Piratenfraktion •Postfach 7121 •24171 Kiel

vorab per Fax: 0721/9101-382

Bundesverfassungsgericht
Schlossbezirk 3

76131 Karlsruhe

Piratenfraktion im
Schleswig-Holsteinischen Landtag

Geschäftsstelle:
Tel.: 04 31 - 9 88 1337
Fax: 04 31 – 9 88 1602

Besuchsadresse:
Düsternbrooker Weg 70
24105 Kiel

Postadresse:
Postfach 7121
24171 Kiel

Twitter @fraktionSH

Kiel, 24.06.2013

Verfassungsbeschwerde

der Abgeordneten

1. Angelika Beer,
2. Patrick Breyer,
3. Wolfgang Dudda,
4. Uli König,
5. Sven Krumbeck und
6. Torge Schmidt,

Anschrift jeweils Düsternbrooker Weg 70, 24105 Kiel.

Wir beantragen,

1. § 180a des Allgemeinen Verwaltungsgesetzes für das Land Schleswig-Holstein (Landesverwaltungsgesetz - LVwG -) in der Fassung der Bekanntmachung vom 2. Juni 1992 (GVOBl. 1992, 243, 534), eingefügt durch Gesetz vom 21.06.2013 (GVOBl. 2013, 254), sowie § 8a Absatz 1 des Schleswig-Holsteinischen Landesverfassungsschutzgesetzes vom 23. März 1991 (GVOBl. 1991, 203), zuletzt geändert durch Gesetz vom 21.06.2013 (GVOBl. 2013, 254), für unvereinbar mit Arti-

kel 2 Absatz 1 in Verbindung mit Artikel 1 Absatz 1 sowie mit Artikel 10 Absatz 1 des Grundgesetzes und für nichtig zu erklären,

2. § 15 Absatz 5 Satz 4 des Telemediengesetzes vom 26.02.2007 (BGBl. 2007, 179), zuletzt geändert durch Gesetz vom 31.05.2010 (BGBl. 2010, 692), für unvereinbar mit Artikel 2 Absatz 1 in Verbindung mit Artikel 1 Absatz 1 des Grundgesetzes und für nichtig zu erklären.

1. Sachverhalt

Die Beschwerdeführer wenden sich gegen Vorschriften zur Neuregelung der Bestandsdatenauskunft. Sie rügen eine Verletzung des Rechts auf informationelle Selbstbestimmung gemäß Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG sowie des Telekommunikationsgeheimnisses gemäß Art. 10 Abs. 1 GG. Die Beschwerdeführer wenden sich daneben gegen eine Vorschrift zur Herausgabe von Telemedien-Nutzungsdaten an den Staat. Sie rügen insoweit eine Verletzung des Rechts auf informationelle Selbstbestimmung gemäß Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG.

Die Beschwerdeführer sind jeweils Inhaber von Festnetz- und Internetanschlüssen sowie von E-Mail-Postfächern, sie nutzen außerdem jeweils mindestens ein Mobiltelefon. Als Abgeordnete im schleswig-holsteinischen Landtag sind sie darauf angewiesen, anonyme und nicht rückverfolgbare Hinweise beispielsweise über Missstände im Land erhalten zu können, da diese nicht selten nur im Schutz der Anonymität gegeben werden. In diesem Zusammenhang müssen sie auch selbst geschützt kommunizieren und im Internet recherchieren können. Die Beschwerdeführer nutzen das Internet und dort verschiedenste Kommunikations- und Informationsdienste intensiv sowohl zu privaten als auch zu beruflichen Zwecken. Beispielsweise informieren sie sich über Nachrichten auf Internetportalen wie spiegel.de.

2. Zulässigkeit der Beschwerde

2.1. Betroffenheit der Beschwerdeführer

Die angegriffenen Vorschriften betreffen die Beschwerdeführer unmittelbar, selbst und gegenwärtig. An einer unmittelbaren Selbstbetroffenheit fehlt es in Bezug auf die angegriffenen Vorschriften nicht deshalb, weil diese erst auf der Grundlage weiterer Vollzugsakte in Form von Auskunftserteilungen und Datenübermittlungen wirksam werden. Von Auskünften über ihre Daten werden die Beschwerdeführer wahrscheinlich keine Kenntnis erlangen. Viele Auskünfte führen nicht zu weiteren Maßnahmen gegen die Betroffenen, etwa wenn die Identitäten zu Rufnummern eines

aufgefundenen Telefonbuchs oder der sich in einer Funkzelle aufhaltenden Personen abgefragt werden. Eine Benachrichtigung ist in vielen Fällen nicht vorgesehen (z.B. in den Fällen des § 180b Abs. 1 i.V.m. § 180a Abs. 1 LVwG oder in Fällen von Spontanübermittlungen nach § 15 Abs. 5 S. 4 TMG). Bei Abfragen von IP-Adressen, Zugangssicherungscodes und Telemediendaten unterliegt die Benachrichtigungspflicht so vielen Einschränkungen (z.B. Vereitelung des Zwecks der Auskunft, überwiegende schutzwürdige Belange Dritter oder der betroffenen Person selbst), dass die Beschwerdeführer auch von solchen Maßnahmen in den meisten Fällen nicht erfahren werden. Dies legen auch Studien des Max-Planck-Instituts zu vergleichbar eingeschränkten Benachrichtigungspflichten der Strafprozessordnung nahe.

Da die Beschwerdeführer keine zuverlässige Kenntnis von dem Normenvollzug erlangen, reicht die Darlegung aus, mit einiger Wahrscheinlichkeit von solchen Maßnahmen berührt zu werden. Maßgeblich ist hierfür insbesondere, dass die durch die angefochtenen Vorschriften ermöglichten Auskünfte eine große Streubreite haben und Dritte auch zufällig erfassen können. Darlegungen, durch die sich die Beschwerdeführer selbst einer Straftat bezichtigen müssten, sind zum Beleg der Selbstbetroffenheit ebenso wenig erforderlich wie der Vortrag, für sicherheitsgefährdende oder nachrichtendienstlich relevante Aktivitäten verantwortlich zu sein.[1]

2.2. Wahrung der Beschwerdefrist

Die Wahrung der Beschwerdefrist bezüglich der angefochtenen Landesvorschriften ergibt sich daraus, dass das am 21.06.2013 beschlossene Gesetz zu ihrer Einführung am 27.06.2013 verkündet worden ist.

Die Wahrung der Beschwerdefrist in Bezug auf § 15 Abs. 5 S. 4 TMG ergibt sich daraus, dass die Vorschrift durch das Gesetz zur Änderung des Telekommunikationsgesetzes und zur Neuregelung der Bestandsdatenauskunft eine grundlegend veränderte Bedeutung bekommen hat. Bislang war die sehr weit reichende Übermittlungsbefugnis des § 15 Abs. 5 S. 4 TMG insoweit unschädlich als Nutzer von Telemedien, die sich nicht freiwillig mit ihren wahren Daten identifizierten, trotz Auskünften über ihre Nutzungsdaten weitgehend im Schutz der Anonymität bleiben konnten. Bisher war § 113 TKG nämlich nicht zu entnehmen, dass er die Identifizierung anhand von IP-Adressen, also die Zuordnung auch von Telemedien-Nutzungsdaten, erlauben sollte.[2] Auskünfte über IP-Adressen waren daher nur nur unter qualifizierten Voraussetzungen wie etwa im Strafrecht nach § 100g StPO erlaubt.[3]

Der Bundesgesetzgeber hat sich mit dem Gesetz zur Neuregelung der Bestandsdatenauskunft nun aber entschieden, keinerlei qualifizierte Voraussetzungen für die

–1– Vgl. BVerfGE 125, 260 (305).

–2– BVerfGE 130, 151, Abs. 172 ff.

–3– Vgl. BVerfGE 130, 151, Abs. 164.

Zuordnung von Internet-Nutzungsdaten zu fordern, sondern sie allgemein zum Zweck der Verfolgung von Straftaten oder Ordnungswidrigkeiten, zur Abwehr von Gefahren für die öffentliche Sicherheit oder Ordnung oder für die Erfüllung der gesetzlichen Aufgaben der Nachrichtendienste zuzulassen, und zwar ohne Richtervorbehalt (vgl. nur § 100j StPO, §§ 7, 20b, 22 BKAG, 8d BVerfSchG). Wird auf diese Weise der Anonymität im Internet der Schutz genommen, gewinnt die Vertraulichkeit des Internet-Nutzungsverhaltens und namentlich die Blanko-Übermittlungsbefugnis des § 15 Abs. 5 S. 4 TMG eine ganz neue Bedeutung. Die nun äußerst weit reichenden Identifizierungsmöglichkeiten von IP-Adressen verleihen der Preisgabe unseres Telemedien-Nutzungsverhaltens einen neuen, weitaus belastenderen Inhalt. Die Eingriffsbehörden können nun in großer Menge Internet-Nutzungsdaten erheben und sie auch massenhaft zuordnen (z.B. alle Interessenten an einer Internetseite oder alle Nutzer eines „verdächtigen“ Suchbegriffs). Auf diese Weise hat das Gesetz zur Änderung des Telekommunikationsgesetzes und zur Neuregelung der Bestandsdatenauskunft die Beschwerdefrist bezogen auf § 15 Abs. 5 S. 4 TMG neu in Gang gesetzt. In der Rechtsprechung des Hohen Gerichts ist anerkannt, dass die Beschwerdefrist neu zu laufen beginnt, wenn eine Vorschrift durch Änderung anderer Normen einen neuen, den Beschwerdeführer erheblich belastenderen Inhalt als zuvor gewinnt.[1]

3. Begründetheit der Beschwerde

Prüfungsmaßstab ist im Schwerpunkt das Recht auf informationelle Selbstbestimmung gemäß Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG. Soweit die Vorschriften zur Identifizierung des Anschlussinhabers anhand dynamischer IP-Adressen ermächtigen, greifen sie in das Telekommunikationsgeheimnis gemäß Art. 10 GG ein.[2] Soweit eine Benachrichtigung des Betroffenen von einer Übermittlung seiner Daten nicht oder nur eingeschränkt vorgesehen ist, liegt zudem ein Eingriff in das Grundrecht auf effektiven Rechtsschutz nach Art. 19 Abs. 4 GG vor.

Die angefochtenen Grundrechtseingriffe sind verfassungsrechtlich nicht zu rechtfertigen:

3.1. §§ 180a, 180b des Landesverwaltungsgesetzes

3.1.1. Eingriffsschwelle der „bevorstehenden Gefahr“

§ 180a Abs. 1 LVwG (auch in Verbindung mit Abs. 2) verletzt die Gebote der Verhältnismäßigkeit und der Normenklarheit, soweit verpflichtende Auskunftsersuchen über Bestandsdaten zugelassen werden, wenn dies „zur Abwehr einer im einzelnen Falle

–1– BVerfGE 78, 350 (356), Abs. 23.

