Die Bundesbeauftragte
für den Datenschutz und
die Informationsfreiheit

Andrea Voßhoff

Stellungnahme der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit

zu den Verfassungsbeschwerden gegen das Gesetz zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten

Az.: 1 BvR 141/16
Az.: 1 BvR 229/16
Az.: 1 BvR 2023/16
Az.: 1 BvR 2683/16
Az.: 1 BvR 2821/16

Zu den Verfassungsbeschwerdeverfahren

1 BvR 141/16
1 BvR 229/16
1 BvR 2023/16
1 BvR 2683/16
1 BvR 2821/16

nehme ich gemäß § 27a BVerfGG wie folgt Stellung:

Die in den Verfassungsbeschwerdeverfahren angegriffenen Vorschriften des Gesetzes zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten vom 10. Dezember 2015 sind verfassungswidrig und mit den Anforderungen des Europäischen Gerichtshofs an entsprechende Regelungen zur vorsorglichen Datenspeicherung nicht vereinbar.

A) Verfassungswidrigkeit der §§ 113b, 113c TKG

Ausweislich der Gesetzesbegründung dient die Einführung einer gesetzlichen Pflicht zur Speicherung von Verkehrsdaten einer effektiven Strafverfolgung, insbesondere einer möglichst vollständigen Wahrheitsermittlung im Strafverfahren und einer wirksamen Aufklärung gerade schwerer Straftaten (BT-Drs. 18/5088, S. 21).

1) Geeignetheit

Die angegriffenen Vorschriften sind zur Erreichung dieses Zwecks nicht geeignet. Der Gesetzesentwurf begründet die Notwendigkeit der Regelung mit *„der zunehmenden Bedeutung der Telekommunikation für die Vorbereitung und Begehung von Straftaten“* (BT-Drs. 18/5088, S. 21, 22), 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 der angegriffenen Vorschriften für die Vorbereitung und Begehung von Straftaten genutzt werden kann. Ausweislich der Gesetzesbegründung zu § 113a TKG gehören zum Kreis der zur Speicherung Verpflichteten nicht solche Anbieter, die ihren Kunden nur eine kurzzeitige Nutzung eines Telekommunikationsanschlusses zur Verfügung stellen wie zum Beispiel Callshops, Internet-Cafés und öffentlich zugängliche Telefon- oder WLAN-Angebote in Restaurants oder Hotels (BT-Drs. 18/5088, S. 37). Auch E-Mail-Verkehrsdaten sind keine zu speichernden Daten. Die Nutzung dieser

Kommunikationswege ist somit ohne das Hinterlassen von Spuren in den auf Vorrat gespeicherten Daten möglich. Potentielle Straftäter können die für eine Strafverfolgung relevante Korrespondenz auf die von der Vorratsdatenspeicherung gemäß § 113a TKG ausgenommenen Kommunikationswege verlagern. Die von der Vorratsdatenspeicherung erfassten Daten werden daher zu einem noch größeren Prozentsatz solche von unbescholtenen Bürgerinnen und Bürgern sein, die keinen Anlass zu einer strafrechtlichen Verfolgung geben. Eine effektivere Strafverfolgung und Wahrheitsermittlung im Strafverfahren wird durch die Vorratsdatenspeicherung hingegen nicht erreicht. Gerade solche Kriminellen, die sich im organisierten Umfeld bewegen oder Straftaten in professionalisierter Weise begehen, werden die genannten Umgehungsmöglichkeiten kennen und nutzen. Das lässt im Ergebnis erwarten, dass die Vorratsspeicherpflicht eher zur Überführung von Bagatell- und Gelegenheitsstraftätern führen wird.

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 (BVerfG, Urteil vom 02.03.2010, Az.: 1 BvR 256/08, 1 BvR 263/08, 1 BvR 586/08, Rn. 207). Der Entscheidung lag indes keine gesetzliche Regelung zugrunde, in der mit der E-Mail eines der meistgenutzten Telekommunikationsmittel aus der Erfassung ausgeschlossen wurde und damit nicht einmal mehr ein großer Aufwand wie die Beschaffung ausländischer SIM-Karten betrieben werden muss, um einer Speicherung zu entgehen. Im Jahr 2017 wurden in Deutschland rund 800 Milliarden E-Mails (ohne Spamnachrichten) verschickt (https://de.statista.com/statistik/daten/studie/392576/umfrage/anzahl-der-versendeten-e-mails-in-deutschland-pro-jahr/).

Was unter „ähnlichen Nachrichten" im Sinne des § 113b Absatz 2 Satz 2 Nr. 1 TKG zu verstehen ist, bleibt unklar. Die Begründung nennt zwar mit EMS (Enhanced Message Service) ein Beispiel. Es stellt sich jedoch die Frage, ob auch Messengerdienste unter „ähnliche Nachrichten" zu fassen sind und damit der Speicherpflicht unterliegen. Aufgrund der aktuellen Unklarheit über deren Status als Telekommunikationsdienste-Anbieter (TK-Anbieter) dürfte die Einordnung als „ähnliche Nachricht" im Sinne des § 113b Absatz 2 Satz 2 Nr. 1 TKG fraglich sein und sich erst mit der geplanten E-Privacy-Verordnung ändern. Selbst bei Annahme der TK-Anbietereigenschaft, von der ich aktuell ausgehe, würde die Auskunftserteilung praktisch an der Vollstreckbarkeit der Anordnung scheitern, da Messengerdienste wie zum Beispiel WhatsApp, Skype oder Facebook (Messenger) nicht nur über keinen Sitz in Deutschland verfügen, sondern auch ihre Server in Drittstaaten stehen. Gerade WhatsApp wird aber in Deutschland von rund 60% aller mobilen Internetnutzer verwendet

(https://de.statista.com/themen/1995/whatsapp/). Auch die Nutzung von Messengerdiensten, über die nicht nur Textnachrichten verschickt, sondern auch Sprach- und Videoanrufe getätigt werden können, ist damit ohne das Hinterlassen von Spuren in den auf Vorrat gespeicherten Daten möglich.

Im Gegensatz zu der Entscheidung des BVerfG vom 02.03.2010 liegt dem aktuellen Verfahren damit ein Sachverhalt zugrunde, bei dem nicht nur Einzelfälle aus dem Raster fallen. Von einer generellen Zweckförderung kann bei der aufgezeigten Vielzahl der aus dem Raster fallenden Fälle aber nicht mehr gesprochen werden.

