FREY Rechtsanwälte • Kaiser-Wilhelm-Ring 40 • 50672 Köln

Vorab per Email
Deutscher Bundestag
Ausschuss für Kultur und Medien
Herrn MdB Sebastian Blumenthal,
Vorsitzender des UA Neue Medien
Platz der Republik 1
11011 Berlin

Rechtsanwälte
Dr. Dieter Frey, LL.M. (Brügge)*
Fachanwalt für Urheber- und Medienrecht

Dr. Matthias Rudolph*
Fachanwalt für Urheber- und Medienrecht

Dr. Philip Lüghausen
Rechtsanwalt

*Partner

Dr. Dieter Frey LL.M.
Tel. +49 (0) 221 / 420 748 00
Fax +49 (0) 221 / 420 748 29
Dieter.frey@frey.tv

Köln, den 18. Mai 2012

Aktenzeichen: (12)K0193
(Bitte bei Schriftverkehr angeben)

Deutscher Bundestag – Unterausschuss Neue Medien
Stellungnahme zum Thema „Vermarktung und Schutz kreativer Inhalte im Internet“

Sehr geehrter Herr Blumenthal,

gerne komme ich der Einladung des Unterausschusses Neue Medien nach, als Sachverständiger zu der öffentlichen Anhörung zum Thema „Vermarktung und Schutz kreativer Inhalte im Internet“ beizutragen.

Mit der nachstehenden Stellungnahme erlaube ich mir, die Antworten auf die von Ihnen übermittelten Fragen vorab zusammenzufassen. Dabei habe ich mich auf rechtliche Fragestellungen konzentriert, die das diskutierte „vorgerichtliche Warnhinweismodell“ aufwirft.

Zudem möchte ich auf das gemeinsam mit meinen Kollegen Dr. Matthias Rudolph und Dr. Jan Oster erstellte Rechtsgutachten zum Thema „Internetsperren und Schutz der Kommunikation im Internet“ verweisen. Dieses Rechtsgutachten, das als Beilage zu der Zeitschrift Multimedia und Recht im März 2012 erschienen ist, haben wir im Auftrag des eco-Verband – der deutschen Internetwirtschaft e.V. erarbeitet. Auch wenn wir uns im Rahmen dieses

Rechtsgutachtens insbesondere mit Internetsperren auseinandergesetzt haben, sind viele der dort ausgeführten Ergebnisse auch für die Diskussion über ein „vorgerichtliches Warnhinweismodell“ von Bedeutung. Aus diesem Grund erlauben wir uns, das Rechtsgutachten in der Anlage für die Mitglieder des Unterausschusses Neue Medien per Email zu übermitteln.

Zu Teil 1: Modelle zur Versendung von Warnhinweisen (aktuelle Gutachten)

Frage 1: Wie bewerten Sie das von Prof. Schwartmann im Rahmen des Wirtschaftsdialogs des BMWi vorgestellte vorgerichtliche Mitwirkungsmodell? Welche Alternativen böten sich aus Ihrer Sicht dazu an? Wie bewerten Sie die Gegenargumentation der Studie „Vergleich von Modellen zur Versendung von Warnhinweisen durch Internet-Zugangsanbieter an Nutzer bei Urheberrechtsverletzungen“ von Prof. Hoeren?

1. Das von Prof. Schwartmann mit seinem Autorenteam vorgeschlagene „vorgerichtliche Warnhinweismodell“ (von den Autoren auch als „vorgerichtliches Mitwirkungsmodell“ bezeichnet) und die dazu angebrachte rechtliche Begründung (nachfolgend „Schwartmann-Gutachten“) werden wir nachstehend insbesondere im Lichte des Telekommunikationsgeheimnisses bewerten.

2. Prof. Hoeren stellt in seinem Gutachten (nachfolgend „Hoeren-Gutachten“) das Verhältnis zwischen Rechteinhabern und Zugangsanbietern sowie deren Rechtspositionen in den Vordergrund. Wir teilen insofern wesentliche Kritikpunkte des Hoeren-Gutachtens an den Ergebnissen des Schwartmann-Gutachtens, ohne dass wir darauf im Einzelnen nachfolgend weitere eingehen. Auch das Schwartmann-Gutachten setzt den Schwerpunkt auf das Verhältnis zwischen Rechteinhabern und Zugangsanbietern. Dabei wird nach unserer Auffassung zu wenig berücksichtigt, dass sich das vorgeschlagene „vorgerichtliche Warnhinweismodell“ zentral auf die Nutzer auswirken und schwerwiegende Eingriffe in ihre Rechtspositionen nach sich ziehen würde.

A. Bewertung eines „vorgerichtlichen Warnhinweismodells“ gem. Schwartmann-Gutachten

3. In dem Schwartmann-Gutachten wird zunächst auf den Auskunftsanspruch nach § 101 UrhG, welcher mit dem zweiten Korb der Urheberrechtsreform eingeführt wurde, Bezug genommen. Dieser Anspruch setzt gem. § 101 Abs. 9 UrhG wegen des Rückgriffs auf Verkehrsdaten eine richterliche Anordnung für die Auskunftserteilung durch Zugangsanbieter voraus. Hierauf wird auch in dem Schwartmann-Gutachten

ausdrücklich (vgl. S. 305) verwiesen. Allerdings sei, so das Schwartmann-Gutachten, die Durchsetzung dieses Anspruchs gegenüber Access-Providern rechtlich und tatsächlich problematisch. Die Verwendung der hierdurch erlangten Informationen sei wenig zielgerichtet. Der hinter einer IP-Adresse stehende Klarname könne sich auf einen wenig gravierenden Einzelfall beziehen oder einen Mehrfachtäter treffen, insbesondere letzterer sei aber für den Rechteinhaber relevant.

4. Das „vorgerichtliche Warnhinweismodell" soll daher das bestehende System von Auskunftsanspruch und nachfolgender zivilrechtlicher Durchsetzung des urheberrechtlichen Anspruchs effektuieren. Dazu heißt es auf Seite 305f. des Schwartmann-Gutachtens wörtlich:

> „Die Zugangsanbieter sollte zum einen die Pflicht treffen, Warnhinweise an die Anschlussinhaber zu versenden, deren IP-Adresse im Zusammenhang mit der gemeldeten Rechtsverletzung ermittelt wurde. Sie sollte zum anderen die Pflicht treffen, […] eine gegenüber Dritten **anonymisierte Verstoßliste** zu führen und diese ab einer bestimmten Anzahl von festgehaltenen Verstößen, dem Rechteinhaber bekannt zu geben. Dieser kann dann, wie bisher, im Wege eines gerichtlichen Auskunftsverlangens Namen und Anschrift des Rechteinhabers[1] heraus verlangen. […] Der besondere Nutzen der Verstoßliste liegt darin, dass der Rechteinhaber hieraus ersehen kann, welche für ihn anonyme Person häufig oder gravierend Urheberrechte verletzt hat. Auf dieser Basis kann er seinen Auskunftsanspruch gegen den Provider gezielt mit Blick auf solche Fälle beschränken, die für eine gewerbsmäßige Urheberrechtsverletzung i. S. v. § 101 Abs. 2 Nr. 3 UrhG[2] in Betracht kommen.
>
> Das **Modell verbindet** damit die als solche sanktionslose **Warnhinweisregelung** über einen effektuierten **Auskunftsanspruch** mit der zivilrechtlichen Durchsetzung des Anspruchs als Sanktion der Rechtsverletzung. Dabei verzichtet der Ansatz aber auf eine Sanktion, die – wie Sperren oder Drosselung von Anschlüssen in Frankreich und Irland – über das derzeit in Deutschland geltende Recht hinausgeht. Da die Warnhinweisregelung selbst keine unmittelbare Sanktion kennt, ist es auch nicht zwingend, dass dem Zugangsanbieter durch den Rechteinhaber ein gerichtsfester Nachweis einer Rechtsverletzung überbracht wird, der über das zur Identifizierung des Anschlussinhabers und der Feststellung der Verletzung hinausgeht.
>
> Unabhängig davon erfasst der Ansatz über die Warnhinweise insbesondere auch solche Personen, die in Unkenntnis der Rechtslage Urheberrechte im Netz

---

1 Anmerkung: Hier muss es Anschlussinhabers heißen.

2 Anmerkung: Es ist davon auszugehen, dass hier die Verletzung einer Person in „gewerblichem Ausmaß" gem. § 101 Abs. 1 UrhG in Bezug genommen werden sollte.

verletzen. Aber auch Personen, die bewusst gegen Urheberrecht verstoßen, um eigennützig kostenfrei an Inhalte zu gelangen, würde über die Warnhinweise deutlich gemacht, dass sie auf der Verstoßliste geführt werden und einer zivilrechtlichen Inanspruchnahme entgegensehen." [*Hervorhebungen im Original, Anmerkungen wurden hinzugefügt*]

I. Vorgeschlagenes Modell eines „vorgerichtlichen Warnhinweismodells" praktisch unausgereift

5. Das vorgeschlagene „vorgerichtliche Warnhinweismodell" soll auch nach den Autoren des Schwartmann-Gutachtens nur einen Denkansatz darstellen. Allerdings lässt es zentrale Eckpunkte offen, die die Eingriffsintensität eines solchen Modells beeinflussen. Dies soll kurz anhand der Verstoßliste illustriert werden.

