

## ENTSCHEIDUNGEN

### Eilanträge gegen das Vorratsdatenspeicherungsgesetz erfolglos

*BVerfG*, Beschl. v. 8.6.2016 – 1 BvQ 42/15\*

**Eine Aussetzung der durch §§ 113a, 113b TKG angeordneten Speicherpflicht von Telekommunikations-Verkehrsdaten scheidet aus. Auch hinsichtlich der Regelung zur Nutzung dieser Daten für bestimmte Anlässe der Strafverfolgung ist eine vorläufige Aussetzung der angegriffenen Vorschriften nicht geboten (Leitsatz der Schriftleitung).**

In dem Verfahren über den Antrag, im Wege der einstweiligen Anordnung die Art. 1 und 2 des Gesetzes zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten gemäß dem vom Deutschen Bundestag am 16. 10. 2015 verabschiedeten Gesetzentwurf der Fraktionen der CDU/CSU und SPD (BT-Drs. 18/5088) in der vom Ausschuss für Recht und Verbraucherschutz geänderten Fassung (BT-Drs. 18/6391) mit Wirkung von ihrem Inkrafttreten an außer Kraft zu setzen ... hat die 3. Kammer des Ersten Senats des *BVerfG* ... einstimmig beschlossen:

**Der Antrag auf Erlass einer einstweiligen Anordnung wird abgelehnt.**

#### Gründe:

##### A.

- 1 Die Beschwerdeführer begehren mit ihrem Eilantrag, die durch das Gesetz zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten vom 10. 12. 2015 (BGBl. I, S. 2218; im Folgenden: Vorratsdatenspeicherungsgesetz) eingeführte Vorratsspeicherung von Telekommunikations-Verkehrsdaten zu Zwecken der öffentlichen Sicherheit außer Kraft zu setzen.
- 2 I. 1. Ein Abruf von Telekommunikations-Verkehrsdaten - etwa gem. § 100g Abs. 1 StPO - hatte bisher nur dann Erfolg, wenn der ersuchte Diensteanbieter die Daten zu eigenen Zwecken gespeichert hatte, etwa gem. § 97 Telekommunikationsgesetz (im Folgenden: TKG) zur Entgeltmittlung und Entgeltabrechnung oder gem. § 100 TKG zur Feststellung, Eingrenzung und Beseitigung der Störung einer Telekommunikationsanlage. Tatsächlich ist es in erheblichem Umfang vom Zufall abhängig, welche Daten bei einer Abfrage nach § 100g StPO abgerufen werden können (vgl. BT-Drs. 18/5088, S. 21).

- 3 Das Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen vom 21. 12. 2007 (BGBl. I, S. 3198; im Folgenden: Gesetz zur Neuregelung der Telekommunikationsüberwachung), das in Umsetzung der Richtlinie 2006/24/EG des Europäischen Parlaments und des Rates vom 15.3.2006 über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste oder öffentlicher Kommunikationsnetze erzeugt oder verarbeitet werden, und zur Änderung der Richtlinie 2002/58/EG (ABl Nr. L 105 vom 13.4.2006, S. 54; im Folgenden: Richtlinie 2006/24/EG), erlassen wurde, sollte dem durch eine vorsorgliche Speicherpflicht der Telekommunikations-Verkehrsdaten durch die Diensteanbieter entgegenwirken. Es ist aus verfassungsrechtlichen Gründen nicht wirksam geworden. Mit Beschluss vom 11.3.2008 hat der *Erste Senat* des *BVerfG* dem Antrag auf einstweilige Anordnung gegen das Gesetz teilweise stattgegeben (vgl. BVerfGE 121, 1 [19 ff.]) und mit Urteil vom 2.3.2010 die §§ 113a und 113b TKG sowie § 100g Abs. 1 S. 1 StPO, soweit danach Verkehrsdaten nach § 113a TKG erhoben werden durften, in der Fassung des Gesetzes zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG vom 21.12.2007 (BGBl. I, S. 3198), wegen Verstoßes gegen Art. 10 Abs. 1 GG für nichtig erklärt (vgl. BVerfGE 125, 260 [262 f., 307 ff.]). Die *Große Kammer* des *EuGH* erklärte mit Urteil vom 8. April 2014 auf Vorabentscheidungsersuchen des Irischen High Court und des Österreichischen Verfassungsgerichtshofs dann auch die Richtlinie 2006/24/EG für ungültig, weil der Unionsgesetzgeber beim Erlass der Richtlinie die Grenzen überschritten habe, die er zur Wahrung des Grundsatzes der Verhältnismäßigkeit im Hinblick auf die Art. 7, 8 und 52 der Europäischen Grundrechtecharta (GRCh) einhalten musste (vgl. *EuGH*, Urt. v. 8.4.2014 - C-293/12, C-594/12, NJW 2014, S. 2169 [2173]).

