BUNDESRECHTSANWALTSKAMMER

Stellungnahme Nr. 7
März 2025

Referentenentwurf des Bundesministeriums der Justiz eines Gesetzes zur Einführung einer Sicherungsanordnung für Verkehrsdaten in der Strafprozessordnung und zum Entwurf eines Gesetzes zur Einführung einer Mindestspeicherung von IP-Adressen für die Bekämpfung schwerer Kriminalität (BT-Drs. 20/13748)

Mitglieder des Ausschusses Strafrecht (Strauda):

RAin Dr. Carolin Arnemann
RA Prof. Dr. Jan Bockemühl
RA Prof. Dr. Alfred Dierlamm
RA Prof. Dr. Björn Gercke
RA Dr. Mayeul Hiéramente
RA Thomas C. Knierim (Berichterstatter)
RA Dr. Daniel M. Krause
RAin Theres Kraußlach
RA Prof. Dr. Holger Matt (Vorsitzender)
RA Prof. Dr. Ralf Neuhaus
RA Prof. Dr. Tido Park
RAin Dr. Hellen Schilling
RA Dr. Jens Schmidt
RAin Dr. Annette von Stetten

RAin Leonora Holling, Schatzmeisterin, Bundesrechtsanwaltskammer

Verteiler: Bundesministerium der Finanzen
Bundesministerium der Justiz
Bundesministerium des Innern und für Heimat
Justizministerien der Länder
Innenministerien der Länder
Rechtsausschuss des Deutschen Bundestages
Arbeitskreise Recht der Bundestagsfraktionen
Rechtsanwaltskammern
Der Generalbundesanwalt beim BGH
Bundesgerichtshof
Bundesverband der Freien Berufe
Bundesnotarkammer
Bundessteuerberaterkammer
Deutscher Steuerberaterverband
Wirtschaftsprüferkammer
Institut der Wirtschaftsprüfer
Deutscher Anwaltverein
Deutscher Notarverein
Deutscher Richterbund
Deutscher Juristinnenbund
Bundesvorstand Neue Richtervereinigung
Strafverteidigervereinigungen
Deutsche Strafverteidiger e.V.
Neue Richtervereinigung e.V.
Bund Deutscher Kriminalbeamter
Redaktionen der NJW,
Beck Verlag, Deubner Verlag, Jurion, Juris, LexisNexis,
Otto Schmidt Verlag,
Strafverteidiger,
Neue Zeitschrift für Strafrecht,
ZAP Verlag,
Zeitschrift für höchstrichterliche Rechtsprechung im Strafrecht,
Neue Zeitschrift für Wirtschafts-, Steuer- und Unternehmensstrafrecht,
wistra - Zeitschrift für Wirtschafts- und Steuerstrafrecht,
Zeitschrift HRR-Strafrecht,
Kriminalpolitische Zeitschrift
FAZ, Süddeutsche Zeitung, Die Welt, Handelsblatt, Tagesspiegel, LTO, Der Spiegel, Focus, Die ZEIT

Die Bundesrechtsanwaltskammer (BRAK) ist die Dachorganisation der anwaltlichen Selbstverwaltung. Sie vertritt die Interessen der 28 Rechtsanwaltskammern und damit der gesamten Anwaltschaft der Bundesrepublik Deutschland mit rund 166.000 Rechtsanwältinnen und Rechtsanwälten[1] gegenüber Behörden, Gerichten und Organisationen – auf nationaler, europäischer und internationaler Ebene.

Stellungnahme

Zusammenfassung/Abstract

Die Bundesrechtsanwaltskammer begleitet die Fortentwicklung der Debatte um die Speicherung und den Abruf von Vorratsdaten zur Bekämpfung schwerer Kriminalität mit Skepsis.

Mit dem Referentenentwurf eines „Gesetzes zur Einführung einer Sicherungsanordnung für Verkehrsdaten in der Strafprozessordnung“ des Bundesministeriums der Justiz („BMJ“) vom 24.10.2024 wird eine an strafprozessualen Kriterien ausgerichtete anlassabhängige Vorratsdatenspeicherung (sog. „Quick-Freeze-Modell“) vorgestellt. Zwar soll mit der Einführung des Quick-Freeze-Modells nur ein kurzzeitiger, anlassabhängiger Eingriff für Strafverfolgungsorgane zur Bekämpfung der schweren Kriminalität geschaffen werden. Jedoch werden zwingende Vorgaben der Rechtsprechung des Bundesverfassungsgerichts und des Europäischen Gerichtshofes zur Vorratsdatenspeicherung nicht konsequent beachtet. So kann die angenommene Löschung von „eingefrorenen“ Daten durch in der Praxis häufig vorkommende mehrfache Eingriffe umgangen werden. Dadurch kann sogar weitergehend ein umfassender Datenbestand von Verbindungs- und Standortdaten sämtlicher Nutzer bei Unternehmen, die Telekommunikationsdienstleistungen erbringen, entstehen. Das Fehlen einer fallbezogenen Zweckbindung für das „Auftauen“ solcher Datenmengen kann intensive Eingriffe in das Privatleben der Nutzer ermöglichen, was der Rechtsprechung zum Schutz der Grundrechte des Einzelnen auf eine unüberwachte, ungestörte Telekommunikation, der Wohnung und der privaten Lebensgestaltung sowie dem Schutz des Grundrechts auf informationelle Selbstbestimmung zuwiderläuft. Derartige Eingriffe betreffen auch den Beratungs- und Schutzauftrag der Rechtsanwälte und Verteidiger.

