

Nichtamtliche Übersetzung des Bundesministeriums der Justiz und für
Verbraucherschutz

EUROPÄISCHER GERICHTSHOF FÜR MENSCHENRECHTE

FÜNFTE SEKTION

RECHTSSACHE B. ./ DEUTSCHLAND
(Individualbeschwerde Nr. 50001/12)

URTEIL

Artikel 8 • Achtung des Privatlebens • gesetzliche Verpflichtung von Diensteanbietern, personenbezogene Daten von Nutzern* von Prepaid-Mobilfunkkarten zu speichern und den Behörden auf Verlangen zur Verfügung zu stellen • Eingriff betreffend einen begrenzten Datensatz • Datenabruf durch Behörden von angemessenen Schutzvorkehrungen begleitet • beanstandete Speicherung in Bezug auf die legitimen Ziele der nationalen Sicherheit und Kriminalitätsbekämpfung verhältnismäßig

STRASSBURG

30. Januar 2020

*Dieses Urteil wird nach Maßgabe des Artikels 44 Abs. 2 der Konvention endgültig.
Es wird gegebenenfalls noch redaktionell überarbeitet.*

* In dieser Übersetzung umfassen Personenbezeichnungen im Sinne der Gleichbehandlung grundsätzlich alle Geschlechter, es sei denn, sie beziehen sich spezifisch auf einzelne Personen.

In der Rechtssache B. ./ Deutschland

verkündet der Europäische Gerichtshof für Menschenrechte (Fünfte Sektion) als Kammer mit den *Richterinnen* und *Richtern*

Yonko Grozev, *Präsident*,

Angelika Nußberger,

Síofra O’Leary,

Carlo Ranzoni,

Mārtiņš Mits,

Lətif Hüseyinov,

Lado Chanturia

sowie Claudia Westerdiek, *Sektionskanzlerin*,

nach nicht öffentlicher Beratung am 3. Dezember 2019

das folgende, an diesem Tag gefällte Urteil:

VERFAHREN

1. Der Rechtssache lag eine Individualbeschwerde (Nr. 50001/12) gegen die Bundesrepublik Deutschland zugrunde, die zwei deutsche Staatsangehörige, Herr P. B. und Herr J. B. („die Beschwerdeführer“), am 27. Juli 2012 nach Artikel 34 der Konvention zum Schutz der Menschenrechte und Grundfreiheiten („die Konvention“) beim Gerichtshof eingereicht hatten.

2. Die deutsche Regierung („die Regierung“) wurde durch ihre Verfahrensbevollmächtigten, Herrn H.-J. Behrens und Frau K. Behr vom Bundesministerium der Justiz und für Verbraucherschutz, vertreten.

3. Die Beschwerdeführer rügten unter Berufung auf die Artikel 8 und 10, aufgrund der gesetzlichen Verpflichtung aus § 111 Telekommunikationsgesetz (TKG) seien von ihnen als Nutzer von Prepaid-Mobilfunkkarten bestimmte personenbezogene Daten durch ihre jeweiligen Diensteanbieter gespeichert worden.

4. Am 21. März 2016 wurde die Beschwerde der Regierung zur Kenntnis gebracht.

5. Es gingen schriftliche Stellungnahmen von Privacy International und ARTICLE 19 ein, die vom Vizepräsidenten ermächtigt worden waren, sich als Drittparteien am Verfahren zu beteiligen (Artikel 36 Abs. 2 der Konvention und Artikel 44 Abs. 2 der Verfahrensordnung des Gerichtshofs).

SACHVERHALT

I. DIE UMSTÄNDE DER RECHTSSACHE

A. Der Hintergrund der Rechtssache

6. Die 19.. bzw. 19.. geborenen Beschwerdeführer leben in W.. Beide Beschwerdeführer waren in einer Bürgerrechtsorganisation aktiv, die gegen die allgemeine Vorratsdatenspeicherung von Telekommunikationsdaten eintrat. In diesem Zusammenhang organisierten beide Beschwerdeführer öffentliche Proteste und veröffentlichten Artikel, in denen die staatliche Überwachung kritisiert wurde. Der erste Beschwerdeführer war zudem Mitglied eines Landtags.

7. Im Juni 2004 wurde durch Änderungen des Telekommunikationsgesetzes eine gesetzliche Verpflichtung für Telekommunikationsanbieter eingeführt, personenbezogene Daten aller ihrer Kunden zu speichern, insbesondere auch von Kunden, bei denen diese Daten für Abrechnungszwecke oder aus sonstigen vertraglichen Gründen nicht erforderlich sind (Prepaid-Mobilfunkkarten („pay as you go“)). Bis zum Inkrafttreten dieser Änderungen waren Telekommunikationsdiensteanbieter nur berechtigt, die für das Vertragsverhältnis erforderlichen Daten zu erheben und zu speichern. Bei Prepaid-Mobilfunkkarten wurden solche Daten nicht für erforderlich gehalten. Die Änderungen erfolgten im Rahmen einer grundlegenden Überarbeitung des Telekommunikationsgesetzes, die nach dem Erlass (am 7. März bzw. 12. Juli 2002) von fünf EU-Richtlinien geboten schien, die bis Juli bzw. Oktober 2003 in deutsches Recht umgesetzt werden mussten.

8. Beide Beschwerdeführer nutzen Prepaid-Mobilfunkkarten und mussten bei der Aktivierung dieser SIM-Karten gemäß § 111 TKG bestimmte persönliche Daten bei ihrem jeweiligen Diensteanbieter angeben.

B. Verfahren vor dem Bundesverfassungsgericht

9. Am 13. Juli 2005 erhoben die Beschwerdeführer Verfassungsbeschwerden gegen verschiedene Vorschriften, u. a. die §§ 111, 112 und 113 TKG. Mit § 111 TKG wurde die Verpflichtung zur Erhebung und Speicherung der Rufnummern, des Namens, der Anschrift und des Geburtsdatums des Anschlussinhabers sowie des Datums des Vertragsbeginns eingeführt (siehe Rdnrn. 27-28). Die §§ 112 und 113 TKG beinhalteten ein automatisiertes und ein manuelles Verfahren zum Zugriff auf die nach § 111 TKG gespeicherten Daten (siehe Rdnrn. 29 und 31). Die Beschwerdeführer machten geltend, durch die genannten Vorschriften in ihrem Recht auf das Brief-, Post- und Fernmeldegeheimnis und in ihrem

Recht auf informationelle Selbstbestimmung verletzt worden zu sein (siehe Rdnr. 25).

10. § 111 TKG wurde durch ein Gesetz vom 21. Dezember 2007 geändert, mit dem die Verpflichtung zur Speicherung von Teilnehmerdaten auf andere Anschlusskennungen erstreckt wurde und für Fälle, in denen neben dem Mobilfunkanschluss auch ein Mobilfunkendgerät zur Verfügung gestellt wird, die zu speichernden Daten um die entsprechende Gerätenummer ergänzt wurden.

11. Die Beschwerdeführer erweiterten ihre anhängige Verfassungsbeschwerde um die geänderte Fassung des Telekommunikationsgesetzes. Deshalb berücksichtigte das Bundesverfassungsgericht in seinem Urteil das Telekommunikationsgesetz in der am 1. Januar 2008 geltenden Fassung.

C. Entscheidung des Bundesverfassungsgerichts (1 BvR 1299/05)

12. Am 24. Januar 2012 entschied das Bundesverfassungsgericht, soweit für die vorliegende Rechtssache maßgeblich, dass die §§ 111 und 112 TKG mit dem Grundgesetz (GG) vereinbar seien, dass § 113 Abs. 1 TKG in verfassungskonformer Auslegung mit dem Grundgesetz vereinbar sei und dass die §§ 112 und 113 TKG für den Abruf von Daten durch die darin genannten oder in Bezug genommenen Behörden eigene Ermächtigungsgrundlagen voraussetzten (siehe Rdrrn. 29 und 31). Bezüglich der Teile der Verfassungsbeschwerde, die nicht Gegenstand des vorliegenden Verfahrens sind, befand das Bundesverfassungsgericht, dass das manuelle Auskunftsverfahren gemäß § 113 Abs. 1 TKG nicht zur Zuordnung dynamischer IP-Adressen angewendet werden dürfe und dass die Sicherheitsbehörden Auskünfte über Zugangssicherungs-codes gemäß § 113 Abs. 1 TKG nur dann verlangen dürften, wenn die gesetzlichen Voraussetzungen für ihre Nutzung gegeben seien.

13. Es wies ferner darauf hin, dass das automatisierte Auskunftsverfahren gemäß § 112 TKG der Regierung zufolge von besonderer Bedeutung sei. Wie die Erfahrung gezeigt habe, liege die Zahl der manuellen Abrufe im Verfahren nach § 113 TKG zwischen 3 % und 5 % der Zahl der automatisierten Ersuchen nach § 112 TKG.

14. Bezüglich der hier relevanten Teile der Verfassungsbeschwerde der Beschwerdeführer stellte das Bundesverfassungsgericht zunächst fest, dass die beanstandeten Vorschriften in das Recht auf informationelle Selbstbestimmung eingriffen. Ferner führte es Folgendes aus (Verweise auf die Rechtsprechung des Bundesverfassungsgerichts werden in den nachfolgend zitierten Passagen ausgelassen):

„122. a) Das Recht auf informationelle Selbstbestimmung trägt Gefährdungen und Verletzungen der Persönlichkeit Rechnung, die sich unter den Bedingungen moderner Datenverarbeitung aus informationsbezogenen Maßnahmen ergeben. Die freie

Entfaltung der Persönlichkeit setzt den Schutz des Einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten voraus. Dieser Schutz ist daher vom Grundrecht des Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG umfasst. Das Grundrecht gewährleistet insoweit die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen. Die Gewährleistung des Grundrechts greift insbesondere, wenn die Entfaltung der Persönlichkeit dadurch gefährdet wird, dass personenbezogene Informationen von staatlichen Behörden in einer Art und Weise genutzt und verknüpft werden, die Betroffene weder überschauen noch beherrschen können. Der Schutzzumfang des Rechts auf informationelle Selbstbestimmung beschränkt sich nicht auf Informationen, die bereits ihrer Art nach sensibel sind und schon deshalb grundrechtlich geschützt werden. Es gibt angesichts der Verarbeitungs- und Verknüpfungsmöglichkeiten kein schlechthin, also ungeachtet des Verwendungskontextes, belangloses personenbezogenes Datum. Insbesondere fallen unter den Schutz der informationellen Selbstbestimmung auch personenbezogene Informationen zu den Modalitäten der Bereitstellung von Telekommunikationsdiensten.

123. Vorschriften, die zum Umgang mit personenbezogenen Daten durch staatliche Behörden ermächtigen, begründen in der Regel verschiedene, aufeinander aufbauende Eingriffe. Insbesondere ist insoweit zwischen der Erhebung, Speicherung und Verwendung von Daten zu unterscheiden. Bei der Regelung eines Datenaustauschs zur staatlichen Aufgabenwahrnehmung ist darüber hinaus aber auch zwischen der Datenübermittlung seitens der auskunftserteilenden Stelle und dem Datenabruf seitens der auskunftsuchenden Stelle zu unterscheiden. Ein Datenaustausch vollzieht sich durch die einander korrespondierenden Eingriffe von Abfrage und Übermittlung, die jeweils einer eigenen Rechtsgrundlage bedürfen. Der Gesetzgeber muss, bildlich gesprochen, nicht nur die Tür zur Übermittlung von Daten öffnen, sondern auch die Tür zu deren Abfrage. Erst beide Rechtsgrundlagen gemeinsam, die wie eine Doppeltür zusammenwirken müssen, berechtigen zu einem Austausch personenbezogener Daten. Dies schließt - nach Maßgabe der Kompetenzordnung und den Anforderungen der Normenklarheit - nicht aus, dass beide Rechtsgrundlagen auch in einer Norm zusammengefasst werden können.

124. Die angegriffenen Vorschriften greifen in das Grundrecht auf informationelle Selbstbestimmung der Beschwerdeführer ein. Eingriffe liegen hierbei zunächst in der Erhebungs- und der Speicherungspflicht des § 111 TKG. Eigenständige weitere Grundrechtseingriffe liegen in der durch § 112 Abs. 1 TKG geregelten Pflicht der Diensteanbieter zur Bereitstellung der Daten als Kundendateien, die einem automatisierten Zugriff zugänglich sind, sowie in der Befugnis der Bundesnetzagentur, diese Daten abzurufen und bestimmten Behörden zu übermitteln (vgl. § 112 Abs. 4 TKG). Entsprechend begründen § 113 Abs. 1 Satz 1 und 2 TKG eigene Grundrechtseingriffe, indem sie die Telekommunikationsdiensteanbieter auf Verlangen zu Auskünften hinsichtlich der bei ihnen gespeicherten Daten verpflichten.

125. Ein hiervon zu unterscheidender, eigenständiger Eingriff liegt schließlich in dem von § 112 und § 113 TKG tatbestandlich vorausgesetzten Abruf der Daten seitens der auskunftsberechtigten Behörden in Form eines Ersuchens (§ 112 Abs. 1, 2, 4 TKG) oder Verlangens (§ 113 Abs. 1 TKG). Doch bedarf es dazu nach dem gesetzgeberischen Regelungskonzept einer weiteren Rechtsgrundlage, die je nach Sachbereich im Recht des Bundes oder der Länder zu finden sein muss. Die Vorschriften der §§ 112 und 113 TKG sind - entsprechend der Unterscheidung zwischen Erhebung und Übermittlung in der Regelungstypik der Datenschutzgesetze -

allein als Rechtsgrundlage für die Übermittlung zu verstehen. Sie setzen seitens der auskunftsberechtigten Behörden eigene Erhebungsbefugnisse voraus [...].“

15. Im Zusammenhang mit § 111 TKG befand das Bundesverfassungsgericht, dass mit der Verpflichtung zur Vorhaltung einer Datenbasis für Bestandsdaten insbesondere das legitime Ziel der Strafverfolgung verfolgt werde. Auch wenn die Datenbasis eine vorsorgliche Erhebung und Speicherung von Daten mit einer großen Streubreite darstelle und Straftäter die Vorschrift immer noch durch die anonyme Nutzung von Telekommunikationsdiensten unter falschem Namen oder mit von Dritten erworbenen Mobilfunkkarten umgehen könnten, sei der Eingriff in die informationelle Selbstbestimmung letztlich aufgrund der relativen Begrenztheit der gespeicherten Daten gerechtfertigt.

16. Zur Verhältnismäßigkeit führte das Bundesverfassungsgericht unter anderem Folgendes aus:

„136. § 111 TKG verstößt nicht gegen die Anforderungen der Verhältnismäßigkeit im engeren Sinne. Auch wenn die Vorschrift eine vorsorglich anlasslose Erhebung und Speicherung von Telekommunikationsdaten mit einer großen Streubreite anordnet, handelt es sich angesichts des nicht sehr weit reichenden Informationsgehalts der erfassten Daten doch um einen Eingriff von nur begrenztem Gewicht.

137. Der Eingriff ist allerdings nicht unerheblich. Gewicht hat er insoweit, als durch § 111 TKG annähernd flächendeckend für alle Telekommunikationsdienste die Zuordnung von Telekommunikationsnummer und Anschlussinhaber ermöglicht und dafür individualisierende Angaben wie Anschrift, Geburtsdatum und Datum des Vertragsbeginns erfasst und staatlich verfügbar gehalten werden. Die Daten bilden eine allgemeine Basis für Auskünfte und erfüllen die Funktion eines Telekommunikationsnummernregisters. Mit ihnen können in der Regel von jeder Person sämtliche Telekommunikationsnummern in Erfahrung gebracht werden; umgekehrt kann praktisch jeder Telekommunikationsvorgang, für den eine Telekommunikationsnummer ermittelt wird, auch einem Anschluss und damit einem Anschlussinhaber zugeordnet werden. Als Daten, die die Grundlagen von Telekommunikationsvorgängen betreffen, liegen sie folglich im Umfeld verfassungsrechtlich besonders geschützter Informationsbeziehungen, deren Vertraulichkeit für eine freiheitliche Ordnung essentiell ist. Zudem werden die entsprechenden Daten ohne Anlass vorsorglich erhoben und gespeichert, um sie der staatlichen Aufgabenwahrnehmung verfügbar zu machen.

138. Dennoch ist der hierin liegende Eingriff nicht von sehr großem Gewicht. Insbesondere ergibt sich ein sehr großes Gewicht hier nicht daraus, dass die Daten vorsorglich gesammelt werden. Denn auch wenn § 111 TKG eine große Streubreite hat, beschränkt sich der Zugriff inhaltlich doch auf eng begrenzte Daten, die aus sich heraus noch keinen Aufschluss über konkrete Aktivitäten Einzelner geben und deren Verwendung der Gesetzgeber zu näher bestimmten Zwecken geregelt hat. In solchen Fällen ist auch eine vorsorgliche Speicherung nicht schon allein deshalb ohne Weiteres ein besonders schwerer Eingriff, weil sie anlasslos erfolgt. Zwar muss eine vorsorgliche Datenspeicherung immer eine Ausnahme bleiben und ist begründungsbedürftig. Es ist aber nicht von vornherein ausgeschlossen, dass auch vorsorgliche Datensammlungen als Grundlagen vielfältiger staatlicher Aufgabenwahrnehmung ihre Berechtigung haben können, wie sie auch bisher in Form

der Melderegister oder im Bereich des Kraftfahrzeugwesens mit dem Zentralen Fahrzeugregister und dem Zentralen Fahrerlaubnisregister bekannt sind [...].

139. Die von § 111 TKG erfassten Daten haben nur eine beschränkte Aussagekraft. Sie ermöglichen allein die individualisierende Zuordnung von Telekommunikationsnummern zu den jeweiligen Anschlussinhabern und damit zu deren potentiellen (und typischen) Nutzern. Nähere private Angaben enthalten diese Daten nicht. Grundlegend anders als im Fall der vorsorglichen Speicherung sämtlicher Telekommunikationsverkehrsdaten umfassen diese Daten als solche weder höchstpersönliche Informationen noch ist mit ihnen die Erstellung von Persönlichkeits- oder Bewegungsprofilen möglich. [...]

140. Ein besonderes Eingriffsgewicht ergibt sich auch nicht daraus, dass die Daten des § 111 TKG kontextbezogen die Zuordnung einzelner, den Behörden bekannter Telekommunikationsvorgänge erlauben und damit unter Umständen deren individualisierende Kenntnisnahme hinsichtlich ihrer Umstände oder ihres Inhalts ermöglichen. Denn ermöglicht wird so von vornherein nur die anlassbezogene Aufklärung einzelner Vorgänge. Die Umstände oder der Inhalt des mit den Daten des § 111 TKG zu individualisierenden Telekommunikationsvorgangs sind der Behörde in diesen Fällen bereits bekannt, sei es, dass sie diese aufgrund eigener Befugnisse - etwa auf der Grundlage des § 100g StPO - unter Eingriff in das Telekommunikationsgeheimnis ermittelt hat, sei es, dass sie diese durch eigene Beobachtungen oder Informationen Dritter ohne einen solchen Eingriff in Erfahrung gebracht hat. Entsprechend begründet sich ein besonderes Eingriffsgewicht umgekehrt nicht daraus, dass sich an eine Abfrage von Telekommunikationsnummern weitere Maßnahmen anschließen können, die unter Umständen mit gewichtigen Eingriffen auch in das Telekommunikationsgeheimnis verbunden sind. Denn solche weiteren Eingriffe sind nur nach Maßgabe eigener Rechtsgrundlagen zulässig, die dem jeweiligen Eingriffsgewicht Rechnung tragen müssen.

141. Die Möglichkeit der Zuordnung der in § 111 TKG erfassten Daten dient einer effektiven Aufgabenwahrnehmung der in den Verwendungsvorschriften näher bestimmten Behörden. Sie ist verfassungsrechtlich dadurch gerechtfertigt, dass der Staat anlassbezogen ein legitimes Interesse an der Aufklärung bestimmter Telekommunikationsvorgänge haben und diesem Interesse zur Erfüllung bestimmter Aufgaben ein erhebliches, in Einzelfällen auch überragendes Gewicht zukommen kann. Dem lässt sich nicht entgegenhalten, dass die unmittelbare Kommunikation ohne Telekommunikationsmittel vergleichbare Eingriffe nicht kenne. Denn dort stellt sich die Sachlage anders dar. Weil die unmittelbare Kommunikation nicht auf technische Kommunikationsmittel zurückgreift, die es erlauben, sich unter Ausschluss öffentlicher Wahrnehmung über jede beliebige Distanz in Echtzeit miteinander auszutauschen, zeigt sich dort weder ein vergleichbares Substrat noch eine vergleichbare Notwendigkeit für ein entsprechendes Register. Die traditionellen Ermittlungsbefugnisse wie die Einvernehmung von Zeugen oder die Beschlagnahme von Unterlagen reichen hier zur Aufklärung weiter als gegenüber einer Kommunikation mittels elektronischer Dienste. Richtig ist allerdings, dass auch die Möglichkeiten der modernen Telekommunikationsmittel keine Rechtfertigung dafür bieten, möglichst alle Aktivitäten der Bürger vorsorglich zu registrieren und so grundsätzlich rekonstruierbar zu machen. Hiervon ist bei der Einrichtung eines Telekommunikationsnummernregisters, auch bei Berücksichtigung des Zusammenspiels mit anderen vorhandenen Dateien, aber nicht die Rede.“

17. Bezüglich § 112 TKG stellte das Bundesverfassungsgericht klar, dass diese Vorschrift

„144. [...] die Verwendung der nach § 111 TKG gespeicherten Daten in Form eines automatisierten Auskunftsverfahrens [regelt], bei dem die Bundesnetzagentur die Daten auf Ersuchen an bestimmte, in § 112 Abs. 2 TKG genannte Behörden zu übermitteln hat. Die Vorschrift ist Rechtsgrundlage nur für die Pflicht zur Bereitstellung der Daten als Kundendateien, für den Zugriff auf diese Daten und für deren Übermittlung, nicht aber auch für den Abruf in Form eines Ersuchens durch die auskunftsberechtigten Behörden.“

Dem Bundesverfassungsgericht zufolge könnten jedoch für ein Ersuchen der auskunftsberechtigten Stelle die allgemeinen Datenerhebungsbefugnisse ausreichen. In diesem Zusammenhang verwendete das Bundesverfassungsgericht das Bild einer Doppeltür (siehe Rdnr. 123 des in Rdnr. 14 zitierten Auszuges der Entscheidung) und führte aus, dass § 112 TKG zwar die Tür zur Übermittlung von Daten öffne, nicht jedoch diejenige zur Abfrage von Daten durch die spezialisierten Behörden.

