WALDORF FROMMER Rechtsanwälte • Beethovenstraße 12 • 80336 München

Notifizierungsverfahren zum Entwurf eines
Dritten Gesetzes zur Änderung des Telemediengesetzes,
Notifizierungsnummer 2017/131/D

Stellungnahme zu dem Gesetzesentwurf der Bundesregierung eines Dritten Gesetzes zur Änderung des Telemediengesetzes (3. TMGÄndG)

WALDORF FROMMER ist eine auf das Urheber- und Medienrecht spezialisierte Rechtsanwaltskanzlei, die zahlreiche namhafte Film-, Musik- und Verlagsmandanten vertritt. Die Kanzlei ist seit vielen Jahren mit der Durchsetzung der Rechte am geistigen Eigentum in Fällen von gewerblichen bzw. nicht gewerblichen Rechtsverletzungen im Internet betraut.

Der gegenüber der Kommission notifizierte und am 5. April 2017 durch das Bundeskabinett beschlossene Gesetzesentwurf (im Folgenden *„Regierungsentwurf“* bzw. *„RegE 3. TMGÄndG“*, Notifizierungsnummer 2017/131/D) führt zu **gravierenden Einschnitten in die gefestigten Rechtspositionen der Rechteinhaber**:

Der Regierungsentwurf **beseitigt sämtliche** anerkannten Möglichkeiten, Access-Provider bei Rechtsverletzungen Dritter auf Beseitigung und Unterlassung in Anspruch zu nehmen (§ 8 Abs. 1 S. 2 TMG-E). Der Entwurf möchte insofern gezielt die Anwendung der aktuellen Rechtsprechung aus den Leitentscheidungen des **Europäischen Gerichtshofes** *McFadden* (Rs. C-484/14) und *UPC Telekabel* (Rs. C-314/12) bzw. des **Bundesgerichtshofes** *Sommer unseres Lebens* (Az. I ZR 121/08) und *Störerhaftung des Access-Providers* (Az. I ZR 174/14) verhindern.

Insbesondere findet keinerlei Ausgleich der wechselseitig betroffenen Interessen statt, wie ihn der Europäische Gerichtshof in ständiger Rechtsprechung fordert, u.a. in seiner Leitentscheidung *Promusicae* (Rs. C-275/06). Vielmehr werden die Interessen der geschädigten Rechteinhaber gegenüber den Interessen der Diensteanbieter bzw. deren Nutzer eklatant missachtet. Ein Interessenausgleich findet erkennbar nicht (mehr) statt.

Es steht zu befürchten, dass der vorliegende Regierungsentwurf, der „in letzter Minute“ zum Ende der laufenden Legislaturperiode als besonders eilbedürftig eingebracht wurde, nicht nur überhastet und daher handwerklich unzureichend, sondern vielmehr unter massivem Verstoß gegen europäisches Recht verabschiedet wird.

I. Ersatzlose Abschaffung jedweder Haftung von herkömmlichen Access-Providern

Der Regierungsentwurf führt – im Vergleich zum Referentenentwurf vom 23.02.2017 – nicht mehr nur zu einer Beschränkung der bestehenden Rechtsverfolgungsmöglichkeiten gegenüber Betreibern drahtloser Netzwerke. Die Bundesregierung schafft die Rechtsverfolgungsmöglichkeiten gegenüber herkömmlichen Access-Providern nunmehr sogar gänzlich ab.

Hatte der Referentenentwurf zunächst noch das neu eingeführte Rechtsinstitut der *Nutzungssperre* auch gegenüber herkömmlichen Access-Providern vorgesehen, beschränkt der Regierungsentwurf diese Anspruchsgrundlage nunmehr explizit auf *„Diensteanbieter nach § 8 Absatz 3 TMG“*, also auf Betreiber drahtloser Netzwerke.

Die bestehenden Möglichkeiten, herkömmliche Access-Provider, also Anbieter von Festnetz- und Mobilfunk-Internetzugängen, bei Rechtsverletzungen Dritter in Anspruch zu nehmen (vgl. u.a. EuGH *UPC Telekabel*), sollen zukünftig also ersatzlos entfallen.

Der Regierungsentwurf ist damit mit den europäischen Vorgaben unvereinbar (siehe hierzu unter IV.).