2) Erforderlichkeit

Erhebliche Zweifel bestehen auch an der Erforderlichkeit der in den angegriffenen Vorschriften geregelten Vorratsdatenspeicherung. In der Gesetzesbegründung heißt es, dass die aus betrieblichen Gründen bei den TK-Anbietern vorhandenen Daten in Verbindung mit den bestehenden Auskunftsrechten zu Unzulänglichkeiten bei der Strafverfolgungsvorsorge und Gefahrenabwehr führen (BT-Drs. 18/5088, S. 21). Grund hierfür sei 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“* (BT-Drs. 18/5088, S. 21). Nach meinen umfangreichen Prüferfahrungen im Bereich Telekommunikation ist diese Aussage nicht nachvollziehbar. So werden Verkehrsdaten von Telefonverbindungen zu betrieblichen Zwecken regelmäßig zwischen drei und sechs Monaten vorgehalten (Anlage Leitfaden der BfDI und der Bundesnetzagentur für eine datenschutzgerechte Speicherung von Verkehrsdaten). Diese Notwendigkeit besteht bereits aufgrund des den Kunden zustehenden, in § 45i Absatz 1 TKG gesetzlich geregelten Einspruchszeitraums 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 von § 113b Absatz 1 Nr. 1 TKG festgelegten Zeitraum von zehn Wochen – ohnehin vorhanden ist und somit auch nach Maßgabe des geltenden Rechts für Auskünfte an die Sicherheitsbehörden zur Verfügung steht. Dies gilt auch für im Zusammenhang mit sog. Flatrategesprächen anfallende Verkehrsdaten, wenn es sich nicht um netzinterne Verbindungen handelt. Zwar werden die im Zusammenhang mit Flatrategesprächen anfallenden Verkehrsdaten nicht für die Abrechnung mit dem Teilnehmer benötigt. Allerdings erheben Netzbetreiber Entgelte, wenn sie Gespräche von anderen Netzbetreibern entgegennehmen. Aus diesem Grund müssen für die Abrechnung die Verkehrsdaten der Flatrategespräche, die Kunden verschiedener Netzbetreiber miteinander führen, gespeichert werden.

Eine Ausnahme von der Tatsache, dass Verkehrsdaten regelmäßig zwischen drei und sechs Monaten vorgehalten werden, bilden die den Teilnehmern zugewiesenen IP-Adressen, die grundsätzlich nur bis zu sieben Tagen gespeichert werden, die Standortdaten in Form der Funkzellen sowie die unter eine sog. Flatrate fallenden netzinternen Verbindungen, die – abhängig vom System des jeweiligen TK-Anbieters – üblicherweise zwischen sieben und dreißig Tagen abrufbar sind.

Im Ergebnis ist die durch die angegriffenen Vorschriften gesetzlich angeordnete Doppelspeicherung von unzähligen Verkehrsdaten daher nicht erforderlich. Als milderes – wenngleich nicht angemessenes – Mittel könnte sich die Speicheranordnung auf IP-Adressen, Standortdaten und netzinterne Flatrate-Daten beschränken und lediglich für diese eine längere Speicherfrist festsetzen.

3) Angemessenheit

Die angegriffenen Vorschriften stehen nicht in einem angemessenen Verhältnis zum beabsichtigten Zweck.

a) Vorgaben des BVerfG

Nach der Rechtsprechung des BVerfG handelt es sich bei der Vorratsdatenspeicherung um einen schwerwiegenden Grundrechtseingriff von besonderem Ausmaß (BVerfG, Urteil vom 02.03.2010, Az.: 1 BvR 256/08, 1 BvR 263/08, 1 BvR 586/08). Die vom BVerfG an eine verfassungsrechtliche Unbedenklichkeit einer vorsorglich anlasslosen Speicherung der Telekommunikationsdaten gestellten Anforderungen an eine verhältnismäßige Ausgestaltung des mit den angegriffenen Vorschriften einhergehenden Grundrechtseingriff werden nicht erfüllt.

Für die verfassungsrechtliche Unbedenklichkeit einer vorsorglich anlasslosen Speicherung von Telekommunikationsverkehrsdaten fordert das BVerfG, dass diese eine Ausnahme bleibt und auch nicht im Zusammenspiel mit anderen vorhandenen Dateien zur Rekonstruierbarkeit praktisch aller Aktivitäten der Bürger führen darf (BVerfG, Urteil vom 02.03.2010, Az.: 1 BvR 256/08, 1 BvR 263/08, 1 BvR 586/08, Rn. 218). Diese Möglichkeit einer „Gesamtüberwachung“ wird jedenfalls im Bereich der Überwachung der Internetnutzung außer Acht gelassen. Aufgrund der weitreichenden Verpflichtung zur Speicherung von IP-Adressen wird bereits nur aufgrund der Vorgaben des § 113b TKG ein äußerst umfangreicher Datenpool geschaffen. Die TK-Branche stellt gegenwärtig die von ihr angebotenen Telefonanschlüsse großflächig auf IP-basierte Angebote um. 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. 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 zum Beispiel 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 Bundeskriminalamts erforderlich sein muss.

IP-Adressen sind nicht nur als Verkehrsdaten im Sinne des TKG, sondern auch als Nutzungsdaten im Sinne des Telemediengesetzes (TMG) betroffen. Nutzungsdaten im Sinne des § 15 TMG sind zum Beispiel die IP-Adresse sowie Datum, Uhrzeit und aufgerufene Seite. Es handelt sich um Daten, die beim Besuch einer Website immer und auch ohne Anmeldung anfallen. Gerade letztere vermitteln aber detailliertere 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 somit zumindest über mehrere Wochen das Surfverhalten der Internetnutzer bei den jeweiligen Telemediendiensten äußerst detailliert überwachen. Durch die in § 113c Absatz 1 Nr. 3 TKG mit § 113 TKG geschaffene Verknüpfung können Nachrichtendienste die in den Vorratsdaten gespeicherten IP-Adressen zumindest mittelbar nutzen.

b) Vorgaben des EuGH

Die angegriffenen Vorschriften stellen aber nicht nur einen unverhältnismäßigen Eingriff in deutsche, sondern auch in europäische Grundrechte dar.

Die Maßstäbe für die Zulässigkeit von Vorschriften zur Vorratsdatenspeicherung hat der EuGH bereits in seinem Urteil vom 08.04.2014, Az.: C-293/12 und C-594/12 zur Nichtigkeit der Richtlinie 2006/24/EG in der Rechtssache „Digital Rights" dargelegt und nunmehr in seinem Urteil vom 21.12.2016, Az. C-203/15 und C-698/15, konkretisiert. Nach der Rechtsprechung des EuGH stellen Regelungen zur Vorratsdatenspeicherung einen schwerwiegenden Eingriff in Art. 7, 8, 11 und 52 der Charta der Grundrechte der Europäischen Union (Charta) dar, in deren Lichte Art. 15 Absatz 1 der Richtlinie 2002/58 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation in der durch die Richtlinie 2009/136 geänderten Fassung (Richtlinie) auszulegen ist.

