Arnold von Bosse

Verfassungsbeschwerde gegen das Bestandsdaten-Auskunftsgesetz Mecklenburg-Vorpommern

Das heimliche Abrufen von elektronisch generierten Telekommunikations-Daten durch Verfassungsschutz und Polizei ist im Telekommunikationsgesetz des Bundes (TKG) und in den entsprechenden Landesvorschriften normiert. Wie wird hier die Balance zwischen Sicherheitsinteressen auf der einen Seite und Schutz der Intimsphäre auf der anderen Seite austariert?

Immerhin geht es einerseits z.B. um das Verhindern eines im Internet angekündigten Selbstmordes oder Amoklaufes, andererseits um die Missbrauchsgefahr, die im staatlich erfolgten Abruf tausendfacher Zugangssicherungscodes (PIN, PUK, Passwörter, Zugang zu E-Mail-Konten oder Cloud-Speichern) liegen kann.

Um das zu überprüfen, ist im Juni 2014 eine durch die Partei Bündnis 90/Die Grünen initiierte Verfassungsbeschwerde beim Landesverfassungsgericht Mecklenburg-Vorpommern in Greifswald eingelegt worden. Der sperrige Name des angegriffenen Gesetzes: „Gesetz zur Änderung des Landesverfassungsschutzgesetzes und des Sicherheits- und Ordnungsgesetzes zur Regelung der Bestandsdatenauskunft v. 2.7.2013“ (Lt-Drucksache 6/1630) – kurz: Bestandsdaten-Auskunftsgesetz M-V (siehe Auszug im grauen Kasten).

Dabei ist schon der Name irreführend und verharmlosend: „Bestandsdaten“ sind z.B. die Adress- und Vertragsdaten (Kundendaten im Sinne der §§ 95, 111 TKG der Telekommunikations-Dienste-Anbieter (Provider)). Diese Daten sind am wenigsten schützenswert und nicht Gegenstand der verfassungsrechtlichen Kritik: Eigentlich hätte das Gesetz „Inhalts- und Verkehrsdaten-Auskunftsgesetz“ heißen müssen. Denn diese Daten sind es, die die geschützte Intimsphäre offen zu legen in der Lage sind: Weil nämlich indirekt durch das im angegriffenen Gesetz erlaubte Abrufen von Zugangssicherungscodes von Handys und Computern auch Inhaltsdaten, z.B. durch Bewegungsprofile, sichtbar werden. Die zweite Daten-Kategorie im angegriffenen Gesetz sind die Verkehrsdaten, zu denen die „dynamischen Internet-Protokoll-Adressen (IP-Adressen)“ gehören. Diese werden dem Internet-Nutzer immer wieder neu beim Aufschlagen einer Homepage zugeordnet: Auch hier sind Rückschlüsse auf Inhalte möglich.

Im Folgenden sollen die wesentlichen Angriffspunkte der Beschwerde aufgezeigt werden. Motivation der Beschwerde war, dass das o.g. Landesgesetz bzgl. des Schutzes der persönlichen Verbindungsdaten hinter ähnlichen Gesetzen aller anderen Bundesländer und des Bundes zurück bleibt.

Die Verfassungsbeschwerde macht geltend, dass die neuen, zum 1.7.2013 in Kraft getretenen Vorschriften des Bestandsdaten-Auskunftsgesetz M-V mit Verweis auf das Landesverfassungsschutz-Gesetz M-V (LVerfSchG) und das Sicherheits- und Ordnungs-Gesetz M-V (SOG) gegen das Datenschutzgrundrecht aus Art. 6 (1) Landesverfassung M-V (LV) und die Rechtsschutzgarantie (Art. 19 (4) Grundgesetz) verstoßen und daher nichtig sind.

Art. 6 (1) LV lautet:
„Jeder hat das Recht auf Schutz seiner personenbezogenen Daten. Dieses Recht findet seine Grenzen in den Rechten Dritter und in den überwiegenden Interessen der Allgemeinheit.“

Art. 6 (1) LV als Datenschutzgrundrecht findet seine Inhaltsbestimmung auch in Art. 10 GG (Fernmeldegeheimnis) und im informationellen Selbstbestimmungsrecht (Art. 2 (1) i. V. m. Art. 1 (1) GG sowie in der speziellen Ausprägung als „Recht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme“.

