Ausschussvorlage

Ausschuss: INA

Stellungnahmen zu:
Gesetzentwurf Drucks. 18/7137
– HSOG/LfV –

Bund Deutscher Kriminalbeamter
Landesverband Hessen

BDK Landesvorstand| Alt Langenhain 35| D-65719 Hofheim/Ts.

Hessischer Landtag
Innenausschuss
Postfach 3240

65022 Wiesbaden

Ihr/e Zeichen/Nachricht vom
I A 2.6 / 17.04.2013
Ihr/e Ansprechpartner/in
Günter Brandt
Funktion
Landesvorsitzender
E-Mail
guenter.brandt@bdk.de
Telefon
+49 (0) 69 - 755.52.602
Telefax
+49 (0) 6187 - 93.50.52
mobil
+49 (0) 177 - 74.24.496

Hofheim/Ts., den 27.05.2013

Gesetzentwurf der Fraktionen der CDU und der FDP für ein Gesetz zur Änderung des Hessischen Gesetzes über die öffentliche Sicherheit und Ordnung und des Gesetzes über das Landesamt für Verfassungsschutz - Drucks. 18/7137 –

hier: Stellungnahme vom Bund Deutscher Kriminalbeamter (BDK), Landesverband (LV) Hessen

Ihr Schreiben vom 17.04.2013 / Schriftliche Anhörung im Innenausschuss des Hessischen Landtages

Der Bund Deutscher Kriminalbeamter, Landesverband Hessen stimmt dem obig genannten Gesetzesentwurf der Fraktionen der CDU und der FDP vom 12.03.2013 zu und führt in seiner Stellungnahme folgende fachliche Bemerkungen an:

Am 24.10.2012 verabschiedete das Bundeskabinett den Gesetzentwurf zur Änderung des Telekommunikationsgesetzes und zur Neuregelung der Bestandsdatenauskunft. Ziel des Gesetzes ist, dem vom Bundesverfassungsgericht am 24.01.2012 (1 BvR 1299/05) geforderten "Doppeltürenmodell" Rechnung zu tragen, und bezüglich der Bestandsdatenauskunft klare, gesetzliche Kompetenzen sowohl für Telekommunikationsanbieter als

auch für berechtigte Behörden zu erlassen. Am 03.05.2013 stimmte der Bundesrat dem Gesetz zu. Damit werden die Vorgaben des Bundesverfassungsgerichts auf Bundesebene umgesetzt.

Der Gesetzesentwurf der Fraktionen der CDU und der FDP (Drucks. 18/7137) beinhaltet nach Bewertung des Bund Deutscher Kriminalbeamter, LV Hessen alle notwendigen Gesetzesänderungen in den Landesgesetzen (HSOG und VerfSchutzG HE), um Abfragen von Bestandsdaten von hessischen Sicherheitsbehörden bei den Telekommunikationsdienstleistungsanbietern zur Abwehr von Gefahren für die öffentliche Sicherheit oder Ordnung auf Grundlage der Neuregelungen im § 100 j StPO zu vollziehen.

Mit der sogenannten Schnittstellenklausel in § 113 Absatz 5 TKG wird eine elektronische Entgegennahme von Auskunftsverlangen geschaffen. Eigenständige Recherchen durch die Behörden sind weder erlaubt noch technisch vorgesehen. Die Vorschrift betrifft ca. 30 Unternehmen, von denen aktuell fünf eine entsprechende Schnittstelle vorhalten.

Die neuen Rechtsgrundlagen gewährleisten in Zusammenwirken mit den TK-Anbietern eine schnelle Abwicklung notwendiger Auskunftsersuchen gegenüber den Sicherheitsbehörden und leisten damit einen notwendigen Beitrag zu den kriminalpolizeilichen Präventivmaßnahmen und Einsätzen im Landesamt für Verfassungsschutz zum Erhalt der Inneren Sicherheit in Hessen.

Mit den besten Wünschen!

Günter Brandt - Landesvorsitzender

DPolG
DEUTSCHE POLIZEIGEWERKSCHAFT
im DBB
Landesverband Hessen

Landesgeschäftsstelle
Otto-Hesse-Straße 19 / T3
64293 Darmstadt
Telefon (06151) 27 94 500
Telefax (06151) 27 94 502
kontakt@dpolg-hessen.de
www.dpolg-hessen.de

Steuer-Nr. 07 224 0101 5
Finanzamt Darmstadt

DPolG Landesverband Hessen, Otto-Hesse-Str. 19/T3, 64293 Darmstadt

Hessischer Landtag
Innenausschuss
Herrn Vorsitzenden
Horst Klee, MdL
Schlossplatz 1 – 3

65183 Wiesbaden

GS/MS 28.05.2013

Stellungnahme zum Gesetzentwurf der Fraktionen der CDU und der FDP für ein Gesetz zur Änderung des Hessischen Gesetzes über die öffentliche Sicherheit und Ordnung und des Gesetzes über das Landesamt für Verfassungsschutz
- Drucks. 18/7137 -

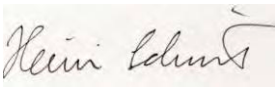
Sehr geehrter Herr Vorsitzender Klee,
sehr geehrte Damen und Herren,

zum vorliegenden Gesetzentwurf nehmen wir wie folgt Stellung:

Wir begrüßen den Gesetzentwurf, weil mit ihm die Entscheidung des Bundesverfassungsgerichts über die Vorgaben zur Neuregelung der Bestandsdatenauskunft umgesetzt wird.
Die Aufgabe des Landesgesetzgebers, unabhängig von der Schaffung einer Datenübermittlungsnorm als „erste Tür“ im Telekommunikationsgesetz durch den Bund, die „zweite Tür“, nämlich die Abrufnorm im HSOG und im LfV-Gesetz zu schaffen, wird damit erfüllt.
Insgesamt wird neben der Änderung des TKG nun auf hessischer Ebene der Weg für die Bestandsdatenauskunft gesetzgeberisch geebnet.

Wir halten die Bestandsdatenauskunft für ein unverzichtbares Instrument bei der Kriminalitätsbekämpfung, ebenso wie die Vorratsdatenspeicherung.

Mit freundlichen Grüßen



(Heini Schmitt)
Landesvorsitzender

GEWERKSCHAFT
DER POLIZEI

Mitglied der
European Confederation
of Police (EUROCOP)

Landesbezirk Hessen

Jörg Bruchmüller
Landesvorsitzender

Wilhelmstraße 60 a
65183 Wiesbaden

Telefon
+49 (0) 611 – 99 227 – 0

Telefax
+49 (0) 611 – 99 227 - 27

E-Mail
gdphessen@t-online.de

www.gdp.de/hessen

Gewerkschaft der Polizei • Wilhelmstraße 60 a • 65183 Wiesbaden

An den
Vorsitzenden
des Innenausschusses
Hessischer Landtag

per E-Mail

Ihr Zeichen	Ihr Schreiben	Unser Zeichen	Datum
		JB/rb	28. Mai 2013

Stellungnahme zu dem Gesetzesentwurf der Fraktionen der CDU und der FDP für ein Gesetz zur Änderung des Hessischen Gesetzes über die öffentliche Sicherheit und Ordnung und des Gesetzes über das Landesamt für Verfassungsschutz – Landtagsdrucksache (Drs.) 18/7137

Sehr geehrte Damen und Herren,

vorab sei deutlich gemacht, dass die Stellungnahme der Gewerkschaft der Polizei – Landesbezirk Hessen (GdP) überwiegend aus praxis- und beschäftigtenorientierter Sichtweise erfolgt.

So ist es zunächst auch angezeigt darauf hinzuweisen, dass sich immer weitergehende erhebliche Qualitätsprobleme in der aktuellen Polizeirechtsentwicklung abzeichnen, die sich zum Teil auch in dem vorliegenden Entwurf widerspiegeln. Es gibt eine fortschreitende Tendenz hin zu immer komplexeren Vorschriften, die in der Praxis und auch für die Rechtsadressaten (betroffene Bürgerinnen und Bürger) nicht ohne Weiteres lesbar und verständlich sind. Da es sich um polizeirechtliche Bestimmungen handelt, sollte die Anwendung für jeden Polizeibeschäftigten ohne Schwierigkeiten möglich sein.

Leider hat der Gesetzgeber auch bei dieser Änderung des Gesetzes über die öffentliche Sicherheit und Ordnung (HSOG) die Chance vertan, diskutierbare Punkte im HSOG mit anzupacken. Zu erwähnen sind beispielsweise die konkrete Ausgestaltung der Gefährderansprache oder des Gefährderanschreibens als Standardmaßnahme zu regeln, so wie es teilweise gefordert wird[1] und andere Landesgesetzgeber[2] bereits vorantreiben. Diese Maßnahme wird seit nunmehr über 10 Jahren auf die Generalklausel

[1] Andrea Kießling, Die dogmatische Einordnung der polizeilichen Gefährderansprache in das allgemeine Polizeirecht, DVBl. 2012, 1210-1217.
[2] Gesetz zur Änderung des Niedersächsischen Gesetzes über die öffentliche Sicherheit und Ordnung v. 10.07.2012 (Drs. 16/4965).

(§ 11 HSOG) gestützt, mit der Problematik, dass eine „konkrete Gefahr“ vorliegen muss. Bei einer Formulierung „wenn tatsächliche Anhaltspunkte“ oder „wenn Tatsachen die Annahme rechtfertigen“, wäre den Kolleginnen und Kollegen schon geholfen. Oder auch die spezielle Legitimierung des Annäherungs- und Kontaktverbotes im Rahmen häuslicher Gewalt. Hierbei gibt es bei der Legitimierung durch § 11 HSOG durchaus Unsicherheiten dank hessischer Rechtsprechung[3], bei der die Generalklausel nicht als zulässige Ermächtigungsgrundlage für die zuvor genannten Verbote gesehen wird. Diese Anwenderunsicherheiten hätte man für die Polizeibeschäftigten angehen können. Stattdessen wurde, obwohl seit 24.01.2012 [Entscheidung des Bundesverfassungsgerichtes in der Sache § 113 Telekommunikationsgesetz (TKG)] bekannt war, dass diese Regelung bis maximal 30.06.2013 angewendet werden darf, auch in diesem Fall wieder sehr kurzfristig reagiert. Nunmehr werden auf den letzten Drücker (Drs. 18/7137 vom 12.03.2013) die zwingenden Vorgaben des Bundesverfassungsgerichtes umgesetzt.

Im Einzelnen:

Änderungen zum Hessischen Gesetz über die öffentliche Sicherheit und Ordnung

Änderungen in § 15a HSOG

Die Streichung des § 113a TKG und die Änderung des Klammervermerks in § 15a Abs. 2 S. 1 HSOG sind obligatorisch. Seitens der GdP wird ausdrücklich begrüßt, dass, auf diese Weise parallel zur Bundesgesetzgebung gearbeitet wird, damit für die Polizei keine Regelungslücke entsteht. Dies wurde bereits zutreffend durch Herrn Staatsminister Rhein in der ersten Lesung im Landtag hervorgehoben[4].

Die Ergänzungen in Abs. 2 sind für die Polizei keine neuen Befugnisse. Wie bereits dargestellt, werden lediglich alte Befugnisse auf einwandfreie rechtliche Grundlagen gestellt. Sowohl die Eingriffsnotwendigkeit „tatsächlicher Anhaltspunkte“ (§ 15a Abs. 2 S. 3 iVm. § 12 Abs. 1 S. 1 HSOG) als auch die Unterrichtungspflicht bei verdeckter Datenerhebung (§ 15a Abs. 2 iVm. § 29 Abs. 6 HSOG) werden befürwortet.

