Betreff: Stellungnahme zum öffentlichen Anhörung zum Telekommunikationsgesetz
Von: Patrick Breyer <P.Breyer@vorratsdatenspeicherung.de>
Datum: 12.03.2013 08:26
An: innenausschuss@bundestag.de
Kopie (CC): Arbeitskreis Vorratsdatenspeicherung <kontakt@vorratsdatenspeicherung.de>, kattascha <kattascha@toxisch.net>

Sehr geehrte Damen und Herren,

bezüglich der öffentlichen Anhörung des Innenausschusses zum Entwurf eines Gesetzes zur Änderung des Telekommunikationsgesetzes und zur Neuregelung der Bestandsdatenauskunft (BT-Drucksache 17/12034) darf ich Ihnen in der Anlage die Stellungnahme des Arbeitskreises Vorratsdatenspeicherung übersenden. Ich bitte darum, diese wie die übrigen Stellungnahmen zu verumdrucken, zu verteilen und zu veröffentlichen.

Mit freundlichem Gruß,
Patrick Breyer
Arbeitskreis Vorratsdatenspeicherung
--
Unser PGP-Schlüssel/our PGP key:
http://www.vorratsdatenspeicherung.de/images/akvorrat.asc
Nicht rückverfolgbar antworten/untraceable reply:
http://www.vorratsdatenspeicherung.de/content/view/70/82/lang,de/

Anhänge:

AK-Vorrat_Bestandsdaten-StN.pdf 27 Bytes

Stellungnahme des Arbeitskreises Vorratsdatenspeicherung zum Regierungsentwurf eines Gesetzes zur Änderung des Telekommunikationsgesetzes und zur Neuregelung der Bestandsdatenauskunft (BT-Drs. 17/12034)

Zusammenfassung

Der Regierungsentwurf eines Gesetzes zur Änderung des Telekommunikationsgesetzes und zur Neuregelung der Bestandsdatenauskunft geht deutlich über die bisherige Rechtslage hinaus und baut Schutzvorschriften ab:

1. Künftig soll der Zugriff auf Kommunikationsdaten nicht mehr auf Einzelfälle beschränkt sein.
2. Es soll eine elektronische Schnittstelle zur vereinfachten Abfrage von Kommunikationsdaten eingeführt werden.
3. Die Bekanntgabe von Zugriffscodes wie PINs und Passwörter an Unbefugte soll künftig nicht mehr mit Bußgeld bedroht sein.
4. Bundeskriminalamt und Zollkriminalamt sollen in weitem Umfang Zugriff auf Kommunikationsdaten erhalten, wo Eingriffe in das Fernmeldegeheimnis bisher nicht gestattet sind (z.B. als Zentralstelle, zum Personenschutz).

In mehreren Punkten halten wir den Gesetzentwurf für verfassungswidrig:

1. Es fehlt bereits die verfassungsrechtlich gebotene abschließende Bestimmung, welche Vorschriften einen Zugriff auf Kommunikationsdaten erlauben sollen (einfachgesetzliches Zitiergebot).
2. Es fehlt die verfassungsrechtlich geforderte Beschränkung des Datenzugriffs auf Einzelfälle.
3. Entgegen den Vorgaben des Bundesverfassungsgerichts sollen Zugriffe auf Kommunikationsdaten durch Polizeibehörden nicht beschränkt werden auf Fälle konkreter Gefahr oder des Verdachts einer Ordnungswidrigkeit oder Straftat. Entgegen den Vorgaben des Bundesverfassungsgerichts soll die Identifizierung von Internetnutzern selbst zur Ermittlung geringfügiger Ordnungswidrigkeiten zugelassen werden.
4. Entgegen den Vorgaben des Bundesverfassungsgerichts soll die Identifizierung von Internetnutzern durch Geheimdienste keine tatsächlichen Anhaltspunkte für das Vorliegen einer konkreten Gefahr voraussetzen.
5. Es ist unklar und nicht kontrollierbar, unter welchen Voraussetzungen Anbieter Zugriffscodes wie Mailbox-PINs oder E-Mail-Passwörter an Staatsbehörden herausgeben dürfen.

6. Es fehlt die verfassungsrechtlich gebotene Benachrichtigung von Internetnutzern, deren Identität ermittelt worden ist. Der Bund will Anbietern sogar verbieten, ihre Kunden freiwillig zu benachrichtigen, selbst wo die Länder Stillschweigen nicht anordnen (z.B. bei Suizidgefahr oder Vermissten).
7. Den Datenzugriff durch eine elektronische Schnittstelle weiter zu erleichtern, ist unverhältnismäßig und verfassungswidrig.

Unsere Position ist: Der Staat darf auf Kommunikationsdaten allenfalls mit richterlicher Anordnung und zur Aufklärung schwerer Straftaten oder zur Abwehr von Gefahren für wichtige Rechtsgüter zugreifen. Einen Zugriff durch Geheimdienste lehnen wir in jedem Fall ab, ebenso wie die Herausgabe von Zugriffscodes wie PINs und Passwörtern.

