IRIS plus

2013-6

Sind personenbezogene Daten wirklich privat?

LEITBEITRAG

Das Urheberrecht und der Schutz personenbezogener Daten

Intermediäre im Spannungsfeld zweier Rechtsgebiete

- Rechtsgrundlagen auf europäischer Ebene
- Konkret auftretende Konfliktfelder

BERICHTERSTATTUNG

Jüngste geltende Rechtsprechung

- Deutschland
- Finnland
- Frankreich
- Vereinigtes Königreich
- Niederlande
- Russische Föderation

ZOOM

Der Patriot Act und der Vierte Verfassungszusatz

Wie die amerikanische Regierung insgeheim ihre Befugnisse zur Sammlung persönlicher Daten ihrer Bürger ausweitet

OBSERVATOIRE EUROPÉEN DE L'AUDIOVISUEL
EUROPEAN AUDIOVISUAL OBSERVATORY
EUROPÄISCHE AUDIOVISUELLE INFORMATIONSSTELLE

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

IRIS *plus* 2013-6
Sind personenbezogene Daten wirklich privat?

ISBN (Druckausgabe): 978-92-871-7792-6
Preis: EUR 25,50
ISBN (PDF-elektronische Ausgabe): 978-92-871-7795-7
Preis: EUR 34,50
Europäische Audiovisuelle Informationsstelle, Straßburg 2013

IRIS *plus* Publikationsreihe 2013
ISSN (Druckausgabe): 2078-9467
Preis: EUR 100
ISSN (PDF-elektronische Ausgabe): 2079-1089
Preis: EUR 130

Verlagsleitung:
Dr. Susanne Nikoltchev, Geschäftsführende Direktorin der Europäischen Audiovisuellen Informationsstelle
E-mail: susanne.nikoltchev@coe.int

Wissenschaftliche Betreuung und Koordination:
Dr. Susanne Nikoltchev, LL.M. (Florenz/Italien, Ann Arbor/MI)

Verlagsassistentin:
Michelle Ganter
E-mail: michelle.ganter@coe.int

Marketing:
Markus Booms
E-mail: markus.booms@coe.int

Satz:
Pointillés, Hoenheim (Frankreich)

Druck:
Pointillés, Hoenheim (Frankreich)
Europarat, Straßburg (Frankreich)

Umschlaggestaltung:
Acom Europe, Paris (Frankreich)

Herausgeber:
Europäische Audiovisuelle Informationsstelle
76 Allée de la Robertsau
F-67000 Strasbourg
Tel.: +33 (0)3 90 21 60 00
Fax: +33 (0)3 90 21 60 19
E-mail: obs@obs.coe.int
www.obs.coe.int

OBSERVATOIRE EUROPÉEN DE L'AUDIOVISUEL
EUROPEAN AUDIOVISUAL OBSERVATORY
EUROPÄISCHE AUDIOVISUELLE INFORMATIONSSTELLE

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

Beitragende Partnerorganisationen:

Institut für Europäisches Medienrecht (EMR)
Franz-Mai-Straße 6
D-66121 Saarbrücken
Tel.: +49 (0) 681 99 275 11
Fax: +49 (0) 681 99 275 12
E-mail: emr@emr-sb.de
www.emr-sb.de

Institut für Informationsrecht (IViR)
Kloveniersburgwal 48
NL-1012 CX Amsterdam
Tel.: +31 (0) 20 525 34 06
Fax: +31 (0) 20 525 30 33
E-mail: website@ivir.nl
www.ivir.nl

Moskauer Zentrum für Medienrecht und Medienpolitik
Moscow State University
ul. Mokhovaya, 9 - Room 338
125009 Moscow
Russische Föderation
Tel.: +7 495 629 3804
Fax: +7 495 629 3804
www.medialaw.ru

Bitte zitieren Sie diese Publikation wie folgt:
IRIS *plus* 2013-6, Sind personenbezogene Daten wirklich privat?,
Susanne Nikoltchev (Herg.) Europäische Audiovisuelle Informationsstelle, Straßburg 2013

Sind personenbezogene Daten wirklich privat?

Vorwort

2010 erklärte Mark Zuckerberg, Mitbegründer und CEO von Facebook, „Menschen haben sich mittlerweile daran gewöhnt, nicht nur mehr und unterschiedliche Informationen auszutauschen, sondern dies auch offener und mit mehr Menschen zu tun. Diese soziale Norm hat sich einfach mit der Zeit entwickelt." Seit es das Internet gibt, scheint sich in der Tat vieles geändert zu haben, insbesondere die Art und Weise, wie wir Informationen öffentlich zur Verfügung stellen. Es sind neue Erwartungen entstanden, was für jeden von uns frei verfügbar sein sollte. Und manche sind der Ansicht, diese Änderungen sollten sich auch in der Gesetzgebung widerspiegeln.

Die Gesetzgebung folgt gesellschaftlichen Entwicklungen natürlich immer mit einer gewissen Verzögerung und hält so häufig mit weit verbreiteten Einstellungen und Verhaltensweisen scheinbar nicht mehr Schritt. Bedeutet das aber, dass Gesetzgebung sich immer sozialen Normen anpassen sollte? Während Letztere in der Regel die vorherrschende Sichtweise abbilden, resultieren Gesetze aus einem Balanceakt, bei dem unterschiedliche Rechte und Interessen, unter anderem auch die von Minderheiten, bedacht und gegeneinander abgewogen werden müssen. Und wer entscheidet überhaupt, was eine soziale Norm ist? Sicherlich nicht allein Mark Zuckerberg...

Allgemein gefasst bedeutet die Privatsphäre das Recht eines Menschen, bestimmte personenbezogene Informationen nicht öffentlich zu machen. Ob sich dieses Recht in einem Online-Umfeld durchsetzen lässt, beschäftigt viele Menschen, und nicht nur Facebook-Nutzer. Jede Nutzer hinterlässt bei seinen Internetaktivitäten eine Spur „digitaler Krümel", die Hinweise auf seine Lebensweise geben. Diese Informationen können von Dritten gesammelt und in vielerlei Weise gewinnbringend genutzt werden. In manchen Fällen wurden die Informationen vom Nutzer bewusst, in anderen vielleicht unbeabsichtigt herausgegeben. Manchmal verlangen jedoch Dritte Einblicke in das Leben eines Nutzers, die über das hinausgehen, was für den Nutzer noch hinnehmbar ist. Zwei entsprechende Beispiele haben kürzlich besondere Aufmerksamkeit erregt. Im ersten Beispiel geht es um Rechteinhaber, die die Identität und den Aufenthaltsort Internetnutzer herausfinden möchten, um sie wegen Urheberrechtsverletzungen zu belangen. Im zweiten geht es um die Abhöraktivitäten, mit denen nationale Geheimdienste ihre Bürger vor terroristischen und sonstigen kriminellen Aktivitäten zu schützen suchen. Wenngleich in beiden Fällen weitreichende Daten benötigt werden, heißt es doch nicht, dass auch ein rechtlicher Anspruch auf deren Erhebung besteht.

Diese IRIS *plus*-Ausgabe analysiert die Grenzen der Privatsphäre und ihren Stellenwert im Vergleich zu anderen Grundrechten. Der Leitbeitrag untersucht das einigermaßen angespannte Verhältnis zwischen Urheberrecht und dem Schutz personenbezogener Daten. Der Abschnitt Berichterstattung stellt jüngste geltende Rechtsprechung zu den Fragen vor, die im Leitbeitrag angesprochen werden. Im Abschnitt Zoom geht es um den aktuellen Skandal, der durch die Presseveröffentlichung zugespielter Dokumente über die geheimen Überwachungsprogramme von US-Geheimdiensten ausgelöst wurde.

Straßburg, November 2013

Susanne Nikoltchev
Geschäftsführende Direktorin
Europäische Audiovisuelle Informationsstelle

INHALTSVERZEICHNIS

LEITBEITRAG

BERICHTERSTATTUNG

ZOOM

IRIS plus
2013-6 p.7

Das Urheberrecht und der Schutz personenbezogener Daten

Intermediäre im Spannungsfeld zweier Rechtsgebiete

Dr. Martin Rupp und Mag. Peter Matzneller, LL.M. Eur.,
Institut für Europäisches Medienrecht e.V. (EMR), Saarbrücken/Brüssel

I. Einleitung

Das Urheberrecht und der Datenschutz stehen zueinander in einem Spannungsverhältnis. Das liegt im Wesentlichen daran, dass beiden Rechtsinstituten eine potentiell widerstreitende Idee zugrunde liegt. Es besteht ein Zielkonflikt zwischen dem Urheber- und dem Datenschutzrecht. Dabei offenbart sich dieser Konflikt bei einer Gegenüberstellung der jeweiligen gesetzgeberischen Intention keineswegs sofort.

Das *Urheberrecht* schützt in ideeller, vor allem aber auch in materieller Hinsicht das geistige Eigentum des Urhebers. Durch die Bestimmungen zu Inhalt, Umfang, Übertragbarkeit, zu den Folgen einer Verletzung und zur Durchsetzbarkeit urheberrechtlicher Ansprüche soll der Urheber in die Lage versetzt werden, sein Werk wirtschaftlich zu verwerten.

Das *Datenschutzrecht* hingegen soll dem Einzelnen die Möglichkeit gewähren, grundsätzlich selbst über die Preisgabe und Verwendung der ihn betreffenden persönlichen Informationen zu bestimmen.

Es leuchtet nicht unmittelbar ein, inwiefern eine „friedliche Koexistenz" beider Rechtsinstitute problematisch sein sollte. Ein Zielkonflikt entsteht jedoch spätestens dann, wenn ein Rechteinhaber einer Verletzung seiner Urheberrechte nachgehen will. In diesem Fall wird der Rechteinhaber an der Durchsetzung seiner urheberrechtlichen Ansprüche gegen den Verletzer interessiert sein. Diese mögen auf Unterlassung, Schadensersatz, Vernichtung oder sonstiges abzielen. Um diese Ansprüche geltend zu machen, muss der Rechteinhaber den Verletzer zunächst identifizieren. Zum Zwecke dieser Identifikation stattet das Urheberrecht den Rechteinhaber mit besonderen Auskunftsrechten – auch gegen Dritte – aus.

Genau an dieser Stelle geraten das Datenschutzrecht und das Urheberrecht in Konflikt. Das Datenschutzrecht setzt der „unbegrenzten Auskunft" Grenzen. Auch dem Urheberrechtsverletzer – oder gar nur dem potentiellen Schädiger – stehen die Rechte zu, die ihm das Datenschutzrecht zur Wahrung seiner informationellen Selbstbestimmung gewährt. Die Rechtsordnung ist daher gehalten, diesen sensiblen Bereich zu kalibrieren. Einerseits bedarf der Rechteinhaber zur effektiven Durchsetzung seiner Rechte gewisser Informationen. Andererseits verlangt das Datenschutzrecht, einer Ausuferung dieser Auskünfte entgegenzutreten. Dieses Spannungsverhältnis betrachtet der vorliegende Beitrag.

Zur Untersuchung des Spannungsverhältnisses werden zunächst die Rechtsquellen des Urheberrechts und des Datenschutzrechts der Europäischen Union und des Europarats dargestellt. Die Grundlagen bilden hierbei die so genannten Gründungsverträge[1] der Europäischen Union wie auch die Konvention zum Schutz der Menschenrechte und Grundfreiheiten[2] (EMRK) des Europarats, in denen die Grundfreiheiten und Grundrechte der Bürger festgehalten sind. Das zentrale Augenmerk liegt jedoch auf der sekundärrechtlichen Ausgestaltung des Urheber- und Datenschutzrechts. Beide Rechtsgebiete hat die Europäische Union mit diversen Richtlinien europaweit entscheidend geprägt.

Im Anschluss daran werden konkrete Konfliktfelder aufgezeigt. Aktuelle Beispiele, insbesondere aus der Rechtsprechung des Gerichtshofs der Europäischen Union (EuGH), sollen die Problematik verdeutlichen und die widerstreitenden Interessen auch in praktischer Hinsicht veranschaulichen. Ein Blick in einzelne nationale Rechtsordnungen beleuchtet alternative Modelle einer „datenschonenden" Durchsetzung von Urheberrechten.

II. Rechtsgrundlagen auf europäischer Ebene

Die Rechtsgrundlagen auf europäischer Ebene sind in erster Linie im Recht der Europäischen Union verankert. Daneben finden sich wichtige Bestimmungen in den Rechtsakten des Europarats.

1. Grundrechtliche Aspekte

1.1. Charta der Grundrechte der Europäischen Union

Von Bedeutung für das Spannungsverhältnis zwischen den Belangen des Urheberrechts und des Datenschutzes ist in besonderem Maße die Charta der Grundrechte der Europäischen Union.[3]

In der vorliegenden Konstellation streitet für das Urheberrecht bzw. für die Rechteinhaber stets das Eigentumsrecht aus Art. 17 EU-Grundrechtecharta, dessen Abs. 2 ausdrücklich auch das geistige Eigentum schützt. Dem steht Art. 8 EU-Grundrechtecharta gegenüber, der den Schutz personenbezogener Daten grundrechtlich verankert. In bestimmten Fallkonstellationen kommen darüber hinaus die Berufsfreiheit bzw. die unternehmerische Freiheit nach Art. 15 bzw. 16 EU-Grundrechtecharta zum Tragen. Spätestens beim Einsatz von Filtersystemen zur Verhinderung von Urheberrechtsverletzungen wird auch die Informationsfreiheit nach Art. 11 EU-Grundrechtecharta relevant.[4] Der Gerichtshof der Europäischen Union nimmt im Konfliktfall häufig eine Abwägung der kollidierenden Interessen vor, um die widerstreitenden Interessen in Einklang zu bringen.

1.2. Konvention zum Schutz der Menschenrechte und Grundfreiheiten

Datenschutz auf der einen sowie der Schutz der Rechte der Urheber auf der anderen Seite sind darüber hinaus auch im Rechtekanon des Europarats geschützt. Art. 8 EMRK gewährleistet das Recht auf Achtung des Privat- und Familienlebens. Art. 1 des Ersten Zusatzprotokolls zur EMRK sieht den Schutz des Eigentums vor. Betrachtet man die Verbreitung von urheberrechtlich geschützten Werken auch unter dem Blickwinkel der Verbreitung von Informationen und Meinungen, kommen zusätzlich nach Art. 10 EMRK das Recht auf freie Meinungsäußerung und die Informationsfreiheit zum Tragen.[5] Auch der Europäische Gerichtshof für Menschenrechte (EGMR)

---

1) Dies sind im Einzelnen der Vertrag über die Europäische Union in der Fassung des Vertrags von Lissabon (EUV) vom 13. Dezember 2007 (ABl. Nr. C 306 S. 1, ber. ABl. 2008 Nr. C 111 S. 56, ABl. 2009 Nr. C 290 S. 1, ABl. 2011 Nr. C 378 S. 3) und der Vertrag über die Arbeitsweise der Europäischen Union (AEUV) in der Fassung der Bekanntmachung vom 9. Mai 2008 (ABl. Nr. C 115 S. 47).
2) Konvention zum Schutz der Menschenrechte und Grundfreiheiten, UNTS Band 213 S. 221.
3) Charta der Grundrechte der Europäischen Union vom 12. Dezember 2007, ABl. Nr. C 303 S. 1.
4) Siehe hierzu Angelopoulos, C, Filterung des Internets nach urheberrechtlich geschützten Inhalten in Europa, IRIS *plus* 2009-4.
5) Entsprechend Art. 11 der EU-Grundrechtecharta.

betont in Fällen des Zielkonflikts des Urheberrechts mit anderen Interessen das Bedürfnis nach einer Abwägung.

Der EGMR hat sich in seiner bisherigen Rechtsprechung kaum mit dem spezifischen Konflikt zwischen Urheberrecht und Datenschutz auseinandergesetzt. Der „Klassiker" medienrechtlicher Rechtsprechung des EGMR ist der Widerstreit von Art. 8 und Art. 10 EMRK. Dies sind meist Fälle, in denen die mediale Berichterstattung in die Privatsphäre des Betroffenen eingreift. Das Urheberrecht zeigt sich bislang recht „unberührt" von der Rechtsprechung des EGMR. Aus der jüngeren Zeit sind zwei Urteile hervorzuheben. Hierzu gehört zunächst das Urteil *Ashby Donald u.a. gegen Frankreich*.[6] Im zugrundeliegenden Fall geriet das Urheberrecht mit Art. 10 EMRK in Konflikt. Modefotographen hatten urheberrechtlich geschützte Fotos von Modeschauen ohne die Zustimmung der Modehäuser veröffentlicht. Die nationalen Gerichte Frankreichs verurteilten die Fotographen zu Geldbußen und Schadensersatz wegen einer Urheberrechtsverletzung. Der EGMR bestätigte den Vorrang des Urheberrechts in dieser Konstellation. Geldbuße und Schadensersatz seien nicht unverhältnismäßig gewesen und die Entscheidung der nationalen Gerichte könne als angemessener Ausgleich der kollidierenden Interessen angesehen werden.

Für die Rolle der Intermediäre von besonderem Interesse ist der Beschluss des EGMR vom 19. Februar 2013 im Rechtsstreit *Neij und Sunde Kolmisoppi gegen Schweden*.[7] Die Beschwerdeführer waren Entwickler und Pressesprecher von The Pirate Bay, dem weltweit größten so genannten BitTorrent-Tracker.[8] Obgleich der Austausch der Dateien nicht über den Server des Diensteanbieters ablief, wurden sie im nationalen Verfahren vor den schwedischen Gerichten wegen Beihilfehandlungen zu Urheberrechtsverletzungen zu zehn bzw. acht Monaten Freiheitsstrafe und Schadensersatz in Höhe von EUR 5 Mio. verurteilt.

Der EGMR erachtet den Dienst The Pirate Bay als von Art. 10 EMRK geschützt und das Urteil der schwedischen Gerichte demzufolge als Eingriff in das Recht auf freie Meinungsäußerung. Entscheidend kam es daher darauf an, ob dieser Eingriff „in einer demokratischen Gesellschaft notwendig ist", so die Terminologie von Art. 10 Abs. 2 EMRK. Im Ergebnis wurde dies vom EGMR angenommen und eine Verletzung des Art. 10 EMRK somit verneint. Aufgrund der gewichtigen Interessen des schwedischen Staates, das urheberrechtliche Eigentum zu schützen, sei es nicht zu beanstanden, die Dienste von The Pirate Bay als strafbare und haftungsbegründende Beihilfehandlungen zu werten. Hierbei berücksichtigte der EGMR den Umstand, dass sich die Betreiber auch auf mehrfache Aufforderung hin weigerten, die Torrent-Dateien zu entfernen.

Über die Rechtsprechung des EGMR hinaus erlangt die EMRK auch auf nationaler Ebene Bedeutung. Die Konvention gilt in sämtlichen Mitgliedstaaten des Europarats in Form unmittelbar nationalen Rechts, sei es mit einem Rang, der die EMRK über einfachen Gesetzen einordnet[9] oder sie gar mit Verfassungsrang ausstattet.[10] Darüber hinaus sind die Grundrechte der EMRK gemäß Art. 6 Abs. 2 und 3 EUV auch Bestandteil des Unionsrechts.

6) Urteil vom 10. Januar 2013, Beschwerdenummer 36769/08, abrufbar in französischer Sprache unter http://hudoc.echr.coe.int/sites/fra/pages/search.aspx?i=001-115845; s. auch Voorhoof, D., IRIS 2013-3/1.
7) Beschwerdenummer 40397/12, abrufbar in englischer Sprache unter http://hudoc.echr.coe.int/sites/fra/pages/search.aspx?i=001-117513, s. auch Voorhoof, D., IRIS 2013-5/2.
8) Ein BitTorrent-Tracker führt den Tausch von Dateien nicht selbst durch, sondern hilft Anbietern und Suchenden von bestimmten Dateien lediglich, sich gegenseitig zu finden. Diese tauschen sodann die Dateien direkt und ohne Nutzung des Trackers aus.
9) So in den meisten Staaten wie etwa in Belgien, Frankreich, Portugal, Schweiz, Spanien, Griechenland.
10) So in Österreich. In Deutschland, Italien und Großbritannien hat die EMRK den Rang eines einfachen Gesetzes, wobei auch in diesen Staaten die EMRK bei der Auslegung anderer Gesetze besonders berücksichtigt werden muss und so faktisch über sonstigem einfachen Recht steht.

2. Primärrecht

Die Bedeutung des Urheberrechts und des Datenschutzes für die Rechtsetzung durch die Organe der Europäischen Union wird schon am Primärrecht deutlich, das die Grundlage des Handelns der Europäischen Union bildet.

2.1. Urheberrecht

Das Urheberrecht weist einen starken ökonomischen Bezug auf, der besondere Bedeutung für den freien Waren- und Dienstleistungsverkehr und den freien Wettbewerb mit sich bringt. Die Entstehung, die Verwertung und die Durchsetzung urheberrechtlich geschützter Werke ist dabei kein rein nationaler Vorgang, sondern überschreitet spielerisch Grenzen[11] – nicht zuletzt in Anbetracht der vielfältigen technischen Möglichkeiten. Dies gilt insbesondere für die Verbreitung solcher Werke durch audiovisuelle Mediendienste.[12]

Die Europäische Union ist nach Art. 26 AEUV bestrebt, einen Binnenmarkt ohne Binnengrenzen zu schaffen, in dem der freie Verkehr von Waren (Art. 28 ff. AEUV) und Dienstleistungen (Art. 56 ff. AEUV) sowie ein freier und fairer Wettbewerb (Art. 101 ff. AEUV) gewährleistet ist. Damit einher geht das Bemühen, die Rechtsordnung(en) innerhalb der Europäischen Union zu harmonisieren. Art. 114 AEUV verlangt insoweit ausdrücklich eine Angleichung. Mit dem Vertrag von Lissabon ist für das Urheberrecht in Art. 118 AEUV eine ausdrückliche Kompetenzgrundlage geschaffen worden. Danach soll die Europäische Union auf „einen einheitlichen Schutz der Rechte des geistigen Eigentums in der Union" hinwirken. Ebenso wurde im Zuge des Vertrags von Lissabon das geistige Eigentum in Art. 207 Abs. 1 Satz 1 AEUV als Bestandteil der gemeinsamen Handelspolitik anerkannt.

Auf dieser Grundlage hat die Europäische Union für das Urheberrecht eine Reihe an Richtlinien erlassen, die die nationalen Rechtsordnungen der Mitgliedstaaten deutlich prägen (hierzu sogleich).

2.2. Datenschutzrecht

Wie urheberrechtlich geschützte Werke haben auch personenbezogene Daten häufig einen wirtschaftlichen Wert. Die Informationen werden zur Durchführung von Geschäften genutzt und sind – wie im vorliegenden Fall – von besonderer Relevanz zur notfalls zwangsweisen Durchsetzung von Urheberrechten. Daher sieht sich die Europäische Union aus den gleichen Binnenmarktaspekten wie beim Urheberrecht gehalten, regulativ einzugreifen. Auch für den Datenschutz hält der AEUV eine Sonderregelung bereit. Art. 16 Abs. 1 AEUV postuliert zunächst das Recht auf den Schutz eigener personenbezogener Daten. Art. 16 Abs. 2 AEUV in Verbindung mit Art. 39 EUV formuliert darüber hinaus einen datenschutzrechtlichen Gesetzgebungsauftrag an die Europäische Union und die Mitgliedstaaten. Dieser richtet sich allerdings nicht nur auf den Daten*schutz*, sondern auch auf die Gewährung eines freien Datenverkehrs.[13]

11) S. hierzu die Mitteilung der Kommission „Verbesserung der Durchsetzung von Rechten des geistigen Eigentums im Binnenmarkt" vom 11. September 2009, KOM(2009) 467 final, sowie die Mitteilung der Kommission über Inhalte im digitalen Binnenmarkt vom 18. Dezember 2012, COM(2012) 789 final.

12) Yliniva-Hoffmann, A./Matzneller, P., Der rechtliche Schutz der Rundfunkunternehmen – Herausforderungen durch neue Dienste, IRIS *plus* 2010-5, alle hier zitierten Leitbeiträge der IRIS *plus* sind abrufbar unter www.obs.coe.int/oea_publ/iris/iris_plus/index.html

13) Der nach Art. 16 Abs. 2 AEUV zu gewährleistende Datenschutz bindet indes primär die Organe, Einrichtungen und Stellen der Europäischen Union sowie die Mitgliedstaaten soweit sie Tätigkeiten ausüben, die in den Anwendungsbereich des Unionsrechts fallen.

3. Sekundärrecht

Das Urheber- wie auch das Datenschutzrecht finden insbesondere in den einschlägigen Richtlinien und Verordnungen der Europäischen Union eine detaillierte Ausgestaltung.

3.1. Urheberrecht

Das Urheberrecht der Europäischen Union setzt sich aus einer Vielzahl von Richtlinien und weiteren Rechtsakten zusammen. Für das Konfliktfeld zwischen Datenschutz und Urheberrecht von hervorgehobener Bedeutung ist zunächst die Richtlinie zur Harmonisierung bestimmter Aspekte des Urheberrechts und der verwandten Schutzrechte in der Informationsgesellschaft (2001/29/EG).[14] Das Bestreben dieser Richtlinie ist die EU-weite Anpassung des Urheberrechts an die digitale Welt und den elektronischen Geschäftsverkehr. Hierzu werden die Rechte der Urheber – wie etwa das Vervielfältigungsrecht und das Recht der öffentlichen Wiedergabe und Zugänglichmachung – insbesondere auch für den Online-Sektor angepasst und so die Positionen der Urheber gestärkt. In Art. 8 Abs. 3 der Richtlinie sind gerichtliche Anordnungen gegen Vermittler (für die Zwecke dieses Beitrags auch Intermediäre genannt) vorgesehen, wenn deren Dienste von einem Dritten zu Urheberrechtsverletzungen genutzt werden.[15] Die Richtlinie 2001/29/EG steht in engem Zusammenhang mit der Richtlinie zum elektronischen Geschäftsverkehr (E-Commerce-Richtlinie 2000/31/EG[16]). Diese enthält in den Art. 12, 13 und 14 ganz wesentliche Haftungsprivilegien für den Intermediär. Dieser ist als Diensteanbieter grundsätzlich nicht verantwortlich für Informationen und Inhalte,

- die von ihm lediglich übermittelt werden (Art. 12: Reine Durchleitung),
- die von ihm automatisch und zeitlich begrenzt zwischengespeichert werden (Art. 13: Caching) sowie solche Informationen und Inhalte, und
- die vom Nutzer eingegeben und vom Intermediär im Auftrag des Nutzers gespeichert werden (Art. 14: Hosting).

Diese Haftungsprivilegien berühren dabei jedoch nicht die Pflicht eines Diensteanbieters, Rechtsverletzungen abzustellen oder zu verhindern, und erlauben den Mitgliedstaaten ausdrücklich, ihren Gerichten und Verwaltungsbehörden entsprechende Anordnungen zu ermöglichen.

Darüber hinaus hält Art. 15 Abs. 1 der E-Commerce-Richtlinie fest, dass die Intermediäre nicht verpflichtet sind, die von ihnen übermittelten und gespeicherten Daten gleich wie zu überwachen oder aktiv nach Umständen zu forschen, die auf rechtswidrige Inhalte hinweisen. In Abs. 2 ist hingegen die Möglichkeit vorgesehen, dass Intermediäre in den einzelnen Mitgliedstaaten verpflichtet werden können, mutmaßlich rechtswidrige Inhalte den zuständigen Behörden zu übermitteln. Daneben können die nationalen Rechtsordnungen den zuständigen Aufsichtsbehörden einen Anspruch gegen Intermediäre zugestehen, der sich auf die Auskunft zu Informationen über die jeweiligen Nutzer richtet. Denkbar sind Konstellationen, in denen das Urheberstrafrecht greift und die nationalen Ermittlungsbehörden, wie etwa die Staatsanwaltschaften, sich mit einem Auskunftsverlangen an Intermediäre richten.