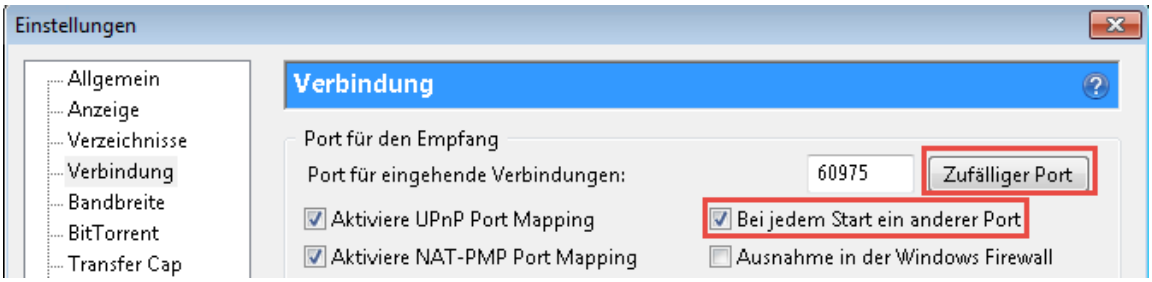
II. Völlig unzureichende Haftung der Betreiber drahtloser Netzwerke

Aber auch die – im Vergleich zum Referentenentwurf vom 23.02.2017 – nur noch gegenüber Betreibern drahtloser Netzwerke vorgesehene **Nutzungssperre** ist als alleinige Rechtsschutzmöglichkeit **völlig unzureichend** (§ 7 Abs. 4 TMG-E):

- Der Regierungsentwurf (S. 8) geht insbesondere fälschlich davon aus, dass **Portsperren** eine technisch wirksame Maßnahme darstellen, *„um den Zugang zu Peer-to-Peer Netzwerken zu verhindern“* bzw. *„den Zugriff auf illegale Tauschbörsen“* am WLAN-Router zu sperren. Anders als noch vor einigen Jahren, greifen diese Technologien jedoch nicht auf bestimmte, im Vorhinein sperrbare Ports zurück:

  > *„In der Rechtsprechung sind verschiedene Sperr- und Filterpflichten diskutiert worden. Dabei sind Portsperren Einstellungen des Netzwerks, durch die der Datenverkehr bestimmter Programme, zum Beispiel von Filesharing-Software, von vornherein unterbunden werden soll. Es hat sich allerdings herausgestellt, dass diese Maßnahme praktisch unwirksam und leicht zu umgehen ist. Handelsübliche Filesharing-Programme funktionieren weitgehend trotz solcher Portsperren. Auch aus diesem Grunde besteht überwiegende Einigkeit, dass vom Access Provider Portsperren nicht verlangt werden können.“* (Richter am Landgericht Mantz / RA Sassenberg, NJW 2014, 3537; Hervorhebungen durch die Unterzeichner)

  Sämtliche gängigen Filesharing- bzw. Tauschbörsenprogramme vergeben die für die Kommunikation notwendigen Ports bei jedem Programmstart neu aus der gesamten verfügbaren Menge aller Ports. Für eine wirksame Port-Sperre müsste der Betreiber eines drahtlosen Netzwerkes folglich **sämtliche Ports sperren**, was einer kompletten Abschaltung des Zugangs zum Internet als Ganzes gleichkäme.



Exemplarisch: Filesharingprogramm BitTorrent bzw. µ-Torrent

- Anders als die Bundesregierung meint, kann der Betreiber eines drahtlosen Netzwerkes die Nutzung von *„illegalen Tauschbörsen“* auch nicht durch **Webseitensperren** unterbinden (RegE 3. TMGÄndG S. 11). Bei Tauschbörsen handelt es sich gerade nicht um „Webseiten“, sondern dezentrale Netzwerke, bei denen sämtliche Nutzer gerade nicht über eine Webseite, sondern direkt und unmittelbar mittels einer Filesharing-Software kommunizieren, um Daten zu „tauschen“.

  Sinnvoll sind Webseitensperren hingegen bei herkömmlichen Access-Providern. Dort können sie den Zugriff auf illegale Webseiten effektiv unterbinden und damit herkömmliche Rechtsverletzungen im Internet gezielt verhindern. In diesem Bereich stellen sie daher auch europaweit die Regel dar (vgl. EuGH *UPC Telekabel*). Exakt diese kürzlich auch vom Bundesgerichtshof in der Entscheidung *Störerhaftung des Access-Providers* für die Bunderepublik Deutschland bestätigte Rechtsschutzmöglichkeit wird durch die Änderungen im Regierungsentwurf nun jedoch explizit ausgeschlossen.

  Dort, wo Webseitensperren wirkungslos sind (Tauschbörsen), sollen sie gesetzlich zulässig sein. Dort, wo sie sinnvoll sind (Sperrung von illegalen Webseiten durch herkömmliche Access-Provider), wird deren Anordnung hingegen explizit verboten!