–2– BVerfGE 130, 151 (179 ff.).

bevorstehenden Gefahr für die öffentliche Sicherheit erforderlich ist“.

Nach der Rechtsprechung des Bundesverfassungsgerichts ist im Bereich der Gefahrenabwehr eine konkrete Gefahr im Sinne der polizeilichen Generalklauseln Mindestvoraussetzung einer verhältnismäßigen staatlichen Bestandsdatenerhebung.[1] Konkrete Gefahr ist eine Sachlage, bei der im konkreten Fall die hinreichende Wahrscheinlichkeit besteht, dass in absehbarer Zeit ein Schaden für Rechtsgüter eintreten wird.[2]

Nach der polizeilichen Generalklausel des § 174 LVwG haben die Ordnungsbehörden und die Polizei „Gefahren abzuwehren, durch die die öffentliche Sicherheit bedroht wird“. Vorausgesetzt ist danach sowohl von Gesetzes als auch von Verfassungs wegen eine aktuell bestehende Gefahr, also ein absehbar bevorstehender Schadenseintritt.

Wenn § 180a Abs. 1 LVwG demgegenüber bereits eine „bevorstehende Gefahr“ genügen lassen will, erfasst er dem Wortlaut nach auch Situationen vor dem Eintritt einer Gefahrensituation, also im sogenannten „Gefahrenvorfeld“. Wenn eine Gefahr bevorsteht, liegt sie noch nicht vor. Präventive Auskünfte über Telekommunikationsdaten auch außerhalb von Gefahrensituationen zuzulassen, verletzt das Verhältnismäßigkeitsgebot.

Zwar soll mit dem Begriff der „im einzelnen Falle bevorstehenden Gefahr“, der auch an anderen Stellen des Landesverwaltungsgesetzes verwendet wird, ausweislich der Begründung des Regierungsentwurfs eine „konkrete Gefahr“ und nicht das Gefahrenvorfeld gemeint sein.[3] Der Wortlaut macht dies aber nicht so deutlich, wie es das Gebot der Normenklarheit in Anbetracht der Tiefe des Grundrechtseingriffs erfordert. Nichtjuristen als Adressaten und Anwender der Norm können nicht erkennen, dass mit „bevorstehender Gefahr“ eine „bestehende Gefahr“ gemeint sein soll, zumal in der Generalklausel des § 174 LVwG eine andere Formulierung für den Begriff der konkreten Gefahr verwendet wird. Hinzu kommt, dass der Landtag die Formulierung der „bevorstehenden Gefahr“ übernommen hat, obwohl wir im Gesetzgebungsverfahren wiederholt auf die Problematik des Wortlauts hingewiesen hatten. Wenn die nahe liegende Möglichkeit einer Klarstellung wissentlich nicht genutzt wird, spricht dies gegen eine vom Wortlaut abweichende Auslegung.

Telekommunikationsanbieter dürfen gemäß § 113 Abs. 2 TKG Auskünfte zwar nur erteilen, wenn diese u.a. „zur Abwehr von Gefahren für die öffentliche Sicherheit oder Ordnung“ verlangt werden. Der Anbieter kann und darf die materielle Frage des Vorliegens einer konkreten Gefahr jedoch nicht prüfen (§ 113 Abs. 2 S. 3 TKG). Auch die Bundesregierung bestätigt in ihrer Gegenäußerung, dass die materielle Eingrenzung „nicht (mehr) in § 113 TKG geregelt werden kann“, weil sie „nicht die

–1– BVerfGE 130, 151, 205 f., Abs. 177 f.

–2– BVerfGE 115, 320 (364), Abs. 144.

–3– LT-Drs. 18/713, 13.

Übermittlungspflicht des Telekommunikationsanbieters, sondern die Erhebungsbefugnis der Behörden“ betrifft.[1]

3.1.2. Fehlende Beschränkung von Auskunftsersuchen auf Einzelfälle

In § 180a Abs. 1 LVwG (auch in Verbindung mit Abs. 2) fehlt die im bisherigen § 113 TKG enthaltene Bestimmung, dass Auskünfte über Telekommunikationsdaten nur „im Einzelfall“ eingeholt 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 Neuregelung verfassungswidrig.[2]

Der Begriff der Datenerhebung „im Einzelfall“ oder auch „in einzelnen Fällen“ wird in Abgrenzung zur pauschalen Erhebung großer Datenmengen oder „Massendaten“ verwendet. Zwar setzt § 180a Abs. 1 LVwG eine „im Einzelfall bevorstehende Gefahr“ voraus. Diese Anforderung schließt es aber nicht aus, dass die Polizei eine solche Einzelfallsituation zum Anlass nimmt, sich routinemäßig oder massenhaft Bestandsdatenauskünfte erteilen zu lassen. Dies ist insbesondere deshalb nicht auszuschließen, weil § 180a Abs. 1 LVwG auch für Dauergefahren gilt. Die USA legen beispielsweise eine Bestimmung zur Datenerhebung so aus, dass es das dauerhaft bestehende Risiko terroristischer Anschläge rechtfertigen soll, dass die NSA sich sämtliche Verbindungsdaten täglich übermitteln lässt. Dass § 180a Abs. 1 LVwG eine „im einzelnen Falle bevorstehende Gefahr“ voraus setzt, besagt nichts darüber, ob aus Anlass solcher Gefahren nur im Einzelfall oder als Standardmaßnahme und massenhaft Auskünfte eingeholt werden dürfen.

Da es sich bei der Preisgabe von Bestandsdaten um einen schweren Grundrechtseingriff 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 a.F.) ausdrücklich auf Einzelfälle beschränkt bleiben.

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“.[3] Es hat das „Erfordernis der Erforderlichkeit auch im Einzelfall“ als Anforderung des Verhältnismäßigkeitsgrundsatzes eingeordnet.[4] Weil nun auch noch die Beschränkung von

–1– BT-Drs. 17/12034, 20.

–2– Zum Bundesrecht: Unabhängiges Landesdatenschutzzentrum, Stellungnahme vom 27.11.2012, https://www.datenschutzzentrum.de/polizei/20121127-stellungnahme-tkg-aenderung.html, Ziff. I; Bundesrat, BT-Drs. 17/12034, 17; Wirtschaftsausschuss des Bundesrats, BR-Drs. 664/1/12, 2.

–3– BVerfGE 130, 151, 205 f., Absatz-Nr. 177 f.

–4– BVerfGE 130, 151, 200, Absatz-Nr. 163 a.E.

Auskünften auf Einzelfälle dem ohnehin sehr weit reichenden § 180a Abs. 1 LVwG fehlt, ist die Vorschrift verfassungswidrig.

Es kann dabei letztlich offen bleiben, ob die Beschränkung auf Einzelfälle in der Öffnungsnorm des § 113 TKG oder aber in den fachspezifischen Abrufermächtigungen geregelt werden muss, denn sie ist an keiner der beiden Stellen verankert: Die neue Erhebungsbefugnis des § 180a Abs. 1 LVwG bestimmt nicht, dass „Auskünfte ... im Einzelfall angefordert werden“ müssen; sie machen nicht eine „Erforderlichkeit auch im Einzelfall“ zur Voraussetzung der Bestandsdatenerhebung. Zwar sollen die Anbieter Auskünfte nach der Öffnungsnorm des § 113 TKG nur erteilen dürfen, wenn sie „im Einzelfall ... verlangt“ werden (§ 113 Abs. 2 TKG). Die Anbieter sind aber weder berechtigt noch in der Lage, zu prüfen, ob Auskünfte im Einzelfall erforderlich sind; sie führen nur eine formale Prüfung durch (vgl. § 113 Abs. 2 S. 3 und Abs. 5 S. 3 TKG). Die Bundesregierung meint in ihrer Gegenäußerung, dass die Beschränkung auf Einzelfälle „nicht (mehr) in § 113 TKG geregelt werden kann“, weil sie „nicht die Übermittlungspflicht des Telekommunikationsanbieters, sondern die Erhebungsbefugnis der Behörden“ betrifft.[1] In § 180a Abs. 1 LVwG fehlt die Voraussetzung einer „Erforderlichkeit auch im Einzelfall“ dann aber ebenfalls.

3.1.3. Fehlende Beschränkung auf Störer

§ 180a Abs. 1 LVwG geht auch insofern unverhältnismäßig weit als jede Bagatellgefahr zum Anlass genommen werden kann, Bestandsdaten (einschließlich Zugangscodes und IP-Auskünfte) über Personen zu erheben, die für die Gefahr gar nicht verantwortlich sind. Wie bei Verkehrsdatenauskünften (§§ 185a Abs. 3 S. 1, 185 Abs. 2 S. 2 LVwG) ist eine Beschränkung auf Personen geboten, bei denen zumindest Tatsachen dafür sprechen, dass sie als Verantwortliche in Anspruch genommen werden können.[2]

3.1.4. Fehlende Benachrichtigung

Im Fall von Auskünften über elektronische Adressbücher, Identität, Kontoverbindung usw. (§ 180a Abs. 1 LVwG) ist keinerlei Benachrichtigung der Betroffenen von Zugriffen auf ihre Daten vorgesehen. Da eine Benachrichtigung Voraussetzung eines effektiven Rechtsschutzes gegen Grundrechtsverletzungen ist, ist aus Art. 19 Abs. 4 GG eine Benachrichtigungspflicht abzuleiten.[3] Nur wenn Betroffene von der Erhebung ihrer Daten erfahren, können sie gegen rechtswidrige oder gar grundrechtsverletzende Datenerhebungen vorgehen. Gerade im Fall breitflächiger Datenabfragen ist eine Benachrichtigung Voraussetzung der richterlichen Kontrolle der Verhältnismäßigkeit. Eine Benachrichtigung lässt sich auch bei einer Vielzahl von Betroffenen

–1– BT-Drs. 17/12034, 20.

–2– Vgl. auch BVerfGE 113, 348 (380 f., 389), Abs. 130 ff. und 156.

–3– A.A. wohl BVerfGE 130, 151, Abs. 187.

leicht umsetzen. Ebenso wie die Anbieter zur Auskunfterteilung über elektronische Schnittstellen in Anspruch genommen werden, könnte das Verfahren auch auf Benachrichtigung der Betroffenen nach Abschluss des Verfahrens erstreckt werden. Die Anbieter könnten die Betroffenen Kunden auf der Rechnung, per SMS o.ä. informieren, ohne dass dadurch Kosten entstünden.

3.1.5. Mangelnde Kontrolle durch fehlende Statistik

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.