Die Nichtanwendbarkeit von § 12 Abs. 2 HSOG ist zwar im Ergebnis zu unterstützen, aber im Hinblick auf die in der Begründung dargelegten Intention weder schlüssig noch nachvollziehbar. Bei jeglicher polizeilichen Inanspruchnahme bedarf es eines Adressaten. Dieser ergibt sich bei sog. abstrakten Gefahren aus der Norm selbst (sog. Normadressat); was im Übrigen im vorliegenden Gesetzesentwurf geschehen ist, wie § 15a Abs. 2 S. 3 HSOG n.F. dokumentiert, denn dort heißt es „von demjenigen, der geschäftsmäßig Telekommunikationsdienste erbringt oder daran mitwirkt“. In der Begründung ist die Rede vom Telekommunikationsunternehmen als Nichtstörer (§ 9 HSOG); sollte dieser in Anspruch genommen werden, müssen zwingend die vier Voraussetzungen aus § 9 HSOG kumulativ erfüllt sein und die erste von diesen ist schlicht „eine gegenwärtige erhebliche Gefahr“. Somit läuft die in der Begründung dargelegte Argumentation im Hinblick auf die Nichtstörereigenschaft ins Leere; jedoch ist der geplante Gesetzestext, dass § 12 Abs. 2 HSOG im Rahmen des § 15a Abs. 2 HSOG n. F. nicht anzuwenden ist, richtig.

Die Verweisung beim Auskunftsersuchen in § 15a Abs. 2 S. 3 HSOG auch auf § 12 Abs. 4 HSOG (§ 136a StPO - Verbotene Vernehmungsmethoden) klingt ein wenig

[3] Beschluss VG Kassel vom 31.05.2011 (Az.: 4 L 701/11.KS).
[4] 134. Sitzung am 20.03.2013 (PlPr. 18/134, S. 9509).

abenteuerlich, ergibt sich nicht aus der Gesetzesbegründung und ist nach gewerkschaftlicher Einschätzung obsolet.

Unter „A. Allgemeines“ der in Rede stehenden Drs. 18/7137 findet sich auf Seite 3 der Hinweis: „Die Entschädigung des TK-Unternehmens richtet sich im Bereich des HSOG nach § 3 Abs. 2 HSOG, der seinerseits auf das Justizvergütungs- und –entschädigungsgesetz verweist“. Dies ist auch notwendig, wie bereits die Bundesratsdrucksache 664/12 (S. 16) deutlich macht. Im Ergebnis wäre es jedoch aus Klarstellungsgesichtspunkten und Anwenderfreundlichkeit heraus wünschenswert gewesen, einen solchen Hinweis auf § 3 Abs. 2 HSOG im Gesetzestext aufzunehmen. Dies vor allem vor dem Hintergrund, dass der Hauptanwendungsfall des § 3 Abs. 2 HSOG die Vorladung, § 30 HSOG, war[5]; was sich dann möglicherweise zukünftig ändern könnte.

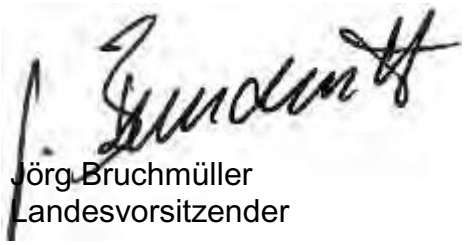
Entfristung

Es ist sehr zu begrüßen, das HSOG nunmehr zu entfristen. Beim HSOG handelt es sich zweifelsohne um eine Rechtsvorschrift, die den überkommenen Grundkanon des originären hessischen Landesrechts bildet und dessen Erforderlichkeit unzweifelhaft ist, wie in der Drs. 18/6022 bereits zutreffend ausgeführt wurde.

Änderungen zum Gesetz über das Landesamt für Verfassungsschutz (LfV)

Alles in allem sind die Folgeänderungen und Ergänzungen nachvollziehbar und schlüssig.

Schließlich hätte aber auch das LfV entfristet werden sollen. Das Landesamt für Verfassungsschutz feierte bereits 2011 sein 60-jähriges Bestehen. Zweifelsohne handelt es sich beim LfV auch um eine Rechtsvorschrift, die den überkommenen Grundkanon des originären hessischen Landesrechts bildet und dessen Erforderlichkeit unzweifelhaft ist und somit keiner Befristung bedarf. Die Auflistung dieser, wie zuvor charakterisierten Rechtsvorschriften, die keiner Befristung bedürfen, wie auch das HSOG, sind nur exemplarisch[6]. Auch das LfV erfüllt diese Voraussetzungen und ist somit zu entfristen.



Jörg Bruchmüller
Landesvorsitzender

[5] So Meixner/Fredrich, HSOG, 11. Auflage 2010, § 3 Rdnr. 8.
[6] Gesetzesentwurf der Landesregierung für ein Gesetz zur Entfristung und zur Veränderung der Geltungsdauer von befristeten Rechtsvorschriften vom 21.08.2012 (Drs. 18/6022, S. 16).

DER HESSISCHE DATENSCHUTZBEAUFTRAGTE

DER HESSISCHE DATENSCHUTZBEAUFTRAGTE
Postfach 31 63 · 65021 Wiesbaden

Herrn Vorsitzenden des Innenausschusses
Horst Klee
Hessischer Landtag
Schlossplatz 1-3
65183 Wiesbaden

Aktenzeichen 56.01.01-de
Bitte bei Antwort angeben

zuständig Frau Dembowski
Durchwahl 14 08 - 126

Ihr Zeichen
Ihre Nachricht vom

Datum 23.05.2013

Gesetzesentwurf der Fraktionen der CDU und der FDP für ein Gesetz zur Änderung des Hessischen Gesetzes über die öffentliche Sicherheit und Ordnung und des Gesetzes über das Landesamt für Verfassungsschutz, Drucks. 18/7134

Sehr geehrter Herr Abgeordneter Klee,

für die Gelegenheit, zu dem oben genannten Gesetzesentwurf Stellung zu nehmen, bedanke ich mich.

In der vorliegenden Form erfüllt der Gesetzentwurf nicht die verfassungsrechtlichen Voraussetzungen für einen Eingriff in das Recht auf informationelle Selbstbestimmung. Die Anforderungen, die das Bundesverfassungsgericht in seinem Beschluss vom 24.01.2012 (1 BvR 1299/05) formuliert hat, sind nur unzureichend umgesetzt.

Ferner ist auch der Entwurf der bundesrechtlichen Regelungen im Gesetz zur Umsetzung des Telekommunikationsgesetzes und zur Neuregelung der Bestandsdatenauskunft, deren Umsetzung in Landesrecht mit diesem Gesetzentwurf erfolgen soll, zwischenzeitlich im Rahmen der parlamentarischen Beratungen nicht unerheblich verändert worden. Diese Veränderungen (in der Fassung des Beschlusses des Bundestags vom 21.03.2013 – BT-Drucks. 17/12879) habe ich meiner Stellungnahme

Gustav-Stresemann-Ring 1 · 65189 Wiesbaden · Telefon (06 11) 14 08-0 · Telefax (06 11) 14 08-9 00 oder -9 01
E-Mail poststelle@datenschutz.hessen.de · Internet http://www.datenschutz.hessen.de
Bankverbindung Kontoinhaber HCC/Kanzlei Hess.Landtag/DB · Kontonummer 100 53 62 · Bankleitzahl 500 500 00

zugrunde gelegt. Die Zitate der Bundesgesetze beziehen sich daher – wenn nicht ausdrücklich anders angegeben – immer auf die Fassung, die sie durch den Gesetzesbeschluss erhalten werden.

Die Verpflichtung zur Auskunftserteilung der Telekommunikationsunternehmen ist (entsprechend dem in der Begründung benannten Doppeltürenmodell des BVerfG) in § 113 TKG geregelt.
Der Landesgesetzgeber hat in diesem Kontext daher die Regelungen zu treffen, die definieren, welche Daten unter welchen Voraussetzungen die jeweiligen Landesbehörden erheben dürfen.

1. Artikel 1 – Hessisches Gesetz über die öffentliche Sicherheit und Ordnung (HSOG)

§ 15a, Datenerhebung durch Telekommunikationsüberwachung

–

Grundsätzlich halte auch ich eine differenzierte Regelung für den Zugriff auf die unterschiedlichen Datenarten, wie sie in § 15a Absatz 2 definiert sind, für zulässig. Die sich aus den jetzt vorgeschlagenen Regelungen ergebende Differenzierungen der Eingriffsvoraussetzungen werden allerdings den verfassungsrechtlichen Anforderungen nicht gerecht.

Aus meiner Sicht wäre es sinnvoll zur Schaffung einer normenklaren und auch verständlichen Regelung eine Struktur zugrunde zu legen, wie sie in den vergleichbaren Bundesgesetzen formuliert wurde – insbesondere im BKA-Gesetzes (§§ 7, 20a und 22).

Für die Bestandsdaten ist es dann grundsätzlich möglich – wie im Ansatz wohl durch den Gesetzentwurf beabsichtigt – zur Zulässigkeit der Erhebung an § 13 HSOG anzuknüpfen. Da im Zeitpunkt der Auskunftseinholung nicht zu erkennen ist, ob die Bestandsdaten einer natürlichen Person zugeordnet sind, ist immer davon auszugehen,

dass die Bestandsdatenabfrage auf die Erhebung personenbezogener Daten gerichtet ist.

Eine differenzierte Betrachtung ist jedoch für die Daten gem. § 113 Abs. 1 S. 2 TKG erforderlich. Zugangssicherungscodes (wie etwa Passwörter, PIN und PUK) selbst sind zwar Bestandsdaten im Sinne des TKG, sie haben jedoch einen höheren Schutzbedarf als die herkömmlichen Bestandsdaten, da mit Ihrer Hilfe nicht nur der Umfang, sondern auch der Inhalt einer Kommunikationsbeziehung erschlossen werden kann. Insoweit entspricht der Eingriffsgehalt bei Auskünften solcher Daten eher dem einer Auskunft zu einer dynamischen IP-Adresse als zu sonstigen Bestandsdaten. Da in aller Regel solche Daten deshalb nur dann erforderlich sein können, wenn auch auf die durch sie erschließbaren Inhaltsdaten zugegriffen werden soll, ist eine entsprechende Einschränkung, wie sie in § 7 Abs. 3 S. 2 BKA-Gesetz formuliert ist, sachgerecht. Der Bundesgesetzgeber hat für diese Daten als weitere Anforderung formuliert, dass eine solche Datenerhebung nur zulässig ist, wenn auch die gesetzlichen Voraussetzungen für die Daten vorliegen, auf die mittels dieser Bestandsdaten zugegriffen werden kann. Dies entspricht auch der Rechtsprechung des BVerfG (BVerfG, Beschluss vom 24.01.2012, 1 BvR 1299/05, Nr. 182, 185). Zugangssicherungssicherungscodes erfordern mit anderen Worten einen vorverlagerten Datenschutz.

Aus dem erhöhten Schutzbedarf der Zugangssicherungscodes folgt meines Erachtens zudem, dass diese Daten nicht – wie im Gesetzentwurf vorgesehen – von der Anwendung des § 15a Abs. 5 und damit der Notwendigkeit einer richterlichen Anordnung ausgenommen werden können. Schließlich halte ich für diese Daten auch eine Benachrichtigung gem. § 29 Abs. 6 für erforderlich. Auch dies entspricht der in § 7 Abs. 6 BKA-Gesetz getroffenen Regelung.

Im Übrigen begrüße ich es ausdrücklich, dass mit § 15a Abs. 2 S. 2 für die Auskunft der zu einem bestimmten Zeitpunkt zugewiesenen IP-Adresse eine erhöhte Schwelle vorgesehen ist, da diese nur zur Abwehr einer gegenwärtigen erheblichen Gefahr verlangt werden darf.

2. Artikel 2 – Gesetz über das Landesamt für Verfassungsschutz (LfV-Gesetz)

§ 4a, Besondere Auskunftsersuchen

Meine Anmerkungen zum HSOG-Entwurf gelten entsprechend auch für die Änderungen im LfV-Gesetz. Insoweit halte ich grundsätzlich eine Orientierung am Bundesverfassungsschutzgesetz (BVerfSchG) in der Sache für angebracht.

Daher sollte auch in § 4a Abs. 3, 2. Hs für eine Abfrage von Zugangssicherungscodes die Einschränkung normiert werden, dass diese nur dann erfolgen darf, wenn die Voraussetzungen für die Nutzung der Daten vorliegen (siehe bereits oben). Dies entspricht der Regelung des § 8d Abs. 1 S. 2 BVerfSchG.