- Erschwerend kommt hinzu, dass der Betreiber eines drahtlosen Netzwerkes eine Nutzungssperre überhaupt nur dann einrichten muss, wenn er hierzu von einem Gericht verurteilt wurde (§ 7 Abs. 3 TMG-E).

  Das Europarecht setzt einen solchen **echten Richtervorbehalt** jedoch gerade nicht voraus. Die gegenteilige Unterstellung der Bundesregierung (RegE 3. TMGÄndG S. 8) steht im klaren Widerspruch zur Rechtsprechung des Europäischen Gerichtshofes. Dem Bundesgerichtshof folgend hat der Europäische Gerichtshof in der Entscheidung *McFadden* die Pflicht zur Absicherung eines drahtlosen Netzwerkes gerade nicht von einer vorherigen gerichtlichen Anordnung abhängig gemacht. Die Sicherungspflichten bestehen – ausgehend von der besonderen Gefährlichkeit anonymer Netze – vielmehr ab Inbetriebnahme des Netzes, um das gebotene Gleichgewicht der Grundrechte zu gewährleisten (EuGH *McFadden*, Rn. 79, 101).

  Ein Richtervorbehalt hätte zur Folge, dass der Betreiber eines drahtlosen Netzwerkes jedwede Sicherungsmaßnahme bis zum rechtskräftigen Abschluss eines Gerichtsverfahrens hinauszögern könnte, ohne Nachteile befürchten zu müssen. Und dies sogar bei expliziter Kenntnis von einer Rechtsverletzung!

- Auch die **Kostenregelung** des § 7 Abs. 4 S. 3 TMG-E beinhaltet einen weiteren Systembruch mit massiven Konsequenzen für die Geschädigten: Die Rechtsanwaltskosten der Anordnung bzw. Durchsetzung einer Nutzungssperre sollen vom Geschädigten selbst getragen werden. Der Betreiber eines drahtlosen Netzwerkes wird also selbst dann, wenn er den Prozess verliert, allenfalls mit den Gerichtskosten belastet.

  Diese rechteinhaberfeindliche und von der sog. Entscheidungsschuldnerhaftung losgelöste Kostenverteilung wird damit gerechtfertigt, dass der Geschädigte die Kosten *„gegenüber dem eigentlichen Rechtsverletzer geltend“* machen könne (RegE 3. TMGÄndG S. 10). Diese Begründung ist erkennbar unredlich, da der eigentliche **Rechtsverletzer** bei Nutzungssperren **nie identifizierbar** ist. Denn das in § 7 Abs. 4 TMG-E verordnete Subsidiaritätsprinzip sieht ausdrücklich vor, dass eine Nutzungssperre überhaupt nur dann angeordnet werden darf, wenn der eigentliche Rechtsverletzer *nicht* in Anspruch genommen werden kann (RegE 3. TMGÄndG S. 9).

  Selbst der scheinbar gut gemeinte Anspruch auf gerichtliche Nutzungssperren führt somit zu einer Verschlechterung der Lage der Geschädigten, da diesen eine erhebliche Kostenlast ohne jede Regressmöglichkeit auferlegt wird. Nach geltendem deutschen Recht trägt der als Störer Verurteilte hingegen auch die Rechtsanwaltskosten des Geschädigten.

Der gegenüber Betreibern drahtloser Netzwerke allein verbliebene Rechtsbehelf der Nutzungssperre ist damit bei zahlreichen Rechtsverletzungen nicht nur technisch unwirksam, sondern auch unter wirtschaftlichen Gesichtspunkten nur im Ausnahmefall überhaupt realisierbar.

III. Keine Möglichkeit der Inanspruchnahme des eigentlichen Rechtsverletzers

Unerklärlich bleibt ohnehin, warum die Bundesregierung auf technisch unwirksame Nutzungssperren setzt, anstatt den Geschädigten ein Vorgehen gegenüber den eigentlichen, anonym agierenden Tätern (Tauschbörsennutzer, Webseitenbetreiber) zu ermöglichen.

Dies gilt erst Recht vor dem Hintergrund, dass die Bundesregierung ebenfalls am 5. April 2017 beschlossen hat, gegenüber den **Betreibern Sozialer Netzwerke** die **Auskunftsansprüche bei anonym begangenen Rechtsverletzungen zu erweitern** (Art. 2 des Regierungsentwurfs eines Gesetzes zur **Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken**, im Folgenden *„Regierungsentwurf zum NetzDG“* bzw. *„RegE NetzDG“*, Notifizierungsnummer 2017/127/D).

