- erschienen in Computer und Recht (CR) 2008, 810 -

Die IP-Adresse als Beweismittel im Zivilprozess

Beweiserlangung, Beweiswert und Beweisverbote

Andreas Gietl/Reto Mantz[*]

Rund um die Verwendung von IP-Adressen im Zivilprozess befindet sich derzeit vieles im Fluss. Der Beitrag soll alle relevanten Themengebiete wie die Möglichkeiten der Zuordnung der IP zu den Anschlussinhabern sowie den Beweiswert dieser Zuordnung darstellen. Abschließend wird die Frage von Beweisverwertungsverboten diskutiert.

I. Einleitung

Mit der Einführung des Auskunftsanspruchs nach § 101 UrhG wird sich der „Erstbearbeitungsaufwand“ bei der Ermittlung von Anschlussinhabern von den Staatsanwaltschaften auf die Gerichte verschieben. Dabei ist derzeit noch unklar, wie der Anspruch in der Praxis angewandt werden soll. Selbst nach erfolgter Auskunft dürfte das eigentliche Problem der Gerichte in allen Verfahren meist darin liegen, dass derzeit vollkommen unklar ist, ob die von den Prozessbevollmächtigten der Medienindustrie vorgelegten Beweis- bzw. Glaubhaftmachungsmittel überhaupt ausreichend sind. Zusätzlich wird seitens der Antragssteller bzw. Kläger sehr häufig ungenügend vorgetragen. Die Rechtsverteidiger der Betroffenen wiederum sind in der Pflicht, ihren Mandanten bestmöglich zu vertreten und daher alle Verteidigungsmittel auszuschöpfen. Allerdings befinden sich Rechtsprechung und Literatur zur Problematik der Beweisverwertung derzeit in einem Umbruch – es herrscht Streit über praktisch alle Gesichtspunkte. Eine Entscheidung des BGH steht noch aus. Im Folgenden sollen deshalb die relevanten Fragen für den mit einem solchen Fall befassten Praktiker behandelt werden. Einführend wird untersucht, wann die Daten an wen herausgegeben werden dürfen (II.). Im Anschluss werden die Tauglichkeit der IP-Adresse als Beweismittel (III.), die Beweisführung (IV.) sowie die Problematik der Beweisverwertungsverbote (V.) untersucht.

II. Möglichkeiten zur Ermittlung des der IP-Adresse zugeordneten Nutzers

1. Auskunftsanspruch (§ 101 UrhG)

Bis zur Novelle des UrhG vom 7.7.2008[1] wurde zur Ermittlung der IP-Adresse insbesondere § 101a UrhG a.F. bemüht. Strittig war insbesondere dessen Anwendbarkeit. Die

[*] Jurist (Univ.) Andreas Gietl, wiss. Mitarbeiter am Lehrstuhl Martin Löhnig, Universität Regensburg; RRef. Dr. jur. Reto Mantz, jur. Mitarbeiter bei Heymann & Partner Rechtsanwälte, Frankfurt/M.

wohl h.M. in Rechtsprechung und Literatur ging schließlich von einer Unanwendbarkeit aus, da die geregelten Ansprüche keine Auskunft von unbeteiligten Dritten erlaubten.[2]

Mit der Umsetzung der Enforcement-RL[3] wurde in § 101 UrhG (und den entsprechenden Parallelregelungen in PatG, MarkenG, etc.) der Auskunftsanspruch neu gefasst. Wichtigste Neuerung in diesem Zusammenhang ist die

Möglichkeit, gegen an der Rechtsverletzung unbeteiligte Dritte vorzugehen – also insb. den Access Provider. Auch die Staatsanwaltschaften dürften Anspruchsinhaber nun vermehrt auf die neuen Ansprüche verweisen.[4]

a. Voraussetzungen

Voraussetzung des Anspruchs nach § 101 UrhG gegen einen Dritten sind eine offensichtliche Rechtsverletzung sowie die für eine *im gewerblichen Ausmaß* vorgenommene Rechtsverletzung genutzte Dienstleistung.

aa) Offensichtliche Rechtsverletzung

Von einer offensichtlichen Rechtsverletzung ist auszugehen, wenn die Rechtsverletzung so eindeutig ist, dass eine ungerechtfertigte Belastung des Dritten ausgeschlossen erscheint.[5] Das ist der Fall, wenn eine Fehlentscheidung oder eine andere Beurteilung mit der Folge einer ungerechtfertigten Belastung im Rahmen richterlichen Ermessens kaum möglich ist.[6] In Anbetracht der fehlenden Eindeutigkeit der Beziehung von IP-Adresse zum tatsächlichen Rechtsverletzer ist bereits die Offensichtlichkeit nicht ohne weiteres anzunehmen, sondern bedarf wenigstens näherer Begründung.[7]

bb) Gewerbliches Ausmaß

Problematisch ist insbesondere das Vorliegen des gewerblichen Ausmaßes nach § 101 Abs. 2 UrhG. Um die Gesetzesformulierung wurde bis zuletzt gestritten.[8] Nach der Regierungsbegründung soll die Verletzung bereits in gewerblichem Ausmaß erfolgt sein, wenn ein komplettes Musikalbum oder ein Film durch den Verletzer angeboten bzw.

---

[1] BGBl. I S. 1191.

[2] Statt vieler *Spindler/Dorschel*, CR 2005, 38; *Splittgerber/Klytta*, K&R 2007, 78 jeweils m.w.N.

[3] RL 2004/48/EG, ABl. EG L 157, S. 45.

[4] S.u. II.2.d.

[5] *Raabe*, ZUM 2006, 439, 442.

[6] OLG Düsseldorf v. 4.6.1992 - 2 U 56/92, GRUR 1993, 818, 821 - Mehrfachkleiderbügel; OLG München v. 24.3.2005 - 6 U 4696/04, MMR 2005, 616; *Spindler/Dorschel*, CR 2006, 341, 343.

[7] Vgl. auch OLG Köln, Beschl. v. 21.10.2008 – 6 Wx 2/08, MIR 2008, Dok. 323.

[8] BT-Drs. 16/5048; BR-Drs. 64/1/07, S. 7.

heruntergeladen wurde.[9] Die diesbezüglichen Gerichtsentscheidungen divergieren bereits jetzt. Während das OLG Köln angenommen hat, dass bei einem Album, das gerade erst veröffentlicht wurde, das gewerbliche Ausmaß anzunehmen sei,[10] sieht das LG Frankenthal ein gewerbliches Ausmaß erst bei 3000 Musikstücken oder 200 Filmen als gegeben an.[11] Erst die Festigung der Rechtsprechung wird endgültig Aufschluss über die Auslegung dieses Tatbestandsmerkmals geben können. Im Ergebnis sind nun die Zivilgerichte in einer ähnlichen Situation wie die Staatsanwaltschaften vorher: Sie müssen entscheiden, ob sie die Vielzahl der Anträge mit der für jeden Einzelfall gebotenen Prüfungstiefe behandeln können,[12] oder ob sie im Hinblick auf die Verhältnismäßigkeit nach § 101 Abs. 4 UrhG strengere Maßstäbe anlegen und sich damit eher am Wortlaut „gewerblich" denn an der gesetzgeberischen Begründung orientieren.