– Im Übrigen ist mir nicht ersichtlich, warum in diesem Kontext (Zugriff auf Bestandsdaten) – anders als für das HSOG – keine ausdrückliche Regelung für den Zugriff auf die dynamischen IP-Adressen getroffen werden soll. Entsprechend der Rechtsprechung des BVerfG handelt es sich bei der Zuordnung von dynamischen IP-Adressen um einen Eingriff in das Telekommunikationsgeheimnis. Die Differenzierung der Eingriffsvoraussetzungen für die Abfrage von Bestandsdaten ist verfassungsrechtlich daher auch für den Verfassungsschutz geboten. Auch dies entspricht im Übrigen der Regelung im BVerfSchG.

Wie oben ausgeführt, ist der Zugriff auf Zugangssicherungscodes in der Eingriffstiefe eher diesen Daten als den allgemeinen Bestandsdaten vergleichbar. Deshalb ist mir nicht ersichtlich, warum die Verfahrensregelungen des § 4a Abs. 5 (bisher Absatz 4) sich nur auf Abfragen gem. Absatz 3 und nicht auf die Befugnisse im (neuen) Absatz 4 beziehen. Ich halte auch für den Zugriff auf die dynamischen IP-Adressen (für die wie oben ausgeführt, das BVerfG den Eingriff in das Telekommunikationsgeheimnis ausdrücklich festgestellt hat) und die Zugangssicherungscodes die Anwendung der

besonderen Verfahrensregelungen unter Einbeziehung des Ministeriums und der G10 Kommission bzw. der parlamentarischen Kontrollkommission für erforderlich.

Der Bundesgesetzgeber hat auch für den Verfassungsschutz im Rahmen dieser Neuregelungen eine Benachrichtigungspflicht eingeführt (§ 8d Abs. 3 BVerfSchG). Ich rege an, auch für den Bereich des Landesrechts eine solche Verstärkung der (nachträglichen) Überprüfungsmöglichkeiten für die Betroffenen zu schaffen.

Mit freundlichen Grüßen

Prof. Dr. Michael Ronellenfitsch

Landesamt für Verfassungsschutz Hessen

HESSEN

Aktenzeichen
L13-257-S-520 020- 0007/2013

Bearbeiter/in Dr. Karrenberg
Durchwahl (06 11) 720-675
Telefax: (06 11) 720-179
E-Mail:

Ihr Zeichen I A 2.6
Ihre Nachricht Vom 17.04.2013

Datum 29. Mai 2013

Landesamt für Verfassungsschutz Hessen ▪ Postfach 39 05 ▪ 65029 Wiesbaden

Hessischer Landtag
Ausschusssekretariat
Postfach 3240

65022 Wiesbaden

Per E-Mail an H.Thaumueller@ltd.hessen.de

Nachrichtlich:

Hessisches Ministerium des
Innern und für Sport
z. Hd. Abt.Leiter MinDirig. Dr. Kanther o.V.i.A.
Friedrich-Ebert-Allee 12

65185 Wiesbaden

Per E-Mail an
Martin.Roessler@hmdis.hessen.de

Gesetzentwurf der Fraktionen der CDU und der FDP für ein Gesetz zur Änderung des Hessischen Gesetzes über die öffentliche Sicherheit und Ordnung und des Gesetzes über das Landesamt für Verfassungsschutz – Drucks. 18/7137 -

Stellungnahme des Landesamtes für Verfassungsschutz für die schriftliche Anhörung im Innenausschuss des hessischen Landtags

Das Landesamt für Verfassungsschutz begrüßt die mit der in Artikel 2 des Gesetzentwurfs vorgesehene Änderung des Gesetzes über das Landesamt für Verfassungsschutz.

Mit der avisierten Änderung wird dem vom Bundesverfassungsgericht im Beschluss vom 24. Januar 2012 -1 BvR 1299/05- statuierten Prinzip der Doppeltür zu § 113 Abs. 1 S. 1 Telekommunikationsgesetz (TKG) Rechnung getragen, wonach es für den Abruf von Bestandsdaten nach §§ 95 und 111 TKG seitens der auskunftsberechtigten Behörden

65187 Wiesbaden, Konrad-Adenauer-Ring 49
Telefon: (0611) 720-0
Telefax: (0611) 720-179
E-Mail: poststelle@lfv.hessen.de
Internet: www.verfassungsschutz.hessen.de

fachrechtlicher, gegebenenfalls landesrechtlicher Ermächtigungsgrundlagen bedarf, die eine Verpflichtung der Telekommunikationsdiensteanbieter gegenüber den abrufberechtigten Behörden eigenständig und normenklar begründen.

Mit der Änderung erhält das Landesamt für Verfassungsschutz die erforderliche Rechtsgrundlage, um für die Aufgabenerfüllung erforderliche Abklärungen von Bestandsdaten nach § 113 Abs. 1 S. 1 TKG durchführen zu können.

Mit freundlichen Grüßen

Gez. Desch

Hessisches Landes-Kriminal-Amt

Abteilung 2

Verwaltung, Zentrale Dienste

HESSISCHES LANDESKRIMINALAMT • POSTFACH 3125 • 65021 WIESBADEN

Hessischer Landtag
Ausschusssekretariat
Schlossplatz 1-3

65183 Wiesbaden

EINGEGANGEN
29. Mai 2013
HESSISCHER LANDTAG

Aktenzeichen *(Bitte bei Antwort angeben)*
21 EG 011/2013

HSG / SG: 21
Bearbeiter/-in: Herr Dr. Bretschneider
Durchwahl: 0611 / 83 - 2102
E-Mail: HSG21.HLKA@polizei.hessen.de
Telefax: 0611 / 83 - 2005

Datum 27. Mai 2013

Schriftliche Anhörung zum Gesetzentwurf der Fraktionen der CDU und der FDP für ein Gesetz zu Änderung des HSOG u.a.– Drucks. 18/7137

Ihr Zeichen: I A 2.6

Sehr geehrte Damen und Herren,

zu dem im Betreff genannten Gesetzentwurf möchte ich aus Sicht des Hessischen Landeskriminalamts wie folgt Stellung nehmen:

Das Bundesverfassungsgericht hat in seiner Entscheidung vom 24. Januar 2012 konkrete Regelungen gefordert, unter welchen Voraussetzungen Telekommunikationsunternehmen in welcher Form Bestandsdaten an die Polizeibehörden herausgeben müssen. In der Folge wurde eine Anpassung des Hessischen Gesetzes über die öffentliche Sicherheit und Ordnung durch den Landesgesetzgeber notwendig.

Bei der Bestandsdatenauskunft handelt es sich aus unserer Sicht um ein unverzichtbares Ermittlungsinstrument für die Strafverfolgungsbehörden; die Schließung der festgestellten Gesetzeslücke ist daher dringend erforderlich. Die von Ihnen nunmehr vorgelegte Neuregelung des § 15a HSOG, welche sowohl die oben zitierte Bundesverfassungsgerichtsentscheidung als auch entsprechende Änderungen im Telekommunikationsgesetz berücksichtigt, schafft Rechtssicherheit und ist im Ergebnis ausdrücklich zu begrüßen.

Im Rahmen der Auskunft über Bestandsdaten erscheint auch das Tatbestandsmerkmal der „gegenwärtigen erheblichen Gefahr" hinsichtlich der Schwere des Eingriffs in das Grundrecht des Art. 10 GG als angemessen, zumal sein Vorliegen in entsprechenden Gefahrenlagen (Suizidenten, Gemenge-Lagen bei Bedrohungen, Gemeingefahren u.ä.) entsprechend begründet werden kann.

Mit freundlichen Grüßen

(Dölger)
Präsident
(Mit der Wahrnehmung der Dienstgeschäfte beauftragt)

Univ.-Professor Dr. Dirk Heckmann

Universität Passau
Lehrstuhl für Öffentliches Recht,
Sicherheitsrecht und Internetrecht
heckmann@uni-passau.de

27. Mai 2013

Stellungnahme zum Gesetzentwurf

der Fraktionen der CDU und FDP für ein Gesetz zur Änderung des Hessischen Gesetzes über die öffentliche Sicherheit und Ordnung und des Gesetzes über das Landesamt für Verfassungsschutz

- Drucks. 18/7137 -

Inhalt

Zusammenfassung

1. Die Auskunft eines Telekommunikationsunternehmens über Bestandsdaten greift grundsätzlich allein in das Grundrecht auf informationelle Selbstbestimmung (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG) ein. Dies gilt auch, wenn Zugangssicherungscodes abgerufen werden.

   Anders ist dies jedoch bei der identifizierenden Zuordnung dynamischer IP-Adressen. Diese weist eine besondere Nähe zu konkreten Telekommunikationsvorgängen auf und fällt deshalb in den Schutzbereich des Art. 10 Abs. 1 GG.

2. Ein kumulativer Verzicht sowohl auf eine unabhängige Vorabkontrolle als auch auf eine nachträgliche Benachrichtigung des Betroffenen – wie dies für die „klassische“ Bestandsdatenabfrage im HSOG beabsichtigt ist – erscheint bei heimlichen Eingriffen nur dann zulässig zu sein, wenn diese – trotz der Heimlichkeit – lediglich geringes Gewicht aufweisen. Dies ist laut Bundesverfassungsgericht zwar bei der „klassischen“ Bestandsdatenauskunft der Fall. Dennoch wäre es aus grundrechtsschonender Perspektive wünschenswert, derartige Vorkehrungen vorzusehen.

3. Auch die Bestandsdatenabfrage anhand dynamischer IP-Adressen wurde durch die Änderung des § 15a Abs. 5 S. 1 HSOG-E bewusst von einem Richtervorbehalt ausgenommen. Dies ist vor dem Hintergrund, dass es sich bei dieser Art von Auskunft um einen heimlichen Eingriff in den Schutzbereich des Telekommunikationsgeheimnisses gem. Art. 10 Abs. 1 GG handelt, als kritisch zu bewerten.

4. Verfassungsrechtlich fraglich an der im HSOG vorgesehenen Regelung zur Abfrage von Zugangssicherungscodes ist, dass sie die Vorgaben, die das Bundesverfassungsgericht aus dem Verhältnismäßigkeitsgrundsatz herleitet, nicht umsetzt. Die Norm lässt nämlich nicht erkennen, dass die Behörden die in § 113 Abs. 1 S. 2 TKG geregelten Zugangscodes nicht unabhängig von den Anforderungen an deren Nutzung und damit gegebenenfalls unter leichteren Voraussetzungen abfragen dürfen.

5. Bei der „klassischen“ Bestandsdatenabfrage nach LfVG-E erscheint es als kritisch, dass die Eingriffsvoraussetzungen denkbar niedrig angesetzt sind. Gem. § 4a Abs. 3 S. 1 LfVG-E soll es ausreichend sein, dass die Auskunft über die Bestandsdaten für die Erfüllung der Aufgaben des Landesamtes für Verfassungsschutz nach § 2 Abs. 2 LfVG erforderlich sind. Dieses

Erforderlichkeitskriterium ist die einzige Beschränkung des Zugriffs auf die Bestandsdaten; weitere materiell-rechtliche oder verfahrensrechtliche Beschränkungen sind nicht vorgesehen.

6. Verfassungsrechtlich äußerst bedenklich hinsichtlich der Bestandsdatenauskunft anhand dynamischer IP-Adressen nach dem LfVG-E ist, dass entgegen der Anordnung des Bundesverfassungsgerichts, dass die Befugnis zur Identifizierung dynamischer IP-Adressen hinreichend normenklar geregelt werden muss, dies keinen Niederschlag im Wortlaut der geplanten Norm gefunden hat. Lediglich der Klammerzusatz des § 4a Abs. 3 S. 1 LfVG-E, der auf § 113 Abs. 1 S. 3 verweist, lässt erkennen, dass auch eine Bestandsdatenabfrage anhand dynamischer IP-Adressen möglich sein soll.

7. Für die Auskunft über Zugangssicherungscodes nach LfVG-E gilt das unter Nr. 4 Gesagte entsprechend.

A. Vorbemerkung

Das Bundesverfassungsgericht hat durch Beschluss vom 24.01.2012[1] das manuelle Auskunftsverfahren nach den §§ 113 Abs. 1 S. 1, 111, 95 Abs. 1 TKG mittels verfassungskonformer Auslegung stark beschränkt. Die Regelung des § 113 Abs. 1 S. 2 TKG hat es für mit dem Grundgesetz unvereinbar erklärt.

Das Bundesverfassungsgericht hat jedoch die weitere Anwendung des derzeit geltenden Rechts unter bestimmten Voraussetzungen bis spätestens 30.06.2013 zugelassen.