Art. 5 Absatz 1 Satz 2 der Richtlinie verpflichtet die Mitgliedstaaten, das Mithören, Abhören und Speichern von Nachrichten und der damit verbundenen Verkehrsdaten durch andere Personen als die Nutzer ohne deren Einwilligung zu untersagen. Gemäß Art. 5 Absatz 1 Satz 2 der Richtlinie gilt diese Pflicht nicht, wenn andere Personen gemäß Art. 15 Absatz 1 der Richtlinie gesetzlich zur Speicherung verpflichtet sind. Art. 15 Absatz 1 der Richtlinie ermächtigt die Mitgliedstaaten zum Erlass von Rechtsvorschriften, die unter anderem die Rechte und Pflichten aus Art. 5 der Richtlinie (Vertraulichkeit der Kommunikation) einschränken. Um eine solche Einschränkung im Sinne des Art. 15 Absatz 1 der Richtlinie handelt es sich bei den im vorliegenden Verfahren angegriffenen nationalen Vorschriften zur Vorratsdatenspeicherung sowie den Zugang der nationalen Behörden zu diesen Daten für Zwecke der Strafverfolgung. In seinem Urteil vom 21.12.2016, Az. C-203/15 und C-698/15 (Rn. 75, 76), hat der EuGH entschieden, dass eine Rechtsvorschrift, die den Betreibern elektronischer Kommunikationsdienste vorschreibt, die Verkehrs- und Standortdaten auf Vorrat zu speichern, sowie eine Rechtsvorschrift, die den Zugang der nationalen Behörden zu den von den Betreibern elektronischer Kommunikationsdienste auf Vorrat gespeicherten Daten betrifft, in den Geltungsbereich der Richtlinie fallen.

Nach der ständigen Rechtsprechung des EuGH ist Art. 15 Absatz 1 der Richtlinie eng auszulegen (EuGH, a.a.O. mit Verweis auf EuGH, Urteil vom 22.11.2012, Az.: C-119/12). Dies bedeutet, dass eine Rechtsvorschrift im Sinne des Art. 15 Absatz 1 der Richtlinie die in Art. 5 Absatz 1 Satz 2 der Richtlinie vorgesehene Pflicht zur Untersagung einer Verkehrsdatenspeicherung nur dann beschränken darf, wenn die Ausnahme vom Verbot des Art. 5 Absatz 1 Satz 2 der Richtlinie nicht zum Regelfall wird. Eingriffe in die Grundrechte auf Achtung des Privatlebens und des Schutzes personenbezogener Daten müssen sich damit auf das Notwendigste beschränken. Nach der Rechtsprechung des EuGH (Urteil vom 21.12.2016, Az. C-203/15 und C-698/15) bewegt sich eine nationale Regelung zur Vorratsdatenspeicherung innerhalb der Grenzen des absolut Notwendigen, wenn sie die nachfolgenden Anforderungen erfüllt.

aa) Die Vorratsdatenspeicherung muss hinsichtlich der Kategorien von zu speichernden Daten, der erfassten Kommunikationsmittel, der betroffenen Personen und der vorgesehenen Speicherdauer auf das absolut Notwendige beschränkt werden.

bb) Die Vorratsdatenspeicherung muss der Bekämpfung schwerer Straftaten dienen.

cc) Die Vorschriften über die Vorratsdatenspeicherung müssen die materiell- und verfahrensrechtlichen Voraussetzungen für den Zugang der zuständigen nationalen Behörden festlegen.

dd) Der Zugang muss einer vorherigen Kontrolle durch ein Gericht oder eine unabhängige Stelle unterliegen.

Um diesen Erfordernissen zu genügen, muss eine nationale Regelung im Sinne des Art. 15 Absatz 1 der Richtlinie *„klare und präzise Regeln über die Tragweite und die Anwendung einer solchen Maßnahme der Vorratsdatenspeicherung vorsehen und Mindesterfordernisse aufstellen, so dass die Personen, deren Daten auf Vorrat gespeichert wurden, über ausreichende Garantien verfügen, die einen wirksamen Schutz ihrer personenbezogenen Daten vor Missbrauchsrisiken ermöglichen. Sie muss insbesondere angeben, unter welchen Umständen und unter welchen Voraussetzungen eine Maßnahme der Vorratsdatenspeicherung vorbeugend getroffen werden darf, um so zu gewährleisten, dass eine derartige Maßnahme auf das absolut Notwendige beschränkt wird."* (EuGH, a.a.O.)

Darüber hinaus *„muss die Vorratsdatenspeicherung der Daten stets objektiven Kriterien genügen, die einen Zusammenhang zwischen den zu speichernden Daten und dem verfolgten Ziel herstellen. Diese Voraussetzungen müssen insbesondere in der Praxis geeignet sein, den Umfang der Maßnahme und infolgedessen die betroffenen Personenkreise wirksam zu begrenzen."* (EuGH, a.a.O.)

zu aa) Beschränkung der Vorratsdatenspeicherung auf das absolut Notwendige

Die Vorgaben des EuGH zur Beschränkung der betroffenen Personen auf solche, die in irgendeiner Weise in eine schwere Straftat verwickelt sind oder deren auf Vorrat gespeicherte Daten aus anderen Gründen zur Verhütung, Feststellung oder Verfolgung schwerer Straftaten beitragen könnten, werden in den angegriffenen Vorschriften nicht umgesetzt. Zwar dürfen gemäß § 100g Absatz 1 StPO Verkehrsdaten nur gezielt für Tatverdächtige erhoben werden, soweit dies für die Erforschung des Sachverhalts erforderlich ist und die Erhebung der Daten in einem angemessenen Verhältnis zur Bedeutung der Sache steht. § 113b TKG bildet diese Begrenzung der betroffenen Personen indes nicht ab. Vielmehr sieht § 113b TKG eine anlasslose Speicherung von Verkehrsdaten ohne jegliche Beschränkung des betroffenen Personenkreises auf solche, die Anlass zur Strafverfolgung gegeben haben, vor. Damit

werden von § 113b TKG nicht nur Verkehrsdaten von Personen erfasst, die Kommunikation betreiben, sondern in Bezug auf die Speicherpflicht von IP-Adressen nach § 113b Absatz 3 TKG sogar die Verkehrsdaten von Personen, die lediglich die technische Infrastruktur vorhalten.

aaa) Einschränkung des Personenkreises und der Kommunikationsmittel

Eine Einschränkung des Personenkreises findet sich lediglich in § 113b Absatz 6 TKG, wonach Verbindungsdaten im Sinne des § 99 Absatz 2 TKG 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, von der Speicherpflicht ausgenommen sind. Diese in § 113b Absatz 6 TKG vorgesehene Ausnahme führt indes nicht zu einer Beschränkung des betroffenen Personenkreises auf solche, die in eine schwere Straftat verwickelt sind oder deren auf Vorrat gespeicherte Daten aus anderen Gründen zur Verhütung, Feststellung oder Verfolgung schwerer Straftaten beitragen könnten.

