



Der Bundesbeauftragte
für den Datenschutz und
die Informationsfreiheit

Deutscher Bundestag

Innenausschuss

Ausschussdrucksache

17(4)680 G

Peter Schaar

Bundesbeauftragter für den Datenschutz
und die Informationsfreiheit

POSTANSCHRIFT Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit,
Postfach 1468, 53004 Bonn

Vorsitzenden des Innenausschusses
des Deutschen Bundestags
Herrn Wolfgang Bosbach
Platz der Republik 1
11011 Berlin

HAUSANSCHRIFT Husarenstraße 30, 53117 Bonn
VERBINDUNGSBÜRO Friedrichstraße 50, 10117 Berlin

TELEFON (0228) 997799-100

TELEFAX (0228) 997799-550

E-MAIL Ref8@bfdl.bund.de

INTERNET www.datenschutz.bund.de

DATUM Bonn, 11.03.2013

BETREFF **Gesetz zur Änderung des TKG und zur Neuregelung der Bestandsdatenaus-**
kunft

HIER Stellungnahme anlässlich der Anhörung im Innenausschuss am 11.03.2013

Sehr geehrter Herr Bosbach,

beim vorliegenden Gesetzesentwurf hat sich die Bundesregierung weitgehend auf die konkrete Umsetzung der Vorgaben des Bundesverfassungsgerichtes beschränkt. Zwar wurden im Rahmen des Gesetzgebungsverfahrens bereits eine Reihe meiner Änderungsvorschläge berücksichtigt, eine meiner wesentlichen Forderungen, die Bestandsdatenauskunft als solche – zumindest hinsichtlich ihres Umfangs – zu hinterfragen, dabei allerdings außer Acht gelassen. Ich halte diesen weiteren Schritt jedoch für zwingend erforderlich, stellt das gegenständliche Auskunftsverfahren doch teilweise einen nicht unerheblichen Eingriff in die Rechte der Betroffenen dar.

Dabei bin ich mir der grundsätzlichen Notwendigkeit der Bestandsdatenauskunft als Mittel einer effektiven Strafverfolgung durchaus bewusst. Gleiches gilt für den Umstand, dass das Bundesverfassungsgericht in seinem Beschluss vom 24.01.2012 den materiellen Rahmen des Auskunftsverfahrens weitgehend als verfassungsgemäß bestätigt hat. Allerdings sollten die Entscheidungen des Bundesverfassungsgerichts als Grenzziehungen angesehen werden und nicht als Verpflichtungen für den Ge-



setzgeber, den dadurch gegebenen verfassungsrechtlichen Rahmen – im Sinne maximal zulässiger Grundrechtseingriffe – voll auszuschöpfen. Politisch muss somit nicht alles umgesetzt werden, was verfassungsrechtlich erlaubt wäre.

Konkret möchte ich zum vorliegenden Gesetzentwurf außerdem noch auf die folgenden datenschutzrechtlich relevanten Punkte hinweisen:

Benachrichtigungspflicht

Der Gesetzentwurf enthält bislang keine Regelungen zur nachträglichen Benachrichtigung der von einem Auskunftersuchen betroffenen Personen. Dass eine solche Information der Betroffenen aber jedenfalls für den Fall eines Auskunftersuchens hinsichtlich des Inhabers einer bestimmten IP-Adresse nach § 113 Abs. 1 S. 3 TKG-E erforderlich ist, hat das Bundesverfassungsgericht bereits in seinem Urteil zur Vorratsdatenspeicherung eindeutig festgestellt (BVerfG, Urteil vom 02.03.2010 – 1 BvR 256/08, Rn. 263, 291). Diese Benachrichtigungspflicht muss sich an die die Daten abfragenden Bedarfsträger richten, da nur diese – und nicht die Telekommunikationsanbieter – beurteilen können, ob und in welchen Fällen ausnahmsweise von einer Benachrichtigung abgesehen werden kann bzw. muss. Dementsprechend ist eine entsprechende Regelung in die jeweiligen sich auf § 113 Abs. 1 S. 3 TKG-E beziehenden fachgesetzlichen Abrufnormen aufzunehmen.