- 4 2. Das im vorliegenden Verfahren angegriffene Gesetz zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten dient nach der Gesetzesbegründung erneut der Vereinheitlichung der Speicherpraxis der Erbringer öffentlich zugänglicher Telekommunikationsdienste. Es soll Unzulänglichkeiten in der Strafverfolgungsvorsorge und der Gefahrenabwehr beseitigen (vgl. BT-Drs. 18/5088, S. 21 f.). Zu diesem Zweck enthält sein Art. 1 Änderungen der Strafprozessordnung und sein Art. 2 Änderungen des Telekommunikationsgesetzes. Die

\* Vom Abdruck des von den Gründen insoweit identischen Beschl. v. 8.6.2016 – 1 BvR 229/16 wurde abgesehen.

von den Beschwerdeführern angegriffenen Regelungen zur Vorratsspeicherung von Telekommunikations-Verkehrsdaten finden sich in den neu geschaffenen §§ 113a bis 113g TKG, die angegriffenen Regelungen über die Erhebung der Verkehrsdaten durch die Strafverfolgungsbehörden und das dabei zu beachtende Verfahren finden sich in dem neu gefassten § 100g StPO und den neu geschaffenen §§ 101a und 101b StPO.

- 5 § 113a Abs. 1 TKG bestimmt mit den Anbietern öffentlich zugänglicher Telekommunikationsdienste für Endnutzer den Verpflichteten der Vorratsdatenspeicherung. § 113b TKG verpflichtet die Anbieter öffentlich zugänglicher Telekommunikationsdienste für Endnutzer sodann, bestimmte einzeln aufgeführte Verkehrs- und Standortdaten unabhängig von einem besonderen Anlass für einen bestimmten Zeitraum zu speichern und für die Nutzung durch Sicherheitsbehörden bereitzuhalten. Verkehrsdaten im Sinne des § 113b Abs. 2 und 3 TKG (z.B. Rufnummern, Datum und Uhrzeit von Beginn und Ende der Verbindung, Internetprotokoll-Adressen) müssen gem. § 113b Abs. 1 Nr. 1 TKG für zehn Wochen gespeichert werden; die Speicherpflicht für Standortdaten nach § 113b Abs. 4 TKG (z.B. die Bezeichnungen der Funkzellen bei der Nutzung mobiler Telefondienste) beträgt demgegenüber vier Wochen (vgl. § 113b Abs. 1 Nr. 2 TKG). Der Inhalt der Kommunikation, Daten über aufgerufene Internetseiten und Daten von Diensten der elektronischen Post dürfen auf Grund dieser Vorschrift nicht gespeichert werden (vgl. § 113b Abs. 5 TKG). Das Gleiche gilt gem. § 113b Abs. 6 S. 1 TKG für Daten, die den in § 99 Abs. 2 TKG genannten Verbindungen zu Anschlüssen von Personen, Behörden und Organisationen in sozialen oder kirchlichen Bereichen zugrunde liegen.
- 6 Die Speicherung der Daten hat allgemein so zu erfolgen, dass Auskunftersuchen der berechtigten Stellen unverzüglich beantwortet werden können (vgl. § 113b Abs. 7 TKG). Nach § 113b Abs. 8 TKG hat der nach § 113a Abs. 1 TKG Verpflichtete die gespeicherten Daten unverzüglich, spätestens jedoch binnen einer Woche nach Ablauf der Speicherfristen nach § 113b Abs. 1 TKG, irreversibel zu löschen oder die irreversible Löschung sicherzustellen. In § 113c TKG werden abschließend (vgl. § 113c Abs. 2 TKG) die zulässigen Verwendungszwecke der nach § 113b TKG gespeicherten Daten normiert. So dürfen etwa gespeicherte Daten an eine Strafverfolgungsbehörde übermittelt werden, soweit diese die Übermittlung unter Berufung auf eine gesetzliche Bestimmung, die ihr eine Erhebung der in § 113b TKG genannten Daten zur Verfolgung besonders schwerer Straftaten erlaubt, verlangt. Die Daten sind dabei so zu kennzeichnen, dass erkennbar ist, dass es sich um Daten handelt, die nach § 113b TKG gespeichert waren (vgl. § 113c Abs. 3 S. 2 TKG). Ob die Behörden berechtigt sind, ein Verlangen i.S.d. § 113c TKG an den Erbringer öffentlich zugänglicher Telekommunikationsdienste zu richten, ist nicht Regelungsgegenstand von § 113c TKG, sondern bestimmt sich nach den für die Strafverfolgungs- und Gefahrenabwehrbehörden jeweils maßgeblichen Regelungen des Fachrechts (vgl. BT Drs. 18/5088, S. 40). Jedoch liegt in der Norm die grundlegende Bestimmung, für welche Zwecke die Daten