Mit dem Entwurf eines Gesetzes des Bundesrats zur Einführung einer Mindestspeicherung von IP-Adressen für die Bekämpfung schwerer Kriminalität (Bundestags-Drucksache 20/13748) vom 13.11.2024 wird weitergehend sogar eine anlassunabhängige, telekommunikationsrechtlich verankerte Dauerspeicherung von IP-Adressen und Portnummern für einen Monat zu Zwecken der Bekämpfung schwerer Kriminalität vorgeschlagen. Eine generelle Speicherpflicht bedeutet für die Unternehmen, die Telekommunikationsdienstleistungen erbringen, eine Inanspruchnahme, die über die von ihnen vertraglich zu erbringende Speicherung hinausgeht. Für Bürger bedeutet das eine Inpflichtnahme ihres Rechts auf Privatheit für die staatliche Kriminalitätsverfolgung. Einem solchen belastenden Eingriff stehen allerdings nicht die erforderlichen hinreichenden Kontrollen der weiteren Verwendung, das notwendige Verbot von Datenkombinationen sowie regelmäßige unabhängige Kontrollen gegenüber. Auch werden keine neuen Freiräume, keine erweiterte Transparenz und kein unmittelbarer Rechtschutz gegen Eingriffe geschaffen. Ein tragfähiges Modell, das der ständigen Rechtsprechung des Europäischen Gerichtshofs, des Bundesverfassungsgerichts sowie des Bundesverwaltungsgerichts zur Vorratsdatenspeicherung entsprechen könnte, ist damit auch hier noch nicht gefunden.

[1] Im Interesse einer besseren Lesbarkeit wird nicht ausdrücklich in geschlechtsspezifischen Personenbezeichnungen differenziert. Die im Folgenden gewählte männliche Form schließt alle Geschlechter gleichberechtigt ein.

I.

1. Überblick

Das im Referentenentwurf („RefE“) des BMJ vorgeschlagene „Quick-Freeze-Modell“ für Vorratsdaten, das strafprozessual verankert ist, wird kritisch bewertet.

Nach der Begründung des RefE orientiert sich das Modell an der Rechtsprechung des EuGH, die verbindliche Grenzen einer anlassunabhängigen Vorratsdatenspeicherung von Verkehrs- und Standortdaten vor allem mit Blick auf die deutschen Regelungen im TKG aufgestellt hat. Diese Rechtsprechung haben auch das Bundesverfassungsgericht und das Bundesverwaltungsgericht bestätigt. Mit Hinweis auf von dieser Rechtsprechung aufgezeigte Freiräume wird im RefE nunmehr ein anlassabhängiges „Quick-Freeze“-Modell auf strafprozessualer Grundlage gem. §§ 100g, 100k StPO-E vorgeschlagen.

Der RefE sieht vor, auf der ersten Stufe („Einfrieren“) sämtliche vorhandenen und zukünftig anfallenden Verbindungs- und Standortdaten der Mobil- und Festnetznutzer aufgrund einer gerichtlichen Entscheidung aus Anlass eines Anfangsverdachts schwerer Straftaten einzufrieren. Es wird ausdrücklich darauf verzichtet, die Maßnahme auf bestimmte Zeiträume, Personen, Personenkreise, regionale oder andere anlassbezogene Kriterien zu beschränken oder zu schützende Personengruppen auszunehmen. Zu präzisieren sind in der gerichtlichen Anordnung lediglich „die zu sichernden Daten.“ Dadurch wird ein strafprozessual fallbezogenes Löschungsverbot dieser Daten für einen Monat erreicht, das zweimalig verlängert werden kann.

