Die Bundesbeauftragte
für den Datenschutz und
die Informationsfreiheit

Andrea Voßhoff
Bundesbeauftragte für den Datenschutz
und die Informationsfreiheit

Stellungnahme der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit zum Entwurf eines Gesetzes zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten (BR-Drucksache 249/15)

Im Folgenden nehme ich Stellung zum Regierungsentwurf des Bundesministeriums der Justiz und für Verbraucherschutz (BMJV) für ein **„Gesetz zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten“**[1] in der Fassung vom 28.05.2015.

Im Ergebnis kann der Entwurf meine bereits geäußerten Bedenken an der Möglichkeit einer verfassungsgemäßen Umsetzung der Vorratsdatenspeicherung nicht ausräumen. Insbesondere entspricht er nicht vollumfänglich dem, was das Bundesverfassungsgericht und der Europäische Gerichtshof in ihren Urteilen für die verfassungskonforme Ausgestaltung einer solchen Maßnahme gefordert haben.

Als zuständige Datenschutzaufsichtsbehörde der TK-Branche mit der daraus resultierenden Kontrollpraxis bei TK-Anbietern vor Ort stelle ich immer wieder fest, wie hochgradig komplex deren Datenverarbeitungssysteme und –verfahren sind.

Zur eine besseren Verständlichkeit dieser Datenverarbeitungssysteme habe ich daher dieser Stellungnahme eine Erläuterung der grundlegenden Begriffe und Prozesse der Verkehrsdatenverarbeitung (in **Anlage 1**), eine graphische Darstellung der Datenflüsse der wichtigsten verkehrsdatenverarbeitenden Systeme (in **Anlage 2**), sowie den von mir in Zusammenarbeit mit der Bundesnetzagentur erstellten „Leitfaden der BfDI und der Bundesnetzagentur für eine datenschutzgerechte Speicherung von Verkehrsdaten“ (in **Anlage 3**) beigefügt.

I. Allgemeine Erwägungen

1. Gesetzgebungsverfahren

Die Art und Weise, in der das Gesetzgebungsverfahren vorliegend vom BMJV betrieben wurde, ist inakzeptabel. Vorgaben der Gemeinsamen Geschäftsordnung der Bundesministerien (GGO), nach der alle Anzuhörenden rechtzeitig zu beteiligen sind, wurden mehrfach ignoriert.

So wurde mir zur Abgabe einer ersten Stellungnahme eine Frist von faktisch weniger als 30 Stunden gewährt. Dass dieser Zeitraum nicht ausreichend ist,

[1] BR-Drucksache 249/15.

um einen umfangreichen Gesetzentwurf wie den vorliegenden sorgsam durchzuarbeiten und zu prüfen, versteht sich von selbst. Auch die Wechselwirkungen zum bestehenden Recht und zu weiteren laufenden Gesetzgebungsverfahren übergreifend in den Blick zu nehmen, ist in einem Gesetzgebungsverfahren mit dieser geradezu absurden Beteiligungsfrist unmöglich. Ebenso wurde auf eine offizielle Ressortbesprechung verzichtet, um den Regierungsentwurf schon sieben Arbeitstage nach Versendung an den Ressortkreis im Kabinett beschließen zu können.

Gründe, warum vorliegend derart kurze Fristen gesetzt wurden, sind nicht erkennbar. Eine erhöhte Eilbedürftigkeit lässt sich weder mit einer unmittelbaren kriminalpolitischen Notwendigkeit begründen, zumal der Gesetzentwurf in § 150 Absatz 13 TKG-E eine Übergangsfrist von 18 Monaten bis zum Beginn der Speicherung vorsieht, noch ist ein zwingendes politisches Handeln zur Umsetzung der Festlegungen im Koalitionsvertrag erforderlich, der lediglich die Umsetzung der europäischen Richtlinie zur Vorratsdatenspeicherung fordert[2], nicht hingegen die Einführung einer von europäischen Vorgaben isolierten nationalen Lösung.

Es ist nicht akzeptabel, dass ein Gesetzesvorhaben, das massive Eingriffe in die Grundrechte der Bürgerinnen und Bürger zur Folge hat und absolute Kernthemen des Datenschutzes (insbesondere im Bereich der meiner Aufsicht unterstehenden Telekommunikationsbranche und Sicherheitsbehörden) betrifft, faktisch ohne meine Beteiligung durchgeführt wird. Dieser Umstand wiegt umso schwerer, als eine Einbindung nach den Vorschriften der GGO auch schon bereits im Rahmen der Erarbeitung des Referentenentwurfes hätte erfolgen können, wenn nicht sogar müssen. Dies wäre auch ohne weiteres möglich gewesen, da der Entwurf vor der offiziellen Versendung an den Ressortkreis ja auch mit Kollegen des Bundesministeriums des Innern und des Bundesministeriums für Wirtschaft und Energie abgestimmt wurde.

2. Verfassungswidrigkeit der Vorratsdatenspeicherung

Der Gesetzentwurf ist nach wie vor nicht in der Lage, die erheblichen Zweifel an der generellen Verfassungsmäßigkeit einer Vorratsdatenspeicherung von Telekommunikationsverkehrsdaten zu beseitigen.

[2] „Deutschlands Zukunft Gestalten“, Koalitionsvertrag zwischen CDU,CSU und SPD, S. 102 f.

a) Geeignetheit

Erhebliche Zweifel bestehen bereits hinsichtlich der Geeignetheit der Maßnahme. Der Gesetzentwurf begründet die Notwendigkeit der Regelung mit *„der zunehmen-den Bedeutung der Telekommunikation für die Vorbereitung und Begehung von Straftaten“*[3], benennt aber gleichzeitig explizit **Umgehungsmöglichkeiten**, die dazu führen, nicht von der Speicherung erfasst zu werden. Er zeigt somit selbst die Wege auf, wie Telekommunikation auch nach Einführung des Gesetzes hervorragend für die Vorbereitung und Begehung von Straftaten genutzt werden kann.

Durch die in der Begründung zu § 113a TKG-E nunmehr offiziell bestätigte Ausnahme von Callshops, Internet-Cafés und öffentlich zugänglichen Telefon- oder W-LAN-Angeboten in Restaurants oder Hotels[4] können sämtliche Kommunikationswege genutzt werden, ohne Spuren in den auf Vorrat gespeicherten Daten zu hinterlassen. Außerdem sollen ebenfalls E-Mail Verkehrsdaten nicht zu den zu speichernden Daten gehören.

Unterstellt man den Kriminellen (insbesondere denjenigen, die schwerste Straftaten verüben und die mit der Vorratsdatenspeicherung bekämpft werden sollen) nicht eine überwiegend ausgeprägt fehlende Intelligenz, dürfte sich ein Großteil der für die Strafverfolgung relevanten Korrespondenz in Zukunft auf die oben dargestellten Kommunikationswege verlagern. Die mit der Vorratsdatenspeicherung erfassten Daten werden daher zu einem noch größeren Prozentsatz solche von unbescholtenen Bürgerinnen und Bürgern sein, die keinerlei Anlass für eine strafrechtliche Verfolgung geben, als dies schon ohnehin der Fall ist.

Zwar hat das Bundesverfassungsgericht (BVerfG) in diesem Zusammenhang ausgeführt, die Möglichkeit des Unterlaufens der Speicherung im Einzelfall führe nicht zwingend zur Ungeeignetheit der Maßnahme, solange die Zweckerreichung generell gefördert wird.[5] Hierbei legte das Gericht aber noch nicht eine Speicherpraxis zu Grunde, in der mit der E-Mail eines der meistgenutzten Telekommunikationsmittel aus der Erfassung ausgeschlossen wurde. Gegenwärtig werden pro Jahr über 500 Milliarden E-Mails (ohne Spam) verschickt.[6] Zudem sind möglicherweise auch Messengerdienste wie das zu Facebook gehörende

[3] Begründung des Regierungsentwurfs, S. 23.
[4] Begründung des Regierungsentwurfs, S. 42.
[5] BVerfG, NJW 2010, S. 833 (835), Absatz Nr. 207.
[6] http://de.statista.com/statistik/daten/studie/392576/umfrage/anzahl-der-versendeten-e-mails-in-deutschland-pro-jahr/ (zuletzt aufgerufen am 29.05.2015).

WhatsApp nicht von der Speicherpflicht umfasst und können somit nicht zur Auskunftserteilung herangezogen werden (siehe III.1.b) unten). Gerade letzterer wird aber in Deutschland von fast 60% aller mobilen Internetnutzer verwendet.[7] Bereits im Jahr 2012 hatte die Anzahl der mit Messengerdiensten verschickten Nachrichten die Anzahl der verschickten SMS überholt, Ende 2013 war die Zahl sogar doppelt so groß.[8]

Anders als vom BVerfG zu Grunde gelegt, geht es vorliegend also nicht mehr bloß um Einzelfälle, die durch das Raster fallen. Zudem muss auch kein erhöhter Aufwand wie die Beschaffung ausländischer SIM-Karten mehr betrieben werden, um der Speicherung zu entgehen. Die Nutzung der nicht von der Vorratsdatenspeicherung erfassten E-Mail ist auch bequem von der heimischen Couch aus möglich. Im Ergebnis wird bei einem dermaßen großen selbstgeschaffenen „Blindspot“ auch unter der Maßgabe des BVerfG das Vorliegen einer geeigneten Maßnahme äußerst fraglich.

b) Erforderlichkeit

Die im Rahmen der Erwägung zur Geeignetheit (siehe a) oben) geäußerten Bedenken, der gewünschte Effekt einer Verbesserung der Strafverfolgung und Gefahrenabwehr werde durch den vorliegenden Gesetzentwurf nicht erreicht, verstärken sich noch, da auch die Erforderlichkeit der Maßnahme nicht hinreichend belegt wird.

