Gewerblicher Rechtsschutz und Urheberrecht Rechtsprechungs-Report

GRUR RR

Zeitschrift der Deutschen Vereinigung für gewerblichen Rechtsschutz und Urheberrecht

5/2006
Seite 145–176
6. Jahrgang · Mai 2006

In Gemeinschaft mit Gerhard Schricker und Joseph Straus herausgegeben von Rainer Jacobs und Peter Mes

Rechtsprechungsbericht

Rechtsprechungsbericht zur Auskunftspflicht des Access-Providers nach Urheberrechtsverletzungen im Internet

Anmerkung zu LG Flensburg, GRUR-RR 2006, 174

Ralf Dietrich *

I. Ausgangslage

Das vorliegende Urteil ist neben seiner unmittelbaren rechtlichen Bewertung insbesondere auf Grund seiner weiteren Auswirkungen auf den Schutz von Urheberrechten im Internet von großer Bedeutung. Das Urteil stellt fest: Accessprovider schulden den urheberrechtlich Verletzten nicht nur keine Auskünfte[1], sondern auch schon keine Speicherung von Daten, die zur Ermittlung der Täter dienen können. Dies bedeutet: Die durch Datenaustausch im Internet Verletzten können ihre Rechte kaum noch wahren.

Der Prozess ist nur vor dem Hintergrund der aktuellen rechtlichen und tatsächlichen Entwicklungen des Datenaustausches im Internet verständlich[2]: Durch Datenaustausch im Internet (Filesharing) werden heutzutage massenweise Computersoftware, Musikstücke und Videofilme illegal getauscht. Diesem „Treiben" wollten die Verletzten nicht länger tatenlos zusehen. Um gegen die Filesharer vorgehen zu können, müssen sie jedoch deren Identität kennen. Diese Identität als Dienstleistung zu ermitteln, hatte sich die Verfügungsbeklagte zur Aufgabe gemacht. Sie ermittelte im Tatzeitpunkt die IP-Adresse (die unverwechselbare Anschlusskennung des eingewählten Rechners, im Folgenden IP), um anhand dieser den Täter ermitteln und verfolgen zu können. Nur der Accessprovider als Zugangsvermittler zum Internet kann allerdings Auskunft geben, welcher Nutzer unter der ermittelten IP zum fraglichen Zeitpunkt eingewählt war und somit als Täter in Frage kommt. Es wurde jedoch erst kürzlich entschieden, dass das Urheberrecht den Verletzten keinen Auskunftsanspruch nach § 101 a UrhG zubilligt[3]. Diese schlugen daher einen Umweg ein: Etliche tausend Vorgänge wurden bei der Staatsanwaltschaft unter Angabe der verwendeten IP angezeigt. Der Staatsanwaltschaft wiederum teilten die Provider mit, wem die IP zugeordnet war. In der Folge forderten die Verletzten Akteneinsicht und verfolgten die ihnen nun bekannten Teilnehmer mit Hilfe des Urheberrechts.

Problematisch an diesem Vorgehen ist jedoch, dass die IP nicht – wie etwa eine Telefonnummer – statisch einem Nutzer zugeteilt wird. Dem Nutzer wird vielmehr bei jedem Einwahlvorgang eine andere IP zugewiesen (*dynamische IP*). Die Information, wem der Provider im fraglichen Moment die IP zugewiesen hatte, wer also für die illegale Handlung in Betracht kommt, muss der Provider aber unverzüglich löschen. Nur ausnahmsweise darf er dies mitspeichern und zwar dann, wenn er Anhaltspunkte dafür hat, dass der Zugang rechtsmissbräuchlich genutzt wird, § 100 III TKG. Das Unternehmen musste also die Provider dazu bewegen, diese Informationen, die Einwahldaten, zumindest abzuspeichern und für die Abfrage der Staatsanwaltschaften bereit zu halten, da ansonsten auch das Ermittlungsverfahren der Staatsanwaltschaft ins Leere ginge. Aus diesen Gründen versandte die Verfügungsbeklagte per E-Mail Angaben über die automatisiert ermittelten Vorgänge und zugeteilten IP an die zugehörigen Provider, verbunden mit der Aufforderung, die Verbindungsdaten mitzuspeichern. Die Anhaltspunkte für eine Speicherung lagen also vor.

Die Verfügungsklägerin wehrte sich hiergegen und machte diese Anfragen zum Streitgegenstand, zunächst per einstweiliger Verfügung. Sie machte geltend, dass bei diesen massenhaften Anfragen – über 500 Mails innerhalb weniger Tage, darunter 167 Mails an einem Tag – der Betrieb zum Teil erheblich gestört werde. Das vorliegende Urteil des Hauptsacheverfahrens gab dem Provider Recht.

II. Das Urteil

1. Eingriff in den eingerichteten und ausgeübten Gewerbebetrieb

Das Gericht wertete diese massenweisen Anfragen als rechtswidrigen Eingriff in den eingerichteten und ausgeübten Gewerbebetrieb. Dass eine solche Flut von zu bearbeitenden E-Mails – schließlich müssen sie jeweils geöffnet werden, um

* Rechtsanwalt und wiss. Angestellter der Universität Tübingen.

1) *OLG Frankfurt a. M.*, GRUR-RR 2005, 147 sowie *OLG Hamburg*, GRUR-RR 2005, 209; ausf. und zusammenf.: *Stadler*, Haftung für Informationen im Internet, 2005, Rdnrn. 141 ff.

2) Dazu *Dietrich*, NJW 2006, 809.

3) S. o. Fußn. 1.

zu kontrollieren, ob es sich nicht um dringliche Kundenanfragen oder ähnliches handelt – einen Geschäftsbetrieb erheblich beeinträchtigen kann, steht außer Frage. Das Gericht wertete das Versenden der E-Mails nach den Grundsätzen der Rechtsprechung als unmittelbaren und betriebsbezogenen Eingriff[4].