Auf der zweiten Stufe („Auftauen“) soll der Abruf und die Verwendung derart gespeicherter Daten nach den allgemeinen Anforderungen des § 100g Abs. 1 StPO-E erlaubt sein, was einen entsprechenden Verdachtsgrad für die im Straftatenkatalog gem. § 100a Abs. 2 StPO normierten Tatbestände erfordert. In diesem Fall werden die „eingefrorenen“ Daten „aufgetaut“ und für strafprozessuale Zwecke „erhoben“. Allerdings sieht der RefE nicht vor, dass die das „Auftauen“ veranlassenden Stelle an den identischen Zweck gebunden ist, der zu der Anordnung des „Einfrierens“ führte. Vielmehr soll jedes Strafverfolgungsorgan unter den allgemeinen Voraussetzungen des § 100g Abs. 1 StPO-E, also auch bei einer völlig anderen Fallkonstellation, auf den eingefrorenen Datenbestand zugreifen können. Die etwaig angedachte Löschungspflicht für den durch das „Einfrieren“ geschaffenen Datenbestand wird folglich nicht eintreten, wenn allein aufgrund einer zeitnah neu hinzutretenden Verfolgungssituationen erneute Sicherungs- und Erhebungsanordnungen ergehen. Bei praxisnaher Betrachtung kann daher erwartet werden, dass in kurzen Abständen ein oder mehrere Gerichtsbeschlüsse erlassen werden, die die Löschung von „eingefrorenen“ und damit „vorhandenen“ Verbindungs- und Standortdaten verbieten. Damit bewirkt der Eingriff, dass es im Zweifel zu einer langfristigen, flächendeckenden Bevorratung sämtlicher Telekommunikationsverbindungsdaten bei Telekommunikationsdienstleistern kommt, mithin zu einem umfassenden „Datenpool“, auf den Strafverfolgungsorgane und ggfls. unter den jeweiligen gesetzlichen Voraussetzungen auch Sicherheitsbehörden zugreifen können. Der RefE zeigt keinerlei zwingende Notwendigkeit für derart weitreichende Folgen auf. Vielmehr wird offen bekannt, dass die Einführung auf rein spekulativer Tatsachengrundlage und trotz bereits bestehender hoher Aufklärungsquote erfolgen würde. So heißt es auf S. 16 des RefE *„Ob und wie viele Fälle hätten aufgeklärt werden können, gäbe es die Vorratsdatenspeicherung, bleibt damit letztlich Spekulation. Den Strafverfolgungsbehörden ist es ausweislich der polizeilichen Kriminalstatistik (PKS) für das Jahr 2023 gelungen, 87,2% der bekannt gewordenen Fälle der Verbreitung kinderpornographischer Inhalte im Sinne von § 184b Abs. 1, Satz 1 des Strafgesetzbuches a.F. aufzuklären.“* Dies ist als Basis für derart grundlegende Grundrechtseingriffe vollkommen unzureichend.

Wegen des Fehlens einschränkender, fallbezogener Zweckbindungen und der einfach zu durchbrechenden Löschungspflicht für derartig anlassabhängig gesicherte Daten, stellt das Vorhaben einen intensiven Eingriff in den Grundrechtsschutz auf unüberwachte, ungestörte Telekommunikation, der Wohnung und der privaten Lebensgestaltung sowie den Schutz des Grundrechts auf informationelle Selbstbestimmung dar. Bestimmungen über Freiräume für die private Lebensführung, die Transparenz und Kontrolle staatlichen Vorgehens und über einen unmittelbaren Rechtschutz gegen Eingriffe sind im RefE nicht vorgesehen. Ebenso fehlt es an einer präventiven gerichtlichen Kontrolle der Datenerhebung und -verarbeitung.

2. Beurteilungsmaßstab

Betroffen von einer gesetzlichen Regelung zur Vorratsdatenspeicherung sind namentlich die Grundrechte auf freie Entfaltung der Persönlichkeit (Art. 2 Abs. 1 GG), auf informationelle Selbstbestimmung (Art. 2 Abs. 1 i.V.m Art. 1 Abs. 1 GG), und auf Telekommunikationsfreiheit (Art. 10 Abs. 1 GG).[2] Eine Einschränkung dieser Grundrechte bedarf einer gesetzlichen Regelung, die an den rechtsstaatlichen Erfordernissen der Normenklarheit, Normenbestimmtheit und Justiziabilität ausgestaltet sein muss und lediglich einen an dem Gewicht dieser Grundrechte orientierten, nach dem Grundsatz der Verhältnismäßigkeit beschränkten Eingriff für schwerwiegende Einzelfälle erlauben darf.[3]

Damit korrespondieren die europäischen Grundrechte auf Achtung des Privat- und Familienlebens (Art. 7 Abs. 1 GRCh), auf den Schutz personenbezogener Daten (Art. 8 Abs. 1 GRCh) und auf Meinungsfreiheit (Art. 11 Abs. 1 GRCh). Diese europäischen Grundrechte sind von großem Ausmaß und besonderer Schwere, so dass eine Einschränkung jeweils einer besonderen gesetzlichen Begründung bedarf (Art. 52 GRCh). In Anwendung des europäischen Rechtsrahmens hat der EuGH in ständiger Rechtsprechung den hohen Stellenwert dieser Grund- und Freiheitsrechte des Einzelnen gegenüber nationalen gesetzlichen Eingriffen hervorgehoben, die eine verdachtslose Vorratsdatenspeicherung bewirkt hätten.[4] Danach verstoßen generelle Speicherpflichten verschiedenster Daten, die bei Diensten der Telekommunikation anfallen, gegen diese Grundrechte.

