Ausarbeitung

Die Umsetzung der Vorgaben des Bundesverfassungsgerichts zur Vorratsdatenspeicherung durch den Gesetzentwurf der Bundesregierung vom 27. Mai 2015

Die Umsetzung der Vorgaben des Bundesverfassungsgerichts zur Vorratsdatenspeicherung durch den Gesetzentwurf der Bundesregierung vom 27. Mai 2015

Aktenzeichen:	WD 3 - 3000 - 108/15
Abschluss der Arbeit:	09.06.2015
Fachbereich:	WD 3: Verfassung und Verwaltung

Inhaltsverzeichnis

1. Fragestellung und Gang der Untersuchung

Am 27. Mai 2015 hat die Bundesregierung den „Entwurf eines Gesetzes zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten“ (im Weiteren „Gesetzentwurf“ genannt) beschlossen[1], der einen Tag später beim Bundesrat eingebracht wurde.[2] In diesem Zusammenhang ist die Frage aufgeworfen worden, ob die in dem Gesetzentwurf vorgesehenen neuen Regelungen zur anlasslosen Speicherung von Telekommunikationsdaten (im Weiteren auch „Vorratsdatenspeicherung“ genannt) die Vorgaben des Bundesverfassungsgerichts in der Entscheidung vom 2. März 2010 zur Vorratsdatenspeicherung[3] richtig umsetzen.[4]

Bei dem Gesetzentwurf handelt es sich um ein so genanntes Artikelgesetz, durch das eine Reihe von Vorschriften zu unterschiedlichen Sachthemen in verschiedene Gesetze eingeführt wird. Da nach dem Gutachtenauftrag nur die Einhaltung der Vorgaben des Bundesverfassungsgerichts zur Vorratsdatenspeicherung untersucht werden soll, wird im Folgenden zunächst der Umfang der Untersuchung definiert und auch erläutert, welche Teile und Aspekte des Gesetzentwurfs nicht dazugehören (dazu unten Ziff. 2). Anschließend wird zunächst kurz die Struktur der neuen Regelungen zur Vorratsdatenspeicherung dargestellt (dazu unten Ziff. 4.). Darauf folgt die Prüfung, ob die neuen Regelungen die Vorgaben zur Vorratsdatenspeicherung richtig umsetzen (dazu unten Ziff. 4). In einem Fazit wird das Ergebnis der Untersuchung schließlich zusammengefasst (dazu unten Ziff. 5.).

2. Umfang der Untersuchung

Da der Gesetzentwurf eine Reihe von Regelungen vorsieht, die mit der anlasslosen Speicherung von Telekommunikationsdaten nicht in unmittelbarem Zusammenhang stehen, ist der Umfang der vorliegenden Untersuchung wie folgt zu begrenzen:

Entsprechend dem Gutachtenauftrag sind allein die Regelungen des Gesetzentwurfs, die sich direkt auf die Vorratsdatenspeicherung beziehen, Gegenstand der Untersuchung.[5] Zu diesen Regelungen gehören nicht nur die geplanten Vorschriften über die anlasslose Speicherung von Telekommunikationsdaten durch Telekommunikationsunternehmen (im Weiteren auch „Diensteanbieter“ genannt) sondern auch die Vorschriften über die anlassbezogene Verwendung dieser Daten durch den Staat. Daten, die die Diensteanbieter aus geschäftlichen oder vertraglichen Gründen speichern, insbesondere zur Abrechnung und zum Nachweis ihrer Leistungen gegenüber ihren Kunden,

---

1 Der Gesetzentwurf ist im Internet veröffentlicht unter: http://www.bmjv.de/SharedDocs/Downloads/DE/pdfs/Gesetze/RegE_Hoechstspeicherfrist.pdf?__blob=publicationFile.

2 BR-Drs. 249/15.

3 BVerfGE 125, 260.

4 Die Frage, ob dieser Gesetzentwurf die Vorgaben der Rechtsprechung des Europäischen Gerichtshofes richtig umsetzt, wird von dem Fachbereich Europa (PE 6) in einem gesonderten Gutachten beantwortet.

5 In der Entscheidung zur Vorratsdatenspeicherung hat das Bundesverfassungsgericht neben der Speicherung und Verwendung von Vorratsdaten auch Ausführungen zu Auskünften über Anschlussinhaber von dynamischen IP-Adressen gemacht (BVerfGE 125, 260, 340 ff.). Diese wurden jedoch bereits vom Gesetzgeber in § 100j Abs.2 StPO umgesetzt und bleiben daher an dieser Stelle unberücksichtigt (vgl. dazu auch BT-Drs. 17/12034, S. 13).

fallen nicht unter den Begriff der Vorratsdatenspeicherung. Die Regelungen des Gesetzentwurfs, die sich auf die Verwendung dieser Daten beziehen (z.B. 100g Abs. 1 StPO-E), bleiben daher in diesem Gutachten unberücksichtigt.

Auch die weiteren neuen Regelungen des Gesetzentwurfs, die sich nicht unmittelbar auf die Vorratsdatenspeicherung beziehen, wie z.B. der neue Straftatbestand der Datenhehlerei (§ 202d StGB-E), sind nicht Gegenstand des Gutachtens. Gleiches gilt für die flankierenden Regelungen in Bezug auf die Änderung des Justizvergütungs- und entschädigungsgesetzes oder die Einführungs- und Übergangsregelungen für die neuen Vorschriften in § 12 EGStPO-E.

Bei der Prüfung der neuen Regelungen zur Vorratsdatenspeicherung bleibt außerdem die Frage unberücksichtigt, ob die Verwendung dieser Daten durch den Staat die Effektivität der Gefahrenabwehr und der Strafverfolgung überhaupt fördern und sich dadurch z.B. die Aufklärungsrate von Straftaten erhöhen kann.[6] Abgesehen davon, dass dies keine rechtliche, sondern eine tatsächliche Frage ist, hat das Bundesverfassungsgericht in seiner Entscheidung vom 2. März 2010 festgestellt, dass der Gesetzgeber die Vorratsdatenspeicherung als zur Erreichung seiner Ziele geeignet ansehen darf. Es würden damit Aufklärungsmöglichkeiten geschaffen, die sonst nicht bestünden und die angesichts der zunehmenden Bedeutung der Telekommunikation für die Vorbereitung und Begehung von Straftaten in vielen Fällen erfolgsversprechend seien.[7]

In der Untersuchung werden auch solche Aspekte und Wirkungen der neuen Regelungen nicht berücksichtigt, die sich nicht vordringlich aufgrund der normativen Ausgestaltung, sondern eher aufgrund der technischen Strukturen der Telekommunikationseinrichtungen und der technischen Definition von Telekommunikationsbegriffen ergeben.[8]

Die verfassungsrechtliche Prüfung beschränkt sich schließlich – dem Gutachtenauftrag entsprechend – auf die Frage, ob die Anforderungen, die das Bundesverfassungsgericht in der Entscheidung vom 2. März 2010 zur alten Regelung der Vorratsdatenspeicherung aufgestellt hat, in den vorgeschlagenen Regelungen zur Vorratsdatenspeicherung richtig umgesetzt werden. Daher wird in diesem Gutachten auch nicht weiter untersucht, ob die neuen Regelungen zur Vorratsdatenspeicherung im Gesetzentwurf gegen sonstige verfassungsrechtliche Vorgaben verstoßen könnten, die nicht Gegenstand der Entscheidung des Bundesverfassungsgerichts zur Vorratsdatenspeicherung vom 2. März 2010 waren.

---

6 Vgl. dazu sehr kritisch die Stellungnahme des Deutschen Anwaltsvereins vom 20.05.2015, S. 5 ff., im Internet aufrufbar unter: http://anwaltverein.de/de/newsroom/sn-25-15-referentenentwurf-des-bundesministeriums-der-justiz-und-fuer-verbraucherschutz-fuer-ein-gesetz-zur-einfuehrung-einer-sp sowie die Stellungnahme des Bundesverbands Informationswirtschaft, Telekommunikation und neue Medien e.V. (BITKOM) vom 22.05.2015, im Internet aufrufbar unter: http://www.bitkom.org/files/documents/20150522_Stellungnahme_VDS.pdf.

7 Zu dieser Argumentation des Bundesverfassungsgerichts ausführlich: BVerfGE 125, 260, 317 f.

8 Zu diesem Aspekt gehört beispielsweise die Frage, wie das Tatbestandsmerkmal „Beginn der Internetverbindung“, bei der die Funkzelle (Standortdaten) gespeichert werden muss (§ 113b Abs. 4 Satz 2 TKG-E), technisch zu verstehen ist. Vgl. zu dieser Diskussion z.B. Volker Tripp, Referentenentwurf zur VDS: Der rechtsstaatliche Lack ist ab, Beitrag vom 18.05.2015 im Blog des Digitale Gesellschaft e. V., im Internet aufrufbar unter: https://digitale-gesellschaft.de/2015/05/vds-lack-ist-ab/.

3. Struktur des neuen Regelungen zur Vorratsdatenspeicherung

Die Struktur der neuen Regelungen zur Vorratsdatenspeicherung ist dadurch gekennzeichnet, dass die Vorschriften über die anlasslose Speicherung der Telekommunikationsdaten einerseits und die Vorschriften über ihren anlassbezogenen Abruf andererseits getrennt geregelt werden. In das Telekommunikationsgesetz (TKG[9]) sollen die Vorschriften über die Speicherung der anlasslos gespeicherten Daten (im Weiteren auch „Vorratsdaten“ genannt) durch die Diensteanbieter eingefügt werden. Der Gesetzentwurf sieht in seinem Art. 2 daher die Aufnahme der §§ 113a bis 113g in das TKG vor. Die Vorschriften zur Verwendung der Vorratsdaten durch die Strafverfolgungsbehörden sollen sich zukünftig in der Strafprozessordnung (StPO[10]) in den neuen §§ 100g, 101a und 101b StPO-E finden (Art. 1 des Gesetzentwurfs). Diese gesetzliche Struktur, d.h. die gesetzgeberische Trennung von Speicherung und Verwendung der Vorratsdaten in den bereichsspezifischen Gesetzen, folgt im Übrigen auch den Vorgaben des Bundesverfassungsgerichts.[11]

Darüber hinaus greift der Gesetzentwurf auch das in der Rechtsprechung des Bundesverfassungsgerichts geforderte so genannte Doppeltürprinzip auf. Danach bedarf es sowohl für die Datenübermittlung aus Sicht des Datenabsenders als auch für die Abfrage aus Sicht des Datenempfängers einer gesonderten, bereichsspezifischen Befugnisnorm.[12] Dementsprechend sieht § 113c Abs. 1 Nr. 1 TKG-E die Befugnis der Diensteanbieter vor, die Vorratsdaten unter den dort genannten Voraussetzungen an die Strafverfolgungsbehörden weiterzuleiten. Eine dieser Voraussetzungen ist, dass für die Strafverfolgungsbehörden eine gesetzliche Erlaubnis besteht, diese Daten entsprechend erheben zu dürfen. Diese Erlaubnis für die Strafverfolgungsbehörden ist im Gesetzentwurf in § 100g StPO-E vorgesehen. Der Gesetzentwurf sieht aus Sicht der Diensteanbieter darüber hinaus die Befugnis vor, die Vorratsdaten den Gefahrenabwehrbehörden der Länder unter den ebenfalls dort genannten Voraussetzungen zu übermitteln (§ 113c Abs. 1 Nr. 2 TKG-E). Da hier ausdrücklich nur die Behörden der Länder genannt sind und die Gesetzgebungskompetenz über die Gefahrenabwehr in den Ländern insoweit den Ländern zusteht, findet sich in dem Gesetzentwurf des Bundes keine dem Doppeltürprinzip entsprechende Befugnisnorm für diese Landesbehörden. Nur wenn die Länder entsprechende Erhebungsvorschriften für die nach dem TKG gespeicherten Vorratsdaten vorsehen und diese den verfassungsrechtlichen sowie den Vorgaben des § 113c Abs. 1 Nr. 2 TKG-E entsprechen, dürfen die Diensteanbieter diese Daten an die Gefahrenabwehrbehörden der Länder zukünftig übersenden.

4. Prüfung der neuen Regelungen zur Vorratsdatenspeicherung anhand der Entscheidung des Bundesverfassungsgerichts vom 2. März 2010

In dem Gesetzentwurf fällt zunächst auf, dass die Vorgaben des Bundesverfassungsgerichts zur Vorratsdatenspeicherung teilweise nahezu wörtlich übernommen wurden. Insbesondere bei der

---

9 Telekommunikationsgesetz vom 22. Juni 2004 (BGBl. I S. 1190), das zuletzt durch Artikel 22 des Gesetzes vom 25. Juli 2014 (BGBl. I S. 1266) geändert worden ist.

10 Strafprozessordnung in der Fassung der Bekanntmachung vom 7. April 1987 (BGBl. I S. 1074, 1319), die zuletzt durch Artikel 2 Absatz 3 des Gesetzes vom 21. Januar 2015 (BGBl. I S. 10) geändert worden ist.

11 BVerfGE 125, 260, 345 f.

12 BVerfGE 130, 151, 184 – Bestandsdatenabfrage: *„Der Gesetzgeber muss, bildlich gesprochen, nicht nur die Tür zur Übermittlung von Daten öffnen, sondern auch die Tür zu deren Abfrage.“*

Grundstruktur, d.h. bei den Merkmalen der Vorratsdatenspeicherung (dazu unten Ziff. 4.1.), bei den Regelungen zur Speicherung der Daten (dazu unten Ziff. 4.2.) und der Verwendung der Daten (dazu unten Ziff. 4.3.) und schließlich bei den Regelungen zum Richtervorbehalt, zur Transparenz und zum Rechtsschutz (dazu unten Ziff. 4.4.), greift der Gesetzentwurf diese Rechtsprechung auf. In Einzelheiten, die nachfolgend im Zusammenhang mit den jeweiligen verfassungsgerichtlichen Vorgaben erläutert werden, bleibt der Gesetzentwurf jedoch unklar, sodass die Forderung des Bundesverfassungsgerichts nach normenklaren Regelungen nicht durchgängig eingehalten wird.

4.1. Merkmale der Vorratsdatenspeicherung

Neben der anlasslosen Speicherung von Telekommunikationsdaten[13] charakterisiert das Bundesverfassungsgericht die Vorratsdatenspeicherung durch zwei weitere Merkmale: Zum einen sei die Vorratsdatenspeicherung dadurch gekennzeichnet, dass nur die Verbindungsdaten und nicht auch der Inhalt der Telekommunikation, d.h. beispielsweise der Inhalt von Telefongesprächen, Telefaxen und E-Mails, gespeichert werde.[14] Zum anderen erfolge die Speicherung nicht durch den Staat selbst, sondern durch die Telekommunikationsunternehmen.[15] Das letztere Merkmal nennt das Bundesverfassungsgericht als Voraussetzung dafür, dass die Vorratsdatenspeicherung überhaupt verfassungsrechtlich zulässig sein kann. Die Speicherung durch die Diensteanbieter stelle sicher, dass die Daten der Bürger auf verschiedene Stellen verteilt seien. Der Staat dürfe keinen direkten Zugriff auf die Gesamtheit aller Daten haben. Der Zugriff des Staates müsse daher erst in einem zweiten Schritt anlassbezogen erfolgen.[16]

Diese beiden Merkmale wurden schon durch die Regelungen zur Vorratsdatenspeicherung in der Fassung vom 21. Dezember 2010 (§§ 113a und 113b TKG a.F.), die das Bundesverfassungsgericht im Übrigen als verfassungswidrig verwarf, erfüllt. Auch die im aktuellen Gesetzentwurf vorgeschlagenen Regelungen zum TKG[17] und zur StPO berücksichtigen diese Merkmale und entsprechen daher diesen Vorgaben des Bundesverfassungsgerichts.

4.2. Regelung zur Speicherung der Daten

Die Regelungen zur Speicherung der Daten sollen durch die neuen §§ 113a bis 113g TKG-E eingeführt werden. Zu dieser Speicherung hat das Bundesverfassungsgericht eine Reihe von Anforderungen aufgestellt. Diese werden im Folgenden erläutert und es wird geprüft, ob die neuen Regelungen diese Anforderungen erfüllen.

---

13 Siehe dazu oben Ziff. 2, S. 5.

14 BVerfGE 125, 260, 347.

15 BVerfGE 125, 260, 321.

16 Ebenda.

17 Siehe zum Verbot der Speicherung der Kommunikationsinhalte: § 113b Abs. 5 TKG-E.

4.2.1. Dauer der Speicherung

In der Entscheidung zur Vorratsdatenspeicherung hat das Bundesverfassungsgericht die damals vorgesehene Speicherdauer von sechs Monaten als absolute Obergrenze einer verfassungsrechtlich zulässigen Vorratsdatenspeicherung angesehen.[18] § 113b Abs. 1 TKG-E sieht eine Speicherdauer von zehn Wochen für die Telekommunikationsdaten (§ 113b Abs. 2 und 3 TKG-E) und von vier Wochen für Standortdaten (bei Kommunikation über Mobiltelefone, § 113b Abs. 4 TKG-E) vor. Damit bleibt der Gesetzentwurf hinter der alten Regelung deutlich zurück und hält sich in dem Rahmen, den das Bundesverfassungsgericht als zulässige Speicherdauer angesehen hat.