---

14) Richtlinie 2001/29/EG des Europäischen Parlaments und des Rates vom 22. Mai 2001 zur Harmonisierung bestimmter Aspekte des Urheberrechts und der verwandten Schutzrechte in der Informationsgesellschaft („Urheberrechts-" oder „Informationsgesellschaft-Richtlinie"), ABl. L 167 vom 22. Juni 2001, S. 10–19.

15) S. auch Erwägungsgrund 59: „Insbesondere in der digitalen Technik können die Dienste von Vermittlern immer stärker von Dritten für Rechtsverstöße genutzt werden. Oftmals sind diese Vermittler selbst am besten in der Lage, diesen Verstößen ein Ende zu setzen. Daher sollten die Rechtsinhaber – unbeschadet anderer zur Verfügung stehender Sanktionen und Rechtsbehelfe – die Möglichkeit haben, eine gerichtliche Anordnung gegen einen Vermittler zu beantragen, der die Rechtsverletzung eines Dritten in Bezug auf ein geschütztes Werk […] in einem Netz überträgt. […] Die Bedingungen und Modalitäten für einen derartige gerichtliche Anordnung sollten im nationalen Recht der Mitgliedstaaten geregelt werden.".

16) Richtlinie 2000/31/EG des Europäischen Parlaments und des Rates vom 8. Juni 2000 über bestimmte rechtliche Aspekte der Dienste der Informationsgesellschaft, insbesondere des elektronischen Geschäftsverkehrs, im Binnenmarkt („Richtlinie über den elektronischen Geschäftsverkehr"), ABl. L 178 vom 17. Juli 2000, S. 1–16.

Der genannte Auskunftsanspruch des Art. 15 der E-Commerce-Richtlinie steht freilich nur „zuständigen Behörden" zu. Hierzu gehören gerade nicht die Rechteinhaber, die in der Regel ein großes Interesse daran haben, ihre Ansprüche bei Urheberrechtsverletzungen geltend zu machen, die gerade im Online-Sektor zahlreich vorkommen.[17] Eine Haftung der Intermediäre als Dritte oder „Störer" scheidet aufgrund der genannten Art. 12 bis 14 der E-Commerce-Richtlinie aus. Daher sind die Rechteinhaber gehalten, sich an den eigentlichen Rechtsverletzer zu halten. Um dessen Identität in Erfahrung zu bringen, bedürfen sie jedoch solcher Auskunftsansprüche, wie sie Art. 15 der E-Commerce-Richtlinie für die Behörden vorsieht.

Einen solchen – bis dato in einigen Mitgliedstaaten noch nicht bestehenden – Auskunftsanspruch für die Rechteinhaber gewährt die Durchsetzungsrichtlinie 2004/48/EG.[18] Der Anspruch wurde mit der Intention geschaffen, die Diskrepanzen der Bestimmungen für einstweilige Maßnahmen zur Sicherung von Beweismitteln oder zur Beendung von Rechtsverstößen einzudämmen[19] und ist als Recht auf Auskunft in Art. 8 der Durchsetzungsrichtlinie verankert.[20]

Gemäß Art. 8 müssen die Mitgliedstaaten sicherstellen, dass Gerichte in Verfahren wegen Urheberrechtsverletzungen auf Antrag des Klägers Auskünfte auch von Dritten (mithin auch von Intermediären) verlangen können, sofern besondere Voraussetzungen wie ein gewerbliches Ausmaß der Rechtsverletzung vorliegen. Dieses Auskunftsverlangen umfasst den Ursprung und den Vertriebsweg der urheberrechtsverletzenden Tätigkeiten. Es kann sich, soweit angebracht, aber auch auf Namen und Adressen der an der Rechtsverletzung Beteiligten erstrecken. Art. 8 der Durchsetzungsrichtlinie enthält im Vergleich zu früheren Plänen der Europäischen Kommission ein „gelockertes Auskunftsrecht". Art. 9 des ursprünglichen Kommissionsvorschlags für eine Richtlinie über die Maßnahmen und Verfahren zum Schutz der Rechte an geistigem Eigentum[21] enthielt ein weitergehendes Recht auf Auskunft gegen „jede Person", wobei schon der Verdacht auf eine Rechtsverletzung ausreichen sollte. Dies wurde aus Datenschutzkreisen scharf kritisiert, da diese Fassung das Recht auf Auskunft nicht auf den Rahmen eines anhängigen Verfahrens beschränkt hätte. Stattdessen hätte der Auskunftsanspruch im zivilrechtlichen Verfahren „gegen Unbekannt" durchgesetzt werden können.[22] Vor diesem Hintergrund wurde eine Ausforschung der Zugangsprovider schon bei bloßen Verdachtsfällen befürchtet. Das Recht auf Auskunft erstreckte sich im Richtlinienvorschlag zudem auf jede Privatperson und nicht nur auf den Rechtsverletzer im gewerblichen Ausmaß. Weiterhin sollten nach Art. 9 Abs. 4 des Richtlinienvorschlags Zoll- und Polizeibehörden die ihnen im Zusammenhang mit Urheberrechtsverletzungen bekannt gewordenen Daten automatisch an die jeweiligen Rechteinhaber weiterleiten. Auch diese Regelung wurde in die endgültige Fassung der Durchsetzungsrichtlinie nicht aufgenommen.

3.2. Datenschutzrecht

Das urheberrechtliche Sekundärrecht steht nahezu umfassend unter dem Vorbehalt der datenschutzrechtlichen Bestimmungen des Unionsrechts. Gemäß Art. 2 Abs. 3 lit. a) der Durchsetzungsrichtlinie 2004/48/EG berühren die Bestimmungen dieser Richtlinie die Datenschutzrichtlinie 95/46/EG[23] nicht. Das Datenschutzrecht erhält somit eine grundsätzliche Vorrangstellung gegenüber urheberrechtlichen Bestimmungen, denn auch die sonstigen

17) Der „Umweg" über die Staatsanwaltschaft, die Identität des Rechtsverletzers in Erfahrung zu bringen, ist häufig dort notwendig, wo die nationale Rechtsordnung einen direkten Auskunftsanspruch des Rechteinhabers gegen den Zugangsprovider nicht vorsieht.
18) Richtlinie 2004/48/EG des Europäischen Parlaments und des Rates vom 29. April 2004 zur Durchsetzung der Rechte des geistigen Eigentums in der Fassung der Berichtigung vom 30. April 2004, ABl. L 157 vom 30. April 2004, S. 45–86.
19) Siehe Erwägungsgrund 7 der Durchsetzungsrichtlinie (2004/48/EG).
20) Art. 8 der Durchsetzungsrichtlinie 2004/48/EG konkretisiert insoweit den allgemein gehaltenen Rechtsbehelf in Art. 8 Abs. 3 der Urheberrechtsrichtlinie 2001/29/EG.
21) KOM/2003/0046 endg. – COD 2003/0024; die Durchsetzungsrichtlinie (2004/48/EG) basiert auf diesem Vorschlag.
22) So etwa der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit in Deutschland, s. Pressemitteilung vom 10. März 2004: „Schaar begrüßt Stärkung des Datenschutzes bei der IPR-Enforcement-Richtlinie, abrufbar in deutscher Sprache unter www.bfdi.bund.de/DE/Oeffentlichkeitsarbeit/Pressemitteilungen/Archiv/06-04StaerkungDesDatenschutzesBeiDerIPR-Enforcement-Richtlinie.html?nn=409394
23) Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, ABl. L 281 vom 23. November 1995, S. 31–50

hier einschlägigen und angeführten Richtlinien gelten grundsätzlich unter dem Vorbehalt anderweitiger Regelungen in der Datenschutzrichtlinie oder verlangen zumindest die Achtung der Datenschutzbestimmungen bei der Anwendung des Urheberrechts.[24] Auch für den Bereich des elektronischen Geschäftsverkehrs verweist die E-Commerce-Richtlinie in Erwägungsgrund 14 vollumfänglich auf die Datenschutzrichtlinie. Diese genießt – gerade in Anbetracht von Auskunftsansprüchen nach der E-Commerce-Richtlinie – grundsätzlich Vorrang.[25]

Die Datenschutzrichtlinie enthält die im Sekundärrecht der Europäischen Union grundlegenden Bestimmungen und Prinzipien zum Datenschutz, die in den Datenschutzgesetzen aller Mitgliedstaaten umgesetzt sind. Zu diesen Prinzipien gehört der Grundsatz des Verbots mit Erlaubnisvorbehalt: Nach Art. 7 der Datenschutzrichtlinie sollen personenbezogene Daten grundsätzlich nur dann erhoben oder verarbeitet werden, wenn der Betroffene hierzu ausdrücklich einwilligt.[26] Eine Ausnahme sieht Art. 7 jedoch in verschiedenen Fällen vor:

„lit. c) Die Datenverarbeitung ist zur Erfüllung einer rechtlichen Verpflichtung erforderlich, der der für die Verarbeitung Verantwortliche unterliegt."[27]

„lit. f) Die Datenverarbeitung ist erforderlich zur Verwirklichung des berechtigten Interesses, das von den Dritten wahrgenommen wird, denen die Daten übermittelt werden, sofern nicht das Interesse oder die Grundrechte und Grundfreiheiten der betroffenen Person überwie[g]en."[28]

3.3. Rechtsakte des Europarats

Im Bereich des Datenschutzes hat der Europarat mit der Datenschutzkonvention vom 28. Januar 1981 eine Vorreiterrolle in der Schaffung eines europaweiten Datenschutzstandards.[29] In der Rechtspraxis ist das Unionsdatenschutzrecht inzwischen jedoch von größerer Bedeutung als die Konvention.

Auch der Thematik des Urheberrechts im Online-Sektor hat sich der Europarat gewidmet und dabei den Konflikt mit den Interessen der Nutzer erkannt.

Am 12. März 2010 verabschiedete die Parlamentarische Versammlung des Europarats (PACE) die Empfehlung 1906 (2010), die sich mit den Rechten des geistigen Eigentums in der digitalen Gesellschaft befasst.[30] Damit sollte die Diskussion über ein Modell angestoßen werden, das die Urheberrechte von Autoren geistiger Werke, Investoren und der Allgemeinheit harmonisiert. Der PACE sieht das Gleichgewicht zwischen diesen Interessengruppen angesichts der Entwicklung der digitalen Gesellschaft als beträchtlich gestört an: Die internationalen Instrumente seien nicht mehr geeignet, Autoren eine angemessene Vergütung für ihre Werke und gleichzeitig den Schutz

24) Siehe Erwägungsgründe 57 und 60 der Urheberrechtsrichtlinie (2001/29/EG); Art. 1 Abs. 5 lit. b sowie Erwägungsgrund 14 der E-Commerce-Richtlinie (2000/31/EG); vgl. zum Konflikt des Datenschutzrechts mit den Medienfreiheiten *Scheuer, A./Schweda, S.*, Der Schutz personenbezogener Daten und die Medien, in: Die Grenzen der Nutzung persönlicher Daten, IRIS *plus* 2011-6, S. 7 bis 29.

25) Erwägungsgrund 14 der E-Commerce-Richtlinie (2000/31/EG): „Der Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten ist ausschließlich Gegenstand der Richtlinie 95/46/EG [... Diese] begründe[t] bereits einen gemeinschaftsrechtlichen Rahmen für den Bereich personenbezogener Daten, so daß diese Frage in der vorliegenden Richtlinie nicht geregelt werden muß. [...] Die Grundsätze des Schutzes personenbezogener Daten sind bei der Umsetzung und Anwendung dieser Richtlinie uneingeschränkt zu beachten, insbesondere in bezug auf [...] die Verantwortlichkeit von Vermittlern."

26) So auch Art. 6 des Vorschlags für Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung) vom 25. Januar 2012.

27) Dies ist etwa dann der Fall, wenn ein Intermediär zur Herausgabe der persönlichen Daten seines Kunden aufgrund eines Auskunftsanspruchs eines Dritten verpflichtet ist.

28) Im Richtlinientext – wohl infolge eines redaktionellen Versehens – „überwiesen".

29) Übereinkommen zum Schutz des Menschen bei der automatisierten Verarbeitung personenbezogener Daten (Konvention Nr. 108) vom 28. Januar 1981.

30) Recommendation 1906 (2010), Rethinking creative rights for the Internet age, abrufbar in englischer Sprache unter http://assembly.coe.int/Main.asp?link=/Documents/AdoptedText/ta10/EREC1906.htm; eine nichtamtliche Übersetzung ins Deutsche findet sich in: IRIS *plus* 2012-1, S. 39 f., s. auch Breemen, V., IRIS 2010-10/4

personenbezogener Daten zu gewährleisten. Das Überleben der kreativen Berufe stehe der Gefahr einer Internetüberwachung gegenüber, so die Empfehlung.

Zwar sieht der Europarat zuvörderst die Mitgliedstaaten in der Pflicht, einen Ausgleich zu schaffen. Er sieht sich jedoch gehalten, sich bei der Gestaltung einzubringen. Dabei wird unter 8.4 der Empfehlung auch auf die besondere Rolle der Vermittler hingewiesen („*access providers, content-sharing platforms, search engines*").

Doch auch schon ein Jahrzehnt zuvor war der Europarat nicht untätig geblieben, wenngleich der Fokus seinerzeit deutlich auf den Schutz der Urheberrechte gerichtet war und weniger auf deren Ausgleich mit dem Schutz personenbezogener Daten. In der Empfehlung Rec(2001)7 über Maßnahmen zum Schutz des Urheberrechts und verwandter Schutzrechte und zur Bekämpfung der Piraterie, insbesondere im digitalen Umfeld,[31] widmet sich das Ministerkomitee dem Aufkommen neuer Formen von Piraterie.[32] Im Hinblick auf zivilrechtliche Instrumente verlangt die Empfehlung die Ermächtigung der Justizbehörden zur Verhängung vorläufiger Maßnahmen zur Verhinderung und Verfolgung von Rechtsverletzungen, die gegebenenfalls auch ohne Anhörung der anderen Partei ergriffen werden sollen. Auch für die Beweissicherung sind nach der Empfehlung Beibringungspflichten der Rechtsverletzer vorzusehen. Ebenso müsse der Rechtsverletzer die Identität Dritter offenlegen, soweit diese in die Rechtsverletzung involviert sind. Einen Anspruch gegen Vermittler sieht die Empfehlung indes nicht vor.

Ebenfalls aus dem Jahr 2001 stammt das Übereinkommen über Computerkriminalität.[33] Zwar hat dieses Übereinkommen einen eindeutig strafrechtlichen Ansatz, der die Konstellation von Auskunftsansprüchen von Rechteinhabern gegen Intermediäre nicht anspricht. „Eingedenk des Rechts auf den Schutz personenbezogener Daten" und des Datenschutzübereinkommens von 1981[34] sieht es allerdings Auskunftspflichten der Intermediäre gegenüber den zuständigen Behörden vor.[35] Danach können diese anordnen, dass Diensteanbieter Bestandsdaten ihrer Kunden vorlegen. Die Bestandsdaten im Sinne dieses Übereinkommens („*subscriber information*") umfassen unter anderem die Art und Dauer des genutzten Dienstes und die Identität des Nutzers (z. B. Hausanschrift, Telefonnummer). Zwar ist die Konstellation, dass staatliche Einrichtungen derartige Auskünfte einholen, durchaus von datenschutzrechtlicher Brisanz. Im Fokus der vorliegenden Darstellung soll jedoch das Verhältnis der drei Positionen Rechteinhaber, Intermediär und Endnutzer stehen. Strafverfahrensrechtliche „Umwege" mögen für den Rechteinhaber ein Weg sein, den Urheberrechtsverletzer zu identifizieren. Dieser Weg erweist sich jedoch meist als wenig effektiv.

Folgerichtig erkennt das strafrechtlich geprägte Übereinkommen über Computerkriminalität andere zivilrechtliche Instrumente an: Nach Art. 10 Abs. 3 ist eine strafrechtliche Verantwortlichkeit gar verzichtbar, „sofern andere wirksame Abhilfen zur Verfügung stehen". Als eine andere wirksame Abhilfe kann es demnach angesehen werden, wenn der Rechteinhaber mit effektiven zivilrechtlichen Mitteln ausgestattet wird, um seine Rechte zu verfolgen.

III. Konkret auftretende Konfliktfelder

Um seine Urheber- oder verwandten Schutzrechte geltend zu machen, benötigt der Inhaber, sei es eine Verwertungsgesellschaft, ein exklusiver Lizenznehmer oder der Urheber selbst, ein

31) Recommendation Rec(2001)7 of the Committee of Ministers to member states on measures to protect copyright and neighbouring rights and combat piracy, especially in the digital environment, in englischer Sprache abrufbar unter: https://wcd.coe.int/ViewDoc.jsp?Ref=Rec%282001%297&Language=lanEnglish&Ver=original&Site=CM&BackColorInternet=C3C3C3&BackColorIntranet=EDB021&BackColorLogged=F5D383, nichtamtliche Übersetzung in IRIS *plus* 2012-1, S. 41 ff.; s. auch Thórhallsson, P., IRIS 2001-9/7

32) Die Empfehlung beruht auf älteren Empfehlungen aus den Jahren 1988 bis 1995.

33) Vom 23. November 2001, ETS 185, abrufbar unter http://conventions.coe.int/Treaty/GER/Treaties/Html/185.htm; s. auch Asscher, L./McGonagle, T., IRIS 2001-5/2; Gentile, I.; IRIS 2001-7/1.

34) S. die Präambel des Übereinkommens über Computerkriminalität.

35) Art. 18 des Übereinkommens über Computerkriminalität.

Mindestmaß an persönlichen Informationen über seinen Anspruchsgegner. Um mit ihm in Kontakt treten zu können, aber auch um gegebenenfalls seine Ansprüche gerichtlich durchsetzen zu können, benötigt er zumindest den Namen und die Anschrift des Betroffenen. Daneben ist es für den Rechteinhaber häufig von besonderem Interesse zu wissen, wie und in welchem Umfang Urheberrechtsverletzungen stattgefunden haben. Auch bei diesen Informationen handelt es sich um personenbezogene Daten im Sinne des Datenschutzrechts,[36] dem der Gedanke zugrunde liegt, einen unkontrollierten Fluss persönlicher Information einzudämmen. Es steht also stets das Verwertungsinteresse des Rechteinhabers dem Recht auf Privatsphäre des Betroffenen gegenüber.

1. Recht auf Auskunft gegen den Verletzer

Die naheliegendste Konstellation, bei der Urheberrecht und Datenschutz in Konflikt geraten, ist zunächst diejenige, bei der sich der Rechteinhaber mit seinem Recht auf Auskunft direkt gegen den Rechtsverletzer richtet. Ein solcher Auskunftsanspruch ist in Art. 8 Abs. 1 der Durchsetzungsrichtlinie 2004/48/EG vorgesehen. Mit diesem Auskunftsanspruch wird nicht die Identität des Rechtsverletzers ermittelt (diese muss naturgemäß zuvor schon bekannt sein). Die Auskunft dient vielmehr der Information über die Herkunft rechtsverletzender Dienstleistungen, die Vertriebswege und die Identität der an der Urheberrechtsverletzung Beteiligten. Diese so genannte Drittauskunft dient nach Erwägungsgrund 21 der Durchsetzungsrichtlinie 2004/48/EG einem hohen Schutzniveau für die Urheberrechte, da sie die Verfolgung von weiteren im Zusammenhang stehenden Rechtsverletzungen ermöglicht.

Der Anspruch dürfte sich jedoch immer dann als „stumpfes Schwert" erweisen, wenn dem Rechteinhaber die Identität des Rechtsverletzers schlicht nicht bekannt ist. In diesen Fällen geraten die Intermediäre in den Fokus der Rechteinhaber.

2. Recht auf Auskunft gegen Intermediäre

Konkreter wird der Konflikt zwischen Urheberrecht und Datenschutz dann, wenn sich die Rechteinhaber bei der Verfolgung von Urheberrechtsverstößen im Internet jener Daten bedienen möchten, die ein Internetzugangsprovider oder ein Diensteanbieter im Rahmen der Bereitstellung seiner Dienste über seine Kunden vorhält.

2.1. Identifizierung des Rechtsverletzers

Der Urheberrechtsverletzer, der sich im Internet zunächst anonym bewegen kann, ist in der Regel allein über die ihm zu einem bestimmten Zeitpunkt zugewiesene IP-Adresse identifizierbar – eine Information, über die meist nur der Zugangsprovider verfügt, der die Kundendaten mit den jeweils zugewiesenen IP-Adressen verknüpfen kann.[37] Dasselbe gilt für Internetdienstleister (z. B. so genannte soziale Netzwerke oder Sharehoster), sofern sie von ihren Kunden eine Registrierung mit persönlichen Daten verlangen.

Stellt der Rechteinhaber eine Verletzung an einem urheberrechtlich geschützten Werk im Internet fest, steht ihm zunächst allein die IP-Adresse zur Verfügung. Daher dürfte es für den Rechteinhaber in der Regel attraktiver sein, sich direkt gegen den Intermediär zu wenden und sich bei diesem schadlos zu halten. Der Intermediär ist jedoch seinerseits durch die Haftungsprivilegien der Art. 12 bis 15 der E-Commerce-Richtlinie 2000/31/EG geschützt und haftet grundsätzlich nicht für Rechtsverletzungen, die mittels seines Dienstes begangen werden.[38] Eine Haftung ist nur ausnahmsweise und zwar nur dann denkbar, wenn sich der Intermediär in irgendeiner

36) Personenbezogene Daten sind alle Informationen über eine bestimmte oder bestimmbare natürliche Person, s. Art. 2 lit. a) der Datenschutzrichtlinie 95/46/EG.
37) Dies setzt voraus, dass der Nutzer keine Verschleierungsmaßnahmen wie so genannte Tor-Software oder Proxy-Server einsetzt.
38) Hierzu s.o., Kapitel II.3.1.

Form an der Rechtsverletzung beteiligt, diese duldet oder fördert.[39] In einem solchen Fall wird dem Rechteinhaber ein Vorgehen gegen den Intermediär durch die Impressumspflicht aus Art. 5 Abs. 1 der E-Commerce-Richtlinie erleichtert. Diese gibt dem Intermediär auf, seine persönlichen Daten auf seinem Webauftritt leicht, unmittelbar und ständig verfügbar zu machen. Dem Internetdiensteanbieter wird daher – anders als dem Endnutzer – nicht das Recht gewährt, sich grundsätzlich anonym im Onlinebereich zu bewegen. Vom Diensteanbieter kann der Rechteinhaber nicht nur Schadensersatz wegen bereits eingetretener Rechtsverletzungen verlangen,[40] sondern auch präventiv wegen mutmaßlicher künftiger Rechtsverletzungen gegen ihn vorgehen.[41]

Der Rechteinhaber wird jedoch in erster Linie daran interessiert sein, den Rechtsverletzer zivilrechtlich zur Rechenschaft zu ziehen, wozu er die persönlichen Daten benötigt, die sich hinter der IP-Adresse verbergen (im Wesentlichen Name und Adresse). Hierbei hilft ihm das Recht auf Auskunft gegen den Intermediär aus Art. 8 Abs. 3 der Urheberrechtsrichtlinie 2001/29/EG und Art. 8 der Durchsetzungsrichtlinie 2004/48/EG. Ohne dieses Recht auf Auskunft verbleibt dem Rechteinhaber nur die Möglichkeit, ein Strafverfahren „gegen Unbekannt" einzuleiten. Im Zuge eines strafprozessualen Auskunftsanspruchs kann sodann die Ermittlungsbehörde die Auskunft über die Identität des Rechtsverletzers beim Intermediär einholen.[42] Durch sein Recht auf Akteneinsicht bei der Ermittlungsbehörde könnte der Rechteinhaber schließlich die Identität des Verletzers bei der Ermittlungsbehörde in Erfahrung bringen. Das Recht auf Auskunft verkürzt diesen unsicheren und umständlichen Weg durch eine direkte Inanspruchnahme des Intermediärs.

2.2. Grenzen des Auskunftsanspruchs

Bei der Geltendmachung des Rechts auf Auskunft sind jedoch datenschutzrechtliche Gesichtspunkte zu beachten. Trotz (mutmaßlich) begangener Urheberrechtsverletzung ist die Identität des Verletzenden datenschutzrechtlich geschützt. Eine Einwilligung in die Offenlegung der Identität wird in dieser Konstellation bei lebensnaher Betrachtung nicht vorliegen, so dass nach Art. 7 lit. b) bis d) der Datenschutzrichtlinie 95/46/EG eine besondere Ausnahme greifen muss, die die Verarbeitung ohne Einwilligung rechtfertigt. Nach Art. 13 Abs. 1 lit. g) sind Beschränkungen des Datenschutzes möglich, soweit sie für den Schutz der „Rechte und Freiheiten anderer Personen" erforderlich sind. Diese vage Formulierung ist das „Einfallstor" für das widerstreitende Urheberrecht. Es kommt daher in den Konfliktfällen stets zu einer Interessenabwägung.

Dabei sind auch die Interessen der Intermediäre von Belang. Diese sehen sich durch die Auskunftsansprüche zunächst einem hohen Aufwand und unwirtschaftlichen Kosten ausgesetzt. Hinzu kommt die Sorge, das Vertrauen der Kunden in die möglichst anonyme Nutzung der Dienstleistung zu gefährden, was Kundenverlust und wirtschaftliche Einbußen bei den Intermediären nach sich ziehen kann. Daher wird in der politischen Diskussion um die Pflichten der Intermediäre stets die Notwendigkeit der Haftungsprivilegierung betont, wie sie in der E-Commerce-Richtlinie vorgesehen ist. Je höher das Haftungsrisiko der Intermediäre, desto schwieriger wird es für diese, kostengünstige und attraktive Dienstleistungen anzubieten. Die Intermediäre bilden somit ein „drittes Lager" im Konfliktfeld zwischen Datenschutz und Urheberrecht.[43]

---

39) Zur Konkretisierung der Voraussetzung einer solchen Beteiligung, Duldung oder Förderung soll nach Plänen der Europäischen Union Art. 14 der E-Commerce-Richtlinie überarbeitet werden. Die Konsultation hierzu endete am 11. September 2012, www.ec.europa.eu/internal_market/e-commerce/notice-and-action/index_de.htm

40) S. Art. 13 der Durchsetzungsrichtlinie 2004/48/EG.

41) S. Art. 9 bis 11 der Durchsetzungsrichtlinie 2004/48/EG; z. B. in Form einer Sperre des Zugangs zur betreffenden Internetseite, vgl. Karl, H., IRIS 2011-7/8.

42) S. Art. 15 der E-Commerce-Richtlinie 2000/31/EG.