U.a. hat der EuGH im Urteil vom 20.09.2022[5] zum deutschen TKG (§§ 175 ff. TKG) betont, dass eine anlasslose Vorratsdatenspeicherung, die flächendeckend eine personell, zeitlich und geografisch undifferenzierte Erfassung nahezu sämtlicher Bevölkerungskreise erlaubt, nicht gerechtfertigt ist, selbst wenn die Regelung nur eine kurze Speicherdauer oder auch strenge Regelungen zum Schutz gegen Missbrauch vorsieht. Dieser Rechtsprechung haben sich das BVerwG[6] und das BVerfG[7] angeschlossen.

---

[2] stRspr, vgl. nur BVerfG, Urteil vom 14.07.1999-1 BvR 2226/94, 2420/95 u. 2437/95 (BND-Gesetz); BVerfG, Urteil vom 16.06.2009 - 2 BvR 902/06; BVerfG, Beschluss vom 14.12.2000 - 2 BvR 1741/99 (genetischer Fingerabdruck); BVerfG, Beschluss vom 22.05.2009, 2 BvR 287/09 und 2 BvR 400/09; BVerfG Urteil vom 02.03.2010 – 1 BvR 256/08 (Vorratsdatenspeicherung).

[3] BVerfG, Urteil vom 02.03.2010 – 1 BvR 256/08, 1 BvR 263/08 und 1 BvR 586/08.

[4] EuGH, Urteil vom 30.04.2024, Rs. C-470/21, La Quadrature du Net u. a. & lutte contre la contrefaçon; EuGH, Urteil vom 20.09.2022, verb. Rs. C-793/19 und C-794/19, SpaceNet und Telekom Deutschland; EuGH, Urteil vom 05.04.2022, Rs. C-140/20, Commissioner of An Garda Síochána; EuGH, Urteil vom 06.10.2020, verb. Rs. C-511/18, C-512/18 und C-520/18, La Quadrature du Net u. a..

[5] EuGH, Urteil vom 20.09.2022, verb. Rs. C-793/19 und C-794/19, Rn. 83 ff., 87 ff., 93.

[6] BVerwG, Urteil vom 14.08.2023, 6 C 6.22 und 6 C 7.22; s. dazu der RefE des BMJ S. 19.

[7] BVerfG Beschluss vom 04.12.2023, 1 BvR 229/16; s. dazu der RefE des BMJ S. 19.

Das Bundesverfassungsgericht hatte schon im Urteil zur Vorratsdatenspeicherung vom 02.03.2010[8] hinsichtlich des Zugriffs auf Verkehrsdaten angemahnt, dass zwischen der Speicherung von Verkehrsdaten und deren Abruf zu differenzieren ist: *„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 Erbringer öffentlich zugänglicher Telekommunikationsdienste in Abhängigkeit von den jeweiligen betrieblichen und vertraglichen Umständen – von den Kunden teilweise beeinflussbar – nach dem bisherigen § 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."*

Der EuGH hat ebenfalls die Vorratsdatenspeicherung als einen schwerwiegenden Eingriff in die o.g. europäischen Grundrechte eingeordnet.[9] Der EuGH erkennt zwar in engen Grenzen ein Gemeinwohlinteresse an, das sich auch moderner technischer Instrumente bedienen müsse. Aber aus Gründen der Verhältnismäßigkeit des Eingriffs bedürfe es ausreichend klarer und präziser Regeln für die Tragweite und die Anwendung der Maßnahme, ebenso wie die Aufstellung von Mindestanforderungen, so dass den Betroffenen Garantien für einen Schutz vor Missbrauch und vor einem unberechtigten Zugriff auf ihre Daten gewährt werden müssten. Letztlich sei bei den vom EuGH überprüften europäischen Regeln auch die Verhältnismäßigkeit im engeren Sinne nicht gewahrt, da diese nicht auf das absolut Notwendige beschränkten, sondern sich auf alle Personen und alle elektronischen Kommunikationsmittel sowie auf sämtliche Verkehrsdaten erstreckten, ohne Differenzierung, Einschränkungen oder Ausnahmen vorzusehen.

Namentlich bekräftigt der EuGH[10], dass bei einer **tatsächlichen ernsthaften Bedrohung für die nationale Sicherheit**, die gegenwärtig oder vorhersehbar ist, ein enger Spielraum für eine allgemeine und unterschiedslose Speicherung von Daten bestehe. Diese Speicherung und der Abruf der Daten müsse aber durch zeitliche Begrenzungen und umfassende gerichtliche Kontrollmöglichkeiten verhältnismäßig ausgestaltet werden. Ebenso soll bei einer zukünftigen Regelung zur **Verfolgung schwerer Straftaten** eine verhältnismäßige Ausgestaltung der gezielten Speicherung von Daten verdächtiger Personengruppen möglich sein, sofern die Speicherung hinsichtlich bestimmter Kategorien der zu speichernden Daten, der erfassten elektronischen Kommunikationsmittel, der betroffenen Personen und der vorgesehenen Dauer der Vorratsspeicherung auf das absolut Notwendige beschränkt ist. Als weitere Möglichkeit der Einschränkung führt der EuGH die Speicherung von Verkehrs- und Standortdaten begrenzt durch objektive oder geografische Kriterien – etwa an Verkehrsdrehkreuzen, Flughäfen oder Bahnhöfen – für einen bestimmten Zeitraum an, ebenso wie eine Anordnung von Quick-Freeze in Form des Einfrierens von Verkehrsdaten bei einem konkreten Verdacht.[11] Die Europarechtswidrigkeit der §§ 175 ff. TKG, die der EuGH mit dem Urteil vom 20.09.2022[12] festgestellt