Bedeutung von Bestandsdaten

Der Schutz der Vertraulichkeit von Bestandsdaten ist von hoher Bedeutung, weil durch Identifizierung eines Telefon- oder Internetnutzers die Anonymität der Telekommunikation durchbrochen wird. Durch Identifizierung von Telefon- oder Internetkennungen lassen sich mittelbar Umstände und Inhalt von Telekommunikationsvorgängen individualisieren, wie etwa dann, wenn Inhalt oder Zeitpunkt eines bestimmten Anrufs, der unter der abgefragten Nummer geführt wurde, der Behörde durch Vorermittlungen bekannt ist (BVerfG, 1 BvR 1299/05 vom 24.1.2012, Absatz-Nr. 114). Als Daten, die die Grundlagen von Telekommunikationsvorgängen betreffen, liegen Bestandsdaten im Umfeld verfassungsrechtlich besonders geschützter Informationsbeziehungen, deren Vertraulichkeit für eine freiheitliche Ordnung essentiell ist (BVerfG, 1 BvR 1299/05 vom 24.1.2012, Absatz-Nr. 137).

Die Furcht vor Ermittlungen oder sonstigen Nachteilen infolge von Telekommunikation beeinträchtigt die unbefangene Nutzung von Telefon und Internet, die in bestimmten Bereichen nur im Schutz der Anonymität in Anspruch genommen werden (z.B. medizinische, psychologische oder juristische Beratung, Presseinformanten und Whistleblower, politischer Aktivismus). Deswegen fordern wir, den staatlichen Zugriff auf Telekommunikationsdaten allenfalls in Ausnahmefällen zuzulassen. Der Bedeutung von Kommunikationsdaten als Grundlage und Voraussetzung eines Telekommunikationsverhältnisses wird es nicht gerecht, dass gerade diese besonders sensiblen und besonders geschützten Informationen unter geringeren Voraussetzungen zugänglich sein sollen als beliebige sonstige Kundendaten, die nur mit richterlicher Anordnung beschlagnahmt werden dürfen.

Zuständigkeit, Zustandekommen

Wir kritisieren, dass das Bundesinnenministerium diesen Gesetzentwurf vorgelegt hat, obwohl er in großen Teilen in die Zuständigkeit von Bundeswirtschafts- und Bundesjustizministerium fällt. Dementsprechend freiheitsfeindlich ist der Gesetzentwurf ausgefallen. Unabhängige Bürgerrechts- und Datenschutzorganisationen und auch die Beschwerdeführer, die das bestehende Gesetz zu Fall gebracht hatten, sind in die Anhörung nicht einbezogen worden.

Fehlende Beschränkung auf Einzelfälle

Im Gesetzentwurf fehlt die im geltenden § 113 TKG enthaltene Bestimmung, dass Auskünfte über Telekommunikationsdaten nur „im Einzelfall“ erteilt werden dürfen und nicht routinemäßig oder massenhaft. Da die Beschränkung auf Einzelfälle fehlt, andererseits aber die ausufernd weiten Auskunftsrechte unverändert beibehalten werden sollen, ist das Verhältnismäßigkeitsgebot verletzt und die Neufassung verfassungswidrig.

Das Bundesverfassungsgericht hat § 113 TKG ausdrücklich nur deswegen als „verfassungsrechtlich noch hinnehmbar“ angesehen, weil „Auskünfte nach § 113 Abs. 1 Satz 1 TKG im Einzelfall angefordert werden und erforderlich sein müssen“ (BVerfG, 1 BvR 1299/05 vom 24.1.2012, Absatz-Nr. 177). Es hat die „Erfordernis der Erforderlichkeit auch im Einzelfall“ als Anforderung des Verhältnismäßigkeitsgrundsatzes eingeordnet (BVerfG, 1 BvR 1299/05 vom 24.1.2012, Absatz-Nr. 163). Weil dem Gesetzentwurf die Beschränkung von Auskünften auf Einzelfälle fehlt, ist er verfassungswidrig.

Ausufernde Identifizierung von Internetnutzern

Die Identifizierung von Internetnutzern stellt einen besondern schwerwiegenden Grundrechtseingriff dar, weil sie die personenbezogene Nachverfolgung des Inhalts der abgerufenen oder geschriebenen Texte und Daten im Internet erlaubt. Anders als Auskünfte über Rufnummerninhaber geht die Identifizierung von Internetnutzern mit einem Eingriff in das grundrechtlich besonders geschützte Fernmeldegeheimnis einher.