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).[1] Registriert werden sollte auch Erfolg oder Misserfolg der Maßnahme. Eine solche verfahrensrechtliche Sicherung erscheint bei Bestandsdatenzugriffen allgemein geboten, damit der Gesetzgeber die Entwicklung seiner äußerst weiten Befugnisse zur Erhebung von Telekommunikationsdaten beobachten und sie gegebenenfalls wieder eindämmen kann. Besonders beobachtungsbedürftig ist die Nutzung der elektronischen Schnittstelle zum Datenaustausch, welche übrigens statistisch besonders leicht zu erfassen wäre (vgl. § 112 Abs. 4 TKG).

Zwar mag der Gesetzgeber nicht allgemein verpflichtet sein, Eingriffe in das Recht auf informationelle Selbstbestimmung statistisch erfassen zu lassen. Im vorliegenden Fall handelt es sich aber um Eingriffe in die besonders wichtige Vertraulichkeit von Telekommunikationsverhältnissen, darunter auch die Identifizierung von Internetnutzern und die Anforderung von Codes zur Überwindung von Zugangssicherungen. Wie das Hohe Gericht festgestellt hat, haben die durch die angefochtenen Vorschriften ermöglichten Auskünfte eine große Streubreite und können auch Dritte zufällig erfassen können. Die Schnittstelle zum automatisierten Datenaustausch nach

–1– http://wiki.vorratsdatenspeicherung.de/images/DiskE_.pdf, 6.

§ 113 TKG ermöglicht den massenhaften Abruf und Weiterverarbeitung von Telekommunikationsdaten. Gerade hier ist eine Zugriffsprotokollierung schon datenschutzrechtlich als geboten zu erachten. Weshalb von einer statistischen Auswertung abgesehen werden soll, ist nicht nachvollziehbar.

§ 180a Abs. 1 LVwG (auch in Verbindung mit Abs. 2) sieht keinerlei statistische Erfassung vor, obwohl § 113 TKG den Datenzugriff erheblich ausgeweitet hat. Dies genügt dem Verhältnismäßigkeitsgebot nicht.

3.1.6. Fehlende Subsidiarität des Zugriffs auf Zugangssicherungscodes (PINs, Passwörter)

§ 180a Abs. 2 S. 1 LVwG ermächtigt die Polizei zur Abfrage von Codes und Passwörtern, mittels derer der Zugriff auf Endgeräte (z.B. Smartphones) oder auf Speichereinrichtungen, die in diesen Endgeräten oder hiervon räumlich getrennt eingesetzt werden (z.B. E-Mail-Postfächer), geschützt wird.

Zugangssicherungscodes ermöglichen den Zugriff auf äußerst sensible Inhalte der Telekommunikation und weitere persönliche Inhalte wie Fotos, Tagebücher und Dokumente. Viele integrierte Dienste sichern den Zugang zur Telekommunikation mit demselben Code wie den Zugang zu anderen Diensten (z.B. persönlicher Daten- und Dokumentenspeicher, soziale Netzwerke). Mit der Herausgabe solcher Schlüssel an Staatsbeamte begibt sich der Anbieter der Kontrolle über ihre Verwendung. Der unmittelbare staatliche Fernzugriff auf Speichereinrichtungen (z.B. E-Mail-Postfächer) greift vor diesem Hintergrund weit tiefer in das Grundrecht auf informationelle Selbstbestimmung ein als die Inanspruchnahme des Anbieters zur Auswahl und Übermittlung der Daten. Im Fall der Inpflichtnahme des Anbieters kann diesem die Herausgabe lediglich bestimmter Inhalte aufgegeben werden, ohne dass der Staat sämtliche Daten durchsehen müsste. Die Inpflichtnahme des Anbieters kann auch zeitlich befristet werden, während im Fall der Herausgabe von Zugangssicherungscodes keine externe Kontrolle der Wahrung der zeitlichen Schranken durch den Anbieter erfolgen kann.

Vor diesem Hintergrund ist aus dem Verhältnismäßigkeitsgebot abzuleiten, dass der Staat Zugangssicherungscodes allenfalls dann erheben darf, wenn die damit bezweckte Datenerhebung auf andere Weise - insbesondere durch Inanspruchnahme des Anbieters - nicht erfolgen kann. In Anbetracht der Schwere des Grundrechteeingriffs hätte der Gesetzgeber eine entsprechende Subsidiaritätsklausel ausdrücklich aufnehmen müssen. Im Umkehrschluss zu den Subsidiaritätsklauseln der Strafprozessordnung ergibt sich aus der jetzigen Gesetzesfassung nämlich, dass keine Subsidiarität gewollt ist.[1] In diesem Sinne haben sich Vertreter der Koalitionsfraktionen im Innen- und Rechtsausschuss auch geäußert. Dies wird dem empfindli-

–1– Gegen Subsidiarität auch Buermeyer, Stellungnahme 16/639, https://www.landtag.nrw.de/portal/WWW/dokumentenarchiv/Dokument/MMST16-639.pdf, 9.

chen Grundrechtseingriff aber keinesfalls gerecht.

Deswegen muss zur Wahrung des Verhältnismäßigkeitsgebots der Vorrang der Telekommunikationsüberwachung und der Datensicherstellung unter Mitwirkung des Anbieters vor dem unmittelbaren Zugriff mithilfe von Zugangssicherungscodes ausdrücklich festgeschrieben werden. Wir haben im Gesetzgebungsverfahren vergeblich auf den Unterschied hingewiesen und eine Änderung beantragt.[1]

3.1.7. Mangelnde Sicherheit erhobener Zugangssicherungscodes

Zu beanstanden ist ferner, dass das Gesetz keinerlei Vorkehrung zur Gewährleistung der Sicherheit erhobener Zugangssicherungscodes trifft. Es ist keine separate Aufbewahrung vorgesehen, kein besonderer Schutz vor Übermittlung von Codes oder ihrer Nutzung zu ganz anderen Zwecken (Zweckänderung) und keine Pflicht zu ihrer frühestmöglichen Vernichtung. In Anbetracht der besonders weit reichenden Nutzbarkeit und Verwendungsmöglichkeiten von Zugangsschlüsseln wird ihr mangelhafter Schutz dem Verhältnismäßigkeitsgebot nicht gerecht.

3.1.8. Ausufernde Identifizierung von Internetnutzern

Die Ermächtigung zur Identifizierung von Internetnutzern nach § 180a Abs. 1, Abs. 2 S. 2 LVwG geht unverhältnismäßig weit:

3.1.8.1. Tiefe des Grundrechtseingriffs

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

–1– LT-Umdruck 18/1316, 6.

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.[1]

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.[2] Die „Deanonymisierung“ der Internetnutzung im selben weit reichenden Umfang zuzulassen wie den Blick ins Telefonbuch ist nicht hinnehmbar.[3]

3.1.8.2. Die verfassungsrechtlichen Anforderungen

Das Bundesverfassungsgericht hat sich in seiner Entscheidung zur Bestandsdatenauskunft nicht dazu geäußert, welche Anforderungen aus dem Verhältnismäßigkeitsgebot abzuleiten sind, weil es § 113 TKG so ausgelegt hat, dass er Auskünfte über Internet-Protokolladressen nicht erfasse. In der Entscheidung zur Vorratsdatenspeicherung hat das Bundesverfassungsgericht Auskünfte über Internet-Protokolladressen in sehr weitreichendem Maße zugelassen. Die Erwägungen, die zu dieser Entscheidung geführt haben, können unter den heutigen Bedingungen nicht mehr aufrecht erhalten werden.

Die Argumentation, mit der das Bundesverfassungsgericht geringere verfassungsrechtliche Anforderungen an die Identifizierung von Internetnutzern gestellt hat als an sonstige Eingriff in das Fernmeldegeheimnis, überzeugt nicht. Es ist nicht nachvollziehbar und auch nicht plausibel erklärt, warum die Identifizierung eines Teilnehmers anhand einer IP-Adresse geringeren Anforderungen unterliegen soll als seine Identifizierung anhand anderer Verkehrsdaten (z.B. IMEI-Kennung, Zeitpunkt einer Telefonverbindung). Diese Diskriminierung von Internetverbindungen führt zu unauflösbaren Wertungswidersprüchen: Ruft jemand mit unterdrückter Rufnummer zu einer bekannten Uhrzeit einen bekannten Zielanschluss an, so darf er anhand der bekannten Verbindungsdaten nach Auffassung des Bundesverfassungsgerichts nur mit

---

–1– BVerfGE 125, 260, 342, Abs. 259.

–2– BVerfGE 130, 151, 204, Abs. 174.

–3– Unabhängiges Landesdatenschutzzentrum vom 17.04.2013, https://www.datenschutzzentrum.de/polizei/20130417-anschreiben-tkg-bestandsdaten.pdf, 1; vgl. auch Stellungnahme vom März 2013 des Deutschen Anwaltvereins durch den Ausschuss Gefahrenabwehrrecht, http://anwaltverein.de/downloads/Stellungnahmen-11/DAV-SN17-13.pdf, 14.

richterlicher Anordnung nach Maßgabe des § 100g StPO identifiziert werden („Zielwahlsuche“). Erfolgt der Anruf dagegen unter Verwendung eines anonymen Internettelefoniedienstes (z.B. Skype), so soll die Identifizierung des Anrufers anhand bekannter Verbindungsdaten (IP-Adresse, Zeit) ohne richterliche Anordnung und bereits zur Aufklärung des Verdachts einer „erheblichen“ Ordnungswidrigkeit oder Bagatellstraftat zulässig sein. Sendet jemand ohne Rufnummernübermittlung ein Telefax, so darf seine Anonymität im Wege einer Zielwahlsuche nur mit richterlicher Anordnung nach Maßgabe des § 100g StPO aufgehoben werden. Wird dasselbe Dokument dagegen über ein anonymes E-Mail-Postfach versandt, so soll die Identifizierung des Anschlussinhabers anhand der verwendeten und in der E-Mail enthaltenen IP-Adresse ohne richterliche Anordnung und bereits zur Aufklärung des Verdachts einer „erheblichen“ Ordnungswidrigkeit oder Bagatellstraftat zulässig sein. Die Privilegierung einer Internet-Zielwahlsuche gegenüber einer Telefon-Zielwahlsuche ist sachlich nicht zu rechtfertigen. Auch 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 Kommunikationsteilnehmers.

Das Argument, im Rahmen einer Bestandsdatenauskunft würden intern verarbeitete Verkehrsdaten nicht mitgeteilt, stellt allein auf die Art der verarbeiteten Daten ab. Seit dem Volkszählungsurteil ist aber anerkannt, dass für die Eingriffstiefe nicht die Art der verarbeiteten Daten entscheidend ist, sondern deren Nutzbarkeit und Verwendungsmöglichkeiten.[1] Dass die Zuordnung einer IP-Adresse zur Aufdeckung der gesamten Internetnutzung während der maßgeblichen Verbindung genutzt werden kann, ist bereits ausgeführt worden.