Nach § 101 Abs. 1 Satz 2 kann sich das gewerbliche Ausmaß sowohl aus der Anzahl der Rechtsverletzungen sowie aus der Schwere der Rechtsverletzung ergeben. Jedenfalls bei der Verbreitung von kleinen Mengen, wie bei der Großzahl der angeführten Entscheidungen, dürfte ein „gewerbliches" Ausmaß kaum erreicht sein. Es fällt jedenfalls schwer, sich einen Musikladen mit nur einem Produkt vorzustellen.

Allerdings ist für die Rechtsinhaber die Auskunft mittlerweile mit einem gewissen Kostenrisiko verbunden. Für die Auskunft nimmt das LG Köln scheinbar einen Wert von 200 € pro IP-Adresse an.[13] Ob diese Kosten vom Verletzer, der nicht notwendigerweise mit dem Anschlussinhaber übereinstimmen muss, wieder erlangt werden können, liegt demnach im Risiko des Rechtsinhabers. Zudem fallen die Kosten auch an, wenn die Auskunft beim Access Provider ohne Ergebnis bleibt, weil die Daten bereits gelöscht wurden.[14]

cc) Besonderheiten im einstweiligen Rechtsschutz

Das OLG Köln hat kürzlich angenommen, dass das Verfahren nach § 101 UrhG das Gericht nicht zur Anordnung der Auskunftserteilung im einstweiligen Verfahren berechtigt, da darin eine Vorwegnahme der Hauptsache zu sehen sei. Nur die Anordnung der Aufbewahrung der Daten bis zur Durchführung eines ordentlichen Verfahrens sei durch

---

[9] Zur Formulierung der Antragsbegründung *Heymann*, CR 2008, 568, 570.

[10] Geringe Anforderungen OLG Köln, Beschl. v. 21.10.2008 – 6 Wx 2/08, MIR 2008, Dok. 323; LG Köln, Beschl. v. 2.9.2008 – 28 AR 4-08, MIR 2008, Dok. 290; LG Düsseldorf, Beschl. v. 12.09.2008 - 12 O 425/08; LG Nürnberg-Fürth, Beschl. v. 22.09.2008 – 3 O 8013/08; LG Frankfurt, Beschl. v. 18.09.2008 – 2-06 O 534/08, MIR 2008, Dok. 298; LG Oldenburg, Beschl. v. 15.09.2008 – 5 O 2412/08, MIR 2008, Dok. 299 mit der Auffassung, bereits die Nutzung einer Tauschbörse indiziere das gewerbliche Ausmaß, wobei verkannt wird, dass „nicht privat" nicht gleichzusetzen ist mit „gewerblich".

[11] LG Frankenthal, Beschl. v. 15.09.2008 - 6 O 325/08, MIR 2008, Dok. 289; ebenso vorher die Richtlinien der Staatsanwaltschaft Nordrhein-Westfalen, s. http://www.heise.de/newsticker/meldung/113898.

[12] Vgl. auch BT-Drs. 16/5048, S. 38.

[13] LG Köln, Beschl. v. 2.9.2008 – 28 AR 4-08, MIR 2008, Dok. 290; wegen Vorwegnahme der Hauptsache aufgehoben, OLG Köln, Beschl. v. 21.10.2008 – 6 Wx 2/08, MIR 2008, Dok. 323.

[14] Vgl. *Solmecke*, http://www.wb-law.de/news/it-telekommunikationsrecht/603/lg-koeln-rechteinhaber-muessen-pro-ip-adresse-900-e-zahlen.

§ 101 UrhG gedeckt.[15] Diese Anwendung des § 101 Abs. 7 UrhG – wenn auch vom Gesetzgeber vermutlich anders intendiert – dient dem Schutz der Interessen des betroffenen Anschlussinhabers, ist konsequent und in sich logisch. Im ordentlichen Verfahren sind schließlich die Verteidigungsmöglichkeiten des Betroffenen deutlich besser ausgestaltet.

b. Erlaubnistatbestand für Datenherausgabe?

Auch wenn die Tatbestandsvoraussetzungen für die Herausgabe vorliegen, dürfen die Daten nur herausgegeben werden, wenn hierfür ein Erlaubnistatbestand greift.[16] Solche Erlaubnistatbestände könnten § 101 Abs. 9 S. 8, Abs. 10 UrhG oder die Regelungen der Vorratsdatenspeicherungs-RL (VSRL) darstellen.

aa. § 101 UrhG als Erlaubnistatbestand?

Problematisch war dies bis vor kurzem, weil das Verhältnis von Enforcement-RL und TK-Datenschutz-RL insb. bezüglich der Erlaubnistatbestände der Enforcement-RL, unklar war, da nach Art. 8 Abs. 3 lit. e) Enforcement-RL vorherige Regelungen bezüglich des Schutzes der Verarbeitung personenbezogener Daten unangetastet bleiben. Die Auskunftsansprüche der Enforcement-RL schränken somit nicht die Datenschutzvorgaben der Datenschutz-RL[17] und der insofern spezielleren und anwendbaren TK-Datenschutz-RL ein.[18] Verkehrsdaten sind nach den Regelungen der TK-Datenschutz-RL umgehend zu löschen oder zu anonymisieren, sobald sie für die Übertragung nicht mehr benötigt werden, sofern nicht nach Art. 6 TK-Datenschutz-RL die Daten (1) für

die Abrechnung erforderlich sind oder (2) eine Einwilligung des Nutzers zum Zwecke der Vermarktung vorliegt. Diese Erlaubnistatbestände sind abschließend.[19] Auch die Grenzen für weitere, spezialgesetzliche Erlaubnistatbestände legt die TK-Datenschutz-RL in Art. 15 Abs. 1 unmissverständlich fest: nur Einschränkungen, die für die „nationale Sicherheit, (d. h. die Sicherheit des Staates), die Landesverteidigung, die öffentliche Sicherheit sowie die Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten oder des unzulässigen Gebrauchs von elektronischen Kommunikationssystemen in einer demokratischen Gesellschaft notwendig, angemessen und verhältnismäßig“ sind, können zulässig sein.[20]

---

[15] OLG Köln, Beschl. v. 21.10.2008 – 6 Wx 2/08, MIR 2008, Dok. 323.

[16] § 4 Abs. 1 BDSG; für das TKG BeckTKG-Robert, § 91 Rz. 2; für das TMG *Schmitz,* in: Spindler/Schmitz/Geis, TDG, Einf. TDDSG Rz. 20, § 3 TDDSG Rz. 2 ff.

[17] RL 95/46/EG, ABl. EG Nr. L 281 v. 23.11.1995, 31.

[18] *Czychowski*, MMR 2004, 514, 515]; *Spindler/Dorschel*, CR 2006, 341, 345; zur Anwendung der TK-Datenschutz-RL ausführlich *Mantz*, Rechtsfragen offener Netze, 2008, S. 308 f.