Die Begründung von behördlichen Auskunftsansprüchen ermöglicht es in Verbindung mit der Speicherung der Internetzugangsdaten nach § 100 TKG in weitem Umfang, die Identität von Internetnutzern zu ermitteln. Auch ist die mögliche Persönlichkeitsrelevanz einer Abfrage des Inhabers einer IP-Adresse eine andere als die des Inhabers einer Telefonnummer: Schon vom Umfang der Kontakte her, die jeweils durch das Aufrufen von Internetseiten neu hergestellt werden, ist sie aussagekräftiger als eine Telefonnummernabfrage. Auch hat die Kenntnis einer Kontaktaufnahme mit einer Internetseite eine andere inhaltliche Bedeutung: Da der Inhalt von Internetseiten anders als das beim Telefongespräch gesprochene Wort elektronisch fixiert und länger wieder aufrufbar ist, lässt sich mit ihr vielfach verlässlich rekonstruieren, mit welchem Gegenstand sich der Kommunizierende auseinander gesetzt hat. Die Individualisierung der IP-Adresse als der „Telefonnummer des Internet“ gibt damit zugleich Auskunft über den Inhalt der Kommunikation. Die für das Telefongespräch geltende Unterscheidung von äußerlichen Verbindungsdaten und Gesprächsinhalten löst sich hier auf. Wird der Besucher einer bestimmten Internetseite mittels der Auskunft über eine IP-Adresse individualisiert, weiß man nicht nur, mit wem er Kontakt hatte, sondern kennt in der Regel auch den Inhalt des Kontakts (BVerfG, 1 BvR 256/08 vom 2.3.2010, Absatz-Nr. 259).

Die Identifizierung von dynamischen IP-Adressen ermöglicht in weitem Umfang eine Deanonymisierung von Kommunikationsvorgängen im Internet. Zwar hat sie eine gewisse Ähnlichkeit mit der Identifizierung einer Telefonnummer. Schon vom Umfang, vor allem aber vom Inhalt der Kontakte her, über die sie Auskunft geben kann, hat sie jedoch eine erheblich größere Persönlichkeitsrelevanz und kann mit ihr - so das Bundesverfassungsgericht ausdrücklich - nicht gleichgesetzt werden (BVerfG, 1 BvR 1299/05 vom 24.1.2012, Absatz-Nr. 174).

Eben dies tut aber der Gesetzentwurf. Die Identifizierung von Internetnutzern im selben weit reichenden Umfang zuzulassen wie Auskünfte über Rufnummerninhaber ist nicht hinnehmbar. Wir fordern, dass zumindest eine Gleichstellung mit der Verwendung sonstiger Verkehrsdaten (§ 100g StPO) erfolgt, also im Bereich der Strafverfolgung eine richterliche Anordnung zur Voraussetzung gemacht wird und eine Beschränkung auf Straftaten von erheblichem Gewicht sowie auf Gefahren für wichtige Rechtsgüter erfolgt. Die aktuelle Privilegierung einer Internet-Zielwahlsuche anhand von IP-Adressen gegenüber einer Telefon-Zielwahlsuche (§ 100g StPO) ist sachlich nicht zu rechtfertigen. Es ist nicht plausibel zu machen, weshalb unbedeutende Verkehrsdaten zu schon bekannten Verbindungen (z.B. Datenvolumen, genaue Anrufdauer) einen besseren Schutz genießen sollen als die äußerst grundrechtsbedeutsame Identität eines noch unbekannten Internetnutzers.

Unklarer und unkontrollierter Zugriff auf Zugangssicherungscodes (PINs, Passwörter)

Zugangssicherungscodes (wie Passwörter, PIN oder PUK) sichern den Zugang zu Endgeräten und Speicherungseinrichtungen und damit die Betreffenden vor einem Zugriff auf die entsprechenden Daten beziehungsweise Telekommunikationsvorgänge. Das Bundesverfassungsgericht hat entschieden, dass Staatsbehörden PINs und Passwörter nur anfordern dürfen, wenn die gesetzlichen Voraussetzungen für ihre Nutzung gegeben sind. Diese Formulierung soll nun unverändert in das Gesetz aufgenommen werden.

Rechtspolitisch lehnen wir die Herausgabe von PINs und Passwörtern zur Ermöglichung einer Telekommunikationsüberwachung ab. Anders als im Fall einer Telekommunikationsüberwachung hat der Anbieter nach Herausgabe von Zugangssicherungscodes keine Kontrolle über die Telekommunikationsüberwachung mehr.

Verfassungsrechtlich verletzt die lapidare Bezugnahme auf „die gesetzlichen Voraussetzungen für die Nutzung der Daten“ das Bestimmtheitsgebot. Sie ermöglicht weder der handelnden Behörde, noch dem verpflichteten Anbieter oder dem kontrollierenden Gericht, mit hinreichender Klarheit zu bestimmen, welche Voraussetzungen vorliegen müssen. Auch ist nicht gewährleistet, dass der Anbieter das Vorliegen der Zugriffsvoraussetzungen (z.B. richterliche Anordnung der Telekommunikationsüberwachung) anhand behördlich zur Verfügung gestellter Unterlagen kontrollieren kann. Wenn eine Behörde einen Zugriffscode anfordert, weiß der Anbieter nicht, ob dies zum Zweck der Telekommunikationsüberwachung oder zur Auswertung abgeschlossener Telekommunikation geschieht. Es ist nicht akzeptabel, die Kontrolle der gesetzlichen Voraussetzungen durch den Telekommunikationsanbieter bei der Anforderung von Zugriffscodes quasi ausfallen zu lassen, obwohl solche Codes besonders weitreichende und unkontrollierte Zugriffe ermöglichen.