In der Begründung wird lediglich darauf hingewiesen, die aus betrieblichen Gründen bei den TK-Anbietern vorhandenen Daten würden in Verbindung mit den bestehenden Auskunftsrechten zu Unzulänglichkeiten bei der Strafverfolgungsvorsorge und Gefahrenabwehr führen.[9] Grund wäre der Umstand, dass *„[…] die **Speicherpraxis der Erbringer** öffentlich zugänglicher Telekommunikationsdienste sehr unterschiedlich ist“*, so dass es *„[…] derzeit vom Zufall abhängig [ist], welche Daten bei einer Abfrage nach § 100g StPO abgerufen werden können“*[10].

[7] http://de.statista.com/statistik/daten/studie/299740/umfrage/anteil-der-whatsapp-nutzer-an-allen-mobilen-internetnutzern-weltweit/ (zuletzt aufgerufen am 29.05.2015).
[8] http://www.heise.de/newsticker/meldung/Marktforscher-Messenger-wie-WhatsApp-ueberholen-die-SMS-1852549.html (zuletzt aufgerufen am 29.05.2015).
[9] Begründung des Regierungsentwurfs, S. 22.
[10] a.a.O.

Diese Aussage ist nach meinen umfangreichen und jahrelangen Prüferfahrungen bei den TK-Anbietern nicht nachvollziehbar. So werden beispielsweise Verkehrsdaten von Telefonverbindungen zu betrieblichen Zwecken regelmäßig zwischen drei und sechs Monaten vorgehalten (siehe hierzu auch die in **Anlage 3** aufgeführten Speicherfristen der einzelnen Datenverarbeitungen). Diese Notwendigkeit ergibt sich schon aus dem den Kunden zustehenden, in § 45i Absatz 1 TKG gesetzlich normierten Einspruchszeitraum von acht Wochen nach Rechnungsversand. Somit kann davon ausgegangen werden, dass der überwiegende Teil der zu speichernden Daten bei den TK-Anbietern – jedenfalls in dem vom Gesetzesentwurf festgelegten Zeitraum von zehn Wochen – ohnehin vorhanden ist und somit auch nach Maßgabe des geltenden Rechts für Auskünfte an die Sicherheitsbehörden zur Verfügung steht.

Eine Ausnahme hiervon bilden lediglich die den Teilnehmern zugewiesenen IP-Adressen – die grundsätzlich nur bis zu sieben Tage gespeichert werden –, Standortdaten in Form der Funkzellen sowie unter eine sogenannte Flatrate fallende netzinterne Verbindungen, die jeweils je nach System des TK-Anbieters üblicherweise zwischen 7 und 30 Tage abrufbar sind. Im Gesamtvolumen der zu speichernden Daten dürften diese aber einen eher geringen Anteil ausmachen. Im Ergebnis ist die hier angeordnete Doppelspeicherung von unzähligen Daten daher absolut unnötig.

Als milderes Mittel könnte sich die Speicheranordnung auf die vorab genannten Datenarten beschränken und für diese lediglich eine längere Speicherfrist festsetzen.

Weitere Ausführungen zur Erforderlichkeit finden sich im Gesetzentwurf im Übrigen nicht. Dabei wäre es nicht nur wünschenswert, sondern verfassungsrechtlich geboten, dass der Gesetzgeber die Erforderlichkeit des massiven Grundrechtseingriffs belegt.[11] Dieser Darlegungslast kann vorliegend auch nicht mit dem Argument entgangen werden, das Gesetz sei noch nicht in Kraft, so dass dementsprechend auch noch keine Ergebnisse über die Auswirkungen der Vorratsdatenspeicherung vorlägen.

Da es sich bei der in Rede stehenden Maßnahme nicht um eine neue, sondern um eine neu aufgelegte handelt, gibt es aus der Vergangenheit einschlägige,

[11] BVerfG, NJW 2007, S. 2167 (2169), Absatz Nr. 21.

wenn auch nicht unumstrittene Gutachten[12], die im Ergebnis keine messbare Effektivitätssteigerung durch die damalige Vorratsdatenspeicherung festgestellt haben. Die Bundesregierung verweist in dem vorliegenden Gesetzentwurf auf das BVerfG. Dieses habe wiederholt das verfassungsrechtliche Gebot einer effektiven Strafverfolgung hervorgehoben, das Interesse an einer möglichst vollständigen Wahrheitsermittlung im Strafverfahren betont und die wirksame Aufklärung gerade schwerer Straftaten als einen wesentlichen Auftrag eines rechtsstaatlichen Gemeinwesens bezeichnet. Dass aber eine Steigerung dieser Effektivität durch eine stark eingeschränkte Neuauflage der Vorratsdatenspeicherung erreicht werden kann, ist zu bezweifeln und damit auch das Vorliegen der verfassungsmäßigen Erforderlichkeit des Eingriffs.

c) Verhältnismäßigkeit

Schließlich bestehen grundlegende Bedenken gegenüber der Verhältnismäßigkeit der Maßnahme. Selbst wenn man die Annahme unterstellen würde, dass die Vorratsdatenspeicherung nachweislich förderliche Auswirkungen auf die Effektivität der Strafverfolgung und Gefahrenabwehr hätte, müssten diese Vorteile immer noch in einem angemessenen Rahmen zu der Intensität des Eingriffs stehen.

Da sowohl das BVerfG als auch der Europäische Gerichtshof (EuGH) zweifelsfrei dargelegt haben, dass es sich bei der Vorratsdatenspeicherung um einen schwerwiegenden **Grundrechtseingriff von besonderem Ausmaß** handelt, sind die Anforderungen an die Angemessenheit ebenfalls besonders hoch.

Im Gesetzentwurf werden nicht sämtliche von BVerfG und EuGH an eine verhältnismäßige Ausgestaltung des mit einer Vorratsdatenspeicherung einhergehenden Grundrechtseingriffs geknüpften Anforderungen berücksichtigt, obwohl der im Übrigen sehr detailliert und gründlich ausgearbeitete Entwurf genau diese als allgemeinen Regelungsmaßstab hervorhebt.

(1) Vorgaben des BVerfG

So wird im Entwurf nicht berücksichtigt, dass das BVerfG für *„die verfassungsrechtliche Unbedenklichkeit einer vorsorglich anlasslosen Speicherung der Telekommunikationsverkehrsdaten […] voraus [setzt], dass diese eine Ausnahme bleibt“* und *„sie […] auch nicht im Zusammenspiel mit anderen vorhandenen*

[12] z.B. Gutachten des Max-Planck-Instituts (zweite erweiterte Fassung) Juli 2011, S. 218; Rechtsgutachten des WD des BT vom 25.02.2011, WD 11-3000-18/11.

Dateien zur Rekonstruierbarkeit praktisch aller Aktivitäten der Bürger führen [darf]“[13]. Diese „Überwachungs-Gesamtrechnung“[14] wird jedenfalls im Bereich der **Überwachung der Internetnutzung** außer Acht gelassen. Aufgrund der weitreichenden Verpflichtung zur Speicherung von IP-Adressen (siehe III.1.a) unten) wird bereits nur aufgrund der Vorgaben des vorliegenden Gesetzentwurfes ein äußerst umfangreicher Datenpool geschaffen.

Daneben wurden in den letzten Jahren in immer mehr Gesetzen die Rechtsgrundlagen zur Speicherung und Verarbeitung von IP-Adressen erweitert. Insbesondere im Bereich der Sicherheitsbehörden gibt es z.B. im Bundesverfassungsschutzgesetz weitreichende Zugriffsmöglichkeiten auf entsprechende Daten. Ebenfalls erlaubt etwa § 7 Absatz 4 BKAG die Auskunft über den Inhaber einer IP-Adresse. Die Vorschrift ist nur an die unbestimmte Voraussetzung geknüpft, dass dies für die „Zentralstellenfunktion“ des Bundeskriminalamtes erforderlich sein muss. Mit dem sich aktuell in der parlamentarischen Debatte befindlichen „Entwurfs eines Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz)“ werden den TK-Anbietern weitere Verwendungs- und in diesem Zusammenhang auch indirekt längere Speichermöglichkeiten eingeräumt.

Dabei sind die IP-Adressen nicht nur als Verkehrsdaten im Sinne des TKG, sondern auch als Nutzungsdaten im Sinne des Telemediengesetzes betroffen. Gerade letztere vermitteln aber detaillierte Informationen über die im Internet genutzten Inhalte. Anhand der bei den Telemediendiensten erhobenen Nutzungsdaten können Sicherheitsbehörden im Zusammenspiel mit der Zuordnungsmöglichkeit der IP-Adressen der Vorratsdatenspeicherung (siehe III.2.c) unten) somit zumindest über mehrere Wochen das Surfverhalten der Internetnutzer äußerst detailliert überwachen. Dass es sich hierbei um ein realistisches Szenario handelt, belegt auch die aktuelle Diskussion zum Thema „NSA“, in der unzweifelhaft offen gelegt wurde, dass eine umfassende Überwachung des Internetverkehrs für Nachrichtendienste heute nicht nur kein Problem mehr darstellt, sondern auch tatsächlich praktiziert wird. Durch die in § 113c Absatz 1 Nummer 3 TKG-E geschaffene Verknüpfung mit § 113 TKG können diese auch die in den Vorratsdaten gespeicherten IP-Adressen zumindest mittelbar nutzen (siehe III.2.c) unten).

[13] BVerfG, NJW 2010, S. 833 (839), Absatz Nr. 218.
[14] Bezeichnung nach Roßnagel in NJW 2010, S. 1238 ff.

(2) Vorgaben des EuGH

Der Gesetzentwurf stellt aber nicht nur einen unverhältnismäßigen Eingriff in deutsche, sondern auch in europäische Grundrechte dar. Einerseits ist es erfreulich, dass im Entwurf ausführlich die Anwendbarkeit der **Charta der Grundrechte** der Europäischen Union (Charta) auf das vorliegende Verfahren dargelegt und anerkannt wird.[15] Umso erstaunlicher ist es aber andererseits, dass die Konsequenz nicht die Beachtung der in der Charta garantierten Grundrechte ist.