[19] *Spindler/Dorschel*, CR 2006, 341, 346; s. insb. Erw.Gr. 30 der TK-Datenschutz-RL

[20] Vgl. dazu EuGH v. 29.1.2008 - C-275/06, GRUR 2008, 241 - *Promusicae/Telefónica.*

Entgegen dieser Prämisse und auch der Auffassung der EuGH-Generalanwältin *Kokott*[21] hat der EuGH allerdings festgestellt, dass weder die TK-Datenschutz-RL noch die europäischen Grundrechte eine Herausgabe der Daten per se verbieten würden.[22] Andererseits sah der EuGH auch keine Verpflichtung der Mitgliedstaaten, einen solchen Auskunftsanspruch einzuführen.[23] Es sei vielmehr Aufgabe der Mitgliedsstaaten, durch eine gesetzliche Grundlage einen verhältnismäßigen Ausgleich der Grundrechtspositionen der Beteiligten zu finden.[24] Diesbezüglich stehe den Mitgliedstaaten ein weiter Spielraum zu.[25] Damit dürfte dieser Streit im Grundsatz zunächst entschieden sein[26] - lediglich im Rahmen der Umsetzung, also des Grundrechtsausgleichs, könnten an einer Regelung noch Zweifel bestehen.

Ob mit § 101 Abs. 9 S. 8 und Abs. 10 UrhG ein ausreichender Erlaubnistatbestand zur Herausgabe von Daten durch Access Provider besteht, darf im Hinblick auf die Gesetzesformulierungen sowie die Gesetzesbegründung bezweifelt werden.[27] Als erstes Gericht hat kürzlich das OLG Köln § 101 Abs. 9 UrhG als Erlaubnistatbestand angesehen.[28] Auch die Instanzgerichte scheinen, ohne dies näher zu begründen, von dieser Einschätzung auszugehen.[29] Ob die Instanzgerichte ähnlich den Staatsanwaltschaften erst bei stark steigender Fallzahl eher zu einer engen Auslegung neigen werden, bleibt abzuwarten.

bb. VSRL und aufgrund VSRL gespeicherte Daten

Keine Erlaubnis zur Herausgabe von Daten nach § 101 UrhG stellen jedenfalls die Regelungen der VSRL dar. Art. 3 i.V.m. Art. 5 VSRL erlauben bzw. erzwingen zwar die Speicherung sowohl der Bestands- als auch der Verkehrsdaten. Damit lässt sich aber noch nicht auf einen europarechtlichen Erlaubnistatbestand zur Herausgabe der Daten an Dritte zum Zwecke der Rechtsverfolgung schließen. Ganz im Gegenteil enthält Art. 1 Abs. 1 VSRL eine strenge Zweckbindung der Daten. Die Herausgabe an private Dritte

---

[21] EuGH, Schlussantrag der Generalanwältin Juliane Kokott v. 18.7.2007, Rs. 275/06 - *Promusicae vs. Telefónica*.

[22] EuGH v. 29.1.2008 - C-275/06, GRUR 2008, 241 Rz. 70 - *Promusicae/Telefónica*; kritisch dazu *Spindler*, GRUR 2008, 574; *Spindler*, ZUM 2008, 640.

[23] EuGH v. 29.1.2008 - C-275/06, GRUR 2008, 241 - *Promusicae/Telefónica*.

[24] Vgl. auch BVerfG v. 24.2.1971 - 1 BvR 435/68, BVerfGE 30, 173, 195 - *Mephisto*; BVerfG v. 17.7.1984 - 1 BvR 816/82, BVerfGE 67, 213, 228; *Duttge*, Der Staat 36 (1997), 281, 292 f.; *Sachs*, in: Sachs, GG, 4. Aufl. 2007, vor. Art. 1 GG Rz. 129; *v. Münch*, in: von Münch/Kunig, GG, 5. Aufl. 2000, vor Art. 1-19 GG Rz. 47.

[25] EuGH v. 29.1.2008 - C-275/06, GRUR 2008, 241 Rz. 68 - *Promusicae/Telefónica*.

[26] *Spindler*, ZUM 2008, 640, 641.

[27] Dazu *Spindler*, ZUM 2008, 640, 645 f. („allenfalls versteckte Befugnisnorm"); *Mantz*, aaO, S. 304 ff.; *Bäcker*, ZUM 2008, 391, 393; *Hoeren*, NJW 2008, 3099, 3100; a.A. OLG Köln, Beschl. v. 21.10.2008 – 6 Wx 2/08, MIR 2008, Dok. 323; *Czychowski/Nordemann*, NJW 2008, 3095, 3097.

[28] OLG Köln, Beschl. v. 21.10.2008 – 6 Wx 2/08, MIR 2008, Dok. 323 unter Verweis auf BT-Drs. 16/5048, 40.

[29] S.o. II.1.a.

ist hiervon nicht gedeckt.[30] Erwägungsgrund 25 der VSRL wiederum lautet: „Diese Richtlinie berührt nicht das Recht der Mitgliedstaaten, Rechtsvorschriften über den Zugang zu und die Nutzung von Daten durch von ihnen benannte nationale Behörden zu erlassen." Im Umkehrschluss daraus ist gerade Privaten gegenüber die Herausgabe nicht erlaubt. In logischer Folge ist auch nach § 113b TKG die Herausgabe der Daten nicht zulässig.[31]

Unabhängig davon ist noch immer ungeklärt, ob die VSRL überhaupt mit europäischem Vertragsrecht und die Umsetzung mit deutschem Verfassungsrecht vereinbar sind.[32] Es lässt sich also festhalten: Zum einen sieht die VSRL selbst keine Herausgabebefugnis vor, zum anderen schränkt sie mit der Zweckbindung bereits die Anwendbarkeit von möglichen Befugnisnormen deutlich ein.

cc. Tatsächliche Trennung der aufgrund VSRL gespeicherten Daten als Beweisproblem?

Das Verbot der Herausgabe von Nutzungsdaten, die aufgrund der Pflicht zur Vorratsdatenspeicherung gespeichert werden, führt zu der Frage, ob aufgrund der §§ 97 ff. TKG zu Abrechnungszwecken gespeicherte Daten einerseits und im Rahmen der Vorratsdatenspeicherung angelegte Daten andererseits tatsächlich voneinander getrennt sind bzw. sich trennen lassen. Denn für Abrechnungszwecke ist die Speicherung erlaubt und daher auch die Verwendung für die Auskunft nach § 101 UrhG. Dies gilt zumindest nach Auffassung des Bundesdatenschutzbeauftragten auch bei sog. Flatrates zumindest für kurze Zeit.[33] Eine Datentrennung bedeutet in diesem Fall im Grunde eine doppelte Speicherung dieser Daten - einmal für die Abrechnung und erneut für die Vorratsdatenspeicherung[34] - ein erhöhter Aufwand, der auf Optimierung bedachten Datenbankdesignern aufstoßen dürfte. Von daher ist es nicht unwahrscheinlich, dass tatsächlich die entsprechenden Daten nur einmal und für beide Zwecke gespeichert werden. Mindestens dürfte aber eine Sperrung der Daten nach Ablauf des erlaubten Zeitraums zur Speicherung für die Abrechnung oder für die Verfolgung von Störungen notwendig sein.[35] Wenn die Daten aber nicht faktisch getrennt werden bzw. Vorkehrungen für die Sperrung getroffen wurden und effektiv Anwendung finden, könnte sich die nach der VSRL vorgesehene klare Zweckbindung der Daten, die die Herausgabe zur privaten Rechtsverfolgung nicht erfasst,[36] in der Form auswirken, dass auch für die Abrech-

---

[30] Ebenso EuGH, Schlussantrag der Generalanwältin Juliane Kokott v. 18.7.2007, Rs. 275/06 - *Promusicae vs. Telefónica*, Rz. 122 ff.; *Kitz*, ZUM 2006, 444, 449; *Spindler*, ZUM 2008, 640, 646; *Splittgerber/Klytta*, K&R 2007, 78, 84; *Hoeren*, NJW 2008, 3099, 3100.