Die Kernpunkte der Entscheidung des Bundesverfassungsgerichts sollen thesenartig wiedergegeben werden, soweit sie für das Verständnis der Abrufregelungen der Bestandsdaten erforderlich sind:

- Die Auskunft eines Telekommunikationsunternehmens über Bestandsdaten greift grundsätzlich allein in das Grundrecht auf informationelle Selbstbestimmung (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG) ein.[2] Das Telekommunikationsgeheimnis ist in der Regel nicht betroffen.[3]

- Anders liegt es demgegenüber bei der identifizierenden Zuordnung dynamischer IP-Adressen. Diese weist eine besondere Nähe zu konkreten Telekommunikationsvorgängen auf und fällt deshalb in den Schutzbereich des Art. 10 Abs. 1 GG. Die Anwendbarkeit des Art. 10 GG begründet sich daraus, dass die Telekommunikationsunternehmen für die Identifizierung einer dynamischen IP-Adresse in einem Zwischenschritt die – dem Telekommunikationsgeheimnis unterliegenden – entsprechenden Verbindungsdaten ihrer Kunden sichten müssen, mithin auf konkrete Telekommunikationsvorgänge zugreifen.

- Das Bundesverfassungsgericht statuiert für zukünftige Bestandsdatenauskünfte das Bedürfnis einer doppelten gesetzlichen Grundlage (sog. Doppeltürmodell). Bei Regelungen eines Datenaustauschs zur staatlichen Aufgabenwahrnehmung ist zwischen der Datenübermittlung seitens der auskunftserteilenden Stelle und dem Datenabruf seitens der auskunftssuchenden Stelle zu unterscheiden. Ein Datenaustausch vollzieht sich durch die einander korrespondierenden Eingriffe von Abfrage und Übermittlung, die jeweils einer eigenen Rechtsgrundlage bedürfen.[4] Mit anderen Worten muss zum einen eine gesetzliche Grundlage das Telekommunikationsunternehmen ermächtigen, Bestandsdaten an Bedarfsträger zu übermitteln (Übermittlungsermächtigung). Zum anderen muss das jeweilige

[1] BVerfG, Beschl. v. 24.01.2012 – 1 BvR 1299/05.
[2] BVerfG, Beschl. v. 24.01.2012 – 1 BvR 1299/05, Rn. 122-125.
[3] BVerfG, Beschl. v. 24.01.2012 – 1 BvR 1299/05, Rn. 110-115.
[4] BVerfG, Beschl. v. 24.01.2012 – 1 BvR 1299/05, Rn. 123.

Fachgesetz die öffentliche Stelle, die auf die Bestandsdaten zugreifen will, zur Erhebung der Daten ermächtigen (Abrufermächtigung). Beide gesetzlichen Ermächtigungen müssen „wie eine Doppeltür zusammenwirken“; erst beide gemeinsam ermächtigen zum Datenaustausch.

- Beide Ermächtigungsgrundlagen müssen Anlass, Zweck und Umfang des jeweiligen Eingriffs bereichsspezifisch, präzise und normenklar festlegen (Gebot der Normenklarheit und -bestimmtheit).[5]

- Die Sicherheitsbehörden dürfen gemäß dem Verhältnismäßigkeitsgebot Auskünfte über Zugangssicherungscodes (§ 113 Abs. 1 S. 2 TKG) nur dann verlangen, wenn die gesetzlichen Voraussetzungen für deren Nutzung gegeben sind.[6]

- Aus den Anforderungen des Verhältnismäßigkeitsgrundsatzes ergibt sich für Bestandsdatenauskünfte – auch auf der Ebene der fachrechtlichen Abrufnormen, wo solche Regelungen kompetenzrechtlich anzusiedeln sind – kein flächendeckendes Erfordernis zur Benachrichtigung der von der Auskunft Betroffenen.
  Ob jedoch Benachrichtigungspflichten oder weitere Maßgaben wie der Vorrang der Datenerhebung beim Betroffenen für bestimmte Fälle bereits in den Abrufnormen geboten sein können, hat das Bundesverfassungsgericht bewusst offen gelassen.[7]

Die Bundesregierung hat infolge des Bundesverfassungsgerichtsurteils den Entwurf eines Gesetzes zur Änderung des Telekommunikationsgesetzes und zur Neuregelung der Bestandsdatenauskunft in den Bundestag eingebracht.[8] Der Bundesrat hat am 03.05.2013 diesem Gesetz in der Ausschussfassung des Innenausschusses [9] zugestimmt.[10]

Ziel des vorliegenden Gesetzesentwurfs ist es, im Zusammenwirken mit dem Gesetz zur Änderung des Telekommunikationsgesetzes und zur Neuregelung der Bestandsdatenauskunft das vom Bundesverfassungsgericht in seiner Entscheidung kreierte Doppeltürmodell umzusetzen. Während die Datenübermittlung dabei im

[5] BVerfG, Beschl. v. 24.01.2012 – 1 BvR 1299/05, Rn. 169.
[6] BVerfG, Beschl. v. 24.01.2012 – 1 BvR 1299/05, Rn. 185.
[7] BVerfG, Beschl. v. 24.01.2012 – 1 BvR 1299/05, Rn. 187.
[8] BT-Drs. 17/12034.
[9] BT-Drs. 17/12879.
[10] BR-Drs. 251/13.

Telekommunikationsrecht des Bundes geregelt wurde, obliegt es dem Landesgesetzgeber, den Abruf der Daten für die Sicherheitsbehörden nach dem Hessischen Gesetz über die öffentliche Sicherheit und Ordnung (HSOG) und dem Gesetz über das Landesamt für Verfassungsschutz (LfV-Gesetz) zu regeln.

B. Bestandsdatenauskunft im HSOG

I. „Klassische" Bestandsdatenauskunft, § 15a Abs. 2 S. 3 HS. 1 HSOG-E i.V.m. § 113 Abs. 1 S. 1 TKG

1. Anforderungen des BVerfG

Wie bereits ausgeführt greift die „klassische" Bestandsdatenabfrage, d.h. ohne die Zuordnung von dynamischen IP-Adressen, nicht in den Schutzbereich des Telekommunikationsgeheimnisses gem. Art. 10 GG ein. Maßstab ist im Schwerpunkt vielmehr das Recht auf informationelle Selbstbestimmung gem. Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG.

Das Bundesverfassungsgericht führt in seiner Entscheidung aus, dass im Abruf der Daten seitens der auskunftsberechtigten Behörden in Form des Verlangens ein eigenständiger Eingriff liegt, der nach dem gesetzgeberischen Regelungskonzept einer weiteren eigenen fachrechtlichen Rechtsgrundlage bedarf.[11]

Weil der Bund auf der Grundlage des Art. 73 Abs. 1 Nr. 7 GG nur die Öffnung der Datenbestände für die staatliche Aufgabenwahrnehmung regeln kann, nicht aber auch den Zugriff auf diese Daten selbst, muss die Inpflichtnahme der Telekommunikationsdiensteanbieter als private Auskunftspersonen in Materien, die der Regelung der Länder vorbehalten sind, in der Abrufnorm geregelt werden. Hierfür reichen Rechtsgrundlagen nicht aus, die bloß eine schlichte Datenerhebung von frei zugänglichen Informationen erlauben, nicht aber auch selbst eine Auskunftspflicht Dritter begründen (wie etwa § 13 Abs. 1 des Hessischen Gesetzes über die öffentliche Sicherheit und Ordnung).[12]

Auch mit Rücksicht auf den Grundsatz der Normenklarheit, dem bei Eingriffen in das Recht auf informationelle Selbstbestimmung eine spezifische Funktion zukommt, ist zu verlangen, dass für die Datenabfrage in Form eines unmittelbar an private Dritte gerichteten Auskunftsverlangens spezifische Rechtsgrundlagen vorliegen, die eine Auskunftsverpflichtung der Telekommunikationsunternehmen eigenständig begründen. Das Bundesverfassungsgericht führt in diesem Zusammenhang weiter aus: Wenn eine

[11] BVerfG, Beschl. v. 24.01.2012 – 1 BvR 1299/05, Rn. 125, 167.
[12] BVerfG, Beschl. v. 24.01.2012 – 1 BvR 1299/05, Rn. 167.

gesetzliche Regelung zu einem Eingriff in das Recht auf informationelle Selbstbestimmung ermächtigt, so hat das Gebot der Bestimmtheit und Klarheit auch die spezifische Funktion, eine hinreichend präzise Umgrenzung des Verwendungszwecks der betroffenen Informationen sicherzustellen. Auf diese Weise wird das verfassungsrechtliche Gebot der Zweckbindung der erhobenen Informationen verstärkt. Anlass, Zweck und Umfang des jeweiligen Eingriffs sind dabei durch den Gesetzgeber bereichsspezifisch, präzise und normenklar festzulegen. Bei gestuften oder in verschiedene Eingriffe gegliederten Formen des Informationsaustauschs erstreckt sich das Gebot der Normenklarheit auf jede dieser Stufen.

Das Bundesverfassungsgericht führt in seiner Entscheidung weiter aus, dass es zur Begründung von Auskunftspflichten Privater vielmehr klarer Bestimmungen bedarf, gegenüber welchen Behörden die Anbieter konkret zur Datenübermittlung verpflichtet sein sollen. Nur dies rechtfertigt dann auch den Eingriff in das Recht auf informationelle Selbstbestimmung gegenüber den Datenbetroffenen. Eine solche Regelung treffen aber nicht solche Vorschriften, die – wie etwa § 8 Abs. 1 Bundesverfassungsschutzgesetz oder § 21 Abs. 1 Bundespolizeigesetz – lediglich eine Datenerhebungsbefugnis ohne ausdrückliche Auskunftsverpflichtung gegenüber Dritten enthalten.

2. Eingriffsvoraussetzungen des § 15a Abs. 2 S. 3 HS. 1 HSOG-E

Die für die Bestandsdatenauskunft erforderliche spezifische Ermächtigungsgrundlage regelt nunmehr § 15a Abs. 2 S. 3 HS. 1 HSOG-E.

Inhaltlich greift die Vorschrift auf die bereits bestehende Auskunftsregelung in § 12 HSOG mit Ausnahme von dessen Abs. 2 zurück. Die Befragung von Personen durch die Polizei nach § 12 HSOG ist zulässig, wenn tatsächliche Anhaltspunkte die Annahme rechtfertigen, dass die Person sachdienliche Angaben zur Aufklärung des Sachverhalts in einer polizeilichen Angelegenheit machen kann. Ergänzend sind gem. § 12 Abs. 3 HSOG die Vorschriften über die Verarbeitung personenbezogener Daten anzuwenden.

§ 12 Abs. 3 S. 3 HSOG-E begründet laut Gesetzesbegründung in den Fällen des § 12 Abs. 1 HSOG zugleich eine Auskunftspflicht des Telekommunikationsunternehmens.[13] § 12 Abs. 2 HSOG wurde bewusst von der Anwendung ausgenommen, da sonst eine Auskunftspflicht der Telekommunikationsunternehmen, die regelmäßig Nichtstörer sind, nur bestünde, wenn eine gegenwärtige erhebliche Gefahr abzuwehren wäre.[14] Die Gesetzesbegründung stellt zu Recht fest, dass die Bestandsdaten nicht dem Telekommunikationsgeheimnis gem. Art. 10 Abs. 1 GG unterliegen. Daraus folgert sie,

[13] LT-Drs. 18/7137, 4.
[14] LT-Drs. 18/7137, 4.

dass § 12 Abs. 1 HSOG zusammen mit den ergänzend heranzuziehenden Vorschriften über die Erhebung personenbezogener Daten ein ausreichendes Schutzniveau gewährleistet.[15]

Kritisch ist hierzu jedoch anzumerken, dass Maßnahmen, die nach § 12 Abs. 1 HSOG vorgenommen werden, offen dem Betroffenen gegenüber erfolgen, während hingegen die Bestandsdatenauskunft eine heimliche Maßnahme darstellt, von denen der Betroffene keine Kenntnis nimmt.