Die Vorgaben des EuGH im Urteil zur Gültigkeit der Vorratsdatenspeicherungs-Richtlinie 2006/24/EG, nach denen unter anderem eine **Beschränkung der betroffenen Personen** auf solche, die in irgendeiner Weise in eine schwere Straftat verwickelt sein oder deren auf Vorrat gespeicherte Daten aus anderen Gründen zur Verhütung, Feststellung oder Verfolgung schwerer Straftaten beitragen könnten, erforderlich ist,[16] werden jedenfalls weder durch die neuen Vorschriften selber berücksichtigt, noch im Rahmen deren Begründung thematisiert. In letzterer wird lediglich ausgeführt, die vom Gericht gemachten Vorgaben seien im Entwurf hinreichend berücksichtigt worden, da *„vor allem die Kombination der umfassenden Datenspeicherung für einen Zeitraum zwischen sechs und 24 Monaten ohne Differenzierungsmöglichkeit für Datenarten oder die Zwecke der Speicherung […] nach dem Urteil des Gerichtshofs zu einer unverhältnismäßigen Regelung [führen]“*[17].

Mit dieser knappen und nicht überzeugenden Argumentation wird aber gerade der vom EuGH an erster Stelle aufgeführte Grund für die Unverhältnismäßigkeit des Eingriffs der Richtlinie in die Grundrechte auf Achtung des Privat- und Familienlebens in Artikel 7 und Schutz personenbezogener Daten in Artikel 8 der Charta schlichtweg ignoriert. Dies erscheint umso bedenklicher, als der EuGH die herausragende Bedeutung dieser Grundrechte gleich an mehreren Stellen besonders hervorgehoben hat.[18] Im Ergebnis führt der „Verzicht“, die Vorgaben des Gerichts vollumfänglich und insbesondere in einem der Kernpunkte umzusetzen, dazu, dass das vorliegende Gesetzgebungsvorhaben auch die an eine noch verhältnismäßige Einschränkung der Charta zu stellenden Anforderungen nicht erfüllt.

[15] Begründung des Regierungsentwurfs, S. 24.
[16] EuGH, NJW 2014, S. 2169 (2172), Absatz Nr. 59.
[17] Begründung des Regierungsentwurfs, S. 25.
[18] EuGH, NJW 2014, S. 2169 (2171), Absatz Nr. 48 sowie S. 2169 (2172), Absatz Nr. 53.

3. Erfüllungsaufwand

Da ich nicht hinreichend in das Gesetzgebungsverfahren eingebunden wurde (siehe 1 oben), war auch der mir durch die geplanten Regelungen entstehende Erfüllungsmehraufwand im Referentenentwurf nicht berücksichtigt worden. Nach entsprechendem diesseitigem Hinweis, findet sich im Regierungsentwurf immerhin die Formulierung, dass *„Mehraufwand […] auch bei der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit im Rahmen ihrer Kontroll- und Aufsichtstätigkeit [entsteht].“*[19]

Sollte das Gesetz in Kraft treten, würde ich einen erheblich erhöhten Kontrollaufwand hinsichtlich der praktischen Umsetzung der gesetzlichen Vorgaben leisten müssen. Gerade weil es sich bei den geplanten Vorschriften um einen erheblichen Eingriff in die vom Grundgesetz und der Charta geschützten Rechte der Telekommunikationsnutzer handelt, ist eine engmaschige Überwachung sowohl der Speicherpraxis bei den TK-Anbietern als auch der Datenerhebung und Verwendung durch die meiner Aufsicht unterstehenden Sicherheitsbehörden erforderlich.

In diesem Zusammenhang werden daher nicht nur anlassbezogene, sondern auch engmaschige Grundsatzkontrollen durchgeführt werden müssen. Gerade im TK-Bereich, wo der Gesetzentwurf selbst von ca. 1.000 zur Speicherung verpflichteten Unternehmen ausgeht,[20] wird die Anzahl der Grundsatzkontrollen erheblich erhöht werden müssen, um auch nur annähernd eine dem Thema angemessene Kontrollfrequenz bei den einzelnen Unternehmen erreichen zu können. Diese sind bisher schon nicht annäherungsweise möglich.

Neben der massiv auszuweitenden Kontrolltätigkeit ist auch ein Anstieg des zu erwartenden Beratungsbedarfs seitens der TK-Anbieter zu berücksichtigen, der auch schon im Nachgang der Vorratsdatenspeicherung im Jahre 2007 festzustellen war.

Nicht zuletzt sieht auch der Gesetzentwurf selbst neue Aufgaben für mich vor. So werde ich maßgeblich an der Erstellung und kontinuierlichen Pflege des Anforderungskatalogs nach § 113f TKG-E mitwirken (siehe III.4 unten).

---

[19] Regierungsentwurf, S. 4.
[20] a.a.O., S. 3.

Im Ergebnis führt dieser Mehraufwand bei mir nach ersten Schätzungen zu einem zusätzlichen Bedarf von mindestens acht Planstellen/ Stellen mit jährlichen Personalkosten in Höhe von insgesamt ca. 750 000 Euro zuzüglich der entsprechenden Sachmittelpauschale.

II. Änderung der Strafprozessordnung (Artikel 1)

1. zu Nummer 2 (§ 100g StPO)

§ 100g StPO regelt, in welchen Fällen die Strafverfolgungsbehörden auf **Telekommunikationsverkehrsdaten** zugreifen können. Das Gesetz trennt dabei zwischen Verkehrsdaten, die aus betrieblichen Gründen anfallen, und solchen, die aufgrund der Vorratsdatenspeicherung vorhanden sind.

Darüber hinaus enthält der Entwurf in § 100g Absatz 3 StPO-E erstmals eine ausdrücklich dafür benannte Rechtsgrundlage für **Funkzellenabfragen**.

Der Schutz von Berufsgeheimnisträgern ist von § 160a StPO abweichend in **Absatz 4** geregelt.

a) Funkzellenabfragen (§100g Absatz 3 StPO-E)

Die neue Regelung der Funkzellenabfragen enthält nicht die datenschutzrechtlich notwendigen Einschränkungen. Bislang ist die Funkzellenabfrage nur „am Rande“ von § 100g Absatz 2 Satz 2 StPO erfasst. Dabei handelt sich um eine *„erst im Rechtsausschuss eingefügte und deshalb unsystematisch in § 100h Abs. 1 a.F. im Zusammenhang mit der Regelung von Formalien in das Gesetz eingerückte Regelung“*[21]. Mit dem neuen § 100g Absatz 3 StPO-E wird sie erstmals ausdrücklich und eigenständig auf der materiellen Ebene geregelt.

Notwendig ist eine Neuregelung wegen der besonderen **Eingriffsintensität der Maßnahme**. Sie war nach Funkzellenabfragen bei Demonstrationen in Dresden verschiedentlich gefordert worden.[22]

---

[21] Hauck in: Löwe-Rosenberg, StPO, 26. Auflage 2014, § 100g Rn. 43

[22] vgl. dazu Prüfbericht des Sächsischen Datenschutzbeauftragten vom 8.9.2011; SLT-Drs. 5/6787, abrufbar unter: https://www.saechsdsb.de/oeffentlichkeitsarbeit/420-medieninformation-zur-funkzellenabfrage-mit-downloads (zuletzt aufgerufen am 29.05.2015).

Das BVerfG fordert für eingriffsintensive Maßnahmen eine normenklare und verhältnismäßige Regelung. Je größer der Grundrechtseingriff, desto genauer muss der Gesetzgeber die Voraussetzungen und Eingriffsschwellen regeln. Die Funkzellenabfrage ist eine solche schwerwiegende Maßnahme.

Die Funkzellenabfragen erfassen eine Vielzahl von Betroffenen. Konkret wird nicht nur durch die Vorratsdatenspeicherung eine Vielzahl von Personen gespeichert, die dafür keinen konkreten Anlass gegeben haben. Mit der Funkzellenabfrage greifen die Ermittlungsbehörden nun auch auf diese Daten einer Vielzahl von Personen zu. Damit erfassen sie alle Menschen, die sich mit ihrem aktiven Mobiltelefon in einem bestimmten Zeitraum in einer bestimmten Funkzelle aufgehalten haben. Je nach Funkzelle(n) und Zeitraum kann dies tausende oder hunderttausende Menschen betreffen. In das Visier konkreter Ermittlungen kommt dann derjenige, der bei einem „Kreuz- oder Mehrfachtrefferabgleich“ auffällig wird.[23]

Eingesetzt wurden Funkzellenabfragen nicht nur in Fällen wie etwa bei dem bekannten Fall des Autobahnschützen, dem ein versuchtes Tötungsdelikt vorgeworfen wurde[24]. Ebenso wurde in höchst umstrittener Weise versucht, mit Funkzellenabfragen Gewalttätigkeiten bei Demonstrationen zu verfolgen[25]. Bei solchen Aktionen erfasst die Polizei aber nicht nur Gewalttäter, sondern z. B. auch den Gemeindepfarrer oder die Abgeordnete des Landtags.

