**LANDTAG NORDRHEIN-WESTFALEN**
16. Wahlperiode

Drucksache **16/1467**

20.11.2012

# Antrag

**der Fraktion der PIRATEN**

**Zum Schutz der Vertraulichkeit und Anonymität der Telekommunikation**

I. Allgemeines

Bestandsdaten sind die bei Telefon-, Mobiltelefon-, E-Mail- und Internetzugangsanbietern ständig gespeicherten Kundendaten wie Name, Anschrift, Geburtsdatum, Rufnummer, Kontoverbindung, PIN, Passwort und elektronisches Adressbuch. Als Angaben, 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).

Der Schutz der Vertraulichkeit von Bestandsdaten ist von hoher Bedeutung, weil durch Identifizierung eines Telefon- oder Internetnutzers anhand seiner Rufnummer oder IP-Adresse die Anonymität der Telekommunikation aufgehoben und die Zuordnung seiner Kommunikationsbeziehungen, seiner Bewegungen und seines Internet-Nutzungsverhaltens ermöglicht wird. 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).

Der Vertraulichkeit und Integrität der Kommunikation kommt essentielle Bedeutung in einer Demokratie zu. Der Zugriff auf derart sensible Daten sollte - wenn überhaupt - nur in Ausnahmefällen, im Einzelfall und unter Richtervorbehalt zulässig sein. Der Regierungsentwurf eines Gesetzes zur Änderung des Telekommunikationsgesetzes und zur Neuregelung der Bestandsdatenauskunft sieht derartige Kontrollinstanzen nicht vor.

Die vorgesehene Einrichtung einer Schnittstelle für Datenabfragen durch Verfassungsschutz, Bundeskriminalamt, Polizei, Zoll und den Militärischen Abschirmdienst stellt einen massiven Eingriff in die Grundrechte der Betroffenen dar. Derartige Schnittstellen in Kombination mit weitreichenden Eingriffsbefugnissen bereiten den Boden für eine systematische Ausdehnung der staatlichen Zugriffsbefugnisse weit über das grundrechtlich noch hinnehmbare Maß hinaus.

Datum des Originals: 20.11.2012/Ausgegeben: 20.11.2012

Zudem ist nicht vorgesehen, die Betroffenen über durchgeführte Abfragen zu informieren. Ohne Kenntnis getätigter Grundrechtseingriffe ist ein effektiver Rechtsschutz gegen illegitime Abfragen von Bestandsdaten nicht zu gewährleisten. Bei PINs und Passwörtern kommt erschwerend hinzu, dass Betroffene sich ohne Benachrichtigung nicht gegen zukünftige rechtswidrige Eingriffe schützen können: im Unwissen über die Weitergabe ihrer Passwörter sind sie nicht veranlasst, diese zu ändern.

Die Herausgabe von Zugangssicherungscodes an Behörden nimmt Anbieter und Betroffenem die Kontrolle über Art und Umfang der durchgeführten Überwachung. Durch PIN-Codes und Passwörter geschützte private Inhalte berühren den Kernbereich der privaten Lebensgestaltung. Daher stellt die Verpflichtung von Anbietern zur Herausgabe von Zugangssicherungscodes einen besonders schwerwiegenden Grundrechtseingriff dar.

Der Gesetzentwurf der Bundesregierung zur Änderung des Telekommunikationsgesetzes und zur Neuregelung der Bestandsdatenauskunft bedarf umfassender Änderungen, um die Vertraulichkeit der Telefon- und Internetnutzung angemessen zu gewährleisten. Der vorliegende Antrag orientiert sich an der Stellungnahme des Arbeitskreises Vorratsdatenspeicherung (http://wiki.vorratsdatenspeicherung.de/Bestandsdaten-StN), auf die wegen der näheren Einzelheiten Bezug genommen wird.

II. Zum Änderungsbedarf im Einzelnen

**Einführung eines Zitiergebots (im Beschluss Punkt 1.)**

Laut Bundesverfassungsgericht ist es nicht ausreichend, allgemeine Befugnisse zur Erhebung von Bestandsdaten zu nutzen. Es bedarf klarer Regelungen, welche Daten an welche Behörden weitergegeben werden dürfen bzw. müssen. Vor allem die Weitergabe der besonders schützenswerten Bestandsdaten muss dabei sorgfältig geregelt werden und darf nicht unter eine allgemeine Regelung für alle Daten subsumiert werden.

