Bundesministerium
der Justiz und
für Verbraucherschutz

POSTANSCHRIFT Bundesministerium der Justiz und für Verbraucherschutz, 11015 Berlin

Frau
Anna Biselli
[redacted]

HAUSANSCHRIFT Mohrenstraße 37, 10117 Berlin
POSTANSCHRIFT 11015 Berlin

BEARBEITET VON Referat Z A 4
TEL (+49 30) 18 580 - 0
FAX (+49 30) 18 580 - 95 25
E-MAIL poststelle@bmjv.bund.de

AKTENZEICHEN [redacted]

DATUM Berlin, 11. November 2015

BETREFF: **Auskunft nach dem Informationsfreiheitsgesetz (IFG)**
HIER: Erwiderung der Bundesregierung auf die Stellungnahme der EU-Kommission zum Gesetzentwurf zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten
BEZUG: Ihr Antrag vom 12. Oktober 2015 über www.fragdenstaat.de
ANLAGE: - 8 -

Sehr geehrte Frau Biselli,

mit E-Mail vom 12. Oktober 2015 über www.fragdenstaat.de bitten Sie unter Berufung auf das IFG um Übersendung der „Erwiderung auf die Stellungnahme der EU-Kommission [https://netzpolitik.org/2015/wir-veroeffentlichen-stellungnahme-der-eu-kommission-zu-vorratsdatenspeicherung-noch-viele-weitere-maengel/] zum Gesetzesentwurf zur Vorratsdatenspeicherung".

Ich gebe Ihrem Antrag statt.

Beigefügt erhalten Sie die gewünschten Unterlagen.

Mit freundlichen Grüßen
Im Auftrag
(Lehmann)

LIEFERANSCHRIFT Kronenstraße 41, 10117 Berlin
VERKEHRSANBINDUNG U-Bahnhof Hausvogteiplatz (U2)

Europäische Kommission
Unternehmen und Industrie

v. 1.0

Richtlinie 98/34/EG

Land
D - Deutschland

Mitteilung
201

Sprache
DE - Deutsch

3A. Zuständiger Dienst

Bundesministerium für Wirtschaft und Energie, Referat E B 2, 11019 Berlin,
Tel.: 0049-30-2014-6353, Fax: 0049-30-2014-5379, E-Mail: infonorm@bmwi.bund.de

3B. Urheberdienst

Bundesministerium der Justiz und für Verbraucherschutz, Referat R B 3, Mohrenstrasse 37,
10117 Berlin, Tel.: 0049-30-18580-9623, Fax: 0049-30-18580-9518, E-Mail: rb3@bmjv.bund.de

6. Wesentlicher Inhalt

I. Ausführliche Stellungnahme

Die Bundesregierung teilt die Einschätzung der Kommission, dass die Pflicht zur Speicherung der Verkehrsdaten im Inland (§ 113b Absatz 1 StPO-E) eine Beschränkung der Dienstleistungsfreiheit darstellt. Sie ist jedoch der Auffassung, dass diese Beschränkung gerechtfertigt ist.

Die Kommission hat in ihrer Stellungnahme ausgeführt, dass die im Gesetzentwurf dargelegten Bedenken im Hinblick auf die Gewährleistung der Datensicherheit bei Speicherung im europäischen Ausland angesichts des durch die Richtlinien 95/46/EG und 2002/58/EG harmonisierten Datenschutzregimes ihrer Auffassung nach nicht durchgreifen.