6. Access-Provider stünden zwischen einer sehr großen Zahl von Rechteinhabern einerseits und einer sehr großen Zahl von Kunden andererseits. Access-Provider müssten zur Realisierung der Verstoßliste eine komplexe Datenbankstruktur entwickeln, um Verstoßmeldungen der Rechteinhaber (z.B. Rechteinhaber 1 bis 1000) an Kunden als betroffene Anschlussinhaber (z.B. Kunde 1 bis 1 Mio.) zuzuordnen. Die Verstoßliste soll nach den Vorstellungen der Autoren des Schwartmann-Gutachtens die Anonymität der betroffenen Kunden wahren. Zur Erreichung der skizzierten Zwecke würde es sich allerdings tatsächlich nur um eine pseudonymisierte Liste handeln: Die Verstoßliste soll schließlich insbesondere dazu dienen, Kunden des Access-Providers zu identifizieren, über deren Anschluss mehrfach vermeintliche Rechtsverletzungen erfolgten. Der Access-Provider müsste daher weiterhin in der Lage sein, die Zuordnung einer zweiten Meldung vorzunehmen. Dabei müsste er aber auch feststellen können, ob etwa Rechteinhaber 1 im Hinblick auf den Kunden 1 einen zweiten Rechtsverstoß gemeldet hat. Problematisch wird dieser Ansatz besonders dann, wenn ein zweiter Rechtsverstoß nicht von Rechteinhaber 1 gemeldet wird, sondern z.B. Rechteinhaber 2 vorbringt, Kunde 1 habe seine Rechte verletzt. Der Access-Provider hätte in letzterem Fall zwar eine zweite Meldung über einen Rechtsverstoß, welche indes nicht den Rechteinhaber 1 betreffen würde.

7. Es bliebe daher vollkommen offen, wie vermeintliche Rechtsverstöße eines Kunden gegenüber unterschiedlichen Rechteinhabern zu behandeln sind. Dabei ist zu beachten, dass die beschriebene Problematik in der Praxis häufig anzutreffen Situation ist, etwa immer dann, wenn über einen Anschluss z.B. sog. Chart-Container verfügbar sind, in denen üblicherweise Musikdateien vieler verschiedener Rechteinhaber enthalten sind. Soll etwa der Access-Provider, nachdem ein zweiter oder dritter Rechtsverstoß eines Kunden durch unterschiedliche Rechteinhaber gemeldet wurde, sodann allen vermeintlich betroffenen Rechteinhabern das Verstoßregister dieses

Kunden übermitteln? Oder soll der Access-Provider das Verstoßregister des betreffenden Kunden auf betroffene Rechteinhaber aufteilen, indem nur vermeintliche Verstöße gegen urheberrechtlich geschützte Rechte des jeweils betroffenen Rechteinhabers gemeldet werden? Alternativ könnten wiederum alle Verstöße an alle betroffenen Rechteinhaber übermittelt werden, was den jeweils betroffenen Rechteinhabern keinen Aufschluss über die etwaige Qualität des Verstoßes gegen seine Rechtspositionen gibt.

8. Unklar bleibt auch, ob das „vorgerichtliche Warnhinweismodell“ auch implizieren soll, dass Kunden, die ihren Access-Provider wechseln, sich den Verstoßlisten entziehen können. Dies wäre jedenfalls die logische Folge, wenn jeder Access-Provider nur eine isolierte Verstoßliste führen soll. Sollte das vorgeschlagene „vorgerichtliche Warnhinweismodell“ übergreifend für Access-Provider funktionieren, müsste tatsächlich in privater Hand ein Datenpool aufgebaut werden, welcher alle angeblich Urheberrechtsverstöße zusammenfasst, um dann entsprechende Meldungen an Rechteinhaber auszuführen. Andernfalls hätten die Kunden eines Access-Providers einen sehr großen Anreiz, regelmäßig ihre Zugangsanbieter zu wechseln, um – ob berechtigt oder unberechtigt – einer Sanktion durch die Rechteinhaber zu entgehen.

II. Fernmeldegeheimnis nicht ausreichend berücksichtigt

9. Die Autoren des Schwartmann-Gutachtens setzen sich im Zusammenhang mit dem skizzierten „vorgerichtlichen Warnhinweismodell“ ausführlich mit verfassungsrechtlichen Fragen einer Inpflichtnahme der Zugangsanbieter auseinander (vgl. S. 306 ff. des Schwartmann-Gutachtens). Die zentrale Problematik des Eingriffs in das Fernmeldegeheimnis wird indes fast vollständig außer Acht gelassen. In diese Richtung dürfte lediglich der kurze Hinweis auf eine „datenschutzrechtliche Bedachtnahme“ auf Seite 306 zu verstehen sein. Sowohl für eine Versendung von Warnhinweisen als auch für die Führung der Verstoßliste stellten sich „*die angesprochenen Fragen im Zusammenhang mit der Vorratsdatenspeicherung*“. Welche diese sind, wird im Zusammenhang mit dem „vorgerichtlichen Warnhinweismodell“ nicht weiter ausgeführt. Der in eine Fußnote aufgenommene Verweis auf S. 292 des Schwartmann-Gutachtens bringt keinen wesentlichen Aufschluss. Hier wird lediglich kurz zum Urteil des Bundesverfassungsgerichts zur Vorratsdatenspeicherung referiert und sodann auf Seite 293 die nicht weiter vertiefte Frage aufgeworfen, ob die von dem Bundesverfassungsgericht in der Entscheidung zur Vorratsdatenspeicherung aufgestellten Kriterien auch für ein Warnhinweissystems gelten müssten. Das Schwartmann-Gutachten behandelt damit eine zentrale Frage der europarechtlichen und verfassungsrechtlichen Zulässigkeit eines „vorgerichtlichen Warnhinweismodells“ unzureichend.

1. Rückgriff auf Daten der Vorratsdatenspeicherung ausgeschlossen

10. Eine Verwendung von Verkehrsdaten für ein „vorgerichtliches Mitwirkungsmodell“ ist jedenfalls europarechtlich ausgeschlossen, sofern dazu die Daten herangezogen werden sollen, welche auf der Grundlage der Richtlinie 2006/24 (Vorratsdaten-Richtlinie) erhoben und gespeichert werden.

11. Nach dem Urteil des Europäischen Gerichtshofes vom 19. April 2012 in der Rechtssache C 461/10 *Bonnier u.a*. ist europarechtlich geklärt, dass es sich bei der Vorratsdaten-Richtlinie um eine klar abgegrenzte Spezialregelung handelt, welche ausschließlich Daten zum Zwecke der Ermittlung, Feststellung und Verfolgung von **schweren Straftaten** betrifft (vgl. EuGH, Rechtssache C 461/10 Rn. 38). Die zivilrechtliche Aufklärung von Urheberrechtsverletzungen kann daher nicht auf der Grundlage der anlasslos erhobenen Daten, welche auf die Vorratsdatenspeicherung zurückgehen, durchgeführt werden (vgl. auch EuGH, Rechtssache C 461/10 Rn. 44). Vor diesem Hintergrund ist zu konstatieren, dass Daten, die auf der Grundlage der Vorratsdaten-Richtlinie erhoben und gespeichert werden, nicht für die Erfüllung des Auskunftsanspruchs nach § 101 UrhG herangezogenen werden dürfen. Dies gilt erst recht für ein wie auch immer geartetes „vorgerichtliches Warnhinweismodell“, bei dem Private zur Effektuierung der Durchsetzung des Urheberrechts zusammenwirken sollen.

2. Unklar, ob gesetzliches oder freiwilliges Modell intendiert

12. Wenn in der Beschreibung des Modells ausgeführt wird, der Ansatz verzichte auf eine Sanktion, die – wie Sperren oder Drosselungen von Anschlüssen in Frankreich oder Irland – über das derzeit in Deutschland geltende Recht hinausgehe, lassen die Autoren des Schwartmann-Gutachtens zumindest offen, ob ein „vorgerichtliches Warnhinweismodell“ auf der Grundlage des geltenden Rechts verwirklicht werden kann. Eine solche Annahme wäre jedenfalls u.a. im Lichte des Telekommunikationsgeheimnisses rechtlich nicht haltbar.

13. Sollte ein „vorgerichtliches Warnhinweismodell“ auch nach Auffassung der Autoren des Schwartmann-Gutachtens ohne ausdrückliche gesetzliche Regelung nicht umzusetzen sein, ist zu konstatieren, dass zentrale verfassungs- und europarechtliche Anforderungen unberücksichtigt bleiben.

3. Der Schutz der Kommunikation im Internet gem. Art. 10 Abs. 1 GG

14. Die Frage, ob ein „vorgerichtliches Warnhinweismodell“, wie in dem Schwartmann-Gutachten vorgeschlagen, in das gem. Art. 10 Abs. 1 GG verbürgte Telekommunikationsgeheimnis eingreift, ist zentral für die Bewertung der verfassungsrechtlichen Anforderungen. In der jüngsten Rechtsprechung der Zivilgerichte hat sich die Erkenntnis durchgesetzt, dass jedenfalls Internetsperren ohne hinreichende Ermächtigungsgrundlage in unzulässiger Weise in den Schutzbereich des Telekommunikationsgeheimnis gem. Art. 10 Abs. 1 GG eingreifen.[3]

a) Gewährleistung der Privatheit auf Distanz

15. Art. 10 Abs. 1 GG gewährleistet das Telekommunikationsgeheimnis, welches die unkörperliche Übermittlung von Informationen an individuelle Empfänger mit Hilfe des Telekommunikationsverkehrs[4] schützt[5].

16. Das Grundrecht des Telekommunikationsgeheimnisses dient der freien Entfaltung der Persönlichkeit durch einen Kommunikationsaustausch mit Hilfe des Fernmeldeverkehrs[6]. Bei der Nutzung von Telekommunikationseinrichtungen ist die Kommunikation besonderen Gefährdungen der Kenntnisnahme durch Dritte ausgesetzt und unterliegt deshalb besonderem Schutz[7]. Das **Telekommunikationsgeheimnis soll gegen eine vom Betroffenen ungewollte Informationserhebung schützen und die Privatheit auf Distanz gewährleisten**[8]. Telekommunikation bietet die Voraussetzungen für die private Kommunikation zwischen Personen, die nicht am selben Ort sind, und eröffnet so eine neue Dimension der Privatsphäre. Damit verbunden ist ein Verlust an Privatheit; denn die Kommunizierenden müssen sich auf die technischen Besonderheiten eines Kommunikationsmediums einlassen und sich dem eingeschalteten Kommunikationsmittler anvertrauen. Inhalt und Umstände der Nachrichtenübermittlung sind dadurch dem erleichterten Zugriff Dritter ausgesetzt. Die Beteiligten, die ihre Kommunikation mit Hilfe von technischen Hilfsmitteln über Distanz unter Nutzung fremder Kommunikationsverbindungswege ausüben, haben nicht die Möglichkeit, die Vertraulichkeit der Kommunikation sicherzustellen[9]. Art. 10 Abs. 1 GG soll deshalb einen Ausgleich für die technisch bedingte Einbuße an Privatheit schaffen und will den

---

3 Vgl. dazu umfassend *Frey/Rudolph/Oster*, Internetsperren und der Schutz der Kommunikation im Internet, MMR Beilage 3/2012.