18. Dennoch befand das Bundesverfassungsgericht, dass der in § 112 TKG vorgesehene Eingriff – aus mehreren Gründen – von erheblichem Gewicht sei:

„156. Ein nicht unerhebliches Eingriffsgewicht erhält die Regelung allerdings dadurch, dass § 112 TKG die Datenabfragen sehr vereinfacht. Das zentral zusammengefasste und automatisierte Verfahren erlaubt einen Zugang, der praktische Erschwernisse der Datenerhebung weithin beseitigt und die Daten der Betroffenen ohne zeitliche Verzögerungen oder Reibungsverluste in Form von Prüferfordernissen zur Verfügung stellt. Hinzu kommt, dass die Auskünfte erteilt werden, ohne dass Telekommunikationsunternehmen oder sonst Dritte dies wahrnehmen. Zwar sichert die Unbemerktheit der Auskünfte für das Telekommunikationsunternehmen den Datenbetroffenen Diskretion; zugleich fehlt es damit den Eingriffen jedoch an den Hemm- und Kontrollwirkungen, die mit einer Wahrnehmung durch Dritte verbunden sind. Auch eine rechtliche Prüfung seitens der die Daten übermittelnden Bundesnetzagentur findet nur statt, wenn ein besonderer Anlass besteht (vgl. § 112 Abs. 4 Satz 2 TKG). Da die abfragende Behörde ihr Ersuchen aber nicht zu begründen hat, wird ein solcher Anlass kaum je gegeben sein.“

157. Von Gewicht ist weiterhin, dass der Gesetzgeber die Verwendungszwecke der Daten sehr weit gefasst hat. Den in § 112 Abs. 2 TKG genannten Behörden dürfen die Daten allgemein zur Erfüllung ihrer gesetzlichen Aufgaben übermittelt werden. Eingeschränkt ist dies allein für die Polizeivollzugsbehörden gemäß § 112 Abs. 2 Nr. 2 TKG und gemäß § 112 Abs. 2 Nr. 3 und 7 TKG für die dort genannten Behörden des Zolls. Von Bedeutung ist hierbei aber, dass ersteren nach § 112 TKG nur für Zwecke der Gefahrenabwehr Auskünfte erteilt werden dürfen, womit die bloße Gefahrenvorsorge ausgeschlossen ist. Im Rahmen der jeweiligen Aufgaben der abfrageberechtigten Behörden sind die Auskunftspflichten der Bundesnetzagentur gleichfalls nur wenig begrenzt. Insbesondere kennt das Gesetz keine qualifizierten Eingriffsschwellen, sondern öffnet die Auskunftspflicht im gesamten Umfang der jeweiligen Kompetenz der Behörden. Eine sachlich begrenzende Maßgabe von praktischer Bedeutung liegt jedoch darin begründet, dass eine Auskunft nur erteilt werden darf, sofern sie für die Aufgabenwahrnehmung erforderlich ist. Dies stellt sicher, dass Abfragen nicht leichthändig zur bloß orientierenden Vorabinformation

zulässig sind, sondern nur dann, wenn zur Aufgabenwahrnehmung tatsächlich benötigte Informationen auf andere Weise nicht einfacher, aber ebenso effektiv beschafft werden können.

[...]

163. Allerdings beschränkt § 112 TKG Auskünfte tatsächlich nicht auf Abfragen, die durch spezifische, auf das automatisierte Auskunftsverfahren bezogene Rechtsgrundlagen legitimiert sind, sondern lässt auch Ersuchen genügen, die auf schlechte Datenerhebungsbefugnisse gestützt werden. Damit sind auf der Ebene des Fachrechts eine über § 112 Abs. 2 TKG hinausgehende ausdrückliche Konkretisierung der berechtigten Behörden und weitere zu beachtende Maßgaben für den Datenabruf nicht geboten. [...]"

19. Das Bundesverfassungsgericht gelangte dennoch zu dem Schluss, dass § 112 TKG verhältnismäßig sei:

„155. § 112 TKG genügt den Anforderungen des Verhältnismäßigkeitsgrundsatzes. Die Vorschrift dient der Effektivierung der Aufgabenwahrnehmung der in § 112 Abs. 2 TKG genannten Behörden und ist hierfür geeignet und erforderlich. Sie ist auch verhältnismäßig im engeren Sinne.

[...]

158. Trotz des nicht unerheblichen Eingriffsgewichts erweist sich die Regelung als verhältnismäßig. Immerhin bleiben die abrufberechtigten Behörden enumerativ begrenzt. Bei den Zwecken, für die ihnen Auskünfte nach § 112 Abs. 2 TKG erteilt werden, handelt es sich um zentrale Aufgaben der Gewährleistung von Sicherheit. Angesichts der zunehmenden Bedeutung der elektronischen Kommunikationsmittel und des entsprechend fortentwickelten Kommunikationsverhaltens der Menschen in allen Lebensbereichen sind die Behörden dabei in weitem Umfang auf eine möglichst unkomplizierte Möglichkeit angewiesen, Telekommunikationsnummern individuell zuordnen zu können. Es ist insoweit eine verfassungsrechtlich nicht zu beanstandende Entscheidung des Gesetzgebers, wenn er die Übermittlung dieser Auskünfte erlaubt, um Straftaten und Gefahren aufzuklären, verfassungsbedrohliche Entwicklungen zur Information der Regierung und der Öffentlichkeit zu beobachten oder in Notsituationen zu helfen. Weil solche Ermittlungen oft schnell und ohne Kenntnis der Betroffenen durchgeführt werden müssen, ist für sie ein automatisiertes Auskunftsverfahren von besonderer Bedeutung. Auch die Effektivierung der Arbeit der Gerichte ist ein Anliegen, dessen Gewicht eine solche Regelung trägt.

159. Von zentraler Bedeutung für die Abwägung ist die begrenzte Aussagekraft der Daten [...]: Sie geben allein Auskunft über die Zuordnung einzelner Telekommunikationsnummern zu ihrem Anschlussinhaber. Auch wenn sich im Rahmen konkreter Erhebungszusammenhänge daraus sensible Informationen ergeben können, bleibt der Informationsgehalt dieser Auskünfte als solcher doch begrenzt und hängt im Übrigen von weiteren Ermittlungen ab, deren Rechtmäßigkeit nach anderen Vorschriften zu beurteilen ist.

[...]

163. [...] Da es hier um die Übermittlung von Daten seitens einer Behörde geht und deren materielle Maßgaben auch gegenüber dem Datenbetroffenen abschließend und hinreichend klar durch § 112 TKG geregelt werden, ist dies unter Berücksichtigung des begrenzten Eingriffsgewichts der Vorschrift mit dem Verhältnismäßigkeitsgrundsatz vereinbar und entspricht der Regelungstechnik der Vorschriften über den automatisierten Abruf von Fahrzeug- und Halterdaten aus dem

Fahrzeugregister [...] und der Datenübermittlungsbestimmung im Einwohnermelderecht [...] . Dies lässt die Verantwortung des Gesetzgebers - und insoweit gegebenenfalls der Länder - für die rechtsstaatliche Ausgestaltung der Datenerhebungsvorschriften, die selbst nicht Gegenstand des vorliegenden Verfahrens sind, freilich unberührt. [...]"

Darüber hinaus hob das Gericht die Verantwortung der öffentlichen Stellen hervor, diese Vorschriften so anzuwenden, dass den Anforderungen des § 112 Abs. 1 und 2 TKG und insbesondere dem Erfordernis der Erforderlichkeit der Datenerhebung auch im Einzelfall differenziert Rechnung getragen und den weiteren Anforderungen des Verhältnismäßigkeitsgrundsatzes genügt wird.

20. Bezüglich § 113 TKG befand das Bundesverfassungsgericht, dass diese Vorschrift lediglich als Öffnungsklausel zu verstehen sei und dass eine zusätzliche Rechtsgrundlage für den Abruf von Daten durch die Behörden erforderlich sei. Auch gebe es in Bezug auf die ersuchenden Behörden keine Einschränkung, außer durch deren Aufgaben; zudem seien die Zwecke des Datenabrufs sehr weit gefasst. Es gelangte dennoch zu dem Schluss, dass angesichts des für sich gesehen begrenzten Informationsgehalts der betreffenden Daten sowie ihrer großen Bedeutung für eine effektive Aufgabenwahrnehmung die Weite der Vorschrift verfassungsrechtlich nicht zu beanstanden sei.

21. Das Bundesverfassungsgericht führte unter anderem Folgendes aus:

„176. Allerdings öffnet § 113 Abs. 1 Satz 1 TKG das manuelle Auskunftsverfahren sehr weit. Er erlaubt Auskünfte zum Zweck der Gefahrenabwehr, zur Verfolgung von Straftaten oder Ordnungswidrigkeiten sowie zur Wahrnehmung nachrichtendienstlicher Aufgaben. Dabei enthält die Vorschrift auch keine ihre Reichweite näher begrenzenden, spezifischen Eingriffsschwellen. Vielmehr erlaubt sie Auskünfte im Einzelfall immer, wenn dies zur Wahrnehmung der genannten Aufgaben erforderlich ist.

177. Angesichts des für sich gesehen begrenzten Informationsgehalts der betreffenden Daten sowie ihrer großen Bedeutung für eine effektive Aufgabenwahrnehmung ist diese Weite der Vorschrift jedoch verfassungsrechtlich nicht zu beanstanden. Dabei ist zu berücksichtigen, dass sie keineswegs Auskünfte ins Blaue hinein zulässt. Vielmehr liegt eine begrenzende Wirkung darin, dass Auskünfte nach § 113 Abs. 1 Satz 1 TKG im Einzelfall angefordert werden und erforderlich sein müssen. Bezogen auf die Gefahrenabwehr, in die der Gesetzgeber die Gefahrenvorsorge gerade nicht einbezogen hat, ergibt sich bei verständiger Auslegung das Erfordernis einer „konkreten Gefahr“ im Sinne der polizeilichen Generalklauseln als Voraussetzung für solche Auskünfte. Diese Schwelle ist freilich niedrig und umfasst auch den Gefahrenverdacht. Ebenso beschränkt sie Auskünfte nicht von vornherein auf Polizeipflichtige im Sinne des allgemeinen Polizei- und Ordnungsrechts. Sie ist damit jedoch nicht so entgrenzt, dass sie angesichts des gemäßigten Eingriffsgewichts unverhältnismäßig wäre. Insbesondere werden damit Auskünfte nicht als allgemeines Mittel für einen gesetzesmäßigen Verwaltungsvollzug ermöglicht, sondern setzen im Einzelfall einen sicherheitsrechtlich geprägten Charakter der betreffenden Aufgabe voraus. Bezogen auf die Nachrichtendienste, die grundsätzlich unabhängig von konkreten Gefahren im Vorfeld tätig werden, fehlt es zwar an einer vergleichbaren Eingriffsschwelle. Dies

rechtfertigt sich aber aus deren beschränkten Aufgaben, die nicht unmittelbar auf polizeiliche Maßnahmen ausgerichtet sind, sondern nur auf eine Berichtspflicht gegenüber den politisch verantwortlichen Staatsorganen beziehungsweise der Öffentlichkeit zielen. Im Übrigen ergibt sich auch hier aus dem Erfordernis der Erforderlichkeit im Einzelfall, dass eine Auskunft gemäß § 113 Abs. 1 Satz 1 TKG zur Aufklärung einer bestimmten, nachrichtendienstlich beobachtungsbedürftigen Aktion oder Gruppierung geboten sein muss. Soweit sich Auskünfte auf die Verfolgung von Straftaten und Ordnungswidrigkeiten beziehen, ergibt sich aus dem Erfordernis der Erforderlichkeit im Einzelfall, dass zumindest ein Anfangsverdacht vorliegen muss.

178. Insgesamt sind diese Schwellen zwar nicht hoch, aber verfassungsrechtlich noch hinnehmbar. Hierbei ist im Vergleich zu § 112 TKG zu berücksichtigen, dass ein manuelles Auskunftsverfahren für die abfragende Behörde einen gewissen Verfahrensaufwand mit sich bringt, der dazu beitragen dürfte, dass die Behörde die Auskunft nur bei hinreichendem Bedarf einholt.“

22. Was die Rechtsschutzmöglichkeiten gegen Auskunftersuchen gemäß den §§ 112 und 113 TKG angeht, führte das Bundesverfassungsgericht Folgendes aus:

„186. [...] Auch ist nicht zu beanstanden, wenn angesichts der geringen Eingriffstiefe kein spezifisches Rechtsschutzverfahren gegen Auskünfte nach den §§ 112 und 113 TKG vorgesehen ist. Rechtsschutz kann insoweit nach allgemeinen Regeln - insbesondere inzident im Zusammenhang mit Rechtsschutzverfahren gegenüber abschließenden Entscheidungen der Behörden - gesucht werden.

187. Aus den Anforderungen des Verhältnismäßigkeitsgrundsatzes ergibt sich für Auskünfte gemäß § 112 und § 113 TKG [...] kein flächendeckendes Erfordernis zur Benachrichtigung der von der Auskunft Betroffenen.“

23. Das Bundesverfassungsgericht stellte in seiner Entscheidung fest, dass im Jahr 2008 26,6 Millionen Datensätze – entweder die Identität oder die Telefonnummer des Teilnehmers – gemäß § 112 TKG abgefragt worden seien. Bei dieser Zahl wurde nicht nach Datensätzen betreffend „pay as you go“-Mobilfunknutzer und anderen Kunden unterschieden.

II. EINSCHLÄGIGES INNERSTAATLICHES RECHT UND EINSCHLÄGIGE INNERSTAATLICHE PRAXIS

A. Das Grundgesetz

24. Die einschlägigen Bestimmungen des Grundgesetzes, soweit für die vorliegende Rechtssache relevant, lauten wie folgt:

Artikel 1

„(1) Die Würde des Menschen ist unantastbar. Sie zu achten und zu schützen ist Verpflichtung aller staatlichen Gewalt. [...]“

Artikel 2

„(1) Jeder hat das Recht auf die freie Entfaltung seiner Persönlichkeit, soweit er nicht die Rechte anderer verletzt und nicht gegen die verfassungsmäßige Ordnung oder das Sittengesetz verstößt. [...]“

Artikel 10

„(1) Das Briefgeheimnis sowie das Post- und Fernmeldegeheimnis sind unverletzlich.

(2) Beschränkungen dürfen nur auf Grund eines Gesetzes angeordnet werden. Dient die Beschränkung dem Schutze der freiheitlichen demokratischen Grundordnung oder des Bestandes oder der Sicherung des Bundes oder eines Landes, so kann das Gesetz bestimmen, daß sie dem Betroffenen nicht mitgeteilt wird und daß an die Stelle des Rechtsweges die Nachprüfung durch von der Volksvertretung bestellte Organe und Hilfsorgane tritt.“

25. In seinem Urteil vom 15. Dezember 1983 (1 BvR 209, 269, 362, 420, 440, 484/83) legte das Bundesverfassungsgericht das Recht auf informationelle Selbstbestimmung fest und befand:

„Unter den Bedingungen der modernen Datenverarbeitung wird der Schutz des Einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten von dem allgemeinen Persönlichkeitsrecht des GG Art 2 Abs. 1 in Verbindung mit GG Art 1 Abs. 1 umfaßt. Das Grundrecht gewährleistet insoweit die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen.“

26. In seinem Urteil vom 2. März 2010 (1 BvR 256, 586, 263/08) entschied das Bundesverfassungsgericht über die Verfassungsmäßigkeit von Vorschriften zur Umsetzung der EU-Richtlinie 2006/24/EG (siehe Rdrrn. 49 und 50) in deutsches Recht (§§ 113a, 113b TKG, § 100g StPO), mit denen die Diensteanbieter verpflichtet wurden, für einen begrenzten Zeitraum (6 Monate) sämtliche Telekommunikationsverkehrsdaten zu speichern, und mit denen die Verwendung dieser Daten für Strafverfolgungszwecke gestattet wurde. Das Bundesverfassungsgericht erklärte § 113a TKG (Speicherungspflicht) für verfassungswidrig und nichtig, weil er das Recht auf Schutz des Telekommunikationsgeheimnisses verletze. Es befand, dass eine Speicherungspflicht in dem vorgesehenen Umfang zwar nicht von vornherein schlechthin verfassungswidrig sei. Es fehle aber an einer dem Verhältnismäßigkeitsgrundsatz entsprechenden Ausgestaltung. Die angegriffenen Vorschriften gewährleisteten weder eine hinreichende Datensicherheit, noch eine hinreichende Begrenzung der Verwendungszwecke der Daten. Auch genügten sie nicht in jeder Hinsicht den verfassungsrechtlichen Transparenz- und Rechtsschutzanforderungen.

B. Telekommunikationsgesetz

27. § 111 TKG verpflichtet Diensteanbieter, bestimmte persönliche Daten ihrer Kunden zu erheben und zu speichern. Damit schafft er die

Grundlage für Auskunftersuchen gemäß den §§ 112 und 113 TKG. Zur maßgeblichen Zeit und soweit relevant lautete er wie folgt:

„(1) Wer geschäftsmäßig Telekommunikationsdienste erbringt oder daran mitwirkt und dabei Rufnummern oder andere Anschlusskennungen vergibt oder Telekommunikationsanschlüsse für von anderen vergebene Rufnummern oder andere Anschlusskennungen bereitstellt, hat für die Auskunftsverfahren nach den §§ 112 und 113

1. die Rufnummern und anderen Anschlusskennungen,
2. den Namen und die Anschrift des Anschlussinhabers,
3. bei natürlichen Personen deren Geburtsdatum,
4. bei Festnetzanschlüssen auch die Anschrift des Anschlusses,
5. in Fällen, in denen neben einem Mobilfunkanschluss auch ein Mobilfunkendgerät überlassen wird, die Gerätenummer dieses Gerätes sowie
6. das Datum des Vertragsbeginns

vor der Freischaltung zu erheben und unverzüglich zu speichern, auch soweit diese Daten für betriebliche Zwecke nicht erforderlich sind; das Datum des Vertragsendes ist bei Bekanntwerden ebenfalls zu speichern. Satz 1 gilt auch, soweit die Daten nicht in Teilnehmerverzeichnisse eingetragen werden. [...] Wird dem Verpflichteten nach Satz 1 oder Satz 3 eine Änderung bekannt, hat er die Daten unverzüglich zu berichtigen; in diesem Zusammenhang hat der nach Satz 1 Verpflichtete bisher noch nicht erhobene Daten zu erheben und zu speichern, sofern ihm eine Erhebung der Daten ohne besonderen Aufwand möglich ist. Für das Auskunftsverfahren nach §113 ist die Form der Datenspeicherung freigestellt.

(2) Bedient sich der Diensteanbieter nach Absatz 1 Satz 1 oder Satz 3 eines Vertriebspartners, hat der Vertriebspartner die Daten nach Absatz 1 Satz 1 und 3 unter den dort genannten Voraussetzungen zu erheben und diese sowie die nach § 95 erhobenen Daten unverzüglich dem Diensteanbieter zu übermitteln; Absatz 1 Satz 2 gilt entsprechend. Satz 1 gilt auch für Daten über Änderungen, soweit sie dem Vertriebspartner im Rahmen der üblichen Geschäftsabwicklung zur Kenntnis gelangen.

(3) Für Vertragsverhältnisse, die am Tage des Inkrafttretens dieser Vorschrift bereits bestehen, müssen Daten im Sinne von Absatz 1 Satz 1 oder Satz 3 außer in den Fällen des Absatzes 1 Satz 4 nicht nachträglich erhoben werden.

(4) Die Daten sind mit Ablauf des auf die Beendigung des Vertragsverhältnisses folgenden Kalenderjahres zu löschen.

[...]“

28. Im Juli 2016 wurde § 111 TKG geändert und eine Verpflichtung der Diensteanbieter eingeführt, die persönlichen Daten der Mobilfunknutzer vor der Erhebung zu überprüfen. Bei der erstmaligen Registrierung der Daten ist die Vorlage eines Ausweises, Passes oder sonstigen Identitätsdokuments erforderlich. Die Änderung war als notwendig erachtet worden, um die Möglichkeiten zur Umgehung der Pflichten aus § 111 TKG weiter einzuschränken. Laut Bundestagdrucksache 18/8702 (S. 22) habe sich gezeigt, dass die Kundendatenbanken der

Telekommunikationsdiensteanbieter eine erhebliche Anzahl fehlerhafter Daten enthielten, wobei es sich um Erscheinungen mit Massencharakter handele. Die Auskunftersuchen der entsprechenden Behörden gemäß den §§ 112, 113 TKG hätten daher in vielen Verfahren zu keinen brauchbaren Informationen geführt. Eine Verfassungsbeschwerde zur Vereinbarkeit dieser Änderung mit dem Grundgesetz ist derzeit beim Bundesverfassungsgericht anhängig (1 BvR 1713/17).

29. § 112 TKG schafft ein automatisiertes Verfahren für die gemäß § 111 TKG gespeicherten Daten. Nach diesem Verfahren müssen Anbieter von Telekommunikationsdiensten die Daten so zur Verfügung stellen, dass sie die Bundesnetzagentur ohne Kenntnis der Anbieter abrufen kann. Darüber hinaus muss gewährleistet sein, dass der Abruf von Daten unter Verwendung unvollständiger Abfragedaten oder die Suche mittels einer Ähnlichenfunktion erfolgen kann. Zur maßgeblichen Zeit lauteten die relevanten Passagen des § 112 TKG wie folgt:

„(1) Wer öffentlich zugängliche Telekommunikationsdienste erbringt, hat die nach § 111 Abs.1 Satz 1, 3 und 4 und Abs. 2 erhobenen Daten unverzüglich in Kundendateien zu speichern [...]. Der Verpflichtete hat zu gewährleisten, dass

1. die Bundesnetzagentur jederzeit Daten aus den Kundendateien automatisiert im Inland abrufen kann,

2. der Abruf von Daten unter Verwendung unvollständiger Abfragedaten oder die Suche mittels einer Ähnlichenfunktion erfolgen kann.