2. Rechtswidrigkeit oder Anspruch auf Speicherung?

Weitere Voraussetzung für einen Abwehranspruch gegen diesen Eingriff ist dessen Rechtswidrigkeit. Diese entfiele jedenfalls, sollte das Versenden rechtmäßig gewesen sein. Dann müsste der Provider den Bearbeitungsaufwand schlicht hinnehmen.

Der Eingriff wäre dann rechtmäßig, wenn er zur Durchsetzung eines Anspruchs erforderlich war. Ein solcher Anspruch wäre dann etwa gegeben, wenn der Provider der Verfügungsbeklagten zwar nicht Auskunft, aber doch immerhin Speicherung der Daten schuldete.

Dieser Anspruch auf Speicherung lässt sich jedoch nicht herleiten. Das Gericht führt hier zutreffend die §§ 8 und 9 TDG an. Das TDG ist auf Access-Providing anwendbar, auch wenn man diesen Dienst als Telekommunikationsdienst begreift[5]. TKG und TDG schließen sich insoweit nicht aus. Die Anwendung dieser Regelungen des TDG gebietet die richtlinienkonforme Auslegung[6]. Die genannten Normen regeln explizit, dass der Provider für nur durchgeleitete Informationen grundsätzlich nicht verantwortlich ist[7]. Ihn trifft auch keine Prüfpflicht, ob die Informationen rechtsmissbräuchlich durchgeleitet werden[8]. Grundsätzlich sind die Provider damit in ihrer Haftung privilegiert[9]. Nach dem Gesetzeswortlaut schuldet der Provider, wenn er von einem Rechtsverstoß eines Nutzers Kenntnis erlangt hat, ausnahmsweise die Sperrung des Zugangs und die Beseitigung der Information. Nach Kenntniserlangung besteht damit eine verschuldensunabhängige Störerhaftung als Ausnahme zum Grundsatz der Nichtverantwortlichkeit für fremde Informationen[10]. Diese führt jedoch nur zu einem Abwehranspruch in Form eines Unterlassungsanspruchs, nicht zu einem Schadensersatz- und Auskunftsanspruch[11]. Im zu Grunde liegenden Fall wurde statt einer Sperrung und Löschung dagegen eine Speicherung der Verbindungsdaten gefordert. Einen Anspruch darauf gäbe es nur, wenn man die Speicherung als ein Minus zur Sperrung und Entfernung begriffe oder die Ausnahmepflicht darauf analog ausdehnend und damit die Privilegierungsregelung einschränkend anwenden wollte[12]:

a) Der Anspruch auf Sperrung und Entfernung ist als Unterlassungsanspruch zu verstehen[13]. Demgegenüber sind Auskunfts- und Rechnungslegungsansprüche als Hilfsansprüche zum Schadensersatzanspruch anerkannt[14]. Die Speicherung von Daten stellt mitnichten ein Unterlassen oder einen Unterfall davon dar. Wie die Auskunft, so dient auch die Speicherung der Verfolgung; sie ist also nicht gleichzusetzen mit einer Sperrung, die im Sinne einer Unterlassung der Zugangsgewährung auf Verhinderung abzielt[15]. Das Speichern ist damit kein Minus zur Sperrung sondern ein Aliud, das argumentum a maiore ad minus greift nicht[16]. Es wird daher nicht von der Ausnahmeregelung umfasst.

b) Auch ist die Ausnahmeregelung nicht auf dem Wege der Analogie auf die Speicherung anzuwenden. Der Grundsatz ist die Nichtverantwortlichkeit. Die Ausnahme davon, nämlich die Pflicht zur Sperrung und Entfernung bei Kenntnis nach allgemeinen Grundsätzen, ist geregelt. Eine analoge Erweiterung von Ausnahmen ist methodisch problematisch und bedarf besonderer teleologischer Prüfung[17]: Der Zweck des Gesetzes war hier die Umsetzung der europarechtlichen Vorgaben. Da die Umsetzung als Vollharmonisierung gedacht ist, sind weder weitere noch engere Regelungen durch die Mitgliedstaaten im nationalen Recht möglich[18]. Die geregelte Ausnahme entspricht Art. 12 der Richtlinie 2000/31/EG. Diese sieht eine grundsätzliche Privilegierung vor. Sie lässt nur in Art. 12 III die Ausnahmepflicht, eine Rechtsverletzung abzustellen oder zu verhindern, zu. Weitergehende Ausnahmen gestattet sie nicht. Es besteht damit hier keine (planwidrige) Lücke, die der Ausfüllung bedarf und diese rechtfertigt, denn der Gesetzgeber wollte abschließend regeln und hat abschließend geregelt, argumentum e silentio (legis completae)[19]. Auch aus den weiteren Normen des TDG oder des UrhG – etwa § 101 a UrhG – ergibt sich kein andersgearteter Anspruch[20].

c) Demnach schuldete der Accessprovider der Verfügungsklägerin keine Auskunft. Der Unterlassungsanspruch ist in der Tat auf die Sperrpflicht begrenzt[21]. Ein Anspruch auf Speicherung, und dadurch diesen Anspruch durch Anfragen geltend zu machen, besteht nicht.

Bei einem angenommenen Eingriff in den Gewerbebetrieb führt dies jedoch noch nicht zwingend zur Rechtswidrigkeit. In einem weiteren Schritt muss diese auf Grund einer umfassenden Güter- und Interessenabwägung positiv festgestellt werden[22]. Zwar bestand durchaus Veranlassung, den Provider um Speicherung zu bitten. Eine Einzelmail unter Bündelung aller Anfragen statt 167 Einzelfragen am Tag wäre kaum Bedenken ausgesetzt, was das Gericht leider nicht ausdrücklich feststellte. Jedoch bestand kein Anlass, dieses Ansinnen in der berichteten massiven Weise zu verfolgen, insbesondere nicht mit dieser Anzahl an E-Mails. Das Gericht wertete unter Einbeziehung der Zahl der Anfragen und nahm im Ergebnis die Rechtswidrigkeit des Eingriffs an. Dem ist zuzustimmen: Auf Grund der bloßen Quantität von Anfragen, für die kein Rechtsgrund vorliegt, entsteht die Beeinträchtigung des Unternehmens, die es nicht hinzunehmen braucht. Die weiteren Voraussetzungen des Abwehranspruchs waren gegeben. Das Urteil ist daher im Ergebnis zu begrüßen.