Für die Bundesregierung spricht jedoch ein anderes Argument entscheidend gegen die Speicherung im EU-Ausland, das in der Begründung zu dem Gesetzentwurf ebenfalls angeführt ist: die Gefahr der Umgehung der im Gesetzentwurf vorgesehenen engen Verwendungsregeln bei Speicherung im EU-Ausland (vgl. dazu unten Ziffer 1). Es handelt sich dabei also nicht um die Sorge einer möglichen missbräuchlichen Verwendung der Daten im Ausland, sondern um die Sorge, dass die Daten im Ausland rechtmäßig von den dortigen Geheimdiensten und Strafverfolgungsbehörden zu Zwecken verwendet werden könnten, die nach deutschem Recht ausgeschlossen sind (vgl. dazu unten Ziffer 2). Gegen diese mögliche zweckändernde Verwendung gibt es auf europäischer Ebene keine Schutzmechanismen, da die entsprechenden Richtlinien Ausnahmen zulassen, wenn bestimmte Voraussetzungen vorliegen (vgl. dazu unten Ziffer 3). Dies trifft auch zu, wenn man berücksichtigt, dass es sich bei den Vorratsdaten nur um eine Teilmenge der Daten handelt, die die Unternehmen aus geschäftlichen Gründen speichern (vgl. dazu unten Ziffer 4).

1. Vorgaben des deutschen Grundgesetzes und der Charta der Grundrechte der Europäischen Union zur Verwendung verpflichtend zu speichernder Verkehrsdaten

Der Gesetzentwurf enthält sehr strenge Beschränkungen in Bezug auf die Verwendung der verpflichtend gespeicherten Daten. Die Daten dürfen nur für zwei Zwecke verwendet werden: für die Verfolgung besonders schwerer Straftaten einerseits und für die Prävention besonders schwerer Gefahren durch die Polizeien der Länder andererseits. Eine Übermittlung an deutsche Nachrichtendienste oder auch an das Bundeskriminalamt ist unzulässig. Die Strafprozessordnung zählt die Straftaten auf, für deren Ermittlung auf die verpflichtend zu speichernden Verkehrsdaten zugegriffen werden darf. Zusätzlich sieht sie weitere Voraussetzungen für den Zugriff vor. So muss die Verkehrsdatenerhebung zum Beispiel in einem angemessenen Verhältnis zur Bedeutung der Sache stehen. Diese engen Verwendungsregeln wurden aus zwei Gründen in den Gesetzentwurf aufgenommen:

Erstens hat das Bundesverfassungsgericht in seinem Urteil, in dem es das deutsche Gesetz zur Umsetzung der Richtlinie 2006/24/EG für nichtig erklärt hat (Urteil vom 2. März 2010, Rn. 226 ff.), sehr klar herausgestellt, dass die Verfassungsmäßigkeit einer Vorratsdatenspeicherung eine enge Definition der Straftaten voraussetzt, für deren Ermittlung auf die verpflichtend zu speichernden Daten zurückgegriffen werden kann. Diese Straftaten müssen vom Gesetzgeber in Form eines Kataloges festgelegt werden:

„Eine Speicherung von Telekommunikationsverkehrsdaten [...] setzt weiterhin gesetzliche Regelungen zur Verwendung dieser Daten voraus. Die verhältnismäßige Ausgestaltung dieser Verwendungsregeln entscheidet damit nicht nur über die Verfassungsmäßigkeit dieser einen eigenen Eingriff begründenden Bestimmungen selbst, sondern wirkt auf die Verfassungsmäßigkeit schon der Speicherung als solcher zurück. [...]"

6. Wesentlicher Inhalt

"Die Verwendung der durch eine anlasslos systematische Speicherung praktisch aller Telekommunikationsverkehrsdaten gewonnenen Datenbestände unterliegt dementsprechend besonders hohen Anforderungen. Insbesondere ist diese nicht in gleichem Umfang verfassungsrechtlich zulässig wie die Verwendung von Telekommunikationsverkehrsdaten, die die Diensteanbieter in Abhängigkeit von den jeweiligen betrieblichen und vertraglichen Umständen - von den Kunden teilweise beeinflussbar - nach § 96 TKG speichern dürfen. Angesichts der Unausweichlichkeit, Vollständigkeit und damit gesteigerten Aussagekraft der über sechs Monate systematisch vorsorglich erhobenen Verkehrsdaten hat ihr Abruf ein ungleich größeres Gewicht. Da eine Auswertung dieser Daten tief in das Privatleben eindringende Rückschlüsse und unter Umständen detaillierte Persönlichkeits- und Bewegungsprofile ermöglicht, kann insoweit nicht ohne weiteres davon ausgegangen werden, dass der Rückgriff auf diese Daten grundsätzlich geringer wiegt als eine inhaltsbezogene Telekommunikationsüberwachung. Vielmehr kann auch die Verwendung solcher Daten nur dann als verhältnismäßig angesehen werden, wenn sie besonders hochrangigen Gemeinwohlbelangen dient. Eine Verwendung der Daten kommt deshalb nur für überragend wichtige Aufgaben des Rechtsgüterschutzes in Betracht, das heißt zur Ahndung von Straftaten, die überragend wichtige Rechtsgüter bedrohen oder zur Abwehr von Gefahren für solche Rechtsgüter."