Ein heimlicher Eingriff in Grundrechte wiegt stets schwerer als ein offen ausgeführter Grundrechtseingriff.[16] Vor diesem Hintergrund wäre zu überlegen, ob nicht der Bestandsdatenabruf an zusätzliche verfahrensrechtliche Schutzvorkehrungen gebunden werden sollte. Zu denken wäre zunächst an einen Richter- oder einen sonstigen Kontrollvorbehalt, um den Grundrechten des Betroffenen bereits bei der Entscheidung über einen Bestandsdatenabruf Rechnung zu tragen. Allerdings müssen von Verfassungs wegen nicht alle heimlichen Grundrechtseingriffe unter Richtervorbehalt gestellt werden. Maßgeblich kommt es hierfür vor allem auf die Intensität des jeweils geregelten Grundrechtseingriffs an.[17] Bei Grundrechtseingriffen geringerer Intensität bietet sich auch ein sog. Behördenleitervorbehalt an. Einen solchen Vorbehalt sieht beispielsweise der nordrhein-westfälische Gesetzesentwurf zur Bestandsdatenabfrage vor, vgl. § 20a Abs. 3 S. 1 PolG NRW-E.[18] Zudem ist in diesem Entwurf vorgesehen, dass der Antrag der Schriftform bedarf und die Anordnung die tragenden Erkenntnisse für das Vorliegen der Gefahr und die Begründung der Verhältnismäßigkeit der Maßnahme sowie – soweit vorhanden – weitere Angaben anzugeben hat.[19]

Daneben stellt sich die Frage, ob der Betroffene zumindest im Anschluss an einen heimlich durchgeführten Bestandsdatenabruf von dem Abruf zu benachrichtigen ist, damit er seine informationelle Stellung gegenüber der handelnden Behörde einschätzen und gegebenenfalls Rechtsbehelfe einlegen kann. Die Heimlichkeit der Maßnahme führt nämlich dazu, dass der effektive Rechtsschutz der Betroffenen einstweilen vereitelt wird.

Das BVerfG hat daher dem Gesetzgeber sehr strikte Vorgaben für die nachträgliche Benachrichtigung auferlegt:

---

[15] LT-Drs. 18/7137, 4.
[16] vgl. BVerfGE 115, 166, 196; BVerfG, WM 2008, 503, 508; *Petri* in: Lisken/Denninger, Handbuch des Polizeirechts, 5. Aufl. 2012, Kapitel G, Rn. 51.
[17] BVerfGE 125, 260, 337; BVerfGE 120, 274, 331; BVerfGE 118, 168, 202.
[18] LT-Drs. 16/2256.
[19] LT-Drs. 16/2256.

> *„Bei nicht erkennbaren Eingriffen steht dem Grundrechtsträger auf Grund der Gewährleistung effektiven Grundrechtsschutzes grundsätzlich ein Anspruch auf spätere Kenntnis der staatlichen Maßnahme zu [...]. Ohne eine solche Kenntnis können die Betroffenen weder die Unrechtmäßigkeit der Informationsgewinnung noch etwaige Rechte auf Löschung der Aufzeichnungen geltend machen."*[20]

Jedoch ist eine aktive Benachrichtigung des Betroffenen nach einem heimlichen Eingriff nicht durchweg verfassungsrechtlich geboten. Auch hier ist die Intensität des jeweils geregelten Grundrechtseingriffs entscheidend. [21] Für eine etwaige Benachrichtigungspflicht ist zudem bedeutsam, ob für den Betroffenen auch ohne aktive Benachrichtigung eine hinreichende und zumutbare Möglichkeit besteht, von dem Eingriff Kenntnis zu nehmen. [22] Eine derartige Benachrichtigungspflicht enthält beispielsweise die geplante Regelung zur Bestandsdatenabfrage in NRW, vgl. § 20a Abs. 4 PolG NRW-E.[23]

Zu berücksichtigen ist dabei, dass die Benachrichtigungspflicht denselben Schranken unterliegt wie das materiell betroffene Grundrecht selbst, also gesetzlich vorübergehend ausgesetzt werden kann. Die (zeitweise) Geheimhaltung bedarf dann aber ihrerseits – insbesondere hinsichtlich ihrer zeitlichen Dauer – der Rechtfertigung am Maßstab der Verhältnismäßigkeit. Daraus folgt, dass Betroffene von allen heimlichen Eingriffen *sobald als irgend möglich* zu benachrichtigen sind.[24] Ausnahmen sind nur so lange möglich, wie der Zweck der Datenerhebung dies (weiter) verhältnismäßig erscheinen lässt, oder insoweit, als die Betroffenen anderweitig ohnehin tatsächlich informiert werden.

Ein kumulativer Verzicht sowohl auf eine unabhängige Vorabkontrolle als auch auf eine nachträgliche Benachrichtigung des Betroffenen erscheint bei heimlichen Eingriffen nur dann zulässig zu sein, wenn diese – trotz der Heimlichkeit – lediglich geringes Gewicht aufweisen, es sich also um einen Bagatelleingriff handelt. Denn wenn beide

---

[20] BVerfGE 109, 279, 364.
[21] BVerGE 130, 151, 210; BVerfGE 125, 260, 346 f.
[22] BVerfGE 118m 168, 200 u. 208 ff.; so auch *Bäcker* in Stellungnahme zu dem Entwurf eines Gesetzes zur Änderung des Telekommunikationsgesetzes und zur Neuregelung der Bestandsdatenauskunft (BT-Drs. 17/12034), S. 9.
[23] LT-Drs. 16/2256.
[24] So *Buermeyer* in Stellungnahme zu dem Antrag der Fraktion der PIRATEN zum Schutz der Vertraulichkeit und Anonymität der Telekommunikation (LT-Drs. 16/1467), S. 12.

Sicherungsmaßnahmen fehlen, wird die Exekutive faktisch sehr weitgehend von einer Grundrechtskontrolle durch eine unabhängige Stelle freigestellt.

Zur rechtspolitischen Verdeutlichung, dass die heimliche Abfrage von Bestandsdaten sensible Bereiche des Datenschutzes berührt und nach rechtsstaatlichen Grundsätzen andere weniger eingreifende – insbesondere offen vorgenommene – Maßnahmen vorrangig einzusetzen sind, wäre auch ein ausdrücklicher Erforderlichkeits- bzw. ein Subsidiaritätsvorbehalt möglich gewesen. So sieht § 20a Abs. 1 S. 2 HS. 1 PolG NRW-E vor, dass eine Bestandsdatenabfrage nur zulässig ist, „soweit die Erreichung des Zwecks der Maßnahme auf andere Weise aussichtslos oder wesentlich erschwert wäre".[25]

3. Kein Richtervorbehalt aufgrund der Änderung des § 15a Abs. 5 S. 1 HSOG-E

Die Bestandsdatenabfrage wurde durch die Änderung des § 15a Abs. 5 S. 1 HSOG-E bewusst von einem Richtervorbehalt ausgenommen. Laut Gesetzesbegründung soll die Bestandsdatenauskunft gerade nicht dieser restriktiven Regelung unterfallen.[26] Insoweit geht diese Regelung – worauf die Gesetzesbegründung auch hinweist – mit den entsprechenden Regelungen auf Bundesebene konform, die für die Bestandsdatenauskunft grundsätzlich ebenfalls keinen Richtervorbehalt vorsehen.[27]

II. Bestandsdatenauskunft anhand dynamischer IP-Adressen, § 15a Abs. 2 S. 3 HS. 1 und S. 4 HSOG-E i.V.m. § 113 Abs. 1 S. 3 TKG

1. Anforderungen des BVerfG

Das Bundesverfassungsgericht begründet in seiner Entscheidung vom 24.01.2012[28] – wie oben erwähnt –, dass die identifizierende Zuordnung dynamischer IP-Adressen in den Schutzbereich des Art. 10 Abs. 1 GG fällt, weil sie eine besondere Nähe zu konkreten Telekommunikationsvorgängen aufweisen. Allerdings ergibt sich dies, wie das Bundesverfassungsgericht ausführt, nicht schon daraus, dass sich die Zuordnung einer dynamischen IP-Adresse notwendig immer auf einen bestimmten Telekommunikationsvorgang bezieht, über den sie mittelbar damit ebenso Auskunft gibt. Denn auch insoweit bezieht sich die Auskunft selbst nur auf Daten, die einem Anschlussinhaber abstrakt zugewiesen sind. Es besteht insoweit kein grundsätzlicher

[25] LT-Drs. 16/2256.
[26] LT-Drs. 18/7137, S. 4.
[27] Vgl. bspw. § 22a BPolG-E (BT-Drs. 17/12034, S. 7 und BT-Drs. 17/12879, S. 6).
[28] BVerfG, Beschl. v. 24.01.2012 – 1 BvR 1299/05, Rn. 116.

Unterschied zu der Zuordnung statischer IP-Adressen. Die Anwendbarkeit des Art. 10 Abs. 1 GG begründet sich hier jedoch daraus, dass die Telekommunikationsunternehmen für die Identifizierung einer dynamischen IP-Adresse in einem Zwischenschritt die entsprechenden Verbindungsdaten ihrer Kunden sichten müssen, also auf konkrete Telekommunikationsvorgänge zugreifen. Diese von den Diensteanbietern einzeln gespeicherten Telekommunikationsverbindungen fallen unter das Telekommunikationsgeheimnis, unabhängig davon, ob sie von den Diensteanbietern aufgrund gesetzlicher Verpflichtung vorrätig gehalten werden müssen oder von ihnen auf vertraglicher Grundlage gespeichert werden. Soweit der Gesetzgeber die Telekommunikationsunternehmen dazu verpflichtet, auf diese Daten zurückzugreifen und sie für die staatliche Aufgabenwahrnehmung auszuwerten, liegt darin ein Eingriff in Art. 10 Abs. 1 GG. Dies ist nicht nur dann der Fall, wenn die Diensteanbieter die Verbindungsdaten selbst herausgeben müssen, sondern auch dann, wenn sie sie als Vorfrage für eine Auskunft nutzen müssen.

Zudem führt das Bundesverfassungsgericht[29] aus, dass die Befugnis zur Identifizierung dynamischer IP-Adressen hinreichend normenklar geregelt werden muss. 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 nicht gleichgesetzt werden. Insoweit bedarf es einer hinreichend klaren Entscheidung des Gesetzgebers, ob und unter welchen Voraussetzungen eine solche Identifizierung erlaubt werden soll. Eine entsprechende Eingriffsgrundlage muss erkennen lassen, dass die Telekommunikationsunternehmen in Vorbereitung solcher Auskünfte darüber hinaus auch die Verkehrsdaten nach § 96 TKG auszuwerten berechtigt und verpflichtet sein könnten.

2. Anforderungen des § 15a Abs. 2 S. 3 HS. 1, S. 4 HSOG-E

Der Abruf der Bestandsdaten anhand von dynamischen IP-Adressen wird im Vergleich zum „klassischen“ Bestandsdatenabruf an erhöhte materiell-rechtliche sowie verfahrensrechtliche Voraussetzungen geknüpft.

So räumt § 15a Abs. 2 S. 4 HSOG-E die Befugnis zur Auskunft über Bestandsdaten anhand einer dynamischen IP-Adresse „nur zur Abwehr einer gegenwärtigen erheblichen Gefahr“ ein. Die Voraussetzungen orientieren sich dabei hinsichtlich der

[29] BVerfG, Beschl. v. 24.01.2012 – 1 BvR 1299/05, Rn. 174.

Anforderungen an den Gefahrbegriff laut Gesetzesbegründung an § 9 HSOG, der die Inanspruchnahme nicht verantwortlicher Personen regelt.

Eine gegenwärtige Gefahr liegt vor, wenn die Einwirkung des schädigenden Ereignisses bereits begonnen hat oder wenn diese Einwirkung unmittelbar oder in allernächster Zeit mit einer an Sicherheit grenzender Wahrscheinlichkeit bevorsteht.[30] Mit der Voraussetzung einer gegenwärtigen Gefahr fordert das Gesetz folglich eine stärkere zeitliche Nähe des zu erwartenden Schadenseintritts. Mit der Voraussetzung der erheblichen Gefahr hingegen steigert der Gesetzgeber die Anforderungen in qualitativer Hinsicht. Eine solche liegt vor, wenn es sich um eine Gefahr für ein bedeutendes Rechtsgut handelt. Solche Rechtsgüter sind Leben, Gesundheit, Freiheit, Eigentum und sonstige Rechtsgüter von bedeutendem Wert.[31]

Durch § 15a Abs. 2 S. 4 HSOG-E werden also – im Gegensatz zu den Regelungen auf Bundesebene, die keine höheren Anforderungen an die Bestandsdatenauskunft anhand dynamischer IP-Adressen im Vergleich zur „klassischen“ Bestandsdatenauskunft stellen – erhöhte Anforderungen sowohl in zeitlicher Hinsicht als auch hinsichtlich des geschützten Rechtsguts gestellt.