Die verfassungsrechtlichen Prüfgrundsätze ergeben sich dabei vor allem
- aus dem sog. Vorratsdatenurteil des Bundesverfassungsgerichts (BVerfG) v. 2.3.2010 (1 BVR 256/08)
- und aus dem Beschluss des BVerfG v. 24.1.2012 (1 BVR 1299/05) zur Verfassungswidrigkeit des Abrufes von Daten zu Zugangssicherungs-Codes von Mobiltelefonen und Computern und der Daten zu dynamischen IP-Adressen. Die untenstehend geprüften Landesgesetzes-Änderungen sind in Folge dieser Entscheidung ergangen, um den strengen Vorgaben des BVerfG Genüge zu tun. Diese Vorgaben sind aber im Bestandsdaten-Auskunftsgesetz M-V aus Sicht der Beschwerdeführer (und des Autors, der der Verfasser der Beschwerdeschrift ist) nicht erfüllt.

I. Zum neuen § 24b LVerfSchG

Das Landesverfassungsschutz-Gesetz erlaubt u. a. die vorbeugende Sichtung von Gefahren für den Staat und die Benachrichtigung der Regierung über verfassungsrechtlich relevante Einschätzungen durch den Landesverfassungsschutz.

1. Zur Berechtigung bzgl. des Abrufes von Zugangssicherungs-Codes

a. Die sog. Bestimmtheit der gesetzlichen Regelung, die für den Datenabruf gemäß der Schwellen-Vorgaben des Grundrechts auf Datenschutz in Art. 6 LV-MV gefordert wird, ist unzulänglich: Denn die Zwecke des Abrufes der Daten sind nicht normiert. Die vom BVerfG geforderte Normenklarheit fehlt: Der bloße Verweis auf die „gesetzlichen Voraussetzungen“ reicht nicht. Weder der Bürger, der Anspruch auf Rechtsschutz hat (Art. 19 (4) GG) noch der einfache Poli-

zeibeamte haben im Alltag Kenntnis, welche Vorschriften sich dahinter verbergen.

b. Die Normierung der nachträglichen Mitteilungspflichten, nachdem die Daten zu den Codes abgerufen wurden, fehlt. Sucht man danach, findet man zwar § 2 im Gesetz zur Ausführung des Art. 10-Gesetzes, GVBl.M-V 1992, 486 (Gesetz zur Kontrolle des Verfassungsschutzes, wenn in das Telekommunikations-Geheimnis aus Art. 10 GG eingegriffen wird).

Hier wird aber nur die Pflicht zu Mitteilungen für den Abruf von Daten bei laufender Telekommunikation geregelt. Bzgl. der bereits abgelegten Daten (z.B. auf Mobiltelefonen, wenn das „surfen" beendet ist) gibt es keine nachträglichen Mitteilungspflichten.

Der Eingriff in die Privatsphäre hat aber bzgl. des Abrufes von Daten aus laufender und abgeschlossener Kommunikation eine ähnliche Intensität. Das Fehlen dieser Mitteilungspflichten führt zur Verfassungswidrigkeit von § 24b LVerfSchG bzgl. dieses Aspektes, da der Betroffene nach dem heimlichen Abruf der Daten aufgrund Nichtwissens sich nicht wehren kann (Verstoß gegen Art. 6 LV und Art. 19 (4) GG gem. dem vom BVerfG entwickelten Gebot des „effektiven Rechtsschutzes").

c. Es stellt einen verfassungsrechtlichen Mangel dar, dass ein sog. Richtervorbehalt (also die Vorab-Genehmigung vor dem Eingriff in die Privatsphäre) weder für den Abruf von Daten zur laufender Kommunikation noch beim Abruf von abgelegten Daten geregelt ist.

Im Polizeirecht (beim Drohen von Gefahren, siehe unten) gibt es jedoch den Richtervorbehalt zumindest beim Abruf der Daten zu laufender Kommunikation. Es wäre daher auch im Rahmen der bisherigen landesgesetzlichen Systematik konsequent, dies auch im Verfassungsschutzrecht vorzusehen.