4.2.2. Sicherheit der gespeicherten Daten

In seiner Entscheidung zur Vorratsdatenspeicherung hat das Bundesverfassungsgericht hingegen die damalige Regelungen zur Sicherheit der gespeicherten Daten (§ 113a Abs. 10 TKG a.F.) als unzureichend angesehen.[19] Es fordert einen besonders hohen Sicherheitsstandard und führt im Einzelnen aus, wie die Regelungen zur Datensicherheit ausgestaltet sein müssen, um den verfassungsrechtlichen Anforderungen zu genügen. Zunächst sei sicherzustellen, dass sich der Sicherheitsstandard dynamisch an dem Entwicklungsstand neuer Facherkenntnisse anpasse. Normtechnisch könnte dies durch einen Verweis auf den „Stand der Technik“ aufgenommen werden. Weiter solle grundsätzlich eine getrennte Speicherung der Daten, eine anspruchsvolle Verschlüsselung, ein gesichertes Zugriffsregime unter Nutzung etwa des Vier-Augen-Prinzips sowie eine revisionssichere Protokollierung sichergestellt werden. Der Gesetzgeber müsse entsprechende Regelungen normenklar und verbindlich vorgeben.[20]

In § 113d TKG-E sind diese Ausführungen des Bundesverfassungsgerichts teilweise wörtlich übernommen worden.[21] Es fehlt weder der Verweis auf den „Stand der Technik“ (§ 113d Satz 1 TKG-E) noch bleiben die einzelnen Sicherheitsvorgaben in den Nrn. 1 bis 5 des § 113d Satz 2 TKG-E hinter den Anforderungen des Bundesverfassungsgerichts zurück. Es wird ein besonders sicheres Verschlüsselungsverfahren (Nr. 1), die getrennte Speicherung der Daten mit Schutz vor Zugriff aus dem Internet (Nr. 2 und Nr. 3) sowie eine Beschränkung auf besonders ermächtigte Personen im Hinblick auf den Zutritt zu den entsprechenden Datenverarbeitungsanlagen (Nr. 4) und auf den Zugriff auf die Daten (Nr. 5: Vier-Augen-Prinzip) vorgegeben. Damit dürfte die Regelung zur Gewährleistung der Sicherheit der Daten in § 113d TKG-E den Anforderungen des Bundesverfassungsgerichts entsprechen.

---

18 BVerfGE 125, 260, 322.

19 BVerfGE 125, 260, 348.

20 Zum Ganzen: BVerfGE 125, 260, 326 f.

21 Siehe auch Referentenentwurf vom 15.05.2015, S. 46.

4.2.3. Art und Maß der technischen Datensicherung

Das Bundesverfassungsgericht fordert weiter, dass der Staat die genaue Art und das Maß der Datensicherung den Diensteanbietern vorgibt.[22] Dies könne dadurch geschehen, dass einer Aufsichtsbehörde die Konkretisierung der technischen Vorgaben anvertraut wird. Möglich sei auch eine Konkretisierung durch technische Vorschriften auf verschiedenen Normebenen oder durch eine allgemein-generelle Regelung mit verbindlichen Einzelvorgaben der Behörde gegenüber den Diensteanbietern. In jedem Falle müsse die Kontrolle für die Öffentlichkeit transparent durchgeführt werden, in die auch der unabhängige Datenschutzbeauftragte einbezogen werden müsse.[23]

Der Gesetzentwurf hat sich für die Konkretisierung der technischen Vorgaben auf verschiedenen Normebenen entschieden. In § 113f Abs. 1 Satz 1 TKG-E werden die Diensteanbieter allgemein-generell verpflichtet, bei der Speicherung, Verwendung und Sicherung der Vorratsdaten (§§ 113b bis 113e TKG-E) einen besonders hohen Standard bei der Datensicherheit und Datenqualität zu gewährleisten. Die Konkretisierung der technischen Anforderungen wird in einem Katalog[24] festgelegt, den die Bundesnetzagentur (als Aufsichtsbehörde[25]) im Benehmen mit[26] dem Bundesamt für Sicherheit in der Informationstechnik und der oder dem Bundesbeauftragten für den Datenschutz und die Informationstechnik (unabhängiger Datenschutzbeauftragter) erstellt (§ 113f Abs. 1 Satz 2 TKG-E). Dieser Katalog ist fortlaufend darauf zu prüfen, ob er noch dem Entwicklungsstand der Technik entspricht und bei Änderungsbedarf im Benehmen mit den genannten Stellen unverzüglich anzupassen (§ 113f Abs. 2 TKG-E).

Damit dürften die Vorgaben des Bundesverfassungsgerichts zur Konkretisierung der technischen Anforderungen an die Datensicherung im Gesetzentwurf erfüllt sein.

4.2.4. Ausgeglichenes Sanktionensystem

Das Bundesverfassungsgericht hielt außerdem das in den alten Regelungen zur Vorratsdatenspeicherung vorgesehene Sanktionensystem für verfassungswidrig. Nach den damaligen Vorschriften

---

22 In der Entscheidung zur Vorratsdatenspeicherung bemängelte das Bundesverfassungsgericht, dass durch die alten Regelungen (§ 113a TKG a.F.) die genaue technische Ausgestaltung der Sicherungsmaßnahmen den Diensteerbringern allein überlassen bleibe (BVerfGE 125, 260, 349).

23 Zum Ganzen: BVerfGE 125, 260, 327.

24 Der Inhalt dieses Katalogs ist genauer in der Begründung des Gesetzentwurfs, BR-Drs. 249/15, S. 46, beschrieben.

25 Siehe die Begründung des Gesetzentwurfs, BR-Drs. 249/15, S. 45.

26 Die Gesetzesbegründung spricht an dieser Stelle noch von der „Beteiligung“ der genannten Stellen (BR-Drs. 249/15, S. 46), wie es noch in dem Referentenentwurf vorgesehen war. Die Formulierung „im Benehmen mit“ ist eine im öffentlichen Recht bekannte Beteiligungsform (vgl. etwa § 6 Abs. 3 Satz 3 GOBT; § 42 Abs. 1 Arbeitsgerichtsgesetz). Aus dem Begriff „Benehmen“ dürfte in diesem Zusammenhang (§ 113f Abs. 1 Satz 2, Abs. 2 TKG-E) folgen, dass die Bundesnetzagentur die genannten Stellen im Zuge der Erstellung des Katalogs konsultieren muss und sich über ihre Meinungen und Forderungen nur aus gewichtigen Gründen hinwegsetzen darf (vgl. dazu die entsprechenden Kommentierungen bei Ritzel/Bücker/Schreiner, Handbuch für die Parlamentarische Praxis, Kommentierung zu § 6 GOBT, Ziff. III 3. a) sowie bei Prütting, in: Germelmann/Matthes/Prütting, Arbeitsgerichtsgesetz, § 117 ArbGG Rdnr. 4 - zu § 42 Abs. 1 ArbGG). Da das Bundesverfassungsgericht insoweit nur die „Einbeziehung“ und nicht auch eine Mitbestimmung des behördlichen Datenschutzbeauftragten fordert, dürfte diese Beteiligungsform den Vorgaben des Bundesverfassungsgerichts entsprechen.

sei der Bußgeldrahmen für eine Verletzung der Speicherpflichten deutlich weiter als derjenige für die Verletzung der Datensicherheit.[27] Dies sei aufgrund des notwendigen hohen Schutzes der Vorratsdaten mit den Grundrechten der betroffenen Bürger nicht zu vereinbaren. Daher fordert das Gericht ein ausgeglichenes Sanktionensystem, das Verstößen gegen die Vorschriften zur Gewährleistung der Datensicherheit ein angemessenes Gewicht beimisst.[28] Der aktuelle Gesetzentwurf soll ein solches Sanktionensystem durch eine entsprechende Ergänzung der Bußgeldvorschriften in § 149 Abs. 1 Nr. 36 bis 44 TKG-E einführen. In diesen neuen Vorschriften sollen unter anderem Verstöße gegen die Datensicherheit mit demselben Bußgeldrahmen (bis zu 500.000 Euro) bedroht werden, der auch für die Verletzung der Speicherpflichten gilt (§ 149 Abs. 1 Ziff. 40 i.V.m. Abs. 2 Satz 1 Nr. 1 TKG-E). Damit bleiben die möglichen Sanktionen für Verstöße gegen die Datensicherheitsvorschriften nicht mehr hinter den Sanktionen für Verstöße gegen die Speicherpflichten zurück. Folglich dürften die verfassungsgerichtlichen Vorgaben für ein ausgeglichenes Sanktionensystem durch den Gesetzentwurf richtig umgesetzt werden.