Anders als im vorliegenden Regierungsentwurf zum 3. TMGÄndG will die Bundesregierung in ihrem Regierungsentwurf zum NetzDG ein Vorgehen gegen den primären, anonym agierenden Rechtsverletzer also gezielt ermöglichen. Und dies aus gutem Grund: Die Aufhebung der Anonymität der primären Rechtsverletzer gewährleistet einen wesentlich effektiveren und nachhaltigeren Rechtschutz, der bislang im Bereich der Sozialen Netzwerke nicht hinreichend gewährleistet war: *„Die geltende Fassung von § 14 Absatz 2 TMG hat zur Folge, dass trotz Bestehens eines gesetzlichen Auskunftsanspruchs wegen einer **anonym begangenen Verletzung** von Persönlichkeitsrechten der Diensteanbieter nicht befugt ist, Daten zum Zwecke der Auskunftserteilung zu verwenden“* (RegE NetzDG S. 30).

Völlig unverständlich bleibt, warum die Bundesregierung bei Access-Providern, insbesondere den Betreibern drahtloser Netzwerke, hingegen gezielt verhindern will, dass – wie vom EuGH explizit gefordert – *„Nutzer ihre Identität offenbaren müssen, um das erforderliche Passwort zu erhalten und* ***damit nicht anonym handeln können“*** (EuGH *McFadden,* Rn. 96, 101).

Zugleich werden neu eingeführte Pflichten, wie die **Vorratsdatenspeicherung** und die **Identitätsprüfung bei Prepaid-Mobiltelefonen**, geradezu **ad absurdum geführt**, wenn Gefährdern allerorten anonym nutzbare „Hotspots“ zur Verfügung stehen. Die fehlende Identifizierbarkeit der Täter beseitigt jedwede Möglichkeit zur Aufklärung von Straftaten, die über das Internet begangen werden.

Die vom Europäischen Gerichtshof geforderte **Passwortsicherung** wäre für die Betreiber drahtloser Netzwerke sogar **wesentlich einfacher** und **kostengünstiger** umsetzbar, als technisch wirkungslose Nutzungssperren:

- Bereits heute nutzen zahlreiche Hotel-, Gastronomie- und sonstige Gewerbebetriebe Angebote, die die Bereitstellung eines drahtlosen Gäste-Netzwerkes inklusive Nutzer-Registrierung und Beauskunftung kostengünstig ermöglichen (z.B. *The Cloud* sowie *CONTELIO-HotSpot*). Die Kosten für diese Angebote liegen bei monatlich unter 20 Euro.

WIR BIETEN 360°-BETREUUNG. UND 100% SCHUTZ.

Natürlich können und wollen Sie nicht kontrollieren, was Ihre Gäste im Internet sehen. Aber Sie sollen auf der sicheren Seite sein, um nicht unangenehme Überraschungen zu erleben – etwa, wenn versucht wird, etwas illegal als Download zu bekommen.

Deshalb stellt The Cloud Sie von allen Haftungsrisiken frei und übernimmt als Betreiber die Verantwortung und Auskunftspflicht gegenüber den Sicherheitsbehörden.

Als Betreiber speichern wir natürlich nur die rechtlich vorgeschriebenen und benötigten Daten. Deshalb kann im Falle eines Missbrauchs durch The Cloud festgestellt werden, wer der Verursacher war – so sind Sie besser geschützt vor drohenden Abmahnungen wegen möglicher Urheberrechtsverletzungen oder anderer Online-Vergehen.

So haben Sie Rechtssicherheit und Ihre Gäste sind ebenfalls auf der sicheren Seite, denn wir sind „trusted provider“ für die Internetnutzer ebenso wie für unsere Standortpartner, mit denen wir arbeiten.

Sollten Sie noch offene Fragen haben, kontaktieren Sie uns gerne für mehr Informationen unter +49 (0)89 419 422-281 oder nutzen Sie für Ihren Rückrufwunsch das Call Back Formular.

http://www.thecloud.eu/de/hospitality/rechtssicherheit/

Kurzbeschreibung

Der CONTELIO® HotSpot wurde speziell für Hotels, Cafes, Bars, Tagungsstätten und Konferenzzentren, Messen und andere öffentliche Einrichtungen entwickelt.

Realisieren Sie schnell und mit minimalem Kostenaufwand einen kostenfreien oder kostenpflichtigen Hotspot-Dienst in Ihrer Einrichtung. Der Einsatz des CONTELIO® HotSpots kann sowohl für kabelgebundenen als auch für drahtlosen Zugang (WLAN-Hotspot) der Nutzer erfolgen. Die vorhandene Infrastruktur kann hierfür verwendet werden.