4 Vgl. BVerfG, Urt. v. 02.03.2010, Az. 1 BvR 256/08, Rn. 189; BVerfGE 106, 28, 35 f.; 120, 274, 306 f.

5 Vgl. BVerfG, Urt. v. 02.03.2010, Az. 1 BvR 256/08, Rn. 189; BVerfGE 100, 313, 358; 106, 28, 37.

6 BVerfGE 106, 28, 35f.

7 BVerfGE 106, 28, 36; vgl. bereits BVerfGE 67, 157, 171f.; 85, 386, 396.

8 BVerfGE 115, 166, 182; Bs. vom 22.08.2006, 2 BvR 1345/03 – IMSI-Catcher, NJW 2007, 351, 353 – Rn. 51.

9 BVerfG, Bs v. 22.08.2006, 2 BvR 1345/03 – IMSI-Catcher, NJW 2007, 351, 353 – Rn. 53.

Gefahren begegnen, die sich aus dem Übermittlungsvorgang einschließlich der Einschaltung eines Dritten ergeben[10].

17. Das Risiko, dass sich Dritte Zugang zu den Inhalten und Umständen der Kommunikation verschaffen, ist besonders groß, wenn es vielfältige technische Möglichkeiten des Zugriffs durch Dritte gibt, wie dies gegenwärtig angesichts der Vernetzung moderner Infrastrukturen der Telekommunikation und der Einschaltung mehrerer Dienste für einen Übermittlungsvorgang typischerweise der Fall ist[11].

18. Der Schutz des Art. 10 Abs. 1 GG erfasst Telekommunikation, einerlei, welche Übermittlungsart (Kabel oder Funk, analoge oder digitale Vermittlung) und welche Ausdrucksform (Sprache, Bilder, Töne, Zeichen oder sonstige Daten) genutzt werden[12]. Der Schutzbereich dieses Grundrechts ist dabei unabhängig davon betroffen, ob die Maßnahme technisch auf der Übertragungsstrecke oder am Endgerät der Telekommunikation ansetzt[13].

19. Dieser Schutz erfasst dabei nicht nur die Inhalte der Kommunikation. Geschützt ist vielmehr auch die Vertraulichkeit der näheren Umstände des Kommunikationsvorgangs, zu denen insbesondere gehört, ob, wann und wie oft zwischen welchen Personen oder Telekommunikationseinrichtungen Telekommunikationsverkehr stattgefunden hat oder versucht worden ist[14].

20. **Mit der grundrechtlichen Verbürgung der Unverletzlichkeit des Fernmeldegeheimnisses soll vermieden werden, dass der Meinungs- und Informationsaustausch mittels Fernmeldeanlagen deswegen unterbleibt oder nach Form und Inhalt verändert verläuft**, weil die Beteiligten damit rechnen müssen, dass staatliche Stellen sich in die Kommunikation einschalten und Kenntnisse über die Kommunikationsbeziehungen oder Kommunikationsinhalte gewinnen[15]

21. Das Bundesverfassungsgericht stellt in der Entscheidung zur Vorratsdatenspeicherung für die Kommunikation im Internet ausdrücklich fest, dass die Speicherung der den Internetzugang betreffenden Daten einen Eingriff in Art. 10 Abs. 1 GG darstellt. Auch die genutzte (dynamische) IP-Adresse ist durch Art. 10 Abs. 1 GG geschützt. Dies hat das Bundesverfassungsgericht zuletzt in seinem Urteil vom 24. Januar 2012 in Bezug

---

10 BVerfG, Bs v. 22.08.2006, 2 BvR 1345/03 – IMSI-Catcher, NJW 2007, 351, 353 – Rn. 54; vgl. BVerfGE 106, 28, 36; 107, 299, 313.

11 BVerfGE 106, 28, 36.

12 BVerfG, Urt. v. 27.02.2008 – Online-Durchsuchung, NJW 2008, 822, 825 f. - Rn. 183; vgl. BVerfGE 106, 28, 36; 115, 166, 182 f.

13 Vgl. BVerfGE 106, 28, 37f.; 115, 166, 186 f.

14 Vgl. BVerfG, Urt. v. 2.03.2010, Az. 1 BvR 256/08, Rn. 189; BVerfGE 67, 157, 172; 85, 386, 396; 100, 313, 358; 107, 299, 312 f.; 115, 166, 183; 120, 274, 307.

15 BVerfGE 107, 229, 313; 100, 313, 358 f.

auf dynamische IP-Adresse nach der Internet-Protokoll-Version 4 (IPv4) ausdrücklich festgestellt[16]. Die Kenntnis einer Kontaktaufnahme mit einem Internetangebot hat bereits eine inhaltliche Bedeutung: Da der Inhalt von Internetangeboten elektronisch fixiert und länger wieder aufrufbar ist, lässt sich mit der IP-Adresse vielfach verlässlich rekonstruieren, mit welchem Gegenstand sich der Kommunizierende auseinander gesetzt hat[17]. Das Bundesverfassungsgericht leitet aus Art. 10 GG auch das prinzipielle Recht des Einzelnen ab, in der Regel davon ausgehen zu können, das Internet anonym zu nutzen und zu erfahren, dass und warum diese Anonymität aufgehoben wurde[18].

22. Da eine Unterscheidung zwischen Individual- und Massenkommunikation ohne eine der Schutzfunktion des Grundrechts zuwiderlaufende Anknüpfung an den Inhalt der jeweils übermittelten Information nicht möglich ist, ist nach Auffassung des Bundesverfassungsgerichts bereits in der Speicherung der den Internetzugang als solchen betreffenden Daten ein Eingriff zu sehen, auch wenn sie Angaben über die aufgerufenen Internetangebote nicht enthalten[19].

23. Das Bundesverfassungsgericht folgt zu Recht nicht der teilweise im Schrifttum vertretenen Auffassung, wonach sich öffentlich zugängliche Angebote im Internet an die Allgemeinheit richteten und es daher an einer durch Art. 10 Abs. 1 GG geschützten Individualkommunikation fehle[20]. Der Begriff des Fernmeldegeheimnisses ist dynamisch zu verstehen und muss auf technische Weiterentwicklung erstreckt werden[21]. Eine Differenzierung zwischen Massen- und Individualkommunikation wird durch die Konvergenz der Medien zunehmend obsolet[22].

---

16 Vgl. BVerfG, Urtl. V. 24.01.2012, I BvR 1299/05, Rn. 111.

17 BVerfG, Urt. v. 02.03.2010, Az. 1 BvR 256/08, Rn. 259.

18 BVerfG, Urt. v. 02.03.2010, Az. 1 BvR 256/08, Rn. 263.

19 Vgl. BVerfG, Urt. v. 02.03.2010, Az. 1 BvR 256/08, Rn. 192. Das BVerfG stützt sich hierbei auf die entsprechende Auffassung von *Gusy*, in: v. Mangoldt/Klein/Starck, GG, Bd. 1, 5. Aufl. 2005, Art. 10 Rn. 44 und *Hermes*, in: Dreier, GG, Bd. 1, 2. Aufl. 2004, Art. 10 Rn. 39.

20 So *Durner*, ZUM 2010, 833, 838 f., der die angeblich herrschende Meinung unzutreffend wiedergibt.

21 Vgl. BVerfG, Urt. v. 02.03.2006, Az: 2 BvR 2099/04, Rn. 67; *Sieber/Nolde*, Sperrverfügungen im Internet, 2008, S. 81.

22 Vgl. *Degenhart*, CR 2011, 231, 232; *Klesczewski*, in: Säcker (Hrsg.), Berliner Kommentar zum TKG, 2. Aufl. 2009, § 88 Rn. 12; *Hermes*, in: Dreier, GG, Band I 2004, Art. 10 Rn. 20, 39; Pieroth/Schlink, Grundrechte – Staatsrecht II, 26. Aufl. 2010, Rn. 837; *Koreng*, Zensur im Internet, 2010, S. 56; *Sieber/Nolde*, Sperrverfügungen im Internet, 2008, S. 80; *Frey/Rudolph*, Haftungsregimes für Host- und Access-Provider im Bereich der Telemedien, 2009, Rn. 19 m.w.N.; bereits instruktiv *Sievers*, Der Schutz der Kommunikation im Internet durch Art. 10 des Grundgesetzes, S. 129 f.; ebenso *Germann*, Gefahrenabwehr und Strafverfolgung im Internet, S. 118; *Degen*, Freiwillige Selbstkontrolle der Access-Provider, S. 288 f.; differenzierend aber z.B. *Billmeier*, Die Düsseldorfer Sperrungsverfügung, S. 182 ff., der zufolge das Abrufen von Webseiten nur dann dem Schutzbereich des Fernmeldegeheimnisses unterfällt, wenn der Anbieter Vorkehrungen getroffen hat, welche erst noch überwunden werden müssen, sodass nicht jedermann sein Angebot abrufen kann.