"Für die Strafverfolgung folgt hieraus, dass ein Abruf der Daten zumindest den durch bestimmte Tatsachen begründeten Verdacht einer schweren Straftat voraussetzt. Welche Straftatbestände hiervon umfasst sein sollen, hat der Gesetzgeber abschließend mit der Verpflichtung zur Datenspeicherung festzulegen. Ihm kommt hierbei ein Beurteilungsspielraum zu. Er kann dabei entweder auf bestehende Kataloge zurückgreifen oder einen eigenen Katalog schaffen, etwa um Straftaten, für die die Telekommunikationsverkehrsdaten besondere Bedeutung haben, zu erfassen. Die Qualifizierung einer Straftat als schwer muss aber in der Strafnorm - insbesondere etwa durch deren Strafrahmen - einen objektivierten Ausdruck finden. Eine Generalklausel oder lediglich die Verweisung auf Straftaten von erheblicher Bedeutung reichen hingegen nicht aus."

"Über die abstrakte Festlegung eines entsprechenden Straftatenkatalogs hinaus hat der Gesetzgeber sicherzustellen, dass ein Rückgriff auf die vorsorglich gespeicherten Telekommunikationsverkehrsdaten nur dann zulässig ist, wenn auch im Einzelfall die verfolgte Straftat schwer wiegt und die Verwendung der Daten verhältnismäßig ist."

Zweitens hat auch der Gerichtshof der Europäischen Union klargestellt, dass objektive Kriterien die Verwendung der verpflichtend zu speichernden Daten beschränken müssen und dass Straftaten, für deren Ermittlung auf diese Daten zugegriffen werden darf, hinreichend schwer sein müssen (Urteil vom 8. April 2014, Rechtssache C-293/12 und 594/12, Rn. 60f.):

„Zweitens kommt zu diesem generellen Fehlen von Einschränkungen hinzu, dass die Richtlinie 2006/24 kein objektives Kriterium vorsieht, das es ermöglicht, den Zugang der zuständigen nationalen Behörden zu den Daten und deren spätere Nutzung zwecks Verhütung, Feststellung oder strafrechtlicher Verfolgung auf Straftaten zu beschränken, die im Hinblick auf das Ausmaß und die Schwere des Eingriffs in die in Art. 7 und Art. 8 der Charta verankerten Grundrechte als hinreichend schwer angesehen werden können, um einen solchen Eingriff zu rechtfertigen. Die Richtlinie 2006/24 nimmt im Gegenteil in ihrem Art. 1 Abs. 1 lediglich allgemein auf die von jedem Mitgliedstaat in seinem nationalen Recht bestimmten schweren Straftaten Bezug."

"Überdies enthält die Richtlinie 2006/24 keine materiell- und verfahrensrechtlichen Voraussetzungen für den Zugang der zuständigen nationalen Behörden zu den Daten und deren spätere Nutzung. Art. 4 der Richtlinie, der den Zugang dieser Behörden zu den auf Vorrat gespeicherten Daten regelt, bestimmt nicht ausdrücklich, dass der Zugang zu diesen Daten und

6. Wesentlicher Inhalt

gespeicherten Daten regelt, bestimmt nicht ausdrücklich, dass der Zugang zu diesen Daten und deren spätere Nutzung strikt auf Zwecke der Verhütung und Feststellung genau abgegrenzter schwerer Straftaten oder der sie betreffenden Strafverfolgung zu beschränken sind, sondern sieht lediglich vor, dass jeder Mitgliedstaat das Verfahren und die Bedingungen festlegt, die für den Zugang zu den auf Vorrat gespeicherten Daten gemäß den Anforderungen der Notwendigkeit und der Verhältnismäßigkeit einzuhalten sind."