III. Ausblick

Für die Urheberrechtsinhaber mag diese Entscheidung bitter sein, sehen sie ihre Rechte in weiten Teilen im Internet

4) *KG*, GRUR-RR 2005, 66; *OLG München*, MMR 2004, 324 m. w. Nachw.; kritischer die Literatur – stellvertretend: *Staudinger/Beater*, BGB, 13. Aufl. (1999), § 823 Anh. V Rdnr. 55.

5) *Spindler*, in: *Spindler/Schmitz/Geis*, TDG, § 2 Rdnrn. 25 f. m. w. Nachw. Eine obergerichtliche Klärung steht aus.

6) Dies dürfte jedenfalls für die Anwendbarkeit des § 9 TDG ganz überwiegende Ansicht sein, vgl. *Spindler* (o. Fußn. 5).

7) So genannte „Filterfunktion" des § 9 TDG, vgl. *Bohne*, GRUR-RR 2005, 145 (146); ausf. *Heß*, Die Verantwortlichkeit von Diensteanbietern für Informationen im Internet nach der Novellierung des Teledienstgesetzes, 2005, S. 35 ff.

8) Ausf.: *Heß* (o. Fußn. 7), S. 184 ff.

9) *OLG Frankfurt a. M.*, GRUR-RR 2005, 147; – Auskunftsanspruch; *Haug*, Grundwissen Internetrecht, 2005, S. 231 ff.

10) *OLG Frankfurt a. M.*, GRUR-RR 2005, 147; *v. Wolff*, in: *Wandtke/Bullinger*, Praxiskomm. z. UrheberR, 2. Aufl. (2006), § 97 Rdnrn. 25 ff., Erg. Bd., 2003, § 97 Rdnrn. 24 ff.

11) *OLG Frankfurt a. M.*, GRUR-RR 2005, 147; *BGH*, GRUR 2004, 860 (864) – Internet-Versteigerung; GRUR 2002, 618 – Meißner Dekor.

12) So noch das *LG Hamburg*, MMR 2005, 57, aufgehoben durch *OLG Hamburg*, GRUR-RR 2005, 209 = MMR 2005, 453.

13) *Schricker/Wild*, UrheberR, 2. Aufl. (1999), § 97 Rdnr. 46.

14) *Schricker/Wild* (o. Fußn. 13), § 97 Rdnr. 81.

15) Dabei ist beachtlich, dass die Verletzten nicht dazu aufforderten, obwohl es ihr gutes Recht ist, die Verletzungen ihrer Rechte zu unterbinden. Vielmehr kam es ihnen darauf an, Daten für massenhafte zivilrechtliche Schadensersatzansprüche zu erlangen.

16) *Sieber/Höfinger*, MMR 2004, 580; a. A. *Czychowski*, MMR 2004, 514 (516 f.) noch zum Auskunftsanspruch.

17) *Larenz*, Methodenlehre der Rechtswissenschaft, 6. Aufl. (1991), S. 370 ff., 381 ff.; *Canaris*, Die Feststellung von Lücken im Gesetz, 2. Aufl. (1983), S. 189 ff.

18) Begr. RegE BT-Dr 14/6098, S. 22.

19) Vgl. *Canaris* (o. Fußn. 17), S. 50 ff.

20) *Stadler*, Haftung für Informationen im Internet, 2005, Rdnrn. 141 e ff.

21) *Nordemann/Dustmann*, CR 2004, 385.

22) *Erman/Schiemann*, BGB, 11. Aufl. (2004), § 823 Rdnr. 49; *BGHZ* 3, 270 (281) = GRUR 1952, 225 – Constanze.

faktisch schutzlos ausgeliefert. Doch der Gesetzgeber hat sich dieses Problems bereits angenommen. Ein direkter Anspruch gegen die Provider ist in Planung und soll kodifiziert werden[23]. Dies soll nicht zuletzt die Staatsanwaltschaften entlasten. Die Provider befürchten schon jetzt enorme Lasten durch die zu erwartenden Anfragen. Für sie ist immerhin eine Aufwandsentschädigung zum Ausgleich vorgesehen, gem. Abs. 2 a. E. Allerdings drohen bei fehlerhaften Auskünften Schadensersatzverpflichtungen. Auf diesem Weg können also erhebliche Kosten auf sie zu kommen.

Die Wissenschaft sieht solchen Änderungen auch in dogmatischer Hinsicht skeptisch entgegen[24]. § 100 des Ref-E des Gesetzes zur Verbesserung der Durchsetzung von Rechten des geistigen Eigentums sieht vor, einen eigenen Auskunftsanspruch bei offensichtlicher Rechtsverletzung auch gegen Accessprovider festzuschreiben. Dieses soll der Umsetzung des Art. 8 der Richtlinie 2004/48/EG zur Durchsetzung der Rechte des geistigen Eigentums dienen[25]. Letztere schreibt jedoch nur einen Auskunftsanspruch bei Rechtsverletzungen gewerblichen Ausmaßes vor. Der Entwurf schränkt dahingehend jedoch nicht ein. Erst seine Begründung greift dies auf, schließt jedoch auch ein gewerbliches Ausmaß bei Verletzungen durch private Endverbraucher nicht aus, es sei denn, eine „gewisse Nachhaltigkeit" sei zu vermissen. Dies dürfte einer Bagatellgrenze im Ergebnis sehr nahe kommen. Wie das gewerbliche Ausmaß schon im Moment des Auskunftsverlangens festgestellt werden soll, ist dabei bei Verwendung dynamischer IP nicht unproblematisch. § 100 IV UrhG Ref-E enthält daneben eine allgemeine festgeschriebene Verhältnismäßigkeitsgrenze, welche früher nur der Gesetzesbegründung entnehmbar war[26].