Es ist aus diesen Gründen verfassungsrechtlich geboten, die Erhebung von Zugangssicherungscodes in denjenigen Vorschriften zu regeln, die auch deren Nutzung regeln, also z.B. in den §§ 98, 100a und 100b StPO.

Mangelnder Rechtsschutz wegen fehlender Benachrichtigung

Der Gesetzentwurf sieht keine Benachrichtigung der Betroffenen von Zugriffen auf ihre Daten vor. Da eine Benachrichtigung Voraussetzung eines effektiven Rechtsschutzes gegen Grundrechtsverletzungen ist, ist aus Art. 19 Abs. 4 GG eine Benachrichtigungspflicht abzuleiten. Dies gilt insbesondere dann, wenn in das Fernmeldegeheimnis eingegriffen worden ist (IP-Zuordnung) und wenn Zugangssicherungscodes erhoben worden sind. Gerade im Fall der Zugangssicherungscodes haben Betroffene ein hohes Interesse an einer Benachrichtigung, um den Code nach Beendigung des Verfahrens ändern und dadurch rechtswidrigen Zugriffen vorbeugen zu können. Eine anderweitige Benachrichtigung erfolgt bei Drittbetroffenen (z.B. mutmaßlichen Nachrichtenmittlern) nicht, so dass eine besondere Benachrichtigungspflicht aufgenommen werden muss.

Verfassungsrechtlich geboten ist es außerdem, Benachrichtigungspflichten gegenüber identifizierten Internetnutzern vorzusehen, soweit und sobald hierdurch der Zweck der Auskunft nicht vereitelt wird oder sonst überwiegende Interessen Dritter oder des Betroffenen selbst nicht entgegenstehen (BVerfG, 1 BvR 256/08 vom 2.3.2010, Absatz-Nr. 263). Soweit von einer Benachrichtigung nach Maßgabe entsprechender gesetzlicher Regelungen ausnahmsweise abgesehen wird, ist anzuordnen, den Grund hierfür aktenkundig zu machen (a.a.O.). Die Artikel. 2 ff. des vorliegenden Gesetzentwurfs sind verfassungswidrig, weil sie die Identifizierung von Internetnutzern erlauben, ohne eine Benachrichtigung oder Aktennotiz vorzusehen.

Das Urteil des Bundesverfassungsgerichts vom 2.3.2010 ist ungeachtet dessen einschlägig, dass die dortigen Ausführungen zu § 113 TKG im Zusammenhang mit der mittelbaren Nutzung anlasslos und flächendeckend erhobener Verkehrsdaten erfolgt sind. Auf diesen Umstand hat das Bundesverfassungsgericht bei Darstellung der für § 113 TKG maßgeblichen verfassungsrechtlichen Eingriffsgrenzen nicht abgestellt. Es hat umgekehrt Literatur zitiert, welche die Beauskunftung nicht auf Vorrat gespeicherter Daten behandelt (BVerfG, 1 BvR 256/08 vom 2.3.2010, Absatz-Nr. 261). Auch bei der Bestimmung der Eingriffstiefe hat das Gericht auf die Verwendungsmöglichkeiten der Daten abgestellt und nicht darauf, wie sie erhoben worden sind (BVerfG, 1 BvR 256/08 vom 2.3.2010, Absatz-Nr. 258 f.).

Mangelnde Kontrolle durch fehlende Statistik

Der Quick-Freeze-Referentenentwurf des Bundesjustizministeriums sah vor, dass eine Statistik über die Identifizierung von Internetnutzern geführt wird, damit der Gesetzgeber die Entwicklung der Fallzahlen beobachten kann (§ 100k Abs. 4 StPO-RefE). Im vorliegenden Gesetzentwurf fehlt jede statistische Erfassung, obwohl der Datenzugriff erheblich ausgeweitet werden soll. Wir fordern, dass eine Statistik über sämtliche Bestandsdatenzugriffe geführt und veröffentlicht wird, in die auch Erfolg oder Misserfolg der Maßnahmen aufzunehmen ist.

Zu § 113 TKG

Abs. 1 S. 4: Fehlende Beschränkung auf rechtmäßig gespeicherte Daten

Wenn Abs. 1 S. 4 die Heranziehung „sämtlicher unternehmensinterner Datenquellen“ fordert, sind davon dem Wortlaut nach auch rechtswidrig erhobene oder gespeicherte Daten erfasst. Erforderlich wäre die Klarstellung, dass Auskunft nur anhand rechtmäßig gespeicherter Daten erteilt werden darf. Speichert der Anbieter Daten rechtswidrig, darf er sie erst recht nicht weiter verarbeiten. Den Zugriff auch auf Daten zu gestatten, die gar nicht gespeichert sein dürften, ist - zumal im Bereich von Ordnungswidrigkeiten und sonstigen Bagatellen - unverhältnismäßig.

Abs. 3 und 4: Mangelnde Bundeskompetenz

Laut Bundesverfassungsgericht kann der Bund auf der Grundlage des Art. 73 Abs. 1 Nr. 7 GG eine Verpflichtung privater Telekommunikationsunternehmen, einem Auskunftsbegehren Folge zu leisten, nicht abschließend begründen (BVerfG, 1 BvR 1299/05 vom 24.1.2012, Absatz-Nr. 167). Dies gehöre nicht mehr zur Bestimmung der Grenzen des Datenschutzes, sondern sei untrennbarer Bestandteil des Datenabrufs. Der Bund könne auf der Grundlage des Art. 73 Abs. 1 Nr. 7 GG nur die Öffnung der Datenbestände für die staatliche Aufgabenwahrnehmung regeln, nicht aber auch den Zugriff auf diese Daten selbst.

In welcher Form, in welchem Zeitrahmen und Umfang Auskünfte zu erteilen sind („unverzüglich und vollständig“) und ob der Anbieter seine Kunden informieren darf, betrifft nicht lediglich die „Öffnung der Datenbestände“. Deswegen ist der Bund für § 113 Abs. 3 und 4 unzuständig.

Abs. 5: Unverhältnismäßige Abrufschnittstelle

Das Bundesverfassungsgericht hat die „sehr weit“ reichende staatliche Einsicht in Telekommunikationsdaten über § 113 TKG nur deswegen als „verfassungsrechtlich noch hinnehmbar“ bezeichnet, weil „im Vergleich zu § 112 TKG [...] ein manuelles Auskunftsverfahren für die abfragende Behörde einen gewissen Verfahrensaufwand mit sich bringt, der dazu beitragen dürfte, dass die Behörde die Auskunft nur bei hinreichendem Bedarf einholt.“ (BVerfG, 1 BvR 1299/05 vom 24.1.2012, Absatz-Nr. 178 und 180) Wenn über eine elektronische Schnittstelle der Behördenaufwand nun auf das Maß des automatisierten Abrufverfahrens nach § 112 TKG reduziert wird, gleichwohl aber die ausufernde Weite der Zugriffsbefugnisse beibehalten und sogar weiter ausgedehnt wird, ist das Gebot der Verhältnismäßigkeit verletzt und die Vorschrift verfassungswidrig. Dass im Vergleich zu § 112 TKG die Auskunft nach § 113 TKG zeitlich verzögert erteilt würde, ist für den Behördenaufwand nicht entscheidend.

Fehlender Schutz von Zugriffscodes

§ 113 Abs. 1 S. 2 Hs. 2 TKG verbietet bisher unter Bußgeldandrohung, Zugriffscodes wie PINs und Passwörter zu E-Mail-Postfächern an andere als die gesetzlich autorisierten öffentlichen Stellen oder gar an nicht-öffentliche Stellen zu übermitteln. Dieser besondere Schutz von Zugriffscodes soll künftig entfallen, was der Sensibilität dieser Codes nicht gerecht wird, die z.B. ein Abhören von Mailboxen oder ein Mitlesen von E-Mails ermöglichen. Wir fordern, Übermittlungsverbot und Bußgeldandrohung beizubehalten.

Fehlender Schutz des Fernmeldegeheimnisses

§ 113 TKG stellt bislang klar: „Ein Zugriff auf Daten, die dem Fernmeldegeheimnis unterliegen, ist nur unter den Voraussetzungen der hierfür einschlägigen gesetzlichen Vorschriften zulässig.“ Diese Klarstellung soll künftig entfallen. Dies birgt die Gefahr, dass Bestandsdatenauskünfte unter Verwendung von Verkehrsdaten verlangt werden (z.B. wer zum Zeitpunkt X den Anschluss Y angerufen hat), was verfassungswidrig wäre. Wir fordern, in alle Zugriffsnormen eine § 113 Abs. 1 S. 3 TKG entsprechende Vorschrift aufzunehmen.

Fehlendes Zitiergebot

Das Bundesverfassungsgericht hat festgestellt, dass für die Datenabfrage in Form eines unmittelbar an private Dritte gerichteten Auskunftsverlangens spezifische Rechtsgrundlagen erforderlich sind, die eine Auskunftsverpflichtung der Telekommunikationsunternehmen eigenständig begründen, während allgemeine Datenerhebungsbefugnisse nicht genügen (BVerfG, 1 BvR 1299/05 vom 24.1.2012, Absatz-Nr. 168). § 113 TKG-E fordert indes nur eine gesetzliche Bestimmung, die „eine Erhebung der in Absatz 1 in Bezug genommenen Daten erlaubt“. Ihrem Wortlaut nach erlauben die allgemeinen Datenerhebungsbefugnisse die Erhebung sämtlicher personenbezogener Daten, auch von Bestandsdaten. Verfehlt wird auch die Forderung des Bundesverfassungsgerichts, es bedürfe „klarer Bestimmungen, gegenüber welchen Behörden die Anbieter konkret zur Datenübermittlung verpflichtet sein sollen“ (BVerfG, 1 BvR 1299/05 vom 24.1.2012, Absatz-Nr. 171).

Deswegen fordern wir die Einführung eines einfachgesetzlichen Zitiergebots. § 113 TKG-E darf die Erteilung von Auskünften nur auf der Grundlage von Gesetzen erlauben, die dies unter ausdrücklicher Bezugnahme auf § 113 TKG vorsehen. Nur durch ein Zitiergebot können die Anbieter zuverlässig erkennen, ob eine Norm „eine Erhebung der in Absatz 1 in Bezug genommenen Daten erlaubt“.

Zum BKA-Gesetz

§ 7 BKAG-E: Kommunikationsdatenerhebung als Zentralstelle

Anders als bisher soll das Bundeskriminalamt Telefon- und Internetnutzer künftig auch ohne Ersuchen der zuständigen Polizeibehörde identifizieren dürfen. Erstmals soll das Bundeskriminalamt als Zentralstelle sogar in das Fernmeldegeheimnis eingreifen dürfen (§ 7 Abs. 4 BKAG-E). Aus den folgenden Gründen lehnen wir dies ab:

Die Erhebung von Telekommunikationsdaten hat mit der Aufgabe des BKA als Zentralstelle nichts zu tun. Bestandsdaten betreffen weder das polizeiliche Auskunfts- und Nachrichtenwesen, noch die Verhütung und Verfolgung von Straftaten mit länderübergreifender, internationaler oder erheblicher Bedeutung. § 7 BKAG verpflichtet bislang keine privaten Datenverarbeiter zur Auskunft an das Bundeskriminalamt. Es ist vollkommen unangemessen, gerade im Fall der besonders sensiblen Telekommunikationsdaten eine Auskunftspflicht zu begründen. Soweit die Begründung des Gesetzentwurfs auf ungeklärte Zuständigkeiten verweist, rechtfertigt es dieses allgemeine Problem nicht, das Bundeskriminalamt zur Internet-Zentralpolizei zu machen. Das BKA-Gesetz sieht - entgegen der Entwurfsbegründung - keine Zuständigkeit des BKA für die Ermittlung der zuständigen Strafverfolgungsbehörde vor. Das BKA-Gesetz sieht auch keine allgemeine Eilzuständigkeit des BKA in Fällen der Gefahrenabwehr vor. Das BKA mag entsprechende Fälle an die Polizei an seinem Sitz oder am Sitz des zuständigen Providers abgeben.

§ 7 Abs. 3 S. 2 BKAG-E, welcher dem BKA als Zentralstelle den Zugang zu PINs und Passwörtern eröffnen soll, dürfte überdies ohne Anwendungsbereich sein. Denn die dort genannten „gesetzlichen Voraussetzungen für die Nutzung der Daten“ dürften das BKA in seiner Funktion als Zentralstelle nicht erfassen. Namentlich darf das BKA als Zentralstelle keine Datenträger sicherstellen, wie es Voraussetzung eines Zugriffs z.B. auf in einem Mobiltelefon gespeicherte Daten wäre.

§ 7 Abs. 3 und 4 BKAG-E sind überdies ihrer Ausgestaltung nach verfassungswidrig. Nach der Rechtsprechung des Bundesverfassungsgerichts ist im Bereich der Gefahrenabwehr eine konkrete Gefahr, im Bereich der Strafverfolgung der Verdacht einer Straftat (Anfangsverdacht) Voraussetzung einer verhältnismäßigen staatlichen Bestandsdatenerhebung (BVerfG, 1 BvR 1299/05 vom 24.1.2012, Absatz-Nr. 177). § 7 BKAG-E bestimmt aber weder selbst noch durch normenklare Verweisung, dass das BKA als Zentralstelle Bestandsdaten nur zur Abwehr einer Gefahr oder zur Aufklärung eines Tatverdachts erheben darf.

§ 20b BKAG-E: Kommunikationsdatenerhebung zur Abwehr von Gefahren des internationalen Terrorismus

§ 20b Abs. 3 und 4 BKAG-E sind ihrer Ausgestaltung nach verfassungswidrig. Nach der Rechtsprechung des Bundesverfassungsgerichts ist im Bereich der Gefahrenabwehr eine konkrete Gefahr Voraussetzung einer verhältnismäßigen staatlichen Bestandsdatenerhebung (BVerfG, 1 BvR 1299/05 vom 24.1.2012, Absatz-Nr. 177). § 20b BKAG-E bestimmt aber weder selbst noch durch Verweisung normenklar, dass das BKA Bestandsdaten nur zur Abwehr einer konkreten Gefahr erheben darf.

§ 22 BKAG-E: Kommunikationsdatenerhebung zwecks Personenschutzes

Während das BKA Kommunikationsdaten bisher nur zur Gefahrenabwehr erheben darf (§ 113 TKG), soll es Kommunikationsdaten künftig allgemein „für die Aufgabenwahrnehmung nach § 5 BKAG“ erhalten.

Wir lehnen es ab, dem BKA zum Personenschutz die Erhebung von Kommunikationsdaten einschließlich Eingriffen in das Fernmeldegeheimnis zu erlauben. Drohungen kann die zuständige Gefahrenabwehr- oder Strafverfolgungsbehörde nachgehen; dies ist nicht Gegenstand des Personenschutzes.

§ 22 Abs. 2 und 3 BKAG-E sind überdies ihrer Ausgestaltung nach verfassungswidrig. Nach der Rechtsprechung des Bundesverfassungsgerichts ist im Bereich der Gefahrenabwehr eine konkrete Gefahr Voraussetzung einer verhältnismäßigen staatlichen Bestandsdatenerhebung (BVerfG, 1 BvR 1299/05 vom 24.1.2012, Absatz-Nr. 177). § 22 BKAG-E bestimmt aber weder selbst noch durch Verweisung normenklar, dass das BKA zum Personenschutz Bestandsdaten nur zur Abwehr konkreter Gefahren erheben darf und nicht vorsorglich.

Zum Bundespolizeigesetz

Mit der Identifizierung von Internetnutzern sollen der Bundespolizei erstmals in ihrer Geschichte Eingriffe in das Fernmeldegeheimnis erlaubt werden. Dies lehnen wir ab, zumal die Gesetzesbegründung keinen einzigen Fall angibt, in dem eine solche Befugnis erforderlich gewesen wäre.

Insbesondere ist abzulehnen, dass Artikel 10 des Grundgesetzes künftig in § 70 BPolG allgemein eingeschränkt werden soll und nicht beschränkt auf § 22a BPolG-E. Diese Regelungstechnik birgt die Gefahr, dass auch anderen Normen Befugnisse zu Eingriffen in das Fernmeldegeheimnis entnommen werden könnten.

§ 22a BPolG-E: Kommunikationsdatenerhebung zur Aufgabenerfüllung und Verhütung von Straftaten

Während die Bundespolizei Kommunikationsdaten bisher nur zur Gefahrenabwehr erheben darf (§ 113 TKG), soll sie Kommunikationsdaten künftig allgemein „nach Maßgabe von § 21 Absatz 1 und Absatz 2“ BPolG erhalten. Nach der Rechtsprechung des Bundesverfassungsgerichts ist im Bereich der Gefahrenabwehr eine konkrete Gefahr Voraussetzung einer verhältnismäßigen staatlichen Bestandsdatenerhebung (BVerfG, 1 BvR 1299/05 vom 24.1.2012, Absatz-Nr. 177). § 22a BPolG-E bestimmt aber weder selbst noch durch Verweisung normenklar, dass die Bundespolizei Kommunikationsdaten nur zur Abwehr einer konkreten Gefahr erheben darf. Damit verletzt die Norm das Verhältnismäßigkeitsgebot.

Zum Zollfahndungsdienstgesetz

§ 7 ZFdG-E: Kommunikationsdatenerhebung als Zentralstelle

Anders als bisher soll das ZKA Telefon- und Internetnutzer künftig auch ohne Ersuchen der zuständigen Behörde identifizieren dürfen. Erstmals soll das ZKA als Zentralstelle sogar in das Fernmeldegeheimnis eingreifen dürfen (§ 7 Abs. 5 ZFdG-E). Aus den folgenden Gründen lehnen wir dies ab:

Die Erhebung von Telekommunikationsdaten hat mit der Aufgabe des ZKA als Zentralstelle nichts zu tun. § 7 ZFdG verpflichtet bislang keine privaten Datenverarbeiter zur Auskunft gegenüber dem ZKA als Zentralstelle. Es ist vollkommen unangemessen, gerade im Fall der besonders sensiblen Telekommunikationsdaten eine Auskunftspflicht zu begründen.

§ 7 Abs. 5 S. 2 ZFdG-E, welcher dem ZKA als Zentralstelle den Zugang zu PINs und Passwörtern eröffnen soll, dürfte überdies ohne Anwendungsbereich sein. Denn die dort genannten „gesetzlichen Voraussetzungen für die Nutzung der Daten“ dürften den Dienst in seiner Funktion als Zentralstelle nicht erfassen. Namentlich darf das ZKA als Zentralstelle keine Datenträger sicherstellen, wie es Voraussetzung eines Zugriffs z.B. auf in einem Mobiltelefon gespeicherte Daten wäre.

§ 7 Abs. 5 und 6 ZFdG-E sind überdies ihrer Ausgestaltung nach verfassungswidrig. Nach der Rechtsprechung des Bundesverfassungsgerichts ist im Bereich der Gefahrenabwehr eine konkrete Gefahr, im Bereich der Strafverfolgung der Verdacht einer Straftat (Anfangsverdacht) Voraussetzung einer verhältnismäßigen staatlichen Bestandsdatenerhebung (BVerfG, 1 BvR 1299/05 vom 24.1.2012, Absatz-Nr. 177). § 7 Abs. 5 und 6 ZFdG-E bestimmen aber weder selbst noch durch normenklare Verweisung, dass das ZKA als Zentralstelle Bestandsdaten nur zur Abwehr einer Gefahr oder zur Aufklärung eines Tatverdachts erheben darf.