[8] BVerfG, Urteil vom 02.03.2010 – 1 BvR 256/08 u.a., NJW 2010, 833, Rn. 227.

[9] EuGH, Urteil vom 08.04.2014 – verb. Rs C-293/12 und C-594/12 (Digital Rights Ireland, Vorlage Österreich) NJW 2014, 2169, Rn. 37-40.

[10] EuGH, Urteil vom 08.04.2014 – verb. Rs C-293/12 und C-594/12 (Digital Rights Ireland); EuGH Urteil vom 21.12.2016 – verb. Rs C 203/15 und C-698/15 (Tele2/Sverige u.a.); EuGH Urteil v. 6.10.2020 – verb. Rs. C-623/17 (Privacy International) und C-511/18, C 512/18, C 520/18 (La Quadature du Net); EuGH, Urteil vom 20.09.2022, Rn. 114 ff.

[11] BeckOK-StPO/Bär, StPO, 53. Ed. 2024, § 100g Rn. 68b

[12] EuGH, Urteil vom 20.09.2022, - C-793/19 (Spacenet) und C-794/19 (Deutsche Telekom); NJW 2022, 3135 mAnm Roßnagel; vgl. dazu auch BeckOK-StPO/Bär, StPO, 53. Ed. 2024, § 100g Rn. 68b.

hatte, führte nach Auffassung des BVerwG[13] dazu, dass eine Anwendung der §§ 175 ff. TKG nicht mehr möglich ist.

3. Zur „Sicherungsanordnung“ nach dem Referentenentwurf

a) Das Quick-Freeze-Modell orientiert sich an dem vom EuGH europarechtlich für zulässig gehaltenen Gedanken einer anlassabhängigen Vorratsspeicherung durch die Anbieter von Telekommunikationsdienstleistungen.[14] Der rein strafprozessual ausgestaltete Eingriff soll zweistufig erfolgen. In der ersten Stufe des Eingriffs ist ein „Einfrieren“ („Quick-Freeze“) unter den Tatbestandsvoraussetzungen des § 100g Abs. 6 Satz 1 StPO-E vorgesehen, das Verfahren dazu richtet sich dann nach den Vorgaben der §§ 101a Abs. 1a, 100e Abs. 1, 3, 4, 5 S. 1 StPO-E. Auch soll die Maßnahme nur gerichtlich angeordnet werden können, wobei flankierend eine Eilkompetenz der Staatsanwaltschaft vorgesehen ist. Auf der zweiten Stufe ist die Erhebung (Abruf) der derart gespeicherten Daten durch Strafverfolgungsbehörden („Auftauen“) vorgesehen.

Der RefE weist für den Zugriff auf die gespeicherten Daten allgemein (§ 100g Abs. 6 S. 2 StPO-E) auf die Eingriffsbefugnisse der Strafverfolgungsorgane gem. § 100g Abs. 1, 1a und 3 StPO-E.

b) **Gegenstand der Anordnung** sollen die von den Anbietern öffentlicher Telekommunikationsdienste bei der Nutzung eines Dienstes erzeugten oder verarbeiteten und noch vorhandenen Verkehrsdaten[15] sein.[16] Aufgrund der technischen Verknüpfung der Verkehrsdaten mit Standortdaten sind damit sämtliche beim Anbieter vorhandenen Daten aus Vergangenheit, Gegenwart und Zukunft gemeint. Die Anordnung wird allerdings vom Gericht aus Anlass eines Verfolgungsfalls ("soweit die Verkehrsdaten für die Erforschung des Sachverhalts oder zur Ermittlung des Aufenthaltsortes eines Beschuldigten von Bedeutung sein können") ausgerichtet, so dass in der Anordnung die zu speichernde Datenart zu präzisieren ist. Durch § 174a Abs. 1 TKG-E wird ergänzend lediglich vorgegeben, dass aufgrund einer Sicherungsanordnung keine weitergehenden Inhaltsdaten zu speichern sind.

