

**Verband der Österreichischen Musikwirtschaft**

IFPI Austria, Schreyvogelgasse 2/5, A-1010 Wien

Bundesministerium für
Verkehr, Innovation und Technologie
Sektion III, Abteilung PT 2
Ghegastraße 1
1030 Wien

IFPI Austria
Schreyvogelgasse 2/5
A-1010 Wien
T: +43 (1) 535 60 35
F: +43 (1) 535 51 91
E: ifpi@ifpi.at

Per E-Mail:

JD@bmvit.gv.at;begutachtungsverfahren@parlament.gv.at

Wien, 2010-01-14

BMVIT-630.333/0001-III/PT2/2009 117/ME**Stellungnahme des *Verbands der Österreichischen Musikwirtschaft* – *IFPI Austria* zum Ministerialentwurf betreffend ein Bundesgesetz, mit dem das Telekommunikationsgesetz 2003 – TKG 2003 geändert wird**

Sehr geehrte Damen und Herren,

zunächst danken wir für die Gelegenheit zur Stellungnahme im Begutachtungsverfahren und möchten uns nachfolgend auf jene Regelungsinhalte beschränken, die für die Inhaber von Urheber- und Leistungsschutzrechten relevant sind. Wir sind vom Telekommunikations- und Datenschutzrecht unmittelbar betroffen, soweit es um Fragen der Durchsetzung des Urheberrechts und damit in Zusammenhang stehender Auskunftsansprüche gegenüber dem Provider geht.

Das Internet eröffnet der Musik- und andere Kreativbranchen zum einen die Chance, ihre Inhalte auf neuen digitalen Plattformen anbieten zu können; gerade die Musikbranche hat in den letzten Jahren enorm in den Aufbau lizenzierter Online-Shops investiert. Zum anderen bringt das Internet aber auch die Gefahr mit sich, dass Musik und andere urheberrechtlich geschützten Werke und Leistungen ungenehmigt und illegal verbreitet werden, wie dies leider nach wie vor in großem Umfang und mit wirtschaftlich massiv nachteiligen Folgen der Fall ist.

Die Rechtsverfolgung und das Unterbinden von Urheberrechtsverletzungen ist ohne entsprechende Beauskunftung des Namens und der Anschrift des gesetzwidrig handelnden Internetteilnehmers schlicht unmöglich. Ohne diese Auskunft - die ganz ausschließlich der

Provider erteilen kann, weil nur er über diese Informationen verfügt - wären die Rechteinhaber den Eingriffen in ihre Eigentumsrechte völlig schutzlos ausgesetzt. Das Urheberrecht wäre im Internet mangels jeglicher Durchsetzbarkeit nur mehr ein „nacktes Recht“ ohne jeden Wert.

Es handelt sich dabei nicht nur um ein wirtschaftliches Problem, weil dann jedes lizenzierte Online-Geschäftsmodell in einen per se unlauteren Wettbewerb mit illegalen – aber rechtlich nicht angreifbaren - Distributionsplattformen zu treten hätte und konterkariert würde.

Es handelt sich auch um die Aushöhlung des verfassungsrechtlich verankerten Grundrechts auf Eigentumsschutz, das gleichermaßen auch für schöpferisches, geistiges Eigentum gilt (Art 5 StGG von 1867; Art 1 des 1. ZProtMRK; Art 17 EU-Grundrechte-Charta) und nur dann gewährleistet ist, wenn es auch mit entsprechenden Rechtsbehelfen durchsetzbar ist. Diese rechtlichen Grundsätze gelten selbstverständlich auch im Bereich des Internets, das eben nicht nur privates Kommunikationsmittel, sondern auch öffentlicher Marktplatz ist.

Der vorliegende Entwurf einer Novelle zum TKG 2003 schließt aber die Möglichkeit der Rechtsverfolgung von Verletzungen des geistigen Eigentums (etwa das Online-Zugänglichmachen von geschützten Musik- oder Filmaufnahmen), die mit Hilfe eines Internetanschlusses erfolgen, aus. Es wird fälschlicher Weise davon ausgegangen, dass durch die VorratsdatenspeicherungsRL abschließend festgelegt wird, zu welchem Zweck eine Speicherung von Verkehrsdaten erfolgen darf (nämlich der Verfolgung von schweren Straftaten); andere Gesetzesverletzungen sollen hingegen durch den Datenschutz anonymisiert werden und dadurch sanktionslos bleiben. Dies widerspricht verfassungsrechtlichen Grundrechten, rechtsstaatlichen Prinzipien und steht auch nicht im Einklang mit der Absicht und dem Wortlaut der Richtlinie.

