rechtsverletzungen generell Sicherungsmaßnahmen zu verlangen, solange diese nur zumutbar sind. Dies war hier auch der Ausgangspunkt des OLG Frankfurt, das letztlich nur deshalb eine Haftung verneint hat, weil es meint, es könne vom Beklagten nicht verlangt werden, über den Standardpaßwortschutz, der eingestellt war, hinaus weitere Maßnahmen zu ergreifen. Die Forderung nach einfach zu erfüllenden Sicherungsmaßnahmen

* ⟨URL: http://delegibus.com/2010,2.pdf⟩, Erstveröffentlichung auf Telepolis unter ⟨URL: http://www.heise.de/tp/r4/artikel/32/32466/1.html⟩.

** Impressum: ⟨URL: http://dejure.org/impressum.html⟩.

[1] *OLG Düsseldorf*, Beschluß vom 27. Dezember 2007 – 20 W 157/07; *OLG Düsseldorf*, Beschluß vom 11. Mai 2009 – 20 W 146/08.

[2] *OLG Frankfurt a. M.*, Urteil vom 1. Juli 2008 – 11 U 52/07.

erscheint als gerechte Lösung im Sinne eines Ausgleichs zwischen dem Interesse an bequemer Internetnutzung und dem Anliegen, Rechtsverletzungen zu vermeiden. Aber so verlockend diese Lösung ist, so leicht läßt sie übersehen, daß hiermit der zweite Schritt vor dem ersten getan wäre. Übersprungen hätte man die Beantwortung der Frage, ob denn überhaupt eine Gefahr oder besser – worauf es rechtlich ankommt – eine sozial inadäquate Gefahr vorliegt.

Es ist verfehlt, zu meinen, im vorliegenden Fall ginge es lediglich um die Aufstellung von rechtlichen Regeln für Funknetze. Die Frage ist im Kern eine andere und der jetzige Streitfall kann nicht entschieden werden, ohne auf sie eine Antwort zu geben. Es geht um die Frage: Ist eine anonyme Internetnutzung rechtlich mißbilligt? Ist sie eine einzudämmende Gefahr? Daß der hier konkret gewordene Streit um das Ob und Wie einer Verschlüsselung nur eine zufällige Ausprägung des eigentlichen Problems ist, wird deutlich, wenn man sich folgenden Parallelfall vor Augen führt: Der Rechtsstreit wäre kein anderer, wenn es sich um ein verschlüsseltes Netz gehandelt hätte, das von einer Vielzahl von Personen berechtigt genutzt worden wäre, zum Beispiel in einer Wohnanlage, die über eine gemeinsame breitbandige Internetanbindung versorgt wird. Auch in diesem Fall hätte der durch eine Internetaktivität Verletzte auf der Suche nach dem Verletzer eine Rückverfolgung nur zu der Person erreichen können, auf deren Namen der Vertrag mit dem Internetprovider geschlossen ist.

Mehr noch: Die anonyme Internetnutzung ist weit davon entfernt, heute ein singulärer Ausnahmefall zu sein. Fast unüberschaubar sind die vorkommenden Konstellationen. Neben den seit den Frühzeiten des Internets bestehenden "Internetcafés", deren Dienstleistung gerade die Verschaffung eines ad-Hoc-Internetzugangs ist, wird es immer selbstverständlicher, daß Hotels, Gaststätten und Verkehrseinrichtungen, Bibliotheken und sonstige Freizeiteinrichtungen einen Netzzugang anbieten. Dabei spielt es im hiesigen Zusammenhang keine Rolle, ob es sich jeweils um ein Funknetz, verschlüsselt oder unverschlüsselt, oder um einen kabelgebundenen Zugang handelt, denn auch für den Fall, daß der Nutzer sich am Netz identifizieren muß, kann dies bei Rechtsverletzungen später nicht nutzbar gemacht werden: Die Daten, wer wann im Netz eingeloggt war, werden in der Regel nicht dauerhaft gespeichert (und dürfen von Rechts wegen nicht einmal gespeichert werden, siehe nur § 3a Satz 2 BDSG und, soweit anwendbar, § 12 TMG), liegen also nicht mehr vor, wenn ein Anspruchsteller die Verletzungshandlung in ein Netz zurückverfolgt hat.