[31] BVerfG v. 11.3.2008 - 1 BvR 256/08, CR 2008, 287; vgl. OLG Frankfurt v. 1.7.2008 - 11 U 52/07, CR 2008, 582 m. Anm *Mantz/Gietl* MMR 2008, 606; LG Frankfurt, Beschl. v. 1.8.2008 - 2-03 O 376/08; *Jenny*, CR 2008, 282, 284; *Spindler*, ZUM 2008, 640, 647.

[32] S. dazu ausführlich *Gietl*, DuD 2008, 317 m.w.N.; VG Berlin, Beschl. v. 17.10.2008 – VG 27 A 232.08.

[33] *Spindler*, ZUM 2008, 640; *Jenny*, CR 2008, 282, 283.

[34] Ebenso *Eckhart*, CR 2007, 409; Hoeren, NJW 2008, 3099, 3101; a.A. wohl *Czychowski/Nordemann*, NJW 2008, 3095, 3097.

[35] *Jenny*, CR 2008, 282, 284.

[36] S.o. II.1.b.bb.

nungsdaten ein Herausgabeverbot besteht. Mit anderen Worten muss sich der speichernde und herausgebende Access Provider fragen lassen, ob er die Daten tatsächlich

technisch getrennt hat. Ist dies nicht der Fall, steht ein Beweisverwertungsverbot im Raum.[37]

2. Akteneinsicht

Vor Einführung des Auskunftsanspruchs in § 101 UrhG am 1.9.2008 gab es nur einen Weg für Private, den Anschlussinhaber hinter einer IP-Adresse herauszufinden. Es wurde zunächst Strafantrag bei der StA gestellt, die daraufhin nach § 113 TKG ein Auskunftsersuchen beim jeweiligen Provider stellte. Nachdem diese den Anschlussinhaber ermittelt hatte, stellte der Rechtsinhaber Antrag auf Akteneinsicht, § 406e StPO. Dieses Verfahren existiert weiterhin neben § 101 UrhG bzw. den entsprechenden Parallelvorschriften.[38] Es steht darüber hinaus bei Ansprüchen, die nicht mit einer Verletzung von Immaterialgüterrechten einhergehen, wie bspw. Betrug beim Online-Shopping, als einzige Methode zur Verfügung.

a. Verhältnis zu § 101 UrhG

Der Anspruch auf Akteneinsicht steht grundsätzlich neben § 101 UrhG. Im Rahmen der Abwägung der Interessen der Beteiligten dürfte jedoch bei urheberrechtlichen Delikten die Möglichkeit des Rechtsinhabers, das Verfahren nach § 101 UrhG zu benutzen, eine Rolle spielen. Sollte die Akte neben der Information des Anschlussinhabers in solchen Fällen keine Information enthalten, ist mangels ausreichenden Verdachts ohnehin die Akteneinsicht unzulässig, und eine Kollision mit § 101 UrhG daher unmöglich. Erhöht sich dagegen das Verdachtsmoment aufgrund weiterer Ermittlungen, haben die Rechtsinhaber ein berechtigtes Interesse an der Teilhabe am vollständigen Akteninhalt. Sie sind in diesem Fall nicht auf § 101 UrhG zu verweisen. Darüber hinaus ist § 113b S. 1 Hs. 2 TKG bisher nicht vom BVerfG suspendiert worden, so dass hier auf die aufgrund § 113a TKG gespeicherten Daten zugegriffen werden kann.

a. Schutz durch das Fernmeldegeheimnis

Soweit davon ausgegangen wird, dass die Ermittlung und Mitteilung des Anschlussinhabers nicht in Art. 10 Abs. 1 GG in Ausprägung des Fernmeldegeheimnisses eingreifen, wird der Informationsgehalt der Auskunft und womöglich der Schutzbereich des Grundrechts verkannt. Das Grundrecht schützt nicht nur den Inhalt elektronischer Kommunikation, sondern auch die näheren Umstände,[39] nämlich ob und wann zwischen zwei Telekommunikationseinrichtungen Verkehr stattgefunden hat. Da dem Rechtsinhaber bekannt ist, wann eine bestimmte Handlung im Internet erfolgt ist, und aufgrund

---

[37] S. u. V.

[38] Siehe unten II.2.d.

[39] BVerfG v. 2.3.2006 - 2 BvR 2099/04, NJW 2006, 976; *Baldus*, in: BeckOK GG, Art. 10 GG, Rz. 8.

der Auskunft eine Zuordnung dieses Telekommunikationsvorgangs zu einem Anschluss stattgefunden hat, ist diese Information als näherer Umstand geschützt. Darüber hinaus gibt die Auskunft auch die Information preis, dass der Anschluss des Inhabers zum fraglichen Zeitpunkt online war. Die Zuordnung ist daher sehr wohl von Art. 10 GG geschützt. Auch handelt es sich um ein Verfahren, das unter Verwendung von Verkehrsdaten erfolgt und daher dem Schutz der §§ 88, 96 TKG unterliegt.[40] § 101 Abs. 10 UrhG ist zudem so formuliert, dass „für die Auskunft nach Abs. 9 […] das Grundrecht des Fernmeldegeheimnisses […] eingeschränkt" wird. Wohlgemerkt heißt es dort nicht, das Grundrecht *kann* eingeschränkt werden, sondern das Grundrecht *wird* durch die Auskunft eingeschränkt.

Die gegensätzliche Auffassung, die Auskunft bezöge sich nur auf Bestandsdaten, da nur diese herausgegeben werden,[41] trennt künstlich den Inhalt der Anfrage ("Wer hatte die IP-Adresse 1.2.3.4 zum Zeitpunkt XX:YY inne?") und die Antwort. Der Vergleich mit der Frage, wem wann eine Telefonnummer zugeordnet war, wie ihn das OLG Zweibrücken anstellt,[42] hinkt daher. Vielmehr bezieht sich die Auskunft hier im Vergleich auf die Frage, wer wann einen bestimmten anderen Teilnehmer angerufen hat. Ein Vorgang, der dem Fernmeldegeheimnis unterliegt.