43) Datenschutzrechtliche Vorgaben können mitunter auch negative Auswirkungen auf den Verbraucher selbst haben, der sich möglicherweise gegen eine Abmahnung durch den Rechteinhaber wehren und in Erfahrung bringen möchte, in welchem Zusammenhang sein Zugangsprovider über ihn Auskunft erteilt hat. So erklärt beispielsweise in Deutschland der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI), dass ein Zugangsprovider nicht verpflichtet ist, seine Kunden über die Beauskunftung zu informieren. Insbesondere aber darf ein Provider nach Ansicht des BfDI den Inhalt der Beauskunftung nicht speichern, so dass eine solche Auskunft an den Kunden bei Nachfrage nicht möglich ist; siehe 23. Tätigkeitsbericht des BfDI 2009–2010, S. 52, abrufbar unter www.bfdi.bund.de/SharedDocs/Publikationen/Taetigkeitsberichte/TB_BfDI/23_TB_09_10.pdf?__blob=publicationFile

2.3. Der Auskunftsanspruch in der Rechtsprechung des EuGH

Mehrere Urteile des EuGH veranschaulichen, wie er die entgegenstehenden Interessen definiert, sie gewichtet und an welchen Kriterien er die Rechtmäßigkeit der jeweiligen Maßnahmen misst. Dabei lässt sich beobachten, dass der EuGH immer stärker die Grundrechte-Charta der EU in seine Prüfung mit einbezieht und eine Abwägung zwischen den betroffenen Grundrechten vornimmt.

Urteil vom 29. Januar 2008 (Promusicae)

Eine erste Entscheidung des EuGH im Normengeflecht urheberrechtlich motivierter Richtlinien (Urheberrechtsrichtlinie 2001/29/EG, Durchsetzungsrichtlinie 2004/48/EG) und der Datenschutzrichtlinie für elektronische Kommunikation 2002/58/EG[44] erging in der Rechtssache *Promusicae.*[45] *Promusicae*, eine spanische Produzentenvereinigung, verlangte von *Telefónica*, einem spanischen Zugangsprovider, die Offenlegung der Namen und Anschriften verschiedener Kunden, die über einen sogenannten *Shared Folder* des Programms *KaZaA* Urheberrechte verletzten. Das nationale Gericht ersuchte angesichts dieses Auskunftsbegehrens den Gerichtshof um die Auslegung der eingangs erwähnten einschlägigen Richtlinien. Fraglich war, ob das EU-Recht den Mitgliedstaaten vorschreibt, eine Pflicht zur Herausgabe personenbezogener Daten in einem zivilrechtlichen Verfahren zur Sicherung eines effektiven Urheberrechtsschutzes vorzusehen. Während das EU-Recht einen Auskunftsanspruch bei Strafverfahren ausdrücklich vorsieht, schien die Rechtslage bei zivilrechtlichen Ansprüchen unklar. Der EuGH verneinte auf der Basis einer Zusammenschau dieser Richtlinien ein solches Gebot. Zwar müssten die Mitgliedstaaten gemäß Art. 8 Abs. 1 der Durchsetzungsrichtlinie 2004/48/EG sicherstellen, dass die Zivilgerichte bei Verfahren wegen Verletzung von Urheberrechten auf einen begründeten und verhältnismäßigen Antrag des Klägers hin eine Auskunftspflicht des Intermediärs anordnen *können*. Eine allgemeine Pflicht zur Einrichtung eines solchen Auskunftsanspruchs enthalte Art. 8 jedoch gerade nicht. Art. 8 ist nämlich in seinem Anwendungsbereich durch die Bestimmungen zum Datenschutz ausdrücklich begrenzt.[46] Der Gerichtshof machte jedoch gleichzeitig deutlich, dass es den Mitgliedstaaten auch nicht untersagt sei, derartige Auskunftspflichten vorzusehen, wenn es darum geht, einen angemessenen Ausgleich zwischen den verschiedenen unionsrechtlich geschützten Grundrechten[47] zu finden – hier insbesondere das Eigentumsrecht und das Recht auf den Schutz personenbezogener Daten. Bei der Umsetzung solcher Maßnahmen müsse aber selbstverständlich der Grundsatz der Verhältnismäßigkeit beachtet werden.

Beschluss vom 19. Februar 2009 (LSG)

Dieselbe Ansicht brachte der EuGH etwa ein Jahr später in seinem Beschluss in der Rechtssache *LSG*[48] zum Ausdruck. In diesem Verfahren ging es ebenfalls um die Herausgabe von Nutzungsdaten durch einen Internetzugangsprovider. Die österreichische Verwertungsgesellschaft *Wahrnehmung von Leistungsschutzrechten GmbH* (LSG) verlangte im Ausgangsverfahren vom Intermediär *Tele 2 Telecommunication GmbH* Auskunft über Namen und Anschriften von Personen, die sich hinter dynamischen IP-Adressen verbargen, mittels derer illegales Filesharing betrieben wurde. Die Stoßrichtung der Vorlagefrage des österreichischen Obersten Gerichtshofs war hier eine andere: Das Gericht erkundigte sich explizit nach einem unionsrechtlichen Verbot der Herausgabe von

44) Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation), ABl. L 201 vom 31. Juli 2002, S. 37–47, zuletzt geändert durch Richtlinie 2009/136/EG des Europäischen Parlaments und des Rates vom 25. November 2009 zur Änderung der Richtlinie 2002/22/EG über den Universaldienst und Nutzerrechte bei elektronischen Kommunikationsnetzen und -diensten, der Richtlinie 2002/58/EG über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation und der Verordnung (EG) Nr. 2006/2004 über die Zusammenarbeit im Verbraucherschutz, ABl. L 337 vom 18. Dezember 2009, S. 11–36.

45) EuGH, Rs. C-275/06, *Promusicae*, Urteil vom 29. Januar 2008, Slg. 2008, S. I-00271.

46) S. Art. 8 Abs. 3 lit. e) der Durchsetzungsrichtlinie 2004/48/EG.

47) Siehe oben, Kapitel II. 1.

48) EuGH, Rs. C-557/07, *LSG*, Beschluss vom 19. Februar 2009, Slg. 2009, S. I-01227; s. auch Yliniva-Hoffmann, A., IRIS 2009-9/7.

Daten zur zivilrechtlichen Verfolgung von Urheberrechtsverstößen. Da der EuGH diesen Schwenk jedoch bereits in dem vorgenannten Urteil vollzogen hatte, konnte er die Frage hier recht zügig abhandeln; er beließ es daher bei einem Beschluss an Stelle eines Urteils. Der Gerichtshof forderte mit dem Beschluss die Mitgliedstaaten dennoch erneut auf, bei der Schaffung eines zivilrechtlichen Auskunftsanspruchs die Grundrechte und sonstigen allgemeinen Grundsätze des Rechts der Europäischen Union zu achten. Dies betreffe insbesondere den Grundsatz der Verhältnismäßigkeit.

Der stets betonte, aber sehr abstrakte Verhältnismäßigkeitsgrundsatz schafft indes kein hohes Maß an Rechtssicherheit. Es kann allenfalls die Schlussfolgerung zugelassen werden, dass ein zivilrechtlicher Auskunftsanspruch gegen den Zugangsprovider eines Nutzers, der systematisch und in großem Umfang das Urheberrecht verletzt, kaum gegen Unionsrecht verstoßen wird. Demgegenüber ist die Verhältnismäßigkeit schwieriger zu begründen, wenn der Auskunftsanspruch eines Mitgliedstaates infolge einer einzigen mutmaßlichen Urheberrechtsverletzung die Herausgabe der persönlichen Daten des jeweiligen Nutzers ermöglichen würde.[49]

Urteil vom 19. April 2012 (Bonnier Audio)

Den vorläufig letzten Schritt zu diesem Thema markiert das Urteil des EuGH in der Rechtssache *Bonnier Audio,*[50] in der sich zur Familie der zu berücksichtigenden Richtlinien erstmals auch die Vorratsdatenspeicherungsrichtlinie (2006/24/EG[51]) gesellte. Die Ausgangslage war erneut die gleiche wie in den beiden vorangegangenen Verfahren. Schwedische Inhaber von Rechten an Hörbüchern wandten sich mit einem Auskunftsbegehren an einen Zugangsprovider, über dessen Server urheberrechtswidrig Hörbücher verbreitet worden sein sollen. Der EuGH verzichtete auch hier nicht auf einen ausführlichen Verweis auf seine bisherige Rechtsprechung in *Promusicae* und *LSG* und wich im Ergebnis auch nicht davon ab. Allerdings stellte er klar, dass die Vorratsdatenspeicherungsrichtlinie für die Befriedigung zivilrechtlicher Auskunftsansprüche nicht herangezogen werden könne.

Erforderlich für das Verständnis dieses Urteils ist dabei das Verhältnis zwischen der Vorratsdatenspeicherungsrichtlinie 2006/24/EG und der Datenschutzrichtlinie für elektronische Kommunikation 2002/58/EG. Beide behandeln die Speicherung von Verkehrsdaten[52]: auf der einen Seite die Pflicht zur anlasslosen Speicherung zum Zwecke der Ermittlung, Feststellung und Verfolgung schwerer Straftaten oder Terrorismusbekämpfung; auf der anderen Seite – und dies gewissermaßen als Ausnahme von datenschutzrechtlichen Überlegungen – die den Providern eingeräumte Möglichkeit der Speicherung für eine begrenzte Zeit, beispielsweise für Abrechnungszwecke. Die Essenz aus *Bonnier Audio* lässt sich somit wie folgt beschreiben: Daten, die aufgrund einer die Vorratsdatenspeicherungsrichtlinie umsetzenden Pflicht gespeichert wurden, dürfen *nicht* für urheberrechtliche Auskunftsansprüche herangezogen werden. Dies ist ausdrücklich in Art. 4 Satz 1 der Vorratsdatenspeicherungsrichtlinie festgehalten: Danach müssen die Mitgliedstaaten sicherstellen, dass die aufgrund der Richtlinie gespeicherten Daten nur in bestimmten Fällen an nationale *Behörden* weitergegeben werden. Auf Verkehrsdaten jedoch, die beim Provider aufgrund einer Umsetzung der Datenschutzrichtlinie für elektronische Kommunikation 2002/58/EG noch in zulässiger Weise gespeichert sind, darf hingegen sehr wohl zurückgegriffen

49) Die Verhältnismäßigkeit hat in einem solchen Fall allerdings der deutsche Bundesgerichtshof bejaht, Beschluss vom 19. April 2012, Az. I ZB 80/11, abrufbar unter http://lexetius.com/2012,3310

50) EuGH, Rs. C-461/10, *Bonnier Audio*, Urteil vom 19. April 2012; s. Dohmen, F., IRIS 2012-6/4.

51) Richtlinie 2006/24/EG des Europäischen Parlaments und des Rates vom 15. März 2006 über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste oder öffentlicher Kommunikationsnetze erzeugt oder verarbeitet werden, und zur Änderung der Richtlinie 2002/58/EG, ABl. L 105 vom 13. April 2006, S. 54–63.

52) Verkehrsdaten sind gemäß Art. 2 UAbs. 2 lit. b) der Datenschutzrichtlinie für elektronische Kommunikation 2002/58/EG Daten, die zum Zwecke der Weiterleitung einer Nachricht an ein elektronisches Kommunikationsnetz verarbeitet werden. Ein Verkehrsdatum ist in der vorliegenden Konstellation etwa die Information, dass mit einer bestimmten IP-Adresse eine bestimmte Datei zu einer bestimmten Zeit hochgeladen wurde. Für die Rechteinhaber von Interesse sind indes stets die persönlichen Informationen über den Nutzer (auch Stamm-, Bestands- oder Nutzerdaten genannt). Nur diese ermöglichen es, den Nutzer wegen einer Urheberrechtsverletzung in Anspruch zu nehmen.

werden – selbstverständlich immer unter Berücksichtigung des Verhältnismäßigkeitsgrundsatzes und nach erfolgter Interessenabwägung der betroffenen Grundrechte.

Maßgeblich ist daher, ob der nationale Gesetzgeber eine Speicherpflicht oder auch eine Speichererlaubnis fernab der Vorratsdatenspeicherung nach der Richtlinie 2006/24/EG eingerichtet hat. Die Speicherungserlaubnis zu Abrechnungszwecken ist etwa in Art. 6 Abs. 2 der Datenschutzrichtlinie für elektronische Kommunikation 2002/58/EG vorgesehen. Dabei muss die Frage aufgeworfen werden, wie es sich auswirkt, dass die heute geläufige Form der Vertragsabrechnung, die so genannte Flatrate, keiner genauen Verbindungsdaten bedarf, um die Gebühren abzurechnen. Und selbst dort, wo dies notwendig ist, verlangt die Datenschutzrichtlinie für elektronische Kommunikation in Art. 6 Abs. 2 eine Löschung, sobald der Anspruch auf Zahlung geltend gemacht werden kann. Beides führt zunächst zu einer weiteren Reduzierung der für einen Auskunftsanspruch überhaupt verfügbaren Daten und damit zu der Frage, was geschieht, falls der Zugangsprovider die Verbindungsdaten dennoch in rechtswidriger Weise abspeichert. Solche Daten können gleichfalls nicht Gegenstand eines Auskunftsanspruchs sein. Entsprechend hat auch der Oberste Gerichtshof in Österreich mit seiner Entscheidung vom 14. Juli 2009 festgehalten, dass rechtmäßig zu einem legitimen Zweck gespeicherte Daten auch nur zu diesem legitimen Zweck verwendet werden dürfen und danach zu löschen sind.[53] Eine Auskunft durch den Zugangsprovider sei demnach rechtswidrig, solange nicht ein Gesetz ausdrücklich eine entsprechende Auskunftspflicht vorsehe, so der Gerichtshof.

Daten können damit grundsätzlich nur entsprechend der Ausnahmevorschrift des Art. 15 der Datenschutzrichtlinie für elektronische Kommunikation 2002/58/EG genutzt werden. Sie sieht eine Beschränkung der Vertraulichkeit der Daten nur vor, soweit diese verhältnismäßig ist und der nationalen Sicherheit, der Landesverteidigung, der öffentlichen Sicherheit und der Verhütung, Ermittlung und Verfolgung von Straftaten dient. Hierzu zählen nicht die möglichen zivilrechtlichen Schadensersatzansprüche der Rechteinhaber. Es steht den Mitgliedstaaten jedoch frei, zivilrechtliche Auskunftsansprüche zu schaffen. Dies wird an Art. 13 Abs. 1 lit. g) der Datenschutzrichtlinie 95/46/EG deutlich, der ermöglicht, das Datenschutzniveau herabzusenken, sofern Rechte anderer Personen dies erfordern. Art. 15 der Datenschutzrichtlinie für elektronische Kommunikation 2002/58/EG muss daher im Zusammenhang mit Art. 13 Abs. 1 lit. g) gelesen werden. Die beiden Normen erlauben so eine Einschränkung der datenschutzrechtlichen Bestimmungen zugunsten des Schutzes der Urheberrechte. Entscheidend ist daher stets die nationale Rechtsordnung des jeweiligen Mitgliedstaats.

Ungeachtet des Art. 4 Satz 1 der Vorratsdatenspeicherungsrichtlinie 2006/24/EG gab es Medienberichten zufolge Bestrebungen des österreichischen Justizministeriums, die aufgrund der Pflicht zur Vorratsdatenspeicherung bereit gehaltenen Daten einem Auskunftsanspruch von Rechteinhabern zu unterwerfen.[54] Die datenschutzrechtlich brisante „anlasslose Speicherung" von Verkehrsdaten würde hierdurch zugunsten der Verfolgung von Urheberrechtsverstößen erweitert. Eine solche Ausweitung steht in Konflikt mit Art. 4 Satz 1 der Vorratsdatenspeicherungsrichtlinie 2006/24/EG, der eine Weitergabe der auf Vorrat gespeicherten Daten an die zuständigen Behörden und somit nicht an private Dritte vorsieht. Die weitere Entwicklung des Gesetzgebungsverfahrens bleibt abzuwarten. Dieses ist – wohl im Lichte des beim EuGH anhängigen Verfahrens zur Überprüfung der Rechtmäßigkeit der Vorratsdatenspeicherungsrichtlinie[55] – ins Stocken geraten.

53) Oberster Gerichtshof. Entscheidung vom 14. Juli 2009, s. Yliniva-Hoffmann, A., IRIS 2009-9/7.
54) http://akvorrat.at/Ausweitung_der_Vorratsdatenspeicherung_BMJ_lehnt_Dialog_mit_BuergerInnen_ab.
55) Vorabentscheidungsersuchen des High Court of Ireland (Irland), eingereicht am 11. Juni 2012, Rechtssache C-293/12, zur gemeinsamen Entscheidung verbunden mit dem Vorabentscheidungsersuchen des Verfassungsgerichtshofs (Österreich), eingereicht am 19. Dezember 2012, Rechtssache C-594/12.

3. Verhältnismäßigkeit der nationalen Auskunftsansprüche

Der EuGH hat mit seinen Urteilen im Konfliktfeld von Datenschutz und Urheberrecht stets betont, dass ein sachgerechter Ausgleich zwischen den gegenüberstehenden Grundrechten geschaffen werden muss. Um eine solche Verhältnismäßigkeit eines Auskunftsanspruchs zu gewährleisten, bedienen sich die Mitgliedstaaten verschiedener Kriterien. Es bedarf in der Regel besonderer Voraussetzungen, um einen Auskunftsanspruch gegen die Intermediäre wider datenschutzrechtliche Interessen durchzusetzen.

Eine häufig herangezogene Voraussetzung zur Geltendmachung eines Auskunftsanspruchs ist bereits in der Durchsetzungsrichtlinie 2004/48/EG angelegt. Art. 8 verlangt für die Geltendmachung ein „gewerbliches Ausmaß" der Urheberrechtsverletzung. Nur wenn die Handlung des Verletzers durch „unmittelbare oder mittelbare wirtschaftliche oder kommerzielle Vorteile" motiviert ist, soll ein Auskunftsanspruch greifen können. Hierdurch können insbesondere solche Handlungen ausgeschlossen werden, die der einzelne Endverbraucher in gutem Glauben vorgenommen hat.[56]

Dieser Gedanke findet sich in den nationalen Rechtsordnungen wieder. Der deutsche Auskunftsanspruch verlangt ein solches gewerbliches Ausmaß der Rechtsverletzung[57] sowie zusätzlich eine Überprüfung der Verhältnismäßigkeit in jedem Einzelfall und grundsätzlich eine richterliche Anordnung der Auskunft.[58] Ähnliches gilt in Österreich, dessen Auskunftsanspruch[59] sich nach dem Urteil des Obersten Gerichtshofs vom 14. Juli 2009 nicht auf Daten erstreckt, die der Löschungspflicht unterliegen. Der österreichische Auskunftsanspruch erfordert darüber hinaus eine schriftliche und ausreichend begründete Geltendmachung des Auskunftsanspruchs, wodurch der massenhaften Erhebung von Auskunftsansprüchen vorgebeugt wird. Ähnlich gelagert ist die Situation beim schwedischen Auskunftsanspruch,[60] der stets einer richterlichen Anordnung bedarf: Über die hinreichende Begründung hinaus muss auch dargelegt werden, dass die zivilrechtliche Verfolgung der Urheberrechtsverletzung durch die begehrte Auskunft wesentlich erleichtert wird. Allen genannten Ansprüchen gemein ist die für Deutschland bereits erwähnte Klausel, die eine Überprüfung der Verhältnismäßigkeit der Auskunft in jedem Einzelfall verlangt.[61]

4. Pflicht der Intermediäre zur Einrichtung von Filtersystemen

Das Urheberrecht hat seine Reibungspunkte mit dem Schutz personenbezogener Daten nicht nur bei der Problematik der Auskunftsansprüche. Die nationalen Rechtsordnungen haben alternative Modelle zur Durchsetzung des Urheberrechts im Online-Sektor geschaffen. In zwei Verfahren – beide angestrengt von der belgischen Verwertungsgesellschaft *Société d'Auteurs Belge – Belgische Auteurs Maatschappij* (SABAM) – hatte der EuGH über die unionsrechtliche Vereinbarkeit von Filteranordnungen zu befinden.[62]

In der Rechtssache *Scarlet Extended*[63] ging es um die gerichtlich angeordnete allgemeine und vorsorgliche Verpflichtung eines Internetzugangsproviders, mit Hilfe seiner Dienste über Peer-to-Peer-Programme begangene Urheberrechtsverletzungen durch die Einrichtung von Filtersystemen

56) Erwägungsgrund 14 der Durchsetzungsrichtlinie 2004/48/EG.
57) Nach dem Urteil des Bundesgerichtshofs vom 19. April 2012 (Az. I ZB 80/11) reicht es indes auch, wenn die für die rechtsverletzende Tätigkeit genutzte Dienstleistung vom Intermediär in gewerblichem Ausmaß erbracht wird.
58) § 101 des deutschen Urheberrechtsgesetzes.
59) § 87b des österreichischen Urheberrechtsgesetzes.
60) Art. 53c des *Lag (1960:729) om upphovsrätt till litterära och konstnärliga verk* (Gesetz über Urheberrechte an literarischen und künstlerischen Werken).
61) Näher zu den genannten und den entsprechenden Vorschriften in weiteren EU-Mitgliedstaaten Kuner, C./Burton, C./Hladjk, J./Proust, O., Study on Online Copyright Enforcement and Data Protection in Selected Member States, November 2009, abrufbar unter http://ec.europa.eu/internal_market/iprenforcement/docs/study-online-enforcement_en.pdf
62) S. hierzu ausführlich Angelopoulos, C., Filterung des Internets nach urheberrechtlich geschützten Inhalten in Europa, IRIS *plus* 2009-4.
63) EuGH, Rs. C-70/10, *Scarlet Extended*, Urteil vom 24. November 2011; s. Angelopoulos, C., IRIS 2011-6/2; IRIS 2012-1/2.

zu verhindern. Die Rechtssache *Netlog NV*[64] betraf die Verpflichtung eines Betreibers eines sozialen Netzwerks, den Nutzern dieses Netzwerks den Austausch musikalischer und audiovisueller Werke auf ihren jeweiligen Profilseiten zu unterbinden.

In beiden Urteilen stellte der EuGH fest, derartige Verpflichtungen würden die Adressaten zur Errichtung eines Filtersystems zwingen. Dies bedeute eine aktive Überwachung sämtlicher Daten jedes einzelnen Nutzers. Sodann bringt der Gerichtshof mehrere Grundrechte ins Spiel, die es bei der Durchsetzung eines anderen Grundrechts – nämlich des Rechts am geistigen Eigentum (Art. 17 der Grundrechte-Charta) – zu berücksichtigen gilt: Für die jeweiligen Dienstleister ergeben sich Überschneidungen mit dem Schutz der unternehmerischen Freiheit (Art. 16 der Charta); bei den Nutzern erfolgt ein Eingriff in die Informationsfreiheit (Art. 11) und – wie bereits mehrfach angesprochen – in das Recht auf den Schutz personenbezogener Daten (Art. 8).

In beiden Fällen entschied der EuGH nach einer gründlichen Abwägung zu Ungunsten der Verwertungsgesellschaft. Eine von konkreten Inhalten losgelöste Überwachungspflicht sei mit Art. 15 der E-Commerce-Richtlinie 2000/31/EG nicht mehr vereinbar. Mit Blick auf die Dienstleister sei es nicht verhältnismäßig, sie zu zwingen, ein kompliziertes, kostspieliges, auf Dauer angelegtes und allein auf deren Kosten betriebenes Filtersystem einzurichten. Die Grundrechte der Nutzer waren aus datenschutzrechtlichen Gründen höher einzustufen, dies vor allem angesichts der Möglichkeit, Urheberrechtsverletzer durch die Ermittlung und Verarbeitung der IP-Adressen bzw. der Informationen zu den betroffenen Nutzerprofilen zu identifizieren. Bei vorsorglich eingebauten Filtersystemen erfolgt diese systematische Analyse personenbezogener Daten bei jedem Nutzer ohne konkrete Anhaltspunkte einer Urheberrechtsverletzung. Zudem wird nach Ansicht des EuGH die Informationsfreiheit dadurch beeinträchtigt, dass ein solches Filtersystem möglicherweise nicht hinreichend zwischen einem zulässigen und einem unzulässigen Inhalt unterscheiden könne. Unter Umständen führe dies zur Sperrung zulässiger Inhalte: Man denke etwa an gesetzliche Ausnahmen vom Urheberrecht wie zulässige Privatkopien sowie gemeinfreie oder verwaiste Werke.

5. Internetzugangssperren – nationale Ausgestaltungen

Die Mitgliedstaaten der Europäischen Union haben weitere Alternativen zum direkten Auskunftsanspruch des Rechteinhabers gegen den Zugangsprovider auf Auskunft über die personenbezogenen Daten des Rechtsverletzers geschaffen. Aus datenschutzrechtlicher Sicht sind diese Modelle „schonender", soweit der Rechteinhaber nicht ohne weiteres an die personenbezogenen Daten des vermeintlichen Urheberrechtsverletzers gelangt. Stattdessen werden Verfahren zwischengeschaltet, die häufig plakativ als „Three-Strikes-Verfahren" bezeichnet werden und als *ultima ratio* in der Regel eine temporäre Internetzugangssperre vorsehen. Mag das Ausmaß der Verarbeitung personenbezogener Daten dabei geringer sein, so sind die Eingriffe insbesondere in die Informations- und Meinungsfreiheit deutlich intensiver.[65]

5.1. Frankreich: HADOPI

Einen eigenen Weg bei der Verfolgung von Urheberrechtsverletzungen geht seit 2010 Frankreich und bietet damit auch aus datenschutzrechtlicher Sicht Besonderheiten. Mit der Einrichtung der *Haute Autorité pour la diffusion des oeuvres et la protection des droits sur l'Internet* (HADOPI) wurde in Frankreich eine eigene Behörde mit rund 60 Mitarbeitern geschaffen, die sich der Verfolgung von Urheberrechtsverletzungen im Internet widmet.[66] Die HADOPI wird entweder bei Anrufung durch einen Rechteinhaber (meist Berufsinteressenvertretungen, Verwertungsgesellschaften wie die *Société des Auteurs, Compositeurs et Éditeurs de Musique* – SACEM, das *Centre national de la cinématographie*) oder bei Aufforderung durch die Staatsanwaltschaft tätig. Der Rechteinhaber übermittelt der HADOPI dabei den Zeitpunkt einer Urheberrechtsverletzung, die dabei verwendete IP-Adresse, Informationen über die urheberrechtlich geschützten Werke und über

64) EuGH, Rs. C-360/10, *Netlog NV*, Urteil vom 16. Februar 2012; s. Breemen, K., IRIS 2012-3/3.
65) Kritisch etwa die Organisation für Sicherheit und Zusammenarbeit in Europa (OSZE); s. Stone, M., IRIS 2012-2/1.
66) Blocman, A., IRIS 2010-9/24.

den Internetzugangsprovider. Die HADOPI kann daraufhin vom Zugangsprovider die Übermittlung der persönlichen Daten des mit der IP-Adresse verknüpften Nutzers (Name, Telefonnummer, Emailadresse, Postanschrift) verlangen.