Ja, selbst Fälle, an die man in diesem Zusammenhang zunächst nicht denkt, gehören dazu: An Universitäten und Schulen ist es selbstverständlich, daß die Studenten und Schüler in eigener Verantwortung die dort zur Verfügung stehenden Internetzugänge nutzen. Daß hier der berechtigte Personenkreis über Zugangsschutz von vornherein beschränkt ist, ist im Hinblick auf die Möglichkeiten einer späteren Verfolgung von Rechtsverletzungen unergiebig, da auch hier identifizierende Nutzungszeiten nicht gespeichert werden. Die Reihe der Beispiele läßt sich sogar noch um den typischen Computer am Arbeitsplatz erweitern. Der Arbeitnehmer, der vom Büro aus privat das Internet nutzt, ist insofern weitgehend anonym, als daß in der Regel alle Kollegen im gleichen Büro (seien es Dutzende oder Hunderte) sich im Internet mit der gleichen Zugangskennung (IP-Adresse) bewegen. Auch in diesen Fällen wird sich ein Anspruchsteller zunächst nur an die Universitäts- oder Schulverwaltung oder den Arbeitgeber wenden können, um gegebenenfalls von dort aus, mit herkömmlichen Methoden, den Täter zu ermitteln. Es sei denn – und dies wäre die weitergedachte mögliche Folge einer entsprechenden Entscheidung im vorliegenden

Fall des ungeschützten Funknetzes – er könnte sich an die Universität, die Schule (also in der Regel den Staat oder die Gemeinde) oder den Arbeitgeber als mittelbaren Störer oder Verletzer einer Verkehrssicherungspflicht halten, weil sie einen allzu unkontrollierten Internetzugang eröffnet haben.

Auf gleicher Linie liegt es, wenn nach internationalen Vorbildern immer mehr Städte dazu übergehen, Freifunkprojekte, wie es sie bisher aufgrund Privatinitiative gibt, in kommunaler Regie auf den Weg zu bringen. So plant der Berliner Senat, in Zusammenarbeit mit privaten Unternehmen einen flächendeckenden WLAN-Zugang für Bürger und Touristen.

Es ist nicht möglich, die Fälle einer (sei es nun gewollten oder unbewußten) Zugangsgewährung zum Internet durch Privatleute rechtlichen Regeln zu unterwerfen und sich über die Behandlung der Zugangsgewährung zum Internet durch die institutionellen Anbieter (Internetcafés, Gaststätten, Bibliotheken etc.) erst dann Gedanken zu machen, wenn einmal ein Streitfall auftritt. Vereinzelt ist schon auf den Wertungswiderspruch hingewiesen worden, den es darstellen würde, wenn man von Privatanwendern zur Vermeidung einer Haftung eine Absicherung von Funknetzen fordern würde, hingegen die institutionellen Anbieter weiterhin ein anonymes Surfen ermöglichen könnten. Dieser Widerspruch kann in zwei Richtungen gelöst werden: Eine Haftung allein aufgrund der Zugangsvermittlung wird auch für Private verneint oder sie wird einheitlich für Private und institutionelle Anbieter bejaht. Letzteres wird in Stellungnahmen, die den Wertungswiderspruch überhaupt ansprechen, offenbar als natürliche, dann hinzunehmende Folge – als "Kollateralschaden" – einer entsprechenden Entscheidung des BGH angesehen[3].