verwendet werden dürfen. Sie befreit diesbezüglich die Telekommunikationsunternehmen von ihrer im Übrigen geltenden Geheimhaltungspflicht (vgl. entsprechend zur damaligen Regelung BVerfGE 125, 260 [312]). § 113d TKG sieht sodann näher bestimmte Anforderungen an die Gewährleistung der Datensicherheit vor. Der nach § 113a Abs. 1 TKG Verpflichtete hat gem. § 113e TKG sicherzustellen, dass für Zwecke der Datenschutzkontrolle jeder Zugriff, insbesondere das Lesen, Kopieren, Ändern, Löschen und Sperren der gespeicherten Daten protokolliert wird und die Protokolldaten (Zeitpunkt des Zugriffs, zugreifende Personen, Zweck und Art des Zugriffs) nach einem Jahr gelöscht werden. Gem. § 113f Abs. 1 TKG ist seitens der Bundesnetzagentur ein Anforderungskatalog zur Gewährleistung eines besonders hohen Standards der Datensicherheit und Datenqualität zu erstellen. Die Regelung des § 113g TKG ergänzt die Vorschrift des § 109 Abs. 4 TKG und verlangt die Aufnahme spezifischer Schutzmaßnahmen in das zu erstellende Sicherheitskonzept.

- 7 § 100g StPO regelt die Voraussetzungen für die Erhebung von Verkehrsdaten. Während in Absatz 1 die Erhebung von Verkehrsdaten geregelt wird, die aus geschäftlichen Gründen bei den Erbringern öffentlich zugänglicher Telekommunikationsdienste gespeichert werden (§ 96 TKG), legt Absatz 2 fest, unter welchen Voraussetzungen die nunmehr durch die neue Speicherpflicht gespeicherten Daten erhoben werden dürfen: Es bedarf danach den durch bestimmte Tatsachen begründeten Verdacht einer in § 100g Abs. 2 S. 2 StPO enumerativ und abschließend (vgl. BT Drs. 18/5088, S. 31) aufgeführten besonders schweren Straftat, die auch im Einzelfall besonders schwer wiegt. Darüber hinaus muss die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes des Beschuldigten auf andere Weise wesentlich erschwert oder aussichtslos sein und die Erhebung der Daten in einem angemessenen Verhältnis zur Bedeutung der Sache stehen. § 100g Abs. 4 StPO schließt zum Schutz von Berufsgeheimnisträgern i.S.d. § 53 Abs. 1 S. 1 Nrn. 1 bis 5 StPO die Erhebung von Verkehrsdaten nach § 100g Abs. 2 StPO aus. § 101a StPO überträgt den Richtervorbehalt des § 100b Abs. 1 StPO auf die Erhebung von Verkehrsdaten nach § 100g StPO und stellt konkrete Anforderungen an die Gestaltung der Entscheidungsformel und die Begründung des Beschlusses, die einzelfallbezogen sein muss und die wesentlichen Erwägungen zu der Erforderlichkeit und Angemessenheit der Maßnahme darzulegen hat (vgl. § 101a Abs. 2 StPO). § 101a Abs. 6 StPO sieht eine Pflicht zur Benachrichtigung der Beteiligten der betroffenen Telekommunikation nach Maßgabe des § 101 Abs. 4 S. 2 bis 5 und Abs. 5 bis 7 StPO vor. Die Regelung des § 101b StPO sieht schließlich nähere Vorgaben zur statistischen Erfassung der Erhebung von Verkehrsdaten vor.
- 8 II. Die Beschwerdeführer zu 1) bis 3), 5) und zu 7) bis 22) nutzen als Rechtsanwälte, Ärzte, Journalisten und/oder Mitglieder des Bundestages beziehungsweise des Berliner Abgeordnetenhauses privat und geschäftlich verschiedene Telekommunikationsdienste wie Festnetzanschlüsse, Mo-

biltelefone, Internetzugangsdienste und E-Mail-Postfächer. Der Beschwerdeführer zu 4) ist ein Medienverband, der Beschwerdeführer zu 6) ein Landesjournalistenverband.