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 soll demgegenüber nur eine gesetzliche Bestimmung voraus setzen, die „eine Erhebung der in Absatz 1 in Bezug genommenen Daten erlaubt“. Ihrem Wortlaut nach erlauben bereits die allgemeinen Datenerhebungsbefugnisse die Erhebung sämtlicher personenbezogener Daten, auch von Bestandsdaten. Verfehlt wird mit § 113 TKG-E auch die Anforderung 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).

Aus diesen Gründen ist die Einführung eines einfachgesetzlichen Zitiergebots geboten. § 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 solches Zitiergebot können die Anbieter zuverlässig erkennen, ob eine Norm „eine Erhebung der in Absatz 1 in Bezug genommenen Daten erlaubt“ oder nicht.

**Voraussetzungen für die Auslieferung von Telekommunikations-Bestandsdaten (im Beschluss Punkt 2.)**

Um eine unbefangene Nutzung von Telekommunikationsvorgängen zu gewährleisten, deren Vertraulichkeit für eine freiheitliche Ordnung von essentieller Bedeutung ist, sind auch Bestandsdaten als verfassungsrechtlich besonders geschützte Informationen zu betrachten. Denn sie stellen die Grundlagen von Telekommunikations-vorgängen da, die verfassungsrechtlich besonders geschützt sind (Art. 10 GG). Sie sollten daher zumindest mit gleicher Sorgfalt behandelt und ebenso gut vor staatlichen Einblicken geschützt werden wie Verkehrsdaten. Dazu ist es notwendig, dass ein Eingriff in deren Vertraulichkeit nur nach sorgfältiger Prüfung zulässig ist. Solche Eingriffe dürfen deshalb im Regelfall nur nach richterlicher Prüfung zugelassen werden (Richtervorbehalt).

Besonders die Identifizierung von Internetnutzern mithilfe von Verkehrsdaten muss denselben Voraussetzungen unterworfen werden wie der sonstige Zugriff auf Verkehrsdaten. Die Identifizierung von 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 Um-fang, 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), wie es der Gesetzentwurf der Bundesregierung tut.

Da der Inhalt von Internetseiten anders als das beim Telefongespräch gesprochene Wort elektronisch fixiert und länger wieder aufrufbar ist, lässt sich mit einer Auskunft über den Inhaber einer IP-Adresse 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).

Der Gesetzgeber sieht für die Identifizierung von IP-Adressen selbst dort, wo dem Betroffenen nur zivilrechtliche Schritte drohen, einen Richtervorbehalt vor (§ 101 Abs. 9 UrhG). Erst recht muss dies gelten, wo dem Betroffenen infolge einer Daten-auskunft polizeiliche Zwangsmaßnahmen oder eine geheime nachrichtendienstliche Beobachtung und damit weit tiefer greifende Grundrechtseingriffe drohen.

Der Gesetzentwurf der Bundesregierung unterschreitet mehrfach selbst die geringen verfassungsrechtlich unabdingbaren Eingriffsschwellen. Nach der Rechtsprechung des Bundesverfassungsgerichts ist im Bereich der Gefahrenabwehr eine konkrete Gefahr, im Bereich der Strafverfolgung der Verdacht einer Straftat (Anfangsverdacht) Mindestvoraussetzung einer verhältnismäßigen staatlichen Bestandsdatenerhebung (BVerfG, 1 BvR 1299/05 vom 24.1.2012, Absatz-Nr. 177). Die §§ 7 BKAG-E, 20b Abs. 3 und 4 BKAG-E, 22 BKAG-E, 22a BPolG-E, 7 Abs. 5 und 6 ZFdG-E, 15 Abs. 2 und 3 ZFdG-E bestimmen aber weder selbst noch durch normenklare Verweisung, dass die Erhebung von Bestandsdaten nur zur Abwehr einer konkreten Gefahr oder zur Aufklärung eines Tatverdachts erfolgen darf. Den Nachrichtendiensten darf nach der Rechtsprechung des Bundesverfassungsgerichts 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 der Bundesregierung bestimmen aber 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. Auch ist die geforderte Protokollierung nicht vorgesehen.

Der Gesetzentwurf der Bundesregierung soll über § 46 OWiG i.V.m. § 100j StPO-E die Identifizierung von Internetnutzern selbst zur Verfolgung von Ordnungswidrigkeiten jeder Art ermöglichen. Das erhebliche Gewicht des Eingriffs solcher Auskünfte erlaubt es 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.