c) **Adressaten der Sicherungsanordnung** sind sämtliche Anbieter von Internetzugangsdiensten, nummerngebundenen interpersonellen Telekommunikationsdiensten sowie von Diensten, die ganz oder überwiegend in der Übertragung von Signalen bestehen, wie Übertragungsdienste, die für Maschine-Maschine-Kommunikation und für den Rundfunk genutzt werden.[17] Ausgenommen sind lediglich die sog. nummernunabhängigen interpersonellen Telekommunikationsdienste. Diese Ausnahme betrifft in der Praxis vor allem E-Mail-Dienste und Messengerdienste, die damit nicht von der Sicherungsanordnung betroffen sein sollen. Die Verpflichtung der Adressaten wird durch entsprechende Anwendung des § 100a Abs. 4 StPO (strafprozessuale Folgeleistungspflicht) sowie durch § 174a Abs. 1 TKG-E (telekommunikationsrechtliche Umsetzungspflicht) sichergestellt. Dies entspricht dem Doppeltürenmodell des BVerfG.[18]

---

[13] BVerwG, Urteil vom 14.08.2023 – 6 C.13.18, BeckRS 2023, 24616.

[14] Gesetz zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten vom 10.12.2015 (BGBl. I 2015 S. 2218).

[15] Begriffsdefinition gem. §§ 9, 12 Gesetz über den Datenschutz und den Schutz der Privatsphäre in der Telekommunikation und bei digitalen Diensten (TDDDG), § 2a Gesetz über die Errichtung einer Bundesanstalt für den Digitalfunk der Behörden und Organisationen mit Sicherheitsaufgaben (BDBOSG)

[16] RefE S. 20, 29

[17] RefE S. 29: Begriffsdefinition gem. § 3 Nr. 61 Telekommunikationsgesetz (TKG)

[18] BVerfG, Beschluss vom 24.01.2012 – 1 BvR 1299/05; s.a. BVerfG, Beschluss vom 19.04.2021 – 1 BvR 1732/14; BVerfG, Beschluss vom 27.05.2020 – 1 BvR 1873/13, 1 BvR 2618/13.

d) Ein bestimmter Kreis der von der Sicherungsanordnung betroffenen **Endnutzer der Telekommunikationsdienste** wird hingegen im RefE nicht näher bestimmt. Der RefE (S. 31) geht vielmehr davon aus: „…Bewusst weit soll in § 100g Absatz 6 StPO-E schließlich der Kreis der Personen gefasst sein, deren Verkehrsdaten von einer Sicherungsanordnung umfasst sein können („des Betroffenen"). Um die Sicherungsanordnung effizient auszugestalten, sollen nämlich nicht nur Verkehrsdaten von Tatverdächtigen oder von sogenannten Nachrichtenmittlern gesichert werden können, sondern – in den Grenzen der vorgenannten Zweckbindung – auch von anderen Personen. …".

e) Tatbestandlich setzt die Sicherungsanordnung sodann voraus, dass die Anordnung bereits ergehen darf, wenn sich der Verdacht auf die Verwirklichung bzw. den Versuch oder die Tatbeteiligung einer Straftat bezieht, die im **Straftatenkatalog des § 100a Abs. 2 StPO** aufgeführt ist. Damit wird zwar hinsichtlich der Verkehrsdaten die bereits vorhandene Regelung gem. § 100g Abs. 1 Nr. 1 StPO übernommen. Das gilt auch für Standortdaten, soweit bislang auf gegenwärtige und zukünftig entstehende Daten zugegriffen wird. Jedoch werden die Anforderungen hinsichtlich der retrograden Standortdaten (bisheriger § 100g Abs. 1 S. 3 StPO) dadurch abgesenkt. Die Ausweitung der Speicherpflicht hinsichtlich der Standortdaten vertieft daher den Eingriff in die Grundrechte der Nutzer.

f) Es wird nicht verkannt, dass die Bezugnahme des § 100g Abs. 6 S. 1 Hs. 2 StPO-E auf eine „**in Absatz 1 oder 1a bezeichnete Straftat**" eine die Schwere des Eingriffs begrenzende Funktion haben kann, wobei der RefE insbesondere auch die Tatschwere im Einzelfall und auch die Aussichtslosigkeit anderweitiger Aufklärung (Abs. 1a Nr. 2) in die Anordnungsvoraussetzungen der Sicherungsanordnung einbezieht. Es wird aber in der Praxis in der Regel lediglich der Verdachtsgrad der „**zureichenden tatsächlichen Anhaltspunkte**" für eine Tatbegehung, einen Tatversuch oder eine Tatbeteiligung (vgl. etwa auch § 98a Abs. 1 StPO) zugrunde gelegt werden. Damit wird aber wiederum die Eingriffsschwelle der Vorgaben in Absatz 1, 1a und Absatz 3 abgesenkt und klargestellt, dass die Sicherungsanordnung bereits bei einer einfacher gelagerten Verdachtslage möglich sein soll. Dadurch können zwar vage kriminalistische Vermutungen ausgeschlossen werden, allerdings führt dieses Erfordernis nicht zur Beschränkung auf bestimmte Nutzer oder Nutzergruppen. Allein das Vorhandensein zureichender tatsächlicher Anhaltspunkte dient mithin nicht der Eingrenzung des vom Eingriff betroffenen Personenkreises, sondern beschränkt allenfalls die Anordnungshäufigkeit.