Von der Speicherpflicht nicht ausgenommen sind Daten von Berufsgeheimnisträgern wie Rechtsanwälten, Geistlichen oder Ärzten. Diese werden erst nach Maßgabe von § 100g Absatz 4 i.V.m. § 53 StPO geschützt, nach § 113b TKG also erstmal gespeichert. Rechtlich bedenklich ist, dass die Vorratsdaten von Berufsgeheimnisträgern nach Maßgabe des § 100g Absatz 4 StPO nur gesperrt sind, soweit sich die Maßnahme unmittelbar gegen den Zeugnisverweigerungsberechtigten richtet. Wird dieser hingegen 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 (treffend zu diesem Punkt die Stellungnahme des DAV zum Entwurf der verfahrensgegenständlichen Vorschriften in der Fassung des Referentenentwurfs vom 15.05.2015, Stellungnahme Nr. 25/2015, S. 14). 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 auch der EuGH in seinem Urteil vom 08.04.2014, Az.: C-293/12, C-594/12, die Geltung der Richtlinie und damit die Existenz einer Vorratsspeicherpflicht auch für die Kommunikationsvorgänge von Berufsgeheimnisträgern als einen unverhältnismäßigen Eingriff in die Charta. Konsequenterweise kann daher der in § 100g Absatz 4 StPO gewählte Ansatz einer Kombination aus Abruf- und Verwertungsverbot keine hinreichende Alternative zum Verzicht auf eine Speicherung der Daten darstellen.

Von der Speicherpflicht erfasst sind nahezu alle Kommunikationsmittel i.S.d. TKG. Ob von der Speicherpflicht auch Messengerdienste erfasst sind, ist aufgrund der Unklarheit über deren Status als TK-Anbieter aktuell fraglich. Von der Speicherpflicht ausdrücklich ausgenommen sind gemäß § 113b Absatz 5 TKG lediglich die Daten über aufgerufene Internetseiten und Daten von Diensten der elektronischen Post (E-Mail).

Unabhängig davon ist mit der Ausklammerung verschiedener Kommunikationsbereiche keine Beschränkung des betroffenen Personenkreises auf solche, die in eine schwere Straftat verwickelt sind oder deren auf Vorrat gespeicherte Daten aus anderen Gründen zur Verhütung, Feststellung oder Verfolgung schwerer Straftaten beitragen könnten, verbunden.

Letztlich führt auch die in § 113b Absatz 1 TKG erfolgte Differenzierung im Hinblick auf die Dauer der Speicherung von Verkehrs- und Standortdaten nicht zu der vom EuGH geforderten Beschränkung des betroffenen Personenkreises.

Mangels Beschränkung des betroffenen Personenkreises ist die verfahrensgegenständliche Vorschrift des § 113b TKG nicht auf das absolut Notwendigste begrenzt und nach der Rechtsprechung des EuGH damit nicht verhältnismäßig.

bbb) Beschränkung hinsichtlich der Kategorien von zu speichernden Daten

Ausweislich § 113b Absatz 4 TKG sind von der Speicherpflicht pauschal alle Standortdaten erfasst. 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 50 Millionen Menschen ein oder mehrere Smartphones 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 hat die BfDI 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 vor dem Hintergrund, dass die Speicherung der Vorratsdaten anlasslos erfolgt, besteht hier das Potential, die Voraussetzung für eine Profilbildung zu schaffen, die ausweislich der Ausführungen in den Leitlinien vom 15.04.2015 eigentlich vermieden werden sollte (Leitlinien des BMJV zur Einführung einer Speicherpflicht und Höchstspeicherfrist für Verkehrsdaten, S. 2 f.). Die in den Leitlinien des BMJV zur Einführung einer Speicherpflicht und Höchstspeicherfrist für Verkehrsdaten angekündigte Beschränkung des Abrufs von Standortdaten findet sich lediglich an einer einzigen Stelle in der Gesetzesbegründung, wo es heißt: *„Grundsätzlich sollen nur einzelne Standortdaten abgerufen werden, um keine überflüssigen Bewegungsprofile zu erstellen“* (BT-Drs.15/5088, S. 35). 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* (a.a.O).“

Da die Vorratsdatenspeicherung aber insbesondere dazu dienen soll, Ermittlungsansätze im 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.

Zu bb) bestehen keine Anmerkungen.

zu cc) Regelung des Zugangs zu den auf Vorrat gespeicherten Daten

Nach der Rechtsprechung des EuGH ist eine nationale Rechtsvorschrift, die den Zugang zu den auf Vorrat gespeicherten Daten regelt, nur dann auf das absolut Notwendigste begrenzt und damit verhältnismäßig, wenn sie klare und präzise Regeln aufstellt, in denen angegeben ist, unter welchen Umständen und unter welchen Voraussetzungen der Betreiber elektronischer Kommunikationsdienste den zuständigen nationalen Behörden Zugang zu den Daten zu gewähren hat (EuGH, Urteil vom 21.12.2016, Az. C-203/15 und C-698/15 Rn. 117). Unter Verweis auf sein Urteil vom 22.11.2012, Az.: C-119/12, führt der EuGH aus, dass sich die nationale Rechtsvorschrift nicht darauf beschränken darf, dass der Zugang einem der in Art. 15 Absatz 1 genannten Zwecke zu entsprechen hat, sondern vielmehr auch die materiell- und verfahrensrechtlichen Voraussetzungen für den Zugang der zuständigen nationalen Behörden festlegen muss.

Gemäß § 113c TKG dürfen TK-Anbieter die auf Vorrat gespeicherten Daten zur Verfolgung besonders schwerer Straftaten (§ 113c Absatz 1 Nr. 1 TKG) oder zur Abwehr einer konkreten Gefahr für Leib, Leben oder Freiheit einer Person oder für den Bestand des Bundes oder eines Landes (§ 113c Absatz 1 Nr. 2 TKG) an die jeweils zuständige nationale Behörde übermitteln. Diese Regelung widerspricht dem vom EuGH aufgestellten Grundsatz, dass *„im Zusammenhang mit dem Zweck der Bekämpfung von Straftaten Zugang grundsätzlich nur zu den Daten von Personen gewährt werden* (darf)*, die im Verdacht stehen, eine schwere Straftat zu planen, zu begehen oder begangen zu haben oder auf irgendeine Weise in eine solche Straftat verwickelt zu sein.“* (EuGH, a.a.O., Rn. 118). Weder § 113c TKG noch § 100g Absatz 2 StPO beschränken die Übermittlung / Erhebung der auf Vorrat gespeicherten Verkehrsdaten auf Daten von Personen, gegen die der begründete Verdacht einer schweren Straftat i.S.d. § 100g Absatz 2 StPO besteht. Vielmehr ermöglichen sie auch die Übermittlung / Erhebung der auf Vorrat gespeicherten Verkehrsdaten von Personen, die weder Täter noch Teilnehmer einer schweren Straftat sind, deren Daten aber zur Überführung tatverdächtiger Personen beitragen können, ohne dass

hierfür erhöhte materielle Voraussetzungen wie die Bedrohung der nationalen Sicherheit durch terroristische Aktivitäten gelten.

§ 113c TKG 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 gespeicherten Daten ermächtigt.

Die Formulierung der Übermittlungsermächtigung führt zu Anwendungsproblemen in der Praxis. So wird den TK-Anbietern vorliegend kein Prüfungsmaßstab an die Hand gegeben, anhand dessen sie verifizieren können, ob eine Übermittlung tatsächlich zulässig ist. Die Prüfung wird sich daher ausschließlich auf das Vorliegen formeller Voraussetzungen (zum Beispiel das Vorliegen eines richterlichen Beschlusses) beschränken müssen. Dafür spricht auch, dass in der Gesetzesbegründung ausdrücklich eine materielle Prüfpflicht ausgeschlossen wird (BT-Drs. 18/5088, S. 41). Eine formelle Prüfung muss aber zwingend erfolgen, da den TK-Anbietern bei einer zweckwidrigen Verwendung der Daten nach § 149 Absatz 2 Satz 1 Nr. 1 TKG 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 Anforderungen 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 wurde ich von vielen TK-Anbietern darauf hingewiesen, dass die Auskunftserteilung auf der Grundlage von Anträgen, deren formelle Rechtmäßigkeit nicht eindeutig sei, ein erhebliches Risiko für die konkret mit der Auskunftserteilung befassten Mitarbeiter darstelle. 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 in dem Fall, wo ich die Auskunft nicht erteile und deshalb wegen Strafvereitlung angegangen werde.“* Gerade das In-Aussicht-stellen einer Verfahrenseinleitung wegen Strafvereitlung sowie die Ankündigung, Vorstandsmitglieder zu einer Zeugenvernehmung vorzuladen, ist eine von TK-Anbietern gerügte aktuell praktizierte Reaktion der Strafverfolgungsbehörden auf kritische Rückfragen zu formfehlerhaften Auskunftsersuchen.

Gegen die auf §§ 96, 113b und 113c TKG gestützten Anordnungen zur Herausgabe von Verkehrsdaten legt ein von mir beaufsichtigter TK-Anbieter aktuell mit dem Hinweis darauf, dass eine Vorratsdatenspeicherung nicht durchgeführt wird, Beschwerden ein. Ein mir vorliegender Beschluss des Landgerichts Bochum hilft einer solchen Beschwerde unter Verweis auf die Beschlüsse des OVG Nordrhein-Westfalen vom 22.06.2017, Az.: 13 B 238/17 und 13 B 762/17 ab.

Neben den zu ergänzenden Erläuterungen zum Prüfungsmaßstab fehlt in § 113c Absatz 1 TKG die Vorgabe, dass die gemäß § 113b TKG gespeicherten Daten lediglich im Zeitraum des § 113b Absatz 1 TKG übermittelt werden dürfen. Aufgrund der Löschvorschrift in § 113b Absatz 8 TKG 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 zu einer unrechtmäßigen Ausweitung der Speicherdauer führen.

Rechtliche Bedenken bestehen auch gegen die in § 113 Absatz 1 Nummer 3 TKG 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 (BVerfG, Urteil vom 02.03.2010, Az.: 1 BvR 259/08, 1 BvR 263/08, 1 BvR 586/08, Rn. 261). 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)“ (BVerfG, a.a.O., Rn. 256).

Gerade aufgrund der bereits im Rahmen der Erwägungen zur Verhältnismäßigkeit dargelegten umfangreichen Möglichkeiten der Überwachung des Internetnutzungsverhaltens, 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 scheint zumindest ein Richtervorbehalt auch für Bestandsdatenauskünfte nach § 113 Absatz 1 Satz 3 TKG zwingend erforderlich.

Zu dd) bestehen keine Anmerkungen.

B) Keine einheitliche Höchstspeicherfrist

Ich möchte an dieser Stelle noch einmal ausdrücklich darauf hinweisen, dass das Gesetz zur Einführung einer Speicherpflicht und Höchstspeicherfrist für Verkehrsdaten **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 angegriffenen Gesetz festgelegten Fristen exklusiv beziehen. Neben diesen Daten 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 (zum Beispiel zur Abrechnung, Missbrauchserkennung, Störungsbeseitigung, etc.) geben. Ein Großteil dieser Daten wird auch über die in § 113b Absatz 1 TKG vorgesehenen Fristen hinaus gespeichert (s. Anlage, Leitfaden der BfDI und der Bundesnetzagentur für eine datenschutzgerechte Speicherung von Verkehrsdaten).

C) Erkenntnisse aus meiner Beratungs- und Kontrollpraxis

In 2017 habe ich bei einem Unternehmen, das die Vorratsdatenspeicherung als Auftragnehmer für TK-Anbieter durchführt, einen Beratungs- und Kontrollbesuch zur Vorratsdatenspeicherung durchgeführt. Im Rahmen dieses Besuchs wurde unter anderem die Einhaltung des Anforderungskatalogs des § 113f TKG geprüft. Dabei wurde festgestellt, dass der in § 113f TKG geforderte besonders hohe Sicherheits- und Qualitätsstandard bei der Umsetzung der Verpflichtungen zur Vorratsdatenspeicherung nicht gewährleistet wurde. Sowohl aus organisatorischer als auch aus technischer Sicht bestehen Zweifel an der praktischen Umsetzbarkeit der Anforderungen des § 113f TKG (zu den Anforderungen im Einzelnen siehe https://www.bundesnetzagentur.de/DE/Sachgebiete/Telekommunikation/Unternehmen_Institutionen/Anbieterpflichten/OeffentlicheSicherheit/Umsetzung110TKG/VDS_11aTKG/VDS.html). Dies gilt insbesondere im Hinblick auf kleine und mittelständische TK-Anbieter, die nach meinen Erfahrungen regelmäßig nicht über die personellen, räumlichen und finanziellen Möglichkeiten zur Einhaltung der Anforderungen des § 113f TKG verfügen und die Anforderungen an die Rechtmäßigkeit einer Vorratsdatenspeicherung daher nur schwerlich erfüllen können.

D) Funkzellenabfragen nach § 100g Absatz 3 StPO

Die Regelung zur Funkzellenabfrage enthält nicht die datenschutzrechtlich notwendigen Einschränkungen. Dies betrifft zum einen den Zugriff auf die Daten, zum anderen aber auch die weitere Verarbeitung. Auf welche Rechtsgrundlagen der Abgleich gestützt werden kann, ist in erheblicher Weise unklar.

1) Zugriff auf Daten

Notwendig war eine Neuregelung wegen der besonderen Eingriffsintensität der Maßnahme. Sie war nach Funkzellenabfragen bei Demonstrationen in Dresden verschiedentlich gefordert worden (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 16.03.2018)).

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 (vgl. hierzu BT-Drs. 17/14794).

Eingesetzt wurden Funkzellenabfragen nicht nur in Fällen wie etwa bei dem bekannten Fall des Autobahnschützen, dem ein versuchtes Tötungsdelikt vorgeworfen wurde. Ebenso wurde zum Beispiel in höchst umstrittener Weise versucht, mit Funkzellenabfragen Gewalttätigkeiten bei Demonstrationen zu verfolgen (vgl. dazu Prüfbericht des Sächsischen Datenschutzbeauftragten a.a.O).

Bei solchen Maßnahmen erfasst die Polizei aber nicht nur Gewalttäter, sondern ebenso unbeteiligte Personen in großem Umfang.

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 etwa an einer 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 (BVerfG, NJW 1991, S. 91 (94 f.). Mit der Funkzellenabfrage kann ohnehin nicht die Teilnahme an der Demonstration geklärt werden, sondern nur der Aufenthalt in einer bestimmten Funkzelle.