24. Die Kommunikation im Internet ist daher umfassend geschützt. Dies betrifft nicht nur die Konstellationen, in denen eine verbale Kommunikation als ursprünglichste Form der Fernkommunikation über das Internet erfolgt, wie z.B. bei Voice over IP, oder eine Fernkommunikation in Wort und Schrift wie z.B. per E-Mail, durch Chat-Dienste, Instant-Messaging usw. Vielmehr wird die gesamte Kommunikation im Internet durch Art. 10 GG erfasst. Geschützt ist auch die Vertraulichkeit der näheren Umstände des Kommunikationsvorgangs im Internet, zu denen insbesondere gehört, ob, wann und wie oft zwischen welchen Personen oder Telekommunikationseinrichtungen Telekommunikationsverkehr stattgefunden hat oder versucht worden ist.

b) Eingriff in das Telekommunikationsgeheimnis

25. Ein Grundrechtseingriff ist zunächst jede Kenntnisnahme, Aufzeichnung und Verwertung von Kommunikationsdaten sowie jede Auswertung ihres Inhalts oder sonstige Verwendung durch die öffentliche Gewalt[23].

aa) Abgleich, Auswertung und Selektierung

26. In der Erfassung von Telekommunikationsdaten, ihrer Speicherung, ihrem Abgleich mit anderen Daten, ihrer Auswertung, ihrer Selektierung zur weiteren Verwendung oder ihrer Übermittlung an Dritte, liegen damit je eigene Eingriffe in das Telekommunikationsgeheimnis[24].

bb) Zurechenbarer Eingriff durch Access-Provider

27. Teilweise wird in der Literatur[25] im Hinblick auf Sperrungsverfügungen, die von Access-Providern umgesetzt werden sollen, vertreten, dass diese nicht zu Eingriffen in den Schutzbereich des Telekommunikationsgeheimnisses gem. Art. 10 Abs. 1 GG führen, da Access-Provider nicht hoheitlich handeln.

28. Zutreffend ist insoweit, dass das Telekommunikationsgeheimnis nicht unmittelbar vor privatem Handeln schützt, sondern der Sicherstellung einer unbeeinträchtigten Kommunikation der Nutzer dient. Bei behördlichen Sperrverfügungen (ebenso wie bei einem vorgerichtlichen Warnhinweismodell) erhalten staatliche Stellen – anders als beispielsweise bei einer polizeilichen Telefonüberwachung – zudem nicht zwangsläufig

---

23 Vgl. BVerfG, Urt. v. 02.03.2010, Az. 1 BvR 256/08, Rn. 190; BVerfGE 85, 386, 398; 100, 313, 366; 110, 33, 52 f.

25 *Vgl. Büssow/v. Schmeling*, Die Internetaufsicht über unerlaubtes Glücksspiel, ZfWG 2010, 239, 245; siehe auch die Stellungnahme des Bundesinnenministerium im Rahmen der Diskussion zum ZugErschwG http://blog.odem.org/2009/03/12/bmi-stellungnahme-gg10-bild.pdf.

Kenntnis von den Telekommunikationsdaten, sondern zunächst allein die Access-Provider[26].

29. Ein Grundrechtseingriff kann jedoch auch dann vorliegen, wenn die – auf gesetzliche bzw. behördliche Anweisung erfolgte – Nutzung von Kommunikationsdaten durch *private Anbieter* erfolgt. Das Bundesverfassungsgericht hat in seiner Entscheidung zur Vorratsdatenspeicherung hierzu festgestellt:

> „In der Erfassung von Telekommunikationsdaten, ihrer Speicherung, ihrem Abgleich mit anderen Daten, ihrer Auswertung, ihrer Selektierung zur weiteren Verwendung oder ihrer Übermittlung an Dritte liegen damit je eigene Eingriffe in das Telekommunikationsgeheimnis (vgl. BVerfGE 100, 313 <366 f.>). Folglich liegt in der Anordnung gegenüber Kommunikationsunternehmen, Telekommunikationsdaten zu erheben, zu speichern und an staatliche Stellen zu übermitteln, *jeweils* ein Eingriff in Art. 10 Abs. 1 GG (vgl. BVerfGE 107, 299 <313>)“[27]. [Hervorhebung hinzugefügt]

30. Ferner heißt es in dem Urteil:

> „Die Eingriffsqualität des § 113a TKG wird auch nicht dadurch in Frage gestellt, dass die in dieser Vorschrift vorgeschriebene Speicherung **nicht durch den Staat selbst, sondern durch private Diensteanbieter** erfolgt. Denn diese werden allein als Hilfspersonen für die Aufgabenerfüllung durch staatliche Behörden in Anspruch genommen. § 113a TKG verpflichtet die privaten Telekommunikationsunternehmen zur Datenspeicherung allein für die Aufgabenerfüllung durch staatliche Behörden zu Zwecken der Strafverfolgung, der Gefahrenabwehr und der Erfüllung nachrichtendienstlicher Aufgaben gemäß § 113b TKG. Dabei ordnet der Staat die mit der Speicherung verbundene Grundrechtsbeeinträchtigung unmittelbar an, ohne dass den speicherungspflichtigen Unternehmen insoweit ein Handlungsspielraum verbleibt; die Daten sind so zu speichern, dass Auskunftsersuchen der berechtigten öffentlichen Stellen nach § 113a Abs. 9 TKG unverzüglich erfüllt werden können. Unter diesen Voraussetzungen ist die Speicherung der Daten **rechtlich dem Gesetzgeber als unmittelbarer Eingriff in Art. 10 Abs. 1 GG zuzurechnen** (vgl. BVerfGE 107, 299 <313 f.>)“[28]. [Hervorhebungen hinzugefügt]

---

26 Hierauf weisen *Ennuschat/Klestil*, ZfWG 2009, 389, 393 hin.

27 BVerfG, Urt. v. 02.03.2010, Az. 1 BvR 256/08, 1 BvR 263/08, 1 BvR 586/08, Rn. 190 – Vorratsdatenspeicherung.

28 BVerfG, Urt. v. 02.03.2010, Az. 1 BvR 256/08, 1 BvR 263/08, 1 BvR 586/08, Rn. 193 – Vorratsdatenspeicherung.

31. Im Lichte der vorstehend aufgezeigten Rechtsprechung des Bundesverfassungsgerichts ist daher immer dann, wenn der Staat die mit einer Handlung eines Privaten verbundene Grundrechtsbeeinträchtigung unmittelbar anordnet, ohne dass den handelnden Unternehmen insoweit ein Handlungsspielraum verbleibt, von einem dem Staat zurechenbaren unmittelbaren Eingriff in das Telekommunikationsgeheimnis auszugehen.

cc) Telekommunikationsgeheimnis entfaltet auch im Zivilrecht Wirkung

32. Die besondere Bedeutung des Schutzes der Kommunikation im Internet wird von den Zivilgerichten in jüngeren Entscheidungen besonders hervorgehoben. Das LG Hamburg[29] und das LG Köln[30] haben dabei ausdrücklich unterstrichen, dass eine gerichtliche Sperrungsanordnung, unabhängig von der technischen Methode, einen Eingriff in das von Art. 10 GG geschützte Telekommunikationsgeheimnis darstellen würde.

(1) Drittwirkung der Grundrechte

33. Privatpersonen und Unternehmen sind zunächst im Rahmen der sog. mittelbaren Drittwirkung an Grundrechte gebunden[31]. Die Auffassung, dass Art. 10 Abs. 1 GG unmittelbare Drittwirkung zwischen Privaten entfaltet,[32] hat sich nicht durchgesetzt. Die in Art. 10 Abs. 1 GG enthaltene objektive Wertentscheidung strahlt aber im Rahmen der mittelbaren Drittwirkung auf die Auslegung und Anwendung einfachgesetzlicher privatrechtlicher Vorschriften aus[33]. Das Grundrecht ist daher bei der Auslegung und Anwendung privatrechtlicher Vorschriften zu berücksichtigen. Vor allem sog. Generalklauseln stellen „Einbruchstellen“ der Grundrechte in das Bürgerliche Recht dar[34].

34. Die vorliegende Konstellation birgt jedoch gegenüber den „klassischen“ Fällen (mittelbarer) Drittwirkung eine Besonderheit. Der private Access-Provider soll im Rahmen eines „vorgerichtlichen Warnhinweismodells“ dazu angehalten werden, in Kommunikationsvorgänge von nicht am Verfahren Beteiligten, nämlich seiner Kunden, einzugreifen. Anders als in hergebrachten Fällen der Drittwirkung von Grundrechten

---

29 LG Hamburg, Urt. v. 12.03.2010, Az. 308 O 640/08, MMR 2010, 488, 490.

30 LG Köln, Urt. v. 31.08.2011, Az. 28 O 362/10, BeckRS 2011, 22073.

31 BVerfGE 7, 198, 205 f. – Lüth.

32 So *Gusy* in von Mangoldt/Klein/Starck, GG Band 1, 5. Aufl. 2005, Art. 10 Rn. 53 jedenfalls im Hinblick auf die Deutsche Telekom.

33 *Hermes* in Dreier, GG, Band I 2004, Art. 10 Rn. 81; *Baldus* in Epping/Hillgruber, GG, 2009, Art. 10 Rn. 61.

34 BVerfGE 7, 198, 206.

geht es somit nicht nur um eine Abwägung der Grundrechtspositionen von Rechteinhabern und Access-Providern, sondern um den erstrebten Eingriff eines Access-Providers in die Rechte von Personen, die am Verfahren nicht beteiligt sind. Ein Access-Provider würde also im Fall eines „vorgerichtlichen Warnhinweismodells“ instrumentalisiert, um die Rechte eines Rechteinhabers durchzusetzen. Daher erlangen die aus Art. 10 Abs. 1 GG abzuleitenden Schutzpflichten besondere Relevanz.

(2) Schutzpflicht aus Art. 10 Abs. 1 GG

35. Ein „vorgerichtliches Warnhinweismodell“ würde insbesondere die Gefahr bergen, die von Art. 10 Abs. 1 GG begründete Schutzpflicht zu verletzen.