Ordnungswidrigkeiten

Nach § 113 Abs. 3 Nr. 1 TKG-E wird die Auskunft über den Inhaber einer IP-Adresse nach § 113 Abs. 1 S. 3 TKG-E auch zur Verfolgung von Ordnungswidrigkeiten ermöglicht. Mangels entsprechender Beschränkungen im Gesetzentwurf ist über § 46 OWiG i.V.m. § 100j StPO-E die Auskunft für jede noch so „kleine“ Ordnungswidrigkeit zulässig. Dies widerspricht jedoch eindeutig den Vorgaben des Bundesverfassungsgerichts aus dem Vorratsdatenspeicherungsurteil, in dem es explizit ausführt, dass eine entsprechende Auskunft ausschließlich zur Verfolgung besonders gewichtiger Ordnungswidrigkeiten zulässig ist, die vom Gesetzgeber explizit benannt werden müssen (BVerfG, Urteil vom 02.03.2010 – 1 BvR 256/08, Rn. 262). Der Gesetzentwurf ist daher um eine entsprechende Beschränkung zu ergänzen.

Richtervorbehalt

Auch wenn vom Bundesverfassungsgericht nicht explizit gefordert, halte ich die Einführung eines Richtervorbehalts für die Auskunft über den Inhaber einer IP-Adresse nach § 113 Abs. 1 S. 3 TKG-E für datenschutzrechtlich geboten. Diese Notwendig-



keit ergibt sich aus dem nunmehr auch vom Bundesverfassungsgericht im Beschluss vom 24.01.2012 explizit anerkannten Eingriff einer solchen Auskunft in das Fernmeldegeheimnis nach Art. 10 GG. Die hohe Sensibilität von Daten, die das Fernmeldegeheimnis tangieren, zieht unweigerlich das Erfordernis nach sich, den vom Grundgesetz gewährten besonderen Schutz auch auf ihre praktische Handhabung zu übertragen. Dieser Anforderung wird man aber lediglich dann gerecht, wenn – im Verhältnis zur „klassischen“ Bestandsdatenauskunft – die Auskunft über den Inhaber einer IP-Adresse unter die erhöhten Anforderungen einer gerichtlichen Genehmigung gestellt wird.

Die Notwendigkeit eines Richtervorbehalts bekommt noch eine besondere Bedeutung mit Blick auf die gegenwärtige Umstellung des Internetprotokolls von der Version 4 auf die Version 6. Diese Bedenken wurden auch vom Bundesverfassungsgericht aufgegriffen (BVerfG, Beschluss vom 24.01.2012 – 1 BVR 1299/05, Rn. 161). Durch den Wechsel zu IPv6 ist es künftig möglich, jedem Endgerät eine eigene feste IP-Adresse zuzuteilen. Zu den auf diese Weise direkt adressierbaren Geräten werden in Zukunft nicht mehr nur Computer, Tablets oder Smartphones eine IP-Adresse benötigen, sondern im Zusammenhang mit dem „Internet of Things“ auch Kühlschränke, Autos, medizinische Geräte, u.v.m. Selbst wenn auch IPv6-Adressen grundsätzlich dynamisch vergeben werden können, steht zu vermuten, dass gerade von letzteren Geräten der Praktikabilität halber vornehmlich statisch vergebene Adressen verwendet werden. Doch auch bei den „klassischen“ Endgeräten wie Computern ist zum momentanen Zeitpunkt noch nicht sicher absehbar, ob der Wechsel zu IPv6 schon mittelfristig zu einer Abkehr von der dynamischen Vergabe der IP-Adressen führen wird. Dementsprechend bringt die Umstellung der Internetprotokollversion aus Datenschutzsicht jedenfalls ein erhöhtes Gefährdungspotential mit sich. Um diesem von Anfang an angemessen zu begegnen erscheint die Einführung eines Richtervorbehaltes der einzig konsequente Schritt, zumal somit auch der Gefahr vorgebeugt wird, bereits in wenigen Jahren eine erneute gesetzliche Anpassung vornehmen zu müssen, sollte sich das datenschutzrechtliche Gefahrenpotential von IPv6 realisieren.