2. Gefahr der Umgehung der engen Verwendungsregelungen des Gesetzentwurfs bei Speicherung im EU-Ausland

Dürften die verpflichteten Telekommunikationsunternehmen die Daten in einem anderen EU-Mitgliedstaat speichern, hat dieser Staat die Möglichkeit des physischen Zugriffs auf die Daten bzw. auf ihren Speicherort. Die Speicherung der Daten auf seinem Hoheitsgebiet bildet einen Anknüpfungspunkt für eine an das betreffende Telekommunikationsunternehmen gerichtete Anordnung, gespeicherte Daten herauszugeben. Auch die Durchführung einer Durchsuchung und Beschlagnahme der Daten ist möglich. Gegen einen solchen Zugriff auf die Daten durch einen anderen Mitgliedstaat hilft eine Verschlüsselung der Daten nicht; es handelte sich in diesen Fällen nicht um ein Problem des Schutzes gegen eine mögliche missbräuchliche Nutzung, sondern um die rechtmäßige Nutzung der Daten zu Zwecken der Sicherheit des Staates, in dem sich der Speicherort befindet.

Es ist zum Beispiel nicht auszuschließen, dass eine Gefahrenabwehrbehörde eines anderen Mitgliedstaates in Übereinstimmung mit dem Recht des Mitgliedstaates systematisch alle verpflichtend gespeicherten Daten, die auf seinem Staatsgebiet vorgehalten werden, ausleitet, z.B. zum Zweck der Bekämpfung des internationalen Terrorismus. Denkbar ist auch, dass der Mitgliedstaat mit einem ausländischen Geheimdienst kooperiert und alle vorhandenen Verkehrsdaten an diesen weiterleitet. Die Erkenntnisse über die geheimen Datensammlungen der NSA zeigen, dass dies keine rein theoretischen Gefahren sind.

Denkbar ist auch, dass die Strafverfolgungsbehörde des anderen Mitgliedstaats zur Verfolgung von Straftaten auf die Daten zugreift, die nicht in dem Straftatenkatalog des deutschen Gesetzentwurfs enthalten sind.

Diese Beispiele machen deutlich, dass bei der Verwendung der Daten durch einen anderen Mitgliedstaat zu differenzieren ist zwischen einer Verwendung, die zwar rechtlich möglich, aber nach der Rechtsprechung des Gerichthofs der Europäischen Union mit den europäischen Grundrechten unvereinbar sein dürfte (z.B. systematische Ausleitung durch Geheimdienst ohne weitere Beschränkung, Abruf zur Verfolgung von Bagatellkriminalität) und einer Verwendung, die zwar mit der Grundrechtecharta, nicht aber mit den strengen Verwendungsregelungen des deutschen Gesetzes vereinbar ist (z.B. Zugriff auf die Daten zur Verfolgung von schweren Straftaten, die nicht im Katalog des § 100g Absatz 2 StPO-E enthalten sind).

3. Kein hinreichender Schutz gegen die Umgehung der Verwendungsregelungen durch das Recht der Europäischen Union

Nach Auffassung der Bundesregierung bietet das Recht der Europäischen Union keinen hinreichenden Schutz gegen beide Arten der zweckändernden Verwendung.

Zwar sieht Artikel 6 Absatz 1b) der Datenschutz- Richtlinie 95/46 vor, dass Daten für festgelegte eindeutige und rechtmäßige Zwecke erhoben und nicht in einer mit diesen Zweckbestimmungen nicht zu vereinbarenden Weise weiterverarbeitet werden dürfen. Aber Artikel 13 derselben

6. Wesentlicher Inhalt

Richtlinie (bzw. Artikel 15 der Datenschutzrichtlinie für elektronische Kommunikation 2002/58) ermöglicht es den Mitgliedstaaten, von den Verpflichtungen aus Artikel 6 abzuweichen, wenn dies für die Sicherheit des Staates, für die öffentliche Sicherheit, für die Verfolgung von Straftaten oder sogar für Steuerangelegenheiten notwendig ist. Artikel 13 bzw. 15 erlauben es den Mitgliedstaaten also, verpflichtend zu speichernde Verkehrsdaten in einer Art und Weise zu benutzen, die nicht mit den Verwendungsregeln des deutschen Gesetzentwurfs vereinbar ist.