I) Vorgaben der RL 2006/24/EG

1. Wie das Urteil des EuGH vom 10.02.2009 über die Klage der Republik Irland belegt, handelt es sich bei der sog. Vorratsdatenspeicherungs-RL um eine solche, die im Rahmen der „ersten Säule“ erging. Auslöser der Richtlinie waren die Terroranschläge von London und Madrid, in deren Folge sich zeigte, dass die Aufklärung dieser schwerwiegenden Verbrechen in manchen Mitgliedstaaten dadurch erschwert wurde, dass die nachträgliche Erhebung von Kommunikationsdaten wegen bereits erfolgter Löschung nicht mehr möglich war.

Dieser Anlass dokumentiert, dass es das gemeinsame Anliegen gab, in Zukunft sicher zu stellen, dass diese Daten in jedem Staat verlässlich vorhanden sind, widrigenfalls eine Verhinderung bzw. Aufklärung solcher kriminellen Handlungen nicht möglich wäre.

Die Richtlinie will sohin diesbezüglich – nämlich Vorratsdatenspeicherung zum Zweck der Verhütung, Ermittlung, Feststellung und Verfolgung schwerer Straftaten – eine Harmonisierung innerhalb der Mitgliedstaaten schaffen (vgl. ErwG 5 bis 8), ohne aber in ohnehin bereits bestehende innerstaatlich geregelte Datenschutzbestimmungen eingreifen zu wollen, soweit dies nicht ausdrücklich in der Richtlinie zum Ausdruck kommt. Die Richtlinie 2006/24 regelt bekanntlich nicht erstmals die Materie der Datenkategorien und den Umgang mit solchen Daten. Vielmehr existieren bereits mehrere datenschutzrechtliche Richtlinien, die die Mit-

gliedstaaten auch umzusetzen hatten und auf die in den Erwägungsgründen der Richtlinie 2006/24 auch ausdrücklich verwiesen wird.

So findet sich in ErwG 12 der ausdrückliche Hinweis darauf, dass Art 15 Absatz 1 der RL 2002/58 weiterhin für alle Daten gilt, deren Vorratsspeicherung nach der RL 2006/24 nicht ausdrücklich vorgeschrieben ist und die daher nicht in den Anwendungsbereich dieser RL fallen und für die Vorratsdatenspeicherung zu anderen – einschließlich justiziellen – Zwecken als denjenigen, die durch die vorliegende RL abgedeckt sind. Nach dieser Bestimmung sind Beschränkungen der Rechte und Pflichten aus Art 5, Art 6, Art 8 Abs 1 bis 4 sowie Art 9 der RL 2002/58 zulässig, sofern sie gemäß Art 13 Abs 1 der RL 95/46 notwendig, angemessen und verhältnismäßig sind.

Dies zeigt, dass die Speicherung von Verkehrsdaten auch zu anderen, als den in der RL 2006/24 genannten Zwecken, nämlich jenen der zitierten Bestimmungen anderer Richtlinien zulässig ist. Daher stimmt die oftmals aufgestellte Behauptung, insbesondere Verkehrsdaten dürften ausschließlich zur Ermittlung, Feststellung und Verfolgung schwerer Straftaten gespeichert und verwendet werden, mit dem Inhalt und der Intention der Vorratsdatenspeicherungs-RL nicht überein.

2. Diesen Befund bestätigt nun auch der Oberste Gerichtshof in seiner Entscheidung vom 14.7.2009, 4 Ob 41/09x¹. Ausgehend von Art 6 Abs 1 RL 2002/58, der vorsieht, dass Verkehrsdaten außer in gesetzlich geregelten Fällen nicht gespeichert werden dürfen und nach Verbindungsende vom Betreiber unverzüglich zu löschen sind, hält der OGH fest, dass diese Bestimmung vorbehaltlich Art 15 RL 2002/58 gilt.

Dem EuGH folgend führt er weiter aus, dass Art 15 leg.cit. wegen des darin enthaltenen Verweises auf Art 13 Abs 1 RL 95/46 auch Regelungen zum Schutz von Urheberinteressen gestatte und stellt fest, dass es den Mitgliedstaaten damit grundsätzlich freisteht, die Speicherung und Verarbeitung von Verkehrsdaten auch für die Erteilung von Auskünften über nähere Umstände von Urheberrechtsverletzungen zu erlauben. Dies gelte grundsätzlich unabhängig von den Regelungen der RL 2006/24.