§ 15 ZFdG-E: Kommunikationsdatenerhebung zur Erfüllung eigener Aufgaben

§ 15 Abs. 2 und 3 ZFdG-E sind ihrer Ausgestaltung nach verfassungswidrig. Nach der Rechtsprechung des Bundesverfassungsgerichts ist im Bereich der Gefahrenabwehr eine konkrete Gefahr, im Bereich der Strafverfolgung der Verdacht einer Straftat (Anfangsverdacht) Voraussetzung einer verhältnismäßigen staatlichen Bestandsdatenerhebung (BVerfG, 1 BvR 1299/05 vom 24.1.2012, Absatz-Nr. 177). § 15 Abs. 2 und 3 ZFdG-E bestimmen aber weder selbst noch durch normenklare Verweisung, dass das ZKA als Zentralstelle Bestandsdaten nur zur Abwehr einer Gefahr oder zur Aufklärung eines Tatverdachts erheben darf.

Zu den Geheimdiensten

Den Nachrichtendiensten die Identifizierung von Telefon- und Internetnutzern sowie die Erhebung von PINs und Passwörtern zu erlauben, lehnen wir wegen deren mangelnden Kontrollierbarkeit ab.

Die Zugriffsbefugnisse auf die Identität von Internetnutzern sind überdies ihrer Ausgestaltung nach verfassungswidrig. Nach der Rechtsprechung des Bundesverfassungsgerichts darf Nachrichtendiensten die Identifizierung von Internetnutzern nur erlaubt werden, wenn aufgrund tatsächlicher Anhaltspunkte von dem Vorliegen einer konkreten Gefahr auszugehen ist. Die rechtlichen und tatsächlichen Grundlagen entsprechender Auskunftsbegehren sind aktenkundig zu machen (BVerfG, 1 BvR 256/08 vom 2.3.2010, Absatz-Nr. 261). Die Artikel 6-8 des Gesetzentwurfs bestimmen weder selbst noch durch normenklare Verweisung, dass die Nachrichtendienste Bestandsdaten nur erheben dürfen, wenn aufgrund tatsächlicher Anhaltspunkte von dem Vorliegen einer konkreten Gefahr auszugehen ist.

Weiterer Handlungsbedarf

Ordnungswidrigkeiten

Der Gesetzentwurf soll über § 46 OWiG i.V.m. § 100j StPO-E die Identifizierung von Internetnutzern zur Verfolgung von Ordnungswidrigkeiten jeder Art ermöglichen. Das erhebliche Gewicht des Eingriffs solcher Auskünfte erlaubt es indessen nach der Rechtsprechung des Bundesverfassungsgerichts nicht, diese allgemein und uneingeschränkt auch zur Verfolgung jedweder Ordnungswidrigkeiten zuzulassen. Die Aufhebung der Anonymität im Internet bedarf zumindest einer Rechtsgutbeeinträchtigung, der von der Rechtsordnung auch sonst ein hervorgehobenes Gewicht beigemessen wird. Dies schließt entsprechende Auskünfte zur Verfolgung oder Verhinderung von Ordnungswidrigkeiten nicht vollständig aus. Es muss sich insoweit aber um - auch im Einzelfall - besonders gewichtige Ordnungswidrigkeiten handeln, die der Gesetzgeber ausdrücklich benennen muss (BVerfG, 1 BvR 256/08 vom 2.3.2010, Absatz-Nr. 262). Der Gesetzentwurf versäumt dies und verfehlt folglich auch insoweit die verfassungsrechtlichen Anforderungen.

§ 111 TKG: Identifizierungszwang

Das Verbot anonymer Telekommunikation des § 111 TKG lehnen wir ab und fordern dessen Abschaffung. Der Identifizierungszwang ist nutzlos, weil Straftäter dennoch in aller Regel falsch registrierte oder ausländische anonyme Prepaidkarten nutzen. Bei dem Europäischen Gerichtshof für Menschenrechte ist eine Beschwerde gegen das Anonymitätsverbot des § 111 TKG anhängig, das in den meisten europäischen Staaten keine Entsprechung findet.

§ 112 TKG: Automatisiertes Abrufverfahren

Staatsbehörden in einem automatisierten Verfahren unmittelbaren Zugriff auf Kundendaten zu geben, lehnen wir ab, weil es zu einer Explosion der Zahl an Eingriffen in Telekommunikationsbeziehungen führt. Wir fordern, dass sich der Staat auf manuelle Auskunftsersuchen beschränkt, wie es auch in den meisten anderen europäischen Ländern der Fall ist.

22.11.2012

Arbeitskreis Vorratsdatenspeicherung

Der Arbeitskreis Vorratsdatenspeicherung (AK Vorrat) ist ein deutschlandweiter Zusammenschluss, der sich gegen die ausufernde Überwachung im Allgemeinen und gegen die Vollprotokollierung der Telekommunikation und anderer Verhaltensdaten im Besonderen einsetzt.

Homepage und Kontakt: http://www.vorratsdatenspeicherung.de