Um einen angemessenen Schutz der Vertraulichkeit der Telekommunikation zu gewährleisten, sind die für Verkehrsdaten geltenden Eingriffsschwellen auf Bestands-daten zu übertragen, insbesondere wo Bestandsdatenauskünfte unter Nutzung von Verkehrsdaten erteilt werden.

**Beschränkung auf begründete Einzelfälle und Unterbindung einer elektronischen Schnittstelle (im Beschluss Punkt 3.)**

Da es sich bei der Preisgabe von Bestandsdaten um einen nicht unerheblichen Eingriff in die Telekommunikationsfreiheit handelt, muss verhindert werden, dass die Auslieferung von Bestandsdaten zur Massenüberwachung ausartet, in der Bestandsdaten routinemäßig aufgrund kleinster Anlässe oder gar zur Vorsorge im Übermaß angefragt werden. Deshalb muss die Auslieferung von Bestandsdaten wie bisher (§ 113 TKG) ausdrücklich auf Einzelfälle beschränkt bleiben.

Das Bundesverfassungsgericht hat betont, dass dem Verhältnismäßigkeitsgrundsatz nur dann Rechnung getragen wird, wenn die Auskünfte auf Einzelfälle beschränkt werden (BVerfG, 1 BvR 1299/05 vom 24.1.2012, Absatz-Nr. 177). Es hat das „Erfordernis der Erforderlichkeit auch im Einzelfall“ als Anforderung des Verhältnismäßigkeitsgrundsatzes eingeordnet (BVerfG, 1 BvR 1299/05 vom 24.1.2012, Absatz-Nr. 163). Weil sämtlichen Zugriffsnormen des Gesetzentwurfes der Bundesregierung die Beschränkung von Auskünften auf Einzelfälle fehlt, ist er verfassungswidrig.

Das Bundesverfassungsgericht hat die „sehr weit“ reichende staatliche Einsicht in Telekommunikationsdaten über § 113 TKG ferner nur deswegen als „verfassungs-rechtlich 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 des § 113 TKG beibehalten und sogar weiter ausgedehnt wird, ist das Gebot der Verhältnismäßigkeit verletzt und § 113 Abs. 5 TKG-E verfassungswidrig. Die

Einrichtung einer elektronischen Schnittstelle, die eine massenhafte Verarbeitung der Daten erheblich vereinfacht, ist nicht nur für Einzelfälle vorgesehen und hat daher zu unterbleiben.

**Normenklare und restriktive Regelung der Zugangsvoraussetzungen zu Zugangssicherungscodes (im Beschluss Punkt 4.)**

Der Eingriff in einen persönlichen Bereich, der durch einen Zugangssicherungscode gesichert ist, stellt einen besonders schweren Eingriff in das Persönlichkeits- und Kommunikationsfreiheitsrecht des Individuums dar. Durch Weitergabe eines Zugangssicherungscodes verliert das Telekommunikationsunternehmen die Kontrolle über die Überwachung und ist gleichzeitig nicht in der Lage zu überprüfen, ob die gesetzlichen Voraussetzungen jeder Nutzung des Codes erfüllt sind. Die Weitergabe solcher Zugangssicherungscodes an Behörden darf daher, wenn überhaupt, nur unter strengsten Auflagen geschehen.

Die lapidare Bezugnahme im Gesetzentwurf der Bundesregierung auf „die gesetzlichen Voraussetzungen für die Nutzung der Daten“ verletzt das verfassungsrechtliche 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 Zugangssicherungscode anfordert, weiß der Anbieter nicht, ob dies zum Zweck der Telekommunikations-überwachung 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 besonders zu regeln, die auch deren Nutzung regeln, also z.B. in den §§ 98, 100a und 100b StPO.

**Festschreibung des Vorranges der Telekommunikationsüberwachung gegenüber dem unmittelbaren Zugriff mithilfe von Zugangssicherungscodes (im Beschluss Punkt 5.)**

Während es sich bei der Telekommunikationsüberwachung um eine zeitlich befristete Maßnahme handelt, kann eine zeitliche Befristung der Überwachungsmaßnahme bei der Herausgabe von Zugangssicherungscodes technisch nicht gewährleistet werden. Unzulässige Zugriffe auf die durch Zugangssicherungscodes geschützten Daten können seitens des Anbieters oder des Betroffenen nicht unterbunden werden. Aus diesem Grund muss die behördliche Anforderung von Zugangssicherungscodes gesetzlich beschränkt werden auf Fälle, in denen die begehrten Daten nicht durch Inanspruchnahme des Anbieters erhoben werden können.