g) Mit Blick auf das **Anordnungsverfahren** der Sicherungsanordnung gem. Abs. 6 S. 1 beschränkt der RefE (§§ 101a Abs. 1, Abs. 1a StPO-E) aber bereits die Schutzvorschriften gem. § 100e StPO auf die Absätze 1, 3, 4 und 5 S. 1 und 2 StPO. Mithin muss ein Gericht die Anordnung erlassen, gleichwohl besteht eine Eilkompetenz der Staatsanwaltschaft, die einer richterlichen Bestätigung binnen drei Tagen bedarf. Dies soll auch für die Sicherungsanordnung von Standortdaten gelten. Die Anordnung bedarf einer Begründung und muss auf einen Monat befristet sein. Die Frist kann aber zweimalig um einen Monat bei Fortbestehen der Voraussetzungen verlängert werden.

Im Beschluss muss die Art der Daten eindeutig angegeben werden. Eine sonstige Begrenzung auf die Daten bestimmter Mobilgeräte, bestimmter Personen oder Personengruppen oder eine regionale Begrenzung, können, müssen aber nicht angegeben werden. Eine gerichtliche Kontrolle der Umsetzung der Anordnung wird gem. § 100e Abs. 5 StPO auf die allgemeine Beendigungspflicht bei Wegfall der Anordnungsvoraussetzungen (S. 1) sowie den Bericht über das Ergebnis (S. 2) beschränkt. Dies sind allerdings lediglich Formalmitteilungen, eine inhaltliche Bewertung oder Maßnahme oder weitere Kontrollen sieht der Entwurf nicht vor.

h) In der **Bewertung des RefE** ist zunächst zu berücksichtigen, dass der weite Einbezug praktisch sämtlicher Endnutzer von Telekommunikationsdiensten durch das Quick-Freeze-Modell nicht der vom

EuGH[19] vorgegebenen Beschränkung des Eingriffs auf Einzelpersonen oder Personengruppen entspricht. Vorzugswürdig wäre es auch, dass die vom EuGH genannte Spezifizierung auf Personengruppen bzw. regionale Kriterien (bspw. Verkehrsknotenpunkte, Bahnhöfe, Flughäfen, Grenzkontrollstellen etc.) begrenzend eingebracht werden würde. Wie schon bei früheren unzulässigen Regelungen zur Vorratsdatenspeicherung führt auch die im RefE angelegte großzügige unbestimmte Ausgestaltung eines anlassbezogenen Eingriffs zur Speicherung einer unbestimmten Vielzahl von Nutzerdaten der Internet- und Telekommunikationsdienste sämtlicher Nutzer, stellt mithin einen schwerwiegenden Eingriff in die Grundrechte sämtlicher Nutzer dar. Das dadurch angeordnete Löschungsverbot unterliegt einer Zweckbindung im Rahmen der Verdachtsfeststellung. Diese fallbezogene Zweckbindung wird aber telekommunikationsrechtlich nicht verbindlich umgesetzt, es entsteht kein „Sonderdatenbestand“.

Zudem kann die Löschungspflicht der durch „Quick-Freeze“ geschaffenen Vorratsdaten durchbrochen werden, wenn unabhängig von der Erstentscheidung nachfolgende Entscheidungen erneut die Speicherung von vorhandenen und zukünftigen Vorratsdaten anordnen, mithin auch bereits durch Quick-Freeze gespeicherte Datenbestände vollständig oder teilweise erfassen. Bei realitätsnaher Betrachtung der Ermittlungsaktivitäten der Bundesanwaltschaft und der Staatsanwaltschaften in Deutschland kann angenommen werden, dass zeitlich gestaffelt unterjährig immer wieder Quick-Freeze-Anordnungen ergehen, so dass es nicht zu einem Wegfall einer aus einem anderen Anlass geschaffenen Datenspeicherung kommen würde. Mithin tritt die Löschungspflicht nicht ein.

Zwar steht die Eignung der gespeicherten Daten im Falle einer Einfrierens-Anordnung aus einem anderen Anlass nicht von vornherein fest, allerdings ist zu befürchten, dass ohne fallabhängige Spezifizierungen ein umfassender Datenpool entsteht, der bei einem späteren Abruf umfassend eingesetzt werden kann.

Eine bestimmte zwingende Notwendigkeit für einen so intensiv wirkenden Eingriff benennt der RefE nicht. Dem Hinweis des RefE (S. 22), dass eine Verpflichtung nach der Verordnung (EU) 2023/1543 („E-Evidence“-Verordnung) vom 12.07.2023 besteht, eine gesetzliche Grundlage für Sicherungsanordnungen zur Erfüllung einer europarechtlichen Gegenseitigkeit i.S.v. Art. 6 Abs. 3 der E-Evidence-VO zu gewährleisten, kann durch eine Fortentwicklung des geltenden Rechts unter Beachtung der Rechtsprechung des EuGH aus den Urteilen vom 06.10.2020 und 20.09.2022 entsprochen werden.