4.3. Regelungen zur Verwendung der Daten

Nach der Entscheidung zur Vorratsdatenspeicherung unterliegt auch die Verwendung von anlasslos gespeicherten Daten durch den Staat besonders hohen Anforderungen. Diese Verwendung könne nur dann als verhältnismäßig angesehen werden, wenn sie besonders hochrangigen Gemeinwohlbelangen diene.[29] Dafür stellt das Gericht die nachfolgend genannten Voraussetzungen auf.

4.3.1. Qualität der zu schützenden Rechtsgüter

Bei der Ausgestaltung der Regelungen zur Datenverwendung zum Schutz besonders hochrangiger Gemeinwohlbelange unterscheidet das Bundesverfassungsgericht zwischen der Strafverfolgung einerseits und der Gefahrenabwehr andererseits.

4.3.1.1. Datenverwendung zur Strafverfolgung

Zum Zwecke der Strafverfolgung sei die Datenverwendung zulässig, wenn bestimmte Tatsachen den begründeten Verdacht einer schweren Straftat entstehen lassen. Der Gesetzgeber habe diesbezüglich in einem Katalog abschließend festzulegen, welche Straftatbestände als schwere Straftaten gelten. Die Qualifizierung der Straftat als „schwer“ müsse in der Strafnorm selbst, insbesondere etwa durch den Strafrahmen, ihren objektiven Ausdruck finden.[30] Die alte Regelung des § 100g StPO a.F. sah einen solchen abschließenden Katalog nicht vor und wurde daher vom Bundesverfassungsgericht als verfassungswidrig verworfen.[31]

Der neue § 100g Abs. 2 StPO-E des Gesetzentwurfs soll nun diese Anforderungen erfüllen. In Satz 1 dieser Vorschrift ist vorgesehen, die Formulierung des Bundesverfassungsgerichts zum Tatverdacht

---

27 BVerfGE 125, 260, 351.

28 BVerfGE 125, 260, 327.

29 BVerfGE 125, 260, 328.

30 Zum Ganzen: BVerfGE 125, 260, 329.

31 BVerfGE 125, 260, 352 f.

zu übernehmen. Daher ist der Datenzugriff nur erlaubt, wenn „bestimmte Tatsachen den Verdacht“ begründen, dass jemand eine besonders schwere Straftat begangen hat. Um sicherzustellen, dass auch die Verhältnismäßigkeit im Einzelfall gewahrt ist, ist weitere Voraussetzung (Satz 1 2. Halbsatz), dass die Tat auch im Einzelfall schwer wiegt, die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes des Beschuldigten auf andere Weise wesentlich erschwert oder aussichtlos wäre und die Erhebung der Daten in einem angemessenen Verhältnis zur Bedeutung der Sache steht. Mit diesen Regelungen nimmt der Gesetzentwurf die Rechtsprechung des Bundesverfassungsgerichts auf und verpflichtet zunächst die Strafverfolgungsbehörden und später vor allem den über die Datenverwendung entscheidenden Richter (§ 101a Abs. 1 StPO-E i.V.m. § 100b Abs. 1 Satz 1 StPO) abzuwägen, ob auch im Einzelfall die Verhältnismäßigkeit des Eingriffs in die Grundrechte der Betroffenen gewahrt ist. Diese spezifische Entscheidung im Einzelfall, insbesondere durch den entscheidenden Richter, hatte das Bundesverfassungsgericht ausdrücklich gefordert.[32]

Satz 2 des § 100g Abs. 2 StPO-E sieht darüber hinaus nun einen abschließenden Katalog vor, in dem die verschiedenen „besonders schweren Straftaten“ aufgelistet sind, deren Verfolgung den Datenabruf – bei Vorliegen der sonstigen Voraussetzungen – erlaubt. Demgegenüber hatte das Bundesverfassungsgericht in seiner Entscheidung zur Vorratsdatenspeicherung „nur“ einen Katalog von „schweren Straftaten“ gefordert. Hier geht der Gesetzentwurf über diese Entscheidung hinaus und nimmt die Formulierung in Art. 13 Abs. 3 Satz 1 GG auf, nach der eine akustische Wohnraumüberwachung nur zulässig ist, wenn der Verdacht besteht, dass eine „besonders schwere Straftat“ begangen wurde. Auch inhaltlich orientiert sich der Katalog an der Entscheidung des Bundesverfassungsgerichts zur akustischen Wohnraumüberwachung („großer Lauschangriff“).[33] Nach dieser Entscheidung gibt der Strafrahmen einen maßgeblichen Hinweis auf die Schwere der Straftat.[34] Insoweit sei von der besonderen Schwere einer Straftat im Sinne des Art. 13 Abs. 3 GG nur auszugehen, wenn sie mit einer höheren Höchststrafe als fünf Jahre Freiheitsstrafe bewehrt sei.[35] Soweit der Grundtatbestand eine solche Höchststrafe vorsehe, müsse auch die entsprechende Regelung eines minder schweren Falles, für den eine niedrigere Höchststrafe als fünf Jahre Freiheitsentzug vorgesehen sei, nicht aus dem Katalog herausfallen.[36]

Bis auf eine Ausnahme sehen alle in den neuen Katalog des § 100g Abs. 2 Satz 2 StPO-E aufgenommenen Straftaten in ihrem Grundtatbestand eine Höchstfreiheitsstrafe von über fünf Jahren vor und sind damit schon nach der Rechtsprechung des Bundesverfassungsgerichts zum großen Lauschangriff als besonders schwere Straftaten zu qualifizieren. Die Ausnahme bildet die in § 100g Abs. 2 Satz 2 Nr. 1 Buchstabe b) StPO-E aufgenommene Straftat nach § 184c Abs. 2 StGB (gewerbs- oder bandenmäßige Verbreitung, Erwerb und Besitz jugendpornographischer Schriften), für die ein Strafrahmen von 3 Monaten bis 5 Jahren Freiheitsstrafe vorgesehen ist. Insgesamt erscheint die Aufnahme dieser Straftat jedoch noch von der verfassungsgerichtlichen Entscheidung zur Vorratsdatenspeicherung gedeckt. Wie dargestellt, verlangt das Gericht in dieser Entscheidung

32 BVerfGE 125, 260, 329, 334.

33 BVerfGE 109, 279 – Großer Lauschangriff.

34 BVerfGE 109, 279, 347 – Großer Lauschangriff; ebenso: BVerfGE 125, 260, 329 – Vorratsdatenspeicherung.

35 BVerfGE 109, 279, 347 f. – Großer Lauschangriff.

36 BVerfGE 109, 279, 349 – Großer Lauschangriff.

„nur“ eine schwere Straftat und – im Unterschied zur Entscheidung zum großen Lauschangriff – keine besonders schwere Straftat. Der Strafrahmen von bis zu 5 Jahren unter Ausschluss einer Geldstrafe qualifiziert § 184c Abs. 2 StGB nach hiesiger Ansicht als „schwere Straftat“ im Sinne der Entscheidung zur Vorratsdatenspeicherung.

Folglich setzt die Vorschrift zur Verwendung der Vorratsdaten in § 100g Abs. 2 StPO-E die Vorgaben des Bundesverfassungsgerichts wohl richtig um.