Der Gesetzesentwurf zur Bestandsdatenspeicherung in NRW[32] hingegen nimmt vom Vorliegen einer gegenwärtigen Gefahr ausdrücklich Abstand. In der Begründung heißt es dazu: „Diese würde oftmals keine effektive Gefahrenabwehr ermöglichen, da insbesondere bei Einsatzlagen mit suizidgefährdeten oder vermissten Personen zwar eine hohe Wahrscheinlichkeit besteht, dass ein Schaden eintritt, nicht jedoch klar ist, dass dies zeitlich ganz unmittelbar bevorsteht oder schon begonnen hat.“[33] Aus datenschutzrechtlichen Gründen ist es selbstverständlich zu begrüßen, dass nur unter den engeren Voraussetzungen des Vorliegens einer gegenwärtigen Gefahr Bestandsdaten anhand dynamischer IP-Adressen abgefragt werden dürfen. Zu bedenken ist jedoch, ob dies mit den polizeilichen Zwecken der Norm vereinbar ist.

Als verfahrensrechtliche Absicherung enthält § 15a Abs. 2 S. 4 HS. 2 HSOG-E i.V.m. § 29 Abs. 6 HSOG zu Recht eine Benachrichtigungspflicht des Betroffenen für die Abfrage von Bestandsdaten anhand dynamischer IP-Adressen. § 29 HSOG regelt dabei die weiteren Details der Benachrichtigung.

Durch die explizite Nennung der „Auskunft über Bestandsdaten anhand einer zu bestimmten Zeitpunkten zugewiesenen Internetprotokoll-Adresse“ kommt die Vorschrift den Anforderungen des Bundesverfassungsgerichts an eine

[30] *Schmidbauer* in: Schmidbauer/Steiner, Bayerisches Polizeiaufgabengestz, 3. Aufl. 2011, Art. 10 Rn. 9.
[31] *Schmidbauer* in: Schmidbauer/Steiner, Bayerisches Polizeiaufgabengestz, 3. Aufl. 2011, Art. 10 Rn. 10.
[32] LT-Drs. 16/2256.
[33] LT-Drs. 16/2256, S. 23.

bereichsspezifische, normenklare Regelung nach. Allerdings sollte der Wortlaut – den Empfehlungen des Innenausschusses[34] zur bundesgesetzlichen Regelung entsprechend – folgendermaßen angepasst werden:

„Auskunft über Bestandsdaten anhand einer zu einem bestimmten Zeitpunkt zugewiesenen Internetprotokoll-Adresse".

Durch diese geringfügige Wortlautänderung wird – laut Innenausschuss – klargestellt, dass die Bestandsdatenabfrage nach einer IP-Adresse immer anhand eines konkreten Zeitpunktes erfolgen muss, zu dem die IP-Adresse einem Nutzer zugewiesen war.[35]

3. Kein Richtervorbehalt aufgrund der Änderung des § 15a Abs. 5 S. 1 HSOG-E

Auch die Bestandsdatenabfrage anhand dynamischer IP-Adressen wurde durch die Änderung des § 15a Abs. 5 S. 1 HSOG-E bewusst von einem Richtervorbehalt ausgenommen.

Dies ist allerdings im Vergleich zur „klassischen" Bestandsdatenabfrage kritischer zu sehen.

Der Richtervorbehalt als zentrale formelle Eingriffsvoraussetzung im deutschen Strafprozess- und Sicherheitsrecht bezweckt stellvertretenden Rechtsschutz für den Betroffenen durch eine neutrale, unabhängige Instanz, wenn die Betroffenen selbst ihre rechtlichen Interessen aufgrund der Heimlichkeit der Maßnahmen (noch) nicht selbst wahrnehmen können. Maßgeblich kommt es hierfür – wie oben ausgeführt – vor allem auf die Intensität des jeweils geregelten Grundrechtseingriffs an.[36] Nach dem Bundesverfassungsgericht waren bislang heimliche Eingriffe in den Schutzbereich des Art. 10 Abs. 1 – wie dies bei der Bestandsdatenabfrage anhand dynamischer IP-Adressen der Fall ist – entgegen Eingriffen in die informationelle Selbstbestimmung zumeist an einen Richtervorbehalt geknüpft.

III. Auskunft über Zugangssicherungscodes, § 15a Abs. 2 S. 3 HS. 2 i.V.m. § 113 Abs. 1 S. 2 TKG

1. Anforderungen des BVerfG

Nach Auffassung des Bundesverfassungsgerichts ist die Norm verfassungsrechtlichen Einwänden nicht schon deshalb ausgesetzt, weil sie überhaupt einen Zugriff auf die von

[34] BT-Drs. 17/12879.
[35] BT-Drs. 17/12879, S. 10.
[36] BVerfGE 125, 260, 337; BVerfGE 120, 274, 331; BVerfGE 118, 168, 202.

der Vorschrift betroffenen Daten der Zugangssicherung zulässt.[37] Es handelt sich um einen Eingriff in das Grundrecht auf informationelle Selbstbestimmung, der nach allgemeinen Grundsätzen rechtfertigungsfähig ist.

§ 113 Abs. 1 S. 2 TKG betrifft Daten, die als Zugangssicherungscodes (wie Passwörter, PIN oder PUK) den Zugang zu Endgeräten und Speicherungseinrichtungen sichern und damit die Betreffenden vor einem Zugriff auf die entsprechenden Daten beziehungsweise Telekommunikationsvorgänge schützen.[38] Die Vorschrift macht die Zugangssicherungscodes den Behörden zugänglich und versetzt sie damit in die Lage, die entsprechenden Barrieren zu überwinden.

Nach Ansicht des Bundesverfassungsgerichts gebietet es der Verhältnismäßigkeitsgrundsatz jedoch, dass die Behörden die in § 113 Abs. 1 S. 2 TKG geregelten Zugangscodes nicht unabhängig von den Anforderungen an deren Nutzung und damit gegebenenfalls unter leichteren Voraussetzungen abfragen können sollen.[39] Die Erhebung der in § 113 Abs. 1 S. 2 TKG geregelten Zugangsdaten ist mit Blick auf die dort verfolgten Zwecke nur dann erforderlich, wenn auch die Voraussetzungen von deren Nutzung gegeben sind.[40] Die Frage, wann die Behörden von den Sicherungscodes Gebrauch machen und auf die durch sie gesicherten Daten und Telekommunikationsvorgänge Zugriff nehmen dürfen, bestimmt sich nach eigenständigen Rechtsgrundlagen. Dabei unterscheiden sich die insoweit geltenden Anforderungen je nach Art des Eingriffs sowohl in formeller als auch in materieller Hinsicht. Soll etwa die Nutzung des Zugangscodes eine Online-Durchsuchung oder die Überwachung eines noch nicht abgeschlossenen Telekommunikationsvorgangs ermöglichen, setzt dies nach näherer Maßgabe des Fachrechts die Einhaltung strenger materieller Anforderungen und eine richterliche Anordnung oder Bestätigung voraus (vgl. §§ 100a, 100b StPO).[41] Sollen demgegenüber mit dem Code nach Beschlagnahme eines Mobiltelefons auf diesem abgelegte Daten ausgelesen werden, können hierfür geringere Eingriffsschwellen ausreichen. So bedarf es etwa strafprozessrechtlich bei Beschlagnahme unter Gefahr im Verzug keiner vorherigen richterlichen Anordnung (vgl. § 98 Abs. 1 StPO) und auch nur unter gewissen weiteren Voraussetzungen einer nachfolgenden gerichtlichen Bestätigung (vgl. § 98 Abs. 2 StPO).[42]

Der Verhältnismäßigkeitsgrundsatz gebietet allerdings auch nicht umgekehrt, die Erhebung der Zugangscodes ausnahmslos unter die Voraussetzungen zu stellen, die für

[37] BVerfG, Beschl. v. 24.01.2012 – 1 BvR 1299/05, Rn. 182.
[38] BVerfG, Beschl. v. 24.01.2012 – 1 BvR 1299/05, Rn. 184.
[39] BVerfG, Beschl. v. 24.01.2012 – 1 BvR 1299/05, Rn. 183, 185.
[40] BVerfG, Beschl. v. 24.01.2012 – 1 BvR 1299/05, Rn. 185.
[41] BVerfG, Beschl. v. 24.01.2012 – 1 BvR 1299/05, Rn. 184.
[42] BVerfG, Beschl. v. 24.01.2012 – 1 BvR 1299/05, Rn. 184.

deren eingriffsintensivste („maximale“) Nutzungsmöglichkeit gegeben sein müssen.[43] Erforderlich für eine effektive Strafverfolgung und Gefahrenabwehr ist lediglich, die Auskunftserteilung über solche Zugangssicherungen an diejenigen Voraussetzungen zu binden, die bezogen auf den in der Abfragesituation damit konkret erstrebten Nutzungszweck zu erfüllen sind.[44]

2. Eingriffsvoraussetzungen des § 15a Abs. 2 S. 3 HS. 2 HSOG-E

§ 15a Abs. 2 S. 3 HS. 2 HSOG-E sieht für die Abfrage von Daten, mittels derer der Zugriff auf Endgeräte oder auf Speichereinrichtungen, die in diesen Endgeräten oder hiervon räumlich getrennt eingesetzt werden, geschützt wird, die gleichen Eingriffsvoraussetzungen vor wie für die „klassische“ Bestandsdatenabfrage.

Wie oben bereits erläutert, greift die Vorschrift hierfür inhaltlich auf die bereits bestehende Auskunftsregelung in § 12 HSOG mit Ausnahme von dessen Abs. 2 zurück. Entscheidend ist also auch hier, ob tatsächliche Anhaltspunkte die Annahme rechtfertigen, dass die Person sachdienliche Angaben zur Aufklärung des Sachverhalts in einer polizeilichen Angelegenheit machen kann. Ergänzend werden gem. § 12 Abs. 3 HSOG die Vorschriften über die Verarbeitung personenbezogener Daten herangezogen.

Kritisch an dieser Regelung ist zunächst, dass sie die Vorgaben, die das Bundesverfassungsgericht aus dem Verhältnismäßigkeitsgrundsatz herleitet, nicht umsetzt. Die Norm lässt nämlich nicht erkennen, dass die Behörden die in § 113 Abs. 1 S. 2 TKG geregelten Zugangscodes nicht unabhängig von den Anforderungen an deren Nutzung und damit gegebenenfalls unter leichteren Voraussetzungen abfragen dürfen. Die vergleichbare Regelung auf Bundesebene sieht hierfür vor, dass „die Auskunft nur verlangt werden [darf], wenn die gesetzlichen Voraussetzungen für die Nutzung der Daten vorliegen.“[45] Die Aufnahme einer entsprechenden Passage in den Normtext wird aus Verhältnismäßigkeitsgesichtspunkten dringend angeraten.

Weiterhin ist an dieser Vorschrift problematisch, dass sie nur äußerst geringe materiell-rechtliche und keine verfahrensrechtlichen Eingriffsvoraussetzungen hat (vgl. oben). So sieht der Entwurf für die Bestandsdatenabfrage in NRW einen Behördenleitervorbehalt vor, vgl. § 20a Abs. 3 PolG NRW-E.[46] Die Regelungen auf Bundesebene sehen nach der Umgestaltung durch den Innenausschuss sogar vor, dass dieses Auskunftsverlangen „nur auf Antrag des Präsidenten des Bundeskriminalamtes oder seines Vertreters durch das Gericht angeordnet werden“ darf (vgl. § 22 BKAG-E) bzw. „nur auf Antrag des Leiters

[43] BVerfG, Beschl. v. 24.01.2012 – 1 BvR 1299/05, Rn. 185.
[44] BVerfG, Beschl. v. 24.01.2012 – 1 BvR 1299/05, Rn. 185.
[45] BT-Drs. 17/12034.
[46] LT-Drs. 16/2256.

der in der Rechtsverordnung nach § 58 Abs. 1 [BPolG] bestimmten Bundespolizeibehörde oder seines Vertreters durch das Gericht angeordnet werden“ darf (vgl. § 22a BPolG-E).[47]

Auch eine Benachrichtigungsregelung ist nicht vorgesehen, sodass Betroffene nicht über den heimlichen Zugriff auf Zugangssicherungscodes informiert werden müssten.