Da es sich bei den zur Verfügung gestellten Daten um Verkehrsdaten handelt, ist weiter eine vorherige richterliche Anordnung – entsprechend §§ 100 g, h StPO notwendig. Die Gesetzesbegründung nimmt sich dieser Frage, die – wie sie richtig erkennt – eine verfassungsrechtliche ist, an[27]. Es wird ausdrücklich auf Auskünfte in Bezug auf dynamisch vergebene IP-Adressen verwiesen. Einige Gerichte verneinten bisher in diesen Fällen das Vorliegen von Verkehrsdaten und damit das Erfordernis eines richterlichen Beschlusses[28]. Nach richtiger Auffassung erstreckt sich jedoch die Auskunft in ganz typischer Weise auf Verbindungsdaten. Ein richterlicher Beschluss ist damit vonnöten. Eine Klarstellung dessen im Gesetz und nicht erst eine zurückhaltende Erwähnung in der Begründung wäre wünschenswert. Rechtsunsicherheit geht hier auch zu Lasten der Provider, denen schließlich bei fehlerhaft verweigerter Auskunft ein Schadensersatzanspruch droht. Um sie nicht daneben bei fehlerhaft erteilter Auskunft wegen Verletzung des Telekommunikationsgeheimnisses zivilrechtlich belangbar zu machen, werden die Provider in Abs. 5 des Entwurfs von der Haftung weitgehend freigestellt. Wie weit daneben der strafrechtliche Geheimnisschutz des § 206 StGB zu Gunsten der Provider davon eingeschränkt wird und werden soll, bleibt fraglich.

Wie der verschuldensunabhängige Auskunftsanspruch systematisch-dogmatisch in die Konzeption des TDG einzupassen ist, bleibt ebenso offen. Die Wertung des § 100 UrhG Ref-E setzt sich mit der oben dargelegten des TDG in unaufgelösten Widerspruch. Dabei sollte das TDG die Verantwortlichkeit von Teledienstleistern umfassend für alle Rechtsgebiete regeln[29]. Sein eigenes Ziel droht der Gesetzgeber nun durch Ausnahmeregelungen in anderen Gesetzen zu unterlaufen. Ein weiteres Problem ergibt sich aus dem TKG und der dort verankerten Pflicht zur Löschung von Verbindungsdaten, wie sie erst jüngst das *LG Darmstadt* gem. § 96 II 2 TKG hervorhob[30]. Müssen die Daten aber sofort gelöscht werden, dann wären gar keine Daten mehr vorhanden, über die Auskunft erteilt werden könnte. Der Anspruch liefe leer. Ein Rückgriff auf die verdachtsunabhängig gespeicherten Vorratsdaten, wie sie durch die EU derzeit geplant sind, ist schon wegen deren Zweckbindung für die Verfolgung von schweren Straftaten und der Zugriffserlaubnis nur durch Strafverfolgungsbehörden seitens Ziviler nach jetzigem Stand nicht möglich. Eine Aufweichung stieße auf ganz erhebliche verfassungsrechtliche Bedenken. Ein gesonderter vorgeschalteter Anspruch auf Speicherung ist nötig. Eine Reform des § 96 II 1 TKG soll dem zwar Abhilfe schaffen. Die Norm zählt bislang nach dem Wortlaut abschließend die Fälle auf, in denen Verbindungsdaten gespeichert werden dürfen. Durch Anfügen von sonstigen Speicherungsmöglichkeiten, die von „durch andere gesetzliche Vorschriften begründeten Zwecken" eröffnet werden würden, entstünde jedoch eine nicht mehr überschaubare Generalklausel, so ist zu befürchten. Ob eine solche pauschale Aufweichung eines solch wichtigen verfassungsrechtlich geschützten Bereiches der richtige Weg ist, darf bezweifelt werden.

Im vorliegenden Urteil zeigt sich ebenso wie in den angeführten Reformbemühungen, dass die Gerichte und der Gesetzgeber von der technischen Entwicklung und von europarechtliehen Vorgaben zugleich getrieben sind. Der Schutz der Urheberrechte im Internet ist ein wichtiges Anliegen. Ein Auskunftsanspruch muss aber zunächst eine ausgewogene Regelung darstellen, die die Stellung der Verletzten, der Zugangsvermittler wie der Verletzer in Einklang bringt. Daneben sind datenschutz-, telekommunikations- und teledienstrechtliche Implikationen zu beachten. Beides steht noch aus.

---

23) Pressemitteilung des Bundesjustizministeriums v. 12. 12. 2005 – abrufbar unter www.bmj.de – unter ausdrücklicher Bezugnahme auf illegale Tauschbörsen.

24) *Bohne*, GRUR-RR 2005, 145 (146) meint, ein solcher Anspruch wäre „fatal". Instruktiv und umfassend: Die Stellungnahme zu § 101 UrhG-E des Deutschen Forschungsnetzes (DFN) v. 28. 2. 2006, abrufbar unter www.dfn.de.

25) So genannte Enforcement-Richtlinie 2004/48/EG des Europäischen Parlaments und des Rats v. 29. 4. 2004 zur Durchsetzung der Rechte des Geistigen Eigentums (ABlEU Nr. L 195 v. 30. 4. 2004, S. 16).

26) Reg-E BT-Dr 14/6098, S. 23.

27) S. 82 des Ref-E Ges. z. Verbesserung der Durchsetzung von Rechten des geistigen Eigentums v. 3. 1. 2006.

28) *LG Ulm*, MMR 2004, 187; *LG Bonn*, DuD 2004, 628 m. Anm. *Köbele* auf S. 609; *Dietrich*, NJW 2006, 809; a. A. *LG Köln*, Beschl. v. 30. 6. 2004 – 111 Qs 124/04; *LG Stuttgart*, NJW 2005, 614 = CR 2005, 598 ff. m. Anm. *Gerke*, S. 599; *LG Hamburg*, MMR 2005, 711.

29) *Spindler*, (o. Fußn. 5), Vorb. § 8 Rdnr. 1. Die vom Gesetzgeber gewollte „Filterfunktion" für andere Gesetze – s. RegE BT-Dr 14/6098, S. 23 – würde verloren gehen.