b. Zugriff über § 113 TKG

Die Zuordnung der IP-Adresse zu einem Anschluss unterliegt also dem Fernmeldegeheimnis, so dass nach § 113 Abs. 1 S. 3 TKG zusätzlich die "hierfür einschlägigen Vorschriften" erfüllt sein müssen. Aufgrund der Rückverweisung in § 96 auf andere gesetzliche Vorschriften ist daher die Frage, ob die Zuordnung nach § 113 TKG erfolgen kann, jedenfalls fragwürdig. Dies ist jedoch aufgrund einer systematischen Auslegung des § 113b, der nicht vom BVerfG suspendiert wurde[43] ohne Richtervorbehalt möglich – unabhängig davon, ob die Daten aufgrund §§ 96 ff. oder § 113a TKG gespeichert wurden.[44]

c. Ermittlungen bei der Nutzung von Tauschbörsen

Dabei ist im Fall der Tauschbörsennutzung zu beachten, dass es sich bei fast allen relevanten urheberrechtlichen Straftaten um Privatklagedelikte nach § 374 Abs. 1 Nr. 8 StPO handelt. Der Staatsanwalt ist daher nach § 377 Abs. 1 Satz 1 StPO nicht zur Mitwirkung verpflichtet. Er ist jedoch verpflichtet zu ermitteln, ob es sich ggf. um ein Offizialdelikt handelt, oder ob ein öffentliches Interesse an der Erhebung der öffentlichen Klage besteht, so dass er weiter ermitteln müsste, § 376 StPO. Zu diesem Zweck können Vorermittlungen nach § 160 StPO durchgeführt werden, die jedoch diesem Zweck zu dienen haben. Als Offizialdelikt verbleibt der § 108 UrhG, der die gewerbsmäßige

---

[40] Eingehend *Mantz*, aaO, S. 304 ff.

[41] LG Offenburg, Beschl. v. 17.4.2008 - 3 Qs 83/07, CR 2008, 592.

[42] OLG Zweibrücken v. 26.09.2008 - Az. 4 W 62/08 , MIR 2008, Dok. 306.

[43] BVerfG v. 11.3.2008 - 1 BvR 256/08 , CR 2008, 287 - Abs. 10; BVerfG v. 28.10.2008 - 1 BvR 256/08, Abs. 85.

[44] Ausführlich dazu LG Offenburg, Beschl. v. 17.4.2008 - 3 Qs 83/07, CR 2008, 592 m. Anm. *Gietl*, ZUM 2008, 622, 623.

Verletzung von Urheberrechten verlangt. Da die Schaffung einer Einnahmequelle[45] bei der Nutzung der verbreiteten Tauschbörsen auszuschließen ist, verbleibt nur noch das öffentliche Interesse an der Verfolgung der Tat als Grund für ein Offizialdelikt. Dabei stellt sich die Frage, inwieweit die Ermittlung des Anschlussinhabers für die Beantwortung

dieser Frage relevant ist. Im Regelfall wird sich die Frage nicht anhand der Person des Anschlussinhabers, sondern anhand der Umstände der Tat beantworten lassen (Umfang der Urheberrechtsverletzung), so dass die Ermittlung des Anschlussinhabers unnötig und damit unzulässig[46] ist.

d. Gewährung der Akteneinsicht nach § 406e StPO

In der Vergangenheit haben die Staatsanwaltschaften den Rechtsinhabern, soweit sie die Anschlussinhaber ermittelt hatten, wohl stets nach § 406e StPO alleine aufgrund deren Verletzteneigenschaft Akteneinsicht gewährt und sich nicht mit der von § 406e StPO eigentlich vorgesehenen Abwägung zwischen berechtigtem Interesse des Verletzen und schutzwürdigem Interesse des Beschuldigten beschäftigt. Die Staatsanwaltschaften haben die Beschuldigten pflichtwidrig nicht nach § 33 StPO[47] angehört, somit hatten die Beschuldigten keine Möglichkeit sich präventiv gegen die Auskunft zu wehren, auch wenn dies auch noch nach Auskunft[48] möglich ist. Dies hat sich mittlerweile geändert, so dass die ersten Entscheidungen publiziert wurden.

aa. Aktuelle Entwicklungen

Das LG München I argumentiert, eine Akteneinsicht dürfe nur nach vorheriger Abwägung der Interessen des Ermittelten und des Rechtsinhabers erfolgen, wie es § 406e Abs. 2 Satz 1 StPO verlangt. Diese Abwägung ergebe jedoch einen Vorrang der schutzwürdigen Interessen des ermittelten Anschlussinhabers. Alleine die Behauptung des Rechtsinhabers, unter der IP-Adresse seien Dateien zum Upload angeboten oder heruntergeladen worden, stelle noch keinen hinreichenden Tatverdacht gegen den Anschlussinhaber dar: Der Anschluss könne auch von Familienmitgliedern oder Dritten per WLAN genutzt worden sein. Eine Anzeige gegen Unbekannt, die mangels Ermittlung eines Beschuldigten eingestellt werde, trage daher keinen Anspruch auf Akteneinsicht.[49] Unabhängig von der strafrechtlichen Verantwortlichkeit sei auch nicht zwingend ein zivilrechtlicher Anspruch aus § 97 UrhG als Verletzer oder Störer gegeben, da eine solche Verantwortlichkeit des Störers jedenfalls zweifelhaft sei. Daher kann die Akteneinsicht

---

[45] BGHSt 1, 383.

[46] *Wache*, in: Karlsruher Kommentar zur StPO, § 160 Rz. 20.

[47] BVerfG v. 15.4.2005 - 2 BvR 465/05, NStZ-RR 2005, 343; LG Stralsund v. 10.1.2005 - 22 Qs 475/04, StraFo 2006, 76; Meyer-Goßner, StPO, 50. Aufl. 2007, § 406e StPO Rz 9.

[48] LG Stralsund o. Fn 48.

[49] LG München I v. 12.3.2008 - 5 Qs 19/08, MMR 2008, 561.

auch nicht der Vorbereitung eines Zivilprozesses dienen.[50] Insofern ist der Anschlussinhaber nicht Verletzer im Sinne des § 406e StPO, so dass ein Auskunftsanspruch aufgrund seines grundrechtlich geschützten Fernmeldegeheimnisses ausscheidet.[51]

Das LG Saarbrücken stützt sich zur Ablehnung der Akteneinsicht auf fehlende Hinweise auf die Verletzteneigenschaft des Antragstellers und bezweifelt so wohl, dass überhaupt eine relevante Tat begangen wurde. Vielmehr ist aber wohl auch hier davon auszugehen, dass dies in Bezug auf den Anschlussinhaber gemeint ist, und gegen ihn kein hinreichender Tatverdacht vorlag. Noch weiter geht das AG Hamburg-Altona in einem stattgebenden Urteil gegen den Rechtsinhaber auf Schadensersatz wegen Verletzung der Persönlichkeitsrechte des Klägers. Darin nimmt es an, dass gegen den Anschlussinhaber nicht einmal ein "hinreichender Anfangsverdacht" vorliege. Dies jedenfalls soweit nicht ermittelt wurde, ob andere den Anschluss mitbenutzen. Ob es einen „hinreichenden Anfangsverdacht" gibt, mag hier dahingestellt bleiben.[52] Ein Anspruch auf Akteneinsicht liege nur vor, wenn gegen den Beschuldigten mehr als ein Anfangsverdacht besteht, nämlich ein hinreichender Verdacht im Sinne des § 203 StPO.[53] § 203 StPO verlangt zur Eröffnung des Verfahrens, „nach vorläufiger Tatbewertung die Wahrscheinlichkeit der Verurteilung in einer Hauptverhandlung mit vollgültigen Beweisen".[54]

bb. Würdigung

Diese Beschränkung wurde für Fälle entwickelt, in denen der Verletzte Einsicht in beim Beschuldigten beschlagnahmte Akten verlangte, um dem Verhältnismäßigkeitsgrundsatz Folge zu tragen und eine Ausforschung des Beschuldigten zu verhindern. Die schutzwürdigen Interessen des Beschuldigten sollen überwiegen, soweit keine gesicherte Tatsachenbasis für die Täterschaft des Beschuldigten spricht. Da dem Verletzten vor der Akteneinsicht gar kein Verletzer bekannt ist, er kennt schließlich IP-Adresse und Zeitpunkt der vermeintlichen Tat, ist diese Auslegung hier vorliegend wohl zu Recht übertragen worden.