4.3.1.2. Datenverwendung zur Gefahrenabwehr

Im Unterschied zu der Datenverwendung zur Strafverfolgung ist nach der Entscheidung des Bundesverfassungsgerichts zur Vorratsdatenspeicherung im Bereich der Gefahrenabwehr kein abschließender Katalog der möglicherweise geplanten Straftaten erforderlich. Ein solcher Katalog würde in diesem Bereich zu Unklarheiten und Unsicherheiten führen. Stattdessen biete sich an, gesetzlich zum einen unmittelbar die Rechtsgüter zu nennen, deren Schutz eine Verwendung der Vorratsdaten rechtfertigen soll, und zum anderen die Intensität der Gefährdung dieser Rechtsgüter zu definieren, die als Eingriffsschwelle erreicht sein muss. Der Datenabruf sei in diesem Bereich daher nur zur Abwehr von Gefahren für Leib, Leben oder Freiheit einer Person, für den Bestand oder die Sicherheit des Bundes oder eines Landes oder zur Abwehr einer gemeinen Gefahr zulässig. Zudem müssten tatsächliche Anhaltspunkte für eine konkrete Gefahr für diese Rechtsgüter bestehen; Vermutungen und allgemeine Erfahrungssätze würden für den Datenabruf daher nicht ausreichen.[37]

Der Gesetzentwurf nimmt diese Rechtsprechung auf. Er sieht allerdings nur eine Datenverwendung für Gefahrenabwehrbehörden der Länder und nicht auch der entsprechenden Bundesbehörden vor. Letztere dürfen daher nach hiesigem Verständnis auf die Vorratsdaten nicht zugreifen.[38] Da in einem Bundesgesetz aufgrund der fehlenden Gesetzeskompetenz des Bundes der Datenabruf für die Landesbehörden nicht geregelt werden darf, sieht der Gesetzentwurf in § 113 c Abs. 1 Nr. 2 TKG-E nur die Datenweitergabe aus Sicht der Diensteanbieter vor (erster Teil des Doppeltürprinzips[39]). Danach dürfen die Diensteanbieter die Vorratsdaten nur an eine Gefahrenabwehrbehörde eines Landes übermitteln, wenn für diese eine landesgesetzliche Bestimmung vorliegt, die ihr die Datenverwendung zur Abwehr einer konkreten Gefahr für Leib, Leben oder Freiheit einer Person oder für den Bestand des Bundes oder eines Landes erlaubt. Damit übernimmt der Gesetzentwurf nahezu

37 Zum Ganzen: BVerfGE 125, 260, 329 f.

38 So sind im Ergebnis wohl auch die Ausführungen in der Begründung des Gesetzentwurfs, BR-Drs. 249/15, S. 43, zu verstehen. Die Begründung dafür, dass die Übermittlung der Daten an die Nachrichtendienste im Unterschied zur Vorgängerregelung in § 113b Satz 1 Nr. 3 TKG a.F. nicht vorgesehen ist, liegt wohl in den Ausführungen des Bundesverfassungsgerichts zur Datenverwendung durch die Nachrichtendienste. Das Gericht führt aus, dass die Datenverwendung durch Nachrichtendienste ein besonders schwerer Eingriff in die Grundrechte der Betroffenen sei, da die Nachrichtendienste nur Informationen sammeln würden und nicht auch zur Gefahrenabwehr berufen seien. Daher könnte die Datenerhebung in der Regel nicht durch den Schutz hochrangiger Rechtsgüter gerechtfertigt werden, so dass damit die Verwendung der anlasslos gespeicherten Daten durch die Nachrichtendienste in vielen Fällen ausscheiden dürfte (vgl. BVerfGE 125, 260, 329, 331 f.). Vor diesem Hintergrund wurde vermutlich von der Aufnahme der Nachrichtendienste an dieser Stelle abgesehen.

39 Siehe dazu oben S. 6.

wörtlich[40] die Ausführungen des Bundesverfassungsgerichts und setzt damit die entsprechenden Anforderungen wohl richtig um.

4.3.2. Begrenzung der Datenverwendung durch besondere Verfahrensvorschriften

Das Bundesverfassungsgericht fordert außerdem, dass zur Begrenzung der Datenverwendung flankierende Verfahrensvorschriften geschaffen werden. Dazu gehöre, dass die Daten von den Behörden unverzüglich ausgewertet und, sofern sie für Erhebungszwecke unerheblich sind, sofort gelöscht werden. Im Übrigen sei vorzusehen, dass Daten vernichtet werden, sobald sie für die festgelegten Zwecke nicht mehr erforderlich sind.[41]

Der Gesetzentwurf sieht für den Bereich der Strafverfolgung in § 101a Abs. 3 S. 1 StPO-E die unverzügliche Auswertung von „personenbezogenen Daten, die durch Maßnahmen nach § 100g [StPO-E] erhoben wurden“ vor. Nach § 101a Abs. 3 S. 1 StPO-E soll für die Löschung der „personenbezogenen Daten“ § 101 Abs. 8 StPO gelten. Damit beziehen sich diese beiden Pflichten nach ihrem Wortlaut auf „personenbezogene Daten“. In der Ermächtigung der Strafverfolgungsbehörden zur Verwendung der Vorratsdaten werden diese jedoch als „Verkehrsdaten“ bezeichnet (§ 100g Abs. 2 StPO-E). Auch die Absätze 1 und 6 des § 101a StPO-E und die meisten anderen neuen Vorschriften der StPO-E beziehen sich auf „Verkehrsdaten“. Es bleibt unklar, ob diese beiden Begriffe („personenbezogene Daten“ und „Verkehrsdaten“) deckungsgleich sind oder ob gerade die Verkehrsdaten, d.h. insbesondere anlasslos gespeicherten und später erhobenen Vorratsdaten, mehr Daten umfassen. Wäre letzteres der Fall, würde der Gesetzentwurf die Vorgaben des Bundesverfassungsgerichts nicht richtig umsetzen, da das Gericht die unverzügliche Auswertung und spätere Löschung aller anlasslos gespeicherten Daten verlangt. Im Ergebnis scheint es sich hier jedoch eher um einen redaktionellen Fehler zu handeln. Denn auch in der Begründung zu § 101a Abs. 3 S. 1 StPO-E gehen die Begriffe durcheinander. Obwohl die Löschpflicht nach dem Wortlaut der Vorschrift nur für „personenbezogene Daten“ gilt, erläutert die Begründung des Gesetzentwurfs diese Löschung der „Verkehrsdaten“.[42] Da das Bundesverfassungsgericht für die Vorratsdatenspeicherung aber normenklare Regelungen fordert,[43] wird dem nur Rechnung getragen, wenn der Begriff „personenbezogene Daten“ in § 101a Abs. 3 StPO-E durch „Verkehrsdaten“ ersetzt wird. In Bezug auf die unverzügliche Auswertung dieser Daten würden damit die Vorgaben des Bundesverfassungsgerichts richtig umgesetzt.

Die Löschung bzw. Vernichtung der Daten verlangt das Bundesverfassungsgericht für zwei verschiedene Fälle, die es semantisch durch die Worte „unerhebliche“ und „nicht mehr erforderliche“ Daten unterscheidet:[44] Der erste Fall bezieht sich auf Daten, die die Strafverfolgungsbehörden mit der Datenerhebung erhalten, die aber mit der verfolgten Tat nicht in Verbindung stehen und daher

---

40 Das Bundesverfassungsgericht hatte in die entsprechende Aufzählung der Schutzgüter allerdings auch noch die „Sicherheit des Bundes oder eines Landes“ aufgenommen. Es ist nicht ersichtlich und wird auch in der Begründung des Gesetzentwurfs nicht dargelegt, warum dieses Rechtsgut nicht in § 113c Abs. 1 Nr. 2 TKG-E aufgenommen wurde und daher zur Datenerhebung nicht berechtigen soll.

41 Zum Ganzen: BVerfGE 125, 260, 329, 332 f.

42 Begründung des Gesetzentwurfs, BR-Drs. 249/15, S. 36.

43 BVerfGE 125, 260, 329, 325 ff.

44 Zum Ganzen: BVerfGE 125, 260, 329, 332 f.

für die konkrete Strafverfolgung von vornherein „unerheblich“ sind. Diese Daten seien sofort, gewissermaßen vor Beginn der weiteren Ermittlungen, zu löschen. Im zweiten Fall geht es darum, dass eine Strafverfolgung insgesamt, d.h. gegebenenfalls auch der Strafprozess, abgeschlossen ist. Dann müssten auch die zunächst erheblichen, nun aber „nicht mehr erforderlichen“ Daten vernichtet werden. Der Gesetzentwurf verweist in § 101a Abs. 3 Satz 4 StPO-E für die Löschung der Daten auf § 101 Abs. 8 StPO. Nach Satz 1 dieser Vorschrift müssen personenbezogene Daten, die zur Strafverfolgung und für eine etwaige gerichtliche Überprüfung der Maßnahme nicht mehr erforderlich sind, unverzüglich gelöscht werden. Damit formuliert diese Vorschrift die Löschung der Daten im zweiten Fall, in dem diese „nicht mehr erforderlich“ sind. Eine ausdrückliche Regelung über die sofortige Löschung von vornherein „unerheblicher“ Daten fehlt daher. Zwar könnte argumentiert werden, dass es sich hier lediglich um ein Wortspiel handele, da der Begriff „nicht mehr erforderliche Daten“ immer auch „unerhebliche“ Daten umfasse und sich die Löschpflicht des § 101 Abs. 8 StPO daher auch auf diese Daten beziehe. Dem wäre jedoch entgegenzuhalten, dass das Bundesverfassungsgericht normenklare Regelungen verlangt, die Löschung der Daten als besonders bedeutsam bewertet und folglich eine vielleicht durch Verweise mögliche, aber nicht eindeutig verfassungskonforme Auslegung der Vorschriften diesen Anforderungen nicht genügt. Daher werden an dieser Stelle nach Meinung der Verfasserin die entsprechenden Vorgaben des Bundesverfassungsgerichts nicht richtig, insbesondere nicht normenklar umgesetzt.

4.3.3. Weitergabe und Weiterverwendung der Daten für andere Zwecke

Die Vorratsdaten verlieren ihren grundrechtlichen Schutz nach den Vorgaben des Bundesverfassungsgerichts nicht dadurch, dass bereits eine staatliche Stelle von ihnen Kenntnis erlangt hat. Daher sei die Weitergabe der Daten an andere Stellen, die diese zur Verfolgung anderer Zwecke benötigen, nur zulässig, wenn dafür eine gesetzliche Grundlage geschaffen werde. Diese müsse vorsehen, dass die Daten nur dann an eine andere Stelle weitergegeben werden dürfen, wenn diese ihrerseits befugt wäre, diese Daten zu verwenden. Im Übrigen sei die Weitergabe von der weiterleitenden Stelle zu protokollieren.[45] Einen erneuten Richtervorbehalt verlangt das Gericht an dieser Stelle allerdings nicht, so dass allein die Behörden prüfen müssen, ob die Voraussetzungen für die Datenweitergabe vorliegen.

Diese Protokollierung der Datenweitergabe sieht der Gesetzentwurf zwar in § 101a Abs. 4 Satz 2 StPO-E vor und setzt damit diese Vorgabe insoweit richtig um. Im Übrigen ergibt sich in diesem Bereich jedoch eine Reihe von Unklarheiten:

Diese Regelungen zur Datenweitergabe in § 101a Abs. 4 und Abs. 5 StPO-E beziehen sich in ihrem Wortlaut auf „verwertbare personenbezogene Daten“. Damit weichen sie nicht nur von der sonst üblichen Bezeichnung „Verkehrsdaten“ ab, sondern auch von § 101a Abs. 3 StPO-E, der nur von „personenbezogenen Daten“ spricht.[46] Ob mit dem Begriff „verwertbare personenbezogene Daten“ eine weitere, dritte Datenkategorie bezeichnet werden soll, bleibt erneut unklar. Auch hier spricht allerdings die Gesetzesbegründung für ein redaktionelles Versehen, da die Daten dort ohne weitere Begründung unterschiedlich bezeichnet werden („personenbezogene Verkehrsdaten“,

45 Zum Ganzen: BVerfGE 125, 260, 329, 333.

46 Siehe dazu oben S. 13 f.

„Verkehrsdaten“). Die Forderung des Bundesverfassungsgerichts nach einer normenklaren Regelung wird daher an dieser Stelle nicht umgesetzt.

Materiell regelt der Gesetzentwurf, dass die Weitergabe der Daten an eine andere Stelle für andere Zwecke nur zulässig ist, wenn diese Stelle ihrerseits zur Erhebung der Daten berechtigt wäre (§ 101a Abs. 4 Satz 1 Nr. 1 und Nr. 2 StPO-E). Dabei werden die unterschiedlichen Voraussetzungen für die Datenerhebung von Strafverfolgungsbehörden und Behörden zur Gefahrenabwehr berücksichtigt.[47] Eine Unklarheit findet sich dabei allerdings in § 101a Abs. 4 Satz 1 Nr. 1 StPO-E, nach dem die Datenweitergabe zwischen Strafverfolgungsbehörden in zwei Fällen zulässig ist: Erstens, wenn diese Daten auch aufgrund der Vorschriften zur Erhebung von Vorratsdaten erhoben werden dürften (§ 100g Abs. 2, auch in Verbindung mit § 100g Abs. 3 StPO-E) oder, zweitens, wenn sie der Ermittlung des Aufenthalts der einer solchen Straftat beschuldigten Person dienen sollen. Die eigenständige Bedeutung dieser zweiten Variante bleibt unklar. Denn die Vorratsdaten dürfen nach § 100g Abs. 2 StPO (erste Variante) auch erhoben werden, um den Aufenthalt eines Beschuldigten, dem eine der dort genannten Straftaten zur Last gelegt wird, zu ermitteln. Es scheint, als wäre die zweite Variante letztlich doppelt geregelt. Auch aus der Gesetzesbegründung ergeben sich keine weiteren Hinweise darauf, warum diese zwei Varianten gewählt wurden. Die Begründung deutet vielmehr darauf hin, dass auch in diesem Falle ein redaktioneller Fehler vorliegt. Somit fehlt auch hier eine normenklare Regelung.

Bei der Ermächtigung zur Datenweitergabe von den Strafverfolgungsbehörden an die Behörden zur Gefahrenabwehr wird durch § 101a Abs. 4 Nr. 2 StPO-E die Weitergabe nicht ausdrücklich auf Behörden zur Gefahrenabwehr der Länder eingeschränkt. Die Vorschrift nennt lediglich in Klammern die Regelung des § 113 Abs. 1 Nr. 2 TKG-E, der diese Einschränkung vorsieht. Aus welchem Grunde diese Beschränkung auf Landesbehörden an dieser Stelle in den Wortlaut der Vorschrift nicht aufgenommen werden soll, bleibt unklar. Auch die Gesetzesbegründung gibt darüber keine Auskunft. Um die Vorgabe des Bundesverfassungsgerichts zu erfüllen und normenklare Regelungen zu schaffen, müsste daher wohl diese Beschränkung auf Landesbehörden in den Wortlaut aufgenommen oder die Erweiterung auf Bundesbehörden zur Gefahrenabwehr ausdrücklich genannt und dies auch in der Gesetzesbegründung erläutert werden.

Im Hinblick auf eine Datenweitergabe von Strafverfolgungsbehörden an Behörden der Gefahrenabwehr (der Länder) enthält § 101a Abs. 4 Satz 3 und Satz 4 StPO-E Regelungen über die Datenlöschung, die Protokollierung der Löschung und sonstige Zweckbindungen der Daten. Insoweit gibt das Bundesgesetz an dieser Stelle den Landesbehörden zur Gefahrenabwehr diese Regelungen vor, obwohl die Regelungen zur Gefahrenabwehr einschließlich der Datenschutzvorschriften in der Gesetzgebungskompetenz der Länder liegen dürften. Zwar handelt es sich hier um Vorratsdaten, die zunächst aufgrund einer bundesrechtlichen Vorschrift (§ 100g Abs. 2 StPO-E) erhoben wurden. Die Landesbehörden zur Gefahrenabwehr benötigen aber auch für die weitergegebenen Daten ihrerseits eine eigene landesrechtliche Ermächtigungsgrundlage (Doppeltürprinzip), worauf auch die Gesetzesbegründung hinweist.[48] Daher erscheint auch aufgrund des Sachzusammenhangs eine bundesrechtliche Regelung nicht zwingend notwendig. Denn die entsprechenden landesrechtlichen Vorschriften unterliegen ebenfalls den Anforderungen des Bundesverfassungsgerichts, so dass auch sie nur dann Vorratsdaten erheben bzw. deren Weiterleitung von Strafverfolgungsbehörden

47 Vgl. dazu oben Ziff. 4.3.1.1 und Ziff. 4.3.1.2.

48 Begründung des Gesetzentwurfs, BR-Drs. 249/15, S. 37.

erbitten dürfen, wenn das Landesgesetz ausreichende Regelungen zum Datenschutz und insbesondere auch zu ihrer Löschung vorsieht. Die Gesetzgebungskompetenz des Bundes für diese Regelung steht somit in Frage. Auch die Gesetzesbegründung nimmt dazu nicht Stellung.

Insgesamt müsste somit insbesondere § 101a Abs. 4 StPO-E genauer gefasst werden, um die Forderung des Bundesverfassungsgerichts nach normenklaren Regelungen richtig umzusetzen.