Nicht einmal eine Verwendung, die mit den europäischen Grundrechten unvereinbar ist, kann durch EU-Recht sicher ausgeschlossen werden. Denn dass die Grundrechtecharta auch den Staat bindet, in dem die Verkehrsdaten nur gespeichert werden, wenn er sie für seine Zwecke verwenden will, ist durch den Gerichtshof der Europäischen Union bisher nicht entschieden worden. Eine Bindung an die Grundrechtecharta über Artikel 15 Absatz 1 der Richtlinie 2002/58/EG ist ausgeschlossen, da dieser Mitgliedstaat selbst nicht die Speicherpflicht eingeführt hat, aufgrund derer sich die Daten in seinem Hoheitsbereich befinden, die er nunmehr verwenden will. Eine Bindung des verwendenden Staates an die Grundrechtecharta kommt daher nur in Betracht, wenn er beim Zugriff auf die Daten in Durchführung des Rechts der Union handelte (Artikel 51 Absatz 1 der Charta der Grundrechte der Europäischen Union). Das ist deswegen zweifelhaft, weil es bei den in Rede stehenden Verwendungen um Handlungen auf dem Gebiet der Strafverfolgung und der Gefahrenabwehr geht, die durch das EU-Recht gerade nicht harmonisiert sind.

Eine Verwendung der Daten, die aufgrund des deutschen Gesetzes gespeichert werden, ist mit Deutschlands Verpflichtungen aus der Grundrechtecharta nicht vereinbar. Der Gerichtshof der Europäischen Union hat hervorgehoben, dass die Einführung einer Speicherpflicht mit Sicherungen einhergehen muss, die die Verwendung der Daten betreffen. Weil Deutschland die Unternehmen zur Speicherung verpflichtet, ist Deutschland dafür verantwortlich, dass die Daten nur in einer Weise verwendet werden, die der Grundrechtecharta entsprechen. Dies kann jedoch aus Sicht der Bundesregierung nur sicher gewährleistet werden, wenn die Daten in Deutschland gespeichert werden. Das EU-Recht gewährleistet dies nicht - jedenfalls solange die Vorratsdatenspeicherung und die Verwendung verpflichtend zu speichernder Daten in Europa nicht weiter harmonisiert sind.

Entsprechendes gilt für die verfassungsrechtlichen Anforderungen an Regelungen zur verpflichtenden Verkehrsdatenspeicherung.

4. Keine Relativierung der Argumentation durch die Existenz eines parallelen Pools mit von den Unternehmen zu eigenen Zwecken gespeicherten Verkehrsdaten

Dem kann nicht entgegengehalten werden, die Speicherung im Inland sei zur Verhinderung der Umgehung der engen Verwendungsregelung ungeeignet, weil für die von den Unternehmen zu eigenen, geschäftlichen Zwecken freiwillig gespeicherten Daten die Verwendungsregelungen (wie auch die Festlegung eines Speicherortes) nicht gelten und auf diese daher ohnehin ohne so weitgehende Beschränkungen zugegriffen werden könnte.