Schließlich rege ich die Einführung eines Richtervorbehaltes auch für die Auskunft über Daten zur Zugangssicherung i.S.d. § 113 Abs. 1 S. 2 TKG-E an. So ist zu beachten, dass die über diese Auskunftsmöglichkeit zu erlangenden Daten unter anderem auch Zugang zu äußerst sensiblen Informationen der Betroffenen ermöglichen können. Der vorliegende Entwurf entspricht zwar hier formal den Vorgaben des Bundesverfassungsgerichts, durch die offene Formulierung des Gesetzestextes werden aber neben den klassischen Zugangssicherungen bei Mobilfunkendgeräten wie PIN und PUK auch Passwörter erfasst, die den Zugang zu E-Mail-Konten oder Cloud-Speichern ermöglichen. Dies erlaubt unter Umständen den Zugriff der abfragenden



Bedarfsträger auf Informationen, die eventuell sogar der Intimsphäre unterfallen könnten und somit besonders schützenswert sind. Das Bundesverfassungsgericht hat in diesem Zusammenhang neben der Forderung nach einer expliziten Abfragegrundlage in den jeweiligen Fachgesetzen der Bedarfsträger klargestellt, dass eine Abfrage ausschließlich unter den Voraussetzungen zulässig ist, die an die spätere Nutzung der Daten geknüpft werden (BVerfG, Beschluss vom 24.01.2012 – 1 BVR 1299/05, Rn. 184 f.). Inwieweit für die spätere Nutzung der Daten nach § 113 Abs. 1 S. 2 TKG-E tatsächlich eine richterliche Genehmigung erforderlich ist, ist mangels entsprechender Statistiken nicht bekannt. Sollte jedoch ein überwiegender Teil der abgefragten Daten nur unter Richtervorbehalt verwendet werden, wäre es konsequent, auch die vorangehende Abfrage unter einen generellen Richtervorbehalt zu stellen. Hierdurch würde in jedem Fall die Rechtssicherheit erhöht, da im gegenwärtigen Gesetzentwurf abgesehen von der Existenz einer gesetzlichen Abfragegrundlage kein formeller Anknüpfungspunkt für die Provider besteht, an dem die Rechtmäßigkeit des Auskunftsbegehrens gemessen werden könnte.

Elektronische Schnittstelle

Die Einführung der obligatorischen elektronischen Schnittstelle in § 113 Abs. 5 TKG-E begrüße ich unter den im Gesetzentwurf festgelegten Voraussetzungen. Diese Beurteilung wäre lediglich dann zu revidieren, wenn durch Wegfall der manuellen Kontrolle ein quasi-automatisches Auskunftsverfahren i.S.d. § 112 TKG entstehen würde. Solange aber die in § 113 Abs. 5 S. 3 TKG-E geforderte manuelle Prüfung und Freigabe jedes über die Schnittstelle eingegangenen Auskunftsersuchens gewährleistet ist, trägt die Schnittstelle als ein sicheres Übertragungsverfahren zur Erhöhung des Datenschutzniveaus bei Auskunftsersuchen bei. Um eine möglichst umfangreiche Nutzung dieses sicheren Übertragungswegs zu erreichen, plädiere ich dafür, die Verwendung der Schnittstelle nicht nur für die Telekommunikationsanbieter, sondern gleichermaßen auch für die abfragenden Bedarfsträger verpflichtend zu gestalten.

Mit freundlichen Grüßen