36. Infolge der Privatisierung der Deutschen Bundespost werden Telekommunikations- und Postdienstleistungen nicht mehr von einer staatlichen Stelle, sondern von privaten Anbietern erbracht. Das Schutzbedürfnis der Kommunikationsteilnehmer nach der Vertraulichkeit ihrer Kommunikation ist durch die Privatisierung jedoch nicht geringer geworden, sondern hat sich durch die rasante Entwicklung der Telekommunikationsmöglichkeiten im vergangenen Jahrzehnt sogar verstärkt. Eine Ausprägung des Privatisierungsfolgenrechts[35] des ehemaligen Post- und Telekommunikations-Staatsmonopols ist daher, dass der Staat die Kommunikationsdienstleistungen nicht mehr gegenständlich erbringt, dass er jedoch dazu verpflichtet ist, die Bürger vor Missbräuchen privater Anbieter zu schützen[36]. Es ist daher nahezu unstreitig, dass Art. 10 Abs. 1 GG eine staatliche Pflicht zum Schutz privater Fernkommunikation begründet[37].

37. Aus Art. 10 Abs. 1 Alt. 3 GG folgt somit die Pflicht staatlicher Hoheitsträger, die Vertraulichkeit des Fernmeldegeheimnisses gegenüber Übergriffen durch Private zu

---

35 *Ruffert*, AöR 124 (1999), 237, 246; *Schliesky*, Öffentliches Wirtschaftsrecht, 3. Aufl. 2008, S. 284.

36 BVerfG, Beschl. v. 09.10.2002, Az. 1 BvR 1611/96, 1 BvR 805/98, Rn. 24 (juris) – Mithörvorrichtung: „Schutzauftrag“; LG Hamburg, Urt. v. 12.03.2010, Az. 308 O 640/08, Rn. 46 (juris).

37 *Gusy*, in: von Mangoldt/Klein/Starck, GG Band 1, 5. Aufl. 2005, Art. 10 Rn. 61 ff.; *Baldus*, in: Epping/Hillgruber, GG, 2009, Art. 10 Rn. 60; *Klesczewski*, in: Säcker (Hrsg.), Berliner Kommentar zum TKG, 2. Aufl. 2009, § 88 Rn. 9; *Pieroth/Schlink*, Grundrechte – Staatsrecht II, 26. Aufl. 2010, Rn. 827; *Durner*, ZUM 2010, 833, 835 f.; *Löwer*, in: von Münch/Kunig, GG, Band I, 5. Aufl. 2000, Art. 10 Rn. 14; *Groß*, JZ 1999, 326 ff.; *Badura*, Staatsrecht, 4. Aufl. 2010, Teil C Rn. 42; *Hermes*, in: Dreier, GG, Band I 2004, Art. 10 Rn. 83; *Zerres*, in: Scheurle/Mayen, TKG, 2. Aufl. 2008, § 88 Rn. 2; kritisch *Pagenkopf*, in: Sachs, GG, 5. Aufl. 2009, Art. 10 Rn. 21; ablehnend *Schmitt Glaeser*, in: Isensee/Kirchof, HStR VI, 2. Aufl. 2001, § 129 Rn. 66. Zu staatlichen Schutzpflichten allgemein BVerfGE 88, 203, 251 ff.; *Dietlein*, Die Lehre von den grundrechtlichen Schutzpflichten, 1992; *Unruh*, Zur Dogmatik der grundrechtlichen Schutzpflichten, 1996.

schützen. Mit § 88 TKG, flankiert durch § 206 StGB, ist der Gesetzgeber seiner Schutzpflicht aus Art. 10 Abs. 1 GG im Hinblick auf das Verhältnis zwischen Privaten nachgekommen[38]. Dabei übertrug der Gesetzgeber weitgehend die verfassungsrechtlichen Maßgaben auf das einfache Recht[39]. Die Schutzbereiche von Art. 10 Abs. 1 GG und § 88 TKG sind daher in weitem Umfang identisch zu interpretieren[40], da jedenfalls § 88 TKG nicht hinter der sich aus Art. 10 Abs. 1 GG ergebenden Schutzpflicht zurückstehen darf. Daraus folgt, dass die Umsetzung eines „vorgerichtlichen Warnhinweismodells" auch eine Beeinträchtigung der staatlichen Schutzpflicht aus Art. 10 Abs. 1 GG darstellen würde.

(3) Die durch § 88 TKG geschützte Kommunikation im Internet

38. § 88 Abs. 2 Satz 1 TKG verpflichtet jeden Diensteanbieter einfachgesetzlich zur Wahrung des Telekommunikationsgeheimnisses. Gemäß § 88 Abs. 1 Satz 2 TKG unterliegen dem Fernmeldegeheimnis sowohl der Inhalt der Telekommunikation als auch ihre näheren Umstände, *insbesondere* die Tatsache, ob jemand an einem Telekommunikationsvorgang beteiligt ist oder war. Diensteanbietern ist es nach Abs. 3 Satz 1 untersagt, sich oder Anderen über das für die geschäftsmäßige Erbringung der Telekommunikationsdienste einschließlich des Schutzes ihrer technischen Systeme erforderliche Maß hinaus Kenntnis vom Inhalt oder den näheren Umständen der Telekommunikation zu verschaffen. Sie dürfen nach Satz 2 Kenntnisse über Tatsachen, die dem Telekommunikationsgeheimnis unterliegen, nur für die Erbringung der Telekommunikationsdienste einschließlich des Schutzes ihrer technischen Systeme verwenden. Eine Verwendung dieser Kenntnisse für andere Zwecke, insbesondere die Weitergabe an andere, ist nach Satz 3 nur zulässig, soweit das TKG oder eine andere gesetzliche Vorschrift dies vorsieht und sich dabei ausdrücklich auf Telekommunikationsvorgänge bezieht. § 88 Abs. 3 TKG statuiert damit zwei Verbote: zum einen das absolute Verbot in Satz 1, sich Kenntnisse über Tatsachen, die dem Telekommunikationsgeheimnis unterliegen, *zu verschaffen*, wenn dies nicht für die Erbringung der Telekommunikationsdienste erforderlich ist (Erforderlichkeitsgrundsatz), und zum anderen das grundsätzliche Verbot in Satz 2, *bereits vorhandene* Informationen für andere Zwecke als die Erbringung von Telekommunikationsdiensten zu *verwenden* (Prinzip der Zweckgebundenheit).

---

38 BVerfGE 106, 28, 37.

39 *Groß*, JZ 1999, 326, 334 f.

40 *Groß*, JZ 1999, 326, 332 ff.; *Klesczewski*, in: Säcker (Hrsg.), Berliner Kommentar zum TKG, 2. Aufl. 2009, § 88 Rn. 9; *Eckhardt*, in: Spindler/Schuster, Recht der elektronischen Medien, 2. Aufl. 2011, TKG § 88 Rn. 4; *Durner*, ZUM 2010, 833, 836; vgl. *Ellinghaus*, in: Arndt/Fetzer/Scherer, TKG, 2008, § 88 Rn. 7 („vergleichbares Schutzniveau").

39. Eine „vorgerichtliches Warnhinweismodell“ würde im Lichte des geltenden Rechts auch gegen das einfachgesetzlich geschützte Telekommunikationsgeheimnis verstoßen, da weder der Erforderlichkeitsgrundsatz noch das Prinzip der Zweckgebundenheit Beachtung fände.

c) Weitere verfassungsrechtliche Anforderungen

40. Eingriffe in das Telekommunikationsgeheimnis sind gem. Art. 10 Abs. 2 Satz 1 GG nur auf Grund eines Gesetzes zulässig, dass auch im Übrigen verfassungsgemäß sein muss, d.h. insbesondere den Bestimmtheitsgrundsatz und das Zitiergebot gem. Art. 19 GG zu wahren hat. Schließlich gilt es zu berücksichtigen, dass das Gesetz den Grundsatz der Verhältnismäßigkeit zu beachten hat.

41. Ein „vorgerichtliches Warnhinweisverfahren“ würde neben dem Eingriff in das Fernmeldegeheimnis in vielerlei Hinsicht weitere grundrechtliche Relevanz entfalten. Wie sowohl das Schwartmann-Gutachten als auch das Hoeren-Gutachten verdeutlichen, sind hier insbesondere die Berufsfreiheit und der Eigentumsschutz der Access-Provider einschlägig. Gleiches gilt für die Meinungsfreiheit der Anbieter von Inhalten und die Informationsfreiheit der Nutzer.

III. Schutz der Kommunikation im Internet im Recht der Europäischen Union

42. Die Autoren des Schwartmann-Gutachtens deuten an, dass ein „vorgerichtliches Warnhinweismodell“ kompatibel mit dem Recht der Europäischen Union und der Rechtsprechung des EuGH in der Rechtssache *Scarlet* ist (vgl. S. 177f.). Dieses Ergebnis erscheint zweifelhaft.

43. Rechtlicher Maßstab für den Schutz der Kommunikation im Internet ist insbesondere die Charta der Grundrechte der Europäischen Union sowie spezifische Rechtsakte des Sekundärrechts wie die Richtlinie 95/46/EG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, die Richtlinie 2002/58/EG über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation und die Richtlinie 2000/31/EG über den elektronischen Geschäftsverkehr.

1. Charta der Grundrechte

44. Seit dem Inkrafttreten der Charta der Grundrechte der Europäischen Union („Charta“) mit dem Vertrag von Lissabon am 1. Dezember 2009 ist der Schutz der

Kommunikation im Internet auf europäischer Ebene anhand der Grundrechte aus Art. 7, 8 und 11 der Charta zu messen. Die Charta gilt dabei gemäß Art. 6 Abs. 1 EUV gleichrangig neben dem übrigen Primärrecht der Europäischen Union[41].

45. Gemäß Art. 51 Abs. 1 gilt die Charta für die Organe, Einrichtungen und sonstigen Stellen der Union sowie für die Mitgliedsstaaten bei der Durchführung des Rechts der Union[42]. Die Art. 7, 8 und 11 der Charta garantieren das Recht auf Achtung des Privat- und Familienlebens, auf Schutz personenbezogener Daten, die Freiheit der Meinungsäußerung und die Informationsfreiheit.