Es ist richtig, dass der deutsche Gesetzentwurf dazu führt, dass zwei Pools von Daten entstehen: Auf der einen Seite gibt es einen Pool mit den Verkehrsdaten, die die Telekommunikationsanbieter freiwillig zu eigenen Zwecken speichern (§ 96 TKG), wie es Artikel 6 der Richtlinie 2002/58/EG ermöglicht; auf der anderen Seite einen Pool mit den verpflichtend zu speichernden Verkehrsdaten. Der zweite Pool enthält somit eine Teilmenge der Daten des ersten Pools, die in ihm für eine bestimmte Zeit unter besonders hohen Sicherheitsvorkehrungen getrennt aufbewahrt werden. Beide Pools unterscheiden sich grundlegend in dem rechtlichen Regime, das auf sie

6. **Wesentlicher Inhalt**

werden. Dabei sind unterschiedlich grundlegend in dem rechtlichen Regime, das auf die Anwendung findet. Für die verpflichtend zu speichernden Daten gelten die Vorgaben, die der Gerichtshof der Europäischen Union in seinem Urteil vom 8. April 2014 gemacht hat. Für die freiwillig gespeicherten Daten gelten diese Vorgaben aber gerade nicht.

Die Unterscheidung ergibt sich zwangsläufig aus dem Urteil des Gerichtshofs der Europäischen Union und war bereits in der für unwirksam erklärten Richtlinie 2006/24/EG angelegt. Sie gründet darin, dass der Eingriff in die Grundrechte, der mit der Speicherung verbunden ist, für die beiden Datenpools ungleich intensiv ist. In Bezug auf die verpflichtend zu speichernden Daten beruht die Speicherung auf einer staatlichen Anordnung, während bei den nach § 96 TKG gespeicherten Daten die Speicherung erfolgt, damit der Vertrag zwischen Telekommunikationsunternehmen und Kunden ordnungsgemäß erfüllt werden kann. Der Inhalt des Datenpools der auf der Grundlage von § 96 TKG gespeicherten Daten kann demzufolge von den Kunden der Telekommunikationsunternehmen in gewissem Umfang beeinflusst werden. Der Kunde kann sich zum Beispiel ein Unternehmen aussuchen, das keine oder nur wenige Daten für einen sehr kurzen Zeitraum speichert. Oder er kann eine flat rate wählen, so dass die einzelnen Verbindungsdaten für die Abrechnung irrelevant werden. Das Unternehmen kann seinerseits die preiswerteste Möglichkeit der Datenspeicherung wählen – die Einhaltung bestimmter, europarechtlich harmonisierter Datenschutzstandards vorausgesetzt. Diese Einflussmöglichkeiten haben Kunde wie Unternehmen in Bezug auf die verpflichtend zu speichernden Daten nicht. Sie werden allein aufgrund staatlichen Auftrags gespeichert und dienen ausschließlich staatlichen Zwecken. Deshalb stellt die verpflichtende Speicherung auch einen Eingriff in das Eigentumsrecht der Unternehmen dar, die nun für Zwecke tätig werden müssen, die außerhalb ihrer geschäftlichen Interessen liegen.

Die Eignung der Pflicht zur Speicherung im Inland zur Erreichung des damit verfolgten Zwecks kann vor diesem Hintergrund nicht unter Verweis auf die auf der Grundlage von § 96 TKG gespeicherten Verkehrsdaten relativiert werden. Es handelt sich um zwei Datenpools, die einem unterschiedlichen rechtlichen Regime unterliegen und aus diesem Grund getrennt voneinander bewertet werden müssen.

5. Ausblick

Abschließend eine Bemerkung allgemeiner Natur: Mitgliedstaaten, die sich für die Einführung einer Speicherpflicht für Verkehrsdaten entscheiden, agieren derzeit in einem europarechtlichen Spannungsfeld, in dem sich unterschiedliche Regime überschneiden. Einerseits existiert ein umfassend harmonisiertes EU-Datenschutzrecht. Andererseits sind die Voraussetzungen für die Verpflichtung zur Vorratsdatenspeicherung und der Zugriff auf diese Daten auf EU-Ebene gerade nicht harmonisiert und sollen es nach den Verlautbarungen der Kommission auch nicht werden. Dennoch sind die Mitgliedstaaten bei der Einführung einer Speicherpflicht an die Vorgaben der Grundrechtecharta gebunden. Diese verschiedenen Anforderungen in rechtlich stimmiger Weise miteinander in Einklang zu bringen, ist eine Herausforderung. Die Bundesregierung hat sich aus den dargelegten Gründen nach sorgfältiger Prüfung für die mit dem Entwurf vorgelegte Lösung entschieden. Sie möchte bei der Kommission dafür werben, solche nationalen Entscheidungen nicht mit dem scharfen Schwert des Vertragsverletzungsverfahrens zu bedrohen, solange auf der Ebene des EU-Rechts in dieser Sache nicht für Klarheit gesorgt ist.

II. Bemerkungen

1. Vorbemerkung

6. Wesentlicher Inhalt

Die Bundesregierung teilt die von der Kommission in ihrer Pressemitteilung vom 16. September 2015 zum Ausdruck gebrachte Auffassung, nach der allein die Mitgliedstaaten darüber entscheiden, ob sie eine nationale Regelung zur verpflichtenden Speicherung von Verkehrsdaten schaffen oder nicht.

In diesem Lichte hat die Bundesregierung die Bemerkungen der Kommission zu einigen Aspekten der geplanten deutschen Gesetzgebung zur Kenntnis genommen und nimmt dazu im Folgenden Stellung.

2. Speicherdauer

Derzeit besteht in Deutschland keine Pflicht zur Speicherung von Verkehrsdaten, die die notwendigen statistischen Informationen für eine wissenschaftlich fundierte Bewertung der Wirksamkeit einer solchen Maßnahme liefern könnte. Damit eine solche Bewertung in Zukunft möglich ist, sieht der vorgelegte Gesetzentwurf eine umfassende Erhebung von statistischen Daten vor (§ 101b StPO-E). Der Bundestag wird den Entwurf zusätzlich um eine Vorschrift ergänzen, nach der die Wirksamkeit des Gesetzes einige Zeit nach seinem Inkrafttreten durch einen unabhängigen Sachverständigen evaluiert werden soll.

3. Verschiedene Kategorien von Verkehrsdaten

Nach § 96 des Telekommunikationsgesetzes dürfen die dort aufgeführten Verkehrsdaten zum Aufbau und zur Aufrechterhaltung der Telekommunikation, zur Entgeltabrechnung und zur Erkennung, Eingrenzung oder Beseitigung von Störungen oder Fehlern an Telekommunikationsanlagen von den Unternehmen gespeichert werden.

4. Zugang zu Verkehrsdaten zum Zwecke der Strafverfolgung und Funkzellenabfragen

§ 100g Absatz 1 StPO-E bezieht sich nicht auf die verpflichtend zu speichernden Verkehrsdaten, sondern auf Verkehrsdaten, die die TK-Unternehmen zu eigenen Zwecken freiwillig speichern (§ 96 TKG). Der Abruf dieser Daten ist – auch im Rahmen von Funkzellenabfragen – bereits nach dem geltenden Recht möglich. Inhaltliche Änderungen in Bezug auf die erforderlichen Straftaten sind für den Abruf von freiwillig gespeicherten Daten mit dem Gesetzentwurf nicht verbunden. Dabei wird der bereits im geltenden Recht in § 100g Absatz 1 StPO benutzte Begriff der Straftat von auch im Einzelfall erheblicher Bedeutung rechtsstaatlichen Anforderungen an die hinreichende Bestimmtheit von Normen gerecht. Diese verbieten die Verwendung auslegungsfähiger Rechtsbegriffe nicht grundsätzlich. Für eine hinreichende Bestimmbarkeit der erfassten Straftaten ist in diesem Fall schon deshalb gesorgt, weil dem Straftatenkatalog des § 100a StPO Indizwirkung zugesprochen wird („insbesondere eine in § 100a Absatz 2 bezeichnete Straftat").

5. Vorherige Prüfung des Zugangs zu Daten

Die verpflichtend zu speichernden Verkehrsdaten können von den Strafverfolgungsbehörden nur aufgrund einer richterlichen Anordnung abgerufen werden. Dies folgt aus dem Verweis in § 101a Absatz 1 StPO-E auf § 100b Absatz 1 der geltenden StPO. Anders als sonst üblich darf die Staatsanwaltschaft auch in eiligen Fällen nicht anstelle des Richters tätig werden.

6. Überwachung und Prüfung der Verwendung von Daten

Es handelt sich um eine offene Ermittlungsmaßnahme. Die Möglichkeit des nachträglichen

6. Wesentlicher Inhalt

Rechtsschutzes besteht nach den allgemeinen Regeln. Über den Verweis in § 101a Absatz 6 Satz 2 StPO-E findet § 101 Absatz 7 Satz 2 der geltenden StPO Anwendung. Dieser ermöglicht es, dem von der Maßnahme Betroffenen eine gerichtliche Überprüfung herbeizuführen, nachdem er von der Durchführung der Maßnahme benachrichtigt worden ist. Dies ist auch dann möglich, wenn die Maßnahme bereits beendet ist.

7. Anordnungen und Verlängerungen von Maßnahmen

§ 100b Absatz 1 der geltenden StPO, der durch die Verweisung in § 101a Absatz 1 StPO-E Anwendung findet, sieht vor, dass die Anordnung auf höchstens drei Monate zu befristen ist und eine Verlängerung um jeweils nicht mehr als drei Monate nur zulässig ist, wenn die Voraussetzungen der Anordnung unter Berücksichtigung der gewonnenen Ermittlungsergebnisse fortbestehen.

8. Personen, deren Kommunikation gemäß § 53 Absatz 1 Satz 1 Nummer 1 bis 5 StPO der Pflicht des Berufsgeheimnisses unterliegt

Für Personen, Behörden und Organisationen in sozialen oder kirchlichen Bereichen, die grundsätzlich anonym bleibenden Anrufern ganz oder überwiegend telefonische Beratung in seelischen oder sozialen Notlagen anbieten und die selbst oder deren Mitarbeiter insoweit besonderen Verschwiegenheitsverpflichtungen unterliegen, sieht der Gesetzentwurf eine Ausnahme von der Speicherpflicht vor (§ 113b Absatz 6 TKG). Die Besonderheit dieser Dienste ist die Anonymität der Beratung und weniger das zu wahrende Berufsgeheimnis. Um die Anonymität zu gewährleisten, ist schon im geltenden TKG vorgesehen, dass Verbindungen zu den Anschlüssen dieser Dienste nicht in Einzelverbindungsnachweise aufgenommen werden dürfen, wenn diese Anschlüsse auf einer bei der Bundesnetzagentur geführten Liste verzeichnet sind.

Berufsgeheimnisträger sind demgegenüber Gegenstand besonderer Schutzmaßnahmen; nicht weil sie ihre Leistungen – wie die genannten Einrichtungen – anonym erbringen würden (in der Regel tun sie das auch nicht), sondern weil sie zu ihren Kontaktpersonen (Mandanten, Patienten, Quellen) ein besonderes Vertrauensverhältnis haben, das geschützt werden muss, weil es seinerseits der Verwirklichung von Grundrechten dient.

Dementsprechend sieht der Gesetzentwurf anstelle einer Ausnahme von der Speicherpflicht für die Verkehrsdaten von Berufsgeheimnisträgern ein umfassendes gesetzlich explizit geregeltes Erhebungs- und Verwertungsverbot vor (§ 100g Absatz 4 StPO-E). Erhebungs- und Verwertungsverbote sind Schutzinstrumente, die sich bei anderen strafrechtlichen Ermittlungsmaßnahmen bewährt haben. Überwiegend wurden sie von der Rechtsprechung entwickelt. Nur für wenige besonders bedeutende Fälle gibt es bisher gesetzliche Regelungen. Sie genügen höchsten grundrechtlichen Anforderungen.

Zudem ist es auch kaum möglich, vollständige, tagesaktuelle Listen der Telefonnummern sämtlicher Berufsgeheimnisträger an alle Telekommunikationsunternehmen zu verteilen, die in Deutschland tätig sind. Im Übrigen wäre das auch kein Beitrag zum Datenschutz, denn die Erstellung von Listen mit Telefonnummern von bestimmten Personengruppen würde gerade wieder datenschutzrechtliche Bedenken aufwerfen.