Im ersten Schritt erhält der vermeintliche Urheberrechtsverletzer eine E-Mail mit der Aufforderung zur Stellungnahme, im zweiten Schritt ein postalisches Einschreiben. Stößt die HADOPI ein drittes Mal auf denselben Verletzer, kann die Behörde ein vereinfachtes Gerichtsverfahren einleiten, das Sanktionen wie Geldstrafen vorsieht. In den ersten drei Jahren des Bestehens der Behörde war zudem die Sanktion einer – vielfach kritisierten – zeitweisen Sperrung des Internetzugangs vorgesehen. Die Möglichkeit der Zugangssperre wurde – nicht zuletzt infolge des zwischenzeitlichen Regierungswechsels in Frankreich – am 9. Juli 2013 aufgehoben.[67] Sie war zuvor bereits Gegenstand juristischer Auseinandersetzungen. Die ursprüngliche Befugnis der HADOPI, Zugangssperren selbst zu verhängen, erklärte der französische *Conseil constitutionel* (Verfassungsrat) für verfassungswidrig und hob sie auf.[68] Folgerichtig besserte der Gesetzgeber nach, sodass das Gesetz für die Verhängung einer Zugangssperre nun die Anrufung eines Gerichts durch die HADOPI verlangt.[69] In der gesamten Zeitspanne, innerhalb derer eine Internetsperre rechtlich möglich war, kam es indes nur in einem einzigen Fall zur Verhängung dieser Sanktion.[70] Zudem äußerten einige Zugangsprovider zu Beginn Bedenken hinsichtlich der Versendung der Verwarnungs-Emails der HADOPI und weigerten sich, diese an die jeweiligen Nutzer weiterzuleiten. Der französische Gesetzgeber reagierte insoweit und schuf eine gesetzliche Pflicht zur Weiterleitung der Emails. Bei Nichtbeachtung droht dem Zugangsprovider nun ein Bußgeld in Höhe von EUR 1.500.[71]

Mit Blick auf datenschutzrechtliche Anforderungen sieht das französische Recht vor, dass die persönlichen Daten nur der *Commission de protection des droits* bekannt werden, dem Gremium innerhalb der HADOPI, das die Eingaben von Rechteinhabern prüft. Insoweit zeigt sich das Verfahren bei der HADOPI zumindest aus datenschutzrechtlicher Sicht milder als ein allgemeiner Auskunftsanspruch gegen Intermediäre, da die persönlichen Informationen zunächst nur einem Teil einer staatlichen Behörde vorliegen. Beim Modell eines direkten Auskunftsanspruchs gegen den Zugangsprovider hat grundsätzlich jeder private Rechteinhaber potentiell Zugriff auf die persönlichen Informationen der Endnutzer. Gelangt der Rechteinhaber an diese personenbezogenen Daten, ist deren weitere Verwendung beim Rechteinhaber ungewiss. Das HADOPI-Verfahren belässt die personenbezogenen Daten zunächst in den Händen einer staatlichen Behörde, die sie in einem institutionalisierten Verfahren verarbeitet. Das in vielerlei Hinsicht heftig kritisierte Verfahren der HADOPI ist somit datenschutzfreundlicher ausgestaltet als die Einrichtung eines direkten Auskunftsanspruchs, zumal die HADOPI zur Löschung der Daten innerhalb bestimmter Fristen gesetzlich verpflichtet ist.[72]

Die HADOPI soll nach kritischen Forderungen wegen ihrer ineffizienten Arbeitsweise zwar aufgelöst werden, das Verfahren an sich soll jedoch grundsätzlich beibehalten und mit leichten Änderungen dem *Conseil supérieur de l'audiovisuel* (CSA), der Medienaufsichtsbehörde, übertragen werden.[73]

---

67) Décret nº 2013-596 du 8 juillet 2013 supprimant la peine contraventionelle complémentaire de suspension de l'accès à un service de communication au public en ligne et relatif aux modalités de transmission des informations prévue à l'article L. 331-21 du code de la propriété intellectuelle; abrufbar unter http://de.scribd.com/doc/152648389/joe-20130709-0157-0060

68) Urteil Nr. 2009-580 DC vom 10. Juni 2009; s. Blocman, A., IRIS 2009-7/20; s. auch IRIS 2010-9/24.

69) Die Notwendigkeit einer richterlichen Anordnung folgert der *Conseil d'Etat* aus Art. 6 EMRK, dem Recht auf ein faires Verfahren. Art. 6 verlangt ein Gerichtsverfahren bei Sanktionen gleich welcher Art. Während die Kontaktaufnahme durch HADOPI zur Meldung einer Urheberrechtsverletzung noch nicht als Sanktion und auch nicht als Beschuldigung gewertet werden kann, ist dies für die Verhängung einer Zugangssperre definitiv der Fall. Die Entscheidung vom 19. Oktober 2011 ist in französischer Sprache abrufbar unter www.conseil-etat.fr/fr/communiques-de-presse/decrets_hadopi.html; s. auch Blocman, A., IRIS 2011-10/15.

70) So die einschlägigen Medienberichte; s. www.pcinpact.com/news/80487-hadopi-600-d-amende-et-quinze-jours-suspension-pour-abonne.htm

71) Blocman, A., IRIS 2010-10/30.

72) Zwei Monate nach der Meldung durch einen Rechteinhaber etc., wenn keine Warnung erfolgt. Bei erster Warnung nach 14 Monaten, wenn keine zweite erfolgt. Bei zweiter Warnung 20 Monate, sofern keine erneuten Urheberrechtsverletzungen erfolgen.

73) Blocman, A., IRIS 2013-6/19.

Auf unionsrechtlicher Ebene finden sich ähnliche Konzepte im so genannten Gallo-Bericht des Europäischen Parlaments wieder.[74] Darin werden stärkere Sanktionen für Urheberrechtsverletzungen im Online-Bereich gefordert, da die Rechtsordnung allein mit zivilrechtlichen Schadensersatzansprüchen der Lage nicht Herr werde.[75] Der Bericht hebt gleichwohl die besondere Bedeutung des Datenschutzes hervor, die bei der Einrichtung von Sanktionen zu berücksichtigen sei.

5.2. Vereinigtes Königreich: Digital Economy Act

Ein ähnliches Modell wie in Frankreich wird auch im Vereinigten Königreich praktiziert. So sehen §§ 124A–124N des *Communications Act 2003* (eingefügt durch den *Digital Economy Act 2010*) ein umfangreiches Verfahren vor, das es den Rechteinhabern ermöglicht, Internetzugangsprovider, die einen von der britischen Regulierungsbehörde, dem *Office of Communications* (Ofcom) auszuarbeitenden Grundpflichtenkodex (*initial obligations code*) unterzeichnet haben,[76] über Urheberrechtsverletzungen zu informieren und sie anzuweisen, ihre Kunden davon in Kenntnis zu setzen. Erreichen die Meldungen zu einem bestimmten Nutzer eine im Grundpflichtenkodex festzulegende Mindestanzahl, sind die Internetzugangsprovider verpflichtet, diese in einer anonymisierten Liste (*copyright infringement list*) festzuhalten.[77] Auf Anfrage muss die Liste oder Teile derselben in einer datenschutzrechtlich gebotenen anonymen Form an die Rechteinhaber herausgegeben werden.

Auf Grundlage dieser Liste können die Rechteinhaber im Wege einer gerichtlichen Verfügung die Offenlegung der jeweiligen persönlichen Informationen verlangen, um den Urheberrechtsverletzer sodann auf Schadensersatz in Anspruch nehmen zu können. Nach Absatz 33 bis 35 der *Explanatory Notes* kann der *Secretary of State* die Verpflichtung der Zugangsprovider zu weiteren technischen Maßnahmen vorsehen, falls sich das Listenverfahren (allein) als nicht ausreichend erweisen sollte.[78] Dabei werden Internetsperren in den Formen der Bandbreitenbegrenzung oder der vorübergehenden Vollsperrung ausdrücklich in Betracht gezogen.

Die beiden britischen Zugangsprovider *British Telecommunications Plc* und *TalkTalk Telecom Group Plc* gingen gerichtlich gegen diese Bestimmungen vor und machten umfangreiche Verstöße gegen EU-Recht geltend.[79] Unter anderem trugen sie vor, der *Digital Economy Act* sei mit der Datenschutzrichtlinie für elektronische Kommunikation 2002/58/EG unvereinbar. Der *England and Wales High Court (Administrative Court)* verneinte mit seinem Urteil vom 20. April 2011 jedoch einen solchen Datenschutzverstoß, da die Verarbeitung der personenbezogenen Daten zur Erfüllung einer rechtlichen Verpflichtung und zur Achtung des Rechts auf Eigentum erforderlich sei und der Verwirklichung eines berechtigten Interesses (hier der ökonomischen Interessen der Rechteinhaber) diene. Die Verarbeitung der Daten sei somit von Art. 7 lit. c), e) und f) sowie Art. 8 und 15 der Datenschutzrichtlinie 95/46/EG gedeckt.

Auch einen behaupteten Verstoß gegen Art. 12 der E-Commerce-Richtlinie 2000/31/EG bestätigte das Gericht nicht. Die Zugangsprovider würden auf der Grundlage der angefochtenen Bestimmungen nicht für Inhalte haften, sondern lediglich Rechtsverletzungen dokumentieren

74) Entschließung des Europäischen Parlaments vom 22. September 2010 zur Durchsetzung von Rechten des geistigen Eigentums im Binnenmarkt (2009/2178(INI)); abrufbar unter www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+TA+P7-TA-2010-0340+0+DOC+PDF+V0//DE

75) Eine ähnliche Stoßrichtung liegt dem gescheiterten Vorschlag vom 12. Juli 2005 für eine Richtlinie des Europäischen Parlaments und des Rates über strafrechtliche Maßnahmen zur Durchsetzung der Rechte des geistigen Eigentums zugrunde, KOM(2005)276 endgültig, abrufbar unter http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52005PC0276%2801%29:DE:HTML

76) Die Ofcom veröffentlichte im Juni 2012 einen Entwurf dieses Kodex und startete gleichzeitig eine einmonatige Konsultation (abrufbar unter http://stakeholders.ofcom.org.uk/binaries/consultations/online-notice/summary/notice.pdf); eine endgültige Verabschiedung des Kodex ist bislang jedoch noch nicht erfolgt.

77) §§ 124A–124N des *Communication Act 2003*.

78) Die *Explanatory Notes* zum *Digital Economy Act 2010* sind abrufbar unter www.legislation.gov.uk/ukpga/2010/24/notes/contents?view=plain

79) S. hierzu im Einzelnen Prosser, T., IRIS 2011-6/20.

und Rechteinhabern Auskunft erteilen. Das Verbot einer Überwachungspflicht der Provider nach Art. 15 der E-Commerce-Richtlinie sei ebenso wenig verletzt, da nicht die Zugangsprovider selbst die Tätigkeit überwachten, sondern lediglich die Eingaben der Rechteinhaber dokumentierten. Die Kläger blieben auch im Berufungsverfahren vor dem *England and Wales Court of Appeal (Civil Division)* erfolglos. Das Gericht schloss sich mit seiner Entscheidung vom 6. März 2012 den Ausführungen der Vorinstanz weitgehend an.[80]

Der *High Court* nahm auch eine ausführliche Grundrechtsprüfung vor, verneinte aber eine übermäßige Beschränkung des Rechts auf den Schutz personenbezogener Daten durch den *Digital Economy Act*, da das widerstreitende Recht auf Eigentum mindestens ebenso schutzwürdig sei. Es sei zudem keine gleichermaßen wirksame Maßnahme zum Schutz des geistigen Eigentums im Onlinebereich ersichtlich, die aus datenschutzrechtlicher Sicht milder wäre. Das Konzept des *Digital Economy Act* sei daher verhältnismäßig.

Wie das HADOPI-Modell birgt auch dieses System aus datenschutzrechtlicher Sicht den Vorteil, dass die personenbezogenen Daten des (vermeintlichen) Urheberrechtsverletzers zunächst nicht in die Hände privater Dritter gelangen. Das britische System geht sogar so weit, dass die Daten nicht einmal gegenüber einer Behörde offengelegt werden. Es erfolgt lediglich eine Dokumentation beim Zugangsprovider, die anonymisiert herausgegeben wird. Die sich hinter den IP-Adressen verbergenden persönlichen Informationen sind für die Rechteinhaber erst im Zuge eines Gerichtsverfahrens zugänglich. Hinzu kommt, dass sich das Verfahren gegenüber dem Nutzer transparent gestaltet, da dieser schon bei der ersten Meldung vom Zugangsprovider über das Verfahren informiert wird.

5.3. Irland: Selbstregulierung

Irland benutzt ein vergleichsweise staatsfernes Modell der Einbindung von Intermediären in die Verfolgung von Urheberrechtsverletzungen. Dort haben das größte irische Telekommunikationsunternehmen *Eircom* und irische Vertreter der vier großen Labels *EMI*, *Sony*, *Universal* und *Warner* infolge eines Rechtsstreits über die Offenlegung von Kundendaten ein „Three-Strikes-Protokoll" vereinbart.[81] Dieses beruht nicht auf einer gesetzlichen Grundlage, sondern allein auf einem Vergleich zwischen den Parteien.[82]

Nach dem Vergleich agiert *Eircom* gegenüber seinen Kunden in einem dreigestuften Verfahren. Nach der ersten Urheberrechtsverletzung erhält der Kunde eine Meldung von *Eircom*. Bei der zweiten Meldung wird die Internetsperre bereits angedroht und infolge der dritten Meldung in Kraft gesetzt.[83] Der irische Datenschutzbeauftragte schaltete sich in dieses Verfahren ein und erhob Bedenken hinsichtlich Art. 8 und 6 EMRK: Zum einen würde der mit dem Three-Strikes-Modell verbundene Umgang mit persönlichen Informationen die Privatsphäre der Nutzer verletzen. Darüber hinaus würde ein faires Verfahren umgangen, wenn ohne Einschaltung eines Gerichts die Straftat einer Urheberrechtsverletzung festgestellt und eine Sanktion verhängt würde. Diese Einwände wurden von den Gerichten jedoch verworfen.[84] Das Urheberrecht ist seinerseits durch die irische Verfassung geschützt und verdient entsprechenden Schutz. Im Gerichtsverfahren standen ansonsten formell-rechtliche Fragen im Vordergrund, so dass sich die Gerichte in vergleichsweise geringem Umfang mit dem Verhältnis von Urheberrecht und Datenschutzrecht auseinanderzusetzen hatten. Es ist andererseits auch naheliegend, in der irischen Konstellation die rechtliche Problematik eher

80) Prosser, T., IRIS 2012-5/22.
81) McGonagle, M., IRIS 2006-4/26.
82) Damit zeigt sich das irische Modell als innovativ im Sinne der Mitteilung der Kommission „Verbesserung der Durchsetzung von Rechten des geistigen Eigentums im Binnenmarkt" vom 11. September 2009, KOM(2009) 467 final, mit der die Kommission die einander gegenüberstehenden Interessensgruppen aufruft, durch freiwillige Vereinbarungen praxisnahe Lösungen zum Ausgleich von Urheberrecht und dem Schutz personenbezogener Daten herbeizuführen, wenngleich die Gruppe der Nutzer beim vorliegenden Vergleich nicht mitwirken konnte.
83) McGonagle, M., IRIS 2010-6/34.
84) McGonagle, M., IRIS 2012-8/29; zuletzt vom höchsten irischen Gericht, dem *Supreme Court*, mit Entscheidung vom 3. Juli 2013 bestätigt, abrufbar unter www.supremecourt.ie/Judgments.nsf/1b0757edc371032e802572ea0061450e/c9861b9cda79509b80257b9d004e9a7a?OpenDocument

bei der Einschränkung der Informationsfreiheit zu sehen: Die Internetsperren werden fernab einer gesetzlichen Grundlage oder behördlichen Beteiligung verhängt.

5.4. Spanien: Ley Sinde

Ein gänzlich anderes Modell wurde in Spanien eingerichtet. Die Sperren richten sich dabei weniger gegen den Endnutzer als vielmehr gegen die Plattform, mit deren Hilfe die Urheberrechtsverletzungen begangen werden.[85]

Durch das so genannte *Ley Sinde*[86] wurde ein Verfahren geschaffen, durch das Rechteinhaber Internetplattformen melden können, mit deren Hilfe Urheberrechte verletzt werden, insbesondere so genannte Peer-to-peer-Netzwerke. Eine Regierungskommission prüft sodann mögliche Schritte gegen die Betreiber der Plattform. Hält die Kommission die Beschwerde für berechtigt, leitet sie das Verfahren an ein Gericht weiter, das die Sperrung der betreffenden Webseite anordnen kann.

Im Vergleich zu den bisher vorgestellten nationalen Maßnahmen ist die spanische Variante aus Sicht des Endnutzers sicherlich die datenschutzrechtlich mildeste Form der Intervention zum Schutz von Urheberrechten. Die Sanktionsmaßnahmen richten sich hier zunächst allein gegen den Internetdienstleister. Präventive Maßnahmen wie die Sperrung einer Internetseite sind für den Endnutzer notwendigerweise mit einem geringeren Eingriff verbunden, da keine personenbezogenen Daten im Hinblick auf eine konkrete Verletzung gesammelt werden. Gleichwohl sind – wie immer bei derlei präventiven Maßnahmen – die Informations- und Meinungsfreiheit der Nutzer sowie die Interessen der Intermediäre betroffen.

6. Problematik bei entgeltlicher Nutzung

Die bislang dargestellten Fälle betrafen stets das Vorliegen einer urheberrechtswidrigen Nutzung und die daraufhin folgende Durchsetzung etwaiger Schadensersatzansprüche. Ein Konflikt von Datenschutz- und Urheberrecht kommt jedoch auch im Bereich legaler Nutzung in Betracht. So verlangt das Datenschutzrecht etwa von einem Video-on-Demand-Anbieter, dass er im Zusammenhang mit seinem Angebot personenbezogene Daten nur erhebt und verwendet, soweit es für die Abwicklung von Vertragsverhältnissen *erforderlich* ist.[87] Nicht erforderlich sind Angaben zum Geschlecht, zum akademischen Grad, die Telefonnummer oder sonstiges. Ein Mehr an Angaben ist möglich, in diesem Fall allerdings nur mit Einwilligung des Nutzers.[88] Das Datenschutzrecht verbietet es indes, den Zugang zu einem Dienst von der Einwilligung zur Erhebung und Verarbeitung bestimmter Daten abhängig zu machen. Ebenso kritisch ist aus datenschutzrechtlicher Sicht das so genannte Online-Profiling zu bewerten, bei dem z. B. anhand des Setzens von Cookies das Nutzerverhalten aufgezeichnet wird, um ihm so persönlich zugeschnittene Angebote präsentieren zu können. Die Urheberrechtsrichtlinie 2001/29/EG begreift derlei Informationssysteme als Chance zur zeitgerechten Wahrnehmung von Urheberrechten,[89] verlangt aber beim Einsatz solcher Systeme die Achtung der Privatsphäre der Endkunden im Sinne der Datenschutzrichtlinie 95/46/EG.

Ein hohes Datenschutzniveau ist für den Verbraucher und somit für die legale Verwertung von Urheberrechten im Online-Sektor von großer Bedeutung. Eine von IBM durchgeführte Studie ergab, dass 41 Prozent der Internetnutzer in Großbritannien und 56 Prozent in Deutschland vom Erwerb eines Produktes absehen, wenn Unsicherheit über die Verwendung der personenbezogenen

85) Letai, P., IRIS 2012-7/18; 2012-4/22; 2012-2/18.
86) *Real Decreto 1889/2011, de 30 de diciembre, por el que se regula el funcionamiento de la Comisión de Propiedad Intelectual.*
87) S. Art. 7 lit. b) der Datenschutzrichtlinie 95/46/EG bzw. Art. 6 Abs. 1 lit. b) DSGVO-E.
88) Daher findet sich bei der Registrierung bei Internetdienstleistern häufig die Unterscheidung zwischen Pflichtfeldern und freiwilligen Zusatzangaben.
89) Erwägungsgrund 57 der Urheberrechtsrichtlinie 2001/29/EG.

Daten besteht.[90] Ein datenschutzfreundliches Angebot kann sich in dieser Hinsicht als Triebfeder für die Online-Verwertung erweisen.

IV. Fazit

Mit seinen drei wesentlichen Urteilen zum Verhältnis von Urheberrecht und Datenschutzrecht (*Promusicae*, *LSG* und *Bonnier Audio*) hat sich der EuGH dem Konflikt zwischen den urheberrechtlichen Interessen der Rechteinhaber und den datenschutzrechtlichen Interessen der Nutzer gewidmet. Durch den „großzügigen Verweis" auf die Bedeutung des Verhältnismäßigkeitsgrundsatzes kann man den Urteilen wenig an greifbaren Maßstäben für die Auskunftsansprüche entnehmen. Es lässt sich zunächst lediglich festhalten, dass das Datenschutzrecht in der Anwendung einen Vorrang gegenüber den urheberrechtlichen Richtlinien genießt und die unionsrechtliche Zulässigkeit der Herausgabe von Daten und der Schaffung eines Auskunftsanspruchs letztlich stets auf der Abwägung der gegenüberstehenden Grundrechte, namentlich dem Eigentumsrecht einerseits und dem Recht auf den Schutz personenbezogener Daten andererseits beruht. Konkrete Vorgaben für diesen Abwägungsvorgang hat der EuGH mit keinem seiner einschlägigen Urteile geschaffen. Daneben bleibt offen, wie das in seiner unionsrechtlichen Ausgestaltung abstrakt formulierte Recht auf Auskunft in Art. 8 der Durchsetzungsrichtlinie 2004/48/EG und Art. 8 der Urheberrechtsrichtlinie 2001/29/EG konkret umgesetzt werden soll, ohne dass dabei die flankierenden Normen der Datenschutzrichtlinie 95/46/EG und der Datenschutzrichtlinie für die elektronische Kommunikation 2002/58/EG sowie die Haftungsprivilegien der E-Commerce-Richtlinie 2000/31/EG missachtet werden.

Die belgische Kanzlei *Hunton & Williams* stellte in ihrer im Auftrag der Generaldirektion Binnenmarkt und Dienstleistungen der Europäischen Kommission angefertigten Studie fest, dass diese Fragen auf europäischer wie auch nationaler Ebene in vielerlei Hinsicht unbeantwortet sind. Infolgedessen bestehe hinsichtlich des Auskunftsanspruchs gegen Intermediäre bei Urheberrechtsverletzungen ein sehr geringes Maß an Harmonisierung.[91] Es zeichnet sich derzeit nicht ab, dass die Europäische Union in diesem Bereich eine weitere Harmonisierung anstrebt. Zwar sind mit den Entwürfen zu einer Datenschutzgrundverordnung und dem Vorschlag zu einer Richtlinie über Verwertungsgesellschaften[92] umfassende Reformbemühungen in den einschlägigen Rechtsgebieten zu erwarten. Den Widerstreit von Urheber- und Datenschutzrecht lassen diese Reformen dem bisherigen Anschein nach jedoch weitgehend außer Acht und klären insbesondere keine Details zur Frage der Auskunftsansprüche von Rechteinhabern gegen Intermediäre.[93]

Die Alternative zu den Auskunftsansprüchen, nämlich die Möglichkeiten der Filtersysteme und vor allem Internetsperren zeigen sich aus datenschutzrechtlicher Perspektive bisweilen milder, bringen jedoch häufig massive Eingriffe in andere Rechte der Nutzer, aber auch der Intermediäre mit sich. Die Mitgliedstaaten sehen schon jetzt unterschiedliche Ansätze vor; es bleibt abzuwarten, ob sich ein System – und wenn ja welches – zur Durchsetzung von Urheberrechten im Online-Sektor langfristig durchsetzen wird.

90) IBM Multi-National Consumer Privacy Survey, 1999, S. 27, abrufbar unter ftp://www6.software.ibm.com/software/security/privacy_survey_oct991.pdf

91) *Kuner, C./Burton, C./Hladjk, J./Proust, O.*, Study on Online Copyright Enforcement and Data Protection in Selected Member States, November 2009, abrufbar unter http://ec.europa.eu/internal_market/iprenforcement/docs/study-online-enforcement_en.pdf

92) Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über kollektive Wahrnehmung von Urheber- und verwandten Schutzrechten und die Vergabe von Mehrgebietslizenzen für die Online-Nutzung von Rechten an Musikwerken im Binnenmarkt vom 11. Juli 2012, COM(2012) 372 final.

93) Stattdessen eröffnen sich auch neue Konfliktfelder. Exemplarisch sei auf die automatisierte Überwachung der lizenzkonformen Verwendung urheberrechtlich geschützter Werke verwiesen, s. Erwägungsgrund 27 und Art. 22 ff. des Vorschlags zur Richtlinie über die Verwertungsgesellschaften.

IRIS plus
2013-6 p.27

Jüngste geltende Rechtsprechung

Das Verhältnis zwischen Urheberrecht, Meinungsfreiheit und Privatsphäre ist derart konfliktträchtig, dass häufig schwer zu sagen ist, wann ein Recht Vorrang vor einem anderen haben sollte. In solchen Fällen ist es Aufgabe der Gerichte, die komplexen rechtlichen und technologischen Sachverhalte gleichsam mit dem Skalpell zu sezieren, bevor sie dann über Recht und Unrecht entscheiden. Dieser Abschnitt bietet Ihnen einen Überblick über Rechtssachen, die kürzlich von nationalen Gerichten verhandelt wurden, darunter so bekannte Internetdienste wie The Pirate Bay, VKontakte, YouTube oder Rapidshare. Die Entscheidungen zeigen nicht nur die Komplexität der Fragestellung, sondern auch, wie diese Rechtssachen nicht nur von Fall zu Fall, sondern auch von Land zu Land behandelt werden.

2013-6 p.28

Deutschland

BGH konkretisiert Prüfpflichten des File-Hosters "rapidshare"

Christian Lewke
Institut für Europäisches Medienrecht (EMR), Saarbrücken/Brüssel

Der Bundesgerichtshof (BGH) hat mit Urteil vom 15. August 2013 den Umfang der Sorgfaltspflicht des Anbieters eines file-hosting-Dienstes weiter konkretisiert und jenseits der Haftungsprivilegien in § 7 Abs. 2 und § 10 des Telemediengesetzes (TMG) bzw. Art. 14 Abs. 1, Art. 15 Abs. 1 der Richtlinie über den elektronischen Geschäftsverkehr (2000/31/EG) eine teilweise proaktive Prüfpflicht von Host-Providern verlangt.

Der Entscheidung liegt eine Klage der Gesellschaft für musikalische Aufführungs- und mechanische Vervielfältigungsrechte (GEMA) gegen den File-Hoster "Rapidshare" zugrunde. Die GEMA hatte eine große Zahl an bei Rapidshare gespeicherten Musiktiteln abgemahnt, der Provider aber hatte die Musiktitel nicht vollständig entfernt.

In dem Urteil bestätigt der BGH zunächst seine bisherige Rechtsprechung: Den Dienstanbieter treffe nach § 7 Abs. 2 TMG keine allgemeine Überwachungspflicht bezüglich von ihm lediglich gespeicherter Information. Es könne aber nach den konkreten Umständen des Einzelfalls eine Überwachungspflicht in Frage kommen.

Dienstanbieter, die von Nutzern bereitgestellte Informationen speichern, müssten die nach vernünftigem Ermessen von ihnen zu erwartenden Sorgfaltspflichten achten, um bestimmte Arten rechtswidriger Tätigkeiten aufzudecken.

Vorliegend sei das Geschäftsmodell von Rapidshare nicht von vornherein auf die Ermöglichung von Rechtsverstößen angelegt gewesen, da auch legale Nutzungsmöglichkeiten für den Dienst in Frage kämen. Eine anlasslose Überwachungspflicht sei somit nicht anzunehmen.

Es bestehe aber aus mehreren Gründen eine anlassbezogene Überwachungspflicht ab Kenntnis eines konkret abgemahnten Rechtsverstoßes, da Rapidshare durch eigene Maßnahmen die Gefahr einer rechtsverletzenden Nutzung seines Dienstes fördere. So sei die Häufigkeit von 100.000 Downloads bestimmter Dateien, mit der Rapidshare seinen Hostingdienst bewirbt, nur mit hochattraktiven, rechtswidrigen Inhalten zu erreichen. Die Attraktivität für illegale Nutzungen werde durch die Möglichkeit noch gesteigert, die Dienste anonym in Anspruch zu nehmen. Auch die zusätzliche, von der Downloadhäufigkeit abhängige Vergabe von Premium-Punkten an die Nutzer lasse sich als weiteres Indiz für eine Förderung massenhafter Rechtsverletzungen ansehen.