Der Landfriedensbruch ist im Katalog des § 100g Absatz 2 Satz 2 Nr. 1 Buchstabe b StPO enthalten, wenn 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 (dazu unten 2). 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 (zum Beispiel 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 (Bericht des Sächsischen Datenschutzbeauftragten a.a.O., S. 40.).

2) Rechtsgrundlage für den Abgleich

Unklar ist, auf welcher Rechtsgrundlage der Kreuztrefferabgleich durchgeführt werden soll. Nach meiner Auffassung handelt es sich der Sache nach um eine Rasterfahndung gemäß § 98a StPO. Nach einer in der Praxis der Strafverfolgung teilweise vertretenen Auffassung handelt es sich lediglich um einen an niedrigere Voraussetzungen gebundenen einfachen Datenabgleich nach § 98c StPO. Dagegen spricht

aus meiner Sicht, dass die abzugleichenden Daten nicht bei den Strafverfolgungsbehörden ohnehin aus anderen Gründen vorliegen, sondern gerade mit dem Ziel des Abgleichs erhoben werden. Darüber hinaus hängt das Eingriffsgewicht des Datenabgleichs nicht allein davon ab, ob die abzugleichenden Daten „zufällig" vorhanden sind oder gezielt erhoben wurden. Der Gesetzgeber hat trotz der speziellen Regelung der Funkzellenabfrage hierzu keine klare Aussage getroffen.

Ungeachtet dessen geht die polizeiliche Praxis sogar noch einen Schritt weiter. In einer Datei hat das Bundeskriminalamt die Daten aus den Funkzellenabfragen aus einer Vielzahl von Verfahren aus verschiedenen Bundesländern gespeichert und miteinander abgeglichen (siehe meinen 26. Tätigkeitsbericht, Nr. 10.2.9.3.). Dagegen hatte ich kurz nach Kenntnisnahme der entsprechenden Errichtungsanordnung Einwände erhoben. Diese ließ das Bundesministerium des Innern jedoch unbeachtet. Das Bundeskriminalamt und das Bundesministerium des Innern waren der Auffassung, eine solche Datei auf die Generalklausel des § 7 Absatz 1 BKAG stützen zu können. In einer anschließenden datenschutzrechtlichen Kontrolle habe ich die Datei formell gemäß § 25 BDSG beanstandet. Nähere Umstände kann ich wegen der Einstufung als Verschlusssache hierzu nicht ausführen. Eine Antwort zu meinem Prüfbericht liegt mir noch nicht vor. Ob die Datei noch betrieben wird, ist mir deshalb unbekannt.

Ab dem 25. Mai 2018 sieht das Bundeskriminalamtgesetz nicht mehr vor, für die Einrichtung von Dateien Errichtungsanordnungen zu erstellen. Das neue Informationssystem wird laut der neuen gesetzlichen Regelungen auch nicht mehr nach Dateien geordnet sein. Daher besteht die höhere Wahrscheinlichkeit, dass derartige Speichervorgänge meiner Aufmerksamkeit als Datenschutzaufsichtsbehörde künftig entgehen.

Nach meiner Auffassung handelt es sich der Sache nach auch insoweit um eine Rasterfahndung gemäß § 98a StPO. Diese Datenverarbeitung hat eine hohe Streubreite und enthält die Daten einer Vielzahl von Personen, die selbst keinen Anlass für eine Speicherung gegeben haben. Dies kann nur auf Grundlage einer spezifischen Rechtsgrundlage erfolgen, die Voraussetzungen und Umfang verhältnismäßig regelt. Die Generalklausel genügt dafür nicht. Ich sehe mich durch einzelne Gerichtsentscheidungen bestätigt, die bei Funkzellenabfragen gleichzeitig einen Beschluss gemäß § 98a StPO fassen.

Besonders groß 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 ei-

nen Zeitraum zu beobachten (vgl. Bericht des Sächsischen Datenschutzbeauftragten a.a.O. S. 44 ff.). 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 (vgl. a.a.O.). In solchen Fällen wird aus der Vorratsdatenspeicherung dann gewissermaßen eine **„doppelte Vorratsdatenspeicherung"**. Gegen eine solche Praxis sieht das Gesetz zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten 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 genannten Fällen.

Die genannten Funkzellenabfragen in Sachsen hatten erhebliches Echo in den Medien. Der Sächsische Datenschutzbeauftragte ist 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 genommen. Meine datenschutzrechtlichen 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.

Mit freundlichen Grüßen

[redacted]

Andrea Voßhoff

Leitfaden des BfDI und der BNetzA für eine datenschutzgerechte Speicherung von Verkehrsdaten

Stand 19.12.12

Dieser Leitfaden wurde auf Anregung von Telekommunikationsanbietern erstellt. Er soll zu einer datenschutzgerechten und einheitlichen Auslegung des TKG – auch im Sinne von „Best Practices" - führen und stellt für die Beurteilung des Begriffs der „Erforderlichkeit" einen Prüfungsmaßstab dar.

Speicherkategorie	Rechtsgrundlage / max. Speicherdauer	Datenschutzgerechte Auslegung	Datenfelder[1]
A. Telefondienst, SMS **I. Für die Abrechnung mit Teilnehmern[2]**			
1. Entgeltpflichtig, abgehend	§ 97 Abs. 3 Satz 2 TKG: Max. 6 Monate nach Rechnungsversand	In der Regel werden 3 Monate nach Rechnungsversand (s. auch Beanstandungsfrist in § 45i Abs. 1 TKG) als ausreichend angesehen. Wenn nachvollziehbare Gründe vorliegen, können die Daten länger gespeichert werden.	A-, B-Rufnummer, Zeit[3], IMSI
2. Entgeltpflichtig, abgehend, standortabhängiger Tarif	§ 97 Abs. 3 Satz 2 TKG: Max. 6 Monate nach Rechnungsversand	In der Regel werden 3 Monate nach Rechnungsversand (s. auch Beanstandungsfrist in § 45i Abs. 1 TKG) als ausreichend angesehen. Wenn nachvollziehbare Gründe vorliegen, können die Daten länger gespeichert werden.	A-, B-Rufnummer, Zeit, Cell-ID, ggf. IMSI

[1] Technische Parameter, die keine sensiblen Angaben enthalten, z. B. die Leitungsführung zu anderen Anbietern, dürfen zusätzlich in den Datenfeldern enthalten sein, ohne dass diese in der Tabelle gesondert erwähnt werden. Zu den sensiblen Angaben gehören etwa Standortangaben (Cell-ID) oder die IMEI.

[2] Dies betrifft sowohl Postpaid- als auch Prepaiddienste. Bei Prepaiddiensten ist ein fiktives Rechnungsdatum anzunehmen (entweder der Tag, an dem das Gespräch geführt wurde, oder eine virtuelle Monatsabrechnung).

[3] Sofern in dieser Spalte der Begriff „Zeit" verwendet wird, meint er Beginn und Ende (oder Beginn und Dauer) einer Verbindung bzw. Sendezeitpunkt einer SMS nach Datum und Uhrzeit.

3. Freivolumen, danach entgeltpflichtig	§ 97 Abs. 3 Satz 2 TKG: Max. 6 Monate nach Rechnungsversand	Diese Daten können wie die Daten von entgeltpflichtigen Verbindungen gespeichert werden, da die Freiminuten bzw. Frei-SMS die Entgeltpflicht der weiteren Verbindungen begründen.	A-, B-Rufnummer, Zeit, ggf. IMSI, wenn für Abrechnung erforderlich auch Cell-ID
4. Pauschal abgegolten (Flatrate)	§ 97 Abs. 3 Satz 3 TKG: Unverzügliche Löschung nach Ermittlung der Abrechnungsirrelevanz	Unverzügliche Löschung nach Ermittlung der Abrechnungsirrelevanz (je nach systemischer Ausgestaltung spätestens bei Rechnungserstellung).	Keine Daten
5. Pauschal abgegolten (Flatrate), Kundenwunsch auf EVN	§ 99 Abs. 1 Satz 1, 2. Halbsatz TKG: Bis zur Erstellung des EVN	Unverzügliche Löschung nach Erstellung des EVN.	A-, B-Rufnummer, Zeit, ggf. IMSI
6. Nicht entgeltpflichtig (z.B. 0800)	§ 97 Abs. 3 Satz 3 TKG: Unverzügliche Löschung nach Ermittlung der Abrechnungsirrelevanz	Unverzügliche Löschung nach Ermittlung der Abrechnungsirrelevanz.	Keine Daten
7. Ankommend und entgeltlich (z.B. Roaming, R-Gespräch)	§ 97 Abs. 3 Satz 2 TKG: Max. 6 Monate nach Rechnungsversand	In der Regel werden 3 Monate nach Rechnungsversand (s. auch Beanstandungsfrist in § 45i Abs. 1 TKG) als ausreichend angesehen. Wenn nachvollziehbare Gründe vorliegen, können die Daten länger gespeichert werden.	A-, B-Rufnummer, Zeit, ggf. IMSI, wenn erforderlich Cell-ID
8. Ankommend und unentgeltlich	§ 97 Abs. 3 Satz 3 TKG: Unverzügliche Löschung nach Ermittlung der Abrechnungsirrelevanz	Unverzügliche Löschung nach Ermittlung der Abrechnungsirrelevanz.	Keine Daten
9. Verbindungsversuche	Keine Rechtsgrundlage	Keine Speicherung zulässig.	Keine Daten
10. Nicht abrechnungsfähige Daten (aufgrund fehlender Zuordnungsmöglichkeit, z.B. zu entsprechenden Bestandsdaten)	§ 97 Abs. 3 Satz 1 TKG: Unverzügliche Ermittlung der für die Abrechnung erforderlichen Daten	In der Regel werden 3 Monate als ausreichend angesehen. Wenn nachvollziehbare Gründe vorliegen, können diese Daten bis zu 12 Monate gespeichert werden.	A-, B-Rufnummer, Zeit, ggf. Cell-ID, IMSI
11. Bestrittene Forderungen	§ 97 Abs. 3 Satz 4 TKG	Bei bestrittenen Forderungen dürfen die Verkehrsdaten bis zur abschließenden Klärung der Einwendungen (z. B. Anerkenntnis der Forderung durch den Kunden) gespeichert werden.	A-, B-Rufnummer, Zeit, ggf. IMSI, wenn für Abrechnung erforderlich auch Cell-ID

Telefondienst, SMS **II. Für sonstige Zwecke**			
1. Interconnection (Abrechnung mit anderen Dienste-anbietern)	§ 97 Abs. 4 TKG: Soweit erforderlich, max. 6 Monate nach Rechnungsversand (Frist analog zu § 97 Abs. 3 TKG)	In der Regel werden 3 Monate nach Rechnungsversand als ausreichend angesehen. Verträge mit längeren Einwendungsfristen sollten umgestellt werden, so dass mittelfristig eine Anpassung der Speicherdauer möglich ist. Für bestimmte Verbindungen oder Geschäftsmodelle kann eine längere Speicherung erforderlich sein (z.B. Offline-Billing, Auskunftsdienste, Roaming).	A-, B-Rufnummer, Zeit, Angabe zum Carrier, Cell-ID (nur bei Roaming)
2. Abrechnung mit Serviceprovidern	§ 97 Abs. 4 TKG: Soweit erforderlich, max. 6 Monate nach Rechnungsversand (Frist analog zu § 97 Abs. 3 TKG)	In der Regel werden 3 Monate nach Rechnungsversand als ausreichend angesehen. Verträge mit längeren Einwendungsfristen sollten umgestellt werden, so dass mittelfristig eine Anpassung der Speicherdauer möglich ist.	A-, B-Rufnummer, Zeit, IMSI, wenn erforderlich Cell-ID
3. Erkennung, Eingrenzung und Beseitigung von Störungen	§ 100 Abs. 1 TKG: Soweit erforderlich	Ohne konkreten Anlass ist eine Speicherung höchstens 7 Tage zulässig[4]. Sind konkrete Anhaltspunkte für eine Störung festgestellt worden, dürfen im Einzelfall die zum Eingrenzen und Beseitigen der vermuteten Störung erforderlichen Daten länger gespeichert werden. Darüber hinaus kann mit Statistiken oder anonymisierten Daten gearbeitet werden.	Alle Verkehrsdaten, z. B. auch IMEI
4. Aufdeckung von Missbrauch	§ 100 Abs. 3 TKG: Soweit erforderlich	Zum Aufdecken von Missbrauch kann nach § 100 Abs. 3 TKG auf Verkehrsdaten zurückgegriffen werden, die zulässigerweise zu anderen betrieblichen Zwecken gespeichert und nicht älter als 6 Monate sind. Ebenso können hierfür weitere Verkehrsdaten für bis zu 7 Tage verwendet, das heißt auch gespeichert werden. Die zur Aufklärung eines konkret festgestellten Missbrauchsverdachtes erforderlichen Verkehrsdaten dürfen bis zum Abschluss von dessen Bearbeitung verwendet werden.	Alle vorhandenen Verkehrsdaten

[4] Vgl. zur 7-Tage-Frist auch das Urteil des Bundesgerichtshofs vom 13.01.2011, Az: III ZR 146/10.

5. Fangschaltung	§ 101 TKG (nicht für SMS)	Soweit zur Zweckerreichung erforderlich.	A-, B-Rufnummer, Zeit
6. Backup von Rohdaten	§ 97 Abs. 3 Satz 1 TKG: Unverzügliche Ermittlung der für die Abrechnung erforderlichen Daten	Für die „unverzügliche Ermittlung" der für die Abrechnung erforderlichen Daten kann zum Schutz vor einem Datenverlust im Abrechnungsprozess eine bis zu 7-tägige Speicherung von Rohdaten angemessen sein. Bei festgestellten Verarbeitungsfehlern können diese Daten für eine korrekte Berechnung verwendet werden und sind dann zeitnah zu löschen.	Verkehrsdaten, insbesondere nicht oder nicht vollständig verarbeitete CDRs.

B. Internet

I. Echte Flatrate

1. Abrechnung mit Teilnehmer	Keine Rechtsgrundlage	Keine Speicherung	Keine Daten
2. Erkennung, Eingrenzung und Beseitigung von Störungen	§ 100 Abs. 1 TKG: Soweit erforderlich	Ohne konkreten Anlass ist eine Speicherung höchstens 7 Tage zulässig[5]. Sind konkrete Anhaltspunkte für eine Störung festgestellt worden, dürfen im Einzelfall die zum Eingrenzen und Beseitigen der vermuteten Störung erforderlichen Daten länger gespeichert werden. Darüber hinaus kann mit Statistiken oder anonymisierten Daten gearbeitet werden.	Alle erforderlichen Daten (z. B. IP-Adresse, DSL-Kennung, IMSI, Zeit, Datenmenge)
3. Aufdeckung von Missbrauch	§ 100 Abs. 3 TKG: Soweit erforderlich	Zum Aufdecken von Missbrauch kann nach § 100 Abs. 3 TKG auf Verkehrsdaten zurückgegriffen werden, die zulässigerweise zu anderen betrieblichen Zwecken gespeichert und nicht älter als 6 Monate sind. Ebenso können hierfür weitere Verkehrsdaten für bis zu 7 Tage verwendet, das heißt auch gespeichert werden. Die zur Aufklärung eines konkret festgestellten Missbrauchsverdachtes erforderlichen Verkehrsdaten dürfen bis zum Abschluss von dessen Bearbeitung verwendet werden.	Alle vorhandenen Verkehrsdaten

[5] Vgl. zur 7-Tage-Frist auch das Urteil des Bundesgerichtshofs vom 13.01.2011, Az: III ZR 146/10.

II. Volumenabrechnung oder Flatrate mit Drosselung			
1. Abrechnung mit Teilnehmer oder Begründung der Drosselung	§ 97 Abs. 3 Satz 2 TKG (siehe auch Verfügung der BNetzA Nr. 43/2010): Max. 6 Monate nach Rechnungsversand	In der Regel werden 3 Monate nach Rechnungsversand (s. auch Beanstandungsfrist in § 45i Abs. 1 TKG) als ausreichend angesehen. Wenn nachvollziehbare Gründe vorliegen, können die Daten länger gespeichert werden.	Nur bestimmte Daten dürfen gespeichert werden[6], z. B. Nutzerkennung, Datenvolumen, Zeit u. Dauer der Session, nicht aber IP-Adresse
2. Erkennung, Eingrenzung und Beseitigung von Störungen	§ 100 Abs. 1 TKG: Soweit erforderlich	Ohne konkreten Anlass ist eine Speicherung höchstens 7 Tage zulässig[7]. Sind konkrete Anhaltspunkte für eine Störung festgestellt worden, dürfen im Einzelfall die zum Eingrenzen und Beseitigen der vermuteten Störung erforderlichen Daten länger gespeichert werden. Darüber hinaus kann mit Statistiken oder anonymisierten Daten gearbeitet werden.	Alle erforderlichen Daten (s.o.)
3. Aufdeckung von Missbrauch	§ 100 Abs. 3 TKG: Soweit erforderlich	Zum Aufdecken von Missbrauch kann nach § 100 Abs. 3 TKG auf Verkehrsdaten zurückgegriffen werden, die zulässigerweise zu anderen betrieblichen Zwecken gespeichert und nicht älter als 6 Monate sind. Ebenso können hierfür weitere Verkehrsdaten für bis zu 7 Tage verwendet, das heißt auch gespeichert werden. Die zur Aufklärung eines konkret festgestellten Missbrauchsverdachtes erforderlichen Verkehrsdaten dürfen bis zum Abschluss von dessen Bearbeitung verwendet werden.	Alle vorhandenen Verkehrsdaten

[6] Konkrete Ausführungen zu den zu speichernden Daten finden sich unter Punkt 4.3 der Verfügung Nr. 43/2010 der Bundesnetzagentur.
[7] Vgl. zur 7-Tage-Frist auch das Urteil des Bundesgerichtshofs vom 13.01.2011, Az: III ZR 146/10.

C. E-Mail

Gemeint ist hier die klassische E-Mail, für Sonderformen wie De-Mail, E-Mail mit SMS-Bestätigung können andere Regelungen gelten, etwa vergleichbar mit SMS.

1. Abrechnung mit Teilnehmer	Keine Rechtsgrundlage	Keine Speicherung	Keine Daten
2. Erkennung, Eingrenzung und Beseitigung von Störungen	§ 100 Abs. 1 TKG: Soweit erforderlich	Ohne konkreten Anlass ist eine Speicherung höchstens 7 Tage zulässig[8]. Sind konkrete Anhaltspunkte für eine Störung festgestellt worden, dürfen im Einzelfall die zum Eingrenzen und Beseitigen der vermuteten Störung erforderlichen Daten länger gespeichert werden. Darüber hinaus kann mit Statistiken oder anonymisierten Daten gearbeitet werden.	Alle erforderlichen Daten (z. B. E-Mail-Adressen, IP-Adresse, Nutzerkennung, Zeit, Datenmenge), keine Inhalte (z. B. Betreff)
3. Aufdeckung von Missbrauch	§ 100 Abs. 3 TKG: Soweit erforderlich	Zum Aufdecken von Missbrauch kann nach § 100 Abs. 3 TKG auf Verkehrsdaten zurückgegriffen werden, die zulässigerweise zu anderen betrieblichen Zwecken gespeichert und nicht älter als 6 Monate sind. Ebenso können hierfür weitere Verkehrsdaten für bis zu 7 Tage verwendet, das heißt auch gespeichert werden. Die zur Aufklärung eines konkret festgestellten Missbrauchsverdachtes erforderlichen Verkehrsdaten dürfen bis zum Abschluss von dessen Bearbeitung verwendet werden.	Alle vorhandenen Verkehrsdaten

Anmerkung

Das TKG enthält keine gesonderte Speichererlaubnis für Zwecke der Strafverfolgung (insb. keine Vorratsdatenspeicherung). Für eine Auskunftserteilung auf Ersuchen von Sicherheitsbehörden mit Aufgaben im Bereich der Strafverfolgung, Gefahrenabwehr oder der Nachrichtendienste dürfen daher ausschließlich Daten verwendet werden, die aus betrieblichen Gründen im Sinne der obigen Auflistung rechtmäßig gespeichert sind. Sofern diese Daten doppelt in einem eigens für die Behördenauskünfte genutzten System als Kopie der betrieblich genutzten Daten gespeichert werden, wird dies vorläufig toleriert, wenn sichergestellt ist, dass die Löschung zeitgleich mit der Löschung im betrieblich genutzten System durchgeführt wird.

[8] Vgl. zur 7-Tage-Frist auch das Urteil des Bundesgerichtshofs vom 13.01.2011, Az: III ZR 146/10.