Dies wäre ein Irrtum! Eine (künftig sich entwickelnde) Rechtsprechung, die es zum Inhalt hätte, daß die genannten institutionellen Anbieter, um weiter Internetzugang gewähren zu können, die Personalien ihrer Nutzer aufnehmen und vorhalten müssen (andere Zugangskontrollen kommen ja nicht in Betracht), um ihrer Verkehrssicherungspflicht zu genügen, wäre ein Verstoß gegen das Grundgesetz. Ein solches Pflichtenregime kann von der Rechtsprechung nicht unter Anwendung der allgemeinen Regeln der Störerhaftung und/oder der Verkehrssicherungspflicht eingeführt werden. Die Frage, inwieweit hier der richterlichen Rechtsfortbildung an sich schon Grenzen gesetzt sind, kann dahinstehen, denn jedenfalls mit dem Urteil des Bundesverfassungsgerichts vom 2. März 2010 zur Vorratsdatenspeicherung[4] ist geklärt, daß es Aufgabe des Gesetzgebers ist, die hier betroffenen Grundrechtsbelange abzugrenzen. Das BVerfG hat in dieser Entscheidung eine Pflicht des Gesetzgebers zu differenzierten Regelungen hergeleitet. Es kann deshalb nicht in der Hand der Rechtsprechung liegen, den "Markt" der Anbieter freien Internetzugangs aufgrund allgemeiner zivilrechtlicher Grundsätze durchzunormieren. Dementsprechend hat der VI. Zivilsenat des BGH in seinem Urteil vom 23. Juni 2009[5] aus dem Gesetz ein – so ausdrücklich – "Recht des Internetnutzers auf Anonymität" hergeleitet und es deshalb abgelehnt, mit der Anonymität der Internetnutzung Einschränkungen für diejenigen zu begründen, die den Nutzern gewerblich den Zugang zum Internet gewähren.

Ist demnach der potentielle Wertungswiderspruch nicht nach dieser Seite hin (Verbot auch für institutionelle Betreiber) auflösbar, so muß er nach der

[3] Siehe etwa die von ZEIT ONLINE gewählte Überschrift zur mündlichen Verhandlung beim BGH: "BGH macht WLAN-Hotspots wohl dicht", 18. März 2010.

[4] *BVerfG*, Urteil vom 2. März 2010 – 1 BvR 256/08.

[5] *BGH*, Urteil vom 23. Juni 2009 – VI ZR 196/08 – spickmich).

anderen Seite hin aufgelöst werden, das heißt durch eine Verneinung entsprechender Pflichten auch der privaten WLAN-Betreiber.

Ohne daß es auf die Frage ankäme, ob auch bei gesonderter Betrachtung der dem BGH zur Entscheidung vorliegende Fall einen Grundrechtsbezug hat, bildet jedenfalls dieser potentielle Wertungswiderspruch das logische Scharnier, aufgrund dessen sich die anstehende Entscheidung des BGH messen lassen muß an der Rechtsprechung des BVerfG zu dem Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme[6] und der expliziten Aufgabenzuweisung an den Gesetzgeber[7]. Nur dem Gesetzgeber, nicht der Rechtsprechung kommt es zu, in einem demokratischen Prozeß die Entscheidung zu treffen, inwieweit die Freiheit, auch anonym das Internet zu nutzen, zugunsten von anderen berechtigten Interessen eingeschränkt werden soll.

Rechtsprechung

BGH: Urteil vom 23. Juni 2009 – VI ZR 196/08 – spickmich). dejure.org.

BVerfG: Urteil vom 2. März 2010 – 1 BvR 256/08. dejure.org.

BVerfG: Urteil vom 27. Februar 2008 – 1 BvR 370/07. dejure.org.

OLG Düsseldorf: Beschluß vom 11. Mai 2009 – 20 W 146/08. dejure.org.

OLG Düsseldorf: Beschluß vom 27. Dezember 2007 – 20 W 157/07. dejure.org.

OLG Frankfurt a. M.: Urteil vom 1. Juli 2008 – 11 U 52/07. dejure.org.

[6] *BVerfG*, Urteil vom 27. Februar 2008 – 1 BvR 370/07.

[7] *BVerfG*, Urteil vom 2. März 2010 – 1 BvR 256/08.