In der Literatur wird hinsichtlich der auf Bundesebene geregelten strafprozessualen Bestandsdatenauskunft über Zugangssicherungscodes vertreten, dass sowohl ein Richtervorbehalt als auch eine nachträgliche Benachrichtigungspflicht verfassungsrechtlich geboten sind. [48] Maßgeblich hierfür sei die besondere Eingriffsintensität der Zugangsdatenabfrage. Zwar diene diese Datenerhebung letztlich dazu, weitere Daten zu erlangen oder zu entschlüsseln. Diese weiteren Daten können wiederum mit unterschiedlichen Maßnahmen gewonnen werden, die unterschiedlich intensiv in Grundrechte eingreifen. Die Eingriffsintensität einer Zugangsdatenabfrage könne in der Folge – insoweit ähnlich wie bei der Zuordnung einer IP-Adresse – nicht pauschal bestimmt werden. Die Zugangsdatenabfrage zeitige aber in jedem Fall eine zusätzliche eigenständige und erhebliche Eingriffswirkung dadurch, dass sie den informationellen Selbstschutz des Betroffenen vereitelt und so sein Vertrauen in die Privatheit seiner Kommunikationsbeziehungen frustriere. Angesichts dessen müsse zum einen das Geheimhaltungsinteresse des Betroffenen, das sich in der Zugangssicherung manifestiert, vor der Entscheidung über den Bruch dieser Sicherung von einer unabhängigen Stelle mit den gegenläufigen hoheitlichen Erkenntnisinteressen abgewogen werden. Zum anderen müsse der Betroffene über die Vereitelung seines informationellen Selbstschutzes informiert werden, um einschätzen zu können, welche Kenntnisse die Behörden über ihn erlangen konnten.[49]

3. Kein Richtervorbehalt aufgrund der Änderung des § 15a Abs. 5 S. 1 HSOG-E

Vor diesem Hintergrund ist es besonders kritisch zu sehen, dass aufgrund der Änderung des § 15a Abs. 5 S. 1 HSOG-E auch die Bestandsdatenauskunft hinsichtlich Zugangssicherungscodes vom Richtervorbehalt ausgenommen wurde.

---

[47] BT-Drs. 17/12879.
[48] *Bäcker* in Stellungnahme zu dem Entwurf eines Gesetzes zur Änderung des Telekommunikationsgesetzes und zur Neuregelung der Bestandsdatenauskunft (BT-Drs. 17/12034), S. 12.
[49] Vgl. zum Ganzen *Bäcker* in Stellungnahme zu dem Entwurf eines Gesetzes zur Änderung des Telekommunikationsgesetzes und zur Neuregelung der Bestandsdatenauskunft (BT-Drs. 17/12034), S. 12.

C. Entfristung des HSOG, Art. 1 Nr. 3 des Entwurfs

Das HSOG gilt nur befristet und tritt gem. § 115 Abs. 2 HSOG mit Ablauf des 31.12.2014 außer Kraft. Diese Befristung entfällt durch die geplante Aufhebung des § 115 Abs. 2 HSOG. Laut Gesetzesbegründung soll dadurch die im Beschluss der Landesregierung vom 04.10.2011 vorgesehene Entfristung des HSOG umgesetzt werden.

Dieser Beschluss der Landesregierung ist nicht veröffentlicht, sodass zu den Gründen nicht Stellung genommen werden kann.

Die Befristung der Normgebung ist jedoch alte Polizeirechtstradition.[50] Die Befristung dient dem Gesetzgeber als Warnsignal, sich über eine Verlängerung und eventuelle Novellierung rechtzeitig Gedanken zu machen.[51]

Moderne Überwachungs- und Fahndungsmethoden, z.B. die akustische Wohnraumüberwachung oder die Online-Durchsuchung, erfordern einen hohen legislatorischen, darüber hinaus aber auch einen technischen, personellen und damit finanziellen Aufwand.[52] Dieser Kostenaufwand auf der einen Seite und auf der anderen Seite der Umstand, dass es sich bei allen diesen Maßnahmen um erhebliche, zum Teil schwere und schwerste Grundrechtseingriffe handelt, sollten Grund genug sein, den Gesetzgeber bereits vor einer Regelung jeweils zu einer gründlichen Prüfung zu veranlassen, ob eine solche Maßnahme polizeilich notwendig und auch verhältnismäßig ist und unter welchen näheren Voraussetzungen.[53] Doch die Lebensverhältnisse, aber auch die technischen Entwicklungen in diesen Bereichen erweisen sich als so komplex und jegliche Prognosen als so ungewiss, dass jede Regelung den Charakter eines mit „vielen Unsicherheiten belasteten Experiments“ annimmt.[54]

Verfassungsrechtlich hat dies die Konsequenz, dass sich der Gesetzgeber nicht nur im Technik- und Umweltrecht, sondern auch in der Abwehr und Verfolgung von Kriminalität am Konzept eines „dynamischen Grundrechtsschutzes“ ausrichten muss.[55] Dies erfordert eine fortlaufende Beobachtung sowohl der zur Regelung anstehenden tatsächlichen Verhältnisse als auch eine gezielte und systematisch aufbereitete Erfassung der Folgewirkungen des Einsatzes neuer rechtlicher Instrumente.[56] Eine erfolgreiche, qualitativ aussagekräftige und praktisch folgenreiche Evaluation setzt mithin in zeitlicher Folge fünf Schritte voraus:[57]

---

[50] *Denninger* in: Lisken/Denninger, Handbuch des Polizeirechts, 5. Aufl. 2012, Kapitel B, Rn. 69.
[51] *Denninger* in: Lisken/Denninger, Handbuch des Polizeirechts, 5. Aufl. 2012, Kapitel B, Rn. 69.
[52] Vgl. *Denninger* in: Lisken/Denninger, Handbuch des Polizeirechts, 5. Aufl. 2012, Kapitel B, Rn. 66.
[53] Vgl. *Denninger* in: Lisken/Denninger, Handbuch des Polizeirechts, 5. Aufl. 2012, Kapitel B, Rn. 66.
[54] *Denninger* in: Lisken/Denninger, Handbuch des Polizeirechts, 5. Aufl. 2012, Kapitel B, Rn. 66.
[55] *Denninger* in: Lisken/Denninger, Handbuch des Polizeirechts, 5. Aufl. 2012, Kapitel B, Rn. 67.
[56] *Denninger* in: Lisken/Denninger, Handbuch des Polizeirechts, 5. Aufl. 2012, Kapitel B, Rn. 67.
[57] *Denninger* in: Lisken/Denninger, Handbuch des Polizeirechts, 5. Aufl. 2012, Kapitel B, Rn. 68.

- Befristung,
- Beobachtung,
- Berichterstattung,
- Bewertung und
- Besserung.

Vor dem Hintergrund, dass dem Gesetzgeber der Drang verloren geht, die weiteren, oben angeführten Punkte zu beachten, wenn von einer Befristung abgesehen wird, ist diese Entwicklung durchaus als kritisch zu betrachten. Eine sinnvolle Gesetzesevaluierung würde dann nämlich nicht mehr stattfinden.

D. Bestandsdatenauskunft im LfV-Gesetz

I. „Klassische“ Bestandsdatenauskunft, § 4a Abs. 3 HS. 1 LfVG-E i.V.m. § 113 Abs. 1 S. 1 TKG

1. Anforderungen des BVerfG

Zu den verfassungsrechtlichen Anforderungen an die Rechtsgrundlage der „klassischen“ Bestandsdatenauskunft vgl. oben die Ausführungen zu B.I.1.

2. Eingriffsvoraussetzungen

Die für die Bestandsdatenauskunft erforderliche spezifische Ermächtigungsgrundlage regelt nunmehr § 4a Abs. 3 LfVG-E. Die Gesetzesbegründung führt dazu aus, dass § 4a Abs. 3 LfVG-E die Auskunftspflicht der Telekommunikationsunternehmen über Bestandsdaten, über die sie aufgrund der §§ 9 und 111 TKG verfügen, regelt.[58]

Die Regelung ist vergleichbar ausgestaltet wie die schon bestehende Regelung für Auskünfte von Postdienstleistungsunternehmen oder Telemediendiensteanbietern über Daten, die für die Begründung, inhaltliche Ausgestaltung, Änderung oder Beendigung eines Vertragsverhältnisses über Postdienstleistungen oder Telemedien gespeichert werden, vgl. § 4a Abs. 1 LfVG.

Kritisch erscheint, dass die Eingriffsvoraussetzungen denkbar niedrig angesetzt sind. So ist gem. § 4a Abs. 3 S. 1 LfVG-E ausreichend, dass die Auskunft über die Bestandsdaten für die Erfüllung der Aufgaben des Landesamtes für Verfassungsschutz nach § 2 Abs. 2 LfVG erforderlich sind.

[58] LT-Drs. 18/7137, 4.

Dieses Erforderlichkeitskriterium ist die einzige Beschränkung des Zugriffs auf die Bestandsdaten.

Zwar entspricht dies der schon bestehenden Regelung des § 4a Abs. 1 LfVG. Diese Regelung ist jedoch zusätzlich „auf Einzelfälle“ beschränkt.

Zwar unterliegen die Bestandsdaten nicht dem Schutz des Art. 10 Abs. 1 GG. Selbst wenn man den „klassischen“ Bestandsdatenabruf als nur geringen Eingriff in das Grundrecht auf informationelle Selbstbestimmung (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG) betrachten will, darf nicht verkannt werden, dass dieser Eingriff dem Betroffenen gegenüber heimlich erfolgt. Wie oben unter B.I.2. bereits ausgeführt wiegt ein heimlicher Eingriff in Grundrechte stets schwerer als ein offen ausgeführter Grundrechtseingriff.[59]

Vor diesem Hintergrund wäre auch für das LfVG zu überlegen, ob nicht der Bestandsdatenabruf an zusätzliche verfahrensrechtliche Schutzvorkehrungen gebunden werden sollte.[60]

Für Grundrechtseingriffe geringerer Intensität bietet sich auch hier ein Behördenleitervorbehalt an. Zudem wäre es auch hier empfehlenswert, dass der Antrag der Schriftform bedarf und die Anordnung des Behördenleiters die tragenden Erkenntnisse für die Erforderlichkeit und die Begründung der Verhältnismäßigkeit der Maßnahme sowie – soweit vorhanden – weitere Angaben anzugeben hat.

Daneben stellt sich auch hier die Frage, ob der Betroffene zumindest im Anschluss an einen heimlich durchgeführten Bestandsdatenabruf von dem Abruf zu benachrichtigen ist.[61]

Zur rechtspolitischen Verdeutlichung, dass die heimliche Abfrage von Bestandsdaten sensible Bereiche des Datenschutzes berührt und nach rechtsstaatlichen Grundsätzen andere weniger eingreifende – insbesondere offen vorgenommene – Maßnahmen vorrangig einzusetzen sind, wäre auch ein ausdrücklicher Subsidiaritätsvorbehalt möglich. So könnte die Norm um eine zum Ausdruck bringende Formulierung ergänzt werden, dass eine Bestandsdatenabfrage nur zulässig ist, „soweit die Erreichung des Zwecks der Maßnahme auf andere Weise aussichtslos oder wesentlich erschwert wäre“.

[59] vgl. BVerfGE 115, 166, 196; BVerfG, WM 2008, 503, 508; *Petri* in: Lisken/Denninger, Handbuch des Polizeirechts, 5. Aufl. 2012, Kapitel G, Rn. 51.
[60] Vgl. hierzu oben die Ausführungen zum Richtervorbehalt, B.I.2.
[61] Vgl. hierzu oben die Ausführungen zum Richtervorbehalt, B.I.2.

II. Bestandsdatenauskunft anhand dynamischer IP-Adressen, § 4a Abs. 3 HS. 1 LfVG-E i.V.m. § 113 Abs. 1 S. 3 TKG

1. Anforderungen des BVerfG

Zu den verfassungsrechtlichen Anforderungen an die Rechtsgrundlage der Bestandsdatenauskunft anhand dynamischer IP-Adressen vgl. oben die Ausführungen zu B.II.1.