Der Verpflichtete und sein Beauftragter haben durch technische und organisatorische Maßnahmen sicherzustellen, dass ihnen Abrufe nicht zur Kenntnis gelangen können. Die Bundesnetzagentur darf Daten aus den Kundendateien nur abrufen, soweit die Kenntnis der Daten erforderlich ist

1. für die Verfolgung von Ordnungswidrigkeiten nach diesem Gesetz oder nach dem Gesetz gegen den unlauteren Wettbewerb,

2. für die Erledigung von Auskunftersuchen der in Absatz 2 genannten Stellen.

Die ersuchende Stelle prüft unverzüglich, inwieweit sie die als Antwort übermittelten Daten benötigt, nicht benötigte Daten löscht sie unverzüglich; dies gilt auch für die Bundesnetzagentur für den Abruf von Daten nach Satz 7 Nummer 1.

(2) Auskünfte aus den Kundendateien nach Absatz 1 werden

1. den Gerichten und Strafverfolgungsbehörden,

2. den Polizeivollzugsbehörden des Bundes und der Länder für Zwecke der Gefahrenabwehr,

3. dem Zollkriminalamt und den Zollfahndungsämtern für Zwecke eines Strafverfahrens sowie dem Zollkriminalamt zur Vorbereitung und Durchführung von Maßnahmen nach § 23a des Zollfahndungsdienstgesetzes,

4. die Verfassungsschutzbehörden des Bundes und der Länder, der Militärische Abschirmdienst und der Bundesnachrichtendienst,

5. den Notrufabfragestellen nach § 108 sowie der Abfragestelle für die Rufnummer 124 124,

6. der Bundesanstalt für Finanzdienstleistungsaufsicht sowie

7. den Behörden der Zollverwaltung für die in § 2 Abs. 1 des Schwarzarbeitsbekämpfungsgesetzes genannten Zwecke über zentrale Abfragestellen

nach Absatz 4 jederzeit erteilt, soweit die Auskünfte zur Erfüllung ihrer gesetzlichen Aufgaben erforderlich sind und die Ersuchen an die Bundesnetzagentur im automatisierten Verfahren vorgelegt werden.

[...]

(4) Auf Ersuchen der in Absatz 2 genannten Stellen hat die Bundesnetzagentur die entsprechenden Datensätze aus den Kundendateien nach Absatz 1 abzurufen und an die ersuchende Stelle zu übermitteln. Sie prüft die Zulässigkeit der Übermittlung nur, soweit hierzu ein besonderer Anlass besteht. Die Verantwortung für die Zulässigkeit der Übermittlung tragen

1. in den Fällen des Absatzes 1 Satz 7 Nummer 1 die Bundesnetzagentur und

2. in den Fällen des Absatzes 1 Satz 7 Nummer 2 die in Absatz 2 genannten Stellen.

Die Bundesnetzagentur protokolliert für Zwecke der Datenschutzkontrolle durch die jeweils zuständige Stelle bei jedem Abruf den Zeitpunkt, die bei der Durchführung des Abrufs verwendeten Daten, die abgerufenen Daten, ein die abrufende Person eindeutig bezeichnendes Datum sowie die ersuchende Stelle, deren Aktenzeichen und ein die ersuchende Person eindeutig bezeichnendes Datum. Eine Verwendung der Protokolldaten für andere Zwecke ist unzulässig. Die Protokolldaten sind nach einem Jahr zu löschen.

[...]“

30. Im Juni 2017 wurde eine Verordnung über das automatisierte Auskunftsverfahren nach § 112 TKG erlassen. In dieser Kundendatenauskunftsverordnung werden die Möglichkeiten konkretisiert, um auf Grundlage der Anschrift, des Namens oder der Telefonnummer von Teilnehmern um Auskünfte zu ersuchen, und es wird erläutert, welche Angaben ein Ersuchen um die jeweilige Abfrage enthalten muss. Darüber hinaus regelt sie Abfragen auf Grundlage unvollständiger Daten und Suchen mittels einer Ähnlichkeitsfunktion. Zu der Verordnung gehörte eine Technische Richtlinie, in der die technischen Standards für die Abfragen und die Kommunikation zwischen der Bundesnetzagentur, den ersuchenden Stellen und den Telekommunikationsdiensteanbietern festgelegt sind.

31. § 113 TKG sieht ein manuelles Verfahren für Ersuchen um gemäß § 111 TKG gespeicherte Daten vor. Im Unterschied zum automatisierten Auskunftsverfahren sind die Diensteanbieter hier selbst verpflichtet, den auskunftsberechtigten Stellen Auskünfte zu erteilen. Wie beim automatisierten Auskunftsverfahren ist über Auskunftersuchen gegenüber den Personen, die die Daten betreffen, Stillschweigen zu wahren. § 113 enthält keine abschließende Auflistung der nach dieser Vorschrift auskunftsberechtigten Stellen. Auskunftersuchen sind zulässig, soweit sie zum Zweck der Verfolgung von Straftaten oder Ordnungswidrigkeiten, zur Gefahrenabwehr und zur Erfüllung nachrichtendienstlicher Aufgaben

notwendig sind. Zum maßgeblichen Zeitpunkt und soweit relevant lautete § 113 TKG wie folgt:

„(1) Wer geschäftsmäßig Telekommunikationsdienste erbringt oder daran mitwirkt, darf nach Maßgabe des Absatzes 2 die nach den §§ 95 und 111 erhobenen Daten nach Maßgabe dieser Vorschrift zur Erfüllung von Auskunftspflichten gegenüber den in Absatz 3 genannten Stellen verwenden. [...]

(2) Die Auskunft darf nur erteilt werden, soweit eine in Absatz 3 genannte Stelle dies in Textform im Einzelfall zum Zweck der Verfolgung von Straftaten oder Ordnungswidrigkeiten, zur Abwehr von Gefahren für die öffentliche Sicherheit oder Ordnung oder für die Erfüllung der gesetzlichen Aufgaben der in Absatz 3 Nummer 3 genannten Stellen unter Angabe einer gesetzlichen Bestimmung verlangt, die ihr eine Erhebung der in Absatz 1 in Bezug genommenen Daten erlaubt; an andere öffentliche und nichtöffentliche Stellen dürfen Daten nach Absatz 1 nicht übermittelt werden. Bei Gefahr im Verzug darf die Auskunft auch erteilt werden, wenn das Verlangen in anderer Form gestellt wird. In diesem Fall ist das Verlangen unverzüglich nachträglich in Textform zu bestätigen. Die Verantwortung für die Zulässigkeit des Auskunftsverlangens tragen die in Absatz 3 genannten Stellen.

(3) Stellen im Sinne des Absatzes 1 sind

1. 1. die für die Verfolgung von Straftaten oder Ordnungswidrigkeiten zuständigen Behörden;

2. 2. die für die Abwehr von Gefahren für die öffentliche Sicherheit oder Ordnung zuständigen Behörden;

3. die Verfassungsschutzbehörden des Bundes und der Länder, der Militärische Abschirmdienst und der Bundesnachrichtendienst.

(4) Derjenige, der geschäftsmäßig Telekommunikationsdienste erbringt oder daran mitwirkt, hat die zu beauskunftenden Daten unverzüglich und vollständig zu übermitteln. Über das Auskunftersuchen und die Auskunftserteilung haben die Verpflichteten gegenüber den Betroffenen sowie Dritten Stillschweigen zu wahren.

[...]“

C. Rechtsgrundlage für automatisierte Auskunftersuchen gemäß § 112 TKG

32. Auskunftersuchen nach dem automatisierten Verfahren gemäß § 112 TKG im Zusammenhang mit strafrechtlichen Ermittlungen der Staatsanwaltschaft und der Polizei sind in der Strafprozessordnung geregelt. Die anwendbaren Bestimmungen zur maßgeblichen Zeit und soweit relevant lauteten wie folgt:

§ 160

„(1) Sobald die Staatsanwaltschaft durch eine Anzeige oder auf anderem Wege von dem Verdacht einer Straftat Kenntnis erhält, hat sie zu ihrer Entschließung darüber, ob die öffentliche Klage zu erheben ist, den Sachverhalt zu erforschen.

(2) Die Staatsanwaltschaft hat nicht nur die zur Belastung, sondern auch die zur Entlastung dienenden Umstände zu ermitteln und für die Erhebung der Beweise Sorge zu tragen, deren Verlust zu besorgen ist.

(3) Die Ermittlungen der Staatsanwaltschaft sollen sich auch auf die Umstände erstrecken, die für die Bestimmung der Rechtsfolgen der Tat von Bedeutung sind. Dazu kann sie sich der Gerichtshilfe bedienen.

§ 161

„(1) Zu dem in § 160 Abs. 1 bis 3 bezeichneten Zweck ist die Staatsanwaltschaft befugt, von allen Behörden Auskunft zu verlangen und Ermittlungen jeder Art entweder selbst vorzunehmen oder durch die Behörden und Beamten des Polizeidienstes vornehmen zu lassen, soweit nicht andere gesetzliche Vorschriften ihre Befugnisse besonders regeln. Die Behörden und Beamten des Polizeidienstes sind verpflichtet, dem Ersuchen oder Auftrag der Staatsanwaltschaft zu genügen, und in diesem Falle befugt, von allen Behörden Auskunft zu verlangen.“

§ 163

„(1) Die Behörden und Beamten des Polizeidienstes haben Straftaten zu erforschen und alle keinen Aufschub gestattenden Anordnungen zu treffen, um die Verdunkelung der Sache zu verhüten. Zu diesem Zweck sind sie befugt, alle Behörden um Auskunft zu ersuchen, bei Gefahr im Verzug auch, die Auskunft zu verlangen, sowie Ermittlungen jeder Art vorzunehmen, soweit nicht andere gesetzliche Vorschriften ihre Befugnisse besonders regeln.

[...]“

33. Zur Verhütung von Straftaten können das Bundeskriminalamt und die Bundespolizei nach dem automatisierten Verfahren gemäß § 112 TKG und in Übereinstimmung mit den Bestimmungen der folgenden Gesetze um Auskünfte ersuchen; zum maßgeblichen Zeitpunkt lauteten diese wie folgt:

§ 2 Bundeskriminalamtgesetz (BKAG)

„(1) Das Bundeskriminalamt unterstützt als Zentralstelle für das polizeiliche Auskunfts- und Nachrichtenwesen und für die Kriminalpolizei die Polizeien des Bundes und der Länder bei der Verhütung und Verfolgung von Straftaten mit länderübergreifender, internationaler oder erheblicher Bedeutung.

(2) Das Bundeskriminalamt hat zur Wahrnehmung dieser Aufgabe

1. alle hierfür erforderlichen Informationen zu sammeln und auszuwerten,

[...]“

§ 7 Bundeskriminalamtgesetz

„(1) Das Bundeskriminalamt kann personenbezogene Daten speichern, verändern und nutzen, soweit dies zur Erfüllung seiner jeweiligen Aufgabe als Zentralstelle erforderlich ist.

(2) Das Bundeskriminalamt kann, soweit dies zur Erfüllung seiner Aufgabe als Zentralstelle nach § 2 Abs. 2 Nr. 1 erforderlich ist, Daten zur Ergänzung vorhandener Sachverhalte oder sonst zu Zwecken der Auswertung mittels Auskünften oder Anfragen bei öffentlichen oder nichtöffentlichen Stellen erheben. [...]“

§ 21 Bundespolizeigesetz (BPolG)

„(1) Die Bundespolizei kann, sofern in diesem Abschnitt nichts anderes bestimmt ist, personenbezogene Daten erheben, soweit dies zur Erfüllung einer ihr obliegenden Aufgabe erforderlich ist.

(2) Zur Verhütung von Straftaten ist eine Erhebung personenbezogener Daten nur zulässig, soweit Tatsachen die Annahme rechtfertigen, daß

1. die Person Straftaten im Sinne des § 12 Abs. 1 mit erheblicher Bedeutung begehen will und die Daten zur Verhütung solcher Straftaten erforderlich sind oder

2. die Person mit einer in Nummer 1 genannten Person in einer Weise in Verbindung steht oder eine solche Verbindung hergestellt wird, die erwarten läßt, daß die Maßnahme zur Verhütung von Straftaten im Sinne der Nummer 1 führen wird und dies auf andere Weise aussichtslos oder wesentlich erschwert wäre.“

34. Ähnliche Bestimmungen wie § 21 BPolG gibt es auch für die Polizeien der Länder. Ferner ist diesen Polizeien gestattet, personenbezogene Daten zu erheben, soweit dies zur Gefahrenabwehr und zum Schutz der Rechte anderer erforderlich ist.

35. Gemäß den §§ 7 und 27 des deutschen Zollfahndungsdienstgesetzes (ZFdG) dürfen das Zollkriminalamt und die Zollfahndungsämter personenbezogene Daten erheben, soweit dies zur Erfüllung ihrer Aufgaben erforderlich ist. Darüber hinaus dürfen die Zollbehörden nach § 163 StPO (siehe Rdnr. 32) Daten erheben, wenn sie im Bereich der Schwarzarbeit ermitteln.

36. Das Bundesamt und die Landesämter für Verfassungsschutz dürfen um die gemäß § 111 TKG gespeicherten Daten ersuchen, soweit dies für die Erfüllung ihrer Aufgaben erforderlich ist und das Bundesdatenschutzgesetz dem nicht entgegensteht.

37. Der militärische Abschirmdienst darf gemäß § 4 des Gesetzes über den militärischen Abschirmdienst (MADG) um die Informationen ersuchen, die zur Erfüllung seiner Aufgaben erforderlich sind, mit Ausnahme der Beurteilung der Sicherheitslage von Dienststellen und Einrichtungen im Geschäftsbereich des Bundesministeriums der Verteidigung und von Dienststellen und Einrichtungen der verbündeten Streitkräfte und der internationalen militärischen Hauptquartiere.

38. Gemäß § 2 Abs. 1 des Gesetzes über den Bundesnachrichtendienst (BNDG) darf der Bundesnachrichtendienst um gemäß § 111 TKG

gespeicherte Information ersuchen, soweit dies erforderlich ist und das Bundesdatenschutzgesetz dem nicht entgegensteht,

- zum Schutz seiner Mitarbeiter, Einrichtungen, Gegenstände und Quellen gegen sicherheitsgefährdende oder geheimdienstliche Tätigkeiten,
- für die Sicherheitsüberprüfung von Personen, die für ihn tätig sind oder tätig werden sollen,
- für die Überprüfung der für die Aufgabenerfüllung notwendigen Nachrichtenzugänge.

D. Rechtsgrundlage für manuelle Auskunftersuchen gemäß § 113 TKG

39. Aufgrund der vom Bundesverfassungsgericht geäußerten Kritik an § 113 Abs. 1 TKG (siehe RdNr. 12 und 20-21) wurden im Juni 2013 – also nach Einreichung der vorliegenden Beschwerde – mehrere neue Bestimmungen zur Regelung des Datenabrufs durch Behörden nach dem manuellen Verfahren gemäß § 113 TKG eingeführt.

40. Auskunftersuchen der Staatsanwaltschaft und der Polizei wurden nunmehr in § 100j StPO geregelt, der, soweit relevant, wie folgt lautet:

„(1) Soweit dies für die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes eines Beschuldigten erforderlich ist, darf von demjenigen, der geschäftsmäßig Telekommunikationsdienste erbringt oder daran mitwirkt, Auskunft über die nach den §§ 95 und 111 des Telekommunikationsgesetzes erhobenen Daten verlangt werden (§ 113 Absatz 1 Satz 1 des Telekommunikationsgesetzes).

[...]

(5) Auf Grund eines Auskunftsverlangens nach Absatz 1 oder 2 hat derjenige, der geschäftsmäßig Telekommunikationsdienste erbringt oder daran mitwirkt, die zur Auskunftserteilung erforderlichen Daten unverzüglich zu übermitteln. [...]“

Ähnliche Bestimmungen wurden für die Bundespolizei, das Bundeskriminalamt und den Zollfahndungsdienst eingeführt.

41. Nach § 8d Bundesverfassungsschutzgesetz (BVerfSchG) darf das Bundesamt für Verfassungsschutz von den Diensteanbietern die gemäß § 111 TKG erhobenen Daten verlangen; § 8d BVerfSchG, soweit relevant, lautet wie folgt:

„Soweit dies zur Erfüllung der Aufgaben des Bundesamts für Verfassungsschutz erforderlich ist, darf von demjenigen, der geschäftsmäßig Telekommunikationsdienste erbringt oder daran mitwirkt, Auskunft über die nach den §§ 95 und 111 des Telekommunikationsgesetzes erhobenen Daten verlangt werden (§ 113 Absatz 1 Satz 1 des Telekommunikationsgesetzes). [...]“

Ähnliche Bestimmungen wurden für die Landesämter für Verfassungsschutz eingeführt. Auch die Rechtsgrundlagen für manuelle Auskunftersuchen des Militärischen Abschirmdiensts und des Bundesnachrichtendienstes verweisen auf § 8d BVerfSchG.

E. Gerichtliche Überprüfung von Ermittlungsmaßnahmen

42. Gemäß § 98 Abs. 2 StPO kann eine von einer ohne gerichtliche Beteiligung erfolgten Beschlagnahme eines Gegenstands betroffene Person jederzeit die gerichtliche Entscheidung beantragen.

43. Nach der ständigen Rechtsprechung des Bundesgerichtshofs (siehe z. B. 5 ARs (VS) 1/97, 5. August 1998) bietet eine analoge Anwendung des § 98 Abs. 2 StPO die Möglichkeit der gerichtlichen Überprüfung aller abgeschlossenen staatsanwaltlichen Ermittlungsmaßnahmen, wenn eine solche Maßnahme einen tiefgreifenden Eingriff in die Grundrechte der betroffenen Person darstellte.

F. Datenschutzrecht

44. Die relevanten Passagen des Bundesdatenschutzgesetzes in der bis zum 24. Mai 2018 gültigen Fassung lauteten wie folgt:

„§ 1 Zweck und Anwendungsbereich des Gesetzes

(1) Zweck dieses Gesetzes ist es, den Einzelnen davor zu schützen, dass er durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird.

(2) Dieses Gesetz gilt für die Erhebung, Verarbeitung und Nutzung personenbezogener Daten durch

1. öffentliche Stellen des Bundes,
2. öffentliche Stellen der Länder, soweit der Datenschutz nicht durch Landesgesetz geregelt ist und soweit sie
 - a) Bundesrecht ausführen oder
 - b) als Organe der Rechtspflege tätig werden und es sich nicht um Verwaltungsangelegenheiten handelt,

[...]

(3) Soweit andere Rechtsvorschriften des Bundes auf personenbezogene Daten einschließlich deren Veröffentlichung anzuwenden sind, gehen sie den Vorschriften dieses Gesetzes vor. Die Verpflichtung zur Wahrung gesetzlicher Geheimhaltungspflichten oder von Berufs- oder besonderen Amtsgeheimnissen, die nicht auf gesetzlichen Vorschriften beruhen, bleibt unberührt.

§ 2 Öffentliche und nicht-öffentliche Stellen

(1) Öffentliche Stellen des Bundes sind die Behörden, die Organe der Rechtspflege und andere öffentlich-rechtlich organisierte Einrichtungen des Bundes, der bundesunmittelbaren Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts sowie deren Vereinigungen ungeachtet ihrer Rechtsform. [...]

§ 3a Datenvermeidung und Datensparsamkeit

Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten und die Auswahl und Gestaltung von Datenverarbeitungssystemen sind an dem Ziel auszurichten, so wenig personenbezogene Daten wie möglich zu erheben, zu verarbeiten oder zu nutzen. Insbesondere sind personenbezogene Daten zu anonymisieren oder zu pseudonymisieren, soweit dies nach dem Verwendungszweck möglich ist und keinen im Verhältnis zu dem angestrebten Schutzzweck unverhältnismäßigen Aufwand erfordert.

§ 4 Zulässigkeit der Datenerhebung, -verarbeitung und -nutzung

(1) Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten sind nur zulässig, soweit dieses Gesetz oder eine andere Rechtsvorschrift dies erlaubt oder anordnet oder der Betroffene eingewilligt hat.

(2) Personenbezogene Daten sind beim Betroffenen zu erheben. Ohne seine Mitwirkung dürfen sie nur erhoben werden, wenn

1. eine Rechtsvorschrift dies vorsieht oder zwingend voraussetzt oder
2. a) die zu erfüllende Verwaltungsaufgabe ihrer Art nach oder der Geschäftszweck eine Erhebung bei anderen Personen oder Stellen erforderlich macht oder
b) die Erhebung beim Betroffenen einen unverhältnismäßigen Aufwand erfordern würde
und keine Anhaltspunkte dafür bestehen, dass überwiegende schutzwürdige Interessen des Betroffenen beeinträchtigt werden.

§ 13 Datenschutz

(1) Das Erheben personenbezogener Daten ist zulässig, wenn ihre Kenntnis zur Erfüllung der Aufgaben der verantwortlichen Stelle erforderlich ist.

(1a) Werden personenbezogene Daten statt beim Betroffenen bei einer nicht-öffentlichen Stelle erhoben, so ist die Stelle auf die Rechtsvorschrift, die zur Auskunft verpflichtet, sonst auf die Freiwilligkeit ihrer Angaben hinzuweisen.

§ 19 Auskunft an den Betroffenen

(1) Dem Betroffenen ist auf Antrag Auskunft zu erteilen über

1. die zu seiner Person gespeicherten Daten, auch soweit sie sich auf die Herkunft dieser Daten beziehen,
2. die Empfänger oder Kategorien von Empfängern, an die die Daten weitergegeben werden, und
3. den Zweck der Speicherung.

In dem Antrag soll die Art der personenbezogenen Daten, über die Auskunft erteilt werden soll, näher bezeichnet werden. Sind die personenbezogenen Daten weder automatisiert noch in nicht automatisierten Dateien gespeichert, wird die Auskunft nur erteilt, soweit der Betroffene Angaben macht, die das Auffinden der Daten ermöglichen, und der für die Erteilung der Auskunft erforderliche Aufwand nicht außer Verhältnis zu dem vom Betroffenen geltend gemachten Informationsinteresse steht. Die verantwortliche Stelle bestimmt das Verfahren, insbesondere die Form der Auskunftserteilung, nach pflichtgemäßem Ermessen.