**Bußgeldbewehrung der Herausgabe von Zugangssicherungscodes an unberechtigte Behörden oder Dritte (im Beschluss Punkt 6.)**

Derzeit ist es den Telekommunikationsanbietern bei Bußgeldandrohung untersagt, Zugriffscodes an nicht autorisierte öffentlich Stellen oder nicht-öffentliche Dritte weiterzugeben (§ 113 Abs. 1 S. 2 Hs. 2 TKG). Der besondere Schutz von Zugangssicherungscodes ergibt sich aus ihrer Bedeutung für die Persönlichkeitsrechte und den Kernbereich der privater Lebensgestaltung. Der Gesetzesentwurf sieht vor, dass dieser

besondere Schutz durch Bußgeldandrohung und Übermittlungsverbot zukünftig entfallen soll. Dies ist nicht akzeptabel.

**Beschränkung der Auskunft der Anbieter auf rechtmäßig gespeicherte Telekommunikationsdaten (im Beschluss Punkt 7.)**

Da laut Gesetzesentwurf die Heranziehung „sämtlicher unternehmensinterner Datenquellen" für die Ermittlungsbehörden zulässig werden soll (§ 113 Abs. 1 S. 4 TKG-E), werden auch nicht rechtmäßig erhobene oder gespeicherte Daten von der Regelung erfasst. An dieser Stelle ist eine Klarstellung, dass ausschließlich rechtmäßig erhobene und gespeicherte Daten abgerufen werden dürfen, unbedingt erforderlich. In der Vergangenheit sind immer wieder massive Verstöße von Telekommunikationsanbietern in Bezug auf Erhebung und Speicherung von personenbezogenen Daten festgestellt worden. Ein Zugriff auf derart rechtswidrig erlangte Daten von Bürgerinnen und Bürgern ist in jedem Falle auszuschließen. Derartige Zugriffsbefugnisse sind hochgradig unverhältnismäßig in Anbetracht der Tatsache, dass der Abruf von Bestandsdaten sogar für die Ermittlung von Bagatelldelikten zugelassen werden soll.

**Verzicht auf Zugriffsbefugnisse durch Bundeskriminalamt und Zollkriminalamt als Zentralstellen (im Beschluss Punkt 8.)**

Die durch den Gesetzesentwurf vorgesehene Erweiterung der Zugriffsbefugnisse auf Bundeskriminalamt und Zollkriminalamt als Zentralstellen markiert einen Paradigmenwechsel im Verhältnis zwischen Landes- und Bundesbehörden. Erstmals sollen Private verpflichtet werden, Anfragen von Bundeskriminalamt und Zollkriminalamt in ihrer Funktion als Zentralstelle zu beantworten. Bisher besteht die Aufgabe der Zentralstellen lediglich in der Sammlung freiwillig (etwa durch Landesbehörden) übermittelter Informationen. Diese Kompetenzverschiebung hin zu Bundesbehörden markiert eine Zäsur in den Befugnissen des Bundeskriminalamts und Zollkriminalamts. Diese Kompetenzerweiterung setzt Weichen, um Bundeskriminalamt und Zollkriminalamt langfristig weite Teile der Gefahrenabwehr im Internet zu- und den Landesbehörden abzusprechen. Diese Aufgabenerweiterung und Kompetenzverschiebung geht an den originären Aufgaben des Bundeskriminalamts und Zollkriminalamts vorbei und ist im Hinblick auf den Polizeibrief zum Grundgesetz abzulehnen, da hier Exekutivbefugnisse an Bundesbehörden abgetreten werden.

Soweit der Gesetzentwurf auf ungeklärte Zuständigkeiten verweist ohne die Regelung auf diese Fälle zu beschränken, 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 Fälle ungeklärter Zuständigkeit an die Polizei an seinem Sitz oder am Sitz des zuständigen Anbieters abgeben.

**Zeitrahmen und Umfang von Auskünften sowie Informationsmöglichkeit der Anbieter gegenüber ihren Kunden (im Beschluss Punkt 9.)**

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 TKG-E unzuständig. Diese Fragen zu regeln, muss dem zuständigen Fachgesetzgeber – also gegebenenfalls den Ländern – überlassen bleiben.