An den CONTELIO® HotSpot kann jeder Access Point angeschlossen werden. Optional sind spezielle WLAN Access Points verfügbar, welche über den CONTELIO® HotSpot zentral konfiguriert und überwacht werden können. Auch die Einbindung des Systems in vorhandene Kassensysteme/Buchungssysteme oder an bestehende Datenbanken ist optional möglich.

Weitere Informationen zum Aufbau und den Vorrausetzungen eines WLAN HotSpots finden Sie hier.

Rechtliche Sicherheit

Im Mittelpunkt steht hier die Begrifflichkeit der Störerhaftung. Als Störer bezeichnet man jemanden, der zwar selbst nicht der Täter ist, aber der mit seinem Handeln dazu beiträgt, dass es zu Rechtsverletzungen kommt. Der CONTELIO® HotSpot bietet eine sichere und eindeutige Grundlage für die Protokollierung der Internetnutzung auf Ihrem Gäste-WLAN bzw. HotSpot .

Viele der auf dem Markt befindlichen HotSpot-Lösungen bieten eben für diese Problematik keine entsprechende Lösung. Bei einigen Systemen wird das Nutzerverhalten überhaupt nicht protokolliert. Bei anderen wiederum werden die Protokolle aufgrund des Speicherbedarfs nicht lange genug aufbewahrt oder eine spätere Zuordnung zu einer natürlichen Person ist nicht mehr möglich.

Mit dem CONTELIO® HotSpot gehen Sie in dieser Hinsicht in jedem Falle auf Nummer sicher. Jedes ausgestellte Nutzerticket ist einer natürlichen Person zugeordnet. Sämtlicher Datenverkehr wird – unter Einhaltung der datenschutzrechtlichen Anforderungen – protokolliert. Die Protokolle werden mindestens sechs Monate vorgehalten und können durch den Betreiber des Systems nicht gelöscht oder manipuliert werden. Es ist bei dem CONTELIO® HotSpot weiterhin möglich, die Protokolldateien, bevor Sie turnusmäßig nach den sechs Monaten überschrieben werden, auf ein externes Laufwerk zu sichern und dort selbst für spätere Auswertungen zu archivieren.

Sicherheit der Daten

Wer Gästen Zugriff zum öffentlichen Internet gewährt, möchte dass diese auch nur darauf Zugriff erhalten. Da ein Hotspot-System zum ordnungsgemäßen Betrieb (Routing und Konfiguration) zumindest mit einem Anschluss auch im privaten Netzwerk des Betreibers steht, bedarf es einer besonderen Sorgfalt bei der Trennung von Gast- und Firmennetzwerk.

Im Gegensatz zu vielen anderen Systemen am Markt unterbindet der CONTELIO ® HotSpot prinzipiell jedwede Kommunikation von Gast- und Firmennetzwerk. Darüber hinaus kann der Betreiber selbstständig weitere Netzwerke vom Zugriff der Netze ausnehmen.

Zusätzlich werden die Gäste im Funknetzwerk voneinander getrennt gehalten, dadurch kann beispielsweise ein Gast nicht über das Funknetzwerk mit einem anderen Gast kommunizieren und diesen gegebenenfalls ausspionieren oder gar bösartige Software unterschieben.

Die Sicherheit der CONTELIO ® HotSpot Lösung geht zudem weit über das Gäste-Netzwerk hinaus. Mit der Funktion „Multi-SSID" können frei konfigurierbare, zusätzliche Funknetzwerke beispielsweise für Mitarbeiter oder mobile Geräte angelegt werden. Diese können nach den aktuellen Standards abgesichert werden – IEE 802.1X -Standard.

https://contelio.de/mehr/details-contelio-hotspot/

- Alternativ kann aber auch auf entsprechend kostengünstige Komplettlösungen der herkömmlichen Access-Provider zurückgegriffen werden, die neben der Bereitstellung des Internetanschlusses auch die Registrierung der Nutzer und deren Beauskunftung übernehmen (z.B. *WLAN to go* der Deutschen Telekom AG, *Hotspot Plug'n'Play* und *Homespot* von Vodafone sowie *WLAN-Hotspot Business* und *WiFi Spot* von Unitymedia).

Die Unterstellung der Bundesregierung, eine Passwortsicherung sei mit einem *„abschreckenden"* Aufwand verbunden (RegE 3. TMGÄndG S. 10 f.), ist schon deshalb schwer nachvollziehbar. Entsprechend kommt auch der Europäische Gerichtshof zu dem Ergebnis, dass bloß *„in marginaler Weise eine technische Modalität"* festgelegt werde, die von den Nutzern lediglich verlangt, sich ein Passwort geben zu lassen (EuGH *McFadden* Rn. 91 f.)