30) *LG Darmstadt*, GRUR-RR 2006, 173 – Löschung der IP-Adressen (in diesem Heft).

Dietrich: Rechtsprechungsbericht zur Auskunftspflicht des Access-Providers nach Urheberrechtsverletzungen im Internet - Anmerkung zu LG Flensburg, GRUR-RR 2006, 174 GRUR-RR 2006, 145

Rechtsprechungsbericht zur Auskunftspflicht des Access-Providers nach Urheberrechtsverletzungen im Internet
Anmerkung zu LG Flensburg, GRUR-RR 2006, 174

Ralf Dietrich *

I. Ausgangslage

Das vorliegende Urteil ist neben seiner unmittelbaren rechtlichen Bewertung insbesondere auf Grund seiner weiteren Auswirkungen auf den Schutz von Urheberrechten im Internet von großer Bedeutung. Das Urteil stellt fest: Accessprovider schulden den urheberrechtlich Verletzten nicht nur keine Auskünfte[1], sondern auch schon keine Speicherung von Daten, die zur Ermittlung der Täter dienen können. Dies bedeutet: Die durch Datenaustausch im Internet Verletzten können ihre Rechte kaum noch wahren.

Der Prozess ist nur vor dem Hintergrund der aktuellen rechtlichen und tatsächlichen Entwicklungen des Datenaustausches im Internet verständlich[2]: Durch Datenaustausch im Internet (Filesharing) werden heutzutage massenweise Computersoftware, Musikstücke und Videofilme illegal getauscht. Diesem „Treiben" wollten die Verletzten nicht länger tatenlos zusehen. Um gegen die Filesharer vorgehen zu können, müssen sie jedoch deren Identität kennen. Diese Identität als Dienstleistung zu ermitteln, hatte sich die Verfügungsbeklagte zur Aufgabe gemacht. Sie ermittelte im Tatzeitpunkt die IP-Adresse (die unverwechselbare Anschlusskennung des eingewählten Rechners, im Folgenden IP), um anhand dieser den Täter ermitteln und verfolgen zu können. Nur der Accessprovider als Zugangsvermittler zum Internet kann allerdings Auskunft geben, welcher Nutzer unter der ermittelten IP zum fraglichen Zeitpunkt eingewählt war und somit als Täter in Frage kommt. Es wurde jedoch erst kürzlich entschieden, dass das Urheberrecht den Verletzten keinen Auskunftsanspruch nach § 101a UrhG zubilligt[3]. Diese schlugen daher einen Umweg ein: Etliche tausend Vorgänge wurden bei der Staatsanwaltschaft unter Angabe der verwendeten IP angezeigt. Der Staatsanwaltschaft wiederum teilten die Provider mit, wem die IP zugeordnet war. In der Folge forderten die Verletzten Akteneinsicht und verfolgten die ihnen nun bekannten Teilnehmer mit Hilfe des Urheberrechts.

Problematisch an diesem Vorgehen ist jedoch, dass die IP nicht - wie etwa eine Telefonnummer - statisch einem Nutzer zugeteilt wird. Dem Nutzer wird vielmehr bei jedem Einwahlvorgang eine andere IP zugewiesen (*dynamische IP*). Die Information, wem der Provider im fraglichen Moment die IP zugewiesen hatte, wer also für die illegale Handlung in Betracht kommt, muss der Provider aber unverzüglich löschen. Nur ausnahmsweise darf er dies mitspeichern und zwar dann, wenn er Anhaltspunkte dafür hat, dass der Zugang rechtsmissbräuchlich genutzt wird, § 100III TKG. Das Unternehmen musste also die Provider dazu bewegen, diese Informationen, die Einwahldaten, zumindest abzuspeichern und für die Abfrage der Staatsanwaltschaften bereit zu halten, da ansonsten auch das Ermittlungsverfahren der Staatsanwaltschaft ins Leere ginge. Aus diesen Gründen versandte die Verfügungsbeklagte per E-Mail Angaben über die automatisiert ermittelten Vorgänge und zugeteilten IP an die zugehörigen Provider, verbunden mit der Aufforderung, die Verbindungsdaten mitzuspeichern. Die Anhaltspunkte für eine Speicherung lagen also vor.

Die Verfügungsklägerin wehrte sich hiergegen und machte diese Anfragen zum Streitgegenstand, zunächst per einstweiliger Verfügung. Sie machte geltend, dass bei diesen massenhaften Anfragen - über 500 Mails innerhalb weniger Tage, darunter 167 Mails an einem Tag - der Betrieb zum Teil

erheblich gestört werde. Das vorliegende Urteil des Hauptsacheverfahrens gab dem Provider Recht.

II. Das Urteil

1. Eingriff in den eingerichteten und ausgeübten Gewerbebetrieb

Das Gericht wertete diese massenweisen Anfragen als rechtswidrigen Eingriff in den eingerichteten und ausgeübten Gewerbebetrieb. Dass eine solche Flut von zu bearbeitenden E-Mails - schließlich müssen sie jeweils geöffnet werden, um

zu kontrollieren, ob es sich nicht um dringliche Kundenanfragen oder ähnliches handelt - einen Geschäftsbetrieb erheblich beeinträchtigen kann, steht außer Frage. Das Gericht wertete das Versenden der E-Mails nach den Grundsätzen der Rechtsprechung als unmittelbaren und betriebsbezogenen Eingriff[4].

2. Rechtswidrigkeit oder Anspruch auf Speicherung?

Weitere Voraussetzung für einen Abwehranspruch gegen diesen Eingriff ist dessen Rechtswidrigkeit. Diese entfiele jedenfalls, sollte das Versenden rechtmäßig gewesen sein. Dann müsste der Provider den Bearbeitungsaufwand schlicht hinnehmen.

Der Eingriff wäre dann rechtmäßig, wenn er zur Durchsetzung eines Anspruchs erforderlich war. Ein solcher Anspruch wäre dann etwa gegeben, wenn der Provider der Verfügungsbeklagten zwar nicht Auskunft, aber doch immerhin Speicherung der Daten schuldete.