Es stellte sich daher Frage nach dem Umfang der anlassbezogenen Überwachungspflicht des File-Hosters. Mit bisheriger Rechtsprechung hatte der BGH festgestellt, dass es dem Dienstanbieter grundsätzlich zuzumuten sei, jedenfalls eine überschaubare Anzahl einschlägiger Link-Sammlungen auf bestimmte bezeichnete Inhalte zu überprüfen. Jetzt stellte der BGH darüber hinaus klar, dass auch bei einer großen Zahl von über 4800 Musikwerken dem Host-Provider eine regelmäßige Kontrolle der Linksammlungen zugemutet werden könne. Insoweit kann von einem Host-Provider zumindest die Verwendung eines Wortfilters verlangt werden.

Darüber hinaus sei Rapidshare auch verpflichtet, sich über allgemeine Suchmaschinen Kenntnis über weitere rechtsverletzende Links zu verschaffen. Der Hinweis auf vorgenommene allgemeine Präventivmaßnahmen (17-köpfiges "Abuse-Team", MD5-Filter, Lösch-Interfaces für Berechtigte) allein könne den Beklagten insofern nicht entlasten.

- Urteil des BGH vom 15. August 2013 (Az. I ZR 79/12)
  http://merlin.obs.coe.int/redirect.php?id=16700

IRIS 2013-9/9

OLG untersagt Rapidshare Zurverfügungstellung bestimmter Inhalte

Tobias Raab
Institut für Europäisches Medienrecht (EMR), Saarbrücken/Brüssel

Mit zwei Urteilen vom 14. März 2012 hat das Hanseatische Oberlandesgericht (OLG) dem Filehoster Rapidshare die Zurverfügungstellung bestimmter, urheberrechtlich geschützter Inhalte untersagt.

Die Richter schlossen sich damit der Auffassung des Landgerichts (LG) Hamburg an, welches in den vorinstanzlichen Urteilen sowohl den Begehren der Verlage Campus und De Gruyter als auch der Rechtsauffassung der Verwertungsgesellschaft GEMA bezüglich der Verantwortlichkeit und Pflichten von Rapidshare gefolgt war. Rapidshare darf seinen Nutzern somit weder die Sprachwerke der besagten Verlage noch Musikwerke aus dem Repertoire der GEMA zur Verfügung stellen.

Für die Prüfung der Störerhaftung stelle sich vorliegend die Frage, inwieweit Rapidshare für eine missbräuchliche Verwendung seines Dienstes verantwortlich sei und ob der Anbieter insofern eine „aktive Rolle" oder lediglich die Rolle eines „neutralen Vermittlers" einnehme. Hierbei stellte das Gericht zunächst fest, dass Rapidshare seine Nutzer zum maßgeblichen Zeitpunkt von seiner grundsätzlichen Ausrichtung her tendenziös zu Rechtsverletzungen beeinflusst habe und so für das Bereitstellen des Speicherplatzes und die Zuteilung von Links hafte. Erst hierdurch werde die spätere Urheberrechtsverletzung ermöglicht. Außerdem seien die bisher gegen die illegale Nutzung getroffenen Maßnahmen nicht ausreichend. Es genüge nicht, erst nach Hinweisen der Rechteinhaber gegen Urheberrechtsverletzungen vorzugehen und die Links zu löschen. Werde ein rechtswidriger Link gemeldet, müsse zudem auch das „Umfeld" des jeweiligen Links samt Seiten und ähnlichen Links gesucht und überwacht werden. Hierbei müsse Rapidshare auch aktuelle Entwicklungen im Auge behalten, um seiner „Marktbeobachtungspflicht" gerecht zu werden, und dürfe sich nicht nur auf bekannte Linklisten beschränken. Nur so könne eine Wiederholung der Rechtsverletzung wirksam verhindert werden. Da Rapidshare diese Aspekte nicht eingehalten habe, schloss sich das OLG im Ergebnis den vorinstanzlichen Urteilen an und untersagte dem Filehoster die Zurverfügungstellung der betroffenen Inhalte.

Allerdings wichen die Richter von ihrer bisherigen Rechtsprechung in zwei Punkten ab. So korrigierten sie ihre Auffassung, nach der eine Urheberrechtsverletzung bereits zum Zeitpunkt des Hochladens vorliege, da im Zeitalter des Cloud-Computing entsprechende Dienste auch und immer mehr als Speicher für erlaubte Kopien genutzt würden. Da sich Rapidshare in der Zeit zwischen den behandelten Klagen und der Urteilsverkündung am OLG zunehmend als „weitgehend neutraler Anbieter" seriöser Cloud-Computing-Dienste dargestellt habe, liege mittlerweile die früher vorgeworfene tendenziöse Ausrichtung zur Beeinflussung seiner Kunden zu rechtswidrigem Verhalten nicht mehr vor. Dennoch sei eine Störerhaftung von Rapidshare auch nach diesen Änderungen möglich, wenn auch nicht mehr aufgrund eben jener tendenziösen Beeinflussung der Nutzer. Der Grund hierfür liege nun darin, dass Rapidshare seinen Nutzern die anonyme Nutzung seiner Dienste ermögliche und sie so „aktiv" zu Urheberrechtsverletzungen animiere. Auch auf § 13 Abs. 6 Telemediengesetz (TMG), wonach Nutzer die Dienste der Anbieter anonym oder unter Pseudonym nutzen können müssen, könne sich Rapidshare nicht berufen. Das TMG sehe dies nämlich nur vor, soweit es „technisch möglich und zumutbar" sei, was „in Ansehung der Gefahrgeneigtheit des Geschäftsmodells der Beklagten hier ersichtlich nicht erfüllt" und weswegen eine Störerhaftung somit auch künftig potentiell gegeben sei.

- Pressemitteilung des Hanseatichen Oberlandesgerichts zum Urteil (Az. 5 U 87/09), 15. März 2012 http://merlin.obs.coe.int/redirect.php?id=15787

IRIS 2012-5/12

OLG verneint Anspruch gegen YouTube auf Herausgabe von Nutzerdaten

Anne Yliniva-Hoffmann
Institut für Europäisches Medienrecht (EMR), Saarbrücken/Brüssel

Laut Medienberichten hat das Oberlandesgericht (OLG) München am 17. November 2011 in einem Eilverfahren entschieden, dass YouTube nicht verpflichtet ist, Daten zur Identifizierung eines Nutzers, der urheberechtsverletzendes Material eingestellt hat, an den Rechteinhaber herauszugeben.

Im zugrunde liegenden Fall hatte ein YouTube-Nutzer Filmmaterial, das er offenbar durch das Abfilmen einer Kinoleinwand hergestellt hatte, auf dem Videoportal veröffentlicht. Hierdurch sah sich der betroffene Filmverleih in seinen Rechten verletzt und begehrte von YouTube die Entfernung des veröffentlichten Materials sowie Auskunft über die Identität des Nutzers. Ersterem kam YouTube unverzüglich nach, verweigerte jedoch die Herausgabe der Nutzerdaten.

Dem Auskunftsverlangen erteilte das OLG München nun ebenfalls eine Absage und bestätigte damit die Entscheidung der Vorinstanz. Zwar liege ein Verstoß gegen das Urheberrecht vor, jedoch fehle es an dem für den Auskunftsanspruch nach § 101 Urheberrechtsgesetz erforderlichen gewerblichen Ausmaß der unrechtmäßigen Handlungen. Die hierzu vom Antragsteller gemachten Angaben seien unzureichend, insbesondere gebe es keine Anhaltspunkte für die Annahme einer etwaigen Gewinnerzielungsabsicht des Nutzers.

Den Berichten zufolge erwägt der Filmverleih, seinen Anspruch im Hauptsacheverfahren weiter zu verfolgen.

• Beschluss des Oberlandesgericht München vom 17. November 2011 (Az. 29 U 3496/11)

IRIS 2012-1/21

Finnland

ISP-Antrag auf Zulassung der Berufung im Fall The Pirate Bay nicht zugelassen

Anette Alén-Savikko
Institut für internationales Wirtschaftsrecht/Universität Helsinki, Facing the Coordination Challenge/Communication Research Centre, Universität Helsinki

Am 29. Oktober 2012 hat der Oberste Gerichtshof Finnlands die Berufung des Telekommunikations- und IKT-Dienstleisters Elisa Corporation im Fall Pirate Bay (TPB) abgewiesen. Im Gefolge des TPB-Falls in Schweden war im Mai 2011 eine einstweilige Verfügung gegen Elisa vom *Tekijänoikeuden tiedotus- ja valvontakeskus ry* (Urheberrechtsinformations- und Antipiraterie-Zentrum - TTVK) im Namen der finnischen nationalen Gruppe des internationalen Verbands der Phonoindustrie (International Federation of the Phonographic Industry - IFPI) beantragt worden. Ziel war es, die Fortdauer von Urheberrechtsverletzungen zu unterbinden.

Der Antrag stützte sich auf § 60c des finnischen Urheberrechtsgesetzes (404/1961). Danach kann ein Gericht, das die Sache verhandelt, gemäß Absatz 1 auf Antrag des Rechteinhabers einen Vermittler damit beauftragen, die Zugänglichmachung von mutmaßlich urheberrechtsverletzendem Material für die Öffentlichkeit zu unterbinden (Unterlassungsverfügung). Diese Maßnahme muss im Hinblick auf die Rechte des mutmaßlichen Rechteverletzers, des Vermittlers und des Urhebers als angemessen

eingestuft werden können. Absatz 2 regelt die Situation, in der noch keine gerichtlichen Schritte gegen den mutmaßlichen Rechteverletzer unternommen wurden (siehe § 60b). In diesem Fall kann ein Gericht eine einstweilige Verfügung erlassen. Dies ist auch ohne Anhörung des mutmaßlichen Rechteverletzers möglich, wenn es aufgrund der Dringlichkeit des Falls als notwendig betrachtet wird. Die Verfügung bleibt dann bis auf Weiteres in Kraft. Dem mutmaßlichen Rechteverletzer muss unverzüglich Gelegenheit zur Anhörung gegeben werden, und das Gericht muss entscheiden, ob die Verfügung in Kraft bleibt oder aufgehoben wird (Absatz 3). Die Verfügung darf nicht das Recht Dritter einschränken, Nachrichten zu verbreiten und zu empfangen. Sie tritt in Kraft, wenn der Antragsteller dem Vollstreckungsbeamten die Sicherheit stellt. Die einstweilige Verfügung erlischt, wenn innerhalb eines Monats keine Klage eingereicht wurde (Absatz 4).

Am 26. Oktober 2011 entschied das Bezirksgericht Helsinki zugunsten von IFPI Finnland. Es wurde eine einstweilige Verfügung erlassen, und Elisa wurde unter Androhung einer Geldstrafe (EUR 100.000) verpflichtet, TPB-Domänen von ihren Servern zu nehmen und den Zugang zu von TPB verwendeten IP-Adressen zu sperren. Die Maßnahmen in Bezug auf die Abonnements wurden im Januar 2012 nach dem Vollstreckungsbescheid ergriffen. Elisa legte Berufung gegen das Urteil des Bezirksgerichts ein, doch das Berufungsgericht Helsinki revidierte es in seiner Entscheidung vom 15. Juni 2012 nicht. Die einstweilige Verfügung wurde angesichts der offensichtlichen Wirkungslosigkeit rechtlicher Maßnahmen und der Zugänglichkeit des mutmaßlichen Rechteverletzers als erforderlich erachtet. Das Gericht erklärte zudem, die einstweilige Verfügung könne längerfristig sein, wenn die Beklagten in der Hauptsache nicht vorgeladen werden können. Dies allein führe jedoch nicht zu einer unbegrenzten Dauer. Um eine Präzedenzentscheidung zu erwirken, beantragte Elisa schließlich die Zulassung der Berufung vor dem Obersten Gerichtshof, die jedoch nicht erteilt wurde.

- *Helsingin käräjäoikeuden päätös, 26/10/2011, No 41552* (Urteil des Bezirksgerichts Helsinki, 26. Oktober 2011, Nr. 41552)
  http://merlin.obs.coe.int/redirect.php?id=16227

- *Helsingin hovioikeuden päätös, 15/06/2012, No 1687* (Urteil des Berufungsgerichts Helsinki, 15. Juni 2012, Nr. 1687)

- *Korkeimman oikeuden päätös, 29/10/2012, No 2187* (Urteil des Obersten Gerichtshofs, 29. Oktober 2012, Nr. 2187)

IRIS 2013-1/18

Frankreich

Keine Haftung für Website, die über Deep-Linking Zugang zu Catch-up-TV-Sendungen anbietet

Amélie Blocman
Légipresse

Am 31. Oktober 2012 hat der *Cour de cassation* (Oberstes französisches Revisionsgericht) die Berufungsklage des französischen Medienkonzerns M6 gegen das Urteil des Berufungsgerichts zurückgewiesen, das sämtliche Anträge von M6 in einem Rechtsstreit zwischen der Betreibergesellschaft der Online-Plattform TV-replay.fr, die Catch-up-TV-Sendungen anbietet, und M6 abgelehnt hatte (siehe IRIS 2011-6/17). Der Betreiber der Sender M6 und W9 sowie der Videoabrufdienst M6replay und W9replay beanstandete insbesondere, dass Internetnutzer über TV-replay.fr durch sogenanntes Deep-Linking von Hypertext-Links direkten Zugang zu Programmen erhielten, statt zunächst auf die Startseiten von M6replay und W9replay geführt zu werden. M6 erklärte, es handle sich um eine Verletzung der allgemeinen Nutzungsrechte seiner Abrufdienste sowie um eine Verletzung der

Urheberrechte und seiner Rechte als Datenbankhersteller. Die von TV-replay praktizierte Verlinkung auf Video-Clips stelle unlauteren Wettbewerb und Trittbrettfahrertum dar.

Die oberste Gerichtsinstanz gab in einem ersten Schritt dem Berufungsgericht Recht, welches erklärt hatte, das einfache Hochladen der Allgemeinen Geschäftsbedingungen der Internetseiten M6 und W9, die über ein halb verdecktes Tab im unteren Bereich des Bildschirms abgerufen werden können, reiche nicht aus, um die Nutzer der angebotenen Dienste vertraglich zu binden. Auch aus dem Mahnschreiben der Gruppe M6 an die beklagte Betreibergesellschaft der Website TV-replay.fr mit der Aufforderung, die Allgemeinen Geschäftsbedingungen zu respektieren, ergebe sich für die Betreibergesellschaft keine vertragliche Verpflichtung, sich daran zu halten.

Das Oberste Revisionsgericht urteilte ferner, das Berufungsgericht habe zu Recht erklärt, dass die Produktionsgesellschaften von M6 als Rechteinhaber der ausgestrahlten Programme nicht gemeinsam eine Verletzung nicht näher bezeichneter Rechte für sich hätten beanspruchen können. Sie hätten es versäumt, die einzelnen Rechte jeder Gesellschaft an den Werken zu benennen, die die beklagte Gesellschaft auf ihrer Website tv-replay nach Ausstrahlung der Werke über die Fernsehsender zugänglich macht. Das Gericht lehnte zudem den Klagegrund mit Blick auf eine Verletzung der Rechte der Gruppe M6 als Hersteller von Datenbanken ab. Ferner stellte das Gericht fest, dass Nutzer der strittigen Internetseite über ein Navigationsfenster der Catch-up-TV-Internetseiten der Sender zu den von ihnen gesuchten Programmen geführt werden. Dieses Fenster eröffnet für sie den Zugang zu allen Funktionen der Websites sowie zu den Werbebannern. Das Berufungsgericht hatte daraus geschlossen, der Vorwurf des Umgehens des normalen Navigationsverfahrens sei nicht belegt und folglich sei auch der Vorwurf des Trittbrettfahrertums haltlos. Damit habe das Berufungsgericht, so das Revisionsgericht, sein Urteil korrekt begründet. Mit diesem Urteil endet der Rechtsstreit, bei dem nichtsdestoweniger die Frage offenbleibt, mit welchen Mitteln sich die Rechteinhaber gegen den Zugang zu ihren Inhalten über Hyperlinks zur Wehr zu setzen können.

- *Cour de cassation (1re ch. civ.), 31 octobre 2012 - Société Métropole Télévision* (Oberstes Revisionsgericht (1. Zivilkammer), 31. Oktober 2012 - Société Métropole Télévision)

IRIS 2013-1/19

Urteil des Obersten Revisionsgerichts: keine allgemeine Verpflichtung zur Netzkontrolle

Amélie Blocman
Légipresse

Am 12. Juli 2012 hat die 1. Zivilkammer der *Cour de cassation* (Oberstes Revisionsgericht) im Rahmen von drei wichtigen Urteilen das Pariser Berufungsgericht gerügt. Letzteres hatte den Diensten *Google Images* und *Google Vidéo* vorgeworfen, nicht die notwendigen Maßnahmen getroffen zu haben, die das erneute Hochladen von rechtswidrigen Bildern und Filmen verhindert hätten. Für die oberste Gerichtsinstanz wird mit einem derartigen Verbot das Unternehmen Google generell zur Netzkontrolle verpflichtet und ihm die Einrichtung zeitlich unbegrenzter Internetsperren in einer mit Blick auf das anvisierte Ziel unverhältnismäßigen Weise vorgeschrieben.

Das Oberste Revisionsgericht musste sich mit Streitsachen befassen, in denen Rechteinhaber (die Produzenten der Dokumentarfilme „Les Dissimulateurs" und „L'affaire Clearstream" sowie ein Fotograf) Google verklagt hatten, nachdem sie festgestellt hatten, dass auf Internetseiten, die über *Google Images* und *Google Vidéo* zugänglich waren, Links vorhanden waren, die kostenlosen Zugang zu den besagten Filmen gewährten. Die Filme konnten dort in ihrer gesamten Länge im Streaming-Verfahren angeschaut oder heruntergeladen werden und es bestand Zugang zum strittigen Foto. Das Berufungsgericht hatte die Auffassung vertreten, Google habe sich der schadenersatzpflichtigen Urheberrechtsverletzung (*contrefaçon*) schuldig gemacht, indem es Internetnutzern die Möglichkeit

bot, direkt auf den Internetseiten *Google Vidéo France* und *Google Images* die Videos und das strittige Foto, die auf Internetseiten Dritter ins Netz gestellt worden waren, anzusehen. Google habe zudem nicht die notwendige Sorgfaltspflicht walten lassen und ein erneutes Hochladen der Filme und des Fotos, die bereits als rechtswidrig gemeldet worden waren, nicht verhindert. Die Gesellschaft könne nicht die in Artikel 6. I. 2 der *Loi sur la confiance dans l'économie numérique* (Gesetz über das Vertrauen in die digitale Wirtschaft - LCEN) vom 21. Juni 2004 vorgesehene Haftungsbeschränkung für sich in Anspruch nehmen und sei folglich in dieser Sache haftbar. Google war gegen diese Urteile des Berufungsgerichts vor dem Obersten Revisionsgericht in Berufung gegangen. Die oberste Gerichtsinstanz erklärte in einem ersten Schritt, Google habe Internetnutzern tatsächlich die Möglichkeit geboten, über Links, die zu Internetseiten Dritter führten, die Filme auf ihren eigenen Seiten *Google Vidéo* bzw. das Foto auf *Google Images* anzuschauen. Das Berufungsgericht habe folglich zu Recht geschlossen, dass Google eine aktive Funktion nutze, durch die das Unternehmen Zugang zu Inhalten erhalte, die auf Internetseiten Dritter zugänglich seien. Dies ermögliche ihm eine direkte Wiedergabe auf den eigenen Websites für die eigenen Kunden. Das Berufungsgericht habe festgestellt, so die oberste Gerichtsinstanz, dass Google ohne Einwilligung der Rechteinhaber den Film auf seinen Internetseiten wiedergegeben habe, was den Tatbestand der Urheberrechtsverletzung erfülle. Die Gesellschaft habe folglich mehr als nur eine einfache technische Dienstleistung erbracht. Das Urteil des Berufungsgerichts sei somit korrekt begründet.

In einem zweiten Schritt jedoch widersprach das Oberste Revisionsgericht dem Berufungsgericht und hob dessen Urteile auf. Dabei berief es sich auf die Bestimmungen I.2, I.5 und I.7 von Artikel 6 des LCEN, die in den Urteilen des Berufungsgerichts nicht berücksichtigt worden seien. Vielmehr habe es in den Urteilsbegründungen geheißen, die klagenden Gesellschaften hätten keine Maßnahmen zur Verhinderung eines erneuten Hochladens getroffen. Für das Berufungsgericht habe dabei keine Rolle gespielt, dass die Filme und das Foto über andere Adressen als diejenigen zugänglich waren, die im Rahmen des ursprünglichen rechtswidrigen Tatbestands festgestellt worden waren. Laut Auffassung des Obersten Revisionsgerichts käme das Urteil des Berufungsgerichts, Google als Anbieter von Suchmaschinenleistungen dazu zu verpflichten, jegliches erneute Hochladen der rechtswidrigen Filme und des Fotos zu verhindern, auch dann, wenn das Unternehmen nicht durch eine weitere reguläre Meldung, die aber im LCEN vorgeschrieben ist, von derartigen Vorgängen in Kenntnis gesetzt worden sei, einer allgemeinen Verpflichtung gleich, generell die Bilder und Filme, die Google speichere, zu kontrollieren und auf rechtswidrige Wiedergaben zu prüfen. Dies habe zudem zur Folge, dass Google in einer mit Blick auf das anvisierte Ziel unverhältnismäßigen Weise vorgeschrieben werde, zeitlich unbegrenzte Internetsperren einzurichten.

- *Cour de cassation (1re ch. civ.), 12 juillet 2012 - Google c. Bach Films et a. (3 arrêts)* (Oberstes Revisionsgericht (1. Zivilkammer), 12. Juli 2012 - Google gegen Bach Films u. a. (3 Urteile))

IRIS 2012-8/24

TF1 scheitert mit seinen Klagen gegen YouTube

Amélie Blocman
Légipresse

Am 29. Mai 2012 hat das *Tribunal de grande instance* (Landgericht) von Paris in einem 34-seitigen Urteil die Klagen des französischen Fernsehsenders TF1 und seiner Tochtergesellschaften (der Sender LCI, TF1 Vidéo und TF1 International, die für die Herausgabe von Videos, den Erwerb und die Vermarktung der Rechte zuständig sind) gegen das Internet-Videoportal YouTube wegen illegaler Nachahmung, unlauteren Wettbewerbs und Parasitentums abgewiesen. Neben Sperrmaßen hatte der Sender Schadenersatz in Höhe von rund EUR 150 Mio. gefordert, weil YouTube auf seiner Plattform eine Reihe von Filmen, Serien, Sportereignissen und Übertragungen, deren Rechte TF1 für sich beanspruchte, online zur Verfügung gestellt hatte. In einigen Fällen sei die Onlineveröffentlichung vor jeglicher Ausstrahlung oder gewerblichen Nutzung in Frankreich erfolgt.

In einem ersten Schritt untersuchte das Gericht, ob die klagenden Gesellschaften die strittigen Inhalte ausreichend und korrekt zugeordnet und dabei jeden strittigen Inhalt separat auf der Grundlage der Eigenschaften besagter Gesellschaften sowie der vorgebrachten Rechtsgrundlage (Urheberrecht und verwandte Schutzrechte) geprüft hatten. Das Gericht kam hierbei zu dem Ergebnis, dass die klagenden Gesellschaften nicht den Nachweis hatten erbringen können, dass sie Inhaber der von ihnen beanspruchten Rechte sind. Anders als TF1 Vidéo behaupte, sei die Gesellschaft nicht Rechteinhaberin der Produzenten der strittigen Videogramme, da sie nur die Rechte für die Verwertung erworben habe und zudem auch kein Exklusivrecht nachweisen könne, das sie für sich beanspruche. Die Gesellschaft TF1 Droits audiovisuels ihrerseits könne je nach beanstandetem Werk entweder nicht den Nachweis erbringen, Produzentin des audiovisuellen Werkes oder Videogramms zu sein, oder nicht belegen, dass die anderen Ko-Produzenten in die Klage einbezogen worden seien bzw. dass sie deren Einwilligung eingeholt habe, alleine zu handeln. Die Klagen beider Gesellschaften wurden aus diesem Grunde als unzulässig abgewiesen. Mit Blick auf die Sender TF1 und LCI handle es sich laut Gericht um Unternehmen der audiovisuellen Kommunikation, so dass die Wiedergabe bzw. das öffentliche Bereitstellen ihrer Sendungen gemäß Artikel 216-1 des *Code de la propriété intellectuelle* (Gesetz über das geistige Eigentum - CPI) ihrer Einwilligung bedürfe. Allerdings verwies das Gericht darauf, dass keine Vermutungsregel für die Rechteinhaberschaft vorgesehen sei, die diesen Schutz gewährleiste. Es obliege demnach demjenigen, der das Recht für sich beanspruche, die Existenz des Programms zu belegen und nachzuweisen, dass er es bereits vor der Veröffentlichung durch YouTube ausgestrahlt habe. Im besagten Falle wurden die von den Sendern vorgelegten Dokumente (Programmlisten, Pressemitteilungen usw.) vom Gericht als unzureichend erachtet und die Klagen der Sender mit Ausnahme von sieben Sportereignissen, für die das Gericht die notwendigen Nachweise als erbracht ansah, auf der Grundlage von Artikel L. 216-1 des CPI abgewiesen. Das Gericht urteilte ferner, die Sender hätten, gestützt auf das Urheberrecht, nicht die Originalität der Programme (darunter die Fernsehnachrichten) nachweisen können, deren Veröffentlichung im Internet durch YouTube sie aber beanstandeten.

Nach Klärung der Frage der Rechtsinhaberschaft befasste sich das Gericht mit dem Status der Videoplattform. Gemäß dem in Frankreich inzwischen üblichen Schema erklärten die klagenden Gesellschaften, die Plattform habe den Status eines redaktionellen Anbieters von Inhalten (*éditeur*), insofern sie im Sinne von Artikel 6-1-2 der *Loi pour la confiance dans l'économie digitale* (Gesetz über das Vertrauen in die digitale Wirtschaft - LCEN) vom 21. Juni 2004 eine aktive Rolle bei den von den Nutzern ins Internet gestellten Inhalten spiele. YouTube sieht sich im Sinne von Artikel 6-1-2 LCEN als Host-Provider, somit als struktureller Anbieter von Inhalten (*hébergeur*). Das Gericht gab YouTube Recht; es stützte seine Begründung auf Bestimmungen des LCEN, auf die Position des Obersten Revisionsgerichts, die mit der des Gerichtshofs der Europäischen Union übereinstimmt, sowie auf die Nutzungsbedingungen des Dienstes zum Zeitpunkt, an dem das Verfahren eingeleitet worden war. Zudem verwies es auf die Zulässigkeit von Werbemaßnahmen für Host-Provider, ohne dass diese ihren Status verlieren. In Anwendung von Artikel 6 und 7 des LCEN prüfte das Gericht in einem weiteren Schritt die Vorwürfe gegen YouTube als Host-Provider. Es erinnerte daran, dass dieser einen strittigen Inhalt umgehend entfernen müsse, wenn ihm ein solcher gemeldet werde. Im besagten Falle habe die Plattform zu spät reagiert und Videos der sieben beanstandeten Sportereignisse frühestens nach fünf Tagen entfernt. Dieser Zeitraum könne nicht als „angemessen" eingestuft werden und sei somit unzulässig. Allerdings urteilte das Gericht in einer letzten Anmerkung zu diesem Punkt, die Bedingungen von Artikel L. 216-1 des CPI seien nicht erfüllt und es liege somit kein schuldhaftes Verhalten seitens YouTubes vor. Angesichts des kostenlosen Zugangs zur Website sei nämlich die Bedingung, laut derer für das Zugangsrecht ein Betrag entrichtet werden müsse, nicht erfüllt. Abschließend erklärte das Gericht, die Plattform habe am 16. Dezember 2011 ein Abkommen mit TF1 geschlossen, das dem Sender Zugang zum Dienst Content ID gewähre und damit dem Rechteinhaber die Möglichkeit biete, nach Meldung eines strittigen Inhalts das beanstandete Video zu entfernen. Die klagenden Gesellschaften hätten seitdem keine Verletzung gemeldet. Ist der Streit damit beigelegt? TF1 hat die Möglichkeit in Berufung zu gehen…

- *TGI de Paris (3e ch. 1re sect.), 29 mai 2012 - TF1, LCI et autres c/ Youtube* (TGI von Paris (3. Kammer, 1. Abteilung), 29. Mai 2012 - TF1, LCI u. a. gegen YouTube)
  http://merlin.obs.coe.int/redirect.php?id=15997

IRIS 2012-7/22

Strafe für unberechtigte Filmkopien auf einer Videoplattform

Amélie Blocman
Légipresse

Am 9. Mai 2012 fällte der Pariser *Cour d'appel* (Berufungsgericht) sein Urteil im Rechtsstreit zwischen den Produzenten des Films „Sheitan" und dem Videoportal Dailymotion. Der Sachverhalt: Fünf Einzelvideos, die zusammengenommen genau den Film ergeben, standen zum Abruf im Streaming-Verfahren auf der Plattform zur Verfügung, obwohl eine einstweilige Verfügung des Pariser *Tribunal de grande instance* (Landgericht - TGI) vorlag mit der Aufforderung, Daten zur Verfügung zu stellen, die eine Identifizierung der Person ermöglichen, welche die Videos rechtswidrig online gestellt hatte.