Der Richtervorbehalt ist bei erheblichen Eingriffen verfassungsrechtlich geboten. Gewichtige Stimmen von Verfassungsrechtlern (siehe unten zur Literatur/Stellungnahmen) sind der Auffassung, dass der Richtervorbehalt geboten ist, da es sich beim Abruf von Daten zu Codes und IP-Adressen um intensive Eingriffe in die Privatsphäre handelt. Denn aus den sog. Verkehrsdaten kann oft auch – wie oben dargelegt – auf die Inhalte und schützenswerte persönliche Vorlieben geschlossen werden. Der Richtervorbehalt wird weiter unten nochmals thematisiert.

2. Zur Berechtigung bzgl. des Abrufes von Daten zu dynamischen IP-Adressen

a. Die Bestimmtheit fehlt auch hier, die bloße Bezugnahme auf das Bundesgesetz (§ 113 TKG) reicht nicht. Bei Eingriffen in Grundrechte, z.B. Art. 6 LV, müssen die Voraussetzungen des Eingriffes möglichst genau geregelt sein, damit dem Willkür-Verbot aus Art. 20 (3) GG Genüge getan wird. Auch der Europäische Gerichtshof hat am 8.4.2014 (C-293/12 und C-594/12) den Datenschutz gestärkt, indem er forderte, dass klare Schranken bzgl. des Abrufes von privaten Daten normiert werden (Verhältnismäßigkeits-Grundsatz).

b. Mitteilungspflichten sind (im Gegensatz zu den abgelegten Daten zu Codes) beim Abruf der Daten zu dynamischen IP-Adressen im neuen § 24b des LVerfSchG erfreulicherweise geregelt. Allerdings fehlt auch hier der Richtervorbehalt.

II. Zu § 28a SOG M-V

Das Sicherheits- und Ordnungs-Gesetz betrifft das Handeln der Landespolizei beim Drohen von Gefahren für die öffentliche Sicherheit und Ordnung (z.B. Ankündigung von Stalking oder einem Amoklauf im Internet).

1. Abruf von Zugangssicherungscodes

a. Die Bestimmtheit der Regelung des Abrufes der Codes ist auch hier nicht ausreichend. Der Begriff „konkrete" Gefahr fehlt (Vorgabe des BVerfG). Es wird keine Eingrenzung auf nur „gewichtige Ordnungswidrigkeiten" vorgenommen (Vorgabe des BVerfG). Der bloße Verweis auf die „gesetzlichen Voraussetzungen" reicht nicht.

b. Nachträgliche Mitteilungspflichten sind zwar in § 34a (7) SOG geregelt; dies gilt aber nur für den Abruf von Daten zu laufender Kommunikation. § 28a SOG ist also insofern verfassungswidrig, als die Normierung von Benachrichtigungs-Pflichten nach dem heimlichen Abruf von abgelegten Daten fehlt.

c. Sucht man den Richtervorbehalt, so findet man ihn in § 34a (4) SOG. Aber dieser gilt nicht für den Abruf von schon abgelegten Daten. Die Eingriffsintensität in die Privatsphäre ist aber die gleiche wie bei laufender Kommunikation. § 28a SOG ist also bzgl. dieses Aspektes verfassungswidrig, da die aufgrund des Datenschutzgrundrechts in Art. 6 LV notwendige Schwelle des Richtervorbehaltes als einzelfallbezogene Grundrechtssicherung bei abgelegten Daten fehlt.

2.Abruf von Daten zu dynamischen IP-Adressen

a. Die Bestimmtheit reicht nicht; der genaue Zweck ist nicht benannt, siehe oben.

b. Auch hier fehlt nach Auffassung der Beschwerdeführer der Richtervorbehalt. Allerdings widerspricht sich das BVerfG in seiner o.g. Vorratsdaten-Entscheidung selber (mal wird ein intensiver Eingriff in die Intimsphäre angenommen (Rz. 211), mal wird der Richtervorbehalt mit der Begründung abgelehnt, es handele sich nicht um eine große Eingriffsintensität (Rz. 261)). Zudem formulierte das BVerfG, IP-Adressen seien zwar Verkehrsdaten, aber sie seien nicht so eingriffsintensiv wie bei anderen Verkehrsdaten, da die Verwendung nur „mittelbar" erfolge (Vorratsdaten-Urteil, Rz. 254).

Bzgl. dieses Widerspruchs im Vorratsdaten-Urteil des BVerfG befragte der Verfasser der Beschwerdeschrift den Datenschutzbeauftragten von Berlin, Dix. Dieser antwortete am 15.4.2014 wie folgt:

„Das Gericht hatte in der Vorratsdaten-Entscheidung die Tragweite der IP-Adresse als „Generalschlüssel" zum Kommunikationsverhalten der Internet-Nutzer verkannt (trotz entsprechender Hinweise der Sachverständigen in der

mündlichen Verhandlung). Praktisch läuft die Personalisierung der IP-Adressen so, dass eine Strafverfolgungsbehörde, die IP-Adressen hat, zunächst bei der Bundesnetzagentur nachfragen muss, welcher Provider den entsprechenden Block an IP-Adressen vergeben hat. Der jeweilige Provider teilt der Strafverfolgungsbehörde (oder Gefahrenabwehr-Behörde – Einschub durch Verfasser) dann mit, welchem Nutzer eine bestimmte (meist dynamische, selten statische) IP-Adresse zugewiesen war, wenn der Provider die Daten noch hat (noch nicht gelöscht hat). Dieser Prozess hat offenbar das BVerfG zur Wahl des Attributs „mittelbar" veranlasst."

Es spricht also vieles dafür, die Eingriffsintensität bzgl. des Abrufes von dynamischen IP-Adressen als intensiv einzuordnen – mit der Folge der Notwendigkeit eines Richtervorbehaltes.

Abschließend sei angemerkt, dass die Relevanz der „Bestandsdatenauskunft" nicht zu unterschätzen ist: Immerhin erfolgten 2013 bundesweit durch die Behörden z.B. allein von Google 6000 und von Facebook 4000 Datenabrufe (Transparenz-Berichte 5.5.2014). Im Übrigen muss die Entwicklung der sog. statischen IP-Adressen (Version 6) beobachtet werden, da die technische Entwicklung diesbezüglich zu einem noch tieferen Eingriff in die Privatsphäre führen kann, als bisher vorstellbar. Auch daher bietet es sich an, die Eingriffs-Schwellen-Voraussetzungen als Verfahrenssicherung vorsorglich nicht zu niedrig anzusetzen, um nicht alle 2 Jahre die Gesetze an die rasanten technischen Entwicklungen anpassen zu müssen.

Literatur, Stellungnahmen und ein weiteres Urteil zu der obigen Problematik:

Roggenkamp, Neuregelung zur Bestandsdatenauskunft verfassungswidrig!, NJW-aktuell 21/2013, S. 12

Kugelmann, Dalby, Die Neuregelung der Bestandsdatenauskunft gem. § 113 TKG und die Notwendigkeit des Grundrechtschutzes durch Verfahren, Festschrift für Kutscha, Das Recht in guter Verfassung?, 2013, 114 (Kugelmann gab auch eine ähnlich lautende Stellungnahme im Gesetzgebungsverfahren in M-V ab).

Gusy, Stellungnahme v. 2.5.13 zur Anhörung bzgl. der Änderung des Polizeigesetzes NRW – LT-Drs. 16/2256

Neue Richtervereinigung Schleswig-Holstein, Stellungnahme v. 3.6.2013 zur Anpassung des manuellen Abrufs der Bestandsdaten nach dem TKG, LT-Dr. 18/1713

Albrecht, Stellungnahme v. 8.5.2013 zur Anhörung zum Gesetz zur Änderung des Polizeigesetzes NRW, LT-Drs. 16/2256

BVerfGE 120, 274 (Online-Durchsuchung)

Verfassungsgerichtshof Thüringen, Urteil v. 21.11.2012 (VerfGH 19/09)

Die Verfassungsbeschwerde ist unter www.bestandsdatenauskunft-mv.de abrufbar.