Sofern im Regierungsentwurf auf datenschutzrechtliche Belange im Zusammenhang mit einem Passwortschutz verwiesen werden (RegE 3. TMGÄndG S. 11), sei an das von der Bundesregierung angestrengte Verfahren *Patrick Breyer* erinnert. Hierin kommen sowohl der Bundesgerichtshof als auch der Europäische Gerichtshof zu dem Ergebnis, dass datenschutzrechtliche Regelungen einem grundrechtlich gebotenen Ergebnis nicht entgegenstehen können. Wenn eine umfassende Grundrechtsabwägung zu dem zwingenden Ergebnis kommt, dass der Schutz des geistigen Eigentums nur durch eine Passwortsicherung gewährleistet werden kann, können einfachgesetzliche Normen des TMG, TKG bzw. BDSG der Umsetzung dieses Ergebnisses generell nicht (mehr) entgegenstehen. Der Europäische Gerichtshof hat die Aufhebung der Anonymität auch und gerade unter Berücksichtigung der Grundrechte der Betreiber und Nutzer drahtloser Netzwerke für verhältnismäßig und geboten erachtet (EuGH *McFadden* Rn. 80 ff. unter Verweis auf EuGH *Promusicae* Rn. 68 ff.).

IV. Im Ergebnis: Massiver Verstoß gegen das Europarecht

Die vorgeschlagenen Neuregelungen verstoßen eklatant gegen die europäische **Grundrechtecharta**. Sie sind auch mit dem **übrigen Unionsrecht** und damit auch der **deutschen Verfassung** unvereinbar. Dies gilt für die Beschränkung der Haftung von Betreibern drahtloser Netzwerke gleichermaßen wie die völlige Abschaffung der Haftung herkömmlicher Access-Provider:

- Gerade im Hinblick auf **Rechtsverletzungen in Tauschbörsen** hat der Europäische Gerichtshof explizit klargestellt, dass es den Mitgliedstaaten obliegt, ein angemessenes Gleichgewicht zwischen den Grundrechten der Access-Provider, Nutzer und Rechteinhabern sicherzustellen. Dieses Gleichgewicht könne nur durch die Verpflichtung zur *„Sicherung des Internetanschlusses durch ein **Passwort**“* erfolgen, *„soweit diese Nutzer ihre Identität offenbaren müssen, um das erforderliche Passwort zu erhalten und damit nicht anonym handeln können“*. Entsprechende Verpflichtungen sind daher nicht nur zulässig, sondern sogar geboten. Hingegen *„liefe die Auffassung, dass ein Anbieter, der Zugang zu einem Kommunikationsnetz vermittelt, seinen Internetanschluss nicht sichern muss, darauf hinaus, dem Grundrecht auf geistige Eigentum jeden Schutz zu entziehen, was dem Gedanken eines angemessenen Gleichgewichts zuwider liefe“* (EuGH *McFadden* Rn. 96 ff.).

  Diese Vorgaben des Europäischen Gerichtshofs können nicht dadurch umgangen werden, dass allein die Möglichkeit einer Port- bzw. Webseitensperre gewährt wird, die noch dazu an einen Richtervorbehalt geknüpft ist. Denn diese Maßnahmen sind – wie dargestellt – völlig ungeeignet, die Nutzung von Tauschbörsen wirksam zu unterbinden. Zudem schrecken sie die Nutzer auch nicht vor der Begehung von Rechtsverletzungen ab, da sie – anders als bei einer Passwortsicherung – keine Identifizierung und damit auch keine Rechtsverfolgung ermöglichen. Nach dem Vorschlag der Bundesregierung verbliebe bei Rechtsverletzungen über ein drahtloses Netzwerk somit **keine einzige wirksame Rechtsverfolgungsmöglichkeit**. Die Inhaber der Rechte am geistigen Eigentum wären vielmehr – entgegen den zwingenden Vorgaben des Europarechts – völlig schutzlos gestellt.

  Hinzu kommt, dass es sich bei Nutzungssperren noch nicht einmal um ein *„milderes Mittel“* handelt, wie vom Regierungsentwurf unterstellt (RegE 3. TMGÄndG S. 11). Der Europäische Gerichtshof hat vielmehr klargestellt, dass gerade die Passwortsicherung eines drahtlosen Netzwerkes die mildere Maßnahme darstellt, da sie – anders als eine Nutzungssperre – keine rechtmäßige Nutzung von Informationen verhindert (EuGH *McFadden* Rn. 94).

- Auch im Hinblick auf Rechtsverletzungen, die über **Webseiten** begangen werden, hat der Europäische Gerichtshof klargestellt, dass es Geschädigten möglich sein muss, eine Anordnung zu erwirken, *„mit der einem Anbieter von **Internetzugangsdiensten** verboten wird, seinen Kunden den Zugang zu einer Website zu ermöglichen, auf der ohne Zustimmung der Rechtsinhaber Schutzgegenstände online zugänglich gemacht werden“* (EuGH *UPC Telekabel* Rn. 64).

Die Bundesrepublik Deutschland ist gemäß Art. 8 Abs. 3 Urheberrechtsrichtlinie 2001/29 und Art. 11 S. 3 Durchsetzungsrichtlinie 2004/48 verpflichtet, gegenüber Access-Providern bei Verletzungen von Urheberrechten oder sonstigen Geistigen Eigentumsrechten Unterlassungs- und Beseitigungsansprüche vorzusehen. Die Bundesregierung hat sich bislang auf den Standpunkt gestellt, die Umsetzung dieser Ansprüche in deutsches Recht und damit das Herstellen einer EU-konformen Rechtslage sei durch das **Institut der Störerhaftung** gewährleistet. Der Bundesgerichtshof hat zwischenzeitlich bestätigt, dass entsprechende Anordnungen auf dieser Basis erfolgen können (BGH *Störerhaftung des Accessproviders*). Die bestehende Störerhaftung für herkömmliche Access-Provider kann folglich unter keinem rechtlichen Gesichtspunkt **ersatzlos gestrichen** werden.

- Auch im Hinblick auf die **Rechtsverfolgungskosten** hat der Europäische Gerichtshof klargestellt, dass *„wenigstens ein erheblicher und angemessener Teil der zumutbaren Kosten, die der obsiegenden Partei tatsächlich entstanden sind, **von der unterlegenen Partei getragen**“* werden muss, da andernfalls *„Art. 14 der Richtlinie 2004/48 seine praktische Wirksamkeit genommen“* wäre. Auch wäre *„eine solche Regelung […] mit Art. 3 Abs. 2 der Richtlinie 2004/48, wonach die in dieser Richtlinie vorgesehenen Verfahren und Rechtsbehelfe **abschreckend sein müssen**, unvereinbar. Die abschreckende Wirkung einer Klage wegen Verletzung eines Rechts des geistigen Eigentums würde erheblich geschwächt, wenn der Verletzer nur zur Erstattung eines geringen Teils der zumutbaren Anwaltskosten, die dem Inhaber des verletzten Rechts des geistigen Eigentums entstanden sind, verurteilt werden dürfte. Eine solche Regelung würde somit das mit der Richtlinie 2004/48 verfolgte **Hauptziel beeinträchtigen, das darin besteht, ein hohes Schutzniveau für geistiges Eigentum im Binnenmarkt zu gewährleisten**, ein Ziel, das ausdrücklich im zehnten Erwägungsgrund dieser Richtlinie genannt wird und im Einklang mit Art. 17 Abs. 2 der Charta der Grundrechte der Europäischen Union steht“* (EuGH *United Video Properties Inc.*, Rs. C-57/15, Rn. 26 ff.).

  Der Europäische Gerichtshof unterstreicht hierbei, dass diese Grundsätze unabhängig von der Verantwortlichkeit der unterlegenen Partei gelten, da *„Art. 14 der Richtlinie 2004/48 keinen Anhaltspunkt für die Annahme enthält, dass die Mitgliedstaaten die Erstattung der ‚sonstigen Kosten‘ oder der Prozesskosten im Allgemeinen im Rahmen eines Verfahrens zur Durchsetzung eines Rechts des geistigen Eigentums von einem Kriterium des Fehlverhaltens der unterlegenen Partei abhängig machen dürfen“* (EuGH *United Video Properties Inc.* Rn. 37).

  Auch die im Regierungsentwurf vorgesehene prohibitive Kostenregelung erweist sich damit als klar europarechtswidrig.

Die Bundesregierung erkennt zwar an, dass die Mitgliedstaaten gem. Art. 8 Abs. 3 der Urheberrechtsrichtlinie 2001/29 die Möglichkeit gerichtlicher Anordnungen gegen Vermittler sicherzustellen haben. Zudem weist sie sogar explizit darauf hin, *„dass dem Grundrecht auf geistiges Eigentum nicht jeder Schutz entzogen werden darf“*, da dies *„dem Gedanken eines angemessenen Gleichgewichts zwischen den berechtigen Interessen der Beteiligten zuwider“* liefe (RegE 3. TMGÄndG S. 8). Gleichwohl missachten die vorgesehenen Neuregelungen diese zwingenden Vorgaben des Unionsrechts in eklatanter Weise. Sie beseitigen gezielt das bewährte System der Störerhaftung, das sowohl vom Europäischen Gerichtshof (*McFadden*) als auch vom

Bundesgerichtshof (*Störerhaftung des Access-Providers*) als geeignet angesehen wird, um den Vorgaben des Europarechts bei der Haftung von Access-Providern gerecht zu werden. Die vorgesehenen Regelungen laufen nicht nur elementar den Unionsgrundrechten, sondern auch den Vorgaben der Art. 8 Abs. 3 der Urheberrechtsrichtlinie 2001/29 und Art. 11 S. 3 der Durchsetzungsrichtlinie 2004/48 zuwider, die eine Ermöglichung effektiver Anordnungen fordern. Ebenso werden das Gebot effektiven Rechtsschutzes aus Art. 3 sowie die Kostentragungsregelung des Art. 14 der Durchsetzungsrichtlinie 2004/48 konterkariert.

Anstatt die höchstrichterlich bestätigten Rechtsverfolgungsmöglichkeiten gesetzlich zu verankern, beseitigt der Regierungsentwurf das bewährte System und stellt die Geschädigten nicht nur schlechter als zuvor, sondern nahezu schutzlos. Der Regelungsansatz der Bundesregierung führt zu einem nie dagewesenen Systembruch innerhalb eines in sich geschlossenen Haftungssystems der §§ 7-10 TMG bzw. der Art. 12-15 E-Commerce-Richtlinie. Die aktuellen europäischen Bemühungen, den Schutz des Urheberrechts den technischen Entwicklungen anzupassen und dadurch zu stärken, werden hierdurch massiv untergraben.

Im Ergebnis vermittelt das Gesetzesvorhaben den Eindruck, die Bundesregierung wolle rechtsfreie Räume im Internet geradezu aktiv fördern. Das Verbot einer Sicherungs- und Registrierungspflicht für Diensteanbieter steht jedenfalls im unauflösbaren Widerspruch zu den aktuell eingeführten Maßnahmen zur Verbrechensbekämpfung, u.a. der Vorratsdatenspeicherung und der Identifizierungspflicht bei Prepaid-Mobiltelefonen.

V. Appell an die Kommission

In ihrer Mitteilung *„Schritte zu einem modernen, europäischeren Urheberrecht“*, COM(2015) 626, postuliert die Kommission ein „*wirksames und ausgewogenes System der Rechtsdurchsetzung*“. „*Rechte, die nicht wirksam durchsetzbar sind, sind wirtschaftlich wenig wert*“, so die Kommission. Eine *„effektive und ausgewogene zivilrechtliche Durchsetzbarkeit“* sei insofern unabdingbar. Ziel sei dabei auch, die „*Kosten insbesondere kleiner Unternehmen für die Bekämpfung von Zuwiderhandlungen zu senken*“.

Die Kommission äußert insbesondere im Hinblick auf Auskunfts-, Unterlassungs- und Schadensersatzansprüche sowie die Erstattung von Kosten ernsthafte Bedenken dahingehend, dass *„der aktuelle Rechtsrahmen für die Herausforderungen des digitalen Binnenmarkts nicht vollständig geeignet*“ sei.

Diese Bedenken werden von der Kommission in ihrer Mitteilung *„Für eine faire, effiziente und wettbewerbsfähige auf dem Urheberrechtsschutz beruhende europäische Wirtschaft im digitalen Binnenmarkt*“, COM(2016) 592, sogar erneut aufgegriffen.

Es steht zu befürchten, dass durch den vorschnellen deutschen Alleingang im vorliegenden Regierungsentwurf die laufenden europäischen Bestrebungen im Rahmen des Digitalen Binnenmarktes konterkariert werden. Der Regierungsentwurf vereitelt effektiv die bestehenden Rechtsdurchsetzungsmöglichkeiten geschädigter Rechteinhaber. Die ersatzlose Abschaffung (herkömmliche Access-Provider) bzw. massive Beschneidung (Betreiber drahtloser Netzwerke) der bestehenden Rechtsschutzmöglichkeiten würde zu einer deutlichen Absenkung des Schutzniveaus

in Deutschland führen.

Es wird daher angeregt, den vorliegenden Regierungsentwurf für bis zu 18 Monate **zu sperren**, um eine Behinderung der aktuellen Harmonisierungsbestrebungen der Europäischen Union zu vermeiden.

Jedenfalls wird die Kommission ersucht, eine **ausführliche Stellungnahme** abzugeben, in der auf die Widersprüche des RegE 3. TMGÄndG zum geltenden europäischen Recht eingegangen wird.