Das Argument, Bestandsdatenauskünfte beschränkten sich auf punktuelle Informationen, überzeugt im Hinblick auf § 113 TKG nicht: So kann die Zuordnung einer dynamischen IP-Adresse die inhaltliche Rekonstruktion der gesamten Internetsitzung anhand von Nutzungsdaten (z.B. URL, „Referer“) und somit die Erstellung tiefgreifender Persönlichkeitsprofile ermöglichen, wie sie bei Telefon-Verbindungsdaten nicht erstellt werden können. Sogenannte „Cookies“ erlauben die Verfolgung des Nutzers anhand eines Pseudonyms („Identifier“) über Jahre hinweg; die „punktuelle“ Identifizierung eines Nutzungsvorgangs erlaubt dann die Zuordnung der gesamten früheren und zukünftigen Nutzung des Angebots (z.B. der Suchmaschine „Google“). Viele Internetdienste setzen von vornherein eine Registrierung voraus, wobei das gesamte Nutzungsverhalten aufgezeichnet und dem Profil zugeordnet wird (z.B. bei dem Kurznachrichtendienst Twitter oder vielen Internetforen). Die Nutzerkonten werden allerdings aus Datenschutzgründen vielfach unter einem Pseudonym registriert. Erst die Identitätsauskunft anhand der IP-Adresse des Nutzers ermöglicht die namentliche Zuordnung des Profils und damit die direkt personenbezogene Durch-

–1– BVerfGE 65, 1, 45.

leuchtung seines Lese-, Such- und Schreibverhaltens auf dem Dienst. Die für die verfassungsrechtliche Beurteilung entscheidende[1] Nutzbarkeit der Zuordnung einer IP-Adresse ist also sehr hoch.

Soweit das Bundesverfassungsgericht 2010 noch anführte, die §§ 11 ff. TMG verpflichteten Internet-Diensteanbieter grundsätzlich zur Löschung von nicht für die Abrechnung erforderlichen Nutzungsdaten,[2] entspricht dies bei zutreffender Auslegung des Begriffs des Personenbezugs zwar der deutschen Rechtslage, aber leider nicht der Realität. Schon in Deutschland werden diese Vorschriften des Telemediengesetzes in der Praxis verbreitet nicht angewandt und von den Aufsichtsbehörden nicht durchgesetzt. Nach einer Umfrage des Bundesdatenschutzbeauftragten[3] zeichnen selbst Bundesministerien und -behörden bei ihren Internetportalen vielfach das Nutzungsverhalten samt identifizierbarer IP-Adresse auf, ohne dass der Bundesdatenschutzbeauftragte dies auch nur zum Anlass für eine förmliche Rüge genommen hätte. Verbreitet rechtfertigen Anbieter diese Praxis auch mit der Behauptung, der hinter einer IP-Adresse stehende Anschlussinhaber sei für sie nicht bestimmbar (§ 3 Abs. 1 BDSG) und das Datenschutzrecht daher nicht anwendbar (sog. „relativer" Begriff der Bestimmbarkeit). Diese Theorie hält sich in Teilen der Rechtsprechung[4] und selbst in Standardkommentaren[5] hartnäckig. Für die größten, im Ausland ansässigen Anbieter wie Google, Facebook oder eBay gilt das deutsche Telemediengesetz von vornherein nicht. Diese Anbieter erteilen gleichwohl grenzüberschreitend Auskünfte an deutsche Behörden über Internet-Nutzungsprotokolle und ermöglichen diesen dadurch den Nachvollzug potenziell jedes Klicks und jeder Eingabe eines Internetnutzers noch nach Monaten. Alleine der Anbieter Google erhielt 2012 von deutschen Behörden über 3.000 Auskunftsersuchen zu Nutzerdaten, welche sich auf fast 4.000 Nutzer bezogen. Auskünfte erteilt wurden immerhin in über 1.000 Fällen.[6] § 15 TMG könnte ohnehin wegen der geplanten Datenschutz-Grundverordnung der EU, die eine „Vollharmonisierung" anstrebt, vor der Aufhebung stehen. Die Realität ist also, dass fast alle Telemedienanbieter Nutzungsdaten auf Vorrat speichern. Dasselbe gilt für Anbieter von Internet-Kommunikationsdiensten (z.B. E-Mail, Internettelefonie, Internetchat, Internetforen). Hinzu kommt, dass ersichtlich ausländische Geheimdienste sämtliche grenzüberschreitende Internetnutzung auf Verkehrs- und Nutzungsdaten („Metadaten") hin filtern und diese zeitlich unbegrenzt auf Vorrat speichern, offenbar auch an deutsche Behörden weiter geben. Einzig wirksamer und realistischer Schutz der Vertraulichkeit unseres Informations- und Kommu-

–1– BVerfGE 65, 1, 45.

–2– BVerfG, 1 BvR 256/08 vom 2.3.2010, Abs. 270.

–3– http://daten-speicherung.de/data/bfdi_umfrage_surfprotokollierung.pdf.

–4– OLG Hamburg, MMR 2011, 281; LG Wuppertal, MMR 2011, 65; AG München, 133 C 5677/08 vom 30.09.2008; VG Düsseldorf, 27 L 990/09 vom 17.07.2009.

–5– Gola/Schomerus, § 3 Rn. 10; Spindler, Gerald/Schuster, Fabian, Recht der elektronischen Medien Kommentar, 2. Auflage 2011, § 11 TMG Rn. 8.

–6– https://www.google.com/transparencyreport/userdatarequests/DE/.

nikationsverhaltens im Internet ist vor diesem Hintergrund die anonyme Internetnutzung. Nur diese kann bei deutschen Internet-Zugangsanbietern realistischerweise garantiert werden.

Das Bundesverfassungsgericht hat 2010 weiter argumentiert, es bestehe ein gesteigertes Interesse an der Möglichkeit, Kommunikationsverbindungen im Internet zum Rechtsgüterschutz oder zur Wahrung der Rechtsordnung den jeweiligen Akteuren zuordnen zu können. Gesteigert im Vergleich zu unmittelbarer Kommunikation oder zur Telefonnutzung wäre das Identifizierungsinteresse im Internet aber nur, wenn die durchschnittliche Internetverbindung häufiger zu Rechtsverletzungen eingesetzt würde als die durchschnittliche Telefonverbindung oder das durchschnittliche persönliche Gespräch. Dafür ist indes nichts ersichtlich oder gar empirisch belegt. Alleine die Tatsache, dass sich das Medium Internet zunehmend durchsetzt und dadurch naturgemäß die absolute Zahl der hier begangenen Straftaten im gleichen Maß steigt wie die Dauer der Nutzung des Mediums, rechtfertigt es nicht, von den sonst gültigen Eingriffsgrenzen abzugehen. Bei einer solchen Rechnung bliebe unbeachtet, dass die absolute Zahl der registrierten Straftaten seit Jahren fällt, die steigende Zahl registrierter Straftaten im Internet also eine bloße Verlagerung von Kriminalität in moderne Kommunikationsformen darstellt. Bei einer insgesamt fallenden Zahl von Delikten würde es dem Grundgesetz nicht gerecht, eine bloße Kriminalitätsverlagerung zur Rechtfertigung geringerer Eingriffsschwellen heranzuziehen. Dies würde zu einer zunehmenden Aushöhlung und Verminderung des Grundrechtsschutzes führen, anstatt ihn auf neue technische Medien möglichst ungeschmälert zu übertragen, wie es dem Zweck der Grundrechte alleine gerecht wird.

Von einem rechtsfreien Raum wäre das Internet auch dann weit entfernt, wenn man die Identität des Nutzers ebenso schützt wie die sonstigen Umstände der Telekommunikation. Verschiedene Rechtsordnungen unterwerfen seit jeher Bestands- und Verkehrsdaten als „Kommunikationsdaten“ demselben einheitlichen Schutz und identischen Eingriffsschwellen. Niemand würde deswegen ernstlich das Internet in diesen Nachbarstaaten als rechtsfreien Raum bezeichnen. Es ist nicht einmal belegt, dass ein einheitlicher Schutz für Kommunikationsdaten überhaupt eine statistisch nachweisbare, negative Auswirkung auf Aufklärungsquote oder Kriminalitätsrate hätte. Umgekehrt übersteigt die Aufklärungsquote bei Internetdelikten die allgemeine Aufklärungsquote deutlich. Dies gilt auch in vergleichbaren Deliktsfeldern (z.B. Internetbetrug vs. Betrug, Datenveränderung vs. Sachbeschädigung).

Selbst die maßlose EU-Richtlinie 2006/24 zur verdachtslosen Vorratsspeicherung jeglicher Kommunikationsdaten hat die Identität von Internetnutzern demselben Schutz unterworfen wie Verkehrsdaten; beide sollten nur „zum Zwecke der Ermittlung, Feststellung und Verfolgung von schweren Straftaten“ verfügbar gemacht werden. Die Richtlinie behandelte „die zur Rückverfolgung und Identifizierung der Quelle und des Adressaten“ erforderlichen Daten nicht anders als sonstige Kommunikati-

onsdaten. Auch der EuGH hat bei der Würdigung der Richtlinie und ihrer Eingriffstiefe keine Abstriche betreffend die Identifizierung der Internetnutzung gemacht.[1]

Soweit das Urteil des Bundesverfassungsgerichts vom 2. März 2010 demgegenüber noch ausführt, die Offenlegung der Zuordnung einer Internetkennung habe ein erheblich weniger belastendes Gewicht als eine Offenlegung nahezu vollständig gespeicherter Daten sämtlicher Telekommunikationsverbindungen,[2] kann diesem Vergleich nicht beigetreten werden. Die Offenlegung nahezu vollständig gespeicherter Daten sämtlicher über einen Anschluss hergestellter Telekommunikationsverbindungen ist nämlich weitgehend bedeutungslos, solange die Identität des Anschlussinhabers nicht bekannt ist. Gerade die Aufhebung dieser Anonymität ermöglicht § 113 TKG in Verbindung mit den fachrechtlichen Zugriffsnormen in ausufernder Weite. Dass im Internet verbreitet freiwillig eine nahezu vollständige Speicherung der gesamten Telemediennutzung in sogenannten „Logfiles“ erfolgt und diese – anders als Verbindungsdaten – auch nicht dem Schutz des Fernmeldegeheimnisses unterliegen, ist bereits ausgeführt worden. Vor dem Hintergrund kooperationswilliger Telemedienanbieter, die nicht dem Fernmeldegeheimnis verpflichtet sind, stellt § 113 TKG regelmäßig den einzigen Schutz des Internetnutzers vor der potenziell vollständigen Aufdeckung seiner Nutzung eines Telemediums dar. Im Übrigen verkennt der Vergleich des Bundesverfassungsgerichts, dass § 100g StPO nicht nur für die vollständige Offenlegung sämtlicher Telekommunikationsverbindungen gilt, sondern auch etwa für die Mitteilung unbedeutender Verbindungsdetails zu bereits bekannten Verbindungen. Unter Berücksichtigung dessen ist nicht zu vermitteln, weshalb die zentrale Frage der Identität eines Kommunikationsteilnehmers geringeren verfassungsrechtlichen Schutz genießen sollte als unbedeutendste Verbindungsdetails. Dass § 100g StPO einerseits und § 113 TKG andererseits alleine nach der Art der zu beauskunftenden Daten unterscheiden, deren vergleichbare Nutzbarkeit und Verwendungsmöglichkeiten aber ignorieren, ist verfassungsrechtlich nicht haltbar. Insbesondere die Identität der Kommunikationsteilnehmer und der Inhaber der genutzten Internetanschlüsse ist integraler Bestandteil der Internetnutzung und nicht weniger schutzwürdig als diese selbst ist.