Es ist auch der Sache nach verfehlt, den Anbietern eine Information der betroffenen Kunden ausnahmslos zu untersagen. In den im Gesetzesentwurf genannten Fällen von Vermissten oder in Not befindlichen Personen besteht beispielsweise keine Notwendigkeit, den Zugriff auf die Bestandsdaten durch die Behörden dem Betroffenen zu verschweigen. Wie in anderen Staaten sollte eine Pflicht des Anbieters zum Stillschweigen gegenüber seinem Kunden nur gelten, wo die Behörde dies besonders anordnet.

**Benachrichtigung der Betroffenen (im Beschluss Punkt 10.)**

Aus dem Urteil des Bundesverfassungsgerichts zur Vorratsdatenspeicherung geht hervor, dass eine Benachrichtigung der Betroffenen von IP-Auskünften in der Regel verfassungsrechtlich geboten ist (BVerfG, 1 BvR 256/08 vom 2.3.2010, Absatz-Nr. 263). Ohne Information über eine Abfrage ist ein wirksamer Rechtsschutz gegen unrechtmäßige Abfragen unmöglich. Betroffene sollten generell über jegliche Abfrage zumindest im Nachhinein informiert werden um ihnen die Möglichkeit zu geben, sich gegen unrechtmäßige Zugriffe auf dem Rechtsweg zur Wehr zu setzen und deren Rechtmäßigkeit überprüfen zu lassen.

Die Abfrage von Zugangssicherungscodes stellt einen besonders tiefgreifenden Eingriff in die Privatsphäre der Betroffenen dar. Ohne Benachrichtigung kann ein unrechtmäßiger Zugriff auf die Daten zu einem späteren Zeitpunkt nicht ausgeschlossen werden, weil der Betroffene keine Möglichkeit hat, offengelegte Zugangssicherungscodes zu ändern, um sich gegen unbefugten Zugriff zu schützen. Deswegen ist eine Benachrichtigung nach Abschluss der staatlichen Ermittlungen sicherzustellen.

Die Vorgaben des Bundesverfassungsgerichts zur Benachrichtigungspflicht sind ungeachtet dessen einschlägig, dass die Ausführungen zu § 113 TKG im Zusammenhang mit der mittelbaren Nutzung anlasslos erhobener Verkehrsdaten gemacht worden 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.).

**Statistische Erfassung und Veröffentlichung der staatlichen Bestands-datenabfragen (im Beschluss Punkt 11.)**

Eine umfassende statistische Erfassung der staatlichen Bestandsdatenabfragen ist für eine wissenschaftliche Überprüfung und öffentliche Kontrolle der getätigten Grundrechtseingriffe unerlässlich. Die Anzahl der getätigten Zugriffe muss der Öffentlichkeit zugänglich gemacht werden, damit das Ausmaß der getätigten Eingriffe und die damit verbundenen Grundrechtseinschränkungen für Betroffene für die Bürgerinnen und Bürger transparent nachvollziehbar sind. Die Entwicklung der tatsächlichen Nutzung der durch den Gesetzesentwurf vorgesehenen neuen Zugriffsbefugnisse durch Behörden kann so nachverfolgt und eine übergriffige Nutzung des Rechtsrahmens frühzeitig erkannt werden.

Darüber hinaus ist es für eine wissenschaftliche Auseinandersetzung mit der Entwicklung von Abfragezahlen unerlässlich, derartige Daten genau nach Abfragegrund, abfragende Behörde, Zahl der Betroffenen und weiteren für die statistische Erfassung notwendigen Daten aufzuschlüsseln. Nur so kann eine auf wissenschaftlicher Faktenlage basierende unabhängige Evaluierung der Eingriffsbefugnisse gewährleistet werden.

**Informationspflicht bei unrechtmäßiger Kenntniserlangung von Telekommunikationsdaten für staatliche Stellen (im Beschluss Punkt 12.)**

Für private Stellen besteht seit der Novelle des Bundesdatenschutzgesetzes eine bußgeldbewehrte Meldepflicht für unrechtmäßige Datenerhebungen (§ 42a BDSG). Eine derartige Regelung ist in Anbetracht der umfassenden Datenverarbeitung ins-besondere im Sicherheitsbereich auch für staatliche Stellen erforderlich, um Betroffenen die Möglichkeit des Rechtsschutzes (einschließlich der Geltendmachung von Schadensersatzansprüchen) bei Fehlverhalten zu geben und der Aufsichtsbehörde ein Einschreiten zu ermöglichen.

Auskunftsersuchen werden nicht selten falsch oder rechtswidrig beantwortet. Häufige Ursache falscher Auskünfte sind Tippfehler bei der Angabe von Telefonnummern oder IP-Adressen. Teilweise fragt bereits die Behörde irrtümlich nach der falschen Rufnummer oder IP-Adresse, nach einem falschen Zeitpunkt oder einem anderen als den gesuchten Datentyp. Teilweise erteilen Telekommunikationsanbieter trotz richtigen Auskunftsersuchens Auskunft über eine falsche Rufnummer oder IP-Adresse, über eine falsche Uhrzeit, über einen anderen als den gewünschten Datentyp (z.B. Verbindungsdaten statt Bestandsdaten) oder über mehr Daten als angefordert. Teilweise fordern Behörden Auskünfte unter Verletzung der gesetzlichen Zuständigkeits- und Verfahrensregelungen an.

Nur durch eine Meldepflicht können strukturelle Mängel bei dem staatlichen Zugriff auf sensible Daten von Kommunikationsteilnehmern erkannt und angegangen werden.

**Beschluss:**

Der Landtag fordert die Landesregierung auf,

den Entwurf der Bundesregierung eines Gesetzes zur Änderung des Telekommunikations-gesetzes und zur Neuregelung der Bestandsdatenauskunft im Bundesrat abzulehnen, solange nicht

1. durch ein einfachgesetzliches Zitiergebot Klarheit darüber hergestellt wird, welche Gesetze einen staatlichen Zugriff auf Kommunikationsdaten erlauben sollen und welche nicht,

2. für die Auslieferung von Telekommunikations-Bestandsdaten (§ 113 Absatz 1 Satz 1 TKG) an Staatsbehörden mindestens dieselben verfahrensrechtlichen und inhaltlichen Voraussetzungen eingeführt werden wie für die Auslieferung von Telekommunikations-Verkehrsdaten (z.B. Richtervorbehalt, Eingriffsschwellen),

3. die Auslieferung von Bestandsdaten (§ 113 Absatz 1 Satz 1 TKG) gesetzlich ausdrücklich auf Einzelfälle beschränkt bleibt und die Einführung einer elektronischen Auskunftsschnittstelle unterbleibt,

4. eindeutig und restriktiv gesetzlich geregelt wird, unter welchen verfahrens-rechtlichen und inhaltlichen Voraussetzungen Zugangssicherungscodes (wie Passwörter, PIN oder PUK), die den Zugang zu Endgeräten (z.B. Mobiltelefonen) und Speicherungseinrichtungen (z.B. E-Mail-Postfächer) sichern, gegenüber Staatsbehörden preiszugeben sind und deren Nutzung zugelassen wird,

5. der Vorrang der Telekommunikationsüberwachung unter Mitwirkung des An-bieters vor dem unmittelbaren Zugriff mithilfe von Zugangssicherungscodes festgeschrieben wird,

6. die Herausgabe von Zugangssicherungscodes an unberechtigte Behörden oder Dritte bußgeldbewehrt verboten bleibt,

7. festgelegt wird, dass Anbieter Auskünfte ausschließlich anhand rechtmäßig gespeicherter Kommunikationsdaten erteilen dürfen,

8. darauf verzichtet wird, Bundeskriminalamt und Zollkriminalamt als Zentralstellen Zugriff auf Telekommunikationsdaten einzuräumen,

9. der Bund es dem zuständigen Fachgesetzgeber überlässt, zu regeln, in welchem Zeitrahmen und Umfang Auskünfte zu erteilen sind und ob der Anbieter seine Kunden informieren darf,

10. eine Benachrichtigung der Betroffenen mindestens von Eingriffen in das Fernmeldegeheimnis (Identifizierung von Internetnutzern) und von der Auslieferung persönlicher Zugangssicherungscodes sichergestellt wird,

11. Zahl und Art der staatlichen Bestandsdatenabfragen statistisch erfasst und jährlich veröffentlicht werden,

12. auch für staatliche Stellen eine Informationspflicht bei unrechtmäßiger Kenntniserlangung von Telekommunikationsdaten eingeführt wird.

Dirk Schatz
Joachim Paul
Frank Herrmann
Monika Pieper

und Fraktion