Problem ist stets, den wirklichen Täter herauszufiltern. Es liegt in der Natur der Sache, dass die Maßnahme nicht nur die Gewalttäter erfasst, sondern auch viele weitere Personen, die an der Demonstration teilgenommen haben. Gerade bei einem Tatbestand wie dem Landfriedensbruch ist es durchaus kompliziert, konkrete Täter der Tathandlung zuzuordnen. Als Tathandlung setzt die Vorschrift ein „Sich-Beteiligen“ an Gewalttätigkeiten „als Täter oder Teilnehmer“ (§ 25 ff. StGB) voraus. Anders als in der vorhergehenden Gesetzesfassung genügt die bloße Zugehörigkeit zu der unfriedlichen Menschenmenge nicht, weshalb sich die Strafbarkeit auf solche Mitglieder beschränkt, die sich nachweisbar an bestimmten Gewalttätigkeiten beteiligen.[26] Der Landfriedensbruch ist im Katalog des § 100g Absatz 2 Satz 2 Nr. 1 Buchstabe b StPO-E enthalten, wenn

[23] Vgl. dazu Drucksache 17/14794.
[24] a.a.O.
[25] vgl. dazu Prüfbericht des Sächsischen Datenschutzbeauftragten vom 8.9.2011; SLT-Drs. 5/6787, abrufbar unter: https://www.saechsdsb.de/oeffentlichkeitsarbeit/420-medieninformation-zur-funkzellenabfrage-mit-downloads (zuletzt aufgerufen am 29.05.2015).
[26] BVerfG, NJW 1991, S. 91 (94 f.); Schönke/Schröder, StGB, Auflage 2010, § 125 Rn. 12.

dies einen besonders schweren Fall betrifft (§ 125a StGB). Dieser setzt etwa voraus, dass der Täter ein gefährliches Werkzeug bei sich geführt hat und verwenden wollte oder bedeutenden Schaden an fremden Sachen angerichtet hat. Um zu unterscheiden, welcher Teilnehmer eine Waffe dabei hatte oder Schaden angerichtet hat und welcher nicht, ist aber die nichtindividualisierte Funkzellenabfrage völlig ungeeignet. Ebenso erfasst die Maßnahme zunächst auch alle friedlichen Demonstrationsteilnehmer. Die Maßnahme kann nur dazu verwendet werden, mit einer Kreuz- oder Mehrfachtrefferabfrage solche Personen herauszufiltern, die bei mehreren Demonstrationen vor Ort waren, bei denen es zu Ausschreitungen kam. Dass jemand mehrfach bei solchen Anlässen vor Ort war, muss aber nicht an seiner kriminellen Energie liegen. Es kann sein, dass der Betroffene nur an einem bestimmten Thema interessiert ist und deshalb häufiger erfasst wird (z.B. Gegenkundgebungen gegen Neonazis), gleichwohl selbst aber nie an Ausschreitungen beteiligt war. Konkret nahmen etwa an den Demonstrationen in Dresden auch Abgeordnete des Bundestages, mehrerer Landtage und Mitglieder evangelischer Kirchengemeinden teil[27].

Noch größer wird das Risiko, als Unbeteiligter dauerhaft erfasst zu werden, wenn die Polizeibehörden sogenannte Strukturermittlungen durchführen. Dabei geht es darum, Tätergruppen, Organisationen, Banden o.ä. und deren Entwicklung über einen Zeitraum zu beobachten[28]. Dazu gehört dann die Frage, welche Personen möglicherweise dazugehören und welche nicht. Zu diesem Zweck wurden in der Vergangenheit Daten aus Funkzellenabfragen ohne die notwendige Reduktion gespeichert[29]. In solchen Fällen wird aus der Vorratsdatenspeicherung dann gewissermaßen eine **„doppelte Vorratsdatenspeicherung“**. Gegen eine solche Praxis sieht der Entwurf keine ausreichenden Sperren vor. Strukturermittlungen sind in allen Bereichen denkbar, in denen es um Tätergruppierungen geht, und daher besonders in den im Katalog des § 100g Absatz 2 Satz 2 StPO-E genannten Fällen.

Die genannten Funkzellenabfragen in Sachsen hatten erhebliches Echo in den Medien. Der Sächsische Datenschutzbeauftragte ist in einem 53-seitigen Bericht zu dem Ergebnis gekommen, dass die Maßnahmen rechtswidrig waren. Dies ist ein Beispiel dafür, dass einige wenige Störer bereits einen Anlass für die Nutzung der Vorratsdaten einer Vielzahl von Personen geben können. Hier haben diese zudem ein besonders sensibles Grundrecht in Anspruch genom-

[27] Bericht des Sächsischen Datenschutzbeauftragten a.a.O., S. 40.
[28] Vgl. Bericht a.a.O. S. 44 ff.
[29] Vgl. a.a.O.

men. Meine datenschutzrechtliche Kontrollen in der Vergangenheit haben gezeigt, dass auch bei Sicherheitsbehörden des Bundes durchaus solche Demonstranten in Dateien gespeichert waren, bei denen die Zurechnung zu Gewalttaten sehr zweifelhaft oder nicht gegeben war. Hinzu kommt die Praxis, einzelne erfasste Personen zumindest befristet als „Prüffall“ zu speichern.

Diese bestehenden Probleme der Funkzellenabfrage geht der Gesetzeswurf nicht an. Er verharrt vielmehr in dem bisherigen Rechtszustand und erweitert diesen durch die Nutzung von Vorratsdaten.

Durch den Verweis auf Absatz 1 Nummer 1 ist die Eingriffsschwelle für die Maßnahme – ohne Unterschied zur bisherigen Regelung – weiterhin die „Straftat von erheblicher Bedeutung“. Der Verweis in der Nummer 1 auf Absatz 2 ist lediglich deklaratorisch und nicht abschließend. Der Kreis der Straftaten von erheblicher Bedeutung ist erheblich weiter als die in Absatz 2 genannten Straftaten. An der oftmals kritisierten Praxis der Funkzellenabfragen wird sich also künftig nichts ändern, außer dass künftig auch Vorratsdaten zur Verfügung stehen. Nur für diese Fälle greifen die Grenzen des § 100g Absatz 2 StPO-E.

Schließlich ist auch die verwendete **Verweistechnik nicht hinreichend normenklar und bestimmt**. So verweist der Absatz 3 auf „die Voraussetzungen des Absatzes 1 Satz 1 Nummer 1“. Nicht klar ist aber, ob auch die weiteren Voraussetzungen des Absatzes 1 gelten sollen. So bleibt auch unklar, ob Standortdaten auch für die Vergangenheit erhoben werden können.

Im Regierungsentwurf wurde im Vergleich zur Fassung des Referentenentwurfs eine allgemeine Abwägungsregel in den Wortlaut eingefügt, wonach „die Erhebung der Daten in einem angemessenen Verhältnis zur Bedeutung der Sache“ stehen muss (§ 100g Absatz 3 Satz 1 Nummer 2 StPO-E). Dabei handelt es sich aber um eine sehr allgemein formulierte Anforderung zur Verhältnismäßigkeit. Diese wird in der Praxis keine nennenswerten Auswirkungen haben.

Auch wenn es grundsätzlich richtig und notwendig ist, die Funkzellenabfrage eigenständig und gründlich im Gesetz neu zu regeln, muss der konkrete Vorschlag im Ergebnis abgelehnt werden. Er hebt die Schwellen für die Datenerhebung nicht nennenswert an und wirft dazu noch weitere datenschutzrechtliche Probleme auf.

b) Schutz von Zeugnisverweigerungsberechtigten (nur bezogen auf § 100g StPO-E)

Die Vorschrift des § 100g Absatz 4 StPO-E ist angelehnt an die allgemeine Regelung zum Schutz von Berufsgeheimnisträgern in § 160a StPO, weist aber Abweichungen auf.

Die Regelung in § 100g Absatz 4 StPO-E ist ein durchaus zweischneidiges Schwert. Auf der einen Seite enthält sie im Hinblick auf den Datenschutz für Berufsgeheimnisträger im Vergleich zum bestehenden § 160a StPO Vorteile. Über den Schutz des § 160a StPO geht sie insofern hinaus, als sie alle nach § 53 Absatz 1 Satz 1 Nummer 1 - 5 StPO erfassten Personen gleichermaßen schützt. § 160a StPO differenziert hingegen zwischen den einzelnen Gruppen der Berufsgeheimnisträger.

Auf der anderen Seite stellt sich die Frage, ob die Vorschrift in der Praxis die erhoffte Wirkung zeigen wird. Der Zugriff auf die Vorratsdaten ist nur gesperrt, soweit sich die Maßnahme unmittelbar gegen den Zeugnisverweigerungsberechtigten richtet. Wird er als nicht Betroffener miterfasst, unterliegen Erkenntnisse lediglich einem Verwertungsverbot.

Regelmäßig wird sich dabei die Problematik stellen, die Kommunikation von und mit Berufsgeheimnisträgern richtig und rechtzeitig als solche zu identifizieren. Das wird etwa dann schwierig sein, wenn der Betroffene sich selbst nicht ausdrücklich zu erkennen gibt. Es ist durchaus wahrscheinlich, dass dies in der Praxis zu erheblichen Schwierigkeiten führen wird. Man denke nur an einen „inkognito“ handelnden Journalisten.

Ist aufgrund einer nicht rechtzeitig erkannten Zuordnung eines erfassten Metadatums die Kommunikation von oder mit einem **Berufsgeheimnisträger** erst einmal in das Verfahren oder in die Akten eingeflossen, bietet die Strafprozessordnung nur wenig Schutz.[30] Dies gilt beispielsweise, wenn ein Metadatum als Anlasstatsache für weitere Ermittlungen gedient hat oder als Verknüpfungsmerkmal in eine polizeiliche Datenbank eingeflossen ist.

Demzufolge kann ein hinreichender Schutz von Berufsgeheimnisträgern nur dann erreicht werden, wenn ihre Telekommunikation erst gar nicht von der Vorratsdatenspeicherung erfasst wird. So kritisiert daher auch der EuGH in seinem

[30] treffend zu diesem Punkt die Stellungnahme des DAV zum vorliegenden Gesetzentwurf (in der Fassung des Referentenentwurfs vom 15.05.2015), Stellungnahme Nr. 25/2015, S. 14.

Urteil die Geltung der Richtlinie und damit die Existenz einer Vorratsspeicherpflicht auch für die Kommunikationsvorgänge von Berufsgeheimnisträgern als einen unverhältnismäßigen Eingriff in die Charta.[31] Konsequenterweise kann daher der im Gesetzentwurf gewählte Ansatz einer Kombination aus Abruf- und Verwertungsverbot keine hinreichende Alternative zum Verzicht der Speicherung der Daten darstellen.

Im Ergebnis ist es daher rechtlich geboten, die Telekommunikation von Berufsgeheimnisträgern bereits auf Ebene der TK-Anbieter von der Speicherung auszunehmen, indem entsprechend der Regelung in § 113b Absatz 6 TKG-E eine Speicherung nicht nur nicht angeordnet, sondern explizit untersagt wird. Die in der Begründung angeführte Argumentation, eine entsprechende Ausnahme von der Speicherung sei technisch nicht möglich und werfe datenschutzrechtliche Bedenken auf,[32] kann in diesem Zusammenhang nicht überzeugen.

Zum einen ist nicht ersichtlich, wieso zumindest für den großen Bereich der Telefonie, die ohnehin aufgrund von § 99 Absatz 2 TKG **datenschutzkonform geführte zentrale Liste** bei der Bundesnetzagentur nicht entsprechend erweitert werden kann. Erst recht kann eine solche Liste nicht unverhältnismäßig sein, wenn und soweit sie Daten enthält, die ohnehin legal veröffentlicht sind.[33] Zum anderen kann – unterstellt man tatsächlich die technische Unmöglichkeit einer Ausnahme – die Konsequenz einer grundrechtswidrigen Maßnahme nicht sein, dass mittels kosmetischer Eingriffe die Grundrechtswidrigkeit zwar etwas „verschleiert“ wird, im Ergebnis aber nach wie vor bestehen bleibt. In einem solchen Fall, in dem die einzigen umsetzbaren „Verbesserungsmöglichkeiten“ letztlich doch nicht dazu führen können, das Problem der Maßnahme zu beseitigen, muss schlichtweg auf die Maßnahme in Gänze verzichtet werden.

2. zu Nummer 3 bis 5 (Verfahrensregelungen)

a) Zweckbindung (§ 101a Absatz 4 StPO-E)

Eine **Regelung zur Zweckbindung** in der StPO war im Referentenentwurf nicht vorhanden. Diese zu begrüßende Einschränkung ist offensichtlich auf meinen Hinweis im letzten Moment nachgepflegt worden.

---

[31] EuGH, NJW 2014, S. 2169 (2172), Absatz Nr. 58.
[32] Begründung des Regierungsentwurfs, S. 37.
[33] Vgl. etwa http://www.brak.de/fuer-verbraucher/anwaltssuche/ (zuletzt aufgerufen am 29.05.2015).

Die im Regierungsentwurf nachgetragene Regelung begrenzt die weitere Verwendung der Daten auf Fälle des § 100g Absatz 2 StPO-E sowie die Abwehr konkreter Gefahren für Leib, Leben oder Freiheit einer Person oder für den Bestand des Bundes oder eines Landes.

Fraglich ist aber, ob der Entwurf die strikte Zweckbindung der gespeicherten Vorratsdaten auch sicherstellt. Eine wirklich effektive Zweckbindungsregelung muss so ausgestaltet sein, dass ihre Einhaltung bestmöglich garantiert wird. Dies geschieht in § 101a Absatz 4 StPO-E mit den Verkehrsdaten, die unter den Voraussetzungen des § 100g Absatz 2 StPO-E erhoben wurden dürfen.

Bürger, deren Daten z.B. bei dem speichernden Unternehmen gestohlen werden, genießen aber diesen Schutz nicht. Deren gestohlenen Daten dürfen gemäß § 202d Absatz 3 StGB-E beispielsweise straffrei von öffentlich-rechtlich Bediensteten aufgekauft und an Staatsanwälte weitergegeben werden. Selbst die vorsätzlich rechtswidrige Verwendung solcher Daten wäre möglich (siehe IV.1 unten).

Es sollte daher darüber nachgedacht werden, die Regelung in § 101a Absatz 4 StPO-E auf die Verwendung illegal erlangter Daten im Sinne des § 202d StGB-E auszudehnen. In Verfahren, die nicht den Katalog der Straftatbestände in § 100g StPO-E betreffen, dürften also diese illegalen Daten wie in Absatz 4 vorgesehen nicht verwendet werden.

Darüber hinaus ist auch auf die durch die Regelung entstehenden Wertungswidersprüche innerhalb der StPO hinzuweisen (dazu V.1.b) unten).

b) Benachrichtigungspflicht (§ 101a Absatz 6 StPO-E)

Das BVerfG hatte vorgegeben, dass der Gesetzgeber den Zugriff auf Verkehrsdaten als grundsätzlich **offene Maßnahme** ausgestalten muss.[34] *„Dementsprechend ist der Betroffene vor der Abfrage beziehungsweise Übermittlung seiner Daten grundsätzlich zu benachrichtigen. Eine heimliche Verwendung der Daten darf nur vorgesehen werden, wenn sie im Einzelfall erforderlich und richterlich angeordnet ist“*.[35]

[34] vgl. BVerfG, NJW 2010, S. 833 (842), Absatz Nr. 243.
[35] a.a.O.

Der Entwurf verzichtet deshalb auf die bisher in § 100g StPO formulierte Wendung „ohne Wissen des Betroffenen“ und spiegelt damit vor, es handele sich um eine offene Maßnahme. Daher soll sie auch nicht mehr dem Katalog der heimlichen Ermittlungsmaßnahmen nach § 101 StPO zugeordnet werden.

Aus diesem Grund anzunehmen, die Betroffenen würden künftig regelmäßig – vor (!) – der Maßnahme benachrichtigt, ist jedoch praxisfremd. Im Wortlaut des § 101a Absatz 4 StPO-E ist nur die Rede davon, dass der Betroffene „von“ der Erhebung zu benachrichtigen ist, nicht **„vor“ der Erhebung**, obwohl diese Formulierung bereits durch den Austausch eines kleinen Buchstabens möglich wäre. Stattdessen wird in der Begründung[36] entsprechend der Entscheidung des BVerfG[37] ausdrücklich auf das Anhörungsrecht nach § 33 StPO verwiesen.

In der Theorie handelt es sich damit zwar um eine in der Regel offene Maßnahme, nur im Ausnahmefall um eine verdeckte. In der Praxis wird die Strafverfolgung mit an Sicherheit grenzender Wahrscheinlichkeit aber anders aussehen und das Regel-Ausnahme-Verhältnis genau andersherum verteilt sein. So liefert die Gesetzesbegründung den Sicherheitsbehörden direkt den Tipp, wie auf eine Benachrichtigung vor Erhebung der Daten verzichtet werden kann: *„Stehen einer Benachrichtigung zu diesem Zeitpunkt Gründe entgegen, ist sie mit Zustimmung des Gerichts zurückzustellen. In einem solchen Fall wird das Gericht regelmäßig ohne vorherige Anhörung des Betroffenen die Anordnung getroffen haben; in der Praxis kann sich daher empfehlen, dass bereits mit dem Antrag auf Anordnung einer Verkehrsdatenerhebung zugleich der Antrag auf Zustimmung zur Zurückstellung der Benachrichtigung unterbreitet wird“*.[38]

Im Ergebnis handelt es sich hier somit lediglich um eine Pro-Forma-Regelung, die den eigentlichen Zweck und die verfassungsrechtliche Vorgabe nicht erfüllen kann, die Maßnahme auch in der praktischen Umsetzung als offen zu gestalten. In der Praxis ist davon auszugehen, dass die Vorratsdatenspeicherung Spurenansätze liefern oder Strukturermittlungen ermöglichen soll. Gerade in diesen Fällen ist aber nicht damit zu rechnen, dass die Ermittlungsbehörden ihre Ermittlungen offen legen möchten.

[36] Begründung des Regierungsentwurfs, S. 41.
[37] vgl. BVerfG, NJW 2010, S. 833 (842) Abs. Nr. 243.
[38] Begründung des Regierungsentwurfs, S. 41.

c) Statistikregelungen (§ 101b StPO-E)

Die Statistikregelungen sind aus datenschutzrechtlicher Sicht notwendig, um die Auswirkungen der Neuregelung nachverfolgen zu können.[39] Ob alle für eine solche Nachbeobachtung erforderlichen Parameter erfasst werden, kann von mir nicht beurteilt werden. Notwendig wäre jedenfalls, solche Parameter zu erfassen, mit denen sich der Erfolg der gesetzlich geregelten Befugnisse messen lässt. Dies wäre empirisch-wissenschaftlich aufzubereiten.

In diesem Zusammenhang ist zudem bemerkenswert, dass der Gesetzentwurf zwar statistische Erhebungen vorsieht, nicht jedoch, diese zwingend für eine Evaluierung zu verwenden. Sollte das Gesetz tatsächlich in Kraft treten, ist eine solche **Evaluierungspflicht** aber zwingend vorzusehen. Dies schon alleine, um als Gesetzgeber der Verpflichtung nachzukommen, die bereits thematisierte Erforderlichkeit der Maßnahme (siehe I.2.b) oben) zu belegen.

3. zu Nummer 6 Buchstabe a (§ 160a StPO)

§ 160a StPO schützt Zeugnisverweigerungsberechtigte vor Ermittlungsmaßnahmen. Dessen Absatz 2 soll insbesondere Journalisten vor unverhältnismäßigen Ermittlungsmaßnahmen schützen. Das gilt nach § 160a Absatz 4 StPO nicht, wenn der Betroffene in eine Straftat verstrickt ist. Diese sogenannte **Verstrickungsklausel** will der Entwurf in Artikel 1 Nummer 5 mit einem Verweis auf die Datenhehlerei erweitern. Verstrickt ist dann auch der Datenhehler. Es ist daher zu befürchten, dass insbesondere **Journalisten, Blogger, Whistleblower etc.,** die auf Missstände hinweisen, indem sie sich auf nicht frei zugängliches Material berufen, in den Fokus strafrechtlicher Ermittlungen geraten.

III. Änderung des Telekommunikationsgesetzes (Artikel 2)

Sämtliche der folgenden Anmerkungen beziehen sich auf Artikel 2 Nummer 2:

[39] Vgl. etwa BVerfG, NJW 2004, S. 999 (1009) m.w.N.

1. Pflichten zur Speicherung von Verkehrsdaten (§ 113b TKG-E)

In dieser Vorschrift werden vor allem die zu speichernden Datenkategorien sowie deren Speicherfristen benannt. Sie entspricht damit weitestgehend der Regelung des § 113a TKG a.F. und betrifft so den Kern der Vorratsdatenspeicherung.

Absatz 1 legt fest, dass die Verkehrsdaten mit Ausnahme der Standortdaten, für die eine Speicherfrist von vier Wochen gilt, für zehn Wochen gespeichert werden müssen. Darüber hinaus wird die aus Datenschutzsicht zu begrüßende verpflichtende Speicherung der Daten im Inland vorgeschrieben.