(2) Absatz 1 gilt nicht für personenbezogene Daten, die nur deshalb gespeichert sind, weil sie aufgrund gesetzlicher, satzungsmäßiger oder vertraglicher Aufbewahrungsvorschriften nicht gelöscht werden dürfen, oder ausschließlich Zwecken der Datensicherung oder der Datenschutzkontrolle dienen und eine Auskunftserteilung einen unverhältnismäßigen Aufwand erfordern würde.

(3) Bezieht sich die Auskunftserteilung auf die Übermittlung personenbezogener Daten an Verfassungsschutzbehörden, den Bundesnachrichtendienst, den Militärischen Abschirmdienst und, soweit die Sicherheit des Bundes berührt wird, andere Behörden des Bundesministeriums der Verteidigung, ist sie nur mit Zustimmung dieser Stellen zulässig.

(4) Die Auskunftserteilung unterbleibt, soweit

1. die Auskunft die ordnungsgemäße Erfüllung der in der Zuständigkeit der verantwortlichen Stelle liegenden Aufgaben gefährden würde,
2. die Auskunft die öffentliche Sicherheit oder Ordnung gefährden oder sonst dem Wohle des Bundes oder eines Landes Nachteile bereiten würde oder

3. die Daten oder die Tatsache ihrer Speicherung nach einer Rechtsvorschrift oder ihrem Wesen nach, insbesondere wegen der überwiegenden berechtigten Interessen eines Dritten, geheim gehalten werden müssen und deswegen das Interesse des Betroffenen an der Auskunftserteilung zurücktreten muss.

(5) Die Ablehnung der Auskunftserteilung bedarf einer Begründung nicht, soweit durch die Mitteilung der tatsächlichen und rechtlichen Gründe, auf die die Entscheidung gestützt wird, der mit der Auskunftsverweigerung verfolgte Zweck gefährdet würde. In diesem Fall ist der Betroffene darauf hinzuweisen, dass er sich an die Bundesbeauftragte oder den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit wenden kann.

(6) Wird dem Betroffenen keine Auskunft erteilt, so ist sie auf sein Verlangen der oder dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit zu erteilen, soweit nicht die jeweils zuständige oberste Bundesbehörde im Einzelfall feststellt, dass dadurch die Sicherheit des Bundes oder eines Landes gefährdet würde. Die Mitteilung der oder des Bundesbeauftragten an den Betroffenen darf keine Rückschlüsse auf den Erkenntnisstand der verantwortlichen Stelle zulassen, sofern diese nicht einer weitergehenden Auskunft zustimmt.

(7) Die Auskunft ist unentgeltlich.

§ 19a Benachrichtigung

(1) Werden Daten ohne Kenntnis des Betroffenen erhoben, so ist er von der Speicherung, der Identität der verantwortlichen Stelle sowie über die Zweckbestimmungen der Erhebung, Verarbeitung oder Nutzung zu unterrichten. Der Betroffene ist auch über die Empfänger oder Kategorien von Empfängern von Daten zu unterrichten, soweit er nicht mit der Übermittlung an diese rechnen muss. Sofern eine Übermittlung vorgesehen ist, hat die Unterrichtung spätestens bei der ersten Übermittlung zu erfolgen.

(2) Die Benutzung ist nicht zulässig, soweit

1. der Betroffene auf andere Weise Kenntnis von der Speicherung oder der Übermittlung erlangt hat,

2. die Unterrichtung des Betroffenen einen unverhältnismäßigen Aufwand erfordert oder

3. die Speicherung oder Übermittlung der personenbezogenen Daten durch Gesetz ausdrücklich vorgesehen ist.

Die verantwortliche Stelle legt schriftlich fest, unter welchen Voraussetzungen von einer Benachrichtigung nach Nummer 2 oder 3 abgesehen wird.

(3) § 19 Abs. 2 und 4 gilt entsprechend.

§ 21 Anrufung der oder des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit

Jedermann kann sich an die Bundesbeauftragte oder den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit wenden, wenn er der Ansicht ist, bei der Erhebung, Verarbeitung oder Nutzung seiner personenbezogenen Daten durch öffentliche Stellen des Bundes in seinen Rechten verletzt worden zu sein. Für die Erhebung, Verarbeitung oder Nutzung von personenbezogenen Daten durch Gerichte des Bundes gilt dies nur, soweit diese in Verwaltungsangelegenheiten tätig werden.

§ 24 Kontrolle durch die Bundesbeauftragte oder den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit

(1) Die oder der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit kontrolliert bei den öffentlichen Stellen des Bundes die

Einhaltung der Vorschriften dieses Gesetzes und anderer Vorschriften über den Datenschutz.

(2) Die Kontrolle der oder des Bundesbeauftragten erstreckt sich auch auf

1. von öffentlichen Stellen des Bundes erlangte personenbezogene Daten über den Inhalt und die näheren Umstände des Brief-, Post- und Fernmeldeverkehrs und

2. personenbezogene Daten, die einem Berufs- oder besonderen Amtsgeheimnis, insbesondere dem Steuergeheimnis nach § 30 der Abgabenordnung, unterliegen. [...]"

45. Ähnliche Bestimmungen gab es in den Ländern. Ferner haben die Länder ihre eigenen Datenschutzbeauftragten, die die Einhaltung der jeweiligen Datenschutzgesetze durch die Länderbehörden überwachen.

III. RECHT UND PRAXIS DER EUROPÄISCHEN UNION

A. Die Charta der Grundrechte der Europäischen Union

46. Die Artikel 7 und 8 der Charta sehen Folgendes vor:

Artikel 7 – Achtung des Privat- und Familienlebens

„Jede Person hat das Recht auf Achtung ihres Privat- und Familienlebens, ihrer Wohnung sowie ihrer Kommunikation.“

Artikel – 8 Schutz personenbezogener Informationen

„(1) Jede Person hat das Recht auf Schutz der sie betreffenden personenbezogenen Daten.

(2) Diese Daten dürfen nur nach Treu und Glauben für festgelegte Zwecke und mit Einwilligung der betroffenen Person oder auf einer sonstigen gesetzlich geregelten legitimen Grundlage verarbeitet werden. Jede Person hat das Recht, Auskunft über die sie betreffenden erhobenen Daten zu erhalten und die Berichtigung der Daten zu erwirken.

(3) Die Einhaltung dieser Vorschriften wird von einer unabhängigen Stelle überwacht.“

B. EU-Sekundärrecht zum Datenschutz

47. In den Erwägungsgründen 2 und 11 der am 12. Juli 2002 erlassenen Datenschutzrichtlinie für elektronische Kommunikation (Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation) heißt es:

„(2) Ziel dieser Richtlinie ist die Achtung der Grundrechte; sie steht insbesondere im Einklang mit den durch die Charta der Grundrechte der Europäischen Union anerkannten Grundsätzen. Insbesondere soll mit dieser Richtlinie gewährleistet werden, dass die in den Artikeln 7 und 8 jener Charta niedergelegten Rechte uneingeschränkt geachtet werden.“

„(11) Wie die Richtlinie 95/46/EG gilt auch die vorliegende Richtlinie nicht für Fragen des Schutzes der Grundrechte und Grundfreiheiten in Bereichen, die nicht unter das Gemeinschaftsrecht fallen. Deshalb hat sie keine Auswirkungen auf das bestehende Gleichgewicht zwischen dem Recht des Einzelnen auf Privatsphäre und der Möglichkeit der Mitgliedstaaten, Maßnahmen nach Artikel 15 Absatz 1 dieser Richtlinie zu ergreifen, die für den Schutz der öffentlichen Sicherheit, für die Landesverteidigung, für die Sicherheit des Staates (einschließlich des wirtschaftlichen Wohls des Staates, soweit die Tätigkeiten die Sicherheit des Staates berühren) und für die Durchsetzung strafrechtlicher Bestimmungen erforderlich sind. Folglich betrifft diese Richtlinie nicht die Möglichkeit der Mitgliedstaaten zum rechtmäßigen Abfangen elektronischer Nachrichten oder zum Ergreifen anderer Maßnahmen, sofern dies erforderlich ist, um einen dieser Zwecke zu erreichen, und sofern dies im Einklang mit der Europäischen Konvention zum Schutze der Menschenrechte und Grundfreiheiten in ihrer Auslegung durch die Urteile des Europäischen Gerichtshofs für Menschenrechte erfolgt. Diese Maßnahmen müssen sowohl geeignet sein als auch in einem strikt angemessenen Verhältnis zum intendierten Zweck stehen und ferner innerhalb einer demokratischen Gesellschaft notwendig sein sowie angemessenen Garantien gemäß der Europäischen Konvention zum Schutze der Menschenrechte und Grundfreiheiten entsprechen.“

48. Darüber hinaus sieht die Richtlinie, soweit relevant, Folgendes vor:

Artikel 1 – Geltungsbereich und Zielsetzung

„(1) Diese Richtlinie dient der Harmonisierung der Vorschriften der Mitgliedstaaten, die erforderlich sind, um einen gleichwertigen Schutz der Grundrechte und Grundfreiheiten, insbesondere des Rechts auf Privatsphäre, in Bezug auf die Verarbeitung personenbezogener Daten im Bereich der elektronischen Kommunikation sowie den freien Verkehr dieser Daten und von elektronischen Kommunikationsgeräten und -diensten in der Gemeinschaft zu gewährleisten.“

(2) Die Bestimmungen dieser Richtlinie stellen eine Detaillierung und Ergänzung der Richtlinie 95/46/EG im Hinblick auf die in Absatz 1 genannten Zwecke dar. Darüber hinaus regeln sie den Schutz der berechtigten Interessen von Teilnehmern, bei denen es sich um juristische Personen handelt.

(3) Diese Richtlinie gilt nicht für Tätigkeiten, die nicht in den Anwendungsbereich des Vertrags zur Gründung der Europäischen Gemeinschaft fallen, beispielsweise Tätigkeiten gemäß den Titeln V und VI des Vertrags über die Europäische Union, und auf keinen Fall für Tätigkeiten betreffend die öffentliche Sicherheit, die Landesverteidigung, die Sicherheit des Staates (einschließlich seines wirtschaftlichen Wohls, wenn die Tätigkeit die Sicherheit des Staates berührt) und die Tätigkeiten des Staates im strafrechtlichen Bereich.“

Artikel 15 – Anwendung einzelner Bestimmungen der Richtlinie 95/46/EG

„(1) Die Mitgliedstaaten können Rechtsvorschriften erlassen, die die Rechte und Pflichten gemäß Artikel 5, Artikel 6, Artikel 8 Absätze 1, 2, 3 und 4 sowie Artikel 9 dieser Richtlinie beschränken, sofern eine solche Beschränkung gemäß Artikel 13 Absatz 1 der Richtlinie 95/46/EG für die nationale Sicherheit, (d. h. die Sicherheit des Staates), die Landesverteidigung, die öffentliche Sicherheit sowie die Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten oder des unzulässigen Gebrauchs von elektronischen Kommunikationssystemen in einer demokratischen Gesellschaft notwendig, angemessen und verhältnismäßig ist. Zu diesem Zweck können die Mitgliedstaaten unter anderem durch Rechtsvorschriften vorsehen, dass Daten aus den in diesem Absatz aufgeführten Gründen während einer begrenzten Zeit

aufbewahrt werden. Alle in diesem Absatz genannten Maßnahmen müssen den allgemeinen Grundsätzen des Gemeinschaftsrechts einschließlich den in Artikel 6 Absätze 1 und 2 des Vertrags über die Europäische Union niedergelegten Grundsätzen entsprechen.“

49. Am 15. März 2006 wurde die Richtlinie über die Vorratsdatenspeicherung (Richtlinie 2006/24/EG des Europäischen Parlaments und des Rates 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) erlassen. Soweit relevant, sah sie Folgendes vor:

Artikel 1 – Gegenstand und Anwendungsbereich

„(1) Mit dieser Richtlinie sollen die Vorschriften der Mitgliedstaaten über die Pflichten von Anbietern öffentlich zugänglicher elektronischer Kommunikationsdienste oder Betreibern eines öffentlichen Kommunikationsnetzes im Zusammenhang mit der Vorratsspeicherung bestimmter Daten, die von ihnen erzeugt oder verarbeitet werden, harmonisiert werden, um sicherzustellen, dass die Daten zum Zwecke der Ermittlung, Feststellung und Verfolgung von schweren Straftaten, wie sie von jedem Mitgliedstaat in seinem nationalen Recht bestimmt werden, zur Verfügung stehen.

(2) Diese Richtlinie gilt für Verkehrs- und Standortdaten sowohl von juristischen als auch von natürlichen Personen sowie für alle damit in Zusammenhang stehende Daten, die zur Feststellung des Teilnehmers oder registrierten Benutzers erforderlich sind. Sie gilt nicht für den Inhalt elektronischer Nachrichtenübermittlungen einschließlich solcher Informationen, die mit Hilfe eines elektronischen Kommunikationsnetzes abgerufen werden.“

Artikel 3 – Vorratsspeicherungspflicht

„(1) Abweichend von den Artikeln 5, 6 und 9 der Richtlinie 2002/58/EG tragen die Mitgliedstaaten durch entsprechende Maßnahmen dafür Sorge, dass die in Artikel 5 der vorliegenden Richtlinie genannten Daten, soweit sie im Rahmen ihrer Zuständigkeit im Zuge der Bereitstellung der betreffenden Kommunikationsdienste von Anbietern öffentlich zugänglicher elektronischer Kommunikationsdienste oder Betreibern eines öffentlichen Kommunikationsnetzes erzeugt oder verarbeitet werden, gemäß den Bestimmungen der vorliegenden Richtlinie auf Vorrat gespeichert werden.“

50. Im Wesentlichen wurde mit der Verordnung eine Verpflichtung für Anbieter öffentlich zugänglicher elektronischer Kommunikationsdienste oder Betreiber öffentlicher Kommunikationsnetze geschaffen, sämtliche Verkehrs- und Standortdaten für einen Zeitraum von sechs Monaten bis zwei Jahren auf Vorrat zu speichern. Ihr Ziel war es, sicherzustellen, dass die Daten zum Zweck der Ermittlung, Feststellung und Verfolgung von schweren Straftaten, wie sie von jedem Mitgliedstaat in seinem nationalen Recht bestimmt werden, zur Verfügung stehen. Die Speicherpflicht erstreckte sich unter anderem auf zur Rückverfolgung und Identifizierung der Quelle einer Nachricht benötigte Daten, d. h. die Rufnummer und der

Name sowie die Anschrift des Teilnehmers oder registrierten Benutzers (Artikel 5 Abs. 1 Buchst. a und b).

C. Einschlägige Rechtsprechung des Gerichtshofs der Europäischen Union (EuGH)

51. In einem Urteil des Gerichtshofs der Europäischen Union (EuGH) vom 8. April 2014 in dem Verfahren *Digital Rights Ireland* und *Seitlinger u. a.* (verbundene Rechtssachen C-293/12 und C-594/12, EU:C:2014:238) wurde die Richtlinie über die Vorratsdatenspeicherung (siehe Rdnrn. 49 und 50) für ungültig erklärt.

52. In dem Verfahren *Tele2 Sverige* und *Tom Watson u. a.* (verbundene Rechtssachen C-203/15 und C-698/15, EU:C:2016:970), Urteil vom 21. Dezember 2016, hat der EuGH seine Rechtsprechung im Bereich der digitalen Rechte weiterentwickelt. Der EuGH führte unter anderem Folgendes aus (Rdnrn. 103-111, Verweise auf andere EuGH-Urteile werden in den nachfolgend zitierten Passagen ausgelassen):

„103. [...] kann zwar die Wirksamkeit der Bekämpfung schwerer Kriminalität, insbesondere der organisierten Kriminalität und des Terrorismus, in hohem Maß von der Nutzung moderner Ermittlungstechniken abhängen; eine solche dem Gemeinwohl dienende Zielsetzung kann jedoch, so grundlegend sie auch sein mag, für sich genommen die Erforderlichkeit einer nationalen Regelung, die die allgemeine und unterschiedslose Vorratsspeicherung sämtlicher Verkehrs- und Standortdaten vorsieht, für die Kriminalitätsbekämpfung nicht rechtfertigen.

104. Eine solche Regelung hat zum einen in Anbetracht ihrer in Rn. 97 des vorliegenden Urteils beschriebenen charakteristischen Merkmale zur Folge, dass die Vorratsspeicherung der Verkehrs- und Standortdaten die Regel ist, obwohl nach dem mit der Richtlinie 2002/58 geschaffenen System die Vorratsspeicherung von Daten die Ausnahme zu sein hat.

105. Zum anderen sieht eine nationale Regelung wie die im Ausgangsverfahren, die sich allgemein auf alle Teilnehmer und registrierten Nutzer erstreckt und alle elektronischen Kommunikationsmittel sowie sämtliche Verkehrsdaten erfasst, keine Differenzierung, Einschränkung oder Ausnahme in Abhängigkeit von dem verfolgten Ziel vor. Sie betrifft pauschal sämtliche Personen, die elektronische Kommunikationsdienste nutzen, ohne dass sich diese Personen auch nur mittelbar in einer Lage befinden, die Anlass zur Strafverfolgung geben könnte. Sie gilt also auch für Personen, bei denen keinerlei Anhaltspunkt dafür besteht, dass ihr Verhalten in einem auch nur mittelbaren oder entfernten Zusammenhang mit schweren Straftaten stehen könnte. Zudem sieht sie keine Ausnahme vor, so dass sie auch für Personen gilt, deren Kommunikationsvorgänge nach den nationalen Rechtsvorschriften dem Berufsgeheimnis unterliegen.

106. Eine solche Regelung verlangt keinen Zusammenhang zwischen den Daten, deren Vorratsspeicherung vorgesehen ist, und einer Bedrohung der öffentlichen Sicherheit. Insbesondere beschränkt sie die Vorratsspeicherung weder auf die Daten eines Zeitraums und/oder eines geografischen Gebiets und/oder eines Personenkreises, der in irgendeiner Weise in eine schwere Straftat verwickelt sein

könnte, noch auf Personen, deren auf Vorrat gespeicherte Daten aus anderen Gründen zur Bekämpfung von Straftaten beitragen könnten.

107. Eine nationale Regelung wie die im Ausgangsverfahren in Rede stehende überschreitet somit die Grenzen des absolut Notwendigen und kann nicht als in einer demokratischen Gesellschaft gerechtfertigt angesehen werden, wie es Art. 15 Abs. 1 der Richtlinie 2002/58 im Licht der Art. 7, 8 und 11 sowie des Art. 52 Abs. 1 der Charta verlangt.

108. Hingegen untersagt Art. 15 Abs. 1 der Richtlinie 2002/58 im Licht der Art. 7, 8 und 11 sowie des Art. 52 Abs. 1 der Charta einem Mitgliedstaat nicht, eine Regelung zu erlassen, die zur Bekämpfung schwerer Straftaten vorbeugend die gezielte Vorratsspeicherung von Verkehrs- und Standortdaten ermöglicht, sofern die Vorratsdatenspeicherung hinsichtlich Kategorien der zu speichernden Daten, der erfassten elektronischen Kommunikationsmittel, der betroffenen Personen und der vorgesehenen Dauer der Vorratsspeicherung auf das absolut Notwendige beschränkt ist.

109. Um den in der vorstehenden Randnummer des vorliegenden Urteils genannten Erfordernissen zu genügen, muss die betreffende nationale Regelung erstens klare und präzise Regeln über die Tragweite und die Anwendung einer solchen Maßnahme der Vorratsdatenspeicherung vorsehen und Mindestanforderungen 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.

110. Zweitens können sich die materiellen Voraussetzungen, die eine nationale Regelung, die im Rahmen der Bekämpfung von Straftaten vorbeugend die Vorratsspeicherung von Verkehrs- und Standortdaten ermöglicht, erfüllen muss, um zu gewährleisten, dass sie auf das absolut Notwendige beschränkt wird, zwar je nach den zur Verhütung, Ermittlung, Feststellung und Verfolgung schwerer Straftaten getroffenen Maßnahmen unterscheiden, doch muss die Vorratsspeicherung 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.

111. Bei der Begrenzung einer solchen Maßnahme im Hinblick auf die potenziell betroffenen Personenkreise und Situationen muss sich die nationale Regelung auf objektive Anknüpfungspunkte stützen, die es ermöglichen, Personenkreise zu erfassen, deren Daten geeignet sind, einen zumindest mittelbaren Zusammenhang mit schweren Straftaten sichtbar zu machen, auf irgendeine Weise zur Bekämpfung schwerer Kriminalität beizutragen oder eine schwerwiegende Gefahr für die öffentliche Sicherheit zu verhindern.“

53. Im Anschluss an das letztgenannte Urteil haben sich nationale Gerichte aus mehreren EU-Mitgliedstaaten mit Vorabentscheidungsersuchen an den EuGH gewandt und um Klärung des Umfangs und der Wirkungen des Urteils *Tele2 Sverige* gebeten. Zwei dieser Verfahren sind noch anhängig (siehe *Privacy International*, C-623/17 und *Ordre des barreaux francophones et germanophone, Académie Fiscale*

ASBL, UA, Liga voor Mensenrechten ASBL, Ligue des Droits de l'Homme ASBL, VZ, WY, XX, C-520/18).

54. In einem dritten Fall, *Ministerio Fiscal* (C-207/16, EU:C:2018:788), wurde der EuGH gefragt, ob Artikel 15 Abs. 1 der Richtlinie 2002/58 im Licht der Artikel 7 und 8 der Charta dahin auszulegen ist, dass der Zugang öffentlicher Stellen zu Daten, anhand deren die Identität der Inhaber von SIM-Karten, die mit einem gestohlenen Mobiltelefon aktiviert wurden, festgestellt werden soll, wie Name, Vorname und gegebenenfalls Adresse dieser Karteninhaber, einen Eingriff in deren in diesen Artikeln der Charta verankerte Grundrechte darstellt, der so schwer ist, dass dieser Zugang im Bereich der Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten auf die Bekämpfung der schweren Kriminalität beschränkt werden müsste, und nach welchen Kriterien bejahendenfalls die Schwere der in Rede stehenden Straftat zu beurteilen ist.