Durch die Akteneinsicht soll die Identität des Beklagten für einen späteren Zivilprozess oder für eine Abmahnung ermittelt werden. Weitere Informationen wird die Akte in den Standardfällen mangels Ermittlungstätigkeit der Staatsanwaltschaften nicht enthalten. Dem vermeintlichen Verletzer drohen anschließend eine Abmahnung sowie hohe Schadensersatzforderungen, die er ggf. zivilrechtlich abwehren muss. Aufgrund der ungesicherten Rechtslage im Bereich der Störerhaftung von Anschlussinhabern sowie der vielfältigen Möglichkeiten, aufgrund derer andere als der Anschlussinhaber die Tat begangen haben können, besteht ein solcher Anspruch jedoch nicht zwingend. Darüber hinaus greift die Auskunft in das Fernmeldegeheimnis des vermeintlichen Verletzers ein.[55] Die Abwehr dieser Forderungen, ist womöglich mit hohen Kosten verbunden, so

---

[50] Fn. 53.

[51] *Hilger*, in: SK-StPO § 406e Rz. 9.

[52] *Gramse*, NZV 2002, 17.

[53] LG Köln v. 29.6.2004 - 37/04 - 116 Js 192/03, 106 - 37/04, StraFo 2005, 78; LG Staade v. 12.03.2008 - Az.: 5 Qs 19/08, StV 2001, 159.

[54] Vgl. BGHSt 23, 304, 306 = NJW 1970, 1544.

[55] *Spindler*, ZUM 2008, 640, 645; a.A. *Sankol*, K & R 2008, 509, 512.

dass eine Abwägung ergibt, dass der vermeintliche Verletzer, jedenfalls soweit er ohne weitere Ermittlungen nur anhand der IP-Adresse identifiziert ist, als schutzwürdig erscheint.[56] Erhärtet sich der Verdacht hingegen, so dass man von einem hinreichenden Tatverdacht sprechen kann, ist die Auskunft gerechtfertigt. Soweit die Staatsanwaltschaft das Verfahren nach § 170 Abs. 2 StPO einstellen will, muss auch die Unschuldsvermutung mit in die Abwägung mit einbezogen werden, so dass es nicht gerechtfertigt erscheint, die Identität des Beschuldigten dem Verletzten zu offenbaren, wenn eine Einstellung zu erwarten ist.[57]

III. Beweis"wert" der IP-Adresse

Ist die IP-Adresse des potentiellen Verletzers ermittelt, und wird ein Straf- oder Zivilverfahren angestrengt, müssen die jeweiligen Verantwortlichen klären, welchen Beweiswert sie der IP-Adresse zuweisen. Dies hat gravierende Konsequenzen für das weitere Vorgehen und für die Erfolgsaussichten des Rechtsinhabers.

Die IP-Adresse selbst beweist letztlich nichts. Sie stellt für sich gesehen einzig und allein eine Adresse dar. Auch die Zuordnung einer IP-Adresse inklusive einem behaupteten Nutzungszeitpunkt zu einem bestimmten Anschluss belegt nur die Tatsache, dass der Anschluss zum fraglichen Zeitpunkt online war.[58] Aber schon hier bestehen aufgrund der Schnelligkeit und Häufigkeit, mit der die IP-Adressen anderen Teilnehmern zugewiesen werden,

bereits Probleme, wenn etwa die Uhrzeit desjenigen, der festgestellt haben will, wer zu einem bestimmten Zeitpunkt unter einer gewissen IP-Adresse online war, und die Uhr des Providers voneinander abweichen. Eine Sekunde kann hier bereits dazu führen, dass der falsche Anschluss ermittelt wird. Notwendig ist demzufolge, dass sowohl die Zeitangaben der Messprogramme als auch die Zeitangaben beim Auskunft gebenden Access Provider richtig sind bzw. die Abweichungen von der korrekten Zeit festgestellt und protokolliert werden und z.B. durch Prüfprotokolle und Aussage eines vereidigten Sachverständigen überprüfbar sind.[59]

Darüber hinaus beweist die IP-Adresse selbst lediglich die Zuordnung zu einem bestimmten Anschluss und lässt selbst keinerlei Schlüsse darauf zu, ob der Anschlussinhaber selbst oder jemand Anderes (berechtigt oder unberechtigt) den Anschluss zum

---

[56] *Sankol*, K & R 2008, 509, 513.

[57] OLG Koblenz v. 9.3.1990 - 2 VAs 25/89, NStZ 1990, 604.

[58] LG Saarbrücken v. 8.1.2008 - 5 (3) Qs 349/07, MMR 2008, 562; sehr informativ: *Piatek/Kohno/Krishnamurthy*, Challenges and Directions for Monitoring P2P File Sharing Networks - or- Why My Printer Received a DMCA Takedown Notice, http://dmca.cs.washington.edu/uwcse_dmca_tr.pdf.

[59] *Grosskopf*, CR 2007, 122, 123; ähnlich *Dietrich*, NJW 2006, 809, 811.

fraglichen Zeitpunkt benutzt hat.[60] Auch kann keine Aussage darüber getroffen werden, wie viele Personen den Anschluss ggf. benutzt haben.[61]

Dementsprechend sind die notwendigen Beweise anzutreten bzw. die Tatsachen streitig zu stellen.

IV. Beweisführung mit IP-Adressen im Zivilprozess

Sind die vorgenannten Hürden übersprungen, besteht als weitere Problematik, einen bestimmten Vorgang im Internet, also bspw. einen Upload oder Download so zu dokumentieren, dass die Zuordnung beweisfest erfolgen kann. Mit anderen Worten: Der geringe Beweiswert der IP-Adresse an sich zieht strenge Anforderungen an den Vollbeweis durch den Anspruchsteller und ebenso vielfältige Verteidigungsstrategien für den Anspruchsgegner nach sich.