Mit Urteil vom 2. März 2010 ist das Bundesverfassungsgericht noch zu der Auffassung gelangt, die staatliche Identifizierung von Internetnutzern unterliege geringeren verfassungsrechtlichen Anforderungen als die Erhebung des Inhalts oder der sonstigen Umstände einzelner Kommunikationsvorgänge.[3] Dies ist unter den heutigen und in Zukunft absehbaren Bedingungen nicht mehr aufrechtzuerhalten. Die einzige Möglichkeit, die Vertraulichkeit von Inhalt und näheren Umständen der persönlichen Internetnutzung zu gewährleisten, ist faktisch der Schutz der Anonymität der Internetnutzung. Zur Wahrung des Verhältnismäßigkeitsgebots muss daher eine Gleich-

–1– NVwZ 2014, 709.

–2– BVerfG, 1 BvR 256/08 vom 02.03.2010, Abs. 257.

–3– BVerfG, 1 BvR 256/08 vom 2.3.2010, Abs. 254.

stellung mit sonstigen Eingriffen in das Fernmeldegeheimnis erfolgen.

3.1.8.3. Die landesgesetzliche Regelung

§ 180a Abs. 2 S. 2 LVwG erlaubt die Identifizierung von Internetnutzern „zur Abwehr einer im einzelnen Falle bevorstehenden Gefahr für Leib, Leben oder Freiheit einer Person sowie zur Abwehr einer gegenwärtigen Gefahr eines gleichgewichtigen Schadens für Sach- oder Vermögenswerte oder für die Umwelt“. Abgesehen von dem unverhältnismäßig weiten Begriff der „bevorstehenden Gefahr“ (siehe oben) unterschreitet der Gesetzgeber die Voraussetzungen anderer Eingriffe in das Fernmeldegeheimnis bei weitem. Diese setzen nämlich voraus, dass die Datenerhebung zur Abwehr einer „gegenwärtigen Gefahr für Leib, Leben oder Freiheit einer Person ... unerlässlich“ ist (§ 185a LVwG). Diese Anforderungen müssen auch für die Identifizierung der Internetnutzung gelten. § 180a Abs. 2 S. 2 LVwG erscheint im Übrigen widersprüchlich, da ein „Schaden für Sach- oder Vermögenswerte oder für die Umwelt“ nie einer Verletzung von Leib, Leben oder Freiheit einer Person „gleichgewichtig“ ist. Die Einbeziehung auch von Sach- und Umweltschäden ist im Übrigen grob unverhältnismäßig.

3.1.9. Soziale Netzwerke und Internetdienste (Telemedien)

§ 180a Abs. 4 LVwG verpflichtet Anbieter sozialer Netzwerke und anderer Telemedienendienste erstmals, zur Abwehr jeglicher (auch nicht gegenwärtiger) im einzelnen Falle bevorstehenden Gefahr für Leib, Leben oder Freiheit einer Person sowie zur Abwehr einer gegenwärtigen Gefahr eines gleichgewichtigen Schadens für Sach- oder Vermögenswerte oder für die Umwelt ohne richterliche Anordnung Auskunft über Bestandsdaten der Nutzer, über „die Identifikation der Nutzer“ und über „das Datum und die Uhrzeit des Beginns und Endes der Nutzung“ zu erteilen.

Die Datenerhebungsvorschriften begründeten zuvor keine Auskunftspflicht über Informationen betreffend Internetnutzer. Eine Auskunftspflicht über Daten bestand nach der Rechtsprechung des Bundesverfassungsgerichts nur unter den Voraussetzungen, unter denen Datenträger sicher gestellt werden konnten, also nach schleswig-holsteinischem Landesrecht (§ 210 LVwG) dann, wenn dies erforderlich war,

1. zur Abwehr einer gegenwärtigen Gefahr für die öffentliche Sicherheit,
2. zur Verhinderung einer missbräuchlichen Verwendung durch eine Person, die in Gewahrsam genommen worden ist, oder
3. um die Eigentümerin oder den Eigentümer oder die rechtmäßige Inhaberin oder den rechtmäßigen Inhaber der tatsächlichen Gewalt vor Verlust oder Beschädigung einer Sache zu schützen.

3.1.9.1. Tiefe des Grundrechtseingriffs

Der von § 180a Abs. 4 LVwG eröffnete Zugriff auf Bestandsdaten der Nutzer von Telemedien, insbesondere Internetdiensten, greift tief in die Privatsphäre ein:

- Die Vorschrift ermöglicht die Aufdeckung polizeibekannter Pseudonyme (z.B. Benutzernamen), so dass sich die gesamte Aktivität eines Nutzers rückverfolgen lässt, beispielsweise alle in einem Internet-Meinungsforum oder in einem sozialen Netzwerk veröffentlichten oder kommentierten Nachrichten.
- Die Vorschrift ermöglicht es auch, sich zu einer namentlich bekannten Person ihre Pseudonyme mitteilen zu lassen.
- Neben Pseudonym, Identität und Abrechnungsdaten des Nutzers speichern Telemedienanbieter je nach Dienst noch sehr viel weiter reichende Bestandsdaten wie Beziehungsstatus, sexuelle Orientierung oder Religion. Bestandsdaten sind gerade auf dem Gebiet von Telemedien sehr sensibel, denn Telemedien haben das Angebot bestimmter Inhalte zum Gegenstand. Schon die Information, welche Telemedien eine bestimmte Person in Anspruch nimmt, kann weit reichende Rückschlüsse auf ihre politischen, finanziellen, sexuellen, weltanschaulichen, religiösen oder sonstigen persönlichen Interessen und Neigungen zulassen. So kann man aus dem Gegenstand bestimmter Dienste (z.B. Selbsthilfeforen) Schlüsse auf auf eine Missbrauchserfahrung, auf gewalttätige Ehepartner, auf psychische Krankheiten oder auf Suchtabhängigkeiten wie Alkoholismus ziehen.
- Anders als die Strafprozessordnung sieht § 180a Abs. 4 LVwG keinerlei Schutz der Seelsorge, der Suchtberatung, der Schwangerschaftskonfliktberatung, der Presseinformanten oder des Berufsgeheimnisträgern Anvertrauten vor.
- Aufgrund seiner weiten Fassung ermöglicht es § 180a Abs. 4 LVwG, erforderlichenfalls sogar eine Liste sämtlicher Nutzer eines Dienstes samt ihrer Angaben herauszuverlangen („die Identifikation der Nutzer“).
- Zu den Bestandsdaten zählen möglicherweise auch vom Nutzer vergebene Passwörter, die der Polizei direkten Zugang zu den vertraulich gespeicherten geschäftlichen oder privaten Daten des Nutzers (z.B. Texte, Dokumente, Fotos, Videos) eröffnen.

Was § 180a Abs. 4 LVwG mit „Identifikation der Nutzer“ meint ist, ist unklar. Da es sich nicht um Bestandsdaten handeln soll, ist möglicherweise die genutzte Internetkennung (IP-Adresse) als Nutzungsdatum gemeint. Hier dürfte ein Verstoß gegen das Gebot der Normenklarheit vorliegen.

§ 180a Abs. 4 LVwG erlaubt auch einen Zugriff „auf das Datum und die Uhrzeit des Beginns und Endes der Nutzung“. Das Auskunftsverlangen muss sich nach dem

Gesetz nicht auf einen konkreten Nutzungsvorgang beschränken, so dass eine Liste sämtlicher Nutzungszeitpunkte eines Nutzers herausverlangt werden kann. Die Polizei muss nach dem Gesetz nicht einmal einen konkreten Nutzer benennen (anders als etwa nach § 100b StPO). Damit könnte ungezielt Auskunft über sämtliche Nutzer eines Dienstes verlangt werden.

Die Identifizierung von Internetnutzern anhand von Bestandsdaten stellt einen besondern schwerwiegenden Grundrechtseingriff dar, weil sie die personenbezogene Nachverfolgung des Inhalts der abgerufenen oder geschriebenen Texte und Daten im Internet erlaubt. Während traditionell die Kenntnisnahme von, Suche nach und Verteilung von Meinungen und anderen Informationen nirgendwo festgehalten wurde (z.B. Gespräch, Flugblätter und Aushänge, Bücher, Zeitungen und Zeitschriften, Radio und Fernsehen), erfordert das Internet eine eindeutige Adressierung von Informationen und erlaubt erstmals eine personenbezogene Erfassung des gesellschaftlichen Meinungs- und Informationsaustauschs.

Wer wann welche Informationen im Internet liest, schreibt oder sucht, ist eine äußerst sensible Information. Sie lässt regelmäßig Rückschlüsse auf die Lebenssituation und Probleme, auf die Persönlichkeit und Vorlieben, auf die politische Meinung und Betätigung, auf Krankheiten und das Sexualleben zu. Derartiges Wissen verleiht Macht über die Betroffenen (z.B. Erpressbarkeit). Da sich immer größere Teile des Lebens - gerade in der jüngeren Generation - in das Internet verlagern, das Netz vielfach schon zum ständigen Begleiter geworden ist, gibt unsere Internetnutzung potenziell Aufschluss über unser gesamtes Leben, vor allem aber auch über unsere Gedankengänge. Anhand der Daten einer Suchmaschine ist nachgewiesen worden, dass die Beobachtung unserer Interessen über einen gewissen Zeitraum hinweg Aufschluss über ganze Lebensgeschichten und Schicksale geben kann.

Für Telemedien-Bestandsdaten hat der Gesetzgeber betont, dass sie nicht weniger schutzwürdig sind als Nutzungsdaten.[1] Erst Bestandsdaten ermöglichen es, Informationen über die Nutzung von Telemedien einer Person zuzuordnen.

3.1.9.2. Verhältnismäßigkeitsgebot

Die Erforderlichkeit des § 180a Abs. 4 LVwG zu den im Gesetzgebungsverfahren genannten Zwecken ist zu verneinen. § 180a Abs. 4 LVwG geht weit über die zur Begründung genannten Fälle der Identifizierung des Urhebers einer konkreten Suizid- oder Bombendrohung im Internet hinaus, weil er nicht auf die im Einzelfall erforderliche Identifizierung von Personen beschränkt ist, von denen eine gegenwärtige Gefahr für Leib oder Leben ausgeht.

Mindestens eine solche Beschränkung wäre aus Gründen der Verhältnismäßigkeit

–1– BT-Drs. 14/6098, 1 (29): „Hier besteht eine gleichwertige Interessenlage sowohl hinsichtlich der Nutzungsdaten als auch hinsichtlich der Bestandsdaten“.

zu fordern, nachdem Informationen über die Internetnutzung vergleichbar sensibel sind wie Informationen über den Inhalt von Telefongesprächen. Die Nutzbarkeit und Verwendungsmöglichkeiten von Informationen über unsere Internetnutzung geht weit über die Sensibilität von Telefon-Verbindungsdaten hinaus: Schon vom Umfang der Nutzungsdaten her, die jeweils durch das Aufrufen von Internetseiten anfallen, ist sie aussagekräftiger als eine Verbindungsdatenabfrage, die nur einen Datensatz pro Verbindung liefert. 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. Telemedien-Nutzungsdaten geben damit zugleich Auskunft über den Inhalt der Internetnutzung. Die für das Telefongespräch geltende Unterscheidung von äußerlichen Verbindungsdaten und Gesprächsinhalten löst sich hier auf. Wird der Besucher einer bestimmten Internetseite individualisiert, weiß man nicht nur, mit wem er Kontakt hatte, sondern kennt in der Regel auch den Inhalt des Kontakts.[1] Nutzungsdaten bleiben nicht punktuell, sondern können vielfach sitzungsübergreifend miteinander verkettet werden. So können ein Benutzerkonto, ein „Cookie“ oder ein „Browser-Fingerabdruck“ die Verknüpfung des Nutzungsverhaltens einer Person ermöglichen. Dies ist auch angebotsübergreifend möglich (z.B. mithilfe eingebundener Werbebanner, Like-Buttons oder „Browser-Toolbars“).

Der Gesetzgeber hat dieser extrem hohen Aussagekraft unserer Nutzung elektronischer Medien dadurch Rechnung tragen wollen, dass er die Entstehung von Aufzeichnungen darüber von vornherein verhindern wollte (§ 15 Abs. 1 TMG). Dieser richtige nationale Ansatz hat sich leider europaweit und erst recht weltweit nicht durchsetzen lassen, was in Anbetracht der weltweit vernetzten Internetarchitektur von zentraler Bedeutung ist. Auch in Deutschland entfaltet das Protokollierungsverbot kaum noch praktische Wirksamkeit. Vor dem Hintergrund des globalen Internets bedeutet dies, dass sich die Vertraulichkeit der Internetnutzung nur durch Gewährleistung der Anonymität des Nutzers und durch Einschränkung des staatlichen Zugriffs auf vorhandene Aufzeichnungen schützen lässt.

Sind Eingriffe in die Vertraulichkeit unserer Telemediennutzung demzufolge ebenso schwerwiegend wie eine Aufzeichnung unserer Telefongespräche oder SMS, so ist zu beachten, dass das schleswig-holsteinische Landesrecht präventive Eingriffe in das Fernmeldegeheimnis nur zur Abwehr einer gegenwärtigen Gefahr für Leib, Leben oder Freiheit einer Person erlaubt (§ 185a LVwG). Es ist nicht ersichtlich, warum die staatliche Befugnis zur Offenlegung der Internetnutzung weiter reichen dürfte als die Befugnis zur Offenlegung der Telefonnutzung.[2] Die entsprechende Anwendung der Regelungen über die Telekommunikationsbestandsdaten wird den

–1– BVerfGE 125, 260, 342, Abs. 259.

–2– Ebenso bezogen auf Telemedien-Nutzungsdaten ULD, Umdruck 18/1245, S. 2.

grundlegenden Unterschieden zwischen beiden Diensten nicht annähernd gerecht.[1]

Am Rande sei in Frage gestellt, ob die bloße Ankündigung eines Suizids überhaupt den Verdacht einer Gefahr begründet, weil ein vom freien Willen getragener Suizid keine Störung der öffentlichen Ordnung darstellt. Im Fall einer Bombendrohung kann bereits auf der Grundlage der Strafprozessordnung ermittelt werden und bedarf es keiner präventiven Eingriffsbefugnis. Sogenannte Rechtsrock-Konzerte dürften per se ebenfalls noch keine konkrete Gefahr begründen. Wenn solche Konzerte im Internet angekündigt werden, verfügt die Polizei ohnehin schon über die erforderlichen Informationen, ohne dass eine Datenabfrage erforderlich wäre.

Die Furcht vor Ermittlungen oder sonstigen Nachteilen infolge der Internetnutzung beeinträchtigt die unbefangene Nutzung des Mediums, das in bestimmten Bereichen nur im Schutz der Anonymität in Anspruch genommen wird (z.B. medizinische, psychologische oder juristische Beratung, Presseinformanten und Whistleblower, politischer Aktivismus). Der Bedeutung von Bestandsdaten als Grundlage und Voraussetzung der Nutzung von Internetdiensten 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 unter besonderen Voraussetzungen beschlagnahmt werden dürfen.

Abschließend sei darauf hingewiesen, dass aus den genannten Gründen auf Bundesebene eine Befugnis zum Zugriff auf Daten von Internetnutzern bewusst nicht eingeführt worden ist.[2]

3.1.9.3. Gebot der Normenklarheit

Was § 180a Abs. 4 LVwG mit „Identifikation der Nutzer“ meint ist, ist unklar. Hier dürfte ein Verstoß gegen das Gebot der Normenklarheit vorliegen.

Die Auskunft über Telemediendaten soll sich § 180a Abs. 4 LVwG zufolge nach den Vorschriften über die Telekommunikations-Bestandsdatenauskunft richten. Welche dieser Vorschriften aber auf welche Anfrage Anwendung finden sollen, ist unbestimmt. Was ist beispielsweise im Internet die Entsprechung von Zugriffen auf Endgeräte oder auf „räumlich davon getrennte Speichereinrichtungen“ (§ 180a Abs. 2 S. 1 LVwG)? Ist das Passwort zu einem Facebook-Konto oder zu einem Meinungsforum davon erfasst, obwohl es sich nicht um Speicherdienste handelt? Auch was die Entsprechung zu einer Auskunft über die Identität der Nutzer von IP-Adressen sein soll (§ 180a Abs. 2 S. 2 und 3 LVwG), ist vollkommen unbestimmt. Die pauschale Bezugnahme auf Regelungen betreffend Telekommunikationsdienste wird den anders gestalteten und weitaus sensibleren Internetdiensten samt ihrer Nutzer offen-

–1– ULD, Umdruck 18/1245, S. 2 f.; Neue Richtervereinigung, Umdruck 18/1250, S. 2.

–2– Argumentationspapier des Bundesjustizministeriums vom 31.10.2012, http://www.cr-online.de/2012-31-10_Argumentationspapier_zum_Gesetzentwurf.pdf.

sichtlich nicht gerecht.

3.2. § 8a Abs. 1 des Landesverfassungsschutzgesetzes

3.2.1. Eingriffsschwelle der Erforderlichkeit zur Aufgabenerfüllung

§ 8a Abs. 1 LVerfSchG eröffnet dem Verfassungsschutz Zugriff auf Bestandsdaten allgemein „zur Erfüllung [seiner] Aufgaben“. Nach § 1 ist Aufgabe des Verfassungsschutzes ganz allgemein, die Landesregierung und andere zuständige Stellen über Gefahren für die freiheitliche demokratische Grundordnung, den Bestand und die Sicherheit des Bundes und der Länder zu unterrichten.

Das Bundesverfassungsgericht hat schon früh entschieden, dass eine hinreichend normenklare Zweckbestimmung fehlt, wenn die Verarbeitung zu anderen Zwecken erhobener personenbezogener Daten pauschal „zur Erfüllung der gesetzlichen Aufgaben“ einer Behörde erlaubt wird und nicht klar festgelegt wird, „um welche konkreten, klar definierten Zwecke es sich dabei handelt“.[1] Nach der neueren Rechtsprechung des Bundesverfassungsgerichts ist im Bereich der Nachrichtendienste Voraussetzung einer verhältnismäßigen staatlichen Bestandsdatenerhebung, dass diese „zur Aufklärung einer bestimmten, nachrichtendienstlich beobachtungsbedürftigen Aktion oder Gruppierung geboten sein muss“.[2] Hinter dieser verfassungsrechtlich geboteten Eingriffsschwelle bleibt § 8a Abs. 1 S. 1 LVerfSchG zurück und es fehlt an einer klaren Zweckbestimmung, so dass das Verhältnismäßigkeitsgebot verletzt ist.

3.2.2. Fehlende Beschränkung auf Einzelfälle

§ 8a Abs. 1 LVerfSchG fehlt die verfassungsrechtlich gebotene Bestimmung, dass Auskünfte über Telekommunikationsdaten nur „im Einzelfall“ eingeholt dürfen und nicht routinemäßig oder massenhaft. Zur näheren Begründung wird auf die diesbezüglichen Ausführungen zu § 180a LVwG Bezug genommen.

3.2.3. Fehlende Beschränkung auf Störer

§ 8a Abs. 1 LVerfSchG geht auch insofern unverhältnismäßig weit als die Aufgabenerfüllung zum Anlass genommen werden kann, Bestandsdaten (einschließlich Zugangscodes und IP-Auskünfte) über Personen zu erheben, die für etwaige Gefahren für die freiheitliche demokratische Grundordnung, den Bestand und die Sicherheit des Bundes und der Länder gar nicht verantwortlich sind. Absatz 4 beschränkt nur die Auskünfte nach Absatz 2 auf bestimmte Personengruppen, ohne dass eine Rechtfertigung für diese Unterscheidung ersichtlich ist.

–1– BVerfGE 65, 1 (66 f.).

–2– BVerfG, 1 BvR 1299/05 vom 24.1.2012, Abs. 177.

3.2.4. Mangelnder Rechtsschutz wegen fehlender Benachrichtigung

§ 8a Abs. 1 LVerfSchG sieht die wegen Art. 19 Abs. 4 GG verfassungsrechtlich gebotene Benachrichtigung Betroffener von Datenauskünften nicht vor. Zur näheren Begründung wird auf die diesbezüglichen Ausführungen zu § 180a LVwG Bezug genommen.

3.2.5. Mangelnde Kontrolle durch fehlende Statistik

§ 8a Abs. 1 LVerfSchG sieht trotz seiner Weite keinerlei statistische Erfassung seiner Anwendung vor, obwohl § 113 TKG den Datenzugriff erheblich ausgeweitet hat. Dies genügt dem Verhältnismäßigkeitsgebot nicht.

Nach § 8a Abs. 8 LVerfSchG wird das Parlamentarische Kontrollgremium bislang unter anderem über Zugriffe auf Verkehrsdaten unterrichtet. Die Identifizierung von Internetnutzern und auch die Erhebung von Zugangssicherungscodes greift so tief in die Grundrechte der Betroffenen ein, dass eine Unterrichtung gleichfalls erforderlich ist. Dies gilt erst Recht mit Blick auf die bundesgesetzlich neu eingeführte automatisierte Datenschnittstelle, die eine erhebliche Vereinfachung und dadurch Vervielfachung der Datenzugriffe befürchten lässt.

Entsprechend § 8b Abs. 3 S. 2 Bundesverfassungsschutzgesetz ist daneben eine statistische Unterrichtung des Landtags und der Öffentlichkeit erforderlich. Dies 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 durchgeführt werden.

3.2.6. Mangelnde Klarheit der Befugnisse zur Abfrage von Zugangssicherungscodes

Die gesetzlichen Voraussetzungen einer Anforderung von Zugangssicherungscodes (wie Passwörter, PIN oder PUK) sind in § 8a Abs. 1 S. 3 LVerfSchG nicht normenklar und präzise geregelt.

Zugangssicherungscodes sichern den Zugang zu Endgeräten und Speicherungsein-

richtungen und damit die Betroffenen vor einem Zugriff auf äußerst sensible Inhalte. Die Herausgabe von Zugangssicherungscodes an Behörden nimmt Anbieter und Betroffenem die Kontrolle über Art und Umfang der durchgeführten Überwachung. Daher stellt die Verpflichtung von Anbietern zur Herausgabe von Zugangssicherungscodes einen besonders schwerwiegenden Grundrechtseingriff dar.

Das Bundesverfassungsgericht hat entschieden, dass Staatsbehörden PINs und Passwörter nur anfordern dürfen, wenn die gesetzlichen Voraussetzungen für ihre Nutzung gegeben sind. Der Gesetzgeber hat diese Formulierung einfach in § 8a Abs. 1 S. 3 LVerfSchG übernommen, ohne selbst zu definieren, unter welchen Voraussetzungen er die Nutzung von Zugangssicherungscodes erlauben will. Verfassungsrechtlich verletzt die lapidare Bezugnahme auf „die gesetzlichen Voraussetzungen für die Nutzung der Daten“ das Bestimmtheitsgebot.[1] Sie ermöglicht weder der handelnden Behörde, noch dem verpflichteten Anbieter oder dem kontrollierenden Gericht, mit hinreichender Klarheit zu bestimmen, welche Voraussetzungen vorliegen müssen.

Was die „gesetzlichen Voraussetzungen für die Nutzung der Daten“ sein sollen, erschließt sich weder dem Rechtsanwender noch dem betroffenen Bürger. Es gibt schlichtweg kein Gesetz, welches die Nutzung von Zugangssicherungscodes regelt. Zwar wendet die Rechtsprechung auf diese Frage bestimmte allgemeine Normen an (z.B. Telekommunikationsüberwachung, Beschlagnahme). Dies entbindet den Gesetzgeber aber nicht von seiner Verpflichtung, die jetzt getroffene Regelung normenklar und präzise zu formulieren. Die Entscheidung des Hohen Gerichts, die Voraussetzungen der Datennutzung müssten vorliegen, war nicht als Gesetzestext gedacht, sondern bedarf der normenklaren Umsetzung durch den Gesetzgeber. Im Hinblick auf die extreme Sensibilität persönlicher Zugangskennungen muss die Regelung ein hohes Maß an Normenklarheit gewährleisten.

Es ist aus diesen Gründen verfassungsrechtlich geboten, abschließend zu bestimmen, welche materiellen und formellen gesetzlichen Voraussetzungen für die Nutzung von Zugangscodes vorliegen müssen. Während § 180a LVwG eine solche Regelung vorsieht, ist dies im Fall des Verfassungsschutzes nicht erfolgt.

3.2.7. Fehlende Subsidiarität des Zugriffs auf Zugangssicherungscodes (PINs, Passwörter)

Zur Wahrung des Verhältnismäßigkeitsgebots muss der Vorrang des Datenzugriffs

–1– Ebenso Unabhängiges Landesdatenschutzzentrum, Stellungnahme vom 27.11.2012, https://www.datenschutzzentrum.de/polizei/20121127-stellungnahme-tkg-aenderung.html, Ziff. II.3. und Unabhängiges Landesdatenschutzzentrum vom 17.04.2013, https://www.datenschutzzentrum.de/polizei/20130417-anschreiben-tkg-bestandsdaten.pdf, 2; vgl. auch Stellungnahme vom März 2013 des Deutschen Anwaltvereins durch den Ausschuss Gefahrenabwehrrecht, http://anwaltverein.de/downloads/Stellungnahmen-11/DAV-SN17-13.pdf, 9.

unter Mitwirkung des Anbieters vor dem unmittelbaren Zugriff mithilfe von Zugangssicherungscodes ausdrücklich festgeschrieben werden, was § 8a Abs. 1 S. 3 LVerfSchG nicht tut. Zur näheren Begründung wird auf die diesbezüglichen Ausführungen zu § 180a LVwG Bezug genommen.

3.2.8. Mangelnde Sicherheit erhobener Zugangssicherungscodes

Zu beanstanden ist auch an § 8a Abs. 1 S. 3 LVerfSchG, dass das Gesetz keinerlei Vorkehrung zur Gewährleistung der Sicherheit erhobener Zugangssicherungscodes trifft. Zur näheren Begründung wird auf die diesbezüglichen Ausführungen zu § 180a LVwG Bezug genommen.

3.2.9. Unzureichende Eingriffsschwellen für Identifizierung von IP-Adressen

Die Identifizierung von Internetnutzern (§ 8a Abs. 1 S. 4 LVerfSchG) stellt einen besondern schwerwiegenden Grundrechtseingriff dar, weil sie die personenbezogene Rückverfolgung des Inhalts der abgerufenen oder geschriebenen Texte und Daten im Internet erlaubt. Anders als Auskünfte über Rufnummerninhaber geht die Identifizierung von Internetnutzern anhand einer dynamisch zugewiesenen IP-Adresse mit einem Eingriff in das grundrechtlich besonders geschützte Fernmeldegeheimnis einher.

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.[1] § 8a Abs. 1 LVerfSchG bestimmt weder selbst noch durch normenklare Verweisung, dass der Verfassungsschutz IP-Adressen nur identifizieren darf, wenn aufgrund tatsächlicher Anhaltspunkte von dem Vorliegen einer konkreten Gefahr auszugehen ist. Auch ist nicht bestimmt, dass tatsächliche Grundlagen aktenkundig zu machen sind.

§ 8a Abs. 1 LVerfSchG lässt die Identifizierung von IP-Adressen stattdessen unter denselben weit reichenden Voraussetzungen zu wie „einfache“ Bestandsdatenabfragen. Diese Gleichsetzung ist verfassungsrechtlich unzulässig.[2] Von Verfassungs wegen müssen an die Identifizierung von Internetnutzern dieselben Anforderungen gestellt werden wie an sonstige Eingriffe in das Fernmeldegeheimnis. Zur Begründung wird auf die Ausführungen zur Identifizierung von Internetnutzern bezüglich § 180a LVwG Bezug genommen.

–1– BVerfG, 1 BvR 256/08 vom 2.3.2010, Abs. 261.

–2– Ebenso Unabhängiges Landesdatenschutzzentrum, Stellungnahme vom 27.11.2012, https://www.datenschutzzentrum.de/polizei/20121127-stellungnahme-tkg-aenderung.html, Ziff. II.2.

3.2.10. Soziale Netzwerke und Internetdienste (Telemedien)

Zu § 180a LVwG ist bereits erläutert worden, warum ein Zugriff auf die bei Internetdiensten gespeicherten Nutzerdaten ein besonders tiefgreifender Grundrechtseingriff ist. § 8a LVerfSchG lässt den Zugriff auf diese Daten in unverhältnismäßig weit reichendem Umfang zu. Jedoch ist dies bereits vor Inkrafttreten des angefochtenen Gesetzes der Fall gewesen und kann durch diese Verfassungsbeschwerde daher nicht mehr angegriffen werden.

3.3. § 15 Absatz 5 Satz 4 des Telemediengesetzes

Nach § 15 Abs. 5 S. 4 i.V.m. § 14 TMG dürfen Anbieter von Telemedien auf „Anordnung der zuständigen Stellen ... im Einzelfall Auskunft über Bestandsdaten erteilen, soweit dies für Zwecke der Strafverfolgung, zur Gefahrenabwehr durch die Polizeibehörden der Länder, zur Erfüllung der gesetzlichen Aufgaben der Verfassungsschutzbehörden des Bundes und der Länder, des Bundesnachrichtendienstes oder des Militärischen Abschirmdienstes oder des Bundeskriminalamtes im Rahmen seiner Aufgabe zur Abwehr von Gefahren des internationalen Terrorismus oder zur Durchsetzung der Rechte am geistigen Eigentum erforderlich ist“.

3.3.1. Tiefe des Grundrechtseingriffs

Die Offenlegung unserer Internetnutzung gegenüber staatlichen Stellen greift tief in die Grundrechte auf informationelle Selbstbestimmung, auf freie Information und Meinungsäußerung ein. Die Internetnutzung vieler Menschen ist im Zeitalter von Smartphones nahezu permanent und erfasst praktisch alle Bereiche des Privat- und Geschäftslebens. Nutzbarkeit und Verwendungsmöglichkeiten nach zu urteilen bleibt die Eingriffstiefe eines Zugriffs auf unsere Internetnutzung nicht hinter derjenigen einer Telekommunikationsüberwachung zurück.

Im Fall von Telemedien im Internet ist es besonders wichtig, dass sie ebenso unbefangen und ohne das Risiko einer Beobachtung nutzbar bleiben wie die klassischen Medien (z.B. Bücher, Zeitungen, Flugblätter, Plakate, Radio, Fernsehen). Die Telemedien ersetzen die klassischen Medien immer mehr und sind in vielen Bereichen unseres Lebens schon unverzichtbar geworden (z.B. Internet-Steuererklärung für Gewerbetreibende). Sie sind vielfach Voraussetzung für die Ausübung grundrechtlich geschützter Freiheiten, insbesondere des Rechts, seine Meinung in Wort, Schrift und Bild frei zu äußern und zu verbreiten und sich aus allgemein zugänglichen Quellen ungehindert zu unterrichten (Art. 5 GG). Nur umfassende Informationen, die man ungehindert und unbefangen zur Kenntnis nehmen kann, ermöglichen eine freie Meinungsbildung und -äußerung für den Einzelnen wie für die Gemeinschaft. Nur auf der Grundlage eines freien und unbefangenen Informationszugangs kann der Bürger informiert politische Entscheidungen treffen und am freiheitlichen

demokratischen Gemeinwesen mitwirken.

Aus der hohen Bedeutung der Mediennutzung für unser Gemeinwesen und aus der besonderen Sensibilität von Informationen über unsere Interessen und Vorlieben heraus erklärt sich, dass der Gesetzgeber einen sondergesetzlichen Schutz vor Erfassung unserer Mediennutzung vorgesehen hat. Die §§ 13 und 15 TMG garantieren, dass abrechnungsirrelevante Informationen über unsere Nutzung von Telemedien unmittelbar nach Beendigung des Zugriffs gelöscht werden. Jeder Mensch soll die modernen Medien ebenso unbefangen und anonym nutzen können wie die klassischen Medien. Wer sich aus Büchern, Zeitungen, Flugblättern, Plakaten, Radio oder Fernsehen informiert, kann dies ohne Aufzeichnung seiner Informationsinteressen tun (es findet auch keine Aufzeichnung anhand einer eindeutigen Kennung statt). Telemedien sollen nach dem Willen des Gesetzgebers ebenso anonym nutzbar sein. Ihre große Vielzahl und Spezialisierung ermöglicht sogar noch weit tiefgründigere Einblicke in unsere Persönlichkeit, unser Privatleben, unsere Interessen und Vorlieben als die traditionellen Medien. Dem hat der Gesetzgeber zurecht Rechnung getragen. Leider jedoch greifen die Löschungspflichten in der Praxis kaum, weil sie in Deutschland nicht durchgesetzt werden und auf große internationale Internetkonzernen ohnehin keine Anwendung finden. Vor diesem Hintergrund muss der staatliche Zugriff auf Daten, die eigentlich nicht gespeichert werden dürften, höchsten Eingriffsschwellen unterworfen werden.

Eine staatliche Überwachung unseres Informationsverhaltens würde – in den Worten des Bundesgerichtshofs – „die Gefahr begründen, dass der Einzelne aus Furcht vor Repressalien oder sonstigen negativen Auswirkungen sich dahingehend entscheidet“, von dem Abruf öffentlich zugänglicher Informationen abzusehen. Diese Gefahr besteht etwa dort, wo aus dem Seitenabruf wegen des Inhalts der Seite oder des Telemediums auf politische Meinungen, religiöse Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben des Internetnutzers geschlossen werden kann. Der Bundesgerichtshof hat deswegen ausgesprochen, dass die Vorschriften des Telemediengesetzes ein „Recht des Internetnutzers auf Anonymität“ gewährleisten.

Daten über Nutzer von Telemedien sind keinesfalls weniger sensibel als Daten über die Individualkommunikation der Bürger untereinander, die dem Fernmeldegeheimnis unterliegen. Umgekehrt ist in der Diskussion über die Praktiken der NSA deutlich geworden, dass die im Internet anfallenden „Metadaten“ eine viel weiter reichende Durchleuchtung unseres Lebens erlauben als eine Auswertung des Inhalts von Individualkommunikation. Metadaten lassen sich maschinell verknüpfen und auswerten. Dadurch ermöglichen sie eine Massendatenanalyse sowie die Erstellung von Persönlichkeits- und Interessenprofilen. Telemedien-Nutzungsdaten sich auch deshalb Telekommunikationsinhalten vergleichbar, weil sie ganz regelmäßig den Inhalt der abgerufenen Informationen erkennen lassen (z.B. URLs der gelesenen Inter-

netseiten).

3.3.2. Gebot der Normenklarheit

Bedeutung und Reichweite des § 15 Abs. 5 S. 4 i.V.m. § 14 TMG sind unklar. Der Wortlaut lässt offen, ob die Vorschriften eine Übermittlungsbefugnis der Anbieter, eine Erhebungsbefugnis der genannten Stellen und/oder eine Übermittlungspflicht der Anbieter begründen sollen. Während § 113 TKG eine Übermittlungsbefugnis nur „zur Erfüllung von Auskunftspflichten“ begründet, lässt § 15 Abs. 5 S. 4 i.V.m. § 14 TMG offen, ob er eine spezialgesetzlich begründete Auskunftspflicht voraus setzt. Bei grundrechtsfeindlicher Auslegung können die Vorschriften als Blanko-Übermittlungsbefugnis gelesen werden, die die besonderen Voraussetzungen spezialgesetzlicher Vorschriften über die Auskunftserteilung aushebeln, indem sie Diensteanbietern Auskünfte auch ohne Vorliegen der spezialgesetzlichen Vorschriften erlauben. Insgesamt ist zu konstatieren, dass das Telemediengesetz dem „Doppeltürenmodell“ noch keine Rechnung trägt. Die unklare Rechtsfolge der Vorschriften ist mit dem Gebot der Normenklarheit nicht zu vereinbaren.

In keinem Fall weisen die §§ 14 Abs. 2, 15 Abs. 5 S. 4 TMG die erforderliche Normenklarheit und Regelungsdichte auf, um die Erhebung von Telemedien-Bestands- und Nutzungsdaten durch staatliche Stellen eigenständig zu rechtfertigen. Das Bundesverfassungsgericht hat ausdrücklich entschieden, dass eine hinreichend normenklare Zweckbestimmung fehlt, wenn die Verarbeitung zu anderen Zwecken erhobener personenbezogener Daten pauschal „zur Erfüllung der gesetzlichen Aufgaben“ einer Behörde erlaubt wird und nicht klar festgelegt wird, „um welche konkreten, klar definierten Zwecke es sich dabei handelt“.[1]

Zu unbestimmt sind auch die Worte „Auf Anordnung der zuständigen Stellen“. Welche Stellen damit gemeint sind, ist jedenfalls bei Auskunftsersuchen „zur Durchsetzung der Rechte am geistigen Eigentum“ unklar. Rechteinhaber dürfen keine „Anordnungen“ treffen.

3.3.3. Verhältnismäßigkeitsgebot

Wie bereits ausgeführt, sind Daten über Nutzer von Telemedien nicht weniger sensibel als Daten über die Individualkommunikation der Bürger untereinander, die dem Fernmeldegeheimnis unterliegen. Dementsprechend darf unsere Internetnutzung dem staatlichen Zugriff keinesfalls weiter geöffnet werden als es die Vorschriften über Telekommunikationsüberwachung tun.

Um dies zu gewährleisten, dürfte das Telemediengesetz eine Verwendung anfallender Daten für andere Zwecke, insbesondere die Weitergabe an andere, zunächst einmal nur zulassen, soweit eine gesetzliche Vorschrift dies vorsieht und sich dabei

–1– BVerfGE 65, 1 (66 f.).

ausdrücklich auf Telekommunikationsvorgänge bezieht (vgl. § 88 TKG). Nur wenn eine spezialgesetzliche Erhebungsbefugnis gefordert wird, ist gewährleistet, dass sich der Gesetzgeber darüber Gedanken gemacht hat, welche besonderen Vorkehrungen zum Grundrechtsschutz es im Fall der hochsensiblen Internet-Nutzerdaten bedarf. Eine Heranziehung der allgemeinen Erhebungsbefugnisse[1] wird den Anforderungen der Verhältnismäßigkeitsgebots an Zugriffe auf die Internetnutzung nicht annähernd gerecht. Während § 12 Abs. 2 TMG eine gesetzliche Regelung fordert, „die sich ausdrücklich auf Telemedien bezieht", tun dies die §§ 14 Abs. 2, 15 Abs. 5 S. 4 TMG nicht. Eine Öffnung auch für allgemeine Erhebungsbefugnisse verletzt das Verhältnismäßigkeitsgebot.

Inhaltlich dürfte der Zugriff auf Telemediendaten für Zwecke der Strafverfolgung nur unter den Voraussetzungen, in dem Verfahren und nach Maßgabe der §§ 100a und 100b der Strafprozessordnung zugelassen werden. Im Fall der Nachrichtendienste wäre eine Öffnung allenfalls unter den Voraussetzungen, in dem Verfahren und nach Maßgabe des G10-Gesetzes denkbar, wobei die Erforderlichkeit nicht ersichtlich ist. Im Polizeibereich hat das Bundesverfassungsgericht die Voraussetzungen einer verhältnismäßigen Befugnis zur Telekommunikationsüberwachung bereits geklärt. Die uferlose Öffnung durch die §§ 14, 15 TMG verletzt danach das Verhältnismäßigkeitsgebot.

Ob und in welchem Umfang die Herausgabe von Internetnutzungsdaten an Inhaber von Immaterialgüterrechten oder sonst private Dritte überhaupt zugelassen werden darf und, wenn ja, in welchem grundrechtssichernden Verfahren, muss hier nicht abschließend geklärt werden. Die §§ 14, 15 TMG verletzen insoweit schon deswegen das Verhältnismäßigkeitsgebot, weil sie eine spezialgesetzliche Regelung überhaupt nicht zur Voraussetzungen der Übermittlungsbefugnis machen. Die Blankoermächtigung in § 14 Abs. 2 TMG hebelt die besonderen Voraussetzungen der spezialgesetzlichen Vorschriften über die Auskunftserteilung an Rechteinhaber aus, indem sie Diensteanbietern Auskünfte auch ohne Vorliegen der spezialgesetzlichen Vorschriften erlaubt. Inhaltlich ist es unangemessen, dass zugunsten privater Dritter beliebig über sensible Nutzerdaten verfügt werden darf, wie es § 14 Abs. 2 TMG vorsieht. Auf dem Gebiet der Telemedien wollte der Gesetzgeber zurecht „den erweiterten Risiken der Erhebung, Verarbeitung und Nutzung personenbezogener Daten" in diesem Bereich Rechnung tragen,[2] was die Öffnungsklauseln für Auskunftersuchen offensichtlich nicht tun. Selbst die sogenannte Durchsetzungsrichtlinie 2004/48/EG sieht Auskünfte nur auf richterliche Anordnung und vorbehaltlich des Schutzes personenbezogener Daten vor (Art. 8).

–1– Vgl. Bundesrat, BR-Drs. 556/06 (B), 4 f.

–2– Begründung zum Entwurf des Informations- und Kommunikationsdienste-Gesetzes (IuKDG), BT-Drs. 13/7385.

_____

Angelika Beer

_____

Patrick Breyer

_____

Wolfgang Dudda

_____

Uli König

_____

Sven Krumbeck

_____

Torge Schmidt