55. In Rdnr. 51 f. seines Urteils vom 2. Oktober 2018 stellte der EuGH Folgendes fest (Verweise auf andere EuGH-Urteile werden in den nachfolgend zitierten Passagen ausgelassen):

„51. Was das Vorliegen eines Eingriffs in diese Grundrechte betrifft, stellt, wie der Generalanwalt in den Nrn. 76 und 77 seiner Schlussanträge ausgeführt hat, der Zugang der öffentlichen Stellen zu solchen Daten einen Eingriff in das in Art. 7 der Charta verankerte Grundrecht auf Achtung des Privatlebens dar, auch wenn keine Umstände vorliegen, aufgrund deren dieser Eingriff als „schwer“ eingestuft werden kann, und ohne dass es darauf ankommt, ob die betroffenen Informationen über das Privatleben als sensibel anzusehen sind oder die Betroffenen durch diesen Eingriff irgendwelche Nachteile erlitten haben. Zudem stellt ein solcher Zugang einen Eingriff in das in Art. 8 der Charta garantierte Grundrecht auf Schutz personenbezogener Daten dar, da es sich dabei um eine Verarbeitung personenbezogener Daten handelt.

[...]

56. Nach dem Grundsatz der Verhältnismäßigkeit kann ein schwerer Eingriff im Bereich der Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten nämlich nur durch einen Zweck der Bekämpfung einer ebenfalls als „schwer“ einzustufenden Kriminalität gerechtfertigt sein.

57. Ist dagegen der mit einem solchen Zugang verbundene Eingriff nicht schwer, kann dieser Zugang durch einen Zweck der Verhütung, Ermittlung, Feststellung und Verfolgung von „Straftaten“ im Allgemeinen gerechtfertigt sein.

58. Es ist daher zunächst zu prüfen, ob nach den Umständen des vorliegenden Falles der Eingriff in die in den Art. 7 und 8 der Charta verankerten Grundrechte, der mit einem Zugang der Kriminalpolizei zu den im Ausgangsverfahren in Rede stehenden Daten einhergeht, als „schwer“ anzusehen ist.

59. Insoweit ist festzustellen, dass der im Ausgangsverfahren in Rede stehende Antrag, mit dem die Kriminalpolizei für die Zwecke strafrechtlicher Ermittlungen um gerichtliche Erlaubnis zum Zugang zu von den Betreibern elektronischer Kommunikationsdienste gespeicherten personenbezogenen Daten ersucht, ausschließlich darauf abzielt, die Identität der Inhaber von SIM-Karten festzustellen, die in einem Zeitraum von zwölf Tagen mit der IMEI des gestohlenen Mobiltelefons aktiviert wurden. [...] bezieht sich dieser Antrag nur auf den Zugang zu den diesen

SIM-Karten entsprechenden Telefonnummern sowie zu den Daten bezüglich der Identität der Karteninhaber wie deren Name, Vorname und gegebenenfalls Adresse. Dagegen beziehen sich diese Daten [...] weder auf die mittels des gestohlenen Mobiltelefons erfolgte Kommunikation noch auf dessen Ortung.

60. Daher kann mit den Daten, auf die sich der im Ausgangsverfahren in Rede stehende Zugangsantrag bezieht, offenbar nur eine Verbindung zwischen der SIM-Karte oder den SIM-Karten, die mit dem gestohlenen Mobiltelefon aktiviert wurden, und der Identität der Inhaber dieser SIM-Karten während eines bestimmten Zeitraums hergestellt werden. Ohne einen Abgleich mit den Daten bezüglich der mittels dieser SIM-Karten erfolgten Kommunikation und den Standortdaten lassen sich diesen Daten weder das Datum, die Uhrzeit, die Dauer und die Adressaten der mittels der betreffenden SIM-Karte bzw. der betreffenden SIM-Karten erfolgten Kommunikation entnehmen noch die Orte, an denen diese Kommunikation erfolgte, oder die Häufigkeit dieser Kommunikation mit bestimmten Personen während eines bestimmten Zeitraums. Aus diesen Daten lassen sich daher keine genauen Schlüsse auf das Privatleben der Personen ziehen, deren Daten betroffen sind.

61. Unter diesen Umständen kann der Zugang nur zu den Daten, auf die sich der im Ausgangsverfahren in Rede stehende Antrag bezieht, nicht als „schwerer“ Eingriff in die Grundrechte der Personen eingestuft werden, deren Daten betroffen sind.“

IV. VÖLKERRECHT UND VÖLKERRECHTLICHE PRAXIS

56. Der Sonderberichterstatter der Vereinten Nationen über die Förderung und den Schutz des Rechts auf Meinungsfreiheit und freie Meinungsäußerung, David Kaye, sprach in seinem Bericht an den Menschenrechtsrat betreffend die Verwendung von Verschlüsselung und Anonymisierung zur Ausübung des Rechts auf Meinungsfreiheit und freie Meinungsäußerung im digitalen Zeitalter (A/HRC/29/32, 22. Mai 2015, Rdnr. 60) folgende Empfehlung aus:

„Die Staaten sollten die Verschlüsselung und Anonymisierung, durch die die Wahrnehmung des Rechts auf Meinungsfreiheit und freie Meinungsäußerung erleichtert und oft erst ermöglicht wird, nicht beschränken. Pauschale Verbote sind weder erforderlich noch verhältnismäßig. [...] Die Staaten sollten davon absehen, die Identifizierung von Nutzern zur Voraussetzung für den Zugang zu digitaler Kommunikation und zu Online-Diensten zu machen und bei Nutzern von Mobiltelefonen die Registrierung der SIM-Karten zu verlangen.“

57. Das Übereinkommen des Europarats von 1981 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten („das Europäische Datenschutzübereinkommen“), das von allen Mitgliedstaaten des Europarats ratifiziert wurde und für Deutschland am 1. Oktober 1985 in Kraft getreten ist, formuliert eine Reihe zentraler Grundsätze zur Erhebung und Verarbeitung personenbezogener Daten. Gemäß Artikel 1 des Übereinkommens ist sein Zweck, für jedermann sicherzustellen, dass seine Rechte und Grundfreiheiten, insbesondere sein Recht auf einen Persönlichkeitsbereich, bei der automatischen Verarbeitung

personenbezogener Daten geschützt werden. Das Übereinkommen enthält die folgenden Grundprinzipien:

Artikel 2 – Begriffsbestimmungen

„In diesem Übereinkommen:

- a bedeutet "personenbezogene Daten" jede Information über eine bestimmte oder bestimmbare natürliche Person ("Betroffener");
- b bedeutet "automatisierte Datei/Datensammlung" jede zur automatischen Verarbeitung erfaßte Gesamtheit von Informationen;
- c umfaßt "automatische Verarbeitung" die folgenden Tätigkeiten, wenn sie ganz oder teilweise mit Hilfe automatisierter Verfahren durchgeführt werden: das Speichern von Daten, das Durchführen logischer und/ oder rechnerischer Operationen mit diesen Daten, das Verändern, Löschen, Wiedergewinnen oder Bekanntgeben von Daten;“

Artikel 5 – Qualität der Daten

„Personenbezogene Daten, die automatisch verarbeitet werden:

- a müssen nach Treu und Glauben und auf rechtmäßige Weise beschafft sein und verarbeitet werden;
- b müssen für festgelegte und rechtmäßige Zwecke gespeichert sein und dürfen nicht so verwendet werden, daß es mit diesen Zwecken unvereinbar ist;
- c müssen den Zwecken, für die sie gespeichert sind, entsprechen, dafür erheblich sein und dürfen nicht darüber hinausgehen;
- d müssen sachlich richtig und wenn nötig auf den neuesten Stand gebracht sein;
- e müssen so aufbewahrt werden, daß der Betroffene nicht länger identifiziert werden kann, als es die Zwecke, für die sie gespeichert sind, erfordern.“

Artikel 7 - Datensicherung

„Für den Schutz personenbezogener Daten, die in automatisierten Dateien/Datensammlungen gespeichert sind, werden geeignete Sicherungsmaßnahmen getroffen gegen die zufällige oder unbefugte Zerstörung, gegen zufälligen Verlust sowie unbefugten Zugang, unbefugte Veränderung oder unbefugtes Bekanntgeben.“

Artikel 8 – Zusätzlicher Schutz für den Betroffenen

„Jedermann muß die Möglichkeit haben:

- a das Vorhandensein einer automatisierten Datei/Datensammlung mit personenbezogenen Daten, ihre Hauptzwecke sowie die Bezeichnung, den gewöhnlichen Aufenthaltsort oder den Sitz des Verantwortlichen für die Datei/Datensammlung festzustellen;
- b in angemessenen Zeitabständen und ohne unzumutbare Verzögerung oder übermäßige Kosten die Bestätigung zu erhalten, ob Daten über ihn in einer automatisierten Datei/Datensammlung mit personenbezogenen Daten gespeichert sind, sowie zu erwirken, daß ihm diese Daten in verständlicher Form mitgeteilt werden;

c gegebenenfalls diese Daten berichtigen oder löschen zu lassen, wenn sie entgegen den Vorschriften des innerstaatlichen Rechts verarbeitet worden sind, welche die Grundsätze der Artikel 5 und 6 verwirklichen;

d über ein Rechtsmittel zu verfügen, wenn seiner Forderung nach Bestätigung oder gegebenenfalls nach Mitteilung, Berichtigung oder Löschung im Sinne der Buchstaben b und c nicht entsprochen wird.“

Artikel 9 – Ausnahmen und Einschränkungen

„Ausnahmen von den Artikeln 5, 6 und 8 sind nicht zulässig, abgesehen von den in diesem Artikel vorgesehenen.

Eine Abweichung von den Artikeln 5, 6 und 8 ist zulässig, wenn sie durch das Recht der Vertragspartei vorgesehen und in einer demokratischen Gesellschaft eine notwendige Maßnahme ist:

a zum Schutz der Sicherheit des Staates, der öffentlichen Sicherheit sowie der Währungsinteressen des Staates oder zur Bekämpfung von Straftaten;

b zum Schutz des Betroffenen oder der Rechte und Freiheiten Dritter.

Die Ausübung der Rechte nach Artikel 8 Buchstaben b, c und d kann durch Gesetz für automatisierte Dateien/Datensammlungen mit personenbezogenen Daten eingeschränkt werden, die Zwecken der Statistik oder der wissenschaftlichen Forschung dienen, wenn offensichtlich keine Gefahr besteht, daß der Persönlichkeitsbereich der Betroffenen beeinträchtigt wird.“

Das Datenschutzübereinkommen wird derzeit aktualisiert, unter anderem um den mit der Nutzung neuer Informations- und Kommunikationstechnologien verbundenen Herausforderungen besser gerecht zu werden. Ein Änderungsprotokoll zum Datenschutzübereinkommen liegt seit dem 10. Oktober 2018 für die Vertragsstaaten des Übereinkommens zur Unterzeichnung auf und wurde von Deutschland an diesem Tag unterzeichnet.

V. RECHTSVERGLEICHUNG

58. Aus einem rechtsvergleichenden Bericht über die Vorgehensweisen von 34 Mitgliedstaaten des Europarats im Bereich der Speicherung der Teilnehmerdaten von Prepaid-SIM-Kartenkunden geht hervor, dass Telekommunikationsdiensteanbieter in 15 Staaten diese Daten speichern müssen und dass derzeit keiner der untersuchten Staaten seinen Behörden gestattet, ihre eigenen Datenbanken mit personenbezogenen Daten von Telekommunikationsanschlussinhabern zu führen. Ferner gibt es Unterschiede, was die erlaubte Dauer der Speicherung dieser Daten, die Zwecke, für die sie genutzt werden dürfen, und die Verfahrenserfordernisse, die für den Zugriff auf die Daten erfüllt sein müssen, angeht. Insbesondere schreibt eine Mehrheit der Staaten eine Liste konkreter Behörden, denen der Zugang zu Teilnehmerdaten gestattet ist, gesetzlich fest und beschränkt die vertretbaren Zwecke auf die Ermittlung von Straftaten oder die Abwendung von Gefahren für die öffentliche Ordnung. In den meisten Staaten umfassen

die Verfahrenserfordernisse für den Zugang zu gespeicherten Teilnehmerdaten auch eine gerichtliche oder staatsanwaltschaftliche Anordnung, typischerweise wenn die Teilnehmerdaten hauptsächlich für die Zwecke strafrechtlicher Ermittlungen verwendet werden. Schließlich verlangt nur eine Minderheit der Staaten, dass Kunden zu benachrichtigen sind, wenn auf ihre persönlichen Daten zugegriffen wurde.

RECHTLICHE WÜRDIGUNG

BEHAUPTETE VERLETZUNG VON ARTIKEL 8 UND 10 DER KONVENTION

59. Die Beschwerdeführer rügten, aufgrund der gesetzlichen Verpflichtung aus § 111 TKG seien von ihnen als Nutzer von Prepaid-Mobilfunkkarten bestimmte personenbezogene Daten durch ihren jeweiligen Telekommunikationsdiensteanbieter gespeichert worden. Sie beriefen sich auf ihr Recht auf Achtung des Privatlebens und der Korrespondenz nach Artikel 8 der Konvention sowie auf ihr Recht auf freie Meinungsäußerung nach Artikel 10 der Konvention, die, soweit in der vorliegenden Rechtssache relevant, wie folgt lauten:

Artikel 8

„1. Jede Person hat ein Recht auf Achtung ihres Privat(...)lebens ... und ihrer Korrespondenz.

2. Eine Behörde darf in die Ausübung dieses Rechts nur eingreifen, soweit der Eingriff gesetzlich vorgesehen und in einer demokratischen Gesellschaft notwendig ist für die nationale oder öffentliche Sicherheit [...], zur Aufrechterhaltung der Ordnung, zur Verhütung von Straftaten, [...].“

Artikel 10

„1. Jede Person hat das Recht auf freie Meinungsäußerung. Dieses Recht schließt die Meinungsfreiheit und die Freiheit ein, Informationen und Ideen ohne behördliche Eingriffe und ohne Rücksicht auf Staatsgrenzen zu empfangen und weiterzugeben. [...]

2. Die Ausübung dieser Freiheiten ist mit Pflichten und Verantwortung verbunden; sie kann daher Formvorschriften, Bedingungen, Einschränkungen oder Strafdrohungen unterworfen werden, die gesetzlich vorgesehen und in einer demokratischen Gesellschaft notwendig sind für die nationale Sicherheit [...] oder die öffentliche Sicherheit [...], zur Aufrechterhaltung der Ordnung oder zur Verhütung von Straftaten, [...].“

A. Umfang der Beschwerde und Würdigung durch den Gerichtshof

1. Zu prüfende Konventionsrechte

60. Zunächst stellt der Gerichtshof fest, dass sich die Beschwerdeführer auf Artikel 8 (Recht auf Achtung des Privatlebens und der Korrespondenz) und Artikel 10 (Recht auf anonyme Kommunikation als ein Aspekt der freien Meinungsäußerung) beriefen. Er nimmt jedoch auch zur Kenntnis, dass die Beschwerdeführer vor dem Gerichtshof lediglich die Vereinbarkeit des § 111 TKG mit der Konvention in Frage stellten. Sie rügten nicht ausdrücklich die §§ 112 oder 113 TKG, die auch Gegenstand ihrer Beschwerde beim Bundesverfassungsgericht waren, oder etwaige weitere Maßnahmen im Zusammenhang mit der Überwachung oder dem Abfangen von Telekommunikation. Dies bedeutet jedoch nicht, dass sich diese anderen Bestimmungen des TKG bei der Prüfung der Verhältnismäßigkeit des gerügten Eingriffs und seiner Wirkung in der Praxis nicht als relevant erweisen werden (Rdnrn. 97-101).

61. § 111 TKG betrifft nur die Speicherung von Teilnehmerdaten, nämlich die Rufnummer, den Namen und die Anschrift sowie das Geburtsdatum und das Datum des Vertragsbeginns. Die Bestimmung erstreckt sich nicht auf Verkehrsdaten, Standortdaten oder Daten, die Kommunikationsinhalte offenbaren. Auch haben die Beschwerdeführer nicht geltend gemacht, dass ihre Kommunikation abgefangen oder ihre Telekommunikation einer sonstigen Überwachungsmaßnahme unterworfen worden wäre. Der gerügte Eingriff betrifft die Speicherung des vorstehend beschriebenen Datensatzes und die Möglichkeit innerstaatlicher Behörden, unter bestimmten, festgelegten Umständen auf diesen Datensatz zuzugreifen. Daher berücksichtigt der Gerichtshof zwar die Umstände der in Rede stehenden Datenspeicherung und die Nähe dieser Speicherung zur Telekommunikation und zum Recht auf Achtung der Korrespondenz, er ist aber dennoch der Auffassung, dass der Hauptaspekt der Rüge der Beschwerdeführer die Speicherung ihrer persönlichen Daten ist und nicht ein bestimmter Eingriff in ihre Korrespondenz oder ihre freie Meinungsäußerung.

62. Der Gerichtshof hat daher in der vorliegenden Sache nicht darüber zu entscheiden, ob und inwieweit Artikel 10 so verstanden werden kann, dass er Nutzern von Telekommunikationsdiensten ein Recht auf Anonymität garantiert (bezüglich des Interesses von Internetnutzern auf Nichtoffenlegung ihrer Identität, siehe *Delfi AS ./. Estland* [GK], Individualbeschwerde Nr. 64569/09, Rdnr. 147, 16. Juni 2015), und wie dieses Recht gegen andere zwingende Gebote abzuwägen wäre (siehe sinngemäß *K.U. ./. Finnland*, Individualbeschwerde Nr. 2872/02, Rdnr. 49, 2. Dezember 2008).

63. Zusammengefasst sieht es der Gerichtshof als verhältnismäßig an, die Rügen der Beschwerdeführer lediglich im Hinblick auf das Recht auf Achtung des Privatlebens nach Artikel 8 der Konvention zu prüfen.

2. Zeitraum, auf den sich die Prüfung erstreckt

64. Der Gerichtshof nimmt zur Kenntnis, dass die Telekommunikationsdiensteanbieter die Teilnehmerdaten der Beschwerdeführer ab dem Zeitpunkt der Registrierung ihrer SIM-Karten vorübergehend gespeichert haben. Ferner nimmt er zur Kenntnis, dass § 111 TKG in den Jahren 2007 und 2016 geändert wurde. Er stellt jedoch fest, dass das Bundesverfassungsgericht in seinem Urteil vom 24. Januar 2012 das TKG in der am 1. Januar 2008 geltenden Fassung geprüft hat und dass ein Verfahren betreffend eine spätere Änderung des TKG im Jahr 2016 noch bei ihm anhängig ist (siehe Rdnrn. 11 und 28). Daher wird der Gerichtshof die einschlägigen Bestimmungen in der am 1. Januar 2008 geltenden Fassung prüfen.

B. Zulässigkeit

65. Der Gerichtshof stellt fest, dass diese Rüge nicht im Sinne von Artikel 35 Abs. 3 Buchst. a der Konvention offensichtlich unbegründet ist. Sie ist auch nicht aus anderen Gründen unzulässig. Folglich ist sie für zulässig zu erklären.

C. Begründetheit

1. Die Stellungnahmen der Parteien

(a) Die Beschwerdeführer

66. Die Beschwerdeführer machten geltend, die Verpflichtung zur Speicherung ihrer personenbezogenen Daten gemäß § 111 TKG greife in ihr Recht auf Privatsphäre ein, da diese Verpflichtung sie zur Offenlegung ihrer personenbezogenen Daten, die anschließend gespeichert würden, zwingt. Dieser Eingriff sei nicht gerechtfertigt, da er insbesondere unverhältnismäßig und in einer demokratischen Gesellschaft nicht notwendig sei. Zunächst sei die Regelung kein geeignetes Mittel, da es zum damaligen Zeitpunkt problemlos möglich gewesen sei, eine Identifizierung durch Angabe falscher Namen oder Verwendung gestohlener, gebrauchter oder ausländischer SIM-Karten zu umgehen. Weiterhin fehle es an der Notwendigkeit, da verdächtige Mobilfunknutzer problemlos durch andere Ermittlungsmaßnahmen identifiziert werden könnten. Folglich habe die Änderung des § 111 TKG nicht zu einem Rückgang von Straftaten geführt.

67. Die Beschwerdeführer trugen vor, der Eingriff sei sehr schwerwiegend, da es sich um eine vorsorgliche Massenspeicherung von personenbezogenen Daten aller Nutzer von Telekommunikationsdiensten handele. Die Regelung knüpfe die Speicherung an keinerlei Voraussetzungen, sondern gelte allgemein für alle Mobiltelefonnutzer. Die Betroffenen seien ganz überwiegend unschuldige Personen, die auch keine Gefahr oder Bedrohung für die öffentliche oder nationale Sicherheit darstellten. Die Beschwerdeführer trugen in diesem Zusammenhang vor, dass nach Angaben der Bundesnetzagentur die Anzahl der im automatisierten Verfahren nach § 112 TKG abgefragten Datensätze von 26,62 Millionen im Jahr 2008 auf 34,83 Millionen im Jahr 2015 gestiegen sei. Darüber hinaus unterscheide die Regelung auch nicht zwischen „normaler“ Kommunikation und Kommunikation, die durch die Konvention besonders geschützt sei, wie z. B. Anwaltsberatungen oder Arztgespräche. Zudem erhöhe die Speicherung der Daten die Gefahr von Missbrauch und Datenlecks und somit die Gefahr von Identitätsbetrug.

(b) Die Regierung

68. Die Regierung räumte ein, dass § 111 TKG einen Eingriff in das Recht der Beschwerdeführer auf Privatsphäre darstelle. Die Regelung verpflichte die Dienstanbieter zur Speicherung ihrer personenbezogenen Daten. Die Regierung betonte, dass keine so genannten Verkehrsdaten – d. h. im Laufe eines Kommunikationsprozesses anfallende Daten – gespeichert würden, sondern lediglich die oben aufgeführten Teilnehmerinformationen (Rdnr. 61). Darüber hinaus müsse § 111 im Zusammenhang mit den §§ 112 und 113 TKG sowie mit weiteren einschränkenden Regelungen, die den Zugriff auf die gespeicherten Daten regelten, gesehen werden, da die Behörden zum Abruf der Teilnehmerdaten jeweils eine gesetzliche Grundlage benötigten.