Die Absätze 2, 3 und 4 benennen die konkret zu speichernden **Datenkategorien,** die weitestgehend denen des § 113a TKG a.F. entsprechen. Eine Ausnahme besteht lediglich in dem kompletten Verzicht auf die Speicherung von E-Mail-Daten sowie der Ausgliederung der Speicherung von Standortdaten in einen eigenen Absatz.

Die Absätze 5-8 regeln das Verbot der Speicherung von Inhalten und Daten der auf der Liste der Bundesnetzagentur geführten Stellen, für die eine Möglichkeit zur anonymen Kontaktaufnahme vorgesehen ist (z.B. Seelsorge, etc.), sowie die Verpflichtung zur Speicherung der Daten in einer Art und Weise, die eine unverzügliche Auskunft ermöglicht, und Vorschriften zur Löschung der auf Vorrat gespeicherten Daten. Letztere hat unverzüglich, spätestens jedoch innerhalb von einer Woche nach Ablauf der in Absatz 1 vorgesehenen Speicherfristen zu erfolgen.

a) Internet-Telefondienste (§ 113b Absatz 2 Satz 1 Nummer 5 TKG-E)

Datenschutzrechtlich problematisch ist der Umstand, dass die TK-Branche gegenwärtig die von ihr angebotenen Telefonanschlüsse großflächig auf IP-basierte Angebote umstellt. Schon in naher Zukunft dürften daher „klassische Anschlüsse“ eine Ausnahme darstellen oder sogar gänzlich verschwinden. Dementsprechend wird aufgrund der Verpflichtung, bei der VoIP-Telefonie auch die IP-Adresse zu speichern, die Anzahl der insgesamt vorgehaltenen IP-Adressen weiter in die Höhe geschraubt. Die in der Konsequenz entstehenden Möglichkeiten einer immer umfangreicheren **Überwachbarkeit der Internetnutzung** aufgrund der weitreichenden Zuordnungsmöglichkeiten von IP-Adressen wurde bereits hinreichend dargelegt (siehe I.2.c)(1) oben).

b) „ähnliche Nachrichten“ (§ 113b Absatz 2 Satz 2 Nummer 1 TKG-E)

Ein weiterer zu kritisierender Punkt ergibt sich aus der unpräzisen Formulierung bei einzelnen zu speichernden Daten, zum Beispiel bei der Verpflichtung, neben Kurz- und Multimedianachrichten auch weitere „ähnliche Nachrichten“ zu speichern. Hier besteht keine hinreichende Klarheit, was unter dieser Formulierung zu verstehen ist. Die Begründung nennt zwar mit EMS ein Beispiel, es stellt sich jedoch die Frage, ob auch internetbasierte Messengerdienste wie Joyn unter „ähnliche Nachrichten“ zu fassen sind.

Sollte letzteres bejaht werden, stellt sich die Frage, ob auch entsprechende Angebote wie **WhatsApp oder Threema** der Speicherpflicht unterliegen. Dies dürfte allerdings aufgrund der Unklarheit über deren Status als TK-Anbieter fraglich sein. Selbst bei einer Unterstellung der TK-Anbietereigenschaft würde die Auskunftserteilung praktisch wohl an der Vollstreckbarkeit der Anordnung scheitern, da die oben beispielhaft genannten Unternehmen nicht nur über keinen Sitz in Deutschland verfügen, sondern auch ihre Server in Drittstaaten stehen.

Im Ergebnis wird hier wiederum ein riesiger Kommunikationsbereich aus dem Anwendungsbereich des Gesetzes ausgeklammert, so dass das Vorliegen der Geeignetheit der verbliebenen Maßnahmen zur Erreichung des beabsichtigten Zwecks kaum mehr als gegeben betrachtet werden kann (siehe auch I.2.a) oben).

c) Standortdaten (§ 113b Absatz 4 TKG-E)

Die Vorgabe, bei der Speicherverpflichtung zu Standortdaten auch die bei Beginn einer mobilen Internetverbindung genutzte Funkzelle zu erfassen, wird zu einer sehr umfangreichen Speicherung führen. In Deutschland nutzen über 45 Millionen Menschen ein Smartphone und somit mobile Internetverbindungen. Grundsätzlich sind Smartphones im eingeschalteten Zustand immer online, so dass eine Unterbrechung der Verbindung lediglich bei einem Netzverlust oder dem bewussten Ausschalten des Smartphones erfolgen würde.

Tatsächlich gibt es aber viele weitere Gründe, wieso eine mobile Internetverbindung gekappt und wieder neu aufgebaut werden kann. So kann beispielsweise der Wechsel von einer schnellen LTE-Verbindung zu einer langsameren UMTS-Verbindung oder die Verbindung mit einem WLAN-Netz einen Neuaufbau der Datenverbindung erforderlich machen, da diese auf unterschiedlichen

Technologien basieren. Gerade diese Wechsel finden in der Praxis sehr häufig statt, insbesondere wenn sich der Nutzer des Smartphones bewegt und somit unterschiedliche Funkzellen mit unterschiedlichem Technikstand und einer unterschiedlichen Auslastung durch andere Teilnehmer durchquert.

Letztendlich hängt hier sehr viel von den Systemkonfigurationen und Verfahren der einzelnen TK-Anbieter ab. Im Rahmen einer Kontrolle zur Umsetzung der Vorratsdatenspeicherung aus dem Jahre 2007 hatte ich festgestellt, dass beispielsweise ein großer Provider seine Systeme dahingehend konfiguriert hatte, dass alle 15 Minuten eine automatische Neuverbindung stattfand, bei der jeweils die aktuelle Funkzelle gespeichert wurde. In einem solchen Fall würden – jedenfalls für jeweils vier Wochen – Daten erzeugt, die die Erstellung **engmaschiger Bewegungsprofile** ermöglichen.

Gerade in Verbindung mit den äußerst unkonkreten Vorgaben, die an die Erhebung der Vorratsdaten gestellt werden, besteht hier das Potential, die Voraussetzung für eine Profilbildung zu schaffen, die ausweislich der Ausführungen in den Leitlinien vom 15.04.2015 eigentlich gerade vermieden werden soll.[40] Die dort groß angekündigte Beschränkung des Abrufs von Standortdaten findet sich im Gesetzentwurf lediglich an einer einzigen Stelle, versteckt in der Gesetzesbegründung, wieder, wo es heißt: *„Grundsätzlich sollen nur einzelne Standortdaten abgerufen werden, um keine überflüssigen Bewegungsprofile zu erstellen.“*[41] Dies wird freilich direkt im nächsten Satz dahingehend relativiert, dass der zuvor dargelegte Grundsatz nicht gelten soll, wenn die Standortdaten *„im Einzelfall notwendig sind, zum Beispiel, um eine Serientat aufzuklären oder um Anhaltspunkte für vom Beschuldigten angegebene Bewegungen zu gewinnen.“*[42]

Da die Vorratsdatenspeicherung aber insbesondere dazu dienen soll, Ermittlungsansätze um Umfeld einer begangenen oder drohenden schweren Straftat zu liefern, ist es eher wahrscheinlich, dass die oben genannten Ausnahmen vom Grundsatz in der praktischen Anwendung tatsächlich die Regel darstellen werden.

---

[40] Leitlinien des BMJV zur Einführung einer Speicherpflicht und Höchstspeicherfrist für Verkehrsdaten, S. 2 f.
[41] Begründung des Regierungsentwurfs, S 39.
[42] a.a.O.

2. Verwendung der Daten (§ 113c TKG-E)

Die Vorschrift regelt die Verwendung der Daten durch die TK-Anbieter und setzt diesen eine **enge Zweckbegrenzung**. So dürfen die Daten nur aufgrund einer expliziten Anfrage zur Übermittlung an eine Strafverfolgungsbehörde (Absatz 1 Nr. 1) oder eine Gefahrenabwehrbehörde der Länder (Absatz 1 Nr. 2) übermittelt werden, sofern diese sich auf eine gesetzliche Vorschrift berufen können, die sie zur Erhebung von nach § 113b TKG-E gespeicherten Daten ermächtigt. Zu begrüßen ist die in Absatz 3 eingeführte **Kennzeichnungspflicht**, die auch nach der Übermittlung der Daten an eine andere Stelle aufrecht zu erhalten ist.

a) fehlender Prüfungsmaßstab (§ 113c Absatz 1 Nummer 1 und 2 TKG-E)

Die Formulierung der Übermittlungsermächtigung wird zu Anwendungsproblemen in der Praxis führen. So wird den TK-Anbietern vorliegend **kein Prüfungsmaßstab** an die Hand gegeben, anhand dessen sie verifizieren können, ob eine Übermittlung tatsächlich zulässig ist.

Sicherlich wird sich eine solche Prüfung ausschließlich auf das Vorliegen formeller Voraussetzungen (z.B. das Vorliegen eines richterlichen Beschlusses) beschränken müssen; dafür spricht auch, dass in der Gesetzesbegründung ausdrücklich eine materielle Prüfpflicht ausgeschlossen wird.[43] Diese muss aber zwingend erfolgen, da den TK-Anbietern bei einer zweckwidrigen Verwendung der Daten nach § 149 Absatz 2 Satz 1 Nr. 1 TKG-E ein Bußgeld in Höhe von bis zu 500.000 Euro droht. Vor diesem Hintergrund kann von ihnen auch nicht verlangt werden, selbstständig die an die Sicherheitsbehörden gerichteten Anforderung der StPO an eine Datenerhebung mühsam zu ermitteln, zumal diese ohnehin oftmals sehr unzureichend dargestellt und teilweise sogar nur in der Gesetzesbegründung versteckt sind.