Dieser Anspruch auf Speicherung lässt sich jedoch nicht herleiten. Das Gericht führt hier zutreffend die §§ 8 und 9 TDG an. Das TDG ist auf Access-Providing anwendbar, auch wenn man diesen Dienst als Telekommunikationsdienst begreift[5]. TKG und TDG schließen sich insoweit nicht aus. Die Anwendung dieser Regelungen des TDG gebietet die richtlinienkonforme Auslegung[6]. Die genannten Normen regeln explizit, dass der Provider für nur durchgeleitete Informationen grundsätzlich nicht verantwortlich ist[7]. Ihn trifft auch keine Prüfpflicht, ob die Informationen rechtsmissbräuchlich durchgeleitet werden[8]. Grundsätzlich sind die Provider damit in ihrer Haftung privilegiert[9]. Nach dem Gesetzeswortlaut schuldet der Provider, wenn er von einem Rechtsverstoß eines Nutzers Kenntnis erlangt hat, ausnahmsweise die Sperrung des Zugangs und die Beseitigung der Information. Nach Kenntniserlangung besteht damit eine verschuldensunabhängige Störerhaftung als Ausnahme zum Grundsatz der Nichtverantwortlichkeit für fremde Informationen[10]. Diese führt jedoch nur zu einem Abwehranspruch in Form eines Unterlassungsanspruchs, nicht zu einem Schadensersatz- und Auskunftsanspruch[11]. Im zu Grunde liegenden Fall wurde statt einer Sperrung und Löschung dagegen eine Speicherung der Verbindungsdaten gefordert. Einen Anspruch darauf gäbe es nur, wenn man die Speicherung als ein Minus zur Sperrung und Entfernung begriffe oder die Ausnahmepflicht darauf analog ausdehnend und damit die Privilegierungsregelung einschränkend anwenden wollte[12]:

a) Der Anspruch auf Sperrung und Entfernung ist als Unterlassungsanspruch zu verstehen[13]. Demgegenüber sind Auskunfts- und Rechnungslegungsansprüche als Hilfsansprüche zum Schadensersatzanspruch anerkannt[14]. Die Speicherung von Daten stellt mitnichten ein Unterlassen oder einen Unterfall davon dar. Wie die Auskunft, so dient auch die Speicherung der Verfolgung; sie ist also nicht gleichzusetzen mit einer Sperrung, die im Sinne einer Unterlassung der Zugangsgewährung

auf Verhinderung abzielt[15]. Das Speichern ist damit kein Minus zur Sperrung sondern ein Aliud, das argumentum a maiore ad minus greift nicht[16]. Es wird daher nicht von der Ausnahmeregelung umfasst.

b) Auch ist die Ausnahmeregelung nicht auf dem Wege der Analogie auf die Speicherung anzuwenden. Der Grundsatz ist die Nichtverantwortlichkeit. Die Ausnahme davon, nämlich die Pflicht zur Sperrung und Entfernung bei Kenntnis nach allgemeinen Grundsätzen, ist geregelt. Eine analoge Erweiterung von Ausnahmen ist methodisch problematisch und bedarf besonderer teleologischer Prüfung[17]: Der Zweck des Gesetzes war hier die Umsetzung der europarechtlichen Vorgaben. Da die Umsetzung als Vollharmonisierung gedacht ist, sind weder weitere noch engere Regelungen durch die Mitgliedstaaten im nationalen Recht möglich[18]. Die geregelte Ausnahme entspricht Art. 12 der Richtlinie 2000/31/EG. Diese sieht eine grundsätzliche Privilegierung vor. Sie lässt nur in Art. 12IIIdie Ausnahmepflicht, eine Rechtsverletzung abzustellen oder zu verhindern, zu. Weitergehende Ausnahmen gestattet sie nicht. Es besteht damit hier keine (planwidrige) Lücke, die der Ausfüllung bedarf und diese rechtfertigt, denn der Gesetzgeber wollte abschließend regeln und hat abschließend geregelt, argumentum e silentio (legis completae)[19]. Auch aus den weiteren Normen des TDG oder des UrhG - etwa § 101a UrhG - ergibt sich kein andersgearteter Anspruch[20].

c) Demnach schuldete der Accessprovider der Verfügungsklägerin keine Auskunft. Der Unterlassungsanspruch ist in der Tat auf die Sperrpflicht begrenzt[21]. Ein Anspruch auf Speicherung, und dadurch diesen Anspruch durch Anfragen geltend zu machen, besteht nicht.

Bei einem angenommenen Eingriff in den Gewerbebetrieb führt dies jedoch noch nicht zwingend zur Rechtswidrigkeit. In einem weiteren Schritt muss diese auf Grund einer umfassenden Güter- und Interessenabwägung positiv festgestellt werden[22]. Zwar bestand durchaus Veranlassung, den Provider um Speicherung zu bitten. Eine Einzelmail unter Bündelung aller Anfragen statt 167 Einzelfragen am Tag wäre kaum Bedenken ausgesetzt, was das Gericht leider nicht ausdrücklich feststellte. Jedoch bestand kein Anlass, dieses Ansinnen in der berichteten massiven Weise zu verfolgen, insbesondere nicht mit dieser Anzahl an E-Mails. Das Gericht wertete unter Einbeziehung der Zahl der Anfragen und nahm im Ergebnis die Rechtswidrigkeit des Eingriffs an. Dem ist zuzustimmen: Auf Grund der bloßen Quantität von Anfragen, für die kein Rechtsgrund vorliegt, entsteht die Beeinträchtigung des Unternehmens, die es nicht hinzunehmen braucht. Die weiteren Voraussetzungen des Abwehranspruchs waren gegeben. Das Urteil ist daher im Ergebnis zu begrüßen.