1. Beweisführung und Verteidigungsmittel

Zu Zeiten, als noch nicht zehntausende Strafanzeigen gestellt wurden, führten die Staatsanwaltschaften nicht nur eine Abfrage von Nutzerdaten bei den Providern durch. Häufig wurde zusätzlich der Betroffene vernommen und teilweise sogar seine Computeranlage beschlagnahmt. Dies hatte zur Folge, dass das Gericht die Beweiskette (meist mit Hilfe von Sachverständigen) selbst nachvollziehen und überprüfen konnte: Es ließ sich zum einen überprüfen, ob der Betroffene die streitgegenständliche Datei auf seinem Rechner gespeichert hatte. Zum anderen konnte ihm eine eventuell getätigte Aussage vorgehalten werden. Ein Großteil der jetzigen Probleme wurde dadurch vermieden. Auch in zivilprozessualer Hinsicht entspricht dies dem üblichen Verfahren. Bei der derzeitigen mehr als dürftigen Beweislage, die das Gericht regelmäßig vorfindet, lässt sich – unabhängig von einem Beweisverwertungsverbot – kaum noch auf solider Grundlage eine Verurteilung begründen. Schon substantiiert vorgetragene Schutzbehauptungen führen in der Regel dazu, dass Zweifel an der Beweiskette aufkommen müssen, die sich im Hinblick auf den erforderlichen Vollbeweis – mangels gesicherter Beweismittel – kaum rechtsmittelfest umschiffen lassen. Anders ist dies möglicherweise im einstweiligen Verfügungsverfahren, da hier bereits die Glaubhaftmachung ausreicht.[62] Zudem gilt im Auskunftsverfahren mit Richtervorbehalt der Amtsermittlungsgrundsatz nach § 101 Abs. 9 S. 4 UrhG i.V.m. § 12 FGG, so dass in diesem vorgeschalteten Verfahren nur eine Darlegungslast besteht.[63] Dementsprechend ist dem Rechtsinhaber zu raten, Beweismittel möglichst umfangreich zu sichern, dem verteidigenden Anwalt, jedes Glied der Beweiskette substantiiert zu bestreiten. Die Weiterverfolgung der Verteidigung in der Hauptsache verspricht auf jeden Fall Erfolg, wenn im einstweiligen Verfahren lediglich aufgrund des niedrigeren Beweismaßes ein Beschluss erreicht wurde.[64]

---

[60] *Solmecke*, MMR 2006, Heft 7, XIII.

[61] Vgl. *Sankol*, K&R 2008, 509, 512.

[62] *Reichold*, in: Thomas/Putzo, ZPO, 29. Aufl. 2008, § 936 Rz. 2; *Schultz*, MIR 2008, Dok. 102, Rz. 8.

[63] *Bumiller/Winkler*, in: FG, 8. Aufl. 2008, § 12 Rz. 3 f.; s. auch *Czychowski*, GRUR-RR 2008, 265, 268.

[64] *Schultz*, MIR 2008, Dok. 102, Rz. 8.

Einen weiteren Einwand liefern in diesem Zusammenhang „Abmahnbilder-Generatoren“. Dabei handelt es sich um kleine Programme, mit denen sich ein Bildschirmausdruck eines Filesharingprogrammes erstellen lässt.[65] Unter Angabe von Name und gewünschter IP-Adresse kann damit also ein ebensolcher Bildschirmausdruck erstellt und dem Rechtsinhaber entgegengehalten werden - dadurch wird der Beweiswert von Bildschirmausdrucken weiter in Frage gestellt. Die Lücke kann im Grunde nur über eine Zeugenaussage geschlossen werden. Der Zeuge muss sich aber aufgrund der tausendfachen Durchführung solcher Verfahren möglicherweise Erinnerungsschwierigkeiten vorhalten lassen.[66]

2. Hashing und Beweisführung

Schließlich ist noch ein weiterer Aspekt der Beweisführung zu beleuchten: Bei der Vorlage von Ausdrucken aus Filesharing-Programmen muss der Rechtsinhaber nachweisen, dass es sich überhaupt um ein Werk handelt, für das er die Rechte hat. Dies kann er in aller Regel abstrakt für ein Werk, indem er entsprechende Urkunden oder Vollmachten vorlegt. Damit ist aber noch nicht der Beweis geführt, dass die angeblich heruntergeladene Datei auch tatsächlich ein Vervielfältigungsstück seines Werks ist. Um diesen Zusammenhang zu belegen, führt der Kläger bzw. Antragsteller in aller Regel den Hash-Wert einer Datei an. Ein Hash-Wert ist ein aus einer Datenmenge berechneter Wert, der diese eindeutig (zumindest mit sehr hoher Wahrscheinlichkeit) identifiziert. Wenn auf den Ausdrucken aus dem Filesharing-Programm also ein Hash-Wert angegeben ist, dann muss der Rechtsinhaber im einstweiligen Verfügungsverfahren glaubhaft machen, und im Hauptsacheverfahren bei qualifiziertem Bestreiten durch den potentiellen Verletzer beweisen, dass dieser angezeigte Hash-Wert eine solche urheberrechtlich geschützte Datei eindeutig identifiziert. Er muss also nicht nur den Ausdruck, sondern zusätzlich (1) die Datei und (2) das Verfahren, mittels dessen der Hash-Wert berechnet wurde, sowie erläuternde Dokumente und evtl. Programme vorlegen.[67] Der Richter kann dann anhand dieser Datei und des Verfahrens wenigstens die Dateiidentität überprüfen. Schließt der Rechtsinhaber diese Kette nicht, und sind die Tatsachen streitig gestellt, ist der Beweis nicht geführt.[68]

V. Beweisverwertungsverbote im Zivilrechtsprozess

Schlussendlich könnte die Beweisführung bereits dadurch fruchtlos sein, dass schon beim ersten Glied (Zuordnung der IP-Adresse zum Anschlussinhaber) in der Beweisket-

---

[65] S. nur beispielhaft http://www.piratbyran.org/bevismaskinen.

[66] Zur Fehlerträchtigkeit vgl. LG Stuttgart v. 11.7.2007 - 17 O 243/08, CR 2008, 259; dazu *König*, ITRB 2008, 105.

[67] Hierfür gibt es mehrere Verfahren, am gebräuchlichsten ist MD5 (RFC 1312), http://tools.ietf.org/html/rfc1321.

[68] LG Hamburg v. 14.3.2008 - 308 O 76/07, CR 2008, 401 m. Anm. *Stücke*; *Schultz*, MIR 2008, Dok. 102, Rz. 5 ff.; *Intveen*, ITRB 2008, 124, 125; vgl. auch *Sankol*, K&R 2008, 509, 512.

te ein Beweisverwertungsverbot greift. Kann diese Zuordnung nicht anderweitig erfolgen, wäre der Beweis vollständig abgeschnitten, und der Klägerantrag nach Bestreiten durch den Beklagten, abzuweisen.