Bereits bei der zwischen den Jahren 2008 und 2010 gültigen Vorratsdatenspeicherung haben sich viele TK-Anbieter bei mir beschwert, die Auskunftserteilung auf Anträge, deren formelle Rechtmäßigkeit nicht eindeutig sei, stelle für die konkret mit der Auskunftserteilung befassten Mitarbeiter ein erhebliches Risiko dar. In diesem Zusammenhang äußerte sich der zuständige Leiter der Lawful-Interception-Abteilung eines großen TK-Anbieters wie folgt: *„In diesen Fällen stehe ich mit zwei Beinen im Gefängnis. Mit dem einen, wenn ich wegen einer zu Unrecht erteilten Auskunft gegen § 206 StGB verstoße und mit dem anderen*

[43] Begründung des Regierungsentwurfs, S 47.

in dem Fall, wo ich die Auskunft nicht erteile und deshalb wegen Strafvereitlung angegangen werde."[44]

Dementsprechend müsste den TK-Anbietern – wenigstens in der Gesetzesbegründung – ein entsprechender formeller Prüfmaßstab an die Hand gegeben werden. Durch diese **zusätzliche „Kontrollinstanz"** würden zudem die Sicherheitsbehörden angehalten, bei der Abfrage der Daten die Formvorschriften ernst zu nehmen und entsprechend zu beachten.

b) fehlende zeitliche Beschränkung (§ 113c Absatz 1 Nummer 1 und 2 TKG-E)

Neben den zu ergänzenden Erläuterungen zum Prüfungsmaßstab muss in Absatz 1 zwingend im Wortlaut der Vorschrift klargestellt werden, dass die nach § 113b TKG-E gespeicherten Daten lediglich im Zeitraum des § 113b Absatz 1 TKG-E übermittelt werden dürfen. Aufgrund der Löschvorschrift in § 113b Absatz 8 TKG-E können Vorratsdaten auch nach dem Ablauf der Speicherfrist noch bis zu einer Woche vorhanden sein. Würden die Daten auch in diesem Zeitraum beauskunftet, würde dies eine **unrechtmäßige Ausweitung der Speicherdauer** bedeuten.

c) Nutzung der IP-Adressen i.R.d. § 113 TKG (§ 113c Absatz 1 Nummer 3 TKG-E)

Kritisch zu sehen ist auch die in Absatz 1 Nummer 3 erteilte Ermächtigung, die im Rahmen der Vorratsdatenspeicherung vorgehaltenen IP-Adressen als Grundlage für eine Bestandsdatenauskunft nach § 113 TKG zu verwenden. Dies begründet sich vor allem damit, dass eine entsprechende Auskunft auch ohne Richtervorbehalt erteilt werden muss. Zwar hat das BVerfG in seiner Entscheidung zur Vorratsdatenspeicherung klar festgestellt, dass dieser grundsätzlich entbehrlich ist.[45] Dabei ist das Gericht aber auch von dem Grundsatz ausgegangen, dass sich *„systematische Ausforschungen über einen längeren Zeitraum oder die Erstellung von Persönlichkeits- und Bewegungsprofilen […] allein auf Grundlage solcher Auskünfte nicht verwirklichen [lassen]"*.[46]

---

[44] Gerade das In-Aussicht-stellen einer Verfahrenseinleitung wegen Strafvereitlung sowie die Ankündigung, Vorstandsmitglieder zu einer Zeugenvernehmung vorzuladen, war eine von mehreren TK-Anbietern gerügte Reaktion der Strafverfolgungsbehörden auf kritische Rückfragen zu formfehlerhaften Auskunftsersuchen.

[45] BVerfG, NJW 2010, S. 833 (845), Absatz Nr. 261.

[46] BVerfG, a.a.O., Absatz Nr. 256.

Gerade aufgrund der bereits im Rahmen der Erwägungen zur Verhältnismäßigkeit dargelegten umfangreichen Möglichkeiten der Überwachung des Internetnutzungsverhaltens (siehe I.2.c)(1) oben), die zwar nicht alleine aufgrund der Bestandsdatenauskunft bestehen, zu denen diese aber einen wesentlichen Teil beiträgt, haben sich die Voraussetzungen, unter denen das BVerfG seinerzeit seine Entscheidung getroffen hat, mittlerweile grundlegend verändert. Dementsprechend müsste zumindest ein **Richtervorbehalt auch für Bestandsdatenauskünfte** nach § 113 Absatz 1 Satz 3 TKG eingeführt werden.

Ein weiteres Problem, das sich aus der Verweisung ergibt, ist die Tatsache, dass hierdurch auch die nach § 113 Absatz 3 Nummer 3 TKG als Datenempfänger ermächtigten Nachrichtendienste zumindest mittelbar die in der Vorratsdatenspeicherung erfassten IP-Adressen nutzen können. Gerade im Zusammenspiel mit den weitgehenden Abfragebefugnissen zu IP-Adressen als Nutzungsdaten wird hier eine umfangreiche Identifizierung der Adressinhaber mittels der Vorratsdaten ermöglicht (siehe I.2.c)(1) oben).

Konsequenterweise sollte Absatz 1 Nummer 3 daher ersatzlos gestrichen werden und eine Auskunft nach § 113 TKG auf die betrieblich gespeicherten Daten beschränkt werden.

3. Protokollierung (§ 113e TKG-E)

Die Vorschrift orientiert sich an den Vorgaben des BVerfG[47] und schreibt die Protokollierung jeglichen Zugriffs auf die Vorratsdaten zu Zwecken der Datenschutzkontrolle vor. Während dies grundsätzlich zu begrüßen ist, muss dennoch die **fehlende Normenklarheit** kritisiert werden, da die Regelung offen lässt, in welchen Bezug die zu protokollierenden Daten gesetzt werden müssen.

So werden in der Auflistung des Absatz 1, die ihrer Form nach als abschließend zu verstehen ist, nicht die Abfragen selbst erfasst, etwa Rufnummer und Zeitraum, die es ermöglichen, nachträglich die Zuordnung der Zugriffe zu einem Betroffenen zu ermöglichen. Dieses Manko kann auch nicht mit Verweis auf künftige Detailregelungen in dem nach § 113f TKG-E zu erstellenden Anforderungskatalog (siehe 4 unten) beseitigt werden.

[47] BVerfG, a.a.O., S. 833 (848), Absatz Nr. 275.

4. Anforderungskatalog (§ 113f TKG-E)

Nach dieser Vorschrift hat die Bundesnetzagentur unter Beteiligung des BSI und der BfDI einen Anforderungskatalog zu erstellen, in dem Details zu den Vorgaben und Verpflichtungen der §§ 113b - 113e TKG-E festzulegen sind. Meine Beteiligung begrüße ich zwar grundsätzlich, müsste aber **in Form des formellen Benehmens** ausgestaltet sein.

Gerade die Auswirkungen der im Katalog zu regelnden Vorgaben auf den Datenschutz gebieten mein gleichrangiges Mitspracherecht. Ebenso verfüge ich aufgrund langjähriger und umfangreicher Kontrollen bei den TK-Anbietern über weitreichendere praktische Erfahrungen und Detailkenntnisse zu den Systemen der TK-Anbieter als die Bundesnetzagentur. Schließlich ist zu erwarten, dass mit meiner anstehenden Unabhängigkeit auch ein entsprechender ordnungsrechtlicher Kompetenzzuwachs einhergeht, der auch die im Rahmen des Anforderungskatalogs zu regelnden Vorgaben betrifft. Insofern ist mir auch schon bei der Erstellung und Pflege dieser Vorgaben ein echtes Mitspracherecht einzuräumen.

IV. Änderung des Strafgesetzbuches (Artikel 5)

Sämtliche der folgenden Anmerkungen beziehen sich auf Artikel 5 Nummer 2:

1. Datenhehlerei (§ 202d StGB-E)

Der Straftatbestand der Datenhehlerei soll unter anderem dazu dienen, personenbezogene Daten besser zu schützen. Dies ist grundsätzlich zu begrüßen.

Die im Gesetzentwurf dargelegte „Strafbarkeitslücke“ besteht in Anbetracht der Regelungen des § 43 Absatz 2 Nummer 1 und 3 i.V.m. § 44 BDSG allerdings nicht, zumindest aus datenschutzrechtlicher Sicht bezogen auf personenbezogene Daten.

Nach § 44 Absatz 1 i.V.m. § 43 Absatz 2 Nummer 1 und 3 BDSG wird auf Antrag mit Geldstrafe oder Freiheitsstrafe bis zu zwei Jahren bestraft, wer mit Bereicherungs- oder Schädigungsabsicht „unbefugt personenbezogene Daten, die nicht allgemein zugänglich sind, erhebt, verarbeitet, abruft oder sich oder einem anderen aus automatisierten oder nicht automatisierten Dateien verschafft“.

Weder die Ausgestaltung des Straftatbestands der Datenhehlerei als relatives Straf-antragsdelikt (Verfolgung von Amts wegen bei besonderem öffentlichen Interesse an der Strafverfolgung, sonst nur auf Antrag) noch der im Vergleich zu § 44 BDSG um ein Jahr erhöhte Strafrahmen (bis zu drei Jahre) dürfte eine erhebliche Verbesserung des strafrechtlichen Schutzes mit sich bringen. Wie bei § 44 BDSG ist auch bei der hier vorgelegten Regelung (anders als bei der Sachhehlerei) der Versuch nicht strafbar, so dass auch hiervon keine wesentliche Ausweitung der Strafbarkeit ausgeht. § 44 BDSG setzt zudem – im Gegensatz zur Datenhehlerei – keine rechtswidrige Vortat voraus.

Aus datenschutzrechtlicher Sicht ist der – in der Strafjustiz allerdings eher unbekannte – § 44 BDSG durchaus umfassend.

Die Datenhehlerei geht allerdings weiter, weil sie nicht nur personenbezogene Daten, sondern sämtliche Daten i.S.d. § 202a Abs. 2 StGB erfasst. Dabei handelt es sich um alle Informationen, die „elektronisch, magnetisch oder sonst nicht unmittelbar wahrnehmbar gespeichert sind oder übermittelt werden“, allerdings unabhängig vom Personenbezug. Andererseits schützt § 44 BDSG nicht nur „digitale“ Informationen, sondern sämtliche personenbezogenen Daten, unabhängig von ihrer Speicherform (also auch Daten auf Papier).