III. Ausblick

Für die Urheberrechtsinhaber mag diese Entscheidung bitter sein, sehen sie ihre Rechte in weiten Teilen im Internet

faktisch schutzlos ausgeliefert. Doch der Gesetzgeber hat sich dieses Problems bereits angenommen. Ein direkter Anspruch gegen die Provider ist in Planung und soll kodifiziert werden[23]. Dies soll nicht zuletzt die Staatsanwaltschaften entlasten. Die Provider befürchten schon jetzt enorme Lasten durch die zu erwartenden Anfragen. Für sie ist immerhin eine Aufwandsentschädigung zum Ausgleich vorgesehen, gem. Abs. 2 a.E. Allerdings drohen bei fehlerhaften Auskünften Schadensersatzverpflichtungen. Auf diesem Weg können also erhebliche Kosten auf sie zu kommen.

Die Wissenschaft sieht solchen Änderungen auch in dogmatischer Hinsicht skeptisch entgegen[24]. § 100

des Ref-E des Gesetzes zur Verbesserung der Durchsetzung von Rechten des geistigen Eigentums sieht vor, einen eigenen Auskunftsanspruch bei offensichtlicher Rechtsverletzung auch gegen Accessprovider festzuschreiben. Dieses soll der Umsetzung des Art. 8 der Richtlinie 2004/48/EG zur Durchsetzung der Rechte des geistigen Eigentums dienen[25]. Letztere schreibt jedoch nur einen Auskunftsanspruch bei Rechtsverletzungen gewerblichen Ausmaßes vor. Der Entwurf schränkt dahingehend jedoch nicht ein. Erst seine Begründung greift dies auf, schließt jedoch auch ein gewerbliches Ausmaß bei Verletzungen durch private Endverbraucher nicht aus, es sei denn, eine „gewisse Nachhaltigkeit" sei zu vermissen. Dies dürfte einer Bagatellgrenze im Ergebnis sehr nahe kommen. Wie das gewerbliche Ausmaß schon im Moment des Auskunftsverlangens festgestellt werden soll, ist dabei bei Verwendung dynamischer IP nicht unproblematisch. § 100 IV UrhG Ref-E enthält daneben eine allgemeine festgeschriebene Verhältnismäßigkeitsgrenze, welche früher nur der Gesetzesbegründung entnehmbar war[26].

Da es sich bei den zur Verfügung gestellten Daten um Verkehrsdaten handelt, ist weiter eine vorherige richterliche Anordnung - entsprechend §§ 100g, h StPO notwendig. Die Gesetzesbegründung nimmt sich dieser Frage, die - wie sie richtig erkennt - eine verfassungsrechtliche ist, an[27]. Es wird ausdrücklich auf Auskünfte in Bezug auf dynamisch vergebene IP-Adressen verwiesen. Einige Gerichte verneinten bisher in diesen Fällen das Vorliegen von Verkehrsdaten und damit das Erfordernis eines richterlichen Beschlusses[28]. Nach richtiger Auffassung erstreckt sich jedoch die Auskunft in ganz typischer Weise auf Verbindungsdaten. Ein richterlicher Beschluss ist damit vonnöten. Eine Klarstellung dessen im Gesetz und nicht erst eine zurückhaltende Erwähnung in der Begründung wäre wünschenswert. Rechtsunsicherheit geht hier auch zu Lasten der Provider, denen schließlich bei fehlerhaft verweigerter Auskunft ein Schadensersatzanspruch droht. Um sie nicht daneben bei fehlerhaft erteilter Auskunft wegen Verletzung des Telekommunikationsgeheimnisses zivilrechtlich belangbar zu machen, werden die Provider in Abs. 5 des Entwurfs von der Haftung weitgehend freigestellt. Wie weit daneben der strafrechtliche Geheimnisschutz des § 206 StGB zu Gunsten der Provider davon eingeschränkt wird und werden soll, bleibt fraglich.

Wie der verschuldensunabhängige Auskunftsanspruch systematisch-dogmatisch in die Konzeption des TDG einzupassen ist, bleibt ebenso offen. Die Wertung des § 100 UrhG Ref-E setzt sich mit der oben dargelegten des TDG in unaufgelösten Widerspruch. Dabei sollte das TDG die Verantwortlichkeit von Teledienstleistern umfassend für alle Rechtsgebiete regeln[29]. Sein eigenes Ziel droht der Gesetzgeber nun durch Ausnahmeregelungen in anderen Gesetzen zu unterlaufen. Ein weiteres Problem ergibt sich aus dem TKG und der dort verankerten Pflicht zur Löschung von Verbindungsdaten, wie sie erst jüngst das *LG Darmstadt* gem. § 96II 2 TKG hervorhob[30]. Müssen die Daten aber sofort gelöscht werden, dann wären gar keine Daten mehr vorhanden, über die Auskunft erteilt werden könnte. Der Anspruch liefe leer. Ein Rückgriff auf die verdachtsunabhängig gespeicherten Vorratsdaten, wie sie durch die EU derzeit geplant sind, ist schon wegen deren Zweckbindung für die Verfolgung von schweren Straftaten und der Zugriffserlaubnis nur durch Strafverfolgungsbehörden seitens Ziviler nach jetzigem Stand nicht möglich. Eine Aufweichung stieße auf ganz erhebliche verfassungsrechtliche Bedenken. Ein gesonderter vorgeschalteter Anspruch auf Speicherung ist nötig. Eine Reform des § 96II 1 TKG soll dem zwar Abhilfe schaffen. Die Norm zählt bislang nach dem Wortlaut abschließend die Fälle auf, in denen Verbindungsdaten gespeichert werden dürfen. Durch Anfügen von sonstigen Speicherungsmöglichkeiten, die von „durch andere gesetzliche Vorschriften begründeten Zwecken" eröffnet werden würden, entstünde jedoch eine nicht mehr überschaubare Generalklausel, so ist zu befürchten. Ob eine solche pauschale Aufweichung eines solch wichtigen verfassungsrechtlich geschützten Bereiches der richtige Weg ist, darf bezweifelt werden.