Das Pariser TGI hatte die Plattform am 11. Juni 2010 wegen rechtswidriger Vervielfältigung zu Schadensersatz in Höhe von EUR 15.000 (siehe IRIS 2010-7/19) verurteilt; dabei betrachtete das Gericht die Plattform als Host-Provider, was die Filmproduzenten in Abrede stellten. Das Gericht hatte der Gesellschaft aber trotzdem nicht zugestanden, sich auf die begrenzte Haftung nach Artikel 6-I-2 des Gesetzes vom 21. Juni 2004 zu berufen (*Loi pour la confiance dans l'économie numérique* - LCEN; Gesetz über das Vertrauen in die digitale Wirtschaft), weil sie die gefälschten Inhalte, auf die sie von den Produzenten hingewiesen wurde, nicht unverzüglich entfernt hatte. Zur Erinnerung: Laut Gesetz haften natürliche und juristische Personen, die im Internet Speicherplatz anbieten, nur dann nicht, „wenn sie bei Eingang von Hinweisen auf rechtswidrig bereitgestellte Inhalte unverzüglich reagieren und die Inhalte entfernen oder den Zugang dazu sperren". Die Plattform hatte gegen das Urteil Berufung eingelegt. In seinem Urteil vom 9. Mai 2012 stellt das Gericht fest, dass die Parteien sich im Gegensatz zur Vorinstanz und unter Berücksichtigung der zwischenzeitlich begründeten Rechtsprechung nunmehr einig waren, dass Dailymotion der vorgenannten Definition von Host-Providern entspreche, sofern diese Gesellschaft die Tätigkeit der öffentlichen Bereitstellung audiovisueller Inhalte (im konkreten Fall: persönliche Filme) verfolge, die von den Nutzern dieses Providers eingestellt werden, ohne dass dabei eine Prüfung der Inhalte möglich ist. Die Parteien einigten sich folglich darauf, die Haftung von Dailymotion nach den besonderen Bestimmungen des LCEN-Gesetzes zu bewerten, die auf den Bereitsteller von Speicherplatz Anwendung finden. Keine Übereinstimmung gab es jedoch in der Frage, ob die Plattform die mit dieser Eigenschaft verbundenen Auflagen erfüllt hat. Das Gericht erinnert an diese Pflichten und geht in seiner Würdigung in zwei Schritten vor. Nach Artikel 6-I-2 LCEN prüfte das Gericht zunächst, ob die Plattform die gegen die Urheberrechte verstoßenden Inhalte „unverzüglich" nach Inkenntnissetzung entfernt hat. Dabei stellten die Richter fest, dass die Plattform bereits am Tag des Eingangs der gerichtlichen Verfügung ein Schreiben an die Rechtsvertreter einer der klagenden Produktionsgesellschaften gerichtet hatte, das sämtliche Angaben und Daten (Zeitpunkt des Online-Stellens, IP-Adresse der einstellenden Person, statistische Angaben) zu den fünf beanstandeten Videos enthielt. Daher sei die - wie im Urteil vermerkt - „nicht ohne Spitzfindigkeit formulierte" Behauptung der Plattform, die in der gerichtlichen Verfügung aufgeführten Punkte hätten nicht ausgereicht, um die beanstandeten Inhalte zu identifizieren und lokalisieren, unhaltbar. Vielmehr habe sie nach erfolgter Inkenntnissetzung mehr als drei Monate Zeit verstreichen lassen, bis sie die beanstandeten Inhalte entfernt habe. Damit habe sie die für Anbieter von Speicherplatz geltende Pflicht, derartige Inhalte sofort zu entfernen, nicht erfüllt.

In einem zweiten Schritt weist das Gericht darauf hin, dass die Plattform der LCEN-Bestimmung, die das erneute Einstellen bereits enfternter Inhalte verbiete, nicht nachgekommen sei. Denn im Gegensatz zu dem, was Dailymotion zur Verteidigung vorbrachte, hätten sich die auf dem Portal nach der ersten Löschung noch verfügbaren Filmauszüge nicht von den zuvor entfernten Inhalten unterschieden. Sie stellten somit eine rechtswidrige Vervielfältigung desselben Werkes und einen Verstoß gegen die Schutzrechte für geistiges Eigentum dar.

Das Gericht bestätigte die Haftbarkeit von Dailymotion und vertrat gleichzeitig die Auffassung, dass der von den klagenden Produktionsgesellschaften erlittene Schaden in der Vorinstanz als zu gering angesetzt worden sei. Unter Berücksichtigung der Tatsachen, dass die rechtswidrigen Inhalte erst nach mehr als drei Monaten nach dem entsprechenden Hinweis entfernt und nach dem

Entfernen erneut eingestellt wurden und dass die Inhalte bis zur Löschung mehr als 12.000 Mal abgerufen wurden, verurteilte das Gericht Dailymotion zu einer Schadensersatzzahlung von jeweils EUR 30.000 (gegenüber 15.000 in der Vorinstanz) an jede Produktionsgesellschaft.

- *Cour d'appel de Paris (pôle 5, ch. 1), 9 mai 2012 - Dailymotion c. SARL 120 Films et La chauve-souris* (Pariser Berufungsgericht (Abteilung 5, Kammer 1) vom 9. Mai 2012 - *Dailymotion* vs. *SARL 120 Films* und *La chauve-souris*)

IRIS 2012-6/17

Vereinigtes Königreich

Oberster Gerichtshof fordert Internetdienstanbieter zu Sperrung des Zugangs zu Tauschseiten auf

Tony Prosser
School of Law, University of Bristol

In seinem Urteil vom 28. Februar 2013 hat der *High Court* (Oberster Gerichtshof) sechs führende Anbietern von Internetdiensten (ISPs), die einen Marktanteil von 94 Prozent bei den britischen Internetnutzern halten, auf, den Zugang zu drei Peer-to-Peer-Tauschbörsen namens KAT, H33T und Fenopy zu sperren. Vorangegangen waren Beschlüsse des Obersten Gerichtshofs mit der Aufforderung, andere Internetauftritte zu sperren (siehe IRIS 2012-7/25 und IRIS 2011-9/21).

Der Fall wurde von zehn führenden Plattenfirmen im eigenen Namen und im Namen weiterer Mitglieder der Handelsvereinigungen für Tonträger eingebracht. Die drei Websites betreiben jeweils ein umfangreiches rentables Geschäft mit Datentausch, insbesondere Musik. Artikel 97A des Gesetzes über Urheberrechte, Muster und Patente von 1988, welches die Informationsgesellschaftsrichtlinie umsetzt, ermächtigt den High Court, eine einstweilige Verfügung gegen einen Dienstanbieter zu erlassen, „wenn der Diensteanbieter tatsächlich Kenntnis davon hat, dass eine dritte Person seinen Dienst zur Verletzung von Urheberrecht nutzt". Der Gerichtshof war der Auffassung, die Nutzer der Websites mit Konten bei den Beklagten hätten sich am Tausch und somit an der nicht genehmigten Vervielfältigung von Aufzeichnungen beteiligt, und zwar in großem Maßstab. Das Material sei zudem an ein neues Publikum weitergegeben worden, und wenngleich die Unternehmen ihren Sitz außerhalb des Vereinigten Königreichs hätten, seien die Websites auf Großbritannien gerichtet gewesen. Der ganze Zweck jeder dieser Websites habe darin bestanden, das Kopieren zuzulassen. Wenngleich auf den Websites Erklärungen veröffentlicht worden seien, dass die Belegschaft gegen Piraterie sei, seien diese angesichts der Menge an zur Verfügung gestelltem urheberrechtsverletzendem Material, der unwirksamen Reaktionen auf die Aufforderungen, die Inhalte zu entfernen und der Schritte, die sie unternommen hatten, um Zwangsmaßnahmen zu vermeiden, jedoch nicht überzeugend gewesen. Sowohl Nutzer als auch Betreiber der Websites hätten die Dienste der Anbieter genutzt, um Urheberrechte zu verletzen, und die Anbieter seien wöchentlich über rechtsverletzende Aktivitäten informiert worden, hätten also tatsächlich davon Kenntnis gehabt; keiner der Anbieter bestritt, hiervon Kenntnis gehabt zu haben.

Der Gerichtshof war weiterhin der Ansicht, die Anordnungen seien in Abwägung der Eigentumsrechte der Antragsteller gegen das Recht auf freie Meinungsäußerung verhältnismäßig gewesen. In diesem Fall hatten die Diensteanbieter den Anordnungen zugestimmt und nicht versucht, sich mit der Begründung dagegen zu wehren, sie wären über Gebühr belastend oder kostenintensiv; sie könnten zwar umgangen werden, dennoch könnten sie gerechtfertigt sein, wenn sie nur einer Minderheit an Nutzern den Zugang verwehren. Es hatte sich gezeigt, dass derartige Anordnungen hinreichend wirksam sind. Die Anordnungen waren eng gefasst und zielgerichtet und sie waren notwendig und angemessen, um Rechte des geistigen Eigentums zu schützen. Dies überwog eindeutig das Recht

auf Meinungsfreiheit von Nutzern, die das Material über rechtmäßige Quellen beziehen können, und von Website-Betreibern, die Nutzen aus den Rechtsverletzungen zogen.

- *Emi Records and others v. British Sky Broadcasting Ltd and others, [2013] EWHC 379 (Ch)* (Emi Records und andere gegen British Sky Broadcasting Ltd und andere, [2013] EWHC 379 (Ch)) http://merlin.obs.coe.int/redirect.php?id=16413

IRIS 2013-5/29

High Court weist Internetdiensteanbieter an, den Zugang zu „The Pirate Bay" zu sperren

Tony Prosser
School of Law, University of Bristol

Am 2. Mai 2012 hat der *High Court* (oberster Gerichtshof) eine Verfügung nach dem *Copyright, Designs and Patents Act 1988* (Urheberrechts-, Muster- und Patentgesetz) erlassen, in der die großen Internetdiensteanbieter angewiesen werden, den Zugang ihrer Kunden zur Website der *Peer-to-Peer*-Tauschbörse „The Pirate Bay" zu sperren. Das Gesetz berücksichtigt in seiner novellierten Fassung die Richtlinie 2001/29/EG (Richtlinie zur Informationsgesellschaft). Das Verfahren war von Plattenfirmen in ihrem eigenen Namen und im Namen der *British Recorded Music Industry and Phonographic Performance Ltd*. angestrengt worden.

Nach dem Gesetz ist der *High Court* befugt, einstweilige Verfügungen gegen Diensteanbieter zu erlassen, die „unmittelbar Kenntnis" davon haben, dass eine dritte Person Dienste eines Anbieters nutzt, um gegen Urheberrechte zu verstoßen. Das Gericht hatte bereits im Zusammenhang mit der Website „Newzbin2" eine derartige Verfügung erlassen und in einer bereits zuvor ergangenen Entscheidung festgestellt, dass sowohl die Nutzer als auch die Betreiber von „The Pirate Bay" die Urheberrechte der Antragsteller verletzen (siehe IRIS 2011-9/21 und IRIS 2012-4/28). In vorliegenden Fall ging das Gericht davon aus, dass die ISPs unmittelbar Kenntnis von den Urheberrechtsverletzungen hatten, da dies von den Plattenfirmen entsprechend vorgebracht und in einem vorausgegangenen Urteil festgestellt worden war. Ein Erlassen dieser Verfügung steht nach Auffassung des Gerichts nicht im Widerspruch zu Artikel 10 der Europäischen Menschenrechtskonvention bzw. Artikel 11 der Charta der Grundrechte der EU. Die Verfügungen stellen ferner eine angemessene Reaktion dar, da ihre Bestimmungen von den Parteien, die berufsmäßig vertreten waren, ausgehandelt worden waren; weiter sind sie aus Gründen, die im Zusammenhang mit vorausgegangenen Fällen dargelegt worden waren, im Hinblick auf die Nutzer der ISP-Dienste angemessen. Damit konnten die Verfügungen ergehen, die IP-Adressen zu sperren. Dies war durchführbar, da sich „The Pirate Bay" keine Adresse mit anderen teilt.

- *Dramatico Entertainment et al v. Brisith Sky Broadcasting et al, [2012] EWHC 1152 (Ch)* (Dramatico Entertainment et al vs. British Sky Broadcasting et al, [2012] EWHC 1152 (Ch)) http://merlin.obs.coe.int/redirect.php?id=15944

IRIS 2012-7/25

2013-6 p.38

High Court verurteilt Internetdiensteanbieter zur Preisgabe personenbezogener Kundendaten an Pornofilm-Produktionsfirmen, die Urheberrechtsverletzungen geltend machen

Tony Prosser
School of Law, University of Bristol

Der englische *High Court* (oberster Gerichtshof) hat den Internetdiensteanbieter O2 zur Weitergabe der personenbezogener Daten von über 9000 Kunden an ein im Namen von Urheberrechtsinhabern handelndes Unternehmen und an eine Pornofilm-Produktionsfirma verurteilt und gleichzeitig ähnliche Klagen von zwölf weiteren Urheberrechtsinhabern abgewiesen.

Golden Eye International Limited, eine im Namen von Urheberrechtsinhabern handelnde Organisation, und 13 Pornofilm-Produktionsfirmen hatten eine so genannte „Norwich Pharmacal Order" beantragt. Mit dieser Anordnung wollen die Kläger O2 zur Herausgabe der personenbezogenen Daten von 9.124 O2-Kunden zwingen, um von ihnen jeweils GBP 700 Schadenersatz für mutmaßliche Urheberrechtsverletzungen zu verlangen und bei Nichtzahlung mit gerichtlichen Schritte und/oder der Drosselung oder Abschaltung des Internetdienstes zu drohen. In den vorgelegten Anordnungs- bzw. Abmahnungsentwürfen wurde zudem fälschlich behauptet, dass Rechnungsempfänger unabhängig davon, ob sie sie tatsächlich begangen haben oder nicht, für alle Urheberrechtsverletzungen haften, die über ihren Internetanschluss erfolgen. Diese Taktik ist als „spekulative Rechnungsstellung" bekannt und soll Verbraucher durch Einschüchterung zum Zahlen bewegen, ohne dass ein Gericht eingeschaltet werden muss. Der Antrag wurde an den High Court verwiesen. Aus der Erwägung, dass die von dem Antrag auf Datenpreisgabe betroffenen Internetnutzer nicht imstande sein würden, dagegen vorzugehen, ersuchte der Gerichtshof die Verbraucherorganisation Consumer Focus, die Interessen der Nutzer gerichtlich zu vertreten.

Der High Court wog zwischen den Interessen der Urheberrechtsinhaber und dem Recht der Kunden auf Privatsphäre und Datenschutz ab. In Bezug auf Golden Eye und zwölf der Urheberrechtsinhaber gelangte er zu dem Schluss, dass die Anordnung nicht ergehen dürfe, da dies der gerichtlichen Billigung einer Praxis gleich käme, bei der „das Recht der Beklagten auf Privatsphäre und Datenschutz an den Meistbietenden veräußert werde". Die Urheberrechtsinhaber hatten nämlich die Federführung über den Rechtsstreit an Golden Eye übertragen und dieser Firma im Erfolgsfall rund 75 % des Erlöses zugesagt. In Bezug auf Golden Eye und eine Produktionsfirma, Ben Dover Productions, die gemeinsam klagten, hielt das Gericht es für angemessen, die Offenlegung der persönlichen Angaben von Rechnungsempfängern anzuordnen, da einiges dafür spreche, dass viele der Beklagten das Urheberrecht verletzt hätten. Die geplante Anordnung und das Anschreiben an die Kunden müssten jedoch so formuliert werden, dass die rechtmäßigen Interessen von Verbrauchern - insbesondere derjenigen, die die mutmaßlichen Urheberrechtsverletzungen tatsächlich nicht begangen hätten, - angemessen geschützt seien. Der vorliegende Wortlaut der Schreiben sei in mehrfacher Hinsicht zu beanstanden. Vielmehr sollten Kunden, die Urheberrechtsverletzungen einräumten, zu näheren Angaben über ihre Tauschbörsennutzung aufgefordert werden, und anschließend sollten angemessene Einzelvergleiche ausgehandelt werden. Das Gericht wird eine zweite Anhörung durchführen, um entsprechende Vorgaben für den Wortlaut der Abmahnungen und der Anordnung festzulegen.

- *High Court (Chancery Division), Golden Eye (International) and another v. Telefonica UK Ltd [2012] EWHC 723 (Ch), 26 March 2012* (High Court (Chancery Division), Golden Eye (International) and another v. Telefonica UK Ltd [2012] EWHC 723 (Ch), 26. März 2012)
  http://merlin.obs.coe.int/redirect.php?id=15817

IRIS 2012-6/21

Internetdiensteanbieter verlieren Berufungsklage gegen Digital Economy Act

Tony Prosser
School of Law, University of Bristol

Die Internetdiensteanbieter BT und TalkTalk sind mit ihrer Berufungsklage gegen eine Entscheidung des *High Court* (Oberster Gerichtshof), der zufolge die Bestimmungen des *Digital Economy Act* 2010 (Gesetz zur digitalen Wirtschaft) nicht gegen EU-Recht verstoßen (siehe IRIS 2011-6/20) gescheitert.

Nach den Bestimmungen müssen Internetdiensteanbieter (ISPs) Abonnenten benachrichtigen, wenn Inhaber von Urheberrechten melden, dass ihre IP-Adressen zur Verletzung des Urheberrechts genutzt werden. Des Weiteren müssen die ISPs die Anzahl der Meldungen über jeden Abonnenten dokumentieren und eine anonyme Liste der betroffenen Abonnenten erstellen. Nach dem Erwirken einer gerichtlichen Verfügung zum Erhalt personenbezogener Angaben können Urheberrechtsinhaber gerichtlich gegen die Personen auf der Liste vorgehen. Diese Verpflichtungen würden erst wirksam, wenn ein von der Ofcom, dem Kommunikationsregulierer, erstellter und vom Parlament verabschiedeter „Erstverpflichtungskodex" in Kraft getreten ist. Die ISPs argumentierten, diese Anforderungen hätten der Europäischen Kommission gemäß der Richtlinie über Normen und technische Vorschriften mitgeteilt werden müssen, seien nicht mit den Bestimmungen der Richtlinie über den elektronischen Geschäftsverkehr vereinbar, verstießen gegen die Datenschutzrichtlinie für elektronische Kommunikation und seien nicht mit der Genehmigungsrichtlinie vereinbar.

Das Berufungsgericht vertrat die Ansicht, die Bestimmungen des Gesetzes erforderten keine Notifikation, da sie selbst keinerlei rechtliche Wirkung hätten, weil sie durch den Kodex umgesetzt werden müssten. Ein Verstoß der Bestimmungen gegen die Richtlinie über den elektronischen Geschäftsverkehr liege nicht vor, da sie keine Pflichten für ISPs vorsähen und sich in Bezug auf das Urheberrecht außerhalb des von der Richtlinie koordinierten Bereichs befänden, in dem Einschränkungen über die freie Bereitstellung von Diensten der Informationsgesellschaft untersagt seien. Die gesetzlichen Bestimmungen verstießen weder gegen die Datenschutzrichtlinie, da sich die Datenverarbeitung auf rechtmäßige Ansprüche beziehe, noch gegen die Datenschutzrichtlinie für elektronische Kommunikation, da die Einschränkung der Vertraulichkeit von Daten dazu diene, geistige Eigentumsrechte zu schützen. Schließlich erfordere die Genehmigungsrichtlinie nicht, dass alle sektorspezifischen Regelungen in einer allgemeinen Genehmigung statt in einer separaten Gesetzgebung enthalten sein müssten. Zudem stelle der Ausschluss von kleinen ISPs und Mobilfunknetzbetreibern aus dem System keine Unverhältnismäßigkeit dar.

Kritik übten die ISPs auch am Entwurf des Kostenbeschlusses zur Aufteilung der Kosten für den Betrieb des Systems. Der High Court hatte entschieden, die Forderung an die ISPs, einen Teil der Kosten zur Einrichtung des Systems zu tragen, verstoße gegen die Genehmigungsrichtlinie, und dieser Punkt wurde nicht angefochten. Das Berufungsgericht stellte fest, dass die „Fallgebühren" für Berufungskosten ebenso gegen die Richtlinie verstießen.

- *R (on the application of British Telecommunications and TalkTalk Telecom Group) v. Secretary of State for Culture, Media, Olympics and Sport [2012] EWCA Civ 232, 6 March 2012* (R (auf Antrag von British Telecommunications und TalkTalk Telecom Group) gegen das Ministerium für Kultur, Medien, Olympia und Sport [2012] EWCA Civ. 232, 6. März 2012)
  http://merlin.obs.coe.int/redirect.php?id=15770

IRIS 2012-5/22

„The Pirate Bay"-Betreiber verstoßen gegen Urheberrecht

Tony Prosser
School of Law, University of Bristol

Nach einer Entscheidung des *High Court* verletzen die Betreiber und Nutzer der Website „The Pirate Bay" die Urheberrechte von Rechteinhabern in der Musikindustrie. Dies bedeutet, dass Internetdiensteanbieter jetzt gezwungen werden können, ihren Kunden den Zugang zu dieser Website zu sperren.

Ausgangspunkt des Verfahrens war eine Klage großer Plattenfirmen gegen sechs große Internetdiensteanbieter im Vereinigten Königreich. Die Website „The Pirate Bay" ermöglicht es ihren Nutzern, nach urheberrechtlichem Material einschl. Musik und Filmen zu suchen und dieses herunterzuladen Die Plattenfirmen versuchten, eine gerichtliche Verfügung zu erwirken, um die Diensteanbieter zu zwingen, den Zugang ihrer Kunden zur Website zu sperren. Gemäß dem *Copyright, Designs and Patents Act 1988* (Urheberrechts-, Muster- und Patentgesetz in der im Zuge der Umsetzung der EU-Richtlinie Informationsgesellschaft novellierten Fassung) kann eine derartige Verfügung gegen einen Internetdiensteanbieter erwirkt werden, wenn dieser „unmittelbar Kenntnis" davon hat, dass der Dienst genutzt wird, um Urheberrechte zu verletzen. Im Verfahren ging es zunächst um die Klärung der Vorfrage, ob die Nutzer und Betreiber der Website Urheberrechte verletzen.

Das Gericht kam zu dem Schluss, dass die Nutzer von „The Pirate Bay" Urheberrechte verletzt haben. Die Verletzung liege dabei in der Art des Austauschs der Musikdateien; dabei wird aufgezeichnetes Material an ein neues, ein anderes Publikum weitergegeben, was der Art der Weitergabe entspricht, die der EuGH in der Rechtssache C-306/05 Sociedad General de Autores vs. Editores de España (SGAE) vs. Rafael Hoteles SA [2006] ECR I-11519 erkannt hatte (siehe IRIS 2007-2/3). Diese Verstöße gegen das Urheberrecht wurden von den Betreibern von „The Pirate Bay" geduldet, die dafür gesamtschuldnerisch haften; der Name der Website und ihre Finanzierung durch eine schwedische Anti-Copyright-Organisation trugen mit dazu bei, dass die Richter zu dem Schluss gelangten, dass die fraglichen Verstöße seitens der Betreiber „gezielt und beabsichtigt" erfolgten. Nach dem Präzedenzfall Newzbin2, bei dem eine einstweilige Verfügung erwirkt wurde, um einen führenden Internetdiensteanbieter zur Sperrung des Zugangs zu einer Website zu zwingen, die die Urheberrechte von sechs führenden Filmstudios verletzt hatte (siehe IRIS 2011-9/21), wurde in einer weitren Anhörung die Möglichkeit einer Verfügung eröffnet.

- *Dramatico Entertainment Ltd v. British Sky Broadcasting Ltd [2012] EWHC 268 (Ch), 20 February 2012* (Dramatico Entertainment Ltd vs. British Sky Broadcasting Ltd [2012] EWHC 268 (Ch), 20. Februar 2012) http://merlin.obs.coe.int/redirect.php?id=15726

IRIS 2012-4/28

Niederlande

Internetprovider müssen Zugang zu „The Pirate Bay" sperren

Axel M. Arnbak
Institut für Informationsrecht (IViR), Universität Amsterdam

Am 11. Januar 2011 hat das Haager Bezirksgericht zwei niederländische Internetprovider angewiesen, den Zugang zu „The Pirate Bay" zu sperren. Darüber hinaus wurde *Stichting BREIN*, einer Stiftung, die die Interessen der niederländischen Urheber vertritt, das Recht zugesprochen, die Provider unmittelbar aufzufordern, zukünftige IP-Adressen und (Sub-) Domain-Namen, die auf „The Pirate Bay" Bezug

nehmen, als Vorbeugungsmaßnahme zu sperren. Ziggo and XS4ALL, die fraglichen Anbieter, kündigten bereits an, dass sie gegen das Urteil Einspruch erheben werden. *BREIN* hat ihrerseits bekannt gegeben, dass sie ähnliche Maßnahmen auch für andere Anbieter beantragen werde.

Das Bezirksgericht sieht die Rechtsgrundlage für diese Entscheidungen in Art. 11 der niederländischen Umsetzungsgesetze zur Richtlinie 2004/48/EG (Durchsetzungsrichtlinie), in Art. 8 (3) der Richtlinie 2001/29/EG (Urheberrechtsrichtlinie) und im L'Oreal/eBay-Urteil (C-324/09) des Europäischen Gerichtshofs, in dem der EuGH zu dem Schluss kam, dass Maßnahmen gegen Internetdiensteanbieter zur Vorbeugung gegen erneute Verletzungen von Urheberrechten getroffen werden können. In vorausgegangenen Urteilen niederländischer Gerichte gegen "The Pirate Bay" war verfügt worden, dass das beanstandete Material nicht mehr am niederländischen Markt verfügbar gemacht werden dürfe. Da sich "The Pirate Bay" ohnehin nicht daran hielt, wertete das Gericht die von *BREIN* gegenüber den Diensteanbietern getroffenen Maßnahmen in diesem besonderen Fall als rechtmäßig.

Das Bezirksgericht hält fest, dass hier Anlass zu richterlicher Zurückhaltung bestehe, da das Sperren von Websites die durch Artikel 10 EMRK geschützte Meinungsfreiheit berühre. Das Gericht prüfte Fragen der Angemessenheit und Subsidiarität einer Internetsperre für die beiden Anbieter und kam zu dem Schluss, dass in diesem besonderen Fall die Maßnahme gerechtfertigt sei. Die Bewertung der Angemessenheit erfolgte ausgehend von der eingeschränkten Wirkung früherer Entscheidungen anhand von Fakten, die von BREIN vorgelegt worden waren. Das Gericht befand, dass eine ausreichend große Zahl von Kunden „The Pirate Bay" nutzten, um sich verschiedene niederländische Filme herunterzuladen. Darüber hinaus sei das von "The Pirate Bay" angebotene legale Material über andere Websites zugänglich, was in diesem Fall die Auswirkungen einer Zugangssperre im Hinblick auf die Meinungsfreiheit verringere. Schließlich ist das Gericht der Meinung, dass DNS- und IP-Sperren hinsichtlich einer bestimmten Website keine aktive Überwachung des Endnutzer-Internetdatenverkehrs mittels des DPI-Verfahrens (Deep-Packet-Inspection) bedeuten, das der EuGH in seinem jüngsten Urteil (Scarlet/Sabam C-70/10) als nicht rechtmäßig bewertete.

Am 20. Dezember 2011 sprach sich eine Mehrheit des Parlaments in einer Entschließung gegen Internetsperren im Zusammenhang mit Fragen der Durchsetzung von Urheberrechten aus. Die Richter nahmen die Initiative des niederländischen Gesetzgebers zur Kenntnis, ließen sich hiervon in ihrer Entscheidung jedoch zunächst nicht beeinflussen. Man darf also gespannt sein, wie der Gesetzgeber in dieser Frage in nächster Zeit weiter verfährt und wie sich dies auf das von den Betreibern angestrengte Berufungsverfahren auswirkt.

- *Rechtbank 's-Gravenhage, 11 januari 2012, LJN: BV0549, Stichting BREIN tegen Ziggo B.V. & XS4All Internet B.V.* (Bezirksgericht Den Haag, 11. Januar 2012, LJN: BV0549, Stichting BREIN v Ziggo B.V. & XS4All Internet B.V.)
  http://merlin.obs.coe.int/redirect.php?id=15624

- *Tweede Kamer, 29 838 Auteursrechtbeleid, Nr. 35 Motie van het Lid Verhoeven* (Zweite Kammer, 29838, Urheberrechtspolitik, Nr. 35, Motion by MP Verhoeven)
  http://merlin.obs.coe.int/redirect.php?id=15645

IRIS 2012-2/31

2013-6 p.42

Russische Föderation

Soziales Netzwerk „VKontakte“ wegen Piraterie bestraft

Dmitry Golovanov
Moskauer Zentrum für Medienrecht und Medienpolitik

Am 25. Mai 2012 hat das St. Petersburger Berufungsgericht 13 (Handelsgericht zweiter Instanz) ein erstinstanzliches Urteil gegen das populäre soziale Netzwerk VKontakte bestätigt; das Netzwerk wurde der Verletzung geistiger Eigentumsrechte zweier Plattenfirmen (S.B.A. Music Publishing und S.B.A. Production) schuldig gesprochen. VKontakte hatte Musik und Tonträger/Videos von 17 Liedern der russischen Popgruppen „Maksim“ und „Infinity“ auf der Website des Netzwerks eingestellt und öffentlich zugänglich gemacht und wurde deshalb zu einer Geldstrafe in Höhe von RUB 210.000 (ca. EUR 5.000) verurteilt.

Das Einstellen von Inhalten ohne die Zustimmung der Rechteinhaber (d.h. rechtswidrig) auf die Website von vkontakte.ru wurde weder vom Kläger noch vom Beklagten in Abrede gestellt; weniger klar war für das Gericht jedoch, wer die gefälschten Inhalte tatsächlich eingestellt hatte. War es das Management von VKontakte oder ein Nutzer des sozialen Netzwerks? Zentraler Punkt bei der Verhandlung war also die Frage, ob das Management von VKontakte für das öffentliche Bereitstellen rechtswidriger Inhalte haftet. Nach russischem Zivilrecht trägt VKontakte die Schuld.

Das Berufungsgericht orientierte sich bei seiner Entscheidung an den Leitlinien der höchsten Gerichtsinstanz, die diese in ihrer Entschließung vom 1. November 2011 formuliert hatte. Das Urteil des Berufungsgerichts berücksichtigte die wesentlichen Punkte, die auch von Gerichten der ersten Instanz zu beachten sind, wenn es um die Haftung von Hosting-Anbietern geht, die im Internet Videos bereitstellen.

Das Berufungsgericht prüfte mehrere grundlegende Fragen, die in diesem Fall für eine Haftung durch VKontakte sprechen. Zunächst stellte das Gericht fest, dass die Inhalte einer allgemeinen Öffentlichkeit und nicht, wie der Beklagte geltend machte, nur bestimmten Personen zur Verfügung standen. Eine Registrierung gegen Entgelt, die für vkontakte.ru-Nutzer obligatorisch ist, steht jedem Vertreter der allgemeinen Öffentlichkeit offen; durch die Anmeldung entstehen keine speziellen Zielgruppen oder geschlossene Gruppen, die als Nutzer der Inhalte in Erscheinung treten. Daneben befasste sich das Gericht mit der Frage, wie das Einstellen von Inhalten in die VKontakte-Website im Unternehmen geregelt ist. Zwar enthalten die Vertragsbedingungen für Mitglieder von vkontakte.ru den Hinweis, dass sie verpflichtet sind, dafür Sorge zu tragen, dass sie nur rechtmäßige Inhalte einstellen, doch bietet VKontakte eine Reihe technischer Möglichkeiten, die das Einstellen raubkopierter Inhalte zulassen. Das Bestehen dieser Möglichkeiten wurde als Beleg für die Schuld von VKontakte gewertet. Weiter gelangte das Gericht zu der Auffassung, dass durch das Bestehen der vorgenannten Möglichkeiten die Website vkontakte.ru für Unternehmen der Werbewirtschaft, die ihre Werbung im Internet platzieren, attraktiver wird, wodurch sich für VKontakte potentielle Mehrgewinne ergeben. Das Gericht unterstrich, dass Gewinne (auch potentielle Gewinne) aus der rechtswidrigen Nutzung geistigen Eigentums als Beleg für die Schuld von VKontakte zu werten sind.

Abschließend wies das Berufungsgericht darauf hin, dass die Reaktion seitens VKontakte auf die Aufforderung des Klägers, die unrechtmäßigen Aktivitäten einzustellen, passiv und nicht wirksam gewesen war. Der Beklagte machte geltend, dass aus den VKontakte vorliegenden Unterlagen nicht mit Sicherheit hervorgegangen sei, dass die Kläger die rechtmäßigen Rechteinhaber seien. Das Gericht folgte dieser Auffassung nicht und stellte fest, dass der Beschuldigte durchaus die Möglichkeit gehabt habe, den rechtlichen Status der Kläger zu prüfen, etwa anhand von Kopien der Lizenzvereinbarungen oder anderer Unterlagen. Darüber hinaus musste der Beklagte Kenntnis von der Rechtswidrigkeit der Inhalte haben, da das Thema Verbreitung gefälschter Inhalte über das soziale Netzwerk VKontakte Gegenstand der öffentlichen Diskussion war, an der sich auch die Massenmedien beteiligten.

Gegen die Entscheidung des St. Petersburger Handelsgerichts der zweiten Instanz ist Berufung bei Gerichten einer höheren Instanz zulässig.

- *Постановление Тринадцатого арбитражного апелляционного суда 25 мая 2012 года по делу № А56-57884/2010* (Entscheidung vom 25. Mai 2012, Handelsgericht der zweiten Instanz (Rechtssache Nr. A56-57884/2010))
  http://merlin.obs.coe.int/redirect.php?id=15989

IRIS 2012-7/36

Der Patriot Act und der Vierte Verfassungszusatz

Wie die amerikanische Regierung insgeheim ihre Befugnisse zur Sammlung persönlicher Daten ihrer Bürger ausweitet

Jonathan Perl
*Locus Telecommunications, Inc.**

I. Einleitung

Der amerikanische Kongress verabschiedete 2001 als Antwort auf die Angriffe des 9. September mit dem *USA Patriot Act* (Gesetz) ein Antiterrorgesetz, durch das die Strafverfolgungsbehörden bei der Verhinderung derartiger Angriffe in Zukunft unterstützt werden sollten.[1] Dieses richtungsweisende Gesetz verschaffte der amerikanischen Bundesregierung (Regierung) durch umfassende Änderungen der Gesetze zur Regelung von Durchsuchungen und Überwachungen eine beispiellose Machtfülle zur Sammlung von Daten. Seine Umsetzung vollzog sich zwar im Geheimen, aber nach der Veröffentlichung der Enthüllungen des NSA-Whistleblowers Edward Snowden kommt nun jedoch immer mehr ans Licht, inwieweit die Regierung das Gesetz einsetzt, um persönliche Daten ihrer Bürger zu sammeln. Die daraufhin einsetzende Medienaufmerksamkeit sowie Untersuchungen des US-Kongresses haben offenbart, dass die Regierung insgeheim ihre Befugnisse zur Sammlung persönlicher Daten ihrer Bürger ausweitet, häufig willkürlich, in großem Maßstab und gleichgültig, ob sie irgendeines Vergehens verdächtig sind.

II. Die rechtlichen Einschränkungen der US-Regierung bei der Sammlung von Daten

Die Regierung wird grundsätzlich durch den Vierten Zusatzartikel zur Verfassung der Vereinigten Staaten in ihren Möglichkeiten zur Sammlung persönlicher Daten eingeschränkt. Dort heißt es: „Das Recht des Volkes auf Sicherheit der Person und der Wohnung, der Urkunden und des Eigentums vor willkürlicher Durchsuchung, Festnahme und Beschlagnahme darf nicht verletzt werden, und Haussuchungs- und Haftbefehle dürfen nur bei Vorliegen eines ...Rechtsgrundes ausgestellt werden und müssen die zu durchsuchende Örtlichkeit und die in Gewahrsam zu nehmenden Personen oder Gegenstände genau bezeichnen."[2] Dem liegt der Gedanke zugrunde, dass „Strafverfolgungsbeamte Ihr Haus von der Straße aus beobachten können, sie dürfen aber in den meisten Fällen nicht eindringen, es sei denn, sie können einem Richter nachweisen, dass es erforderlich ist."[3]

---

* Jonathan D. Perl ist Rechtsberater für regulatorische Angelegenheiten bei Locus Telecommunications, Inc. Die in diesem Artikel geäußerten Auffassungen sind persönlicher Natur. Sie stellen keine Auffassungen von Locus Telecommunications Inc. dar und sollten nicht als solche verstanden werden.

1) Siehe USA PATRIOT Act 2001, Pub. Law 107-56, 115 Stat. 272 (2001)

2) Verfassung der Vereinigten Staaten, Zusatz IV

3) Bob Sullivan, Big Brother may not be listening, but he's watching: Why metadata snooping is legal, NBC News, 15. Juni 2013, abrufbar unter:
www.nbcnews.com/technology/big-brother-may-not-be-listening-hes-watching-why-metadata-6C10334990

Der Oberste Gerichtshof der USA (Gerichtshof) wandte den Vierten Verfassungszusatz 1979 erstmals in einem richtungsweisenden Fall auf Informationen *über* Telefonanrufe an (heute als Teil von Metadaten betrachtet).[4] Der Gerichtshof befand, die Informationen über einen Telefonanruf seien nach dem Vierten Verfassungszusatz nicht geschützt, und betrachtete diese getrennt vom Inhalt des Telefonanrufs, auf den nur mit einem Vollstreckungsbefehl zugegriffen werden darf. Der Gerichtshof wandte die „Drittanbieter-Doktrin" an, nach der eine Einzelperson ihren Anspruch auf Datenschutz verliert, wenn sie freiwillig Daten an Dritte weitergibt, und befand, es bestehe kein Anspruch auf Datenschutz in Bezug auf die an einem Gespräch beteiligten Telefonnummern, da durch das Wählen der Nummer die Information freiwillig an die Telefongesellschaft weitergegeben werde.

Der Kongress kodifizierte diese Gerichtsentscheidung 1986 durch Verabschiedung des *Electronic Communications Privacy Act* (ECPA - Gesetz zum Datenschutz in der elektronischen Kommunikation).[5] Das ECPA bestätigte, dass Strafverfolgungsbeamte sich mit einer strafbewehrten rechtlichen Anordnung (*subpoena*) ohne Richtervorbehalt die Informationen über einen Anruf mittels eines *pen register*[6] (Rufdatenerfassungsgerät) und eines *trap and trace device*[7] (Fangschaltungsvorrichtung) beschaffen können. Ein *pen register* ist ein „Gerät oder ein Prozess, das bzw. der Wähl-, Routing-, Adressierungs- oder Signalisierungsinformationen aufzeichnet oder decodiert, die über einen Apparat oder eine Vorrichtung übermittelt werden, von dem bzw. der eine drahtgebundene oder elektronische Kommunikation gesendet wurde, wobei diese Informationen keine Inhalte irgendwelcher Kommunikationen beinhalten dürfen". *Trap and trace device* bedeutet hingegen „ein Gerät oder einen Prozess, das bzw. der die eingehenden elektronischen oder sonstigen Impulse abfängt, die die Ursprungsnummer oder sonstige Wähl-, Routing-, Adressierungs- oder Signalisierungsinformationen identifizieren, die sehr wahrscheinlich den Ursprung einer drahtgebundenen oder elektronischen Kommunikation identifizieren, wobei diese Informationen keine Inhalte irgendwelcher Kommunikationen beinhalten dürfen." Die Verfasser des Gesetzes stellten in einem begleitenden Bericht zum EPCA an den US-Senat fest, es sei keine unabhängige gerichtliche Überprüfung vorgesehen, ob der Antrag dem „Relevanzstandard" genügt, sondern lediglich eine Befugnis der Richter, die Vollständigkeit der Unterlagen zu überprüfen.[8] Dies wurde später auch durch ein Bundesberufungsgericht bestätigt, welches erklärte, „die gerichtliche Rolle … hat Verwaltungscharakter".[9] Viele Richter kamen in der Folge zu dem Schluss, sie hätten praktisch keine Handhabe gegen *pen register*, was einen Bundesrichter in Florida zu der traurigen Feststellung veranlasste, „dem Gerichtshof bleibt nach dem [ECPA] anscheinend nicht mehr als das Durchwinken."[10]

Im Gegensatz dazu ist die Regierung nach dem *Foreign Intelligence Surveillance Act*[11] (Gesetz über nachrichtendienstliche Auslandsüberwachung - FISA-Gesetz) von 1978 und der Durchführungsverordnung 12333[12] berechtigt, Daten über Ausländer im Ausland zu sammeln. Das FISA-Gesetz nimmt Kommunikationen von Ausländern im Ausland vom Schutz nach dem Vierten Verfassungszusatz aus, indem es der Regierung gestattet, Daten über jegliche Kommunikationen zu sammeln, solange sie berechtigte Gründe hat anzunehmen, dass eine der beteiligten Parteien ein Ausländer auf ausländischem Gebiet ist; dabei muss sie weder ihre Zielpersonen noch die überwachten Einrichtungen offenlegen. Das Gesetz gestattet es der Regierung, beim *Foreign Intelligence Surveillance Court* (Gericht für nachrichtendienstliche Auslandsüberwachung - FISA-Gericht) eine einzige gerichtliche Verfügung zu erwirken, mit der sie Tausende, wenn nicht Millionen von Menschen überwachen kann, was eine „zufällige" Überwachung amerikanischer Staatsbürger

4) *Smith gegen Maryland*, 442 U.S. 735 (1979).
5) Electronic Communications Privacy Act of 1986, 18 U.S.C. §§ 2510-2522
6) 18 USC § 3127 (3)
7) 18 USC § 3127 (4)
8) Declan McCullag, *Feds tell Web firms to turn over user account passwords*, CNET (25. Juli 2013), abrufbar unter http://news.cnet.com/8301-13578_3-57595529-38/feds-tell-web-firms-to-turn-over-user-account-passwords/
9) *Vereinigte Staaten gegen Fregoso*, US-Berufungsgericht, 8. Gerichtsbezirk (1995)
10) S. o. Fußnote 8
11) Foreign Intelligence Surveillance Act 1978, Pub. L. 95–511, 92 Stat. 1783, 50 U.S.C. 36 („FISA")
12) 46 FR 59941, 3 CFR, 1981, abrufbar unter: www.archives.gov/federal-register/codification/executive-order/12333.html

einschließt.[13] Über die Arbeitsweise des FISA-Gerichts ist aufgrund seiner Geheimhaltung wenig bekannt; vor Kurzem brachte jedoch James Robertson, ein früherer Bundesrichter, der am FISA-Gericht tätig war, seine Überzeugung zum Ausdruck, das System sei „mangelhaft", da es rechtlichen Gegnern nicht erlaube, Handlungen der Regierung zu hinterfragen, und sei „zu einer Art Verwaltungsbehörde geworden".[14] Die Durchführungsverordnung 12333 gibt der Regierung die Befugnis, geheimdienstliche Informationen zu ausländischen Signalen aus Kommunikationssystemen der gesamten Welt zu sammeln, zu speichern, zu analysieren und weiterzugeben.[15]

Der Kongress stützte sich auf diese Differenzierungen, als er die drei neuen und aktualisierten Instrumente des *Patriot Act* zur Datensammlung entwickelte: (1) *Business Records Orders* (Anordnungen zur Offenlegung von Geschäftsunterlagen) („Paragraf 215"), (2) *Sneak and Peek Warrants* (verdeckte Durchsuchungsbeschlüsse) und (3) *National Security Letters* (Anordnungen zur nationalen Sicherheit - NSL).[16] Die Anordnungen nach Paragraph 215 werden verwendet, um Kundeninformationen etwa zum Führerschein, Hotelbuchungen, Leihwagen, Mietwohnungen, Kreditkartenbewegungen und Buchausleihen zu verlangen, und beinhalten einen „Knebelerlass", der dem Empfänger einer Anordnung untersagt, irgendjemandem zu erzählen, dass er eine solche erhalten hat. Das Gesetz ermöglicht der Regierung darüber hinaus die Beantragung eines *Sneak and Peek Warrant*, um eine Vielzahl von Aufzeichnungen von Telefonmitschnitten bis hin zu Kontoinformationen vorab zu überprüfen. Ein NSL ermöglicht Strafverfolgungsbehörden die Durchsuchung des Hauses eines Verdächtigen einschließlich Zugriff auf dessen Computer über Monate hinweg, ohne den Betroffenen zu informieren. Die *National Security Agency* (NSA), die Regierungsbehörde, „die Geheimdienstinformationen aus ausländischen elektronischen Signalen zu nationalen Geheimdienstzwecken und für Spionageabwehrzwecke sowie zur Unterstützung militärischer Aktionen sammelt, verarbeitet und weitergibt",[17] stützt sich zumeist auf Paragraph 215, da dieser erlaubt, „alle greifbaren Dinge" im Zusammenhang mit einer autorisierten Ermittlung zum Schutz gegen internationalen Terrorismus oder mit geheimen Aufklärungsaktivitäten kraft einer geheimen Anordnung des FISA-Gerichts zu sammeln, wenn „es triftige Gründe zu der Annahme gibt, dass die gesuchten greifbaren Dinge für eine autorisierte Ermittlung von Relevanz sind". Die *American Civil Liberties Union* (Amerikanische Bürgerrechtsunion - ACLU) schätzt die Ausstellung allein zwischen 2003 und 2006 auf etwa 192.000 NSL, von denen eine zur einer Verurteilung wegen Terrorismus führte, und in 2010 auf 3.970 *Sneak and Peek Warrants*, von denen lediglich 1% mit Terrorismus in Zusammenhang standen.[18]

13) Margot Kaminskijun, "PRISM's Legal Basis: How We Got Here, and What We Can Do to Get Back, A privacy scholar explains the recent news about government surveillance", *The Atlantic* (7 June 2013), abrufbar unter: www.theatlantic.com/national/archive/2013/06/prisms-legal-basis-how-we-got-here-and-what-we-can-do-to-get-back/276667/

14) Associated Press, "Former judge admits flaws with secret FISA court", *CBS News*, (9. Juli 2013), abrufbar unter www.cbsnews.com/8301-250_162-57592836/former-judge-admits-flaws-with-secret-fisa-court/

15) *The National Security Agency: Missions, Authorities, Oversight and Partnerships*, National Security Agency (9. August 2013), abrufbar unter: http://i2.cdn.turner.com/cnn/2013/images/08/09/2013_08_09_the_nsa_story1.pdf

16) *Reclaiming Patriotism, A Call to Reconsider the Patriot Act*, American Civil Liberties Union, (März 2009), abrufbar unter: www.aclu.org/pdfs/safefree/patriot_report_20090310.pdf

17) Frequently Asked Questions, National Security Agency, abrufbar unter: www.nsa.gov/about/faqs/index.shtml

18) "Surveillance Under the Patriot Act", American Civil Liberties Union, (Oktober 2011), abrufbar unter: https://www.aclu.org/national-security/surveillance-under-patriot-act. Siehe auch "A Review of the FBI's Use of National Security Letters: Assessment of Corrective Actions and Examination of NSL Usage in 2006", Office of the Inspector General, U.S. Department of Justice, (März 2008).

III. Das Ausmaß der Datensammlung

Am 6. Juni 2013 veröffentlichte die britische Tageszeitung *The Guardian* fünf Folien einer von der NSA erstellten Powerpoint-Präsentation, in der ein streng geheimes US-Nachrichtendienstprogramm mit dem Titel PRISM beschrieben wird.[19] Die Veröffentlichung dieses streng geheimen Dokuments löste eine Flut an zugespielten Dokumenten aus, die aufzeigen, in welchem Ausmaß die Regierung Zugriff auf persönliche Daten hat, solche sammelt und verwendet.

Die Enthüllungen machten deutlich, dass die amerikanische Öffentlichkeit noch keine Kenntnis vom wahren Ausmaß der Überwachung und Datensammlung oder von den Dutzenden an rechtlichen Stellungnahmen zur Rechtfertigung dieser Maßnahmen hat, von denen einige mehrere Hundert Seiten umfassen. Nach eigenen Schätzungen der NSA gab es in der Antiterrordatenbank von PRISM 117.675 aktive Überwachungsziele, was zu 24.005 Berichten im Jahr 2012, das heißt zu „über 2.000 PRISM-gestützten Berichten" jeden Monat,[20] zu über 77.000 nachrichtendienstlichen Berichten, die sich auf das Programm PRISM berufen, 850 Milliarden in NSA-Datenbanken gesammelten und gespeicherten „Anrufereignissen" sowie annähernd 150 Milliarden Internetdatensätzen geführt hat, wobei täglich ein bis zwei Milliarden Datensätze hinzukommen. Noch erschreckender ist, dass die NSA kürzlich eingeräumt hat, sie „streife" geschätzt 1,5% aller Daten im Internet und greife 0,025% der Internetdaten zur Überprüfung heraus.[21]

a. PRISM

Die von Snowden zugespielten streng geheimen Dokumente zeigen, dass PRISM „es einem NSA-Mitarbeiter ermöglicht, den Inhalt von E-Mails, Video- und Audiochats, Videos, Fotos, VoIP-Chats (zum Beispiel Skype), Dateiübertragungen sowie Details aus sozialen Netzwerken anzuschauen, zusammenzutragen, zu überwachen und gegenzuprüfen";[22] dies betrifft alle Daten, auf die auf den Servern von Microsoft, Yahoo, Google, Facebook, PalTalk, AOL, Skype, YouTube und Apple zugegriffen wird[23] und die für die Auslandsaufklärung „relevant" sind. Nachdem ein NSA-Mitarbeiter auf die Daten der Server zugegriffen hat, kann er eine Ermittlung gegen eine Einzelperson einleiten, indem er einen Bericht an einen Dienstvorgesetzten verfasst. Der Antrag wird genehmigt, wenn es „triftigen Grund zur Annahme" gibt, dass die ausgemachte Zielperson ein Ausländer ist, der sich zur Zeit der Datensammlung im Ausland befindet, was als 51 Prozent Zuverlässigkeit definiert ist.[24]

Der US-Geheimdienstkoordinator räumte ein, dass es durch die weite Auslegung durch die NSA zu „zufällig erlangten"[25] Daten von US-Bürgern kommt, obwohl PRISM ausschließlich auf „Nicht-US-Bürger außerhalb der Vereinigten Staaten" *abzielt*. Er betonte jedoch gleichzeitig, die NSA habe „mäßigende Maßnahmen" eingeführt, wodurch PRISM solche Daten als zufällige Einträge kennzeichnet und sie aus dem Arbeitsbereich des Mitarbeiters löscht; der Mitarbeiter muss seinerseits die Daten manuell aussondern, wenn dies nicht automatisch erfolgt.[26] Der Koordinator gab jedoch in einem Schreiben an Senator Ron Wyden zu, das FISA-Gericht habe „zumindest in einem Fall" befunden, die von der Regierung angewandten „mäßigenden Maßnahmen" seien „nach dem Vierten

19) Glenn Greenwald und Ewen MacAskill, "NSA Prism program taps in to user data of Apple, Google and others", *The Guardian* (6. Juni 2013), abrufbar unter: www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data
20) *Ebd*.
21) S. o. Fußnote 15
22) S. o. Fußnote 19
23) Siehe "NSA slides explain the PRISM data-collection program", *The Washington Post* (6. Juni 2013), abrufbar unter: www.washingtonpost.com/wp-srv/special/politics/prism-collection-documents/
24) S. o Fußnote 15 (die zugespielten NSA-Richtlinien finden sich unter www.documentcloud.org/documents/727943-exhibit-a.html)
25) S. o. Fußnote 11
26) Marc Ambinder, "Solving the mystery of PRISM" , *The Week* (7. Juni 2013), abrufbar unter: http://theweek.com/article/index/245360/solving-the-mystery-of-prism

Verfassungszusatz unangemessen."[27] Dieses Eingeständnis unterstreicht die Besorgnis, dass die Daten im Besitz der Regierung bleiben, wenngleich sie „nicht protokolliert, indiziert oder in einem Bericht verwendet werden".[28] Besorgnis herrscht auch darüber, ob und wie die Daten weitergegeben werden. Glaubt ein Mitarbeiter, ein Bürger zeige kriminelle Aktivität oder kriminelle Absichten, löst dies eine Weitergabe der Informationen an das *Federal Bureau of Investigation* (FBI) aus, welches eigene Ermittlungen aufnimmt und dabei den NSA-Hinweis als möglichen Grund heranzieht.[29] Jeder Mitarbeiter muss jedoch subjektiv zwischen relevanter und irrelevanter Kommunikation unterscheiden und die Absichten eines Bürgers oftmals mit minimalen Hintergrundinformationen entschlüsseln. Darüber hinaus können die Informationen an jede der zahlreichen Bundesbehörden weitergegeben werden, von denen viele in zunehmendem Maße Daten von der NSA anfordern.