4.3.4. Übermittlungs- und Verwendungsverbote bei besonderer Vertraulichkeit

In der Entscheidung zur Vorratsdatenspeicherung führt das Gericht weiter aus, dass es verfassungsrechtlich geboten sei, die Übermittlung von Daten über Telekommunikationsverbindungen, die auf eine besondere Vertraulichkeit angewiesen seien, grundsätzlich auszuschließen. Dies betreffe etwa Verbindungen zu Anschlüssen von Personen, Behörden und Organisationen in sozialen oder kirchlichen Bereichen, die grundsätzlich anonym bleibenden Anrufern ganz oder überwiegend telefonische Beratung in seelischen oder sozialen Notlagen anbieten.[49]

Der Gesetzentwurf unterscheidet hier zwei Fälle: Telekommunikationsdaten in Bezug auf Personen, Behörden und Organisationen in sozialen oder kirchlichen Bereichen, wie sie in § 99 Abs. 2 TKG genannt sind, dürfen schon nicht von den Diensteanbietern gespeichert werden (§ 113b Abs. 6 TKG-E). Dies korrespondiert mit dem Verbot der Diensteanbieter, die Telekommunikationsverbindungen dieser Personen etc. für Einzelverbindungsnachweise zu speichern (§ 99 Abs. 2 TKG). Daten von (sonstigen) Personen, denen im Zusammenhang mit diesen Daten nach § 53 Abs. 1 Nr. 1 bis Nr. 5 StPO ein Zeugnisverweigerungsrecht zusteht, dürfen nach dem Gesetzentwurf hingegen „nur“ nicht abgerufen werden (Erhebungsverbot); dennoch erlangte Daten und Erkenntnisse aus diesem Bereich dürfen nicht verwertet (Verwertungsverbot) werden (§ 100g Abs. 4 Satz 1 und Satz 2 StPO-E).

Der Gesetzentwurf geht damit zunächst über die Anforderungen des Bundesverfassungsgerichts in Bezug auf die Telekommunikationsdaten von Personen, Behörden und Organisationen in sozialen oder kirchlichen Bereichen hinaus. Das Gericht hatte für diese Daten nur ein Übermittlungsverbot gefordert, der Gesetzentwurf sieht jedoch schon vorgelagert ein Speicherverbot vor. Damit steht der Entwurf insoweit im Einklang mit dieser Rechtsprechung.

Das Bundesverfassungsgericht hat in der Entscheidung zur Vorratsdatenspeicherung hingegen die Behandlung der Daten von zeugnisverweigerungsberechtigten Personen nicht ausdrücklich erwähnt. Der von dem Gericht genannte besondere Vertrauensschutz dürfte jedoch auch für diese Telekommunikationsvorgänge im Grundsatz gelten. Der Gesetzentwurf sieht hier kein Speicherverbot, sondern „nur“ ein Erhebungsverbot für die Strafverfolgungsbehörden und, falls doch entsprechende Daten (unerkannt) übermittelt werden, ein Verwertungsverbot vor. Für den Bereich der Behörden und Organisationen in sozialen oder kirchlichen Bereichen fordert das Bundesverfassungsgericht ein „Übermittlungsverbot“, so dass die Diensteanbieter diese Daten schon nicht übermitteln dürfen. Bei den Daten, die mit einem Zeugnisverweigerungsrecht in Zusammenhang stehen können, kann aber aufgrund der bestehenden rechtlichen Vorgaben und wohl auch der technischen Abläufe kein solches Übermittlungsverbot gefordert werden. Um einem solchen Verbot nachkommen zu können, müssten die Diensteanbieter erkennen können, ob der

49 BVerfGE 125, 260, 334.

Inhalt eines Telekommunikationsvorgangs und damit auch die zugehörigen Daten einem Zeugnisverweigerungsrecht unterfallen. Den Inhalt eines Telekommunikationsvorgangs dürfen sie jedoch nicht auswerten (§ 88 Abs. 1 i.V.m. § 96 Abs. 1 und Abs. 2 TKG). Auch zu den Inhalten der Ermittlungsakten der Staatsanwaltschaft, aus denen sich gegebenenfalls Hinweise auf ein Zeugnisverweigerungsrecht ergeben können, haben sie keinen Zugang. Insofern sind letztlich nur die Strafverfolgungsbehörden und ihnen folgend die Richter in der Lage, aufgrund der bereits feststehenden Ermittlungsergebnisse zu prüfen, ob ein bestimmter Telekommunikationsvorgang einem Zeugnisverweigerungsrecht im Sinne des § 53 Abs. 1 Nr. 1 bis Nr. 5 StPO unterfällt und daher ein Erhebungsverbot besteht. Vor diesem Hintergrund dürfte das Erhebungs- und das Verwertungsverbot nach § 100g Abs. 4 Satz 1 und Satz 2 StPO-E den Forderungen des Bundesverfassungsgerichts aus der Vorratsdatenentscheidung nicht widersprechen.[50]

4.4. Richtervorbehalt, Transparenz und Rechtsschutz

Neben der Datenspeicherung, -sicherung und -verwendung stellt das Bundesverfassungsgericht noch weitere wichtige Voraussetzungen für die Vorratsdatenspeicherung auf. Dazu gehören die Anordnung der Datenerhebung durch den Richter im Einzelfall, die Information der Betroffenen über die Datenerhebung und die Eröffnung eines Rechtsschutzverfahrens zur nachträglichen Kontrolle der Verwendung der Daten.

4.4.1. Gerichtliche Anordnung der Datenverwendung im Einzelfall

In seiner Entscheidung zur Vorratsdatenspeicherung führt das Bundesverfassungsgericht aus, dass die Verwendung dieser Daten grundsätzlich unter den Vorhabehalt richterlicher Anordnung zu stellen ist. Der Gesetzeber habe in spezifischer und normenklarer Form strenge Anforderungen an den Inhalt und die Begründung der gerichtlichen Anordnung zu stellen. Die Anordnung sei daher hinreichend substantiiert zu begründen. Außerdem müsse darin der Umfang der abzufragenden Daten hinreichend selektiv und für den Diensteanbieter eindeutig beschrieben werden.[51]

Vor diesem Hintergrund sieht der Gesetzentwurf vor, dass die Vorratsdaten ausschließlich aufgrund einer richterlichen Anordnung erhoben werden dürfen (§ 101a Abs. 1 StPO-E i.V.m. § 100b Abs. 1 bis Abs. 4 StPO). Eine Erhebung ohne richterliche Anordnung, insbesondere bei Gefahr im Verzug, soll ausgeschlossen sein (§ 101a Abs. 1 Satz 2 StPO-E).

Darüber hinaus trifft der Gesetzentwurf auch zum Inhalt der richterlichen Anordnung nähere Bestimmungen: In der richterlichen Entscheidungsformel müssen neben den in § 100b Abs. 2 Satz 2 StPO genannten Angaben auch die zu übermittelnden Daten und der Zeitraum, für den sie übermittelt werden sollen, eindeutig angegeben werden (§ 101a Abs. 1 Satz 1 Nr. 1 StPO-E). Dazu ergänzend ist in § 101a Abs. 2 StPO-E vorgesehen, dass in der Begründung der richterlichen Anordnung einzelfallbezogen insbesondere die wesentlichen Erwägungen zur Erforderlichkeit

---

50 Vgl. aber die erhebliche Kritik an dieser geplanten Regelung in der Stellungnahme des Deutschen Anwaltsvereins vom 20.05.2015, S. 12 ff., im Internet aufrufbar unter: http://anwaltverein.de/de/newsroom/sn-25-15-referentenentwurf-des-bundesministeriums-der-justiz-und-fuer-verbraucherschutz-fuer-ein-gesetz-zur-einfuehrung-einer-sp.

51 Zum Ganzen: BVerfGE 125, 260, 337 f., 354 f.

der Maßnahme, auch hinsichtlich des Umfanges der zu erhebenden Daten und des Zeitraums, für den sie erhoben werden sollen, darzulegen sind.

Mit diesen Vorschriften setzt der Gesetzentwurf die Vorgaben des Bundesverfassungsgerichts wohl richtig um.

4.4.2. Information der Betroffenen

Nach den Vorgaben des Bundesverfassungsgerichts muss der Betroffene *vor* der Datenabfrage bzw. *vor* der Übermittlung seiner Daten an die Strafverfolgungsbehörden grundsätzlich benachrichtigt werden. Von dieser Unterrichtung dürfe nur dann abgesehen werden, wenn andernfalls der Zweck der Untersuchung, dem der Datenabruf dient, vereitelt würde und diese heimliche Verwendung richterlich angeordnet werde. Für die Fälle einer Verwendung der Daten ohne Wissen des Betroffenen sei der Gesetzgeber verpflichtet, seine nachträgliche Benachrichtigung vorzusehen.[52]

Der Gesetzentwurf regelt in § 101a Abs. 6 StPO-E, dass die Betroffenen bei einer Erhebung von Vorratsdaten zu benachrichtigen sind. Sowohl das Unterbleiben der Benachrichtigung (Abs. 6 Nr. 1) als auch die Zurückstellung der Benachrichtigung bedürfen einer Anordnung des zuständigen Gerichts (Abs. 6 Nr. 2). Insofern ist auch der vom Bundesverfassungsgericht geforderte Richtervorbehalt bei unterbleibender Benachrichtigung durch den Gesetzentwurf gewahrt.