- 9 Die Beschwerdeführer sind der Ansicht, der Antrag auf Erlass einer einstweiligen Anordnung sei bereits deshalb begründet, weil die mit der Verfassungsbeschwerde angegriffenen Normen offensichtlich gegen das Grundgesetz verstießen. Die Vorgaben des *BVerfG* aus seiner Entscheidung vom 2.3.2010 (vgl. BVerfGE 125, 260 ff.) würden auch bei der Neuregelung der Vorratsdatenspeicherung nicht erfüllt. Schon die Eignung der Vorratsdatenspeicherung sei zweifelhaft, da belastbares Zahlenmaterial, aus dem sich eine Verbesserung der Aufklärungsquote bei der Strafverfolgung ablesen lasse, nicht existiere. Soweit beim Short Message Service (SMS) technisch bedingt nicht nur die Verkehrsdaten, sondern auch die Kommunikationsinhalte im Wege des sogenannten Mitloggens notwendigerweise mitgespeichert würden, sei dies offensichtlich mit dem Grundgesetz nicht vereinbar. Auch der im Gesetz vorgesehene Richtervorbehalt entspreche nicht den Vorgaben des *BVerfG*; das Gesetz stelle keine Anforderungen an eine den technischen Schwierigkeiten und der Belastung der Richter Rechnung tragende Justizorganisation. Der Schutz für Berufsheimnisträger sei unvollkommen, da die sie betreffenden Daten auch dann gespeichert würden, wenn sie voraussichtlich Erkenntnisse erbringen, über die der Berufsheimnisträger gem. § 53 Abs. 1 S. 1 Nrn. 1 bis 5 StPO das Zeugnis verweigern dürfe; der Ausschluss der Erhebung solcher Daten nach § 100g Abs. 4 StPO sei nicht ausreichend. Auch würden zwingende Vorgaben aus der Entscheidung des *EuGH* vom 8.4.2014 (NJW 2014, S. 2169 ff.) nicht erfüllt, wonach eine Vorratsdatenspeicherung nicht anlass-, zusammenhangs- und nahezu ausnahmslos erfolgen dürfe. Die angegriffenen Vorschriften verstießen insofern gegen die Unionsgrundrechte aus Art. 7, 8, 11, 15 und 20 GRCh. Der deutsche Gesetzgeber sei vorliegend gem. Art. 51 Abs. 1 GRCh an die Unionsgrundrechte gebunden, denn es gehe bei der Einführung der Vorratsdatenspeicherung um die Durchführung der Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12.7.2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (ABl Nr. L 201 vom 31.7.2002, S. 37; im Folgenden: Richtlinie 2002/58/EG).
- 10 Das *BVerfG* sei im Rahmen der Folgenabwägung zur Aussetzung des Gesetzes verfassungs- und unionsrechtlich verpflichtet. Die Speicherung der Verbindungsdaten führe zu schweren, irreversiblen Nachteilen. Die angegriffenen Regelungen entfalteten einen erheblichen Einschüchterungseffekt. Ein überwiegendes Interesse am Vollzug der streitgegenständlichen Normen scheidet schon deshalb aus, weil der Gesetzgeber seit der Nichtigerklärung der Vorschriften über die Vorratsdatenspeicherung durch das *BVerfG* im Jahr 2010 mehr als fünf Jahre zugewartet habe, bis er eine neue Regelung erlassen habe. Sollte das *BVerfG* der Auffassung sein, dass sich aus der Entscheidung des *EuGH* vom 8.4.2014 (NJW 2014, S. 2169 ff.) nicht mit hinreichender Klarheit ergebe, dass die angegriffenen Vorschriften gegen Unionsrecht verstießen, sei das Verfahren zur effektiven Durchsetzung des Unionsrechts auszusetzen und ein Vorabentscheidungsverfahren nach Art. 267 AEUV durchzuführen.