69. Dieser begrenzte Eingriff diene den legitimen Zielen der öffentlichen Sicherheit, Aufrechterhaltung der Ordnung, Verhütung von Straftaten und des Schutzes der Rechte und Freiheiten anderer und sei insofern ein geeignetes Mittel, da er den Sicherheitsbehörden erlaube, eine Verbindung zwischen Mobiltelefonnummern von Prepaid-SIM-Karten und einzelnen Personen herzustellen. Diese Möglichkeit trage zu einer effektiven Strafverfolgung bei und diene der Gefahrenabwehr. Die Möglichkeiten zur Umgehung der Regelung seien durch die Gesetzesänderung von 2016 weiter eingeschränkt worden (siehe Rdnr. 28).

70. Die in Frage stehende Regelung entspreche auch den Anforderungen an den Schutz personenbezogener Daten, wie sie vom Gerichtshof in der Rechtssache *S. und Marper ./. Vereinigtes Königreich* ([GK], Individualbeschwerden Nrn. 30562/04 und 30566/04, Rdnr. 103, ECHR 2008) festgelegt worden seien. Sie begrenze die Datenmenge auf das für die Identifizierung unbedingt erforderliche Maß. Die Dauer der

Datenspeicherung sei klar definiert und auf eine Höchstdauer befristet, die die durch den verfolgten Zweck erforderliche Dauer nicht überschreiten dürfe. Darüber hinaus stellten die §§ 112 und 113 TKG in Verbindung mit den jeweiligen besonderen Abrufregelungen wirksame Schutzvorkehrungen gegen Missbrauch dar.

71. Es sei weiterhin zu berücksichtigen, dass der Beurteilungsspielraum (margin of appreciation) der Mitgliedsstaaten relativ groß sei, nicht nur, weil die deutschen Behörden einen Ausgleich zwischen verschiedenen kollidierenden, durch die Konvention geschützten Rechten und Pflichten finden müssten (Verweis auf *Evans ./. Vereinigtes Königreich* [GK], Individualbeschwerde Nr. 6339/05, Rdnr. 77, 10. April 2007), sondern auch, weil kein europäischer Konsens hinsichtlich der Verpflichtung zur Speicherung von Teilnehmerdaten beim Erwerb von Prepaid-Mobilfunkkarten bestehe. Zusammenfassend sei die Speicherung eines äußerst begrenzten Datenbestandes, der durch eine Reihe von verfahrensrechtlichen Vorkehrungen geschützt sei, angesichts der bedeutenden Belange der öffentlichen Sicherheit, Aufrechterhaltung der Ordnung und Verhütung von Straftaten verhältnismäßig.

(c) Die Drittbeteiligten

72. Die Drittbeteiligten Privacy International und ARTICLE 19 unterstrichen die Bedeutung von Anonymität und anonymer Rede für eine demokratische Gesellschaft und die Rechte der Bürger auf Privatsphäre und freie Meinungsäußerung. Deren zentrale Rolle sei zunehmend von innerstaatlichen Gerichten und internationalen Organisationen wie den Vereinten Nationen und dem Europarat anerkannt worden. Darüber hinaus habe der Gerichtshof selbst die Bedeutung von Anonymität in dem Urteil *Delfi AS ./. Estland* (a. a. O., Rdnrn. 147-48) bekräftigt. Weiterhin wiesen die Drittbeteiligten darauf hin, dass die Gerichte in Europa eine pauschale, unterschiedslose Speicherung von der Identifizierung dienenden Informationen und Verkehrsdaten auf Vorrat für den – zweifellos wichtigen – Kampf gegen schwere Straftaten zunehmend als unverhältnismäßig werteten. Dies wurde auch vom EuGH in seinem Urteil *Digital Rights Ireland* und *Seitlinger u. a.* (Rdnr. 51) bestätigt.

2. Würdigung durch den Gerichtshof

(a) Allgemeine Grundsätze

73. Der Gerichtshof erinnert daran, dass der Begriff des „Privatlebens“ weit gefasst und einer abschließenden Definition nicht zugänglich ist. Artikel 8 schützt unter anderem das Recht auf Identität und persönliche Entwicklung sowie das Recht, Beziehungen zu anderen Menschen und zur Außenwelt einzugehen und zu entwickeln. Daher gibt es auch in einem öffentlichen Kontext einen Bereich, in dem eine Person mit anderen

interagiert, der unter den Begriff des „Privatlebens“ fallen kann (*U. ./.* Deutschland, Individualbeschwerde Nr. 35623/05, Rdnr. 43, 2. September 2010).

74. In Bezug auf personenbezogene Daten verwies der Gerichtshof darauf, dass der Begriff „Privatleben“ nicht restriktiv auszulegen sei. Er stellte fest, dass die weite Auslegung mit der des Datenschutzübereinkommens übereinstimmt, dessen Zweck es ist, „im Hoheitsgebiet jeder Vertragspartei für jedermann [...] sicherzustellen, dass seine Rechte und Grundfreiheiten, insbesondere sein Recht auf einen Persönlichkeitsbereich, bei der automatischen Verarbeitung personenbezogener Daten geschützt werden“ (Artikel 1), wobei diese personenbezogenen Daten definiert werden als „jede Information über eine bestimmte oder bestimmbare natürliche Person“ (Artikel 2) (siehe *Amann ./.* Schweiz [GK], Individualbeschwerde Nr. 27798/95, Rdnr. 65, 16. Februar 2000).

75. Aus der ständigen Rechtsprechung des Gerichtshofs folgt ferner, dass im Hinblick auf die Sammlung von Daten über einzelne Personen, die Verarbeitung oder Verwendung personenbezogener Daten oder die Veröffentlichung des betreffenden Materials in einer Weise oder einem Ausmaß, die bzw. das über das üblicherweise vorhersehbare Maß hinausgeht, Erwägungen zum [Schutz des] Privatleben angezeigt seien. Artikel 8 der Konvention gewährt daher das Recht auf eine Form der informationellen Selbstbestimmung, die es dem Einzelnen erlaubt, sich auf sein Recht auf Privatsphäre in Bezug auf Daten zu berufen, die, obwohl sie neutral sind, zusammengekommen und in einer Art oder Weise erhoben, verarbeitet und verbreitet werden, dass sie seine Rechte aus Artikel 8 berühren können (siehe *Satakunnan Markkinapörssi Oy und Satamedia Oy ./.* Finnland [GK], Individualbeschwerde Nr. 931/13, Rdnrn. 136-37, 27. Juni 2017, mit weiteren Nachweisen).

76. Der Gerichtshof stellt fest, dass er zwar bereits mit einer Vielzahl von Eingriffen in das Recht auf Privatleben nach Artikel 8 der Konvention durch die Speicherung, Verarbeitung und Nutzung personenbezogener Daten befasst war – siehe beispielsweise zum Einsatz von GPS-Überwachung bei strafrechtlichen Ermittlungen (*U. ./.* Deutschland, Individualbeschwerde Nr. 35623/05, 2. September 2010, oder *Ben Faiza ./.* Frankreich, Individualbeschwerde Nr. 31446/12, 8. Februar 2018), zur Offenlegung von der Identifizierung dienenden Informationen an Strafverfolgungsbehörden durch Telekommunikationsanbieter (*K.U ./.* Finnland, Individualbeschwerde Nr. 2872/02, 2. Dezember 2008 oder *Benedik ./.* Slowenien, Individualbeschwerde Nr. 62357/14, 24. April 2018), zur unbefristeten Aufbewahrung von Fingerabdrücken, Zellproben und DNA-Profilen nach einem Strafverfahren (*S. und Marper*, a. a. O.), zur Registrierung (metering) oder Erhebung von Nutzungs- oder Verkehrsdaten (*Malone ./.* Vereinigtes Königreich, Individualbeschwerde Nr. 8691/79,

2. August 1984, *Copland* ./ *Vereinigtes Königreich*, Individualbeschwerde Nr. 62617/00, 3. April 2007) oder zur Aufnahme von Sexualstraftätern in eine automatisierte nationale Datei der Justizbehörden nach einer Verurteilung wegen Vergewaltigung (*B.B.* ./ *Frankreich*, Individualbeschwerde Nr. 5335/06, *Gardel* ./ *Frankreich*, Individualbeschwerde Nr. 16428/05 und *M.B.* ./ *Frankreich*, Individualbeschwerde Nr. 22115/06, alle 17. Dezember 2009) – jedoch hat keiner der früheren Fälle die Speicherung eines Datensatzes wie im vorliegenden Fall betroffen.

77. Eine Verpflichtung, ähnlich wie in § 111 TKG, zur Einrichtung von Dateien, in denen Informationen (bei natürlichen Personen Vorname, Name des Vaters und Familienname, Wohnadresse und Passnummer) über alle Teilnehmer gespeichert werden und die den Strafverfolgungsbehörden Fernzugriff auf die Dateien ermöglichen, war Teil des Systems der heimlichen Überwachung, mit dem sich der Gerichtshof im Fall von *Roman Zakharov* ./ *Russland* ([GK], Individualbeschwerde Nr. 47143/06, Rdnrn. 132-33 und 269-70, 4. Dezember 2015) befasst hat. Angesichts anderer Möglichkeiten der russischen Behörden zum Abfangen von Telekommunikation war die bloße Verpflichtung zur Speicherung von Teilnehmerinformationen und zur Ermöglichung eines Fernzugriffs auf diese Datei für den Gerichtshof in diesem Fall jedoch nicht maßgeblich für die Feststellung eines Verstoßes gegen Artikel 8.

78. In seinem Urteil *S. und Marper* (a. a. O., Rdnr. 103) entschied der Gerichtshof wie folgt:

„Der Schutz personenbezogener Daten ist von grundlegender Bedeutung für die Wahrnehmung des Rechts des Einzelnen auf Achtung des Privat- und Familienlebens, das in Artikel 8 der Konvention gewährleistet wird. Das innerstaatliche Recht muss angemessene Schutzvorkehrungen vorsehen, um eine Verwendung personenbezogener Daten zu verhindern, die mit den Gewährleistungen dieses Artikels unvereinbar sein könnte [...]. Solche Schutzvorkehrungen sind umso mehr geboten in Bezug auf den Schutz personenbezogener Daten, die automatisch verarbeitet werden, vor allem auch, wenn diese Daten für polizeiliche Zwecke verwendet werden. Das innerstaatliche Recht sollte insbesondere die Relevanz dieser Daten sicherstellen und dafür Sorge tragen, dass die Datenverarbeitung nicht über die Zwecke, für die sie gespeichert werden, hinausgeht; zudem müssen die Daten in einer Form aufbewahrt werden, die eine Identifizierung der betroffenen Personen nicht länger ermöglicht, als es die Zwecke, für die sie gespeichert wurden, erfordern (siehe Artikel 5 Datenschutzübereinkommen [...], Rdnr. 47). Das innerstaatliche Recht muss auch angemessene Gewährleistungen dafür vorsehen, dass auf Vorrat gespeicherte personenbezogene Daten wirksam vor unsachgemäßem Gebrauch und Missbrauch geschützt werden (siehe Artikel 7 Datenschutzübereinkommen – Rdnr. 47) [...]“.

79. Der Gerichtshof hat anerkannt, dass die nationalen Behörden bei der Abwägung zwischen dem Interesse des beschwerdegegnerischen Staates am Schutz seiner nationalen Sicherheit durch geheime Überwachungsmaßnahmen und der Schwere des Eingriffs in das Recht

eines Beschwerdeführers oder einer Beschwerdeführerin auf Achtung seines bzw. ihres Privatlebens über einen gewissen Beurteilungsspielraum bei der Wahl der Mittel zur Erreichung des legitimen Ziels des Schutzes der nationalen Sicherheit verfügen. Dieser Spielraum unterliegt indes einer europäischen Kontrolle, die sowohl die Gesetzgebung als auch die Entscheidungen, in denen sie angewendet wird, umfasst (*Roman Zakharov*, a. a. O., Rdnr. 232; *Liblik u. a. ./ Estland*, Individualbeschwerden Nrn. 173/15 u. a., Rdnr. 131, 28. Mai 2019; *Szabo und Vissy ./ Ungarn*, Individualbeschwerde Nr. 37138/14, Rdnr. 57, 12. Januar 2016).

80. Die Weite des Beurteilungsspielraums variiert und hängt von verschiedenen Faktoren ab, wie der Art des betroffenen Konventionsrechts, seiner Bedeutung für den Einzelnen, der Art des Eingriffs und dem durch den Eingriff verfolgten Ziel. Der Spielraum ist in der Regel geringer, wenn das betreffende Recht entscheidend dafür ist, dass der Einzelne vertrauliche oder zentrale Rechte wirksam in ausüben kann. Wo jedoch zwischen den Mitgliedstaaten des Europarats kein Konsens besteht – sei es über die relative Bedeutung des fraglichen Belanges oder darüber, wie er am besten geschützt werden kann – ist der Spielraum größer (siehe *S. und Marper*, a. a. O., Rdnr. 102).

(b) Anwendung dieser Grundsätze auf die vorliegende Rechtssache

(i) Vorliegen eines Eingriffs

81. Dass die Verpflichtung der Diensteanbieter zur Speicherung personenbezogener Daten gemäß § 111 TKG einen Eingriff in das Recht der Beschwerdeführer auf Achtung ihres Privatlebens darstellt, da ihre personenbezogenen Daten gespeichert wurden, ist zwischen den Parteien unstrittig. In diesem Zusammenhang weist der Gerichtshof erneut darauf hin, dass die bloße Speicherung von Daten, die das Privatleben einer Person betreffen, einen Eingriff im Sinne von Artikel 8 der Konvention darstellt (*Leander ./ Schweden*, 26. März 1987, Rdnr. 48, Serie A Bd. 116). Er nimmt ferner die Feststellung des Bundesverfassungsgerichts zur Kenntnis, wonach der Schutzzumfang des Rechts auf informationelle Selbstbestimmung sich nach innerstaatlichem Recht nicht auf ihrer Art nach sensible Informationen beschränke und es angesichts der Verarbeitungs- und Verknüpfungsmöglichkeiten kein schlechthin, also ungeachtet des Verwendungskontextes, belangloses personenbezogenes Datum gebe (siehe Rdnr. 14 (Rdnr. 122 der BVerfG-Entscheidung)).

(ii) Rechtfertigung für den Eingriff

82. Der Gerichtshof weist erneut darauf hin, dass ein Eingriff in das Recht eines Beschwerdeführers oder einer Beschwerdeführerin auf Achtung seines bzw. ihres Privatlebens gegen Artikel 8 verstößt, es sei denn, der Eingriff ist „gesetzlich vorgesehen“, verfolgt eines oder mehrere der in

Absatz 2 genannten legitimen Ziele und ist darüber hinaus zur Erreichung dieser Ziele „in einer demokratischen Gesellschaft notwendig“ (siehe *M.N. u. a. ./ San Marino*, Individualbeschwerde Nr. 28005/12, Rdnr. 71, 7. Juli 2015, mit weiteren Nachweisen).

(α) „Gesetzlich vorgesehen“

83. Nach ständiger Rechtsprechung des Gerichtshofs bedeutet das Erfordernis des „gesetzlich vorgesehen“ Eingriffs nicht nur, dass die fragliche Maßnahme eine Grundlage im innerstaatlichen Recht haben, sondern auch, dass das Recht für die betroffene Person verfügbar und in seinen Auswirkungen vorhersehbar sein sollte. Unter anderem im Zusammenhang mit der Speicherung von personenbezogenen Daten sind klare, detaillierte Regelungen für ein Mindestmaß an Schutzvorkehrungen erforderlich, unter anderem in Bezug auf die Dauer, die Speicherung, die Nutzung, den Zugang Dritter, die Verfahren zum Schutz der Integrität und Vertraulichkeit der Daten sowie die Verfahren zu ihrer Vernichtung (siehe *S. und Marper*, a. a. O., Rdnr. 99, mit weiteren Nachweisen).

84. Der Gerichtshof stellt fest, dass die Speicherung der personenbezogenen Daten der Beschwerdeführer beim Erwerb von SIM-Karten für Mobiltelefone auf der Grundlage der Regelung in § 111 TKG erfolgte, die hinsichtlich des Umfangs der gespeicherten Daten hinreichend klar und vorhersehbar war. Darüber hinaus wurde die Dauer der Speicherung klar geregelt und die technische Seite der Speicherung war zumindest nach Erlass der entsprechenden Verordnung und Technischen Richtlinie klar umrissen.

85. Im Hinblick auf Schutzvorkehrungen, den Zugang Dritter und die Weiterverwendung der gespeicherten Daten ist § 111 TKG im Zusammenhang mit den §§ 112 und 113 sowie, gemäß dem durch das Bundesverfassungsgericht erläuterten ‘Doppeltürenmodell’ (siehe Rdnr. § 14 (Rdnr. 123 der BVerfG-Entscheidung)), zusätzlich im Zusammenhang mit der entsprechenden Rechtsgrundlage für individuelle Auskunftersuchen zu betrachten. Der Gerichtshof gelangt indes zu der Auffassung, dass die Frage der Vorhersehbarkeit und der ausreichenden Regelungstiefe dieser Bestimmungen im vorliegenden Fall eng mit den allgemeineren Fragen verbunden ist, ob der Eingriff in einer demokratischen Gesellschaft notwendig und verhältnismäßig war. Er wird diese Fragen daher nachstehend eingehender würdigen (siehe Rdnr. 88-110).

(β) Legitimes Ziel

86. Im Hinblick auf den Kontext der in Rede stehenden Datenspeicherung, und insbesondere auf die Zwecke von Auskunftersuchen und die gemäß den §§ 112 und 113 TKG berechtigten Behörden folgt der Gerichtshof der Argumentation der Regierung, wonach der Eingriff die legitimen Ziele der öffentlichen Sicherheit, der

Aufrechterhaltung der Ordnung, der Verhütung von Straftaten und des Schutzes der Rechte und Freiheiten anderer verfolge.

87. In diesem Zusammenhang bezieht sich der Gerichtshof auf die Begründung der Entscheidung des Bundesverfassungsgerichts, wonach der Zugang zu den gespeicherten Informationen „zum Zweck der Gefahrenabwehr, zur Verfolgung von Straftaten oder Ordnungswidrigkeiten sowie zur Wahrnehmung nachrichtendienstlicher Aufgaben“ erlaubt sei (siehe Rdnr. 21 (Rdnr. 176 der BVerfG-Entscheidung)). Das TKG führt diese Zwecke weiter aus und legt fest, dass Auskunftersuchen zulässig sind, soweit diese zur Verfolgung von Straftaten und Ordnungswidrigkeiten, zur Gefahrenabwehr und zur Erfüllung nachrichtendienstlicher Aufgaben erforderlich sind (siehe Rdnr. 31).

(γ) „Notwendig in einer demokratischen Gesellschaft“

88. Ein Eingriff ist „in einer demokratischen Gesellschaft notwendig“ zur Erreichung eines legitimen Ziels, wenn er ein „dringendes gesellschaftliches Bedürfnis“ erfüllt und in einem angemessenen Verhältnis zu dem verfolgten legitimen Ziel steht. Der Gerichtshof wertet die Verbrechensbekämpfung, insbesondere die Bekämpfung der organisierten Kriminalität und des Terrorismus, die eine der aktuellen Herausforderungen für die europäischen Gesellschaften darstellt, die Aufrechterhaltung der öffentlichen Sicherheit und den Schutz der Bürger als „dringende gesellschaftliche Bedürfnisse“ (vgl. sinngemäß *Szabo und Vissy* ./ Ungarn, a. a. O., Rdnr. 68, 12. Januar 2016; *Ramda* ./ Frankreich, Individualbeschwerde Nr. 78477/11, Rdnr. 96, 19. Dezember 2017). Er erkennt gleichfalls an, dass moderne Telekommunikationsmittel und Veränderungen im Kommunikationsverhalten eine Anpassung der Ermittlungsinstrumente der Strafverfolgungsbehörden und der nationalen Sicherheitsbehörden erfordern (*S. und Marper*, a. a. O., Rdnr. 105).

89. Der Gerichtshof nimmt die Argumentation der Regierung zur Kenntnis, der zufolge die Möglichkeit, eine Verbindung zwischen Mobiltelefonnummern von Prepaid-SIM-Karten und bestimmten Personen herzustellen, für eine wirksame Strafverfolgung und zur Gefahrenabwehr erforderlich sei. Dagegen bestreiten die Beschwerdeführer die Wirksamkeit von § 111 TKG, da es keine empirischen Belege für einen Rückgang von Straftaten aufgrund einer verpflichtenden Registrierung gebe. Darüber hinaus argumentieren sie, dass die Identifizierung problemlos durch die Angabe falscher Namen oder die Verwendung gestohlener, gebrauchter oder ausländischer SIM-Karten umgangen werden könne.

90. Der Gerichtshof erkennt an, dass die vorherige Registrierung von Mobilfunkteilnehmern die Ermittlungen der Strafverfolgungsbehörden deutlich erleichtert und beschleunigt und damit zu einer wirksamen Strafverfolgung und zur Aufrechterhaltung der Ordnung und Verhütung von Straftaten beitragen kann. Darüber hinaus ist er der Auffassung, dass

vorhandene Möglichkeiten zur Umgehung rechtlicher Pflichten kein Grund sein können, den allgemeinen Nutzen und die allgemeine Wirksamkeit einer gesetzlichen Regelung in Frage zu stellen. Schließlich bekräftigt der Gerichtshof, dass die nationalen Behörden im Bereich der nationalen Sicherheit einen gewissen Beurteilungsspielraum bei der Wahl der Mittel zur Erreichung eines legitimen Ziels haben, und stellt den rechtsvergleichenden Ausführungen zufolge fest, dass kein Konsens zwischen den Mitgliedstaaten hinsichtlich der Speicherung von Teilnehmerdaten von Prepaid-Sim-Karten-Kunden besteht (siehe Rdnr. 58). In Anbetracht dieses Beurteilungsspielraums erkennt der Gerichtshof an, dass die Verpflichtung zur Speicherung von Teilnehmerinformationen gemäß § 111 TKG eine grundsätzlich geeignete Reaktion auf Veränderungen im Kommunikationsverhalten und in den Telekommunikationsmitteln darstellt.

91. Es bleibt jedoch die Frage, ob der Eingriff verhältnismäßig war und einen gerechten Ausgleich zwischen den kollidierenden öffentlichen und privaten Belangen geschaffen hat.

92. Zunächst obliegt es dem Gerichtshof, das Gewicht des Eingriffs in das Recht der Beschwerdeführer auf Privatleben festzustellen. In dieser Hinsicht teilt der Gerichtshof die Auffassung des Bundesverfassungsgerichts (siehe Rdnr. 15 (Rdnrn. 138 und 139 der BVerfG-Entscheidung)), dass nur ein begrenzter Datensatz gespeichert worden sei. Diese Daten umfassten weder höchstpersönliche Informationen noch war mit ihnen die Erstellung von Persönlichkeits- oder Bewegungsprofilen der Mobilfunkteilnehmer möglich. Darüber hinaus wurden keine Daten zu einzelnen Telekommunikationsvorgängen gespeichert. Das Eingriffsgewicht ist daher klar von früheren Fällen des Gerichtshofs zu unterscheiden, die z. B. die Registrierung von Kommunikationsdaten (metering) (siehe *Malone und Copland*, a. a. O.), Geolokalisierung (*Uzun und Ben Faiza*, a. a. O.), oder die Speicherung von Gesundheits- oder anderen sensiblen Daten (siehe z. B., *S. und Marper*, a. a. O., M.M. ./.. Vereinigtes Königreich, Individualbeschwerde Nr. 24029/07, 13. November 2012) betrafen. Darüber hinaus ist der vorliegende Fall von Fällen zu unterscheiden, in denen die Registrierung in einer bestimmten Datei zu häufigen Überprüfungen oder zur weiteren Sammlung privater Informationen führte (siehe *Dimitrov-Kazakov ./.. Bulgarien*, Individualbeschwerde Nr. 11379/03, 10. Februar 2011, *Shimovolos ./.. Russland*, Individualbeschwerde Nr. 30194/09, 21. Juni 2011).

93. Soweit die Beschwerdeführer schließlich geltend machen, dass der Eingriff schwerwiegend sei, da § 111 TKG ein Register aller Nutzer von Mobilfunk-SIM-Karten geschaffen habe, und insofern mit der in *Digital Rights Ireland* und *Seitlinger u. a.* sowie *Tele2 Sverige* und *Tom Watson u. a.* (siehe Rdnrn. 51 und 52) in Rede stehenden Datenspeicherung vergleichbar sei, stellt der Gerichtshof fest, dass die in diesen Rechtssachen

gegenständliche Richtlinie auf Verkehrs- und Standortdaten sowohl juristischer als auch natürlicher Personen als auch auf die damit verbundenen Daten, die zur Identifizierung des Teilnehmers oder registrierten Nutzers erforderlich sind, anwendbar ist.

94. Die im vorliegenden Fall betroffenen Daten ähneln tatsächlich eher den in einem anderen Vorabentscheidungsersuchen, *Ministerio fiscal* (Rdnr. 54), betroffenen Daten. Wie der EuGH in diesem letztgenannten Fall feststellte, lassen sich diesen Daten „weder das Datum, die Uhrzeit, die Dauer und die Adressaten der mittels der betreffenden SIM-Karte bzw. der betreffenden SIM-Karten erfolgten Kommunikation entnehmen, noch die Orte, an denen diese Kommunikation erfolgte, oder die Häufigkeit dieser Kommunikation mit bestimmten Personen während eines bestimmten Zeitraums. Aus diesen Daten lassen sich daher keine genauen Schlüsse auf das Privatleben der Personen ziehen, deren Daten betroffen sind.“ Der EuGH kam daher zu dem Schluss, dass der Zugang zu den betreffenden Daten keinen schweren Eingriff in die Grundrechte der Personen, deren Daten betroffen sind, darstellt (siehe Rdnr. 55).

95. Insgesamt wertet der Gerichtshof den Eingriff zwar nicht als geringfügig, aber dennoch als von eher begrenzter Natur.

96. Hinsichtlich der Schutzvorkehrungen stellt der Gerichtshof fest, dass die Beschwerdeführer nicht vorgebracht haben, die fragliche Datenspeicherung sei mit technischen Unsicherheiten behaftet. Zudem ist die Dauer der Speicherung auf den Ablauf des Kalenderjahres begrenzt, das auf das Jahr folgt, in dem das Vertragsverhältnis beendet wurde (§ 111 Abs. 4 TKG – siehe Rdnr. 27). Diese Speicherdauer erscheint nicht unangemessen, da Ermittlungen bei Straftaten einige Zeit in Anspruch nehmen und über das Ende des beendeten Vertragsverhältnisses hinausgehen können. Zudem scheinen die gespeicherten Daten auf die zur eindeutigen Identifizierung des betreffenden Teilnehmers notwendigen Angaben beschränkt zu sein.

97. Der Gerichtshof erkennt ferner, dass beide Parteien von einer Bewertung der Datenspeicherung im Zusammenhang mit den §§ 112 und 113 dieses Gesetzes ausgehen, obwohl die Beschwerdeführer lediglich die Speicherung ihrer personenbezogenen Daten gemäß § 111 TKG beanstanden. Die Regierung argumentierte, dass diese Bestimmungen in Verbindung mit anderen besonderen Regelungen zum Datenabruf den Zugang zu den Daten und deren Nutzung einschränkten und einen wirksamen Schutz gegen Missbrauch darstellten. Die Beschwerdeführer brachten jedoch vor, dass jede weitere Ermittlungsmaßnahme zum Verhalten einer Person – im Rahmen von mobiler Kommunikation – auf den nach § 111 TKG gespeicherten Informationen beruht habe und daher die Möglichkeiten der späteren Verwendung ihrer personenbezogenen Daten bei der Beurteilung der Verhältnismäßigkeit der Regelung in Bezug auf die Datenspeicherung zu berücksichtigen seien. Der Gerichtshof stimmt

mit den Parteien überein, dass im vorliegenden Fall die Würdigung der Verhältnismäßigkeit des Eingriffs nicht möglich ist, ohne den künftigen möglichen Zugang zu den gespeicherten Daten und deren Nutzung eingehend zu prüfen. Er hält es somit für angebracht, die rechtliche Grundlage für Auskunftersuchen und die verfügbaren Schutzvorkehrungen einzubeziehen (siehe sinngemäß *S. und Marper*, a. a. O., Rdnrn. 67, 103, mit weiteren Nachweisen).

98. Hinsichtlich § 112 TKG folgt der Gerichtshof der Auffassung des Bundesverfassungsgerichts (siehe Rdnr. 18 (Rdnr. 156 der BVerfG-Entscheidung)), dass diese Regelung den Behörden die Datenabfragen sehr vereinfacht. Das zentral zusammengefasste und automatisierte Verfahren erlaubt einen Zugang, der praktische Erschwernisse der Datenerhebung weithin beseitigt und die Daten den Behörden ohne zeitliche Verzögerungen oder Reibungsverluste zur Verfügung stellt. Beschränkend wirkt indes die Tatsache, dass § 112 TKG die Behörden, die den Zugang beantragen können, ausdrücklich benennt. Die Liste erscheint zwar breit gefächert, doch alle darin genannten Behörden sind mit der Strafverfolgung oder dem Schutz der nationalen Sicherheit befasst.

99. In Bezug auf § 113 TKG stellt der Gerichtshof zunächst fest, dass der Informationsabruf nicht im gleichen Maße wie gemäß § 112 vereinfacht ist, da Behörden ein schriftliches Ersuchen für die gewünschten Informationen stellen müssen. Ein weiterer Unterschied zwischen § 112 und § 113 TKG besteht darin, dass die nach der letztgenannten Regelung zur Beantragung des Zugangs berechtigten Behörden mit Bezug auf die von ihnen wahrgenommenen Aufgaben identifiziert, aber nicht ausdrücklich aufgeführt werden. Der Gerichtshof hält diese Beschreibung nach Aufgabenbereichen zwar für weniger konkret und offener für Interpretationen, dennoch ist der Wortlaut der Regelung detailliert genug, um klar abzuschätzen, welche Behörden befugt sind, Auskünfte anzufordern. In diesem Zusammenhang weist der Gerichtshof auch darauf hin, dass das Bundesverfassungsgericht zu dem Schluss gekommen ist, dass aufgrund der beschränkten Aufgaben der Nachrichtendienste deren weitreichende gesetzliche Befugnisse zu Auskunftersuchen im Vorfeld [von Gefahren] gerechtfertigt sind (siehe Rdnr. § 21 (Rdnr. 177 der BVerfG-Entscheidung)).

100. In Bezug auf beide Regelungen stellt der Gerichtshof fest, dass die gespeicherten Daten gegen übermäßige oder missbräuchliche Auskunftersuchen weiter dadurch geschützt sind, dass die ersuchende Behörde einer zusätzlichen Rechtsgrundlage für den Abruf der Daten bedarf. Wie das Bundesverfassungsgericht in seinem Doppeltürvergleich (siehe Rdnr. 14 (Rdnr. 123 der BVerfG-Entscheidung)) erläuterte, sehen die §§ 112 und 113 TKG die Freigabe der Daten lediglich durch die Bundesnetzagentur oder den jeweiligen Diensteanbieter vor. Allerdings ist für die Berechtigung zum Stellen von Auskunftersuchen durch die

benannten Behörden eine weitere gesetzliche Regelung erforderlich. Zudem ist der Abruf auf erforderliche Daten beschränkt; dieses Erforderlichkeitsgebot wird durch eine allgemeine Verpflichtung der jeweiligen abrufenden Behörden zur unverzüglichen Löschung nicht benötigter Daten sichergestellt. Das Bundesverfassungsgericht hatte darauf hingewiesen, dass das Erfordernis der „Erforderlichkeit“ im Rahmen der Strafverfolgung bedeute, dass zumindest ein Anfangsverdacht vorliegen müsse (siehe Rdnr. 21 (Rdnr. 177 der BVerfG-Entscheidung)). Der Gerichtshof erkennt an, dass die Befugnis zur Stellung eines Auskunftersuchens ausreichend beschränkt ist und dass das Erfordernis der „Erforderlichkeit“ nicht nur in den besonderen Rechtsvorschriften, die Gegenstand dieser Beschwerde sind, sondern auch im deutschen und europäischen Datenschutzrecht vorgesehen ist.

101. In Anbetracht dieser Aspekte kann der Gerichtshof der Schlussfolgerung des Bundesverfassungsgerichts folgen, wonach die in § 113 TKG vorgesehenen Schwellen verfassungsrechtlich noch hinnehmbar waren, auch unter Berücksichtigung der Tatsache, dass die Verpflichtung zur Stellung eines schriftlichen Auskunftersuchens geeignet war, die Behörde zu veranlassen, die Auskunft nur bei hinreichendem Bedarf einzuholen (siehe Rdnr. 21 (Rdnr. 178 der BVerfG-Entscheidung)). Weiterhin stellt der Gerichtshof in diesem Zusammenhang fest, dass in der Praxis offenbar nur in einer begrenzten Anzahl von Fällen tatsächlich manuelle Abfragen vorgenommen wurden, verglichen mit den automatisierten Abfragen gemäß § 112 TKG (siehe Rdnr. 13).

102. Abschließend wird der Gerichtshof die verfügbaren Möglichkeiten zur Überprüfung und Kontrolle von Auskunftersuchen gemäß den §§ 112 und 113 TKG prüfen. In *K. u. a. ./ Deutschland* (6. September 1978, Rdnr. 55, Serie A Bd. 28) entschied der Gerichtshof, dass die Überprüfung von Eingriffen in das Recht auf Achtung des Privatlebens nach Artikel 8 der Konvention – in diesem Fall Eingriffe in Form von geheimen Überwachungsmaßnahmen – in drei verschiedenen Phasen relevant werden kann: bei der ersten Anordnung des Eingriffs, während der Durchführung oder nach der Beendigung des Eingriffs. Erfolgt die Überprüfung ohne das Wissen der Betroffenen in einer der ersten beiden Phasen, ist es unerlässlich, dass die festgelegten Verfahren selbst geeignete und gleichwertige Garantien zum Schutz der Rechte des Einzelnen vorsehen. Allgemeiner gefasst stellte der Gerichtshof fest (ebda.):

„[...] die Werte einer demokratischen Gesellschaft müssen innerhalb der Kontrollverfahren so gewissenhaft wie möglich beachtet werden, damit die Grenzen des Notwendigen im Sinne von Artikel 8 Abs. 2 (Art. 8-2) nicht überschritten werden. Eines der Grundprinzipien einer demokratischen Gesellschaft ist die Rechtsstaatlichkeit, auf welche sich die Präambel der Konvention ausdrücklich bezieht [...]. Rechtsstaatlichkeit setzt unter anderem voraus, dass ein Eingriff der Exekutive in die Rechte des Einzelnen einer wirksamen Kontrolle unterliegen muss, die normalerweise, zumindest in letzter Instanz, durch die Gerichte sichergestellt

werden muss, da diese die beste Garantie für Unabhängigkeit, Unparteilichkeit und ein ordnungsgemäßes Verfahren bieten.“

103. In der Folge stützte er sich auf diese Grundsätze, insbesondere die Möglichkeit einer wirksamen Kontrolle und Überprüfung, in Bezug auf verschiedene Eingriffe in das Recht auf Achtung des Privatlebens gemäß Artikel 8 der Konvention (siehe zum Beispiel: Speicherung sensibler personenbezogener Daten in Sicherheitsdateien – *Rotaru ./. Rumänien* [GK], Individualbeschwerde Nr. 28341/95, Rdnr. 59, ECHR 2000-V; Beschlagnahme von Bankunterlagen – *M.N. u. a. ./. San Marino*, a. a. O., Rdnrn. 73, 78; Entscheidung bzgl. Aufhebung des Anwaltsgeheimnisses gegen die Offenlegung von Kontoauszügen in Strafverfahren – *Brito Ferrinho Bexiga Villa-Nova ./. Portugal*, Individualbeschwerde Nr. 69436/10, Rdnr. 55, 1. Dezember 2015; Abhören von Telefonen – *Lambert ./. Frankreich*, 24. August 1998, Rdnr. 31, Reports of Judgments and Decisions 1998-V; ein System der geheimen Überwachung von Mobiltelefonen – *Roman Zakharov*, a. a. O., Rdnr. 233; strategische Überwachung der Kommunikation – *W. u. S. ./. Deutschland* (Entsch.), Individualbeschwerde Nr. 54934/00, Rdnr. 117, 29. Juni 2006). Der Gerichtshof stellt jedoch fest, dass es in allen diesen Fällen um individualisierte sowie schwerwiegendere und intensivere Eingriffe in das Recht auf Achtung des Privatlebens ging, die nicht auf den Datenzugang im vorliegenden Fall übertragen werden können. Zusammenfassend ist er der Auffassung, dass der Umfang der Überprüfung und Kontrolle als ein wichtiges, aber nicht entscheidendes Element bei der Beurteilung der Verhältnismäßigkeit der Erhebung und Speicherung eines solch begrenzten Datensatzes zu betrachten ist.

104. Zum Sachverhalt des vorliegenden Falles stellt der Gerichtshof fest, dass § 113 Abs. 2 TKG grundsätzlich festlegt, dass die Verantwortung für die Rechtmäßigkeit des Auskunftersuchens bei der abrufenden Stelle liegt und die Telekommunikationsdiensteanbieter nicht befugt sind, die Zulässigkeit eines Ersuchens zu überprüfen, sofern die Anforderung der Auskunft schriftlich erfolgt und eine Rechtsgrundlage geltend gemacht wird. Gemäß § 112 TKG ist jedoch die Bundesnetzagentur dafür zuständig, die Zulässigkeit der Übertragung zu prüfen, wenn ein besonderer Grund vorliegt.

105. Darüber hinaus werden jeder Abruf und die betreffenden Angaben über den Abruf (Zeit, in diesem Prozess verwendete Daten, abgerufene Daten, Angaben zur eindeutigen Identifizierung der die Daten abrufenden Person, ersuchende Behörde, Aktenzeichen, Informationen zur eindeutigen Identifizierung der die Daten anfordernden Person) zum Zweck der datenschutzrechtlichen Kontrolle aufgezeichnet. Diese Kontrolle erfolgt durch die unabhängigen Datenschutzbehörden des Bundes und der Länder. Letztere sind nicht nur dafür zuständig, die Einhaltung der Datenschutzbestimmungen aller beteiligten Behörden zu überwachen,

sondern sie können auch von allen Personen angerufen werden, die der Ansicht sind, bei der Erhebung, Verarbeitung oder Nutzung ihrer personenbezogenen Daten durch öffentliche Stellen in ihren Rechten verletzt worden zu sein.

106. Abschließend stellt der Gerichtshof fest, dass nach der Feststellung des Bundesverfassungsgerichts Rechtsschutz gegen den Abruf von Informationen nach den allgemeinen Regelungen (Rdnr. 22 (Rdnr. 186)) – insbesondere im Zusammenhang mit Rechtsschutzverfahren gegenüber abschließenden Entscheidungen der Behörden – gesucht werden kann.

107. Der Gerichtshof ist der Auffassung, dass die Möglichkeit der Kontrolle durch die zuständigen Datenschutzbehörden eine Überprüfung durch eine unabhängige Stelle gewährleistet. Da zudem jeder, der sich in seinen Rechten verletzt sieht, einen Rechtsbehelf einlegen kann, sind die fehlende Benachrichtigung und die fehlende Vertraulichkeit des Abrufverfahrens im Hinblick auf die Konvention nicht problematisch.

108. Da zwischen den Mitgliedstaaten kein Konsens über die Erhebung und Speicherung von begrenzten Teilnehmerinformationen besteht (siehe Rdnr. 58), erkennt der Gerichtshof schließlich an, dass die Mitgliedstaaten bei der Wahl der Mittel zur Erreichung der legitimen Ziele des Schutzes der nationalen Sicherheit und der Kriminalitätsbekämpfung einen gewissen Beurteilungsspielraum haben, den Deutschland im vorliegenden Fall nicht überschritten hat.

109. In Anbetracht der vorstehenden Ausführungen gelangt der Gerichtshof zu der Schlussfolgerung, dass die Speicherung der personenbezogenen Daten der Beschwerdeführer durch ihre jeweiligen Diensteanbieter gemäß § 111 TKG (in der durch das BVerfG geprüften Fassung – siehe Rdnr. 64) verhältnismäßig und daher „in einer demokratischen Gesellschaft notwendig“ war.

110. Eine Verletzung von Artikel 8 der Konvention liegt somit nicht vor.

AUS DIESEN GRÜNDEN ENTSCHEIDET DER GERICHTSHOF WIE FOLGT:

1. Er *erklärt* die Individualbeschwerde einstimmig für zulässig;
2. er *erkennt* mit sechs zu einer Stimme, dass Artikel 8 der Konvention nicht verletzt worden ist.

Ausgefertigt in englischer Sprache und schriftlich zugestellt am 30. Januar 2020 nach Artikel 77 Abs. 2 und 3 der Verfahrensordnung des Gerichtshofs.

Claudia Westerdiek
Kanzlerin

Yonko Grozev
Präsident

Gemäß Artikel 45 Abs. 2 der Konvention und Artikel 74 Abs. 2 der Verfahrensordnung des Gerichtshofs ist diesem Urteil das Sondervotum des Richters Ranzoni beigefügt.

YG
CW

ABWEICHENDE MEINUNG DES RICHTERS RANZONI

I. Einführung

1. Ich habe in der vorliegenden Rechtssache für die Feststellung einer Verletzung von Artikel 8 der Konvention gestimmt, weil ich der Mehrheit nicht zustimmen kann, was ihre Bewertung eines Teils der relevanten Tatsachen und ihre Auslegung und Anwendung der allgemeinen Grundsätze des Gerichtshofs angeht.

2. Meiner Ansicht nach stellt sich in der vorliegenden Rechtssache die folgende Hauptfrage: Welche Erfordernisse - insbesondere was Schutzvorkehrungen angeht - ergeben sich aus Artikel 8 im Hinblick auf die Speicherung von personenbezogenen Daten, denen zwar nur begrenztes Gewicht beigemessen wird, die aber von einem breiten Spektrum von Behörden problemlos in großen Mengen abgefragt werden können?

3. Zunächst sollte bedacht und hervorgehoben werden, dass der vorliegende Fall nicht auf Maßnahmen im Zusammenhang mit der Bekämpfung des Terrorismus oder ähnlicher schwerer Straftaten oder auf Fragen der nationalen Sicherheit beschränkt ist. Die vom Gerichtshof zu prüfenden Rechtsvorschriften erlauben die Datenspeicherung auch für weniger schwerwiegende Zwecke und gestatten verschiedenen staatlichen Stellen Zugang zu solchen Daten. Dazu gehören nicht nur Gerichte und Strafverfolgungsbehörden, sondern auch andere Behörden wie etwa der Zollfahndungsdienst, Notdienste, Behörden der Zollverwaltung im Zusammenhang mit Schwarzarbeit, die Bundesanstalt für Finanzdienstleistungsaufsicht und mehrere Nachrichtendienste.

II. Eingriffsgewicht

4. Das erste Problem, das ich mit den Feststellungen der Mehrheit habe, betrifft das Gewicht des Eingriffs. Die Mehrheit ist zu dem Schluss gelangt, dass der Eingriff, also die Speicherung der personenbezogenen Daten der Beschwerdeführer „zwar nicht als geringfügig, aber dennoch als von eher begrenzter Natur“ zu werten sei (siehe Rdnr. 95). Meines Erachtens hat die Mehrheit bei der Beurteilung der Schwere dieses Eingriffs mehrere erhebliche Tatsachen übersehen.

5. Ich stimme mit der Mehrheit und dem Bundesverfassungsgericht überein, dass keine sensiblen Informationen gespeichert wurden. Allerdings hat die Mehrheit übersehen, dass diese Daten der Schlüssel zu (sensiblen) Telekommunikationsdaten sind und es ermöglichen, eine Person einer Rufnummer oder eine Rufnummer einer Person zuzuordnen. Sie erleichtern damit die Identifizierung der Teilnehmer jedes Telefonanrufs oder Nachrichtenaustauschs und die Zuordnung potentiell sensibler Informationen zu einer identifizierbaren Person. Diese Möglichkeit war der

Zweck der in Rede stehenden Regelung. Leider wurde dieser Aspekt von der Mehrheit jedoch nicht berücksichtigt. Dies ist umso bedauerlicher, als sich der Gerichtshof bereits mit dieser Möglichkeit der Identifizierung der an Kommunikationsvorgängen beteiligten Personen befasst hat. In der Rechtssache *Benedik ./. Slowenien* (Individualbeschwerde Nr. 62357/14, 24. April 2018) setzte sich der Gerichtshof mit den Möglichkeiten auseinander, einen Internetnutzer durch die Erlangung der mit einer dynamischen IP-Adresse verbundenen Teilnehmerinformationen zu identifizieren, und hob die Bedeutung des konkreten Kontexts hervor, in dem die Teilnehmerinformationen angefordert wurden. Er stellte Folgendes fest (ebda., Rdnr. 109):

„[...] Bei Sachlagen wie der vorliegenden müssen daher Informationen, bei denen es sich dem Anschein nach um periphere, von der Polizei angeforderte Informationen handelt – d. h. Name und Anschrift eines Teilnehmers – als untrennbar mit dem bereits vorhandenen Inhalt verbunden behandelt werden, der Aufschluss über Daten gibt [...] Eine anderslautende Feststellung würde bedeuten, Informationen den notwendigen Schutz zu versagen, die Aufschluss über einen Großteil der Internetaktivitäten einer Person geben könnten, einschließlich sensibler Details über ihre Interessen, Überzeugungen und ihr Intimleben.“

6. Dieser Aspekt wurde jedoch von der Mehrheit bei der Beurteilung des Eingriffsgewichts nicht berücksichtigt.

7. Unberücksichtigt ließ die Mehrheit auch, dass der vorliegende Fall, insbesondere im Hinblick auf den umfassenden Charakter der Datenspeicherung, mit den vom Gerichtshof der Europäischen Union (EuGH) entschiedenen Verfahren *Digital Rights Ireland* und *Seitlinger u. a.* sowie *Tele2 Sverige* und *Tom Watson u. a.* vergleichbar ist (siehe Rdnrn. 51-52). Die Beschwerdeführer argumentierten, dass die in Rede stehende Datenspeicherung mit der vergleichbar sei, über die der EuGH entschieden habe, denn sie sei insoweit umfangreich, als sie alle Nutzer von Mobilfunkdiensten betreffe, auch wenn es keine Hinweise darauf gebe, dass ihre Handlungen im Zusammenhang mit Straftaten oder anderen Verstößen stehen könnten. Die Mehrheit wies dieses Argument zurück. Meiner Ansicht nach ist der vorliegende Fall aber tatsächlich mit den vom EuGH entschiedenen Fällen vergleichbar. Ziel des § 111 TKG war es, ein umfassendes Register aller Mobilfunknutzer zu schaffen. Dies zeigt sich unter anderem daran, dass die Vorschrift geändert wurde und Nutzer Identitätsnachweise liefern mussten, nachdem sich herausgestellt hatte, dass falsche Informationen gespeichert worden waren. Der Zweck der Vorschrift war tatsächlich eine umfassende Speicherung von Teilnehmerdaten und diese Gesetzgebung wird im vorliegenden Fall abstrakt geprüft.

8. Hätte die Mehrheit akzeptiert, dass § 111 TKG auf die Schaffung eines umfassenden Registers aller Mobilfunknutzer gerichtet war, hätte sie auch die gesellschaftlichen Folgen eines solchen Registers in Erwägung ziehen können. Der Gerichtshof hat bereits anerkannt, dass die Anonymität lange Zeit ein Mittel zur Vermeidung von Repressalien oder ungewollter

Aufmerksamkeit war und daher den ungehinderten Austausch von Ideen und Informationen in entscheidender Weise fördern konnte (siehe *Delfi AS v. Estland* [GK], Individualbeschwerde Nr. 64569/09, Rdnr. 147, 16. Juni 2015). Dies steht beispielsweise im Einklang mit der Meinung des Sonderberichterstatters der Vereinten Nationen über die Förderung und den Schutz des Rechts auf Meinungsfreiheit und freie Meinungsäußerung (siehe Rdnr. 56). Auf diesen Aspekt des Eingriffs wurde von der Mehrheit jedoch nicht eingegangen.

9. Kurz gesagt, meines Erachtens hat die Mehrheit das Eingriffsgewicht nicht angemessen gewürdigt und ist dadurch, dass bestimmte erhebliche Aspekte vernachlässigt wurden, zu dem Ergebnis gelangt, dass der Eingriff von begrenzter Natur sei. Dies hatte jedoch gravierende Folgen für die Prüfung der Rechtssache, weil die Mehrheit in den nachfolgenden Teilen die begrenzte Natur des Eingriffs überbetont und in der Folge auch das Niveau der erforderlichen Schutzvorkehrungen ungebührlich herabgesetzt hat.

III. Verhältnismäßigkeit

10. Ferner bin ich mit bestimmten Aspekten der Verhältnismäßigkeitsprüfung durch die Mehrheit nicht einverstanden.

11. Der Schwerpunkt dieser Prüfung liegt auf der Herbeiführung eines gerechten Ausgleichs zwischen den kollidierenden öffentlichen und privaten Interessen, indem zum einen die Speicherung der konkreten personenbezogenen Daten und zum anderen die einschlägigen Schutzvorkehrungen geprüft werden, um die Maßnahme auf das unbedingt erforderliche Maß zu beschränken, eine den Garantien des Artikels 8 zuwiderlaufende Nutzung der personenbezogenen Daten zu verhindern und somit die personenbezogenen Daten vor unsachgemäßem Gebrauch und Missbrauch zu schützen. Das Ergebnis dieser Abwägung hängt unter anderem davon ab, welches Gewicht den in Rede stehenden personenbezogenen Daten beigemessen wird. Je geringer das Gewicht, das dieser Art von Daten beigemessen wird, desto weniger Schutzvorkehrungen sind notwendig.

12. Diese Logik steckt auch hinter dem EuGH-Verfahren *Ministerio Fiscal* (siehe Rdnrn. 54-55): je weniger schwerwiegend der Eingriff ist, desto einfacher lässt er sich in den Bereichen der Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten rechtfertigen. Die Mehrheit hat auf dieses Vorabentscheidungsverfahren und dessen Ergebnis, „dass der Zugang zu den betreffenden Daten keinen schweren Eingriff [...] darstellt“ (Rdnr. 94) hingewiesen.

13. Vergleicht man jedoch jenen Fall mit dem vorliegenden, müssen einigen entscheidende Unterschiede herausgestellt werden. Der EuGH akzeptierte den Eingriff als „unter den Umständen“ dieses Falls

gerechtfertigt. Der Fall betraf die SIM-Karten eines gestohlenen Mobiltelefons, das während eines Zeitraums von 12 Tagen mit der Identität der Inhaber dieser SIM-Karten in Verbindung gebracht wurde. Der Antrag bezog sich nur auf den Zugang zu den diesen SIM-Karten entsprechenden Telefonnummern sowie zu den Daten bezüglich der Identität der Inhaber dieser Karten. Der Luxemburger Gerichtshof hat nur angesichts dieser Umstände befunden, dass der Zugang zu diesen konkreten Daten keinen schwerwiegenden Eingriff darstelle.

14. Der vorliegende Fall stellt sich jedoch ganz anders dar. Erstens betrifft er nicht unmittelbar den Zugang zu Daten, sondern die Speicherung von Daten. Zweitens bezieht er sich nicht auf ein konkretes strafrechtliches Ermittlungsverfahren, bei dem konkrete Ermittlungsmaßnahmen zu prüfen sind. Drittens geht es – im Unterschied zu *Ministerio Fiscal* – weder um sehr spezifische Daten (SIM-Karten eines Telefons), noch um eine begrenzte Dauer (12 Tage), sondern um die Datensätze von Millionen von Menschen, die über einen viel längeren Zeitraum gespeichert werden. Viertens ist der Datenzugang im vorliegenden Fall nicht auf den Zweck der Bekämpfung von Straftaten – ob schwerwiegend oder nicht – beschränkt. Vielmehr gestattet das Telekommunikationsgesetz den Datenzugang auch bei Ordnungswidrigkeiten und für andere allgemeine Zwecke, die vom Zollfahndungsdienst, von Notdiensten, von Behörden der Zollverwaltung im Zusammenhang mit Schwarzarbeit, von der Bundesanstalt für Finanzdienstleistungsaufsicht und von mehreren Nachrichtendiensten verfolgt werden, wobei letztere unabhängig von konkreten Gefahren tätig werden (siehe Rdnrn. 176-177 der BVerfG-Entscheidung). Demgegenüber beschränken die meisten Mitgliedstaaten, die in dem rechtsvergleichenden Bericht berücksichtigt wurden, die vertretbaren Zwecke auf die Ermittlung von Straftaten oder die Abwehr von Gefahren für die öffentliche Ordnung (siehe Rdnr. 58).

15. Die Kammermehrheit war im vorliegenden Fall der Auffassung, „dass die gespeicherten Daten gegen übermäßige oder missbräuchliche Auskunftersuchen weiter dadurch geschützt sind, dass die ersuchende Behörde einer zusätzlichen Rechtsgrundlage für den Abruf der Daten bedarf“ (siehe Rdnr. 100). Das Bundesverfassungsgericht hat zwar bestätigt, dass eine zusätzliche Rechtsgrundlage für den Datenabruf durch die entsprechenden Behörden erforderlich sei, es räumte aber auch ein, dass allgemeine Befugnisse zu Erhebung von Daten ausreichend seien (siehe Rdnr. 163 der BVerfG-Entscheidung). Betrachtet man die in Rede stehenden Rechtsvorschriften, die in dem Urteil aufgeführt sind (siehe Rdnrn. 32-38), zeigt sich, dass die meisten Behörden eine allgemeine Befugnis haben, zur Erfüllung ihrer gesetzlichen Aufgaben und Pflichten Daten zu erheben. Folglich gibt es keine eindeutige Schwelle, die die Datenerhebung auf die Ermittlung schwerwiegender Straftaten oder auf spezifische ernsthafte Bedrohungen der nationalen Sicherheit beschränkt.

Insoweit sei auch darauf hingewiesen, dass der Gerichtshof die „Generalklausel“ für Ermittlungsmaßnahmen nach § 161 StPO als eine der zusätzlichen Rechtsgrundlagen erachtet hat, die der Mehrheit zufolge Mobilfunkteilnehmer gegen übermäßige oder missbräuchliche Auskunftersuchen schützt. In der Rechtssache *S. ./.* *Deutschland* (Individualbeschwerde Nr. 73607/13, Rdnr. 58, 27. April 2017) kam der Gerichtshof zu dem Ergebnis, dass die Eingriffsschwelle verhältnismäßig niedrig war und die Regelung keine besonderen Schutzvorkehrungen vorsah.

16. Die Zahl der betroffenen Personen, die bereits aufgrund der Breite der rechtlichen Regelungen hoch ist, wird durch die technische Ausgestaltung der Datei und die Abfragemöglichkeiten noch weiter erhöht. Auskunftersuchen müssen nicht auf konkrete Rufnummern oder Namen beschränkt sein. § 112 Abs. 1 TKG gestattet den Behörden Abfragen auf Grundlage unvollständiger Daten mittels einer Ähnlichenfunktion. Deshalb können die abgerufenen Daten eine große Anzahl an Personen betreffen, bei denen es keinerlei Anhaltspunkte dafür gibt, dass ihr Verhalten in einem auch nur mittelbaren oder entfernten Zusammenhang mit Straftaten oder Ordnungswidrigkeiten stehen könnte, außer dass sie einen ähnlichen Namen oder eine ähnliche Rufnummer haben. Dennoch können diese Personen auf Grundlage des Datenabrufs gemäß § 112 TKG weiteren Ermittlungsmaßnahmen unterzogen werden.

17. Wenn bei einem Auskunftersuchen die Datei durchsucht wird, wird der Name/die Nummer mit jedem Mobilfunkteilnehmer in der Datei abgeglichen. Folglich werden also die personenbezogenen Daten jedes Nutzers verarbeitet, wenn auch in begrenzter Art und Weise. Je nach Genauigkeit der Suchkriterien liefert die Suche eine Liste aller Teilnehmer, auf die die Kriterien zutreffen. Berücksichtigt man die Ähnlichenfunktion und die Suche auf Grundlage unvollständiger Daten, kann diese Ergebnisliste immer noch Daten umfassen, die sich auf eine sehr große Personenzahl beziehen. Um diese Liste weiter einzugrenzen – und letztlich die relevante Nummer oder Person zu identifizieren – müssen die Behörden dann zusätzliche Ermittlungsmaßnahmen ergreifen. Das bedeutet, dass diese Personen weiteren Eingriffen auf Grundlage von Datenabfragen gemäß § 112 TKG unterzogen werden können, obwohl sie keinen Anlass für sie betreffende Ermittlungen gegeben haben, außer einen ähnlichen Namen oder eine ähnliche Rufnummer zu haben. Es ist wichtig darauf hinzuweisen, dass 2015 etwa 35 Millionen Datensätze nach dem automatisierten Verfahren abgefragt wurden (siehe Rdnr. 67), wobei jeder Datensatz einer Person entspricht.

18. Einer der wesentlichen Punkte, in denen ich nicht mit der Mehrheit übereinstimme, ist jedoch die Würdigung der Schutzvorkehrungen und der Frage, ob diese, sofern vorhanden, ausreichen, um den unsachgemäßen Gebrauch und Missbrauch personenbezogener Daten wirksam zu verhindern

(*S. und Marper ./. Vereinigtes Königreich* [GK], Individualbeschwerden Nrn. 30562/04 und 30566/04, Rdnr. 103, ECHR 2008; auf dieses Verfahren wird von der Mehrheit in Rdnr. 78 verwiesen). Und hierin liegt meines Erachtens die Krux des Falles.

19. Das Ergebnis der Würdigung hängt unter anderem davon ab, was „wirksame“ Schutzvorkehrungen bedeuten. Ergibt sich aus den innerstaatlichen oder internationalen Rechtsvorschriften für sich genommen eine ausreichende Schutzvorkehrung? Die Antwort müsste „nein“ lauten, denn die Rechtsvorschriften stellen lediglich die Rechtsgrundlage dar, anhand derer sich die Rechtmäßigkeit des Eingriffs bestimmt, sie stellen jedoch nicht zusätzlich und für sich genommen eine wirksame Schutzvorkehrung dar. Nach meinem Verständnis des Erfordernisses wirksamer Schutzvorkehrungen sollen sie den Einzelnen vor der willkürlichen Anwendung des innerstaatlichen Rechts durch innerstaatliche Behörden und vor dem Missbrauch rechtlicher Befugnisse schützen. Dieser Schutz muss über die rechtlichen Regelungen hinausgehen, insbesondere wenn diese Regelungen und rechtlichen Befugnisse breit gefasst sind, wie das Bundesverfassungsgericht im vorliegenden Fall eingeräumt hat, und wenn die Regelungen und Befugnisse den Abruf von Daten auf eine sehr vereinfachte und automatisierte Weise gestatten. Insoweit möchte ich nochmals auf die insgesamt 35 Millionen Datensätze verweisen, die 2015 nach dem automatisierten Verfahren abgefragt wurden.

20. Um das Argument zu stützen, dass ausreichende Schutzvorkehrungen vorhanden gewesen seien, berief sich die Mehrheit auf den Doppeltür-Vergleich des Bundesverfassungsgerichts (siehe Rdnrn. 17, 85 und 100). Wie sich jedoch bereits gezeigt hat, sind die Rechtsvorschriften zum Datenabruf sehr allgemein und weit gefasst. Auch wenn sie als „rechtlicher Schlüssel“ für die Doppeltür ausreichen mögen, so gibt es im Anschluss keinen Mechanismus, um die hindurchgehenden Informationen zu kontrollieren. Die Doppeltür kann mit diesem Schlüssel problemlos geöffnet werden, aber auf der anderen Seite der Tür wartet niemand, der prüft, welche Informationen durch die Tür hindurchgehen und dann verwendet werden.

21. Ferner argumentiert die Mehrheit, dass der Abruf nicht nur durch Rechtsvorschriften geschützt werde, sondern auch auf erforderliche Daten beschränkt sei, und dieses Erfordernis wiederum durch eine allgemeine Verpflichtung zur unverzüglichen Löschung nicht benötigter Daten sichergestellt werde (siehe Rdnr. 100). Was bedeutet das und worin bestehen die Schutzvorkehrungen tatsächlich? Meiner Ansicht nach bestehen sie – vereinfacht gesagt – aus allgemeinen Vorschriften zum Abruf von Daten, die nach Auffassung der Mehrheit durch ein allgemeines Erfordernis der Erforderlichkeit „geschützt“ werden, welches wiederum durch eine weitere allgemeine Verpflichtung „sichergestellt“ wird. Einen echten Schutz vor einem etwaigen unsachgemäßen Gebrauch und

Missbrauch vermag ich nicht zu erkennen. Folglich bietet das Konzept der Doppeltür unter den im vorliegenden Fall gegebenen Umständen keine wirksame Schutzvorkehrung.

22. Der Abruf personenbezogener Daten erfordert keine Anordnung durch eine gerichtliche oder eine sonstige unabhängige Stelle. Während die Bundesnetzagentur – zumindest bei Ersuchen gemäß § 112 TKG – die Zulässigkeit der Übertragung prüfen soll, wenn dafür ein besonderer Anlass besteht, hat das Bundesverfassungsgericht selbst zu Recht darauf hingewiesen, dass eine solche Eventualität kaum je gegeben sein wird, da die abfragende Behörde ihr Ersuchen nicht zu begründen hat (siehe Rdnr. 18). Deshalb kann diese Agentur nicht als wirksame Schutzvorkehrung fungieren. Für Auskunftersuchen gemäß 113 TKG stellt Absatz 2 klar, dass die Verantwortung für die Rechtmäßigkeit des Auskunftersuchens bei der abrufenden Stelle liegt und dass die Telekommunikationsdiensteanbieter nicht befugt sind, die Zulässigkeit eines Ersuchens zu überprüfen, sofern die Anforderung der Auskunft schriftlich erfolgt und eine Rechtsgrundlage geltend gemacht wird. Zusammengefasst heißt das, dass die abrufende Stelle dafür zuständig ist, ein Auskunftersuchen zu stellen und gleichzeitig auch die Zulässigkeit ihres Ersuchens zu prüfen. Anders ausgedrückt: die abrufende Stelle ist ihre eigene Schutzvorkehrung. Es fehlt jedoch an einer wirksamen Überprüfung und Kontrolle von Auskunftersuchen, ob gemäß § 112 oder § 113 TKG gestellt, durch eine gerichtliche oder eine sonstige unabhängige Stelle.

23. Der Gerichtshof hat bereits anerkannt, dass im Zusammenhang mit Sicherheitsoperationen eine nachträgliche Überprüfung von Eingriffen ausreichend sein kann. Auskunftersuchen nach dem automatisierten Verfahren erfolgen jedoch ohne Kenntnis des Telekommunikationsdiensteanbieters oder des betreffenden Teilnehmers, und es gibt keine Verpflichtung, einen Mobilfunkteilnehmer davon zu benachrichtigen, dass seine persönlichen Daten abgefragt wurden. Ähnlich sieht es bei manuellen Auskunftersuchen gemäß § 113 TKG aus, denn Absatz 4 verlangt von den Telekommunikationsdiensteanbietern, über das Auskunftersuchen und die Auskunftserteilung Stillschweigen zu wahren (siehe Rdnr. 31). Somit hat das Opfer des Eingriffs keine Kenntnis und kann keine Überprüfung der Informationsabfrage anstreben.

24. Die Mehrheit hat diese Folge akzeptiert, indem sie sich unter anderem auf das Argument des Bundesverfassungsgerichts berufen hat, dass Rechtsschutz im Zusammenhang mit Rechtsschutzverfahren gegenüber abschließenden Entscheidungen der Behörden gesucht werden könne (siehe Rdnr. 105). Dies gilt jedoch nur für Auskunftersuchen, die zu weiteren Telekommunikationsüberwachungs- oder sonstigen Ermittlungsmaßnahmen geführt haben. Selbst in diesem Fall kann nur die weitere Ermittlungsmaßnahme beanstandet werden, nicht aber die Abfrage und Speicherung der Daten selbst. Zudem steht dieser Art der Überprüfung nur

einer sehr begrenzten Zahl von Opferkategorien offen. Der großen Mehrheit bleibt keinerlei Überprüfungsmöglichkeit.

25. Insoweit verweist das Kammerurteil schließlich auf die Kontrolle durch die Datenschutzbehörden (siehe Rdnr. 107). Ungeachtet der wichtigen Arbeit, die diese Behörden leisten, erscheint es unrealistisch, dass sie in der Lage sind, an die 35 Millionen Datensätze zu überprüfen, die von einem breiten Spektrum unterschiedlicher Behörden angefordert werden. In Anbetracht der personellen Ausstattung dieser Datenschutzbehörden und ihres breiten Aufgabenspektrums stellt dies weder eine angemessene Form der Überprüfung noch eine wirksame Schutzvorkehrung dar.

IV. Schlussfolgerung

26. Meine Bewertung des innerstaatlichen Rechts und der innerstaatlichen Praxis in der vorliegenden Rechtssache führt mich zu dem Schluss, dass die vorhandenen Schutzvorkehrungen in keiner Weise ausreichen, um den unsachgemäßen Gebrauch und Missbrauch riesiger Mengen personenbezogener Daten zu verhindern, und ich sehe dies als wesentlicher gewichtiger an als meine Kolleginnen und Kollegen in der Kammer es getan haben. Ich bin daher der Auffassung, dass der Eingriff in die Rechte der Beschwerdeführer nach Artikel 8 in Bezug auf die verfolgten legitimen Ziele nicht verhältnismäßig war, insbesondere, weil das innerstaatliche Recht nicht auf Maßnahmen zur Bekämpfung des Terrorismus oder anderer schwerwiegender Straftaten oder auf Angelegenheiten der nationalen Sicherheit beschränkt war, sondern noch weit darüber hinaus ging. Der Eingriff entsprach keinem „dringenden gesellschaftlichen Bedürfnis“ und war folglich in einer demokratischen Gesellschaft nicht notwendig.

27. Dies hat mich dazu veranlasst, für die Feststellung eines Verstoßes gegen Artikel 8 der Konvention zu stimmen.