Im vorliegenden Urteil zeigt sich ebenso wie in den angeführten Reformbemühungen, dass die Gerichte und der Gesetzgeber von der technischen Entwicklung und von europarechtliehen Vorgaben zugleich getrieben sind. Der Schutz der Urheberrechte im Internet ist ein wichtiges Anliegen. Ein Auskunftsanspruch muss aber zunächst eine ausgewogene Regelung darstellen, die die Stellung der Verletzten, der Zugangsvermittler wie der Verletzer in Einklang bringt. Daneben sind datenschutz-,

telekommunikations- und teledienstrechtliche Implikationen zu beachten. Beides steht noch aus.

---

* Rechtsanwalt und wiss. Angestellter der Universität Tübingen.

1 *OLG Frankfurt a.M.*, GRUR-RR 2005, 147 sowie *OLG Hamburg*, GRUR-RR 2005, 209; ausf. und zusammenf.: *Stadler*, Haftung für Informationen im Internet, 2005, Rdnrn. 141ff.

2 Dazu *Dietrich*, NJW 2006, 809.

3 S. o. Fußn. 1.

4 *KG*, GRUR-RR 2005, 66; *OLG München*, MMR 2004, 324 m.w. Nachw.; kritischer die Literatur - stellvertretend: *Staudinger/Beater*, BGB, 13.Aufl. (1999), § 823 Anh.V Rdnr.55.

5 *Spindler*, in: *Spindler/Schmitz/Geis*, TDG, § 2 Rdnrn. 25f. m.w. Nachw. Eine obergerichtliche Klärung steht aus.

6 Dies dürfte jedenfalls für die Anwendbarkeit des § 9 TDG ganz überwiegende Ansicht sein, vgl. *Spindler* (o. Fußn. 5).

7 So genannte „Filterfunktion" des § 9 TDG, vgl. *Bohne*, GRUR-RR 2005, 145 (146); ausf. *Heß*, Die Verantwortlichkeit von Diensteanbietern für Informationen im Internet nach der Novellierung des Teledienstgesetzes, 2005, S. 35ff.

8 Ausf.: *Heß* (o. Fußn. 7), S. 184ff.

9 *OLG Frankfurt a.M.*, GRUR-RR 2005, 147; - Auskunftsanspruch; *Haug*, Grundwissen Internetrecht, 2005, S. 231ff.

10 *OLG Frankfurt a.M.*, GRUR-RR 2005, 147; *v. Wolff*, in: *Wandtke/Bullinger*, Praxiskomm. z. UrheberR, 2.Aufl. (2006), § 97 Rdnrn. 25ff., Erg. Bd., 2003, § 97 Rdnrn. 24ff.

11 *OLG Frankfurt a.M.*, GRUR-RR 2005, 147; *BGH*, GRUR 2004, 860 (864) - Internet-Versteigerung; GRUR 2002, 618 - Meißner Dekor.

12 So noch das *LG Hamburg*, MMR 2005, 57, aufgehoben durch *OLG Hamburg*, GRUR-RR 2005, 209 = MMR 2005, 453.

13 *Schricker/Wild*, UrheberR, 2. Aufl. (1999), § 97 Rdnr. 46.

14 *Schricker/Wild* (o. Fußn. 13), § 97 Rdnr. 81.

15 Dabei ist beachtlich, dass die Verletzten nicht dazu aufforderten, obwohl es ihr gutes Recht ist, die Verletzungen ihrer Rechte zu unterbinden. Vielmehr kam es ihnen darauf an, Daten für massenhafte zivilrechtliche Schadensersatzansprüche zu erlangen.

16 *Sieber/Höfinger*, MMR 2004, 580; a.A. *Czychowski*, MMR 2004, 514 (516f.) noch zum Auskunftsanspruch.

17 *Larenz*, Methodenlehre der Rechtswissenschaft, 6. Aufl. (1991), S. 370ff., 381ff.; *Canaris*, Die Feststellung von Lücken im Gesetz, 2. Aufl. (1983), S. 189ff.

18 Begr. RegE BT-Dr 14/6098, S. 22.

19 Vgl. *Canaris* (o. Fußn. 17), S. 50ff.

20 *Stadler*, Haftung für Informationen im Internet, 2005, Rdnrn. 141eff.

21 *Nordemann/Dustmann*, CR 2004, 385.

22 *Erman/Schiemann*, BGB, 11. Aufl. (2004), § 823 Rdnr. 49; BGHZ 3, 270 (281) = GRUR 1952, 225 - Constanze.

23 Pressemitteilung des Bundesjustizministeriums v. 12. 12. 2005 - abrufbar unter www.bmj.de - unter ausdrücklicher Bezugnahme auf illegale Tauschbörsen.

24 *Bohne*, GRUR-RR 2005, 145 (146) meint, ein solcher Anspruch wäre „fatal". Instruktiv und umfassend: Die Stellungnahme zu § 101 UrhG-E des Deutschen Forschungsnetzes (DFN) v. 28. 2. 2006, abrufbar unter www.dfn.de.

25 So genannte Enforcement-Richtlinie 2004/48/EG des Europäischen Parlaments und des Rats v. 29. 4. 2004 zur Durchsetzung der Rechte des Geistigen Eigentums (ABlEU Nr. L 195 v. 30. 4. 2004, S.16).

26 Reg-E BT-Dr 14/6098, S. 23.

27 S. 82 des Ref-E Ges. z. Verbesserung der Durchsetzung von Rechten des geistigen Eigentums v. 3. 1. 2006.

28 *LG Ulm*, MMR 2004, 187; *LG Bonn*, DuD 2004, 628 m. Anm. *Köbele* auf S. 609; *Dietrich*, NJW 2006, 809; a.A. *LG Köln*, Beschl. v. 30. 6. 2004 - 111 Qs 124/04; *LG Stuttgart*, NJW 2005, 614 = CR 2005, 598ff. m. Anm. *Gerke*, S. 599; *LG Hamburg*, MMR 2005, 711.

29 *Spindler*, (o. Fußn. 5), Vorb. § 8 Rdnr. 1. Die vom Gesetzgeber gewollte „Filterfunktion" für andere Gesetze - s. RegE BT-Dr 14/6098, S. 23 - würde verloren gehen.

30 *LG Darmstadt*, GRUR-RR 2006, 173 - Löschung der IP-Adressen (in diesem Heft).