Der Schaffung eines neuen § 202 d StGB-E, insbesondere dessen Absatz 1, bedarf es aus Sicht des Schutzes personenbezogener Daten daher nicht.

Aus datenschutzrechtlicher Sicht hingegen problematisch ist Absatz 3 Nummer 1. Diese Vorschrift stellt Amtsträger in bestimmten Fällen straffrei. So soll der Kauf von – mit welchen rechtswidrigen Mitteln auch immer verschafften – Daten erlaubt sein. Nach dieser Vorschrift sollen solche Handlungen von Amtsträgern oder deren Beauftragten von der Strafvorschrift ausgenommen bleiben, mit denen Daten ausschließlich der Verwertung in einem Besteuerungsverfahren, einem Strafverfahren oder einem Ordnungswidrigkeitenverfahren zugeführt werden.

Damit stellt der Entwurf zugleich *allgemein* klar, dass es sich um eine *rechtmäßige Amtshandlung* (§ 202d Absatz 3 Satz 1 StGB-E) handeln kann, wenn ein Beamter *rechtswidrig* erlangte Daten aus einer rechtswidrigen Vortat in ein Besteuerungs-, Straf- oder Ordnungswidrigkeitenverfahren einführt (§ 202d Absatz

3 Satz 2 Nummer 1 StGB-E). Es steht zu befürchten, dass die geplante Regelung zur illegalen Beschaffung auch personenbezogener Daten nahezu aufruft.

Die in Absatz 3 Nummer 2 geregelte Ausnahme für Berufsgeheimnisträger ist zwar grundsätzlich zu begrüßen, reicht aber im Ergebnis nicht weit genug. So ist nicht hinreichend klargestellt, ob - anders als Berufsjournalisten – insbesondere Gelegenheitsjournalisten, wie etwa Blogger, und Whistleblower auch von der Privilegierung erfasst sein sollen. Gerade letztere sind aber oftmals dafür verantwortlich, dass zum Teil erhebliche Datenschutzverstöße aufgedeckt werden. Insofern ist es nicht im Interesse des Datenschutzes, wenn entsprechende Meldungen in Zukunft aus Angst vor einer eventuellen Strafverfolgung unterbleiben.

V. Sonstiges

1. Wertungswidersprüche

Neben den vorab dargestellten, den geplanten Vorschriften immanenten Auswirkungen, haben diese Regelungen – gerade im Bereich der StPO – einen nicht unerheblichen und vermutlich auch ungewollten Einfluss auf bereits existierende Vorschriften, der mitunter zu **Wertungswidersprüchen in der Gesetzessystematik** führt.

Die in Folge angeführten Beispiele für diese nicht zu vernachlässigende Problematik, die vermutlich auf das bislang überhastet geführte Gesetzgebungsverfahren zurückzuführen ist, müssen nicht zwingend abschließend sein. Gerade aufgrund der hohen Komplexität der vorliegend geregelten Materie sollte daher der Gesetzesentwurf noch einmal ausführlich und mit der gebotenen Zeit und Sorgfalt auf potentielle weitere Wechselwirkungen mit dem geltenden Recht untersucht werden.

a) Subsidiaritätsklausel in § 100g Absatz 1 Satz 2 StPO-E

Nach § 100g Absatz 1 Satz 2 StPO-E ist eine Datenerhebung zur Verfolgung einer „mittels Telekommunikation“ begangenen Straftat nur zulässig, „wenn die Erforschung des Sachverhaltes auf andere Weise aussichtslos wäre.“ Neben dieser enthält die Strafprozessordnung aber auch noch an vielen anderen Stel-

len weitere Subsidiaritätsklauseln, die aber durchaus unterschiedliche Anforderungen an ihr Eingreifen stellen.

So ist etwa die Subsidiaritätsklausel des § 100c Absatz 1 Nummer 4 StPO weniger streng als die hier eingeführte, da dort bereits eine „wesentlich Erschwerung des Erfolgs“ genügt. § 100c StPO betrifft aber die akustische Wohnraumüberwachung („großer Lauschangriff“), die wohl eingriffsintensivste Maßnahme der Strafprozessordnung.

Auch wenn die Strafverfolgungsbehörde eine Person bei einem Spaziergang in einer Grünanlage heimlich mit einem Richtmikrophon abhören möchte, muss sie eine Subsidiaritätsklausel beachten (§ 100f Absatz 2 StPO). Diese ist ebenfalls „milder“ als bei der Verkehrsdatenabfrage im Fall des § 100g Absatz 1 Satz 1 Nummer 2 StPO-E.

Andere Maßnahmen, wie etwa die Wohnungsdurchsuchung, sehen hingegen überhaupt keine Subsidiaritätsklauseln vor.

b) Zweckbindung gemäß § 101a Absatz 4 StPO-E

Die Zweckbindungsregelung in dieser Norm „löst“ lediglich bezogen auf die Vorratsdatenspeicherung das grundsätzliche Problem des Fehlens von Vorgaben zur Zweckbindung in der StPO. Zudem besteht die Gefahr, dass andere verfassungsrechtlich beachtliche Mängel der Strafprozessordnung durch die Regelung möglicherweise sogar verschärft werden, da es auch hier zu **erheblichen Wertungswidersprüchen** kommen kann. Aus der Neuregelung in § 101a Absatz 4 StPO-E kann nämlich der Umkehrschluss gezogen werden, dass entsprechende Restriktionen für andere Maßnahmen gerade nicht gelten sollen.

So sind zwar – zu Recht – die Vorratsdaten von einer allgemeinen Übermittlung an die Nachrichtendienste ausgenommen. Personenbezogene Daten aus anderen ebenso eingriffsintensiven Maßnahmen dürfen jedoch weiterhin nach den recht pauschalen Regelungen der §§ 477 ff. StPO weiterverwendet werden. So können beispielsweise Daten aus Maßnahmen nach § 100a StPO unter den oben dargestellten Voraussetzungen an die Nachrichtendienste übermittelt oder in polizeiliche Datenbanken eingespeist werden. Der bereits im parlamentarischen Verfahren befindliche Entwurf zur Änderung des Bundesverfassungsschutzgesetzes[48] enthält einen Änderungsvorschlag, der die Staatsanwaltschaf-

[48] BR-Drs. 123/15.

ten und Polizeibehörden noch umfangreicher verpflichten wird, personenbezogene Daten an die Nachrichtendienste zu übermitteln.

Dies wird dadurch verstärkt, dass § 477 Absatz 2 Satz 4 StPO ausdrücklich auf §100d Abs. 5, § 100i Abs. 2 Satz 2 und § 108 Abs. 2 und 3 verweist. Dieser wird im vorliegenden Entwurf durch einen Verweis auf § 101a Absatz 4 StPO-E ergänzt. Damit ist klargestellt, dass außerhalb dieser Sonderregelungen Übermittlungen nach den allgemeinen Vorschriften unabhängig von der Schwere des Grundrechtseingriffs und unabhängig von den Restriktionen der Datenerhebungsnorm zulässig sind.

Verfassungsrechtlich beziehen sich die Anforderungen des Art. 10 Absatz 1 GG an eine klare Zweckbindung auch auf die Weitergabe der Daten und Informationen an weitere Stellen, da der Schutz des Grundrechts fortwirkt. Dies schließt zwar Zweckänderungen nicht aus. Diese bedürfen jedoch einer eigenen gesetzlichen Grundlage, die ihrerseits verfassungsrechtlichen Ansprüchen genügt.[49] *„Eine Weitergabe der übermittelten Telekommunikationsverkehrsdaten an andere Stellen darf gesetzlich dementsprechend nur vorgesehen werden, soweit sie zur Wahrnehmung von Aufgaben erfolgt, derentwegen ein Zugriff auf diese Daten auch unmittelbar zulässig wäre […]“*.[50] Diese Aussagen sind ständige Rechtsprechung des BverfG und damit mindestens für Maßnahmen zu verallgemeinern, die in Art. 10, 13 GG eingreifen – eher sogar für alle heimlichen Ermittlungsmaßnahmen.

2. Keine einheitliche Höchstspeicherfrist

Aufgrund aktueller Berichterstattungen, vereinzelter Presseerklärungen und dem irreführenden Titel des vorliegenden Gesetzentwurfes halte ich es für erforderlich, auch an dieser Stelle noch einmal explizit darauf hinzuweisen, **dass der vorliegende Gesetzentwurf nicht zu einer einheitlichen Höchstspeicherfrist für sämtliche Verkehrsdaten führt**.

Die Speichervorgaben sehen lediglich vor, dass ein zusätzlicher Datenpool von Verkehrsdaten geschaffen wird, der ausschließlich zur Auskunftserteilung für Anfragen von Sicherheitsbehörden verwendet wird und auf den sich sämtliche im Gesetzentwurf festgelegten Fristen exklusiv beziehen. Neben diesen Daten

[49] BVerfG, NJW 2010, S. 833 (842), Absatz Nr. 236 m.w.N.
[50] a.a.O.

wird es bei den TK-Anbietern weiterhin nach wie vor die Speicherung und Verarbeitung von Verkehrsdaten zu betrieblichen Zwecken im Sinne der §§ 96 ff. TKG (z.B. zur Abrechnung, Missbrauchserkennung, Störungsbeseitigung, etc.) geben. Ein Großteil dieser Daten wird auch über die in § 113b Absatz 1 TKG-E vorgesehenen Fristen hinaus gespeichert (siehe auch I.2.b) oben).

Eine Übersicht der Speicherfristen für die betriebliche Nutzung von Verkehrsdaten kann dem „Leitfaden der BfDI und der Bundesnetzagentur für eine datenschutzgerechte Speicherung von Verkehrsdaten“ (in **Anlage 3**) entnommen werden.

Mit freundlichen Grüßen

Andrea Voßhoff

Anlagen:
1. Glossar zu den grundlegenden Verkehrsdatenverarbeitungsprozessen
2. Graphik zu den grundlegenden Verkehrsdatenverarbeitungsprozessen
3. Leitfaden zur datenschutzgerechten Speicherung von Verkehrsdaten