- 11 **B.** Der Antrag auf Erlass einer einstweiligen Anordnung ist abzulehnen.
- 12 Nach § 32 Abs. 1 BVerfGG kann das *BVerfG* im Streitfall einen Zustand durch einstweilige Anordnung vorläufig regeln, wenn dies zur Abwehr schwerer Nachteile, zur Verhinderung drohender Gewalt oder aus einem anderen wichtigen Grund zum gemeinen Wohl dringend geboten ist. Dabei haben die Gründe, die für die Verfassungswidrigkeit des angegriffenen Hoheitsakts vorgetragen werden, grundsätzlich außer Betracht zu bleiben, es sei denn, die Verfassungsbeschwerde erweise sich von vornherein als unzulässig oder offensichtlich unbegründet (vgl. BVerfGE 112, 284 [291]; 121, 1 (14 f.); st. Rspr.). Dies lässt sich vorliegend nicht in der für das Eilverfahren gebotenen Kürze der Zeit klären. Über den Antrag auf einstweilige Anordnung ist deshalb nach Maßgabe einer Folgenabwägung zu entscheiden. Danach sind die Folgen, die eintreten würden, wenn die einstweilige Anordnung nicht erginge, die Verfassungsbeschwerde später aber Erfolg hätte, gegen die Nachteile abzuwägen, die entstünden, wenn die begehrte einstweilige Anordnung erlassen würde, der Verfassungsbeschwerde aber der Erfolg zu versagen wäre (vgl. BVerfGE 117, 126 [135]; 121, 1 [17]; st. Rspr.). Diese Abwägung fällt zu Ungunsten der Beschwerdeführer aus.
- 13 1. Wird die Aussetzung des Vollzugs eines Gesetzes begehrt, ist bei der Folgenabwägung ein besonders strenger Maßstab anzulegen (vgl. BVerfGE 3, 41 [44]; 104, 51 [55]; 112, 284 [292]; 121, 1 [17]; st. Rspr.). Das *BVerfG* darf von seiner Befugnis, den Vollzug eines in Kraft getretenen Gesetzes auszusetzen, nur mit größter Zurückhaltung Gebrauch machen, da der Erlass einer solchen einstweiligen Anordnung stets ein erheblicher Eingriff in die Gestaltungsfreiheit des Gesetzgebers ist (vgl. BVerfGE 64, 67 [69]; 117, 126 [135]; 121, 1 [17]; *BVerfG*, Beschl. v. 6.10.2015 - 1 BvR 1571/15 u.a., www.bverfg.de, Rn. 13). Müssen die für eine vorläufige Regelung sprechenden Gründe schon im Regelfall so schwer wiegen, dass sie den Erlass einer einstweiligen Anordnung unabdingbar machen, so müssen sie im Fall der begehrten Außervollsetzung eines Gesetzes darüber hinaus besonderes Gewicht haben (vgl. BVerfGE 104, 23 [27 f.]; 117, 126 [135]; 122, 342 [361 f.]; st. Rspr.). Insoweit ist von entscheidender Bedeutung, ob die Nachteile irreversibel oder nur sehr erschwert revidierbar sind (vgl. BVerfGE 91, 70 [76 f.]; 118, 111 [123]; *BVerfG*, Beschl. v. 6.10.2015 - 1 BvR 1571/15 u.a., www.bverfg.de, Rn. 13), um das Aussetzungsinteresse durchschlagen zu lassen.
- 14 2. Nach diesen Maßstäben war der Antrag auf Erlass einer einstweiligen Anordnung abzulehnen. Eine Aussetzung der durch §§ 113a, 113b TKG angeordneten Speicherpflicht von Telekommunikations-Verkehrsdaten scheidet