1. Grundsätze

Die Frage eines Beweisverwertungsverbots ist von jeher im Zivilprozess umstritten. Teilweise wird vertreten, die Verwertung von rechtswidrig erlangten Beweisen sei weitgehend zuzulassen, wenn sich der Beweisbelastete in Beweisnot befindet und es sich um keine Bagatelle handelt und es sei keine Abwägung vorzunehmen.[69] Soweit andere Autoren dagegen materiell-rechtlich argumentieren[70], ist zu beachten, dass der Anspruch auf Schadensersatz (falls vorhanden) nach §§ 249 ff. BGB auf Naturalrestitution gerichtet ist. Bei der Berechnung bzw. Bestimmung des Inhalts des Schadensersatzanspruchs ist daher im Rahmen der Differenzhypothese auch der womöglich aufgrund der rechtswidrig erlangten Beweise verlorene Prozess einzubeziehen. Der Unterlegene ist vom Beweisbelasteten so zu stellen, als hätte dieser das Beweismittel nie erlangt - und damit ist auch der Prozessverlust auszugleichen. Teilweise wird dagegen die Frage, ob ein Beweisverwertungsverbot besteht, am Schutzzweck der verletzten Norm gemessen.[71] Soweit die Beweiserhebung also auf einem Verstoß gegen Datenschutzvorschriften beruht, die ein Verbot der Verwendung der Daten vorsehen, ist ein Beweisverbot die einzig adäquate Sanktion. Nur so kann der ursprüngliche Schutzweck, nämlich die der Datenschutzvorschrift zugrundeliegende Zweckbindung erreicht werden. Eine andere, wohl derzeit vorherrschende Strömung in Rechtsprechung und Literatur scheint die Frage anhand einer am Schutzzweck der verletzten Norm oder des verletzten Grundrechts (meist des allgemeinen Persönlichkeitsrechts) orientierten Abwägung lösen zu wollen.[72] Soweit der Beweis jedoch aufgrund einer Verletzung des Art. 10 GG erlangt wurde, ist eine solche Abwägung bisher nicht erkennbar, vielmehr ist hier ein Verwertungsverbot die einzig adäquate und vorgeschlagene Konsequenz.[73] Denn eine Verletzung des Wesensgehalts eines Grundrechts führt immer zur Unverwertbarkeit. Art. 10 Abs. 1 GG besitzt im Gegensatz zu Art. 2 Abs. 1 iVm Art. 1 Abs. 1 GG aber wesentlich klarere Konturen, so dass hier nicht von zwischen Rand- und Kernbereich unterschieden werden kann, auch verlangt die Verletzung des Fernmeldegeheimnisses im Gegensatz zum Persönlichkeitsrecht als Rahmenrecht keine Abwägung. Eine Verletzung von Art. 10 Abs. 1 GG trifft daher immer im Kern, so dass ein Verwertungsverbot anzunehmen ist.

---

[69] *H. Roth*, in: Erichsen/Kollhosser/Welp, Recht der Persönlichkeit, S. 279, 294 f.

[70] So *Reichenbach*, § 1004 BGB als Grundlage von Beweisverboten, 2004, S. 130ff.

[71] *Leipold*, in: Stein/Jonas, ZPO, § 284 Rz. 88; OLG Köln v. 5.7.2005 - 24 U 12/05, NJW 2005, 2997, 2999; OLG Karlsruhe v- 8.11.2001 - 12 U 180/01, NJW 2002, 2799, 2800.

[72] Wohl in Bezug auf BVerfG v. 9.10.2002 - 1 BvR 1611/96, 1 BvR 805/98, NJW 2002, 3619, 3624: *Schwab*, FS Hubmann, 421, 431; *Baumgärtel*, FS Klug, 477, 484;; BGH v. 24.11.1981 - VI ZR 164/79, NJW 1982, 277.

[73] OLG Stuttgart v. 1.8.2002 - 2 U 47/01, NJW-RR 2003, 1273, 1277; Zillmer, NJW 1965, 2094 f.; Zillmer, ZZP 1983, 306, 333; *Leipold*, in: Stein/Jonas, ZPO, § 284 Rz. 59.

2. Aktuelle Entwicklungen

Von dementsprechend zentraler Bedeutung für die Annahme eines Beweisverbots ist daher die Frage, ob die Zuordnung einer IP-Adresse zu einem Anschluss einen Eingriff in das Fernmeldegeheimnis des Art. 10 GG darstellt.[74] Alle Gerichte, die sich mit der Frage des Verbots beschäftigt haben, nehmen ein solches an, wenn sie von einem Schutz durch Art. 10 GG ausgehen.[75] Wenn nicht, lehnen sie durchgehend ein solches ab.[76]

Soweit daher die Zuordnung eines Anschlussinhabers zu einem Vorgang im Internet aufgrund informell erlangter Auskünfte von Access Providern erfolgt ist, ist eine Verwertung durch das Zivilgericht verboten. Es stellt sich insoweit die Frage, ob dem Beweisbelasteten auch die rechtswidrige Anwendung von § 113 TKG und § 406e StPO durch die Staatsanwaltschaft zuzurechnen ist und auch diesen Beweisen die Verwertbarkeit zu versagen ist. Dafür spricht, dass es für den Prozessgegner keinen Unterschied macht, wie der Beweisbelastete die Information erlangt. Soweit der Beweisbelastete einen Antrag auf Akteneinsicht nach § 406e StPO gestellt hat, ist ihm aufgrund dieses Antrags die rechtswidrige Auskunft der StA jedenfalls zuzurechnen. Sollte die Auskunft rechtmäßig erfolgt sein, und im Vorfeld die StA die Auskunft rechtswidrig erlangt haben, spricht ebenfalls die Verhinderung weiterer rechtswidriger Grundrechtseingriffe in Art. 10 Abs. 1 GG durch das Gericht für ein solches Beweisverwertungsverbot.[77]

Die Rechtskraft des Urteils im Verfahren nach § 101 UrhG erstreckt sich nicht auf den angeblichen Verletzer und ist daher für die Frage, ob ein Beweisverbot im Prozess zwischen Antragsteller und Anschlussinhaber besteht, irrelevant. Sollte sich die Auskunft als rechtswidrig herausstellen, ist jedoch auch sie unter Verletzung des Fernmeldegeheimnisses zustande gekommen und daher nach oben genannten Grundsätzen unverwertbar. Womöglich unterbricht die erhöhte Richtigkeitsgewähr einer richterlichen Entscheidung hier die Zurechnung. Dies dürfte jedoch keinesfalls bei Entscheidungen im einstweiligen Rechtsschutz anzunehmen sein, wo dem Beweisbelasteten bekannt ist, dass eine allenfalls kursorische Prüfung des Anspruchs stattgefunden hat, und er darüber hinaus aufgrund § 945 ZPO einer verschuldensunabhängigen Risikohaftung unterliegt. Die Zurechnung könnte daher allenfalls eine rechtskräftige Hauptsacheentscheidung erlangen.

VI. Fazit

Die bisherige Praxis der Beweisführung mit IP-Adressen im Zivilprozess wird sich grundlegend ändern. Dies gilt schon aufgrund des Anspruchs aus § 101 UrhG, aber auch wegen einer zu erwartenden und rechtlich verpflichtenden restriktiven Handhabung der

---

[74] Siehe oben II.2.a.aa.

[75] LG Frankenthal v. 21.05.2008 - 6 O 156/0, CR 2008, 666; LG Frankfurt, Beschl. v. 1.8.2008 - 2-03 O 376/08.

[76] OLG Zweibrücken, MIR 2008, Dok. 306; LG Hamburg v. 15.7.2008 - 310 O 144/08, MMR 2008, 685, 686 ohne auf die Frage des Art. 10 GG einzugehen; LG Düsseldorf v. 16.07.2008 - 12 O 232/08, das jedoch nicht auf die Frage des § 406e StPO abstellt, sondern auf eine fehlende Ausspähung des PCs durch den Antragssteller.

[77] So pauschal *Leipold*, in: Stein/Jonas, ZPO, § 284 ZPO Rz. 89.

Akteneinsicht für Verletzte nach § 406e StPO. Aufgrund der Verletzung des Fernmeldegeheimnisses durch jede Auskunft bzgl. des Anschlussinhabers zieht eine rechtswidrige Auskunft im Zivilprozess ein Beweisverwertungsverbot nach sich.