Hinzu kommt, dass der OGH an anderer Stelle seines Urteils (Pkt 7.1) ausführt, dass selbst hinsichtlich der RL 2006/24 eine Beschränkung auf die erwähnten „schweren Straftaten“ nicht zwingend erforderlich sein dürfte, zumal die RL insbesondere *das Sammeln von Beweisen im Zusammenhang mit strafbaren Handlungen, die als solche nichts mit dem Internet zu tun haben, erfasst, hingegen strafbare Handlungen, die direkt im Internet begangen werden und bei denen sich der Täter hinter seiner durch die IP-Adresse begründete Anonymität versteckt, das Verarbeiten auf Vorrat gespeicherter Daten auch für die Aufklärung weniger schwerer Straftaten oder zur Verfolgung zivilrechtlicher Ansprüche rechtfertigen können.*

II) Derzeitige Rechtslage betreffend Auskunft

Der österreichische Gesetzgeber hat mit § 87b Abs 3 UrhG und in den dazugehörigen Materialien zum Ausdruck gebracht, dass die Aufklärung und Verfolgbarkeit von Online-Eingriffen

¹ MR 2009, 251 = jusIT 2009, 178.

in Urheberrechte möglich sein soll. Dies entspricht auch dem verfassungsrechtlich gewährleisteten Eigentumsschutz und seiner Durchsetzung sowie der Sinnhaftigkeit des eigens in multinationalen Völkerrechtsverträgen (TRIPs, WCT, WPPT) und in der österreichischen Rechtsordnung (§§ 18a, 71a, 74 Abs 1, 76 Abs 1, 76a Abs 1, 76d Abs 1 UrhG etc) verankerten öffentlichen Zurverfügungstellungsrechts als Ausschließlichkeitsrecht der Urheber und Leistungsschutzberechtigten.

Allerdings – so konstatiert der OGH in Pkt 6 – steht dem Anspruch nach § 87b Abs 3 UrhG bei dynamischer Vergabe von IP-Adressen des Providers das Fehlen einer Rechtsvorschrift iSv Art 15 Abs 1 RL 2002/58 bzw. das Speicherverbot nach § 99 Abs 1 TKG 2003 entgegen, sodass das dafür erforderliche Speichern und Verarbeiten von Verkehrsdaten derzeit nicht rechtens sei. Der OGH lässt allerdings keinen Zweifel daran, dass eine solche rechtliche Grundlage für die Datenspeicherung und -verarbeitung vom Gesetzgeber zu schaffen ist.

Zusammenfassend sei nochmals festgehalten, dass die für die Aufrechterhaltung des Schutzes geistigen Eigentums im Internet notwendige Auskunft von Teilnehmern nicht dem Regime der VorratsdatenspeicherungsRL bzw. deren Umsetzung unterliegt, sondern das Vorsehen einer entsprechenden gesetzlichen Grundlage unabhängig davon zulässig und notwendig ist.

III) Europarechtliche Vorgaben zum Schutz des geistigen Eigentums im Internet

Der Gesetzgeber ist aufgrund der Vorgaben des europäischen Gemeinschaftsrechtes verpflichtet, Rahmenbedingungen zu schaffen, welche die Verfolgung und Sanktionierung von Urheberrechtsverletzungen im Internet ermöglichen:

a) Gemäß Art. 8 Abs 1 der Richtlinie 2001/29/EG zur Harmonisierung bestimmter Aspekte des Urheberrechts und der verwandten Schutzrechte in der Informationsgesellschaft haben die Mitgliedstaaten bei Verletzungen der in dieser Richtlinie festgelegten Rechte und Pflichten – dazu zählt u.a. das Recht des Urhebers- bzw. Leistungsschutzberechtigten, Dritte von der öffentlichen Zugänglichmachung von Werken auszuschließen (Art 3 RL 2001/29/EG) – angemessene Sanktionen und Rechtsbehelfe vorzusehen und alle notwendigen Maßnahmen zu treffen, um deren Anwendung sicherzustellen.

b) Gemäß Art. 8 Abs 3 der Richtlinie 2001/29/EG zur Harmonisierung bestimmter Aspekte des Urheberrechts und der verwandten Schutzrechte in der Informationsgesellschaft haben die Mitgliedstaaten sicher zu stellen, dass Rechteinhaber gerichtliche Anordnungen gegen Vermittler beantragen können, deren Dienste von einem Dritten zur Verletzung eines Urheberrechts oder verwandter Schutzrechte genutzt werden.

c) Gemäß Art. 8 der Richtlinie 2004/48/EG zur Durchsetzung der Rechte des geistigen Eigentums haben die Mitgliedstaaten unter anderem sicherzustellen, dass die zuständigen Gerichte im Zusammenhang mit einem Verfahren wegen Verletzung eines Rechtes des geistigen Eigentums auf einen begründeten und die Verhältnismäßigkeit wahren Antrag des Klägers hin anordnen können, dass Auskünfte über den Ursprung und die Vertriebswege von Dienstleistungen, die ein Recht des geistigen Eigentums verletzen, nicht nur vom Verletzer,

sondern auch von jeder anderen Person erteilt werden, die nachweislich für rechtsverletzende Tätigkeiten genutzte Dienstleistungen in gewerblichem Ausmaß erbrachte.

d) Gemäß Art. 18 Abs. 1 der Richtlinie 2000/31/EG haben die Mitgliedsstaaten sicherzustellen, dass die nach innerstaatlichem Recht verfügbare Klagemöglichkeiten im Zusammenhang mit Diensten der Informationsgesellschaft – dazu zählt auch das Bereitstellen von Internetzugangsmöglichkeiten (Access-Providing) – ermöglichen, dass rasch Maßnahmen, einschließlich vorläufiger Maßnahme, getroffen werden können, um eine mutmaßliche Rechtsverletzung abzustellen und zu verhindern, dass den Betroffenen weiterer Schaden entsteht.

Die Verletzung von Urheberrechten im Internet bleibt in Österreich hingegen aufgrund der geltenden Rechtslage regelmäßig sanktionslos, wenn der Rechteinhaber nicht mehr Informationen über den Verletzer erlangen kann, als dessen dynamisch zugewiesene IP-Adresse.

IV) Der telekommunikations- und datenschutzrechtliche Handlungsbedarf und der Entwurf

1. Zur Rechtsdurchsetzung benötigen die Inhaber von Urheber- und Leistungsschutzrechten bzw. die damit befassten Behörden lediglich Kenntnis über Name und Anschrift des Internetteilnehmers. Nur im Fall der dynamischen Vergabe von IP-Adressen bedarf es beim Zugangsprovider der internen und nachträglich erfolgenden Heranziehung von Verkehrsdaten, nicht aber deren Weitergabe an Dritte.

Ungeachtet der derzeitigen Wirkungslosigkeit des § 87b Abs 3 UrhG ist auf Grund der Einführung (2003) und Novellierung (2006) dieser Bestimmung der gesetzgeberische Wille, solche Eingriffe aufklärbar zu machen, dokumentiert und geht sowohl aus der Entscheidung des EuGH in der Rs. C-557/07 als auch jener des OGH vom 14.7.2009 hervor, dass die Anonymisierung von Personen, die im Internet Urheberrecht verletzen, nicht ernsthaft rechtsstaatlichen Maßstäben entsprechen kann.

Der vorliegende TKG-Novellen-Entwurf sieht in den §§ 102a und 102b die Speicherung und Auskunft von Verkehrsdaten (=Vorratsdaten) ausschließlich zum Zweck der Ermittlung, Feststellung und Verfolgung schwerer Straftaten vor und normiert in § 99 Abs 1, dass diese Fälle ausschließlich in diesem Gesetz geregelt werden. Urheberrechtsverletzungen sind davon schon wegen der Strafdrohung von bis zu 6 Monaten Freiheitsstrafe (bzw. Geldstrafe) nicht erfasst. Der Entwurf setzt damit in sehr enger Auslegung ausschließlich die VorratsdatenspeicherungsRL um, schneidet dabei aber - in Widerspruch zu dieser Richtlinie - jegliche, außerhalb der VorratsdatenspeicherungsRL zulässige Speichervorschrift zu anderen Zwecken von vornherein ab.

Damit würde der Umsetzungsgesetzgeber den gebotenen Interessenausgleich zwischen den Grundrechten auf Datenschutz bzw. Unverletzlichkeit des Eigentums völlig außer Acht lassen, sondern irriger Weise auch beanspruchen, im TKG bereits über alle bestehenden bzw. allenfalls zukünftig rechtstaatlich erforderlichen gesetzlichen Speichervorschriften bereits vorweg entschieden zu haben.

Auch der vorgesehene § 99 Abs 5 (Z 1) ändert nichts, denn diese Vorschrift sieht ausdrücklich (vorletzter Satz) keine Speicherung von Verkehrsdaten vor, sondern bezieht sich nur auf allenfalls noch vorhandene Verkehrsdaten im „live-System“ (vgl. Erl im BT zu § 99 Abs 5 Z 1). Solche sind aber – wie gleichfalls in den Erläuterungen angemerkt – hinsichtlich IP-Adressen meist lediglich 96 Stunden vorhanden, was wiederum weder verlässlich erscheint, noch einen Zeitraum darstellt, innerhalb dessen eine gerichtliche Auskunftsanordnung und deren Zustellung erreichbar wäre.

Wir halten es darüber hinaus für unangebracht, die Zulässigkeit einer gesetzlich gebotenen Auskunft dem Geschäftsmodell des Betreibers unterzuordnen: gibt er an, mit einer *flat-rate* zu operieren, müssen die Daten nicht zur Verfügung stehen; bei anderer Ausgestaltung des Providers hat der in seinen Rechten verletzte vielleicht Glück und bekommt Auskunft, weil die Daten noch gespeichert sind. Mit derartigen Regelungen würde der Gesetzgeber den Anwendungsbereich seiner Gesetze - unzulässiger Weise - von individuellen wirtschaftlichen Organisationsmaßnahmen des betreffenden Providers abhängig machen.

Überdies sollen Auskünfte über Daten einer Nachrichtenübermittlung (§ 134 Z 2 StPO) gemäß § 135 Abs 2 StPO jedenfalls nur dann zulässig sein, wenn die Aufklärung eines Delikts mit einer Strafdrohung von mehr als sechs Monaten (Z 2) bzw. einem Jahr (Z 3) zu erwarten ist. Dies ist bei Urheberrechtsverletzungen in aller Regel nicht der Fall, weil nicht von einer gewerbsmäßigen Begehung ausgegangen werden kann. Abgesehen davon sei dahingestellt, ob es sich bei den erforderlichen Auskünften überhaupt um Auskünfte gemäß § 134 Z 2 StPO handelt, die von *Auskunft über Verkehrsdaten* sprechen. In den für uns relevanten Fällen ist aber keine Auskunft über Verkehrsdaten, sondern nur deren Verarbeitung notwendig, um letztlich Auskunft über Stammdaten zu geben.

Ungeachtet der Frage, ob die Auskunft strafprozessual und/oder als zivilrechtlicher Anspruch und/oder über andere Wege und Institutionen bewerkstelligt werden soll, ist damit klar, dass es einer ausdrücklichen gesetzlichen Bestimmung bedarf, um die Grundlage für die Speicherung und Verarbeitung der bei dynamischer IP-Vergabe erforderlichen Verkehrsdaten zum Zweck der Beauskunftung von Stammdaten zu schaffen.

2. Daher halten wir es für dringend erforderlich und den Zeitpunkt der Novellierung des TKG 2003 für geeignet, ein Bestimmung vorzusehen, die unmissverständlich klarstellt, dass jene Verkehrsdaten, die notwendig sind, um die Identität des jeweiligen Inhabers einer dynamisch vergebenen IP-Adresse festzustellen, zum Zweck der Verhütung, Ermittlung, Feststellung und Verfolgung von Verletzungen geistigen Eigentums, die im Internet erfolgen, durch den Diensteanbieter zu speichern sind und auf Grundlage spezialgesetzlicher Bestimmungen oder einer gerichtlichen Anordnung verarbeitet werden dürfen.

Als Dauer der Speicherung für diesen Zweck sollten wegen der gewünschten richterlichen Bewilligung ebenfalls sechs Monate vorgesehen werden. Damit wäre kein zusätzlicher administrativ-organisatorischer Aufwand verbunden, weil dieselben Daten ohnehin gemäß § 102a des Entwurfs ohnehin zu speichern sind. Systematisch könnte die Bestimmung als § 99

Abs 6 vorgesehen werden, zumal die Daten und deren Speicherung nicht in den spezifischen Richtlinienbegriff der Vorratsdaten passen (siehe VII. Regelungsvorschläge).

Ab dem Zeitpunkt der konkreten Anforderung der Auskunft beim Vermittler/Betreiber, sollte die Lösungsverpflichtung hinsichtlich der konkret betroffenen Daten gehemmt sein. Damit kann vermieden werden, dass während etwaiger Rechtsstreitigkeiten über die konkrete Auskunft die Unmöglichkeit der Beauskunftung eintritt, obwohl die Anforderung oder die Anordnung noch innerhalb der Aufbewahrungsfrist geltend gemacht wurde.

Mit einer solchen Regelung, die auf die Notwendigkeit einer zusätzlichen Materienbestimmung verweist, würde der Beibehaltung oder Neuschaffung konkreter Auskunftsermächtigungen (etwa in der StPO, im UrhG oder ECG) nicht vorgegriffen. Vielmehr soll dadurch die datenschutz- und telekommunikationsrechtliche Basis geschaffen werden, um vom Gesetzgeber in bestimmten Bereichen als erforderlich und grundrechtlich zulässig angesehene Auskünfte im Sinn der erwähnten OGH-Entscheidung auch bewerkstelligen zu können.

Auf ähnliche Weise ist auch der **deutsche Gesetzgeber** vorgegangen, der in § 101 Abs 9 dUrhG den einschlägigen Auskunftstatbestand geschaffen hat und diesem den § 113 dTKG zur Seite stellt, in dem festgehalten ist, dass die Provider die entsprechenden Verkehrsdaten heranziehen, verarbeiten und die für die Verfolgung erforderlichen Daten (Bestandsdaten) herauszugeben haben.

Es wäre unseres Erachtens unangebracht und legislativ unübersichtlich, würde man stattdessen die datenschutz- und telekommunikationsrechtliche Vorschrift jeweils in die (die Auskünfte regelnden) Materien Gesetze (zB UrhG, MSchG, MuSchG, GMG, PatG, UWG, MedienG) einfügen. Vielmehr passt dies zu den Sonderbestimmungen – etwa zu Verrechnungszwecken – im derzeitigen § 99 TKG 2003. Lediglich die jeweilige Bestimmung der Auskunftsermächtigung sollte im Materiengesetz (zB UrhG) verankert sein, was zumindest systematisch ohnehin auch mit dem letzten Absatz des Entwurfs in § 99 Abs 5 überstimmt.

Für diesen legislativen Weg spricht auch das Urteil des EuGH vom 10.02.2009 (Rs. 301/06), weil dort ausdrücklich festgehalten wird, dass die RL 2006/24 nicht den Zugang zu den Daten oder deren Nutzung, sondern ausschließlich die Tätigkeiten der Diensteanbieter regelt (Rn 80) (vgl. auch Art 1 Abs 2 der RL und ErwG 13).

3. Der deutsche Gesetzgeber hat die Vorratsdatenspeicherungs-RL bereits umgesetzt. Beim BVerfG in Karlsruhe ist bekanntlich ein Verfahren anhängig, in dem das Höchstgericht bisher mehrere einstweilige Anordnungen erlassen hat. Für Auskünfte, wie sie bei urheber- und leistungsschutzrechtlichen Eingriffen im Internet von Bedeutung sind, hat das BVerfG festgestellt, dass diese weder von der umgesetzten Speicherpflicht des § 113a TKG, noch von der Bestimmung des § 113b TKG, der die Verwendung dieser Daten betrifft, berührt werden.

Vielmehr sei laut ergänzendem Beschluss des BVerfG vom 28.10.2008 zu 1 BvR 256/08 in Rz 88² seine einstweilige Anordnung vom 11.3.2008 nicht auf sog. Bestandsdatenauskünfte (= Stammdatenauskünfte) nach § 113 TKG zu erweitern, auch wenn dabei Daten nach § 113a TKG (= zu speichernde Verkehrsdaten) Verwendung finden. Denn er fand im Rahmen der Folgenabwägung keinen Anlass dafür, eine Nutzung dieser Daten im Wege der einstweiligen Anordnung auszusetzen.

Dies begründet das BVerfG damit, dass nur Bestandsdaten beauskunftet werden³. Die Tatsache, dass diese Auskünfte im strafgerichtlichen Kontext an eine öffentliche Stelle (StA) gehen, war in diesem Punkt nicht entscheidungsrelevant. Das deutsche Beispiel des § 113 TKG und der Rechtsprechung des BVerfG zeigt, dass dieser Ansatz (Auskunftsinhalt sind Bestandsdaten) den Kern der spezifischen Problemstellung wesentlich sachgerechter löst, als jegliche „Verkehrsdatenberührung“ in einen Topf zu werfen.

V) Feststellbarkeit von Anschlussinhabern auch wegen Vermittlerpflichten erforderlich

Der EuGH hat in seiner Entscheidung vom 19.02.2009 zur Rs. C-557/07 ausdrücklich festgehalten, dass der Zugangsprovider der Einzigste ist, der im Besitz jener Daten ist, anhand derer die Verletzer von Urheber- und verwandte Schutzrechte identifiziert werden können. Schlösse man den Zugangsprovider daher vom Begriff des Vermittlers aus, würde der von der Info-Richtlinie beabsichtigte Schutz wesentlich verringert werden (Rn 45).

Gemäß Art 8 Abs 3 RL 2001/29 müssen die Mitgliedstaaten sicherstellen, dass die Rechtsinhaber gerichtliche Anordnungen gegen Vermittler beantragen können, deren Dienste von einem Dritten zur Verletzung eines Urheberrechts oder verwandter Schutzrechte genutzt werden (Rn 42).

Der Zugangsprovider kann aber diesen seinen eigenen Verpflichtungen als Vermittler – etwa auf Unterlassung von ungenehmigten, öffentlichen Zurverfügungstellungen von geschützter Musik – auch nur dann nachkommen, wenn er den betreffenden Anschluss feststellen und den missbräuchlich handelnden Anschlussinhaber eruieren darf. Daher ist die verlässliche Verankerung einer gesetzlichen Regelung, wonach die entsprechenden Verkehrsdaten befristet gespeichert und herangezogen werden dürfen, um die Personenidentität zu einer bestimmten für eine Rechtsverletzung verwendeten IP-Adresse festzustellen, auch aus der Sicht des Gesetzgebers in dieser Hinsicht gemeinschaftrechtlich geboten.

Blickt man auf die gleichartige Problematik und deren Lösung etwa in **England und Frankreich**, dann kann kein Zweifel daran bestehen, dass es in diesen Mitgliedstaaten geradezu selbstverständlich ist, dass ein Teilnehmeranschluss, von dem Urheberrechtsverletzungen ausgehen, feststellbar sein muss. Dort stand bzw. steht lediglich die nachfolgende Frage zur Diskussion, ob der betreffende Anschluss im Fall wiederholter Rechtsverletzungen trotz Unterlassungsaufforderung (befristet) vom Netz genommen werden darf. Die Vorfrage betreffend Feststellung und Auskunft des jeweiligen Anschlusses ist aber telekommunikations-, datenschutz- und urheberrechtlich – unbeschadet der erfolgten Umsetzung der Vorratsda-

² Abrufbar unter:

http://www.bundesverfassungsgericht.de/entscheidungen/rs20081028_1bvr025608.html.

tenspeicherungsRL – klar zugunsten der Durchsetzbarkeit der Immaterialgüterrechte geregelt.

VI) Sonstiges

1. Weiters halten wir den Ansatz in den Erläuterungen des Entwurfs zu § 90 Abs 6 und 7 sowie zu § 92 Abs 3 Z 16 für bedenklich, wonach eine statische IP-Adresse nur dann ein Stammdatum darstellen soll, wenn der Vertrag zwischen Provider und Kunden die ausdrücklich Zuweisung einer bestimmten IP-Nummer für die Dauer der Vertragsbeziehung vorsieht. Damit macht der Gesetzgeber den Eintritt bedeutender Rechtsfolgen von der regelmäßig in der Hand des Providers liegenden Vertragsgestaltung abhängig, anstatt sich an faktischen und überprüfbaren Kriterien zu orientieren. Vergibt ein Provider technisch eindeutig statische IP-Adressen, unterlässt es jedoch – bewusst oder unbewusst – im schriftlichen Vertrag die Zusicherung abzugeben, dass dem Kunden auf Vertragsdauer eine gleichbleibende IP-Nummer zukommt, so ginge ein Auskunftersuchen nach § 90 mit Verweis des Providers auf den Vertragsinhalt ins Leere, obgleich die Beauskunftung objektiv lediglich der Nachschau in einem Kundenverzeichnis entspräche.

2. Der Entwurf beinhaltet keine eindeutige Grundlage dafür, dass Name und Adresse von Inhabern statischer IP-Adressen, sohin Auskünfte, die ohne Verarbeitung von Verkehrsdaten möglich sind, anhand der Bestimmung des § 87b Abs 3 UrhG direkt an den in seinen Rechten Verletzten erfolgen können. Dies, obgleich die Unbedenklichkeit eines solchen gesetzlich verankerten Anspruchs niemals ernsthaft strittig war und vom OGH in seiner Entscheidung vom 14.7.2009 (s.o.) in Punkt 5.2 ausdrücklich – auch gemeinschaftsrechtlich – bestätigt wird. Nunmehr wird der Begriff der statischen IP im Entwurf – wie soeben in Punkt 1 dargestellt – „verquert“ und darüber hinaus sollen gemäß § 90 Abs 6 und 7 iVm § 97 Abs 1 Stammdatenauskünfte nur an Verwaltungsbehörden und strafgerichtliche Behörden erfolgen dürfen. Damit wird ein Widerspruch zu § 87b Abs 3 UrhG offenbar bewusst in Kauf genommen und die Rechtsunsicherheit prolongiert, anstatt sie zu lösen.

Zwar soll der vom OGH angeführte § 97 Abs 2 unverändert bleiben, doch wäre es angebracht, die Zulässigkeit solcher Auskünfte auch im TKG klarzustellen und dabei die beabsichtigte Anknüpfung an die Verträge des Betreibers fallen zu lassen.

3. Die zahlreichen Ausnahmen im Gesetz und im Novellenentwurf für das Speichern und Verwenden von Daten zugunsten der Provider, stehen nicht im Einklang mit den vom Entwurf selbst beschworenen, strengen Vorgaben der VorratsdatenspeicherungsRL. Dieser Umstand macht deutlich, dass der vorliegende Entwurf den Providern - im Gegensatz zu staatlichen Stellen und Dritten - eine privilegierte Stellung zuerkennen möchte: Zu ihren eigenen Betriebs- und Geschäftszwecken wird ihnen die Möglichkeit weitgehender Ermittlung, Verarbeitung (und damit Speicherung) und Verwendung zahlreicher Daten ihrer Kunden gewährt (Beispiele: § 96 Abs 2 2. Satz, § 99 Abs 4, § 102 usw.). Die bestehenden Regeln sind jedenfalls derart weit gefasst, dass es der Provider in der Hand hat, die jeweilige Verarbeitung als „betriebsnotwendige Datenverarbeitung“ zu bezeichnen.

³ Vgl. dazu auch seine einstweilige Anordnung mit Beschluss vom 11.3.2008 Rz 173.

Es ist sachlich schlicht nicht nachvollziehbar, weshalb diese Eingriffe in die Grundrechte der Kommunikationsteilnehmer zugunsten von organisatorisch-wirtschaftlichen Interessen der Provider zulässig, hingegen Auskünfte über einen Teilnehmer, der mit seinem Internetanschluss Gesetze verletzt, grundrechtlich unzulässig sein sollen: Eine eindeutige Schieflage in der Interessenabwägung zugunsten der Provider und zulasten des Schutzbedürfnisses anderer Rechteinhaber.

VII) Regelungsvorschläge

Textvorschlag für einen hinzuzufügenden § 99 Abs 6 TKG:

„§ 99 (6) Anbieter von Internet-Zugangsdiensten haben jene Verkehrsdaten, die notwendig sind, um Stammdaten eines Teilnehmers festzustellen, dem eine öffentliche IP-Adresse zu einem bestimmten Zeitpunkt unter Angabe der zugrundeliegenden Zeitzone zugewiesen war, zum Zweck der Verhütung, Ermittlung, Feststellung und Verfolgung von Verletzungen geistigen Eigentums, die mit Hilfe von Internet-Zugängen erfolgen, ab dem Zeitpunkt ihrer Entstehung bis sechs Monate nach Beendigung der Kommunikation zu speichern. Die Verarbeitung dieser Verkehrsdaten ist ausschließlich zum Zweck der Auskunft von Stammdaten auf Grundlage einer gesetzlichen Auskunftsbestimmung [*eventuell: und einer gerichtlichen Anordnung*] zulässig. Auf Auskünfte nach diesem Absatz ist eine gemäß § 94 Abs 2 erlassene Verordnung zur Kostenerstattung anzuwenden.“

§ 109 Abs 3 Z 17b und Z 21 des Entwurfs wären wie folgt einzufügen bzw. anzupassen:

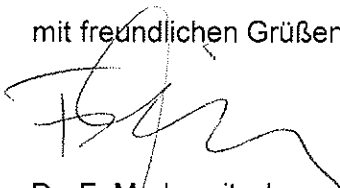
„17b. entgegen § 99 Abs 6 nicht die notwendigen Verkehrsdaten speichert oder nicht Auskünfte über Stammdaten erteilt;“

„21. entgegen § 99 Abs 5 bzw. 6 Auskunft über Stamm- bzw. Verkehrsdaten erteilt oder Verkehrsdaten zu Auskunftszwecken verarbeitet;“

Wir danken für die Gelegenheit zur Stellungnahme und verweisen im Übrigen auch auf unsere bereits vorliegende Stellungnahmen vom 15.5.2007 zum ursprünglichen Entwurf einer TKG-Novelle des BMVIT (630.333/0001-III/PT2/2007).

Mit der Bitte um Kenntnisnahme verbleiben wir

mit freundlichen Grüßen



Dr. F. Medwenitsch
Geschäftsführer