46. Gemäß Art. 52 Abs. 3 der Charta sind den Rechten der Charta, die den durch die Europäische Konvention zum Schutz der Menschenrechte und Grundfreiheiten („EMRK“) garantierten Rechten entsprechen, die gleiche Bedeutung und Tragweite, wie sie ihnen in der genannten Konvention verliehen wird, beizumessen. Daher ist für die Frage der Vertraulichkeit der elektronischen Kommunikation gem. Art. 7 und 8 der Charta auch Art. 8 EMRK heranzuziehen. Hier hat der Europäische Gerichtshof für Menschenrechte („EGMR“) bereits deutlich gemacht, dass die Überwachung der Nutzung von Telefonen, des Emailverkehrs und des Internets in den Schutzbereich von Art. 8 Abs. 1 EMRK fällt[43] .

47. Art. 7 der Charta gibt im Wesentlichen Art. 8 der EMRK wieder, der die Achtung des Privatlebens garantiert[44], und Art. 8 der Charta proklamiert ausdrücklich den Schutz personenbezogener Daten[45]. Der grundrechtliche Schutz der Kommunikation im Internet wird auf der Ebene der Europäischen Union durch Art. 5 der Richtlinie 2002/58/EG weiter ausgeformt. Danach ist die Vertraulichkeit der mit öffentlichen Kommunikationsnetzen und öffentlich zugänglichen Kommunikationsdiensten übertragenden Nachrichten und der damit verbundenen Verkehrsdaten sicherzustellen[46].

---

41 Vgl. *Kingreen* in Callies/Ruffert, EUV Art. 6 Rn. 12; vgl. Allgemein zur Geltung der Charta der Grundrechte und ihrer Auslegung *Huber*, Auslegung und Anwendung der Charta der Grundrechte, NJW 2011, 2385 ff.; *Kirchhoff*, Grundrechtsschutz durch europäische und nationale Gerichte, NJW 2011, 3681 ff.

42 Vgl. im Einzelnen zur Reichweite des Art. 51 der Charta, *Huber*, Auslegung und Anwendung der Charta der Grundrechte, NJW 2011, 2385 ff.

43 EGMR, Urteil v. 03.04.2007, Copland gegen Vereinigtes Königreich, Beschwerde Nr. 62617/00, Rn. 43 und 44.

44 Ein entsprechender Schutzgehalt ergibt sich sekundärrechtlich auch aus der Richtlinie 2002/58/EG. Gemäß dem 2. Erwägungsgrund ist Ziel dieser Richtlinie die Achtung der Grundrechte und dass sie im Einklang mit den durch die Charta anerkannten Grundsätzen steht. Insbesondere soll mit dieser Richtlinie nach der Rechtsprechung des EuGH gewährleistet werden, dass die in den Art. 7 und 8 der Charta niedergelegten Rechte uneingeschränkt geachtet werden.

45 EuGH, Urteil v. 29.01.2008, Rs. C-275/06 – Promusicae, Rn. 64.

46 Vgl dazu auch die Schlussanträge v. 14.04.2011 des Generalanwalts Cruz Villalón in der Rechtssache C-70/10 – Scarlet Extented, Rn. 73 ff.

48. Bezogenen auf die Kommunikation im Internet verstärkt Art. 8 der Charta als spezielle Ausgestaltung des Schutzes der Privatsphäre gem. Art. 7 der Charta den grundrechtlichen Schutz, wenn personenbezogene Daten betroffen sind. Dabei stellt sich die Frage, ob für die Umsetzung eines „vorgerichtlichen Warnhinweismodells" personenbezogene Daten verarbeitet würden[47]. Die Diskussion betrifft in erster Linie den Aspekt, ob IP-Adressen als personenbezogene Daten geschützt sind. Diese von Datenschützern eindeutig bejahte Frage[48] wurde von dem EUGH in der Vergangenheit insofern positiv beschieden, als IP-Adressen durch Access-Provider zur Erfüllung von Auskunftsansprüchen mit den bei ihnen vorliegenden Kundendaten zusammengeführt wurden[49]. In dem am 24. November 2011 ergangenen Urteil des EuGH in der Rechtssache *Sarlet Extended* machte der Gerichtshof im Zusammenhang mit der gerichtlich geltend gemachten Forderung von Rechteinhabern, ein Access-Provider möge ein Filter- und Sperrsystem gegen Urheberrechtsverletzungen einrichten, ohne Einschränkungen deutlich, dass IP-Adressen als personenbezogene Daten einzustufen sind und somit den Schutz des Art. 8 der Charta genießen[50].

2. Entscheidung des EuGH in der Rechtssache Scarlet Extended vom 24. November 2011

49. In der Rechtsache *Scarlet Extended*[51] musste der EuGH über die Zulässigkeit der Einrichtung eines Filter- und Sperrsystems für die Internetkommunikation im Lichte des Unionsrechts urteilen. Das Vorabentscheidungsersuchen des Brüsseler Berufungsgerichts betraf die durch die belgische Verwertungsgesellschaft SABAM erstrebte gerichtliche Anordnung, durch die Einrichtung eines Filter- und Sperrsystems Urheberrechtsverletzungen im Internet zu verhindern. Der Access-Provider Scarlet Extended sollte verpflichtet werden, ein System der Filterung aller seine Dienste durchlaufenden elektronischen Kommunikationen insbesondere bei der Verwendung von „Peer-To-Peer" Programmen einzurichten. Das System sollte zeitlich unbegrenzt und ausschließlich auf Kosten des Access-Providers eingerichtet werden, unterschiedslos für seine Kunden anwendbar sein und präventiv wirken. Es sollte zudem in der Lage sein, im Netz von Scarlet den Austausch von Dateien zu

---

47 Vgl. dazu *Hawellek*: EUGH: IP-Adressen sind personenbezogene Daten, ZD-Aktuell 2011, 129 ff.

48 Vgl. z.B. Article 29 Working Group, Opinion 2/2010 on online behavioural advertising, 00909/10/EN, S. 9.

49 EuGH, Urteil v. 29.01.2008, Rs. C-275/06 – Promusicae; Beschluss v. 19.02.2009, Rs. C-557/07 – LSG ./. Tele2. Vgl. dazu auch die Schlussanträge v. 17.11.2011 des Generalanwalts Jääskinen in der Rs. C-461/10 Bonnier Audio AB ua., Rn. 42.

50 Vgl. EuGH, Urteil v. 24.11.2011, Rs. C-70/10 – Scarlet Extended, Rn. 51. Siehe auch *Hawellek*, EuGH: IP-Adressen sind personenbezogene Daten, ZD-Aktuell 2011, 129, 130.

51 EuGH, Urteil v. 24.11.2011, Rs. C-70/10 – Scarlet Extended.

identifizieren, die ein Werk der Musik, ein Filmwerk oder audiovisuelle Werke enthalten, an denen SABAM Rechte zu haben behauptet, um die Übertragung von Dateien, deren Austausch gegen das Urheberrecht verstößt, zu sperren[52].

50. Der EUGH verwies in diesem Zusammenhang zunächst auf Art. 8 Abs. 3 der Richtlinie 2001/29/EG (Urheberrechtsrichtlinie) und Art. 11 Satz 3 der Richtlinie 2004/48/EG (Enforcement-Richtlinie), wonach Inhaber von Rechten des geistigen Eigentums gerichtliche Anordnungen gegen Vermittler beantragen können, wenn deren Dienste von einem Dritten zur Verletzung ihrer Rechte genutzt werden. Hiernach seien auch Maßnahmen gegen Access-Provider denkbar. Die Modalitäten einer Anordnung, die Mitgliedsstaaten nach den genannten Bestimmungen vorzusehen hätten, wie beispielweise die Tatbestandsvoraussetzungen einer Anordnung und das einzuhaltende Verfahren, müssten Gegenstand einzelstaatlicher Rechtsvorschriften sein[53]. Solche einzelstaatlichen Rechtsvorschriften sowie ihre Anwendung durch nationale Gerichte hätten indes die Beschränkungen zu berücksichtigen, die sich aus dem gemeinschaftsrechtlichen Sekundärrecht sowie aus den Grundrechten ergeben.

51. Eine Verpflichtung zur präventiven Überwachung sämtlicher Daten der Kunden eines Access-Providers erklärte der EuGH für unzulässig, da Art. 15 Abs. 1 der Richtlinie 2000/31/EG (Richtlinie über den elektronischen Geschäftsverkehr), welcher allgemeine Überwachungsverpflichtungen untersagt, die Auferlegung solcher Pflichten grundsätzlich ausschließt[54]. Des Weiteren unterstrich der EuGH, dass den Grundrechten Rechnung zu tragen ist. In der zu entscheidenden Fallkonstellation standen sich das Recht am geistigen Eigentum, welches durch Art. 17 Abs. 2 der Charta geschützt ist, und die Grundrechte der Nutzer und des Access-Providers gegenüber. Daher müsse ein angemessenes Gleichgewicht zwischen den betroffenen Grundrechten hergestellt werden[55]. Dazu führte der EuGH aus, dass durch das angedachte Filter- und Sperrsystem nicht nur der betroffene Access-Provider in seiner unternehmerischen Freiheit, die durch Art. 16 der Charta geschützt ist, betroffen sei, sondern auch die Grundrechte seiner Kunden beeinträchtigt würden. Der EuGH nahm insoweit ausdrücklich Bezug auf die in Art. 8 und 11 der Charta geschützten Rechte auf den Schutz personenbezogener Daten und auf den freien Empfang bzw. die freie Sendung von Informationen[56]. Der streitgegenständliche Filter- und Sperrmechanismus setzte die Sammlung und Identifizierung der IP-Adressen der Nutzer voraus, um den Abruf unzulässiger Inhalte durch die Kunden des Access-Providers zu unterbinden[57].

---

52 EuGH, Urteil v. 24.11.2011, Rs. C-70/10 – Scarlet Extended, Rn. 15 ff.

53 EuGH, Urteil v. 24.11.2011, Rs. C-70/10 – Scarlet Extended, Rn. 32.

54 Vgl. EuGH, Urteil v. 24.11.2011, Rs. C-70/10 – Scarlet Extended, Rn. 35 f.

55 Vgl. EuGH, Urteil v. 24.11.2011, Rs. C-70/10 – Scarlet Extended, Rn. 45 f.

56 Vgl. EuGH, Urteil v. 24.11.2011, Rs. C-70/10 – Scarlet Extended, Rn. 50.

57 Vgl. EuGH, Urteil v. 24.11.2011, Rs. C-70/10 – Scarlet Extended, Rn. 51.

52. Schließlich unterstrich der EuGH in der Rechtssache *Scarlet Extended*, dass die streitgegenständliche Filter- und Sperranordnung auch die Informationsfreiheit, die durch Art. 11 der Charta geschützt ist, beeinträchtigen kann, wenn ein betreffendes System nicht hinreichend zwischen einem unzulässigen Inhalt und einem zulässigem Inhalt unterscheiden kann[58].

53. Das streitgegenständliche Filter- und Sperrsystem genügte nach dem Urteil des EuGH in der Sache *Scarlet Extended* daher nicht den Anforderungen, die die Grundrechte der Europäischen Union und das europäische Sekundärrecht an den Schutz der Kommunikation im Internet stellen.

3. Fazit

54. Die Vorabentscheidung des EuGH in der Rechtssache *Scarlet Extended* hatte einen qualifizierten Eingriff in die unternehmerische Freiheit des Access-Providers zum Gegenstand. Auch die Intensität der Eingriffe in die Grundrechte aus Art. 8 und 10 der Charta, welche die Nutzer schützen, war erheblich. Schließlich sollte ihr gesamter Datenverkehr auf urheberrechtsverletzende Kommunikationsinhalte untersucht werden. Auch ein „vorgerichtliches Warnhinweismodell“ würde eine Analyse des Kommunikationsverhaltens der Nutzer anhand der von Rechteinhaber übermitteln IP-Adresse mit sich bringen. Es setzt ebenfalls am Kommunikationsverhalten der Nutzer an und erfordert es, die Kommunikationsziele von Kunden eines Access-Providers zu identifizieren, um den betreffenden Anschlussinhaber gegebenenfalls verwarnen zu können. Ein „vorgerichtliches Warnhinweismodell“ erfordert auch immer einen Rückgriff auf die IP-Adresse der Nutzer. Durch den Schutz der IP-Adresse als personenbezogenes Datum nach Art. 8 der Charta ist auch unionsrechtlich die Vertraulichkeit des Kommunikationsverhaltens der Nutzer im Internet geschützt. Damit wäre eine „vorgerichtliches Warnhinweismodell“ unionsrechtlich entsprechend der durch den EuGH entschiedenen Fallkonstellation als Eingriffe in Art. 8 und 10 der Charta zu beurteilen.

55. Das Unionsrecht – auch das macht der EuGH in dem Urteil *Scarlet Extended* deutlich - sucht einen Ausgleich zwischen widerstreitenden Grundrechtspositionen. Für einen solchen Ausgleich verbleibt den Mitgliedsstaaten ein nicht unerheblicher Beurteilungsspielraum. Der umfassende Schutz der Kommunikation im Internet durch das deutsche Recht, insbesondere durch Art. 10 GG, wird daher durch das Unionsrecht nicht in Frage gestellt.

---

58 Vgl. EuGH, Urteil v. 24.11.2011, Rs. C-70/10 – Scarlet Extended, Rn. 52.

56. Aus der Rechtsprechung des EuGH ergibt sich vielmehr, dass die Mitgliedsstaaten unionsrechtlich verpflichtet sind, dem Vorbehalt des Gesetzes zu genügen[59]. Ein „vorgerichtliches Warnhinweismodell“ wäre daher auch unionsrechtlich allenfalls denkbar, wenn seine Voraussetzungen und das anzuwendende Verfahren detailliert gesetzlich geregelt sind und der Grundsatz der Verhältnismäßigkeit berücksichtigt worden ist. Ein entsprechender gesetzlicher Rahmen besteht im deutschen Recht jedoch nicht, insbesondere wird auch die Frage nach einer ausreichenden rechtsstaatlichen Absicherungsmöglichkeit eines zwischen Privaten ablaufenden vorgerichtlichen Warnhinweismodells durch die Autoren des Schwartmann-Gutachten offen gelassen.

IV. Ergebnis

57. Ein „vorgerichtliches Warnhinweismodell“ würde in den Schutzbereich des durch Art. 10 Abs. 1 GG geschützten Telekommunikationsgeheimnisses eingreifen und wäre nur auf Grund eines Gesetzes, das das Zitiergebot und den Bestimmtheitsgrundsatz wahrt, denkbar. Auch unionsrechtlich wäre ein solches Warnhinweismodell allenfalls zu erwägen, wenn die Voraussetzungen und das Verfahren seiner Anwendung detailliert gesetzlich geregelt sind und der Grundsatz der Verhältnismäßigkeit berücksichtigt worden ist. Eine Regelung, die den vorstehend skizzierten Anforderungen entsprechen könnte, wird von den Autoren des Schwartmann-Gutachtens nicht vorgeschlagen. Vielmehr bestehen erhebliche Zweifel, ob eine solche Regelung gelingen kann, die die Kontrolle der durch das Telekommunikationsgeheimnis geschützten Kommunikation im Internet in die Hände Privater legen soll. Eine verfassungskonforme Absicherung eines solchen Modells, das auf eine zielgerichtete Verfolgung von Urheberrechtsverletzungen verzichtet, erscheint auch im Lichte des legitimen Zwecks, die Rechtsdurchsetzung in der Internetsphäre zu verbessern, kaum vorstellbar.

58. Darüber hinaus wirft das Modell unter weiteren rechtsstaatlichen Gesichtspunkten Bedenken auf. Ziel ist die effektive Bekämpfung der sog. „Internetpiraterie“. Dazu müsste offensichtlich auf eine Prüfung im Einzelfall durch unabhängige Richter verzichtet und Access-Provider müssten zur Durchsetzung der privaten Interessen der Rechteinhaber für Unterstützungsleistungen in Anspruch genommen werden. Eine solche Privatisierung der zivilrechtlichen Rechtsdurchsetzung dürfte nur schwerlich mit dem rechtstaatlichen Anspruch auf rechtliches Gehör vereinbar sein und würde Access-Providern ohne entsprechende wirtschaftliche Kompensation ein nicht unbeachtliches Sonderopfer abverlangen.

---

[59] Vgl. dazu auch die Schlussanträge v. 14.04.2011 des Generalanwalts Cruz Villalón in der Rechtssache C-70/10 – Scarlet Extented, Rn. 88 ff.

B. Alternative bei der Rechtsdurchsetzung

59. Einem „vorgerichtlichen Warnhinweismodell“ ist in jedem Fall ein rechtsstaatliches Verfahren vorzuziehen, wie es auf der Grundlage des Auskunftsanspruchs nach § 101 UrhG möglich ist. Unabhängig von dem zu kritisierenden Phänomen, dass einzelne spezialisierte Anwaltskanzleien standardisierte Massenabmahnungen nutzen, um in erster Linie ihr Honoraraufkommen unverhältnismäßig zu steigern, hat das zivilrechtliche Vorgehen gegen Urheberrechtsverletzungen in P2P-Netzen Wirkung gezeigt. Die Zahl von Urheberrechtsverletzungen geht zurück.

60. Daneben sollte im Bereich des Host-Providings verstärkt gegen unseriöse Anbieter vorgegangen werden. Die Fälle „*kino.to*“, „*megaupload.com*“, „*ifile.it*“ und „*library.nu*“ stehen für wichtige Erfolge, mit denen gewerbsmäßige Urheberrechtsverletzungen im Bereich des Sharehostings abgestellt werden konnten. Im deutschen Recht wird als Haftungsmaßstab u.a. auf das Kriterium eines „*von der Rechtsordnung gebilligten Geschäftsmodells*“ zurückgegriffen. Dabei handelt es sich um einen von der Rechtsprechung entwickelten Gedanken, der im Hinblick auf die Bestimmung von Sorgfaltsmaßstäben entwickelt wurde. Verfolgt ein Host-Provider ein generell auf Urheberrechtverletzungen angelegtes „*Geschäftsmodell*“, kann es durch strafrechtliche und zivilrechtliche Maßnahmen unterbunden werden. Ein Notice & Takedown-Verfahren für Host-Provider mit von der Rechtsordnung gebilligten Geschäftsmodellen kann darüber hinaus zu einem Ausgleich zwischen einer effektiven Rechtsdurchsetzung und dem Interesse der Nutzer führen, sich im Internet weitestgehend unbeobachtet zu bewegen. Vorteile eines Notice & Takedown-Verfahrens im Bereich des Host-Providings wären die Vermeidung von Gerichtsverfahren, die schnelle und unkomplizierte Beseitigung der Rechtsverletzung, die Verhinderung ausufernder Überwachungspflichten, die Schaffung von Rechtssicherheit für Host-Provider sowie der Ausschluss der Notwendigkeit einer generellen „Deanonymisierung“ der Nutzer.

61. Neben der zielgerichteten Verfolgung von Rechtsverletzern erscheint für einen effektiven Schutz urheberrechtlich geschützter Werke und die Ausschöpfung des ökonomischen Potentials digitaler Güter auch ein proaktives Vorgehen der Rechteinhaber notwendig. Im Lichte der weiterhin großen Zahl von Rechtsverletzungen steht es Rechteinhaber im digitalen Umfeld offen, digitale Werke durch technische Schutzmaßnahmen und Digital-Rights-Management-Systeme zu kontrollieren. Alle relevanten Rechtsordnungen haben dazu die notwendigen rechtlichen Voraussetzungen geschaffen. Das Ausschöpfen dieses Rechtsrahmens und der Einsatz einfach zu nutzender, interoperabler Schutzmechanismen, die gleichzeitig verbraucherfreundlich sind, kann Rechteinhabern sowohl den urheberrechtlichen Ausschließlichkeitsanspruch als auch eine angemessene Vergütung sichern.