Allerdings regelt der Gesetzentwurf nicht ausdrücklich den Zeitpunkt der Unterrichtung. Das Bundesverfassungsgericht fordert jedoch, dass der Betroffene *vor* der Datenabfrage bzw. *vor* der Übermittlung seiner Daten zu unterrichten ist.[53] In der Begründung zum Gesetzentwurf wird dazu ausgeführt, dass das über die Datenverwendung entscheidende Gericht nach § 33 StPO dem Betroffenen vor seiner Entscheidung Gelegenheit zum rechtlichen Gehör geben muss.[54] Die Entscheidung des Richters ergeht in diesen Fällen außerhalb der Hauptverhandlung und daher nach § 33 Abs. 2 StPO zunächst nur nach schriftlicher oder mündlicher Erklärung der Staatsanwaltschaft. Gemäß § 33 Abs. 3 StPO ist bei einer solchen Entscheidung ein „anderer Beteiligter zu hören, bevor zu seinem Nachteil Tatsachen oder Beweisergebnisse, zu denen er noch nicht gehört worden ist, verwertet werden“. Zwar soll eine Verwendung von Vorratsdaten nach § 100g Abs. 2 StPO-E nur dann zulässig sein, wenn bestimmte Tatsachen den Verdacht begründen, dass jemand eine schwere Straftat begangen hat, so dass es bei der entsprechenden richterlichen Entscheidung in der Regel auch auf Tatsachen im Sinne des § 33 Abs. 3 StPO ankommen dürfte und damit der Betroffene anzuhören wäre. Ob diese gesetzliche Konstruktion über § 33 StPO jedoch dazu führt, dass – wie vom Bundesverfassungsgericht gefordert – in jedem Falle, der nicht ausnahmsweise der Geheimhaltung unterliegt, der Betroffene *vor* der Erhebung informiert werden muss, bleibt unklar. Da das Bundesverfassungsgericht jedoch normenklare Regelungen fordert,[55] wird nach Meinung der Verfasserin auch an dieser Stelle diese Vorgabe des Bundesverfassungsgerichts nicht richtig umgesetzt, zumal § 101a Abs. 6 StPO-E auch nicht – zur Klarstellung – auf § 33 StPO verweist. Daher müsste in § 101a Abs. 6 StPO-E ausdrücklich aufgenommen werden, dass der Betroffene *vor* der

52 Zum Ganzen: BVerfGE 125, 260, 336.

53 BVerfGE 125, 260, 336.

54 Begründung des Gesetzentwurfs, BR-Drs. 249/15, S. 37.

55 Siehe oben Fn. 43.

Datenabfrage bzw. *vor* der Übermittlung seiner Daten zu unterrichten ist. Andernfalls werden die verfassungsrechtlichen Vorgaben nicht richtig umgesetzt.

4.4.3. Rechtsschutzverfahren

Das Bundesverfassungsgericht fordert schließlich die Einrichtung eines Rechtsschutzverfahrens zur nachträglichen Kontrolle der Verwendung der Daten.[56] Diesbezüglich verweist der Gesetzentwurf in § 101a Abs. 6 Satz 2 StPO-E auf eine entsprechende Anwendung des § 101 Abs. 7 StPO. Dieser sieht in seinen Sätzen 2 und 3 ein nachträgliches Rechtsschutzverfahren vor. Diese gesetzliche Konstellation galt schon im Rahmen der alten Vorschriften zur Vorratsdatenspeicherung. In seiner Entscheidung über diese Vorschriften führt das Bundesverfassungsgericht aus, es seien keine Gründe dafür ersichtlich, dass diese Vorschriften einen effektiven Rechtsschutz insgesamt nicht gewährleisten.[57] Damit dürfte auch der aktuelle Gesetzentwurf in Bezug auf ein nachträgliches Rechtsschutzverfahren den verfassungsrechtlichen Anforderungen genügen.

Zu möglichen Sanktionen bei Rechtsverletzungen stellt das Bundesverfassungsgericht in der Vorratsdatenentscheidung fest, dass diese zwar verfassungsrechtlich notwendig seien, es sei dem Gesetzgeber jedoch gestattet, zunächst zu beobachten, ob aufgrund der bestehenden Vorschriften entsprechende Rechtsverletzungen bereits ausreichend sanktioniert werden könnten.[58] Der Gesetzentwurf enthält zwar für die Diensteanbieter bzw. ihre Mitarbeiter eine Bußgeldvorschrift für die Fälle, dass jemand aus diesem Kreise die Vorratsdaten für andere als die erlaubten Zwecke verwendet (§149 Abs. 1 Nr. 39 TKG-E), eine Sanktionsvorschrift für weitere Personen, z.B. Mitarbeiter der Strafverfolgungsbehörden, ist jedoch nicht vorgesehen. Der Gesetzentwurf macht insoweit wohl von dem Hinweis des Bundesverfassungsgerichts Gebrauch, dass der Gesetzgeber zunächst beobachten dürfe, ob die bestehenden Vorschriften ausreichen, um entsprechende Persönlichkeitsrechtsverletzungen zu ahnden.

In diesem Bereich setzt der Gesetzentwurf die Vorgaben des Bundesverfassungsgerichts daher wohl richtig um.

5. Fazit

Bei der Prüfung des Gesetzentwurfs anhand der Vorgaben des Bundesverfassungsgerichts in seiner Entscheidung zur Vorratsdatenspeicherung ergibt sich, dass sich der Entwurf in weiten Teilen eng an diese Vorgaben hält. Dies gilt insbesondere für die neuen Regelungen zur Speicherung der Daten im TKG (dazu oben S. 7 ff.). Bei den neuen Regelungen zur Verwendung der Daten durch die Strafverfolgungsbehörden in der StPO gilt dies insbesondere für die Ermächtigung zur Erhebung der Vorratsdaten (§ 100g Abs. 2 auch i.V.m. Abs. 3 Satz 2 StPO – dazu oben S. 10 ff.). Allerdings enthalten die flankierenden Regelungen etwa zur Datenverwendung, -löschung, -weitergabe eine Reihe von Unklarheiten. Da das Bundesverfassungsgericht nicht nur materiell verfassungsmäßige, sondern auch normenklare Vorschriften fordert, müssen diese Unklarheiten korrigiert werden, um die Vorgaben des Gerichts richtig umzusetzen. Zu diesen Unklarheiten gehört unter anderem

56 BVerfGE 125, 260, 339.

57 BVerfGE 125, 260, 354.

58 BVerfGE 125, 260, 339.

die unterschiedliche Bezeichnung der Daten in § 101a Abs. 3, Abs. 4 und Abs. 5 StPO-E („personenbezogene Daten“, „verwertbare personenbezogene Daten“ auch im Verhältnis zu der sonst gebrauchten Bezeichnung als „Verkehrsdaten“ - dazu oben S. 13 f., S. 14). Zu den unklaren Regelungen gehört auch die Vorschrift über die Löschung der Daten (§ 101a Abs. 3 Satz 4 StPO-E i.V.m. § 101 Abs. 8 StPO). Diese sieht entgegen den Anforderungen des Bundesverfassungsgerichts nach hiesiger Auffassung bisher die Löschung von Daten, die von vornherein für die Erhebungszwecke unerheblich sind, nicht normenklar vor (dazu oben S. 13). Bei der Regelung zur Weitergabe der Vorratsdaten an andere Behörden für andere Zwecke (§ 101a Abs. 4 StPO-E) finden sich ebenfalls einige Unklarheiten, die noch korrigiert werden müssen. Dazu gehört auch die Frage, auf welche Gesetzgebungskompetenz des Bundes sich die Regelungen in § 101a Abs. 4 Satz 3 und Satz 4 StPO-E stützt (dazu oben S. 15). Darin werden den Landesbehörden zur Gefahrenabwehr bestimmte Lösch-, Protokoll und Verwendungspflichten für die an sie weitergeleiteten Daten bundesgesetzlich vorgegeben, obwohl die Länder vor einem Abruf solcher Daten ohnehin zunächst eigene Regelungen zum Abruf, Schutz und zur Löschung dieser Daten vorsehen müssen. Schließlich ist auch die Vorgabe des Bundesverfassungsgerichts, dass der Betroffene grundsätzlich *vor* der Datenerhebung von dieser zu unterrichten ist, nicht richtig, insbesondere erneut nicht normenklar in § 101a Abs. 6 StPO-E umgesetzt (dazu oben S. 18 f.). Diese verfassungsrechtliche Vorgabe müsste direkt in den Wortlaut des § 101a Abs. 6 StPO-E aufgenommen werden.