4. Modell zur Erhebung gespeicherter Verkehrs- und Standortdaten

a) In der zweiten Stufe des Modells soll die **Erhebung der Daten** („Auftauen“) durch die Strafverfolgungsbehörden gemäß § 100g Abs. 6 S. 2 StPO-E nach den Vorgaben des § 100g Abs. 1, 1a und 3 StPO-E erfolgen. Auch weiterhin sollen keine Inhaltsdaten abgerufen werden können (RefE, S. 31). Eine Datenerhebung erstreckt sich auf sämtliche gespeicherte Daten unter den Tatbestandsvoraussetzungen des § 100g Abs. 1, 1a und 3 StPO-E. Auch wenn die bisherige Eingriffsregelung gem. den §§ 100g, 100k StPO den Anforderungen der Rechtsprechung entsprochen hat, muss noch einmal darauf hingewiesen werden, dass eine ungleich veränderte Datenlage durch vorhergehende Datenspeicherungsanordnungen besteht. Außerdem werden sämtliche Nutzer der Telekommunikationsdienste für die staatliche Aufgabe der Strafverfolgung in Pflicht genommen,

[19] EuGH, Urteil vom 20.09.2022, - C-793/19 (Spacenet) und C-794/19 (Deutsche Telekom); NJW 2022, 3135 mAnm Roßnagel; vgl. dazu auch BeckOK-StPO/Bär, StPO, 53. Ed. 2024, § 100g Rn. 68b.

obgleich sich ein zum Abruf berechtigender Verdacht nur bei den im konkreten Verfahren beschuldigten einzelnen Personen ergeben hat.

b) Der RefE **will den Zugriff auf Verbindungs- und Standortdaten** sämtlicher von der Speicherung betroffenen Nutzer durch die Erlaubnis zum Abruf gespeicherter Daten (bisher § 100g Abs. 1 S. 3, Abs. 3 StPO) erleichtern.[20] Die Anforderungen werden in § 100g Abs. 1a StPO-E neu formuliert. Insbesondere die Speicherung **vergangenheitsbezogener (retrograder) Standortdaten** (bisher § 100g Abs. 1 S. 3 StPO), die wegen der Ermöglichung einer Erstellung von Bewegungsprofilen besonders intensiv in die Grundrechte der betroffenen Nutzer eingreift, ist nach geltendem Recht nur unter den engeren Voraussetzungen des § 100g Abs. 2, 4 und § 101a Abs. 2, 4 und 5 StPO (geringerer Umfang des Straftatenkatalogs, besondere Schwere der Straftat im Einzelfall, wesentliche Erschwernis oder Aussichtslosigkeit der Sachverhaltsaufklärung bzw. der Aufenthaltsermittlung, allein richterliche Entscheidungsbefugnis, usw.) zulässig. Im Zuge der nun vorgesehenen Absenkung von Zugriffsschranken auf solche Daten wird eine Erstellung von Persönlichkeits-, Lebensumfeld- und Bewegungsprofilen für Verdächtige, Tatmittler, Opfer und sonstige Personen von Interesse im Sinne des § 100g Abs. 1a StPO-E ermöglicht.

Soweit der RefE (S. 2, 22, 23, 27) auf Verpflichtungen gem. Art. 14 und Art. 16 des (Budapester-) Übereinkommens des Europarats über Computerkriminalität vom 21. November 2001[21] verweist, hatte die geltende Regelung in § 100g Abs. 1 StPO das im Jahr 2008 in Deutschland ratifizierten Übereinkommens beachtet.[22] Für eine Neuregelung gilt auch insoweit, dass eine Ausgestaltung einer solchen Verpflichtung im nationalen Recht den Vorgaben des EuGH entsprechen muss.

c) Für anterograde und retrograde Standortdaten der **Funkzellenabfrage** (§ 100g Abs. 3 StPO) will der RefE ebenfalls die Anforderungen für Speicherung und Erhebung absenken. Dass die Erhebung retrograder Standortdaten in der Funkzelle nach der geltenden Vorschrift gem. § 100g Abs. 3 S. 2 StPO nur unter den Voraussetzungen des Straftatenkatalogs gem. § 100g Abs. 2 StPO erfolgen darf und bei einer Verletzung der Voraussetzungen zu einem Verwertungsverbot führt, ist in der Rechtsprechung des BGH[23] anerkannt. Dies entspricht dem Grundrechtsschutz. Einige Landgerichte[24] vertreten allerdings die Auffassung, die Funkzellenabfrage als solche unterliege nicht den Anforderungen, die an eine Abfrage retrograder Standortdaten zu stellen wären. Die in diesen Entscheidungen vorzufindenden Unterscheidungskriterien nