

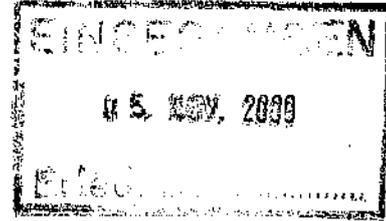


Bundesverfassungsgericht

Erster Senat
- Geschäftsstelle -

Bundesverfassungsgericht • Postfach 1771 • 76006 Karlsruhe

Herrn Rechtsanwalt
Meinhard Starostik
Schillstraße 9
10785 Berlin



Aktenzeichen

Bearbeiter

☎ (0721)

Datum

1 BvR 256/08

(bei Antwort bitte angeben)



04.11.2009

**Verfassungsbeschwerde
des Herrn Prof. Dr. Christoph G u s y ,** 
**und sieben weiterer Beschwerdeführer
vom 31. Dezember 2007**

Dortiges Aktenzeichen: 82/06

Sehr geehrter Herr Rechtsanwalt,

in vorbezeichnetem Verfassungsbeschwerdeverfahren werden Ihnen anliegend die Schreiben des Börsenvereins des Deutschen Buchhandels und des Bundesverbands Musikindustrie vom 6. Februar 2009 sowie der Telecom e.V. vom 30. Oktober 2009 nebst Anlagen zur Kenntnisnahme übermittelt.

Mit freundlichen Grüßen

Auf Anordnung



Regierungshauptsekretärin

Kopie

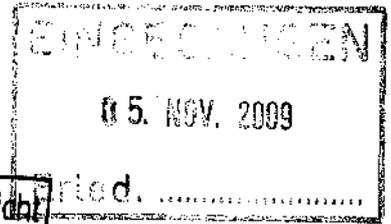
Börsenverein des Deutschen Buchhandels



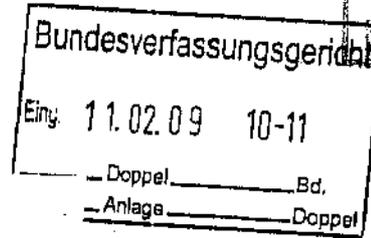
a)

b)

ev. J. 11.2.09



An das
Bundesverfassungsgericht
1. Senat
Postfach 1771
76006 Karlsruhe



Berlin, den 6. Februar 2009

Verfahren: 1 BvR 256/08

Sehr geehrte Frau Dr. Hohmann-Dennhardt, sehr geehrte Herren,

als Vertreter zweier in erheblichem Maße von der massenhaften Internet-Piraterie betroffenen Branchen wenden wir uns in der Verfassungsbeschwerde (Az 1 BvR 256/08) bezüglich des Gesetzes zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG vom 21. Dezember 2007 (BGBl I S. 3198) an Sie. Dies in der Überzeugung, dass die bevorstehende Grundsatz-Entscheidung über die in diesem Verfahren gegenständlichen Rechtsfragen von großer Bedeutung für die von uns vertretenen Rechteinhaber sein kann. Inhaltlich geht es dabei um die Gewährleistung der Rechtsdurchsetzung im „digitalen Zeitalter“, die für uns - wie auch für viele andere betroffenen Rechteinhaber - nur bei Vorliegen einer Datenbasis überhaupt noch möglich ist.

I. Zu den Hintergründen

Illegale Angebote urheberrechtlich geschützter Inhalte im Internet erfolgen heute überwiegend, wenn nicht ausnahmslos, über dynamische IP-Adressen. Allein für die Musikindustrie geht das Marktforschungsinstitut GfK in der für den Bundesverband Musikindustrie erstellten Brennerstudie davon aus, dass im Jahr 2007 rund 312 Millionen Titel illegal aus dem Internet heruntergeladen wurden. Auf einen legal heruntergeladenen Titel kommen nach dieser Erhebung fast 10 illegale.

Bei der zivil- oder strafrechtlichen Verfolgung solcher Urheberrechtsverstöße lässt sich der Sachverhalt nur über eine Zuordnung der bereits im Wege der Ermittlungen bekannt gewordenen Verkehrsdaten (Nummer der dynamischen IP-Adresse und exakte Zeit des illegalen Angebots) zu den nur dem Internetserviceprovider (ISP) bekannten Bestandsdaten (Name und Anschrift des Nutzers) ermitteln. Während bei statischen IP-Adressen einfach nur die Bestandsdaten zu der IP-Adresse herausgesucht zu werden brauchen (wie bei der Zuordnung eines Namens zu einer Nummer im Telefonbuch), muss der ISP bei dynamischen IP-Adressen zunächst die vom „Anzeigerstatter“ ermittelten Verkehrsdaten mit den bei ihm gespeicherten Verkehrsdaten abgleichen (eben um die erforderliche Zuordnung vorzunehmen), um nach erfolgter Zuordnung aber - wie bei einer statischen IP-Adresse - nur die Bestandsdaten herauszugeben.

Das Verfahren ähnelt der Suche nach Name und Adresse eines flüchtigen Unfallverursachers, der das Tatfahrzeug nur gemietet hat. Alle Beweismittel über den Tathergang sind in einem solchen Fall bekannt. Ebenso das Kennzeichen des Fahrzeugs. Als Halter ist aber der Vermieter, nicht der Fahrer registriert. § 28 Abs. 3 Nr. 2 BDSG erlaubt in solchen Fällen dem Vermieter, den strafrechtlichen Ermittlern Name und Adresse des Mieters herauszugeben. § 28 Abs. 3 Nr. 1 BDSG ermöglicht das gleiche auch gegenüber einem privaten Anspruchsteller.

Ebenso wie in diesem Beispiel existiert auch bei Urheberrechtsverletzern, die sich dynamischer IP-Adressen bedienen, keine andere Möglichkeit, den Namen und die Anschrift (also die Bestandsdaten) des Anschlussinhabers (der regelmäßig mit dem Verletzer identisch ist) zu ermitteln, als über den Abgleich mit vom ISP gespeicherten Verkehrsdaten. Hier wie dort geht es aber ausschließlich um die Herausgabe von Bestandsdaten. Der straf- und zivilrechtliche Tatvorwurf als solcher lässt sich vollständig ohne Rückgriff auf die beim ISP gespeicherten Verkehrsdaten darlegen und beweisen. Die Tat ist gewissermaßen dokumentiert und auf Ebene der bekannten (dynamischen) IP-Adresse auch personalisiert. Es fehlen nur noch Name und Anschrift des Anschlussinhabers.

Strafrechtliche Ermittlungen stützen sich bei solchen Auskunftsbegehren auf §§ 161, 163 StPO i. V. m. § 113 TKG. Zivilrechtliche Auskunftsansprüche gegen Diensteanbieter ergeben sich aus dem mit Wirkung zum 1. September 2008 in Kraft getretenen § 101 Abs. 9 UrhG. Diese Vorschrift wurde in Umsetzung der EU-Richtlinie 2004/48/EG in das Urheberrechtsgesetz aufgenommen und lautet wie folgt:

3

„(9) Kann die Auskunft nur unter Verwendung von Verkehrsdaten (§ 3 Nr. 30 des Telekommunikationsgesetzes) erteilt werden, ist für ihre Erteilung eine vorherige richterliche Anordnung über die Zulässigkeit der Verwendung der Verkehrsdaten erforderlich, die von dem Verletzten zu beantragen ist. Für den Erlass dieser Anordnung ist das Landgericht, in dessen Bezirk der zur Auskunft Verpflichtete seinen Wohnsitz, seinen Sitz oder eine Niederlassung hat, ohne Rücksicht auf den Streitwert ausschließlich zuständig. Die Entscheidung trifft die Zivilkammer. (...) Die Vorschriften zum Schutz personenbezogener Daten bleiben im Übrigen unberührt.“

§ 101 Abs. 9 UrhG geht ohne weiteres davon aus, dass die für die Erteilung der Auskunft über Name und Anschrift der Urheberrechtsverletzer erforderlichen Verkehrsdaten dem zur Auskunft Verpflichteten zur Verfügung stehen. Genau dies ist aber durch diese Norm selbst nicht ausdrücklich sichergestellt.

Für die folgenden Darlegungen sei unterstellt, dass möglicherweise zumindest in gewissen Fällen (z.B. bei Flatrate-Nutzern) vom ISP künftig Verkehrsdaten entgegen der bisherigen Praxis sofort nach Ende der Verbindung gelöscht werden. Diese Möglichkeit hat das Bundesverfassungsgericht in seinem Beschluss vom 27. Oktober 2006 (Rz. 26) ausdrücklich erwähnt, soweit es um Fälle der Speicherung aufgrund § 97 Abs. 4 TKG geht. Damit stellt sich die Frage nach der Datenbasis für den Auskunftsanspruch nach § 101 Abs. 9 UrhG:

- Ein zivilrechtlicher Zugriff auf ausschließlich nach § 113a TKG gespeicherten Vorratsdaten – und sei es auch nur zum Abgleich im Rahmen einer Auskunft über Bestandsdaten - ist in § 113b TKG nicht vorgesehen. Sollte sich also die Speicherung der Vorratsdaten allein auf § 113a TKG stützen, ginge der zivilrechtliche Auskunftsanspruch nach § 101 Abs. 9 UrhG ins Leere, obwohl die Daten eigentlich gespeichert vorliegen.
- Nach § 96 Abs. 2 TKG dürfen „die gespeicherten Verkehrsdaten“ über das Ende der Verbindung hinaus nur verwendet werden, soweit sie „für die in §§ 97, 99, 100 und 101 genannten oder für die durch andere gesetzliche Vorschriften begründeten Zwecke erforderlich sind.“ Es wäre also denkbar, sich im Rahmen des zivilrechtlichen Auskunftsverfahren nach § 101 Abs. 9 UrhG (n.F.) auf § 96 Abs. 2, ggf. in Verbindung mit § 100 TKG, zu stützen, weil diese Speicherung für die durch diese gesetzliche Vorschrift begründeten Zwecke, nämlich die Auskunftserteilung nach § 101 Abs. 9 UrhG, erforderlich wäre (so OLG Köln, GRUR- RR 2009, 9, 11). Zwar enthält § 101 UrhG keinerlei Hinweise zur Dauer einer solchen Datenspeicherung, jedoch gilt dies gleichermaßen für die §§ 99 und 101 TKG, die in § 96 Abs. 2 TKG ausdrücklich genannt sind. Gemäß § 100 Abs. 3 S. 2 TKG, der hier wohl in Verbindung mit § 96 Abs. 2 TKG heranzuziehen wäre, darf der Diensteanbieter die erhobenen Verkehrsdaten

in der Weise verwenden, „dass aus dem Gesamtbestand aller Verkehrsdaten, die nicht älter als sechs Monate sind, die Daten derjenigen Verbindungen des Netzes ermittelt werden, für die tatsächliche Anhaltspunkte den Verdacht der rechtswidrigen Inanspruchnahme von Telekommunikationsnetzen und -diensten begründen.“ Damit sind sechs Monate die Obergrenze für die generell-abstrakte Vorhaltung sämtlicher Verkehrsdaten, die indes möglicherweise für die Aufklärung von Urheberrechtsverletzungen gar nicht ausgeschöpft werden müsste. Nach den Vorschriften des TKG bleibt mithin eine generell-abstrakte Speicherung für zivilrechtlich begründete Ansprüche möglich, wenn sie denn, wie hier, durch einen gesetzlich verankerten Zweck (Auskunftserteilung gemäß § 101 Abs. 9 UrhG mit ausdrücklicher Nennung von Verkehrsdaten) gerechtfertigt ist.

Dies aber bedeutet, dass im Ergebnis für zivilrechtliche Zwecke, nämlich zur Durchsetzung des Auskunftsanspruchs des § 101 Abs. 9 UrhG im Hinblick auf die Nutzung dynamischer IP-Adressen, eine ebenso unspezifische generelle Vorratsdatenspeicherung erfolgen müsste, wie sie § 113a TKG für die eng begrenzten Zwecke des Strafrechts und der Gefahrenabwehr vorsieht. Damit stellen sich hier im Wesentlichen ähnliche verfassungsrechtliche Fragen, wie sie das Bundesverfassungsgericht gegenwärtig in der Hauptsache zu § 113a TKG, insbesondere im Hinblick auf §§ 113b, 113 TKG zu entscheiden hat.

II. Zur Hauptsacheentscheidung des Bundesverfassungsgerichts

Laut eines Schreibens des Bundesjustizministeriums vom 28. März 2008 (zu Az. RB 3 zu 4104/11-R5 201/2008, am Ende) bezieht sich die einstweilige Anordnung des Bundesverfassungsgerichts (1 BvR 256/08) ausdrücklich nur auf § 113b Abs. 1 Satz 1 (Halbsatz 1) Nr. 1 TKG i. V. m. § 100g StPO. Von der einstweiligen Anordnung unberührt bleibe deshalb die in § 113b Abs. 1 Satz 1 Halbsatz 2 TKG ausdrücklich geregelte – und vom Bundesverfassungsgericht ausweislich Absatz 10 des Beschlusses vom 11. März 2008 auch gesehene – (unternehmensinterne) Verwendung der allein nach § 113a TKG gespeicherten Daten für die Erteilung von Bestandsdatenauskünften nach § 113 TKG. Auf Fälle, in denen gemäß §§ 161, 163 StPO i. V. m. § 113 TKG u.a. Name und Anschrift des hinter einer bereits bekannten (dynamischen) IP-Adresse stehenden Anschlussinhabers beauskunftet werden soll, habe die einstweilige Anordnung daher keine (beschränkenden) Auswirkungen.

Dies wird vom Bundesverfassungsgericht bestätigt, gilt aber nur für die Einstweilige Anordnung als solche. Denn in der erweiterten einstweiligen Anordnung vom 28. Oktober 2008 (1 BvR 256708 (Rn. 88)) heißt es ausdrücklich:

„Die einstweilige Anordnung ist auch nicht im Hinblick darauf zu erweitern, dass die nach § 113a TKG gespeicherten Daten gemäß § 113b S. 1 Hs. 2 TKG nach der gegenwärtigen Rechtsauslegung und –praxis auch zur Erteilung von Auskünften nach § 113 TKG (sogenannte Bestandsdatenauskunft) verwendet werden (...). Zwar wirkt auch diese Nutzung Rechtsfragen auf, die im Hauptsacheverfahren näherer Prüfung bedürfen. Das Vorbringen der Beschwerdeführer gibt aber keinen Anlass im Rahmen der Folgenabwägung nunmehr zu einem anderen Ergebnis zu kommen und eine Nutzung dieser Daten im Wege der einstweiligen Anordnung vorläufig auszusetzen.“
(Hervorhebung vom Verfasser)

Im Ergebnis bedeuten diese Äußerungen des Bundesverfassungsgerichts, dass im Hauptsacheverfahren auch die Erteilung von Auskünften nach § 113 TKG, soweit sie einen Abgleich mit Vorratsdaten voraussetzen, überprüft werden wird.

Nach dem oben Gesagten entspricht in der gesetzlichen Ausgestaltung die Auskunftserteilung gemäß §§ 113, 111 TKG im strafrechtlichen Bereich ziemlich genau dem Auskunftsverfahren nach § 101 Abs. 9 UrhG i. V. m. § 96 Abs. 2 TKG für den zivilrechtlichen Bereich. Daraus ergibt sich, dass etwaige Erwägungen des Bundesverfassungsgerichts in der Hauptsache zu § 113a TKG, die zu einer möglichen Verfassungswidrigkeit von § 113b S. 1 letzter Hs. i. V. m. § 113 TKG führen sollte, mit großer Wahrscheinlichkeit Auswirkungen auf die Durchsetzbarkeit zivilrechtlicher Auskunftsansprüche nach § 101 Abs. 9 UrhG i.V.m. § 96 Abs. 2 TKG haben dürften, soweit diese Bestandsdaten-Auskünfte nur über Heranziehung von Verkehrsdaten geschehen können, die zu diesem Zwecke gespeichert und vorgehalten werden müssten.

Umgekehrt bedeutet dies aber auch, dass das Auskunftsverfahren nach § 101 Abs. 9 UrhG Anhaltspunkte für die Güterabwägung im Rahmen der Hauptsache-Überprüfung des §§ 113b S. 1 letzter Hs. 113 TKG enthält. Denn ohne Vorratsdatenspeicherung liefe die Auskunftsmöglichkeit bei der Ermittlung dynamischer IP-Adressen regelmäßig leer. Damit wären die Rechte des geistigen Eigentums gegenüber Verletzern, die unter dem Schutz solcher dynamischen IP-Adressen operieren, faktisch nicht mehr durchsetzbar. Ein ganzes Segment von Rechten, die ihrerseits dem Schutz des Art. 14 GG unterfallen, wäre ausgerechnet in einem besonders stark von Rechtsverletzungen betroffenen Bereich zivilrechtlich schutzlos gestellt.

Noch aus einem weiteren Grund ist es für die Abwägung der widerstreitenden Interessen unumgänglich, diese Parallele zwischen zivilrechtlichen Auskunftsansprüchen und Anfragen staatlicher Behörden (die beide ohne Vorratsdatenspeicherung nicht beantwortet werden können) im Rahmen der verfassungsrechtlichen Güterabwägung zu würdigen:

Bis zum Inkrafttreten des § 101 UrhG n.F. zeigte sich zunehmend, dass die Ermittlungsbehörden den bis dahin zwangsläufigen „Umweg“ über das strafrechtliche Ermittlungsverfahren

als belastend und unangemessen betrachten, und zwar selbst dort, wo Verkehrsdaten noch vorhanden waren. Erstmals kam dies in einem (nicht in Rechtskraft erwachsenen) Beschluss des Amtsgerichts Offenburg vom 20. Juli 2007 (Az. 4 Gs 442/07) zum Ausdruck, wo es heißt (S. 7):

„Die Anzeigeerstatter sehen sich zu diesem Umweg über das Strafrecht veranlasst, weil ihnen zivilrechtlich ein eigener Auskunftsanspruch gegen Provider auf Offenlegung der Daten nicht zusteht. Mit der beschriebenen bundesweiten Anzeigenkampagne, die den Strafverfolgungsbehörden mehrere 10.000 Strafverfahren beschert, streben die Anzeigeerstatter also Auskünfte an, die ihnen der Gesetzgeber bewusst versagt hat (...).“

Erst unlängst wies auch das LG München I (5 Qs 19/08) einen solchen auf § 406d StPO gestützten Antrag des verletzten Berechtigten auf Akteneinsicht zurück.

Auch dieses Problem muss die Abwägung einbeziehen, welche im Hauptsacheverfahren anzustellen ist, und zwar für den Fall, dass eine Speicherung von Daten zum Zwecke der auf § 109 Abs. 9 UrhG gestützten Auskunftserteilung verfassungsrechtlich ausgeschlossen sein sollte. Wenn nämlich den Berechtigten die Einsicht in die strafrechtliche Ermittlungsakte für die Durchsetzung ihrer zivilrechtlichen Ansprüche versagt bliebe, würde dies im Ergebnis dazu führen, dass die Rechtsinhaber hinsichtlich der Online-Piraterie mit dynamischen IP-Adressen jeder zivilrechtlichen Möglichkeit zur Durchsetzung ihrer Rechte beraubt wären.

In der Entscheidung des EuGH in Sachen *Promusicae* (GRUR Int. 2008, 323), die sich mit der benachbarten Frage beschäftigt, ob und in welchem Umfang der nationale Gesetzgeber gezwungen ist, zivilrechtliche Vorkehrungen für die Herausgabe personenbezogener Daten bei Urheberrechtsverletzungen zu schaffen, heißt es zu der dabei gebotenen Abwägung (Rz. 70):

„Die Mitgliedstaaten sind gemäß dem Gemeinschaftsrecht jedoch dazu verpflichtet, sich bei der Umsetzung dieser Richtlinien auf eine Auslegung derselben zu stützen, die es ihnen erlaubt, ein angemessenes Gleichgewicht zwischen den verschiedenen durch die Gemeinschaftsrechtsordnung geschützten Grundrechten sicherzustellen.“

Würde das Bundesverfassungsgericht auch die Auskunftserteilung an Strafverfolger gemäß § 113b S. 1 letzter Hs. i. V. m. § 113 TKG in solchen Fällen einschränken oder unterbinden, oder würden tatsächlich künftig solche Verletzterdaten nicht mehr zur zivilrechtlichen Verfolgung an die Opfer weitergereicht, liefe die verfassungsrechtliche Gewährleistung des geistigen Eigentums insoweit gänzlich leer. Sollte aus Sicht des Bundesverfassungsgerichts ein zivilrechtlicher Auskunftsanspruch keine Datenspeicherung zum Zwecke der Ermöglichung eben dieser Auskunft rechtfertigen, wäre es im Rahmen der Hauptsacheentscheidung wichtig zu erfahren, wie nach Auffassung des Bundesverfassungsgerichts *„ein angemessenes Gleichgewicht zwischen den verschiedenen durch die Gemeinschaftsrechtsordnung ge-*

7

„schützten Grundrechten“ im Sinne der *Promusicae*-Entscheidung des EuGH sichergestellt werden kann.

Wir halten es nach alledem für unbedingt geboten, die Notwendigkeit der Vorratsdatenspeicherung zum Zwecke des Abgleichs für eine Auskunft nur über Bestandsdaten eines Verletzers auch bei Verfolgung von Urheberrechtsverletzungen in die Güterabwägung einzubeziehen, die im Zuge der Hauptsacheentscheidung der Verfassungsbeschwerde gegen § 113a TKG anzustellen ist. Dies gilt besonders im Hinblick auf den in § 101 Abs. 9 UrhG ausdrücklich vorgesehenen Auskunftsanspruch und die zu dessen Erfüllung erforderliche Vorratsdatenspeicherung.

Wegen der weiteren Einzelheiten in tatsächlicher Sicht stehen Bundesverband Musikindustrie und Börsenverein jederzeit gern für weitere Auskünfte zur Verfügung.

Mit freundlichen Grüßen

Dr. Florian Drücke, Maître en Droit
- Leiter Recht und Politik -
Bundesverband Musikindustrie e.V.

Dr. Christian Sprang
- Justiziar -
Börsenverein e.V.



ERNEUERUNGSSTAMPEN
 05. NOV. 2009
 Erled.

BUNDESVERBAND DER ANWENDER GESCHÄFTLICHER TELEKOMMUNIKATION

TELECOM e.V. • Niddastraße 49 • D-61440 Oberursel

Bundesverfassungsgericht
 Herr Dr. [redacted]
 Postfach 1771
 76006 Karlsruhe

*Empfangen am 2. 11. 09
 im Sekretariat
 M. 2*

Ihre Zeichen, Ihre Nachricht vom

Unser Zeichen, unsere Nachricht vom

Datum

30. Oktober 2009

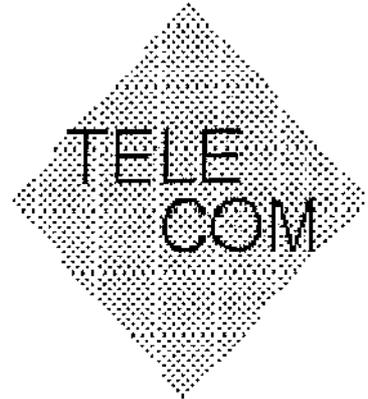
**Verfassungsbeschwerden1
 BvR 256/08 und 586/06, Fragen an Verbände**

Sehr geehrter Herr Dr. [redacted]

wie mit Herrn Kohl besprochen, senden wir Ihnen das Schreiben mit dem Anhang zu.

Mit freundlichen Grüßen
 TELECOM e.V.





TELECOM e.V. • Niddastraße 49 • D-61440 Oberursel

Bundesverfassungsgericht
Postfach 1771
76006 Karlsruhe

Ihre Zeichen, Ihre Nachricht vom

Unser Zeichen, unsere Nachricht vom

Datum

25. Mai 2009

**Verfassungsbeschwerden 1
BvR 256/08, 263/08 und 586/06, Fragen an Verbände**

Sehr geehrte Damen und Herren,

Sie haben an einige Fachverbände der Telekommunikation bzgl. o.a. Verfahren einen Fragebogen verteilt und um Beantwortung der dort aufgeworfenen Fragen gebeten.

Der Telecom e.V. als bereits lange bestehender Verband der Anwender geschäftlicher Telekommunikation war nicht angesprochen, seine Mitglieder sind jedoch insbesondere von der Frage 8 essentiell berührt.

Wir erlauben uns daher auch ungefragt die Frage 8 aus Sicht der geschäftlichen Anwender von Telekommunikation und Betreiber großer Corporate Networks zu beantworten.

Wir bitten um entsprechende Berücksichtigung und bieten gerne auch weiterführende Gespräche zu diesem Thema an.

Mit freundlichen Grüßen
Telecom e.V.



Präsident

Vizepräsident

TELECOM e.V.
Niddastraße 49
D-61440 Oberursel
Registergericht Köln

Registernummer VR 7683

Telefon: +49(0) 6171 279 88 07
Fax: +49(0) 6171 279 88 07
telecom-ev@telecom-ev.de
www.telecom-ev.de
0329002129

Präsident:
Helmut Kohl

USt-IdNr.: DE121948301

Bankverbindung:
Kreissparkasse Köln
BLZ: 37050299
Konto:



TELECOM e.V.

Verband der Anwender
geschäftlicher Telekommunikation

Oberursel, den

22.5.2009

Fragenkatalog zur Vorratsdatenspeicherung

(Verfassungsbeschwerden 1 BvR 256/08, 263/08 und 586/06)

Der Telecom e.V. ist der Verband großer geschäftlicher Anwender von Telekommunikation und vertritt seit über 30 Jahren die Interessen großer Unternehmen, deren Kerngeschäftsfelder außerhalb der Telekommunikation liegen, für die die Telekommunikation jedoch ein wesentlicher Produktionsfaktor ist, das zentrale Nervensystem aller innerbetrieblichen Abläufe und der Zusammenarbeit mit Vorlieferanten und Kunden.

Mit Erstaunen haben wir zur Kenntnis genommen, dass das Bundesverfassungsgericht einen Fragebogen über die Praxis der Vorratsdatenspeicherung an einige Branchenverbände verteilt hat, jedoch den Telecom e.V. ausgenommen hat, obwohl dieser und seine Mitglieder von der Frage 8. über die zur Speicherung Verpflichteten durchaus betroffen sind. Wir erlauben uns, dennoch zur Frage 8 eine Antwort zu geben und bitten, diese gebührend zu berücksichtigen.

In der Praxis speichern die Betreiber von sogenannten Corporate Networks, deren Teilnehmer aus kooperierenden Unternehmen mit einer abzählbaren und namentlich benennbaren Menge von Teilnehmern bestehen, die bei der Nutzung entstehenden Verkehrsdaten nicht bzw. nur insoweit, wie dies für die interne Abrechnung, die Kapazitätsplanung der internen Netze und für die Analyse von Störungen erforderliche ist. Die Daten werden typischerweise unverzüglich, d.h. sobald sie für diese Zwecke nicht mehr benötigt werden, gelöscht.

Das Selbstverständnis der Betreiber von Corporate Networks ist, dass sie keine öffentlich zugänglichen Telekommunikationsdienste anbieten und daher von der Speicherungsverpflichtung des § 113 a TKG bzw. Artikel 1 der Richtlinie 2006/24/EG nicht erfasst werden. Dieses Selbstverständnis beruht auf dem seit spätestens dem Jahr 1990 bestehenden Rechtsverständnis von Telekommunikationsdiensten für die Öffentlichkeit, die Corporate Networks eindeutig davon abgrenzt (vgl. z.B. Richtlinie 90/388/EG, die hierfür lange Zeit maßgeblich war). Dies wurde mit den sogenannten Corporate Network Verfügungen 1, 8 und 9/ 1993 des Bundesministeriums für Post und Telekommunikation für die Anwendung in Deutschland noch einmal deutlich konkretisiert. Wir sehen keine Veranlassung und keine

TELECOM e.V., Niddastraße 49, 61440 Oberursel, Tel: (06171) 279 8807, Fax: (06171) 279 8675

Mail: telecom-ev@telecom-ev.de, www.telecom-ev.de

Vertretungsberechtigte Präsidiumsmitglieder: Helmut Kohl (Präsident),
Raymund Eisele, Dr. Thomas Plückebaum, Bernd Breininger, Wolfgang Kuhl
Amtsgericht Köln VR7683

Grundlage, dieses Verständnis zu ändern. Es deckt sich nach unserer Erfahrung auch immer noch mit der gelebten Praxis in den anderen Mitgliedsstaaten der Europäischen Union.

Es hat, so haben uns einige Mitglieder berichtet, in der jüngeren Vergangenheit in einzelnen Fällen Bestrebungen von Strafverfolgungsbehörden gegeben, Corporate Networks in die Vorratsdatenspeicherung einzubeziehen. Aufgrund der hohen Kosten, die mit einer derartigen Speicherungsverpflichtung und dem geschützten Aufbewahren derartiger Daten einhergehen, würden wir eine Einbeziehung in eine automatische Vorratsdatenspeicherung über längere Zeit für unverhältnismäßig erachten. Zudem sind die Daten, sofern sie das interne Corporate Network verlassen, bei den öffentlichen Diensteanbietern in vielen Teilen im Rahmen der Vorratsdatenspeicherung erfasst. Selbstverständlich wird zudem jeder Betreiber von Corporate Networks bereit sein, ggf. verfügbare Daten für Zwecke einer Strafverfolgung im Rahmen seiner Pflichten als Zeuge herauszugeben, auch schon, um einer möglichen Beschlagnahme seiner für den Unternehmensbetrieb ja essentiell wichtigen Kommunikationssysteme zu vermeiden.

Im Kontext der in der jüngeren Vergangenheit öffentlich gewordenen Fällen von Bespitzelung der Mitarbeiter bzgl. ihrer Kommunikationsbeziehungen (Deutsche Bahn, Deutsche Telekom) wäre das Sammeln und Vorhalten von Daten über eben diese Kommunikationsbeziehungen in allen Unternehmen sowie die Möglichkeit, diese einfach auszuwerten (Vorratsdatenspeicherung für Unternehmensnetze), wie das Öffnen eines großen Tores hin zu Grundrechtsverletzungen (z.B. Verletzung des Fernmeldegeheimnisses). Durch das Tor hindurchgehen darf man nicht – aber die Versuchung wird deutlich größer.

Wir würden es begrüßen, wenn sich das BVerfG im Rahmen der anstehenden Verfahren auch zum Thema des vom Gesetzgeber gewollten Ausparens der Corporate Networks eindeutig klarstellend äußern würde, um zukünftige Diskussionen mit den unterschiedlichen Strafverfolgungsbehörden überflüssig zu machen und auch diesbzgl. Rechtssicherheit zu schaffen.

Für eine vertiefende Behandlung der vielfältigen Aspekte von Corporate Networks bieten wir hiermit gerne weiterführende Gespräche an. Als Ansprechpartner des Telecom e.V. steht Ihnen der Sprecher unseres Arbeitskreises Regulierung



jederzeit gerne zur Verfügung.