Auszug

§ 24b LVerfSchG M-V

Gesetz über den Verfassungsschutz im Lande Mecklenburg-Vorpommern (Landesverfassungsschutzgesetz – LVerfSchG M-V)

Quelle: http://www.lexsoft.de/cgi-bin/lexsoft/justizportal_nrw.cgi?t=14114557 0986982651&sessionID=209388122181 0774250&source=link&highlighting=off &templateID=document&chosenIndex= Dummy_nv_68&xid=188081,35

Abschnitt: Abschnitt 3 – Informationsübermittlung und Auskunftserteilung

§ 24b LVerfSchG M-V – Weitere Auskunftsverlangen

(1) Soweit dies zur Erfüllung der Aufgaben der Verfassungsschutzbehörde erforderlich ist, darf von demjenigen, der geschäftsmäßig Telekommunikationsdienste erbringt oder daran mitwirkt, im Einzelfall Auskunft über die nach den §§ 95 und 111 des Telekommunikationsgesetzes vom 22. Juni 2004 (BGBl. I S. 1190), das zuletzt durch Artikel 1 des Gesetzes vom 20. Juni 2013 (BGBl. I S. 1602) geändert worden ist, erhobenen Daten verlangt werden (§ 113 Absatz 1 Satz 1 des Telekommunikationsgesetzes). Bezieht sich das Auskunftsverlangen nach Satz 1 auf Daten, mittels derer der Zugriff auf Endgeräte oder auf Speichereinrichtungen, die in diesen Endgeräten oder hiervon räumlich getrennt eingesetzt werden, geschützt wird (§ 113 Absatz 1 Satz 2 des Telekommunikationsgesetzes), darf die Auskunft nur verlangt werden, wenn die gesetzlichen Voraussetzungen für die Nutzung der Daten vorliegen.

(2) Die Auskunft nach Absatz 1 darf auch anhand einer zu einem bestimmten Zeitpunkt zugewiesenen Internetprotokoll-Adresse verlangt werden (§ 113 Absatz 1 Satz 3 des Telekommunikationsgesetzes).

(3) Von einer Beauskunftung nach Absatz 2 ist die betroffene Person zu benachrichtigen. …

Auszug

§ 28a SOG M-V

Gesetz über die öffentliche Sicherheit und Ordnung in Mecklenburg-Vorpommern (Sicherheits- und Ordnungsgesetz – SOG M-V) – Landesrecht Mecklenburg-Vorpommern

Quelle: http://www.lexsoft.de/cgi-bin/lexsoft/justizportal_nrw.cgi?t=14114555 2983903551&sessionID=209388122181 0774250&chosenIndex=Dummy_nv_68 &templateID=document&source=conte xt&source=context&highlighting=off&x id=188215,129

Abschnitt: → Unterabschnitt 1 – Datenerhebung

§ 28a SOG M-V – Erhebung von Telekommunikationsdaten im manuellen Auskunftsverfahren

(1) Die Polizei kann zur Abwehr einer im einzelnen Falle bevorstehenden Gefahr von demjenigen, der geschäftsmäßig Telekommunikationsdienste erbringt oder daran mitwirkt (Diensteanbieter), Auskunft über die nach den §§ 95 und 111 des Telekommunikationsgesetzes vom 22. Juni 2004 (BGBl. I S. 1190), das zuletzt durch Artikel 1 des Gesetzes vom 20. Juni 2013 (BGBl. I S. 1602) geändert worden ist, erhobenen personenbezogenen Daten verlangen (§ 113 Absatz 1 Satz 1 des Telekommunikationsgesetzes). Bezieht sich das Auskunftsverlangen nach Satz 1 auf Daten, mittels derer der Zugriff auf Endgeräte oder auf Speichereinrichtungen, die in diesen Endgeräten oder hiervon räumlich getrennt eingesetzt werden, geschützt wird (§ 113 Absatz 1 Satz 2 des Telekommunikationsgesetzes), darf die Auskunft nur verlangt werden, wenn die gesetzlichen Voraussetzungen für die Nutzung der Daten vorliegen.

(2) Die Auskunft nach Absatz 1 darf auch anhand einer zu einem bestimmten Zeitpunkt zugewiesenen Internetprotokoll-Adresse verlangt werden (§ 113 Absatz 1 Satz 3 des Telekommunikationsgesetzes). In diesem Fall ist die betroffene Person über die Beauskunftung zu unterrichten. …