- aus (a). Auch hinsichtlich der Regelung zur Nutzung dieser Daten für bestimmte Anlässe der Strafverfolgung ist eine vorläufige Aussetzung der angegriffenen Vorschriften nicht geboten (b).
- 15 a) Eine Aussetzung des Vollzugs von §§ 113a, 113b TKG scheidet aus.
- 16 Ein besonders schwerwiegender und irreparabler Nachteil, der es rechtfertigen könnte, den Vollzug der Norm ausnahmsweise im Wege einer einstweiligen Anordnung auszusetzen, liegt in der Datenspeicherung allein nicht.
- 17 Zwar kann die gegenüber den Verpflichteten nach § 113a TKG in § 113b TKG angeordnete umfassende und anlasslose Bevorratung sensibler Daten über praktisch jedermann für staatliche Zwecke, die sich zum Zeitpunkt der Speicherung der Daten nicht im Einzelnen absehen lassen, einen erheblichen Einschüchterungseffekt bewirken, weil das Gefühl entsteht, ständig überwacht zu werden. Dieser Effekt ließe sich für die Zeit zwischen dem Inkrafttreten der Norm und der Entscheidung des *BVerfG* selbst dann nicht rückgängig machen, wenn die Verfassungsbeschwerde in der Hauptsache Erfolg haben sollte.
- 18 Der in der Speicherung für Einzelne liegende Nachteil für ihre Freiheit und Privatheit verdichtet und konkretisiert sich jedoch erst durch einen Abruf der Daten zu einer möglicherweise irreparablen Beeinträchtigung. Die Datenbevorratung ermöglicht zwar den Abruf, doch führt erst dieser zu konkreten Belastungen. Das Gewicht eines denkbaren Einschüchterungseffekts hängt dann davon ab, unter welchen Voraussetzungen die bevorrateten Daten abgerufen und verwertet werden können. Je weiter die Befugnisse staatlicher Stellen insoweit reichen, desto eher müssen die Bürgerinnen und Bürger befürchten, dass diese Stellen ihr Kommunikationsverhalten überwachen (vgl. BVerfGE 121, 1 [20]). So ist mit der Speicherung allein jedoch noch kein derart schwerwiegender Nachteil verbunden, dass er die Außerkraftsetzung eines Gesetzes erforderte. Dies gilt auch für die Speicherung der Daten von Berufsgeheimnisträgern.
- 19 Ein die Aussetzung der Speicherpflicht erfordernder besonders schwerer Nachteil ergibt sich auch nicht daraus, dass beim Short Message Service (SMS) Verkehrsdaten und Kommunikationsinhalte möglicherweise nicht getrennt werden können. Nach dem klaren Wortlaut des § 113b Abs. 5 TKG dürfen der Inhalt der Kommunikation, Daten über aufgerufene Internetseiten und Daten von Diensten der elektronischen Post auf Grund dieser Vorschrift nicht gespeichert werden. Die angegriffene gesetzliche Regelung schließt damit ein technisch bedingtes „Mitloggen“ von Kommunikationsinhalten aus. Wenn dies technisch zurzeit noch nicht möglich sein sollte, rechtfertigt das nicht, sich über die Maßgabe des Gesetzes hinwegzusetzen; vielmehr sind dann zunächst die technischen Bedingungen zu schaffen, um die Speicherpflicht erfüllen zu können.
- 20 b) Eine Aussetzung des Vollzugs ist auch nicht hinsichtlich der §§ 100g, 101a und 101b StPO geboten.
- 21 aa) Allerdings liegt in dem Verkehrsdatenabruf nach § 100g Abs. 1 und 2 StPO ein schwerwiegender und nicht mehr rückgängig zu machender Eingriff in das Grundrecht aus Art. 10 Abs. 1 GG. Ein solcher Datenabruf ermöglicht es, weitreichende Erkenntnisse über das Kommunikationsverhalten und die sozialen Kontakte der Betroffenen zu erlangen, gegebenenfalls sogar begrenzte Rückschlüsse auf die Gesprächsinhalte zu ziehen. Zudem weist ein Verkehrsdatenabruf eine erhebliche Streubreite auf, da er neben der Zielperson des Auskunftersuchens notwendigerweise deren Kommunikationspartner erfasst, also vielfach Personen, die in keiner Beziehung zu dem Tatvorwurf stehen und den Eingriff in ihr Grundrecht aus Art. 10 Abs. 1 GG durch ihr Verhalten nicht veranlasst haben (vgl. BVerfGE 107, 299 [318 ff.]; 121, 1 [22]).
- 22 Doch hat der Gesetzgeber mit § 100g Abs. 2 StPO den Abruf von Telekommunikations-Verkehrsdaten i.S.d. § 113b TKG von qualifizierten Voraussetzungen abhängig gemacht, die das Gewicht der dem Einzelnen und der Allgemeinheit durch den Vollzug der Vorschrift drohenden Nachteile für die Übergangszeit bis zur Entscheidung über die Hauptsache hinnehmbar und im Vergleich mit den Nachteilen für das öffentliche Interesse an einer effektiven Strafverfolgung weniger gewichtig erscheinen lassen.
- 23 Maßgeblich ist hierfür die Gewichtung, die auch der Entscheidung des *BVerfG* über den Antrag auf einstweilige Anordnung gegen das Gesetz zur Neuregelung der Telekommunikationsüberwachung vom 21.12.2007 zugrunde lag (vgl. BVerfGE 121, 1 [23 f.]). Das *BVerfG* hatte dort wegen des öffentlichen Gewichts einer wirksamen Verfolgung schwerer Straftaten solche Abrufersuchen zugelassen, die der Verfolgung von Katalogtaten i.S.d. § 100a Abs. 2 StPO dienen, wenn darüber hinaus auch die Voraussetzungen des § 100a Abs. 1 StPO vorlagen, namentlich die Tat auch im Einzelfall schwer wog und die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes des Beschuldigten auf andere Weise wesentlich erschwert oder aussichtslos gewesen wäre.
- 24 Diese Voraussetzungen ergeben sich nunmehr unmittelbar aus § 100g Abs. 2 S. 1 StPO. Danach muss ein auf bestimmte Tatsachen gestützter Verdacht einer besonders schweren Straftat vorliegen, die auch im Einzelfall besonders schwer wiegt. Nach § 100g Abs. 2 S. 1 StPO muss die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes der Beschuldigten darüber hinaus auf andere Weise wesentlich erschwert oder aussichtslos sein und die Erhebung der Daten in einem angemessenen Verhältnis zur Bedeutung der Sache stehen. Daneben steht ein abschließender Katalog besonders schwerer, zur Erhebung von Verkehrsdaten ermächtigender Straftaten als Teilmenge (vgl. BT-Drs. 18/5088, S. 32) der in § 100a Abs. 2 StPO aufgeführten Katalogtaten. Sie begegnen für sich genommen keinen durchgreifenden verfassungsrechtlichen Bedenken gegen die Klassifizierung als Straf-

taten für Maßnahmen der Telekommunikationsüberwachung (vgl. BVerfGE 129, 208 [241 f.]). Sie können vielmehr als Leitlinie dafür gelten, welche Straftaten der Gesetzgeber als so schwerwiegend bewertet, dass sie auch gewichtige Eingriffe in das Grundrecht aus Art. 10 Abs. 1 GG rechtfertigen können (vgl. BVerfGE 121, 1 [25]). Der Gesetzgeber hat den Katalog in § 100g Abs. 2 S. 2 StPO damit auf solche Straftaten reduziert, die der Bekämpfung des Terrorismus oder dem Schutz höchstpersönlicher Rechtsgüter, insbesondere Leib, Leben, Freiheit und sexuelle Selbstbestimmung, dienen. Außerdem sollen besonders schwere Straftaten umfasst sein, bei denen die gespeicherten Verkehrsdaten nach kriminalistischer Erfahrung besonders wertvolle Dienste leisten können (vgl. BT-Drs. 18/5088, S. 32). Im Unterschied zu dem Katalog in § 100a Abs. 2 StPO bilden etwa bestimmte Vermögensdelikte (z.B. §§ 263, 263a, 264 StGB) keine tauglichen Anlasstaten für eine Vorratsdatenspeicherung. Angesichts dieser Einschränkungen hat das öffentliche Strafverfolgungsinteresse grundsätzlich derartiges Gewicht, dass die Aussetzung der Vorschrift durch eine einstweilige Anordnung trotz der entgegenstehenden gewichtigen Nachteile nicht geboten ist.

- 25 bb) Auch in Blick auf §§ 101a, 101b StPO ist eine einstweilige Anordnung, nicht geboten. Gem. § 101a Abs. 1 S. 1 i.V.m. § 100b Abs. 1 S. 1 StPO steht die Erhebung von Verkehrsdaten nach § 100g StPO grundsätzlich unter

Richtervorbehalt; nach § 101a Abs. 1 S. 2 StPO findet zudem in den Fällen des § 100g Abs. 2 StPO (Erhebung von Verkehrsdaten im Sinne des § 113b Abs. 1 TKG) § 100b Abs. 1 Satz 2 und 3 StPO keine Anwendung, sodass die Staatsanwaltschaft auch bei Gefahr im Verzug die Anordnung nicht selbst treffen kann. § 101a Abs. 1 Satz 1 StPO stellt zudem spezifische Anforderungen an die Begründung einer solchen Entscheidung. Ob der Gesetzgeber mit diesen Vorgaben den verfassungsrechtlichen Anforderungen im Einzelnen gerecht geworden ist, ist im Verfahren des Eilrechtsschutzes nicht abschließend zu klären. Jedemfalls ergibt sich aus der vorübergehenden Geltung dieser Vorschriften kein besonders schwerer Nachteil, der im Rahmen der hier gebotenen Folgenabwägung eine Aussetzung des Vollzugs der angegriffenen Vorschriften verlangte.

- 26 c) Ob und gegebenenfalls in welcher Weise die Europäische Grundrechtecharta oder sonstiges Unionsrecht für die Beurteilung der angegriffenen Vorschriften Bedeutung entfaltet, ist im Hauptsacheverfahren zu entscheiden. Dass Unionsrecht dazu verpflichten könnte, die angegriffenen Vorschriften schon im Eilverfahren im Wege der einstweiligen Anordnung außer Kraft zu setzen, ist weder substantiiert vorgetragen noch ersichtlich.
- 27 Diese Entscheidung ist unanfechtbar.