62. Gleichzeitig muss die Fortentwicklung des Urheberrechts vorangetrieben werden. Wie auch die Diskussion über ein „vorgerichtliches Warnhinweismodell“ zeigt, birgt die Fokussierung auf urheberrechtliche Ausschließlichkeitsrechte im digitalen Umfeld die Gefahr unangemessener Freiheitseinbußen durch Überwachungsmaßnahmen, die einer freiheitlich-demokratischen Gesellschaft nicht gerecht werden. Daher sollte de lege ferenda der urheberrechtliche Vergütungsanspruch stärker betont werden, wenn Werke nicht von Urhebern oder Verwertern durch technische Schutzmaßnahmen geschützt werden. Als Ausgleich für den Verzicht auf Ausschließlichkeitsrechte für frei zugängliche Werke im digitalen Umfeld könnten die Systeme der Pauschalvergütung und der kollektiven Rechtewahrnehmung gestärkt werden, um den betroffenen Urhebern eine angemessene Beteiligung an den Früchten ihrer schöpferischen Leistung zu gewährleisten.

4) Welchen Beitrag leisten die Netzwerkprovider zur Bewusstseinsstärkung und Rechtsdurchsetzung im Falle von Urheberrechtsverletzungen? Wie bewerten Sie die Forderungen aus Wirtschaft und Politik, dass diese einen Beitrag auch aus Gründen der Corporate Social Responsibility leisten sollten?

63. Access-Provider leisten gegenwärtig einen beachtlichen Beitrag bei der Rechtsdurchsetzung von Urheberrechtsverletzungen, indem sie - nach Angaben des eco-Verbands - im Rahmen des zivilrechtlichen Auskunftsanspruchs pro Monat Benutzerdaten zu 300.000 Internetanschlüssen an Rechteinhaber übermitteln.

64. Access-Provider könnten sich zusätzlich an allgemeinen Aufklärungskampagnen beteiligen, um auf die Beachtung fremder Urheberrechte und sonstiger Immaterialgüterrechte hinzuweisen. Ergänzend könnten sie Aufklärungsmaterial in einer für Nichtjuristen verständlichen Art und Weise auf einer medientypisch verfügbaren Webseite des Access-Providers bereithalten.

5) Welche Konsequenzen hätte die Implementierung von Filter- und Analysetechniken in die Netzwerke hinsichtlich Vertraulichkeit und Integrität von Datenübertragungen aus Ihrer Sicht?

65. Die Implementierung von Filter- und Analysetechniken in Netzwerken zur Unterbindung von Urheberrechtsverletzungen hätte gravierende Konsequenzen für die Vertraulichkeit und Integrität von telekommunikationsrechtlich geschützten Kommunikationsinfrastrukturen. Siehe hierzu bereits Frage 1).

7) Sind sie der Auffassung, dass ein Warnhinweismodell bzw. ein vorgerichtliches Mitwirkungsmodell angesichts der damit einhergehenden Grundrechtseingriffe auf

freiwilliger Basis im Rahmen einer Selbstregulierung umgesetzt werden könnte oder sollte dies auf gesetzlicher Grundlage erfolgen?

66. Wie in der Antwort auf Frage 1) bereits ausgeführt, ist ein vorgerichtliches Warnhinweismodell nach geltendem Telekommunikation- und Verfassungsrecht, auch unter Berücksichtigung des Unionsrechts, nicht zulässig. Hieran scheitert insbesondere auch ein Modell auf freiwilliger Basis im Rahmen einer Selbstregulierung.

8) Wie bewerten sie das „vorgerichtliche Mitwirkungsmodell" im Hinblick auf seine verfassungsrechtliche und europarechtliche Vereinbarkeit?

67. Siehe hierzu die Antwort zu Frage 1).

9) Welche Konsequenzen ergeben sich für das „vorgerichtliche Warnhinweismodell" aus der Entscheidung des Bundesverfassungsgerichtes vom 24. Januar 2012 (1 BvR 1299/05), in der die Zuordnung von dynamischen IP-Adressen ausdrücklich als ein Eingriff in Art. 10 Abs. 1 GG festgestellt wurde?

68. Wie bereits in der Antwort auf Frage 1) ausgeführt, folgt aus dieser Entscheidung des Bundesverfassungsgerichts, dass ein vorgerichtliches Warnhinweismodell nach geltendem Recht das in Art. 10 Abs. 1 GG verbürgte Telekommunikationsgeheimnis verletzt (vgl. zu den Einzelheiten oben die Antwort auf Frage 1).

10) Sind sie der Auffassung, dass ein Warnhinweis- oder vorgerichtliches Mitwirkungsmodell als eine Kooperationsmöglichkeit anzusehen ist, die der Verpflichtung im ACTA-Abkommen entspricht, Kooperationsbemühungen im Wirtschaftsleben zu fördern, die darauf gerichtet sind, Verstöße gegen Marken, Urheberrechte oder verwandte Schutzrechte wirksam zu bekämpfen?

69. Art. 27 Abs. 3 ACTA[60] enthält das Gebot an die Vertragsstaaten, „*bestrebt zu sein, Kooperationsbemühungen im Wirtschaftsleben*" zur wirksamen Bekämpfung von Schutzrechtsverletzungen zu fördern.

70. Die Regelung lautet (in der deutschen Übersetzung) wie folgt: *„Jede Vertragspartei ist bestrebt, Kooperationsbemühungen im Wirtschaftsleben zu fördern, die darauf gerichtet sind, Verstöße gegen Marken, Urheberrechte oder verwandte Schutzrechte wirksam zu bekämpfen und gleichzeitig den rechtmäßigen Wettbewerb und – in Übereinstimmung mit den Rechtsvorschriften der jeweiligen Vertragspartei – Grundsätze wie freie Meinungsäußerung, faire Gerichtsverfahren und Schutz der Privatsphäre zu beachten."*

---

[60] Anti-Counterfeiting Trade Agreement, Interinstitutionelles Dossier des Rats der Europäischen Union, Az.: 12196/11, abzurufen unter „http://register.consilium.europa.eu/pdf/de/11/st12/st12196.de11.pdf".

71. Die Bestimmungen sind auslegungsbedürftig. Gemäß Art 31 Abs. 1 WVRK[61] ist ACTA als völkerrechtlicher Vertrag „*nach Treu und Glauben in Übereinstimmung mit der gewöhnlichen, seinen Bestimmungen in ihrem Zusammenhang zukommenden Bedeutung und im Lichte seines Zieles und Zweckes*“ auszulegen. Zur Auslegung kann nach Art. 31 Abs. 2 WVRK auch der Wortlaut der Präambel herangezogen werden.

72. Das Gebot aus Art. 27 Abs. 3 ACTA konkretisiert den in der Präambel niedergelegten Wunsch der Vertragsparteien, „*die Zusammenarbeit zwischen Dienstleistern und Rechteinhabern zu fördern, um einschlägigen Rechtsverletzungen im digitalen Umfeld entgegenzuwirken.*“ Zweck des Vertrages ist damit ausdrücklich, die Zusammenarbeit zwischen privaten Wirtschaftsunternehmen auf der horizontalen Ebene zu stärken. Access-Provider sind Dienstleister im Sinne des ACTA, insbesondere unter Berücksichtigung der Stellung des Art. 27 ACTA im 5. Abschnitt „Durchsetzung der Rechte des geistigen Eigentums im digitalen Umfeld“.

73. Gemessen an der skizzierten Ausgangsposition lässt sich zunächst festhalten, dass ein „vorgerichtliche Mitwirkungsmodell“ als Instrumentarium angeführt werden kann, das dazu geeignet ist, eine Zusammenarbeit zwischen Rechteinhabern und Access-Providern herbeizuführen. Eine Umsetzung des Modells in nationales Recht entspräche damit grundsätzlich dem Gebot, Kooperationen im Wirtschaftsleben zu fördern.

74. Art 27 Abs. 3 ACTA enthält jedoch zugleich die einschränkende Formulierung, dass das Gebot der Förderung von Kooperationsbemühung unter Beachtung der Rechtsvorschriften der jeweiligen Vertragspartei umzusetzen ist. Als Maßstab ist hier der „rechtmäßige Wettbewerb“ sowie – nicht abschließend – Grundsätze der freien Meinungsäußerung, faire Gerichtsverfahren und der Schutz der Privatsphäre genannt. Das „vorgerichtliche Mitwirkungsmodell“ ist aber – wie unter Frage 1 erläutert - nur schwer mit den unions- und verfassungsrechtlichen Vorgaben in Einklang zu bringen. Zugleich entspräche es damit auch nicht der Einschränkung des Art. 27 Abs. 3 2. HS ACTA, da es nicht in „*Übereinstimmung mit den Rechtsvorschriften des jeweiligen Mitglieds*“ umgesetzt werden kann.

11) Können ihrer Meinung nach bereits heute Warnhinweise anstelle kostenintensiver Abmahnungen verschickt werden? Bedarf es hierfür einer zusätzlichen Inpflichtnahme der Internetzugangsanbieter?

75. Es bleibt den Rechteinhabern unbenommen, anstelle von kostenpflichtigen Abmahnung den Anschlussinhabern Warnhinweise zuzusenden, von denen sie meinen, dass nach Durchsetzung des zivilrechtlichen Auskunftsanspruchs eine

[61] Wiener Übereinkommen über das Recht der Verträge v. 23. Mai 1969, BGBl. 1985 II, S. 927 ff.; UNTS Bd. 1155, S. 331 ff.

Urheberrechtsverletzung ausgeht. Allerdings dürften Rechteinhaber an einer solchen Form von Warnhinweisen kein Interesse haben, da sie trotz der Kosten des Auskunftsanspruchs von den vermeintlichen Rechtsverletzern keinen Schadensersatz realisieren würden.

Mit freundlichen Grüßen

Dr. Dieter Frey
(Rechtsanwalt)