2. Eingriffsvoraussetzungen

Der Abruf der Bestandsdaten anhand von dynamischen IP-Adressen wird an die gleichen Eingriffsvoraussetzungen geknüpft wie der „klassische“ Bestandsdatenabruf. Beide Auskünfte sind in einem gemeinsamen Satz geregelt, vgl. § 4a Abs. 3 S. 1 LfVG-E.

Überraschenderweise stellt der Entwurf des § 4a Abs. 3 S. 1 LfVG-E – im Gegensatz zur geplanten Regelung im HSOG, die eine Befugnis zur Auskunft über Bestandsdaten anhand einer dynamischen IP-Adresse „nur zur Abwehr einer gegenwärtigen erheblichen Gefahr“ zulässt – keine erhöhten materiell-rechtlichen oder verfahrensrechtlichen Anforderungen.

Einzige Restriktion der Bestandsdatenauskunft anhand von dynamischen IP-Adressen ist somit auch hier die Erforderlichkeit für die Erfüllung der Aufgaben des Landesamtes für Verfassungsschutz nach § 2 Abs. 2 LfVG. Es werden also keine erhöhten Anforderungen – weder in zeitlicher Hinsicht noch hinsichtlich des geschützten Rechtsguts – gestellt.

Dies ist bei dieser Art der Bestandsdatenabfrage verfassungsrechtlich als besonders kritisch zu betrachten, weil im Gegensatz zu „klassischen“ Bestandsdatenabfrage hier zusätzlich ein Eingriff in das Telekommunikationsgeheimnis gem. Art. 10 Abs. 1 GG vorliegt.

Zu überlegen wäre hier, ob man nicht diese Auskunft vom Vorliegen „tatsächlicher Anhaltspunkte für schwerwiegende Gefahren für die in § 2 Abs. 2 S. 1 genannten Schutzgüter“ wie dies die bereits bestehende Regelung des § 4a Abs. 2 LfVG für Finanzauskünfte und Auskünfte von Luftfahrunternehmen vorsieht, oder nur unter den Voraussetzungen des § 3 Abs. 1 des Artikel 10-Gesetzes zulässt, wie dies § 4a Abs. 3 LfVG in seiner derzeitigen Fassung tut.

Jedenfalls empfehlenswert wäre es, diese Auskunftsart unter einen Behördenleitervorbehalt oder sogar unter den Vorbehalt, wie er in § 4a Abs. 4 LfVG in seiner derzeitigen Fassung vorhanden ist („Auskünfte […] dürfen nur auf Anordnung des für den Verfassungsschutz zuständigen Ministeriums eingeholt werden. [2]Die Anordnung

ist durch die Leiterin oder den Leiter des Landesamts für Verfassungsschutz oder seine Vertreterin oder seinen Vertreter schriftlich zu beantragen. [3]Der Antrag ist zu begründen."), zu stellen.

Als verfahrensrechtliche Absicherung erscheint eine Benachrichtigungspflicht des Betroffenen über die Abfrage von Bestandsdaten anhand dynamischer IP-Adressen für geboten.

Die vergleichbare Regelung auf Bundesebene hat deshalb in der Beschlussempfehlung des Innenausschusses dahingehend eine Änderung erfahren, dass die betroffene Person in den Fällen der Bestandsdatenauskunft anhand von dynamischen IP-Adressen über die Beauskunftung zu benachrichtigen ist, vgl. § 8d Abs. 3 S. 1 BVerfSchG-E.[62] In den Sätzen 2 bis 4 des § 8d Abs. 3 BVerSchG wird die Benachrichtigungsregelung dann näher ausgestaltet.

Verfassungsrechtlich äußerst bedenklich ist, dass entgegen der Anordnung des Bundesverfassungsgerichts[63], dass die Befugnis zur Identifizierung dynamischer IP-Adressen hinreichend normenklar geregelt werden muss, dies keinen Niederschlag im Wortlaut der Norm gefunden hat. Lediglich der Klammerzusatz des § 4a Abs. 3 S. 1 LfVG-E, der auf § 113 Abs. 1 S. 3 verweist, lässt erkennen, dass auch eine Bestandsdatenabfrage anhand dynamischer IP-Adressen möglich sein soll. Ob dies dem Erfordernis des Bundesverfassungsgerichts nach einer hinreichend normenklaren Befugnis zur Identifizierung auch von dynamischen IP-Adressen entspricht, erscheint äußerst zweifelhaft.

Dringend zu empfehlen wäre also die Aufnahme einer ähnlichen Regelung wie in der Empfehlung des Innenausschusses[64] zur bundesgesetzlichen Vorschrift:

„Die Auskunft über Bestandsdaten darf auch anhand einer zu einem bestimmten Zeitpunkt zugewiesenen Internetprotokoll-Adresse verlangt werden (§ 113 Abs. 1 Satz 3 TKG)".

III. Auskunft über Zugangssicherungscodes, § 4a Abs. 3 HS. 2 LfVG-E i.V.m. § 113 Abs. 1 S. 2 TKG

1. Anforderungen des BVerfG

Zu den verfassungsrechtlichen Anforderungen an die Rechtsgrundlage der Bestandsdatenauskunft über Zugangssicherungscodes vgl. oben die Ausführungen zu B.III.1.

[62] BT-Drs. 17/12879, S. 8.
[63] BVerfG, Beschl. v. 24.01.2012 – 1 BvR 1299/05, Rn. 174.
[64] BT-Drs. 17/12879.

2. Eingriffsvoraussetzungen

§ 4a Abs. 3 S. 1 HS. 2 HSOG-E sieht für die Abfrage von Daten, mittels derer der Zugriff auf Endgeräte oder auf Speichereinrichtungen, die in diesen Endgeräten oder hiervon räumlich getrennt eingesetzt werden, geschützt wird, die gleichen Eingriffsvoraussetzungen vor wie für die „klassische" Bestandsdatenabfrage.

Wie oben bereits erläutert wird der Eingriff lediglich durch das Erforderlichkeitskriterium beschränkt. Entscheidend ist also einzig, ob diese Zugangssicherungscodes für die Erfüllung der Aufgaben des Landesamtes für Verfassungsschutz nach § 2 Abs. 2 LfVG erforderlich sind.

Verfassungsrechtlich kritisch an dieser Regelung ist zunächst – vergleichbar der Regelung im HSOG –, dass sie die Vorgaben, die das Bundesverfassungsgericht aus dem Verhältnismäßigkeitsgrundsatz herleitet, nicht umsetzt. Die Norm lässt nämlich nicht erkennen, dass die Behörden die in § 113 Abs. 1 S. 2 TKG geregelten Zugangscodes nicht unabhängig von den Anforderungen an deren Nutzung und damit gegebenenfalls unter leichteren Voraussetzungen abfragen dürfen. Auch hier ist die Aufnahme einer Passage in den Normtext, dass „die Auskunft nur verlangt werden [darf], wenn die gesetzlichen Voraussetzungen für die Nutzung der Daten vorliegen", aus Verhältnismäßigkeitsgesichtspunkten dringend angeraten.

Weiterhin ist an dieser Vorschrift problematisch, dass sie nur äußerst geringe, bis faktisch keine materiell-rechtlichen und keine verfahrensrechtlichen Eingriffsvoraussetzungen hat.

So sieht der Entwurf für die Zugangssicherungscodesabfrage auf Bundesebene in der Fassung der Empfehlung des Innenausschusses in § 8d Abs. 2 S. 2 BVerfSchG-E einen Verweis auf § 8b Abs. 1 S. 1 und 2 sowie Abs. 2 BVerfSchG vor.[65] Danach dürfen entsprechende Anordnungen nur vom Behördenleiter oder seinem Vertreter beantragt werden. Der Antrag ist zudem schriftlich zu stellen und zu begründen. Zuständig für die Anordnungen ist das Bundesministerium des Innern. In Abs. 2 ist zudem geregelt, dass das Bundesministerium des Innern monatlich die G 10-Kommission (§ 1 Abs. 2 des Artikel 10-Gesetzes) vor dem Vollzug der Anordnungen unterrichtet. Des Weiteren prüft die G 10-Kommission von Amts wegen oder aufgrund von Beschwerden die Zulässigkeit und Notwendigkeit der Einholung von Auskünften. § 15 Abs. 5 des Artikel 10-Gesetzes ist mit der Maßgabe entsprechend anzuwenden, dass die Kontrollbefugnis der Kommission sich auf die gesamte Erhebung, Verarbeitung und Nutzung der erlangten personenbezogenen Daten erstreckt. Entscheidungen über Auskünfte, welche die G 10-Kommission für unzulässig oder nicht notwendig erklärt, hat das Bundesministerium

[65] BT-Drs. 17/12879.

des Innern unverzüglich aufzuheben. Die Daten unterliegen in diesem Falle einem absoluten Verwendungsverbot und sind unverzüglich zu löschen. Ferner ist für die Verarbeitung der erhobenen Daten § 4 des Artikel 10-Gesetzes entsprechend anzuwenden.

Auch eine Benachrichtigungsregelung ist im Entwurf des § 4a LfVG-E für die Abfrage der Zugangssicherungscodes nicht vorgesehen, sodass Betroffene nicht über den heimlichen Zugriff auf Zugangssicherungscodes informiert werden müssten.

Zur Eingriffsintensität und den in der Literatur daraus gefolgerten Eingriffsvoraussetzungen des Richtervorbehalts und der nachträglichen Benachrichtigungspflicht vergleiche oben die Ausführungen zu B.III.2.

Auch die bundesrechtliche Vorschrift in der Fassung der Empfehlung des Innenausschusses sieht daher für die Fälle des Abrufs von Zugangssicherungscodes eine solche nachträgliche Benachrichtigungspflicht vor.[66] Nach § 8d Abs. 2 BVerSchG-E[67] ist die betroffene Person in diesen Fällen über die Beauskunftung zu benachrichtigen. Die Benachrichtigung erfolgt, soweit und sobald eine Gefährdung des Zwecks der Auskunft und der Eintritt übergreifender Nachteile für das Wohl des Bundes oder eines Landes ausgeschlossen werden können. Sie unterbleibt, wenn ihr überwiegende schutzwürdige Belange Dritter oder der betroffenen Person selbst entgegenstehen. Wird die Benachrichtigung zurückgestellt oder von ihr abgesehen, sind die Gründe aktenkundig zu machen.

Mit der – insbesondere für die Bestandsdatenabfrage anhand dynamischer IP-Adressen – vorgesehenen Benachrichtigungspflicht soll zur Sicherstellung hoher rechtsstaatlicher Hürden dem Grundsatz der Transparenz Rechnung getragen und damit auch die Möglichkeit für nachträglichen Rechtsschutz eröffnet werden. Diese hohen Verfahrenssicherungen sollen laut der Gesetzesbegründung – wegen des damit verbundenen mittelbaren Grundrechtseingriffs – auch für die Beauskunftung von sogenannten Zugangssicherungscodes (z. B. PIN und PUK) gelten.[68]

IV. Entschädigungsregelung, § 4a Abs. 6 LfVG-E

Die Änderung des § 4a Abs. 6 LfVG-E enthält – entsprechend der geplanten Einführung des § 8d BVerfSchG-E – eine Entschädigungsregelung für die Auskunftspflichtigen.

Begründet wird dies damit, dass sich der von den Telekommunikationsunternehmen zu erbringende Aufwand für die Erteilung von Verkehrs- und Bestandsdatenauskünften an

[66] BT-Drs. 17/12879.
[67] BT-Drs. 17/12879.
[68] BT-Drs. 17/12879, 11.

die Sicherheitsbehörden nicht von dem Aufwand unterscheidet, den diese für die Erteilung von Verkehrs- und Bestandsdatenauskünften an die Strafverfolgungsbehörden erbringen müssen.[69]

Verfassungsrechtlich erscheint diese Regelung unproblematisch.

V. Redaktionelle Fehler

Art. 2 Nr. 3 des Gesetzentwurfs enthält einen redaktionellen Fehler. Der Verweis auf „Satz 1 und 9“ müsste richtigerweise „Satz 1 und 8“ lauten.

[69] LT-Drs. 18/7137, 4.