Microsoft, Yahoo, Google, Facebook und PalTalk bestritten, an PRISM „wissentlich teilgenommen" zu haben.[30] Man sollte dabei jedoch nicht vergessen, dass ihnen der Knebelerlass untersagt, schon allein die Existenz des Programms zuzugeben. Eine solche Zusammenarbeit, sollte sie sich bewahrheiten, stünde dabei in keinerlei Gegensatz zu früherem Verhalten, da die Unternehmen 2006 einräumten, freiwillig an einer früheren Version des Programms teilgenommen zu haben, bis dies von der New York Times aufgedeckt wurde.[31] Diese Enthüllung wurde im Nachhinein bestätigt, als der Kongress ihnen im FISA-Änderungsgesetz 2008 Blankoimmunität gewährte.[32]

b. Zugang zu Einzelgesprächsnachweise – „Niemand belauscht Ihre Telefongespräche"

Die Enthüllungen zeigten darüber hinaus, dass das FISA-Gericht im April 2013 eine Anfrage der NSA nach Zugang zu allen Telefonnummern von Verizon - einer der größten Telefongesellschaften in den USA - genehmigte, willkürlich, in großem Maßstab und gleichgültig, ob die Abonnenten eines Vergehens verdächtig sind. Gemäß der Anordnung war Verizon verpflichtet, der NSA elektronische Kopien „aller Einzelgesprächsnachweise oder ‚Telefonie-Metadaten', die Verizon für Kommunikationsverbindungen zwischen den Vereinigten Staaten und dem Ausland" oder „gänzlich innerhalb der Vereinigten Staaten einschließlich Ortsgesprächen auf aktueller Tagesbasis erstellt hatte", ab Datum der Anordnung bis zum 19. Juli 2013 zur Verfügung zu stellen.[33] Insbesondere wurde Verizon verpflichtet, „Informationen zur Verbindungsidentifikation" wie „Quell- und Zielrufnummern", die Dauer der einzelnen Gespräche, Telefonkartennummern, Amtsleitungskennung, IMSI-Nummern sowie „umfassende Informationen zum Verbindungsrouting" bereitzustellen. Es ist nicht bekannt, ob diese Anordnung einmalig oder lediglich die letzte in einer Reihe ähnlicher Anordnungen war. Es bleibt auch weiterhin unklar, ob Verizon der einzige Anbieter ist, den eine solche Anordnung getroffen hat. Ein Bericht in der *USA Today* aus dem Jahr 2006, in dem aufgezeigt wird, dass die NSA ein Programm zur massenhaften Sammlung inländischer Telefon-, Internet- und E-Mail-Verbindungen von AT&T, Verizon und BellSouth eingeführt hatte, das von Präsident Bush geheim genehmigt wurde, lässt vermuten, dass die NSA in der Vergangenheit von allen großen Mobilfunknetzen Verbindungsdaten gesammelt hat.

27) Spencer Ackerman, "U.S. Admits Surveillance Violated Constitution At Least Once", *Wired* (20. Juli 2012), abrufbar unter: www.wired.com/dangerroom/2012/07/surveillance-spirit-law/; siehe auch: http://apps.washingtonpost.com/g/page/national/first-direct-evidence-of-illegal-surveillance-found-by-the-fisa-court/393/
28) Eli Lake, "The Surveillance Scandals, Former NSA Director Michael Hayden Responds to Edward Snowden Claim", *The Daily Beast* (12. Juni 2013) (Er zitiert einen Fall, *U.S. gegen Sattar,* in dem die Regierung tausende Stunden an abgefangener Kommunikation aufgezeichnet hatte, die zwar minimiert, jedoch nicht gelöscht wurden)
29) S. o. Fußnote 27
30) Chris Gayomali, "Here are the tech companies denying involvement with the NSA's PRISM program", *The Week* (7. Juni 2013), abrufbar unter http://theweek.com/article/index/245325/here-are-the-tech-companies-denying-involvement-with-the-nsas-prism-program
31) Barton Gellman, "U.S. surveillance architecture includes collection of revealing Internet, phone metadata", *The Washington Post* (12. März 2004), abrufbar unter www.washingtonpost.com/investigations/us-surveillance-architecture-includes-collection-of-revealing-internet-phone-metadata/2013/06/15/e9bf004a-d511-11e2-b05f-3ea3f0e7bb5a_story.html?hpid=z1
32) FISA-Änderungsgesetz 2008, Pub.L. 110–261, 122 Stat. 2436, H.R. 6304 (2008)
33) Glen Greenwald, "NSA collecting phone records of millions of Verizon customers daily", *The Guardian* (5. Juni 2013), abrufbar unter: www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order

c. XKeyscore

Darüber hinaus wurde enthüllt, dass die NSA auch ein Datensammelprogramm mit dem Namen XKeyscore verwendet, von dem sie behauptet, es sei das „weitestreichende" System zur „Nachrichtenbeschaffung aus Computernetzwerken".[34] In zugespielten Schulungsunterlagen erklärt die NSA, das Programm decke „fast alles ab, was ein durchschnittlicher Nutzer im Internet macht", einschließlich Inhalten von E-Mails, besuchten Websites und Suchanfragen sowie deren Metadaten, und darüber hinaus auch das Abfangen der Internetaktivitäten von Einzelpersonen in „Echtzeit". NSA-Mitarbeiter nutzen es, um gigantische Behördendatenbanken zu durchforsten, wobei sie lediglich eine allgemeine Begründung für die Suche angeben, die vor der Ausführung nicht gerichtlich oder von anderen NSA-Mitarbeitern überprüft wird. Ein NSA-Tool namens DNI Presenter ermöglicht es einem Mitarbeiter, mithilfe von XKeyscore zudem den Inhalt von Chats oder persönlichen Mitteilungen auszulesen. Inhalte werden im System für lediglich drei bis fünf Tage, Metadaten hingegen 30 Tage gespeichert.

IV. Die rechtlichen Begründungen der Regierung für ihre Geheimprogramme

Als Reaktion auf die gesteigerte Medienaufmerksamkeit und die öffentliche Diskussion veröffentlichte Präsident Obama ein 22-seitiges Weißbuch, in dem die Rechtsgrundlage für die verschiedenen NSA-Überwachungsprogramme erläutert wird.[35] Darin heißt es, die Programme seien gerechtfertigt, da sie einer breiter gefassten Definition von „Relevanz" nach Paragraph 215 entsprechen. Die Definition von „Relevanz" müsse „zumindest so weit" ausgelegt werden, wie es in einer Reihe von Fällen erfolgt sei, in denen es um die Offenlegung von Dokumenten bei „ordentlichen zivilrechtlichen Offenlegungsverfahren und straf- und verwaltungsrechtlichen Ermittlungen" ging, da „der ‚Relevanzstandard' nötigenfalls und je nach Kontext einen beträchtlichen Spielraum gewährt, eine große Menge an Daten zu sammeln, um die darin enthaltenen entscheidenden Informationen aufzuspüren". Alle Telefon-Metadaten seien zudem nach Paragraph 215 relevant, da irgendwo in diesem enormen Datenbestand einzelne Datenelemente vorhanden sein könnten, die tatsächlich relevant sind. Die Regierung warnte vor dem Eindruck, dies gewähre eine breite Befugnis zur Sammlung Daten anderer Art wie Patientendaten oder Ausleihdaten von Bibliotheken, und stellte klar, sie erhebe keine Informationen dieser Art für Antiterrorzwecke, da diese Datenkategorien grundsätzlich nicht mit Verbindungsmetadaten als Mittel vergleichbar seien, zuvor unbekannte terroristische Aktivisten oder Netzwerke aufzudecken. Diese Auslegung ist jedoch beunruhigend, da sie eigentlich besagt, „wir glauben nicht, dass das Sammeln von Patientenakten notwendig ist, um Terrorismus zu stoppen, aber wenn wir es glaubten, könnten wir sie sammeln". In einem solchen Fall „... wäre es der Regierung gestattet, annähernd alle Daten mit der Begründung einzusammeln, einige davon könnten sich später als relevant erweisen", zum Beispiel „Milliarden von Patientenakten oder Ausleihbelegen von Bibliotheken ohne gerichtliche Anordnung - eine verfassungswidrige Pauschalausforschung wie aus dem Lehrbuch".[36]

Präsident Obama hatte eine Reform von Paragraph 215 des Patriot Act versprochen. Insbesondere hatte er erklärt, die Reformen würden eine neue Website umfassen, die den Amerikanern und den Menschen weltweit mehr Informationen über die Überwachungsprogramme vermittelt, daneben ein externes Beratergremium zur Überprüfung der Überwachungsprogramme, einen Datenschutzbeauftragten bei der NSA sowie einen unabhängigen Anwalt, der die Argumente und politischen Maßnahmen der Regierung vor Gericht überprüft.[37] Die Vorschläge stießen auf Kritik

34) Glen Greenwald, "XKeyscore: NSA tool collects 'nearly everything a user does on the internet'", *The Guardian* (31. Juli 2013), abrufbar unter: www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data
35) Weißbuch der Regierung, *Bulk Collection of Telephony Metadata Under Section 215 of the USA Patriot* Act (9. August 2013), abrufbar unter: http://big.assets.huffingtonpost.com/Section215.pdf
36) Jeffrey Rosen, *The Lies Aren't What Make Obama's NSA Stance So Awful*, The New Republic (12. August 2013), abrufbar unter: www.newrepublic.com/article/114276/obama-surveillance-comments-dishonesty-isnt-only-problem
37) Siehe Obama announces NSA surveillance reform RT (9. August 2013), abrufbar unter http://rt.com/usa/obama-nsa-statement-transparency-308/

seitens führender republikanischer Kongressabgeordneter, die davor warnten, dass ein Anwalt in Verfahren des Geheimgerichts, das die umfassende Telefondatensammlung der NSA beaufsichtigt, Antiterroranstrengungen verzögern würde, während die Zeit dränge.[38]

V. Regierung räumt Kompetenzüberschreitung ein

Im August 2013 wurde durch die Enthüllung eines internen NSA-Gutachtens aufgezeigt, dass die Behörde jährlich tausendfach Datenschutzregeln gebrochen und ihre rechtlichen Befugnisse überschritten hat.[39] Das Gutachten vom Mai 2012 weist 2.776 Fälle nicht genehmigter Sammlung, Speicherung, Zugriff oder Verbreitung gesetzlich geschützter Kommunikationen allein in den vorangegangenen zwölf Monaten aus. Es wurde zwar festgestellt, dass die meisten unbeabsichtigt waren, bei vielen wurde aber auch die nötige Sorgfalt missachtet oder gegen Standardvorgehensweisen verstoßen. Die hervorzuhebenden Fälle umfassen einen Verstoß gegen einen Gerichtsbeschluss und die nicht genehmigte Nutzung von Daten über mehr als 3.000 Amerikaner und Green-Card-Inhaber, Schreibfehler, die zu einem unbeabsichtigten Abfangen amerikanischer E-Mails und Telefonanrufe führten, und sogar einen Beschluss, dass eine unbeabsichtigte Überwachung amerikanischer Staatsbürger nicht gemeldet werden muss. In dem Gutachten wurden auch bis in das Jahr 2008 zurückreichende Verstöße angeführt, unter anderem das Abhören einer „großen Zahl" von Anrufen, die von Washington aus getätigt wurden, als aufgrund eines Programmierfehlers die amerikanische Ortsvorwahl 202 mit der internationalen Vorwahl für Ägypten 20 verwechselt wurde. Als anderer Verstoß wurde im Beschluss des FISA-Gerichts aufgedeckt, die NSA habe gegen die Verfassung verstoßen, indem sie dem Gericht eine neue Datensammlungsmethode erst viele Monate nach ihrer Einführung offenlegte. Ein weiteres Beispiel für Kompetenzüberschreitung ist die Umleitung großer internationaler Datenmengen, die über Glasfaserkabel in den Vereinigten Staaten übertragen wurden, in einen Vorratsspeicher, in dem das Material vorübergehend zur Verarbeitung und Selektion gespeichert werden konnte. Die Zahl der Verstöße dürfte wesentlich höher sein, da das Gutachten lediglich Vorfälle im NSA-Hauptsitz Fort Meade erfasste und weitere operative NSA-Einheiten und regionale Erhebungszentren außer Acht ließ.

VI. Fazit

Die Befürworter der Programme behaupten, diese würden nicht in die Privatsphäre eingreifen, da die Regierung letztlich keine Inhalte anschaue. Aber selbst wenn dies für alle NSA-Programme zutreffen sollte, wird diese Differenzierung in zunehmendem Maße gegenstandslos, da Metadaten, um einen Fachmann zu zitieren, häufig „sehr viel stärker als Inhalte in die Privatsphäre eingreifen" können.[40] In der Praxis kann die Regierung daraus „eine enorme Menge an personenbezogenen Informationen ableiten".[41] So kann eine Abfolge von Telefonanrufen führender Unternehmensvertreter bevorstehende Firmenübernahmen andeuten, Anrufe bei einem Gynäkologen, einem Onkologen und dann bei nahen Familienangehörigen können auf einen besonderen Gesundheitszustand hinweisen, und Informationen von Mobilfunkmasten können den Aufenthaltsort und die Bewegungen des Anrufers enthüllen. Diese Beispiele werden durch die Erkenntnisse zahlreicher Studien belegt; so kann etwa eine Einzelperson allein dadurch identifiziert werden, dass ihr Aufenthaltsort zu vier unterschiedlichen Gelegenheiten bekannt ist;[42] die Vorlieben, die politische Ausrichtung sowie eine Vielzahl weiterer Charakterzüge einer Person lassen sich allein durch die „Gefällt mir"-Klicks

38) Janet Hook und Sarah Portlock, "Republicans Warn on NSA Changes", *The Wall Street Journal* (11. August 2013), abrufbar unter: http://blogs.wsj.com/washwire/2013/08/11/republicans-warn-against-nsa-changes/?mod=WSJ_hpp_MIDDLENexttoWhatsNewsForth

39) http://apps.washingtonpost.com/g/page/national/nsa-report-on-privacy-violations-in-the-first-quarter-of-2012/395/

40) Nidhi Subbaraman, *Facebook forensics? What the feds can learn from your digital crumbs*, NBC News (8. Juni 2013), abrufbar unter: www.nbcnews.com/technology/facebook-forensics-what-feds-can-learn-your-digital-crumbs-6C10240840

41) Bob Sullivan, *Big Brother may not be listening, but he's watching: Why metadata snooping is legal*, NBC News (15. Juni 2013)

42) Yves-Alexandre de Montjoye, César A. Hidalgo, Michel Verleysen & Vincent D. Blondel, *Unique in the Crowd: The privacy bounds of human mobility*, Scientific Reports (25. März 2013)

bei Facebook erkennen.[43] Diese neue Realität hat „die Unterscheidung zwischen Anklopfen und Eindringen sehr viel komplizierter gemacht".[44]

Bislang ist nicht klar, welche Abhilfemaßnahmen der Kongress oder das Gericht möglicherweise ergreifen werden. Selbst Befürworter im Kongress haben jedoch bereits Bedenken geäußert. Einige beklagten, sie seien nicht vollständig über die Datensammlung im Schleppnetzverfahren informiert worden,[45] während andere wie zum Beispiel einer der Verfasser des ursprünglichen *Patriot Act* bemängelten „die geheime Auslegung steht nicht im Einklang mit der ursprünglichen Absicht der Gesetzgebung". Zur Behebung des Problems wurden vier Gesetzesvorlagen eingebracht, die jeweils einen unterschiedlichen Ansatz verfolgten: (1) Anhebung der Mindestanforderung, indem verlangt wird, dass „spezifische und artikulierbare Fakten" vorgelegt werden und „jede der" Geschäftsunterlagen in Bezug zu einer Ermittlung stehen muss,[46] (2) Nachweis, dass die Aufzeichnungen „maßgeblich" oder von signifikanter Relevanz für eine Ermittlung sind, (3) Anforderung, dass jede Anordnung eine Begründung enthalten muss, weshalb die Aufzeichnungen eine Einzelperson „betreffen" oder für eine Ermittlung „relevant" sind,[47] und (4) als jüngste Vorlage, die zur Abstimmung kam, die Benennung einer konkreten Zielperson durch die NSA, wenn sie Telefonmitschnitte erstellen möchte.[48] Wenngleich die jüngste Vorlage mit 205 zu 217 Stimmen abgelehnt wurde, zeigt sich doch, dass eine Beschränkung der NSA-Befugnisse zunehmend Unterstützer findet und schließlich auch verabschiedet werden könnte, da die traditionellen Trennlinien zwischen den beiden Parteien in dieser Frage aufgehoben sind. Die gemeinsame Unterstützung konservativer und liberaler Abgeordneter und das knappe Abstimmungsergebnis waren besonders überraschend, da die Führungen beider Parteien gegen die Vorlage waren.

Es gab in jüngster Zeit auch Anzeichen dafür, dass sich der *Supreme Court* (Oberste Gerichtshof) der USA möglicherweise nicht zur Verfassungsmäßigkeit dieser Programme äußern wird. Im Februar 2012 befand der Gerichtshof, die Antragsteller - Rechtsanwälte, Journalisten und Menschenrechtsaktivisten - in einem Verfahren zur Überprüfung der Verfassungsmäßigkeit des Gesetzes, welches PRISM genehmigt, seien nicht klageberechtigt, da sie nicht darlegen konnten, dass sie durch das Gesetz persönlich betroffen waren.[49] Der Gerichtshof führte aus, die Annahme einer Überwachung sei zu spekulativ und die Überwachung der Kläger sei nicht „mit Sicherheit zu erwarten". Wenngleich die neuen Enthüllungen möglicherweise „zeigen, dass Überwachung ‚mit Sicherheit zu erwarten' ist, weil wir wissen, dass das PRISM-Programm existiert", gebe es immer noch Zweifel, ob dies ausreiche zu zeigen, dass die Regierung sie „im Besonderen" ausspioniert habe.

Allmählich jedoch wächst die Forderung nach einem Sonderermittlungsausschuss des Kongresses, nach mehr Transparenz und mehr Verantwortlichkeit. Die Bewegung wird von einer Koalition aus mehr als 100 Bürgerrechtsgruppen angeführt.

43) Michal Kosinski, David Stillwell, und Thore Graepel, *Private traits and attributes are predictable from digital records of human behavior*, Proceedings of the National Academy of Sciences of the United States (12. Februar 2013)
44) *S. o.* Fußnote 3
45) *S. o.* Fußnote 38
46) Mark M. Jaycox, *Bills Introduced by Congress Fail to Fix Unconstitutional NSA Spying,* Electronic Frontier Foundation (15. Juli 2013), abrufbar unter www.eff.org/deeplinks/2013/07/bills-fail-fix-unconstitutional-nsa-spying
47) Änderungsgesetz 2013 zum Electronic Communications Privacy Act, Bericht an den Senat zum Änderungsgesetz 2013 mit zusätzlichen Stellungnahmen zu Art. 607, Rechtsausschuss (16. Mai 2013), abrufbar unter: www.fas.org/irp/congress/2013_rpt/ecpa_amend.html
48) Ginger Gibson, "Justin Amash, John Conyers introduce NSA bill", *Politico* (18. Juni 2013), abrufbar unter www.politico.com/story/2013/06/justin-amash-john-conyers-nsa-bill-92982.html#ixzz2bUBXZXie
49) Cindy Cohn und Trevor Timm, *Supreme Court Dismisses Challenge to FISA Amendments Act; EFF's Lawsuit Over NSA Warrantless Wiretapping Remains*, Electronic Frontier Foundation, (27. Februar 2013), abrufbar unter www.eff.org/deeplinks/2013/02/supreme-court-dismisses-challenge-fisa-warrantless-wiretapping-law-effs-lawsuit

OBSERVATOIRE EUROPÉEN DE L'AUDIOVISUEL
EUROPEAN AUDIOVISUAL OBSERVATORY
EUROPÄISCHE AUDIOVISUELLE INFORMATIONSSTELLE

Informationen für den audiovisuellen Sektor

Der Auftrag der Europäischen Audiovisuellen Informationsstelle ist die Schaffung von mehr Transparenz im europäischen audiovisuellen Sektor. Die Umsetzung dieses Auftrags erfordert die Sammlung, Bearbeitung und Verbreitung von aktuellen und relevanten Informationen über die verschiedenen audiovisuellen Industrien.

Die Audiovisuelle Informationsstelle hat sich für eine pragmatische Definition des Begriffs des audiovisuellen Sektors entschieden. Die wichtigsten Arbeitsbereiche sind: Film, Fernsehen, Video/DVD, audiovisuelle nicht lineare Mediendienste, staatliche Maßnahmen für Film und Fernsehen. Auf diesen fünf Tätigkeitsfeldern bietet die Audiovisuelle Informationsstelle Informationen im juristischen Bereich sowie Informationen über die Märkte und die Finanzierungsmöglichkeiten an. Die Audiovisuelle Informationsstelle erfasst und analysiert Entwicklungen in ihren Mitgliedstaaten und auf europäischer Ebene. Wenn es angebracht erscheint, werden darüber hinaus auch außereuropäische Länder, die für Europa relevant sind, in die Beobachtung einbezogen. Die verschiedenen Phasen bis zur Informationsbereitstellung umfassen die systematische Sammlung, Analyse und Aufbereitung von Informationen und Daten. Die Weitergabe an die Nutzer erfolgt in Form von Publikationen, Online-Informationen, Datenbanken und Verzeichnissen von Internet-Links sowie Konferenzvorträgen. Die Arbeit der Informationsstelle stützt sich in hohem Maße auf internationale und nationale Quellen, die relevante Informationen bereitstellen. Zu diesem Zweck hat die Informationsstelle ein Netzwerk aus Partnerorganisationen und -institutionen, Informationsdienstleistern und ausgewählten Korrespondenten aufgebaut. Die primären Zielgruppen der Informationsstelle sind Fachleute im audiovisuellen Sektor: Produzenten, Verleiher, Kinobetreiber, Rundfunkveranstalter und Anbieter anderer Mediendienste, Mitarbeiter internationaler Organisationen im audiovisuellen Bereich, Entscheidungsträger innerhalb der verschiedenen Medienbehörden, nationale und europäische Gesetzgeber, Journalisten, Wissenschaftler, Juristen, Investoren und Berater.

Die Europäische Audiovisuelle Informationsstelle wurde im Dezember 1992 gegründet und ist dem Europarat über ein „Erweitertes Teilabkommen" angegliedert. Ihr Sitz befindet sich in Straßburg, Frankreich. Die Mitglieder der Informationsstelle sind zurzeit 39 europäische Staaten sowie die Europäische Union, vertreten durch die Europäische Kommission. Jedes Mitglied entsendet einen Vertreter in den Exekutivrat. Das internationale Team der Informationsstelle wird von einem Geschäftsführenden Direktor geleitet.

Die Produkte und Dienstleistungen der Informationsstelle lassen sich in vier Gruppen unterteilen:

- **Publikationen**
- **Online-Informationen**
- **Datenbanken und Verzeichnisse**
- **Konferenzen und Workshops**

Europäische Audiovisuelle Informationsstelle
76 Allée de la Robertsau – F-67000 Strasbourg – France
Tel.: +33 (0) 3 90 21 60 00 – Fax: +33 (0) 3 90 21 60 19
www.obs.coe.int – E-mail: obs@obs.coe.int

OBSERVATOIRE EUROPÉEN DE L'AUDIOVISUEL
EUROPEAN AUDIOVISUAL OBSERVATORY
EUROPÄISCHE AUDIOVISUELLE INFORMATIONSSTELLE

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

Juristische Informationsdienste der Europäischen Audiovisuellen Informationsstelle

Bestellen Sie:
- **unter http://www.obs.coe.int/about/order**
- **per Email: orders-obs@coe.int**
- **per Fax : +33 (0)3 90 21 60 19**

IRIS Newsletter

Rechtliche Rundschau der Europäischen Audiovisuellen Informationsstelle

Online, kostenlos!

Der IRIS Newsletter ist ein aktueller und zuverlässiger monatlicher Informationsdienst, der alle für den audiovisuellen Sektor rechtlich relevanten Ereignisse in Europa erfasst und aufbereitet. IRIS deckt alle für die audiovisuelle Industrie wichtigen juristischen Bereiche ab. Den Schwerpunkt der IRIS-Beiträge bilden Artikel über die rechtlichen Entwicklungen in den rund 50 Ländern eines erweiterten Europas. IRIS berichtet sowohl über Mediengesetzgebung als auch über wichtige Entwicklungen, Urteile, Verwaltungsentscheidungen und politische Beschlüsse mit möglichen rechtlichen Konsequenzen.
IRIS kann kostenlos per Email bezogen und über die IRIS Webseite abgerufen werden: http://merlin.obs.coe.int/newsletter.php

IRIS *plus*

Brandaktuelle Themen aus verschiedenen Blickwinkeln

Durch rechtliche, wirtschaftliche oder technologische Entwicklungen im audiovisuellen Sektor entstehen Themenkomplexe, die einen akuten Informationsbedarf aufwerfen. Diese Themen zu erkennen und den dazugehörigen rechtlichen Hintergrund zu liefern, das ist das Ziel von IRIS *plus*. Dazu bietet Ihnen IRIS *plus* eine Kombination aus einem Leitbeitrag, einer Zusammenstellung von Einzelberichterstattungen sowie ein *Zoom*-Kapitel mit Übersichtstabellen, aktuellen Marktdaten oder anderen praktischen Informationen. Dadurch erhalten Sie das notwendige Wissen, um den aktuellen Diskussionen im und über den audiovisuellen Sektor zu folgen.
Weitere Informationen: http://www.obs.coe.int/irisplus

IRIS Merlin

Datenbank für juristische Informationen von Relevanz für den audiovisuellen Sektor in Europa

Die Datenbank IRIS Merlin ermöglicht den Zugang zu mehr als 6.500 Beiträgen über juristische Ereignisse mit Bedeutung für den audiovisuellen Sektor. Darin beschrieben werden maßgebliche Gesetze, Entscheidungen verschiedener Gerichte und Verwaltungsbehörden sowie Strategiepapiere (policy documents) aus über 50 Ländern. Darüber hinaus enthalten sie Informationen über Rechtsinstrumente, Entscheidungen und Strategiepapiere der wichtigsten europäischen und internationalen Institutionen.
Freier Zugang unter: http://merlin.obs.coe.int

IRIS *Spezial*

Umfassende Fakten gepaart mit detaillierten Analysen

In den Ausgaben der Reihe IRIS *Spezial* geht es um aktuelle Fragen aus dem Medienrecht, die aus einer juristischen Perspektive aufbereitet werden. Die Reihe IRIS *Spezial* bietet einen umfassenden Überblick über die relevanten nationalen Gesetzgebungen und erleichtert so den Vergleich zwischen den jeweiligen Rechtsrahmen verschiedener Länder. Sie befasst sich immer mit hochgradig relevanten Themen und beschreibt den europäischen und internationalen rechtlichen Kontext, der Einfluss auf die jeweilige nationale Gesetzgebung hat. IRIS *Spezial* vermittelt die juristischen Analysen zudem in einer sehr zugänglichen Art und Weise, die sich auch Nicht-Juristen erschließt! Jede einzelne Ausgabe zeichnet sich gleichermaßen durch einen hohen praktischen Nutzen und eine streng wissenschaftliche Vorgehensweise aus. Eine Liste aller bisherigen IRIS *Spezial*-Ausgaben finden Sie unter: http://www.obs.coe.int/oea_publ/iris_special/index.html

OBSERVATOIRE EUROPÉEN DE L'AUDIOVISUEL
EUROPEAN AUDIOVISUAL OBSERVATORY
EUROPÄISCHE AUDIOVISUELLE INFORMATIONSSTELLE

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

IRIS *plus* 2013-6
Sind personenbezogene Daten wirklich privat?
25,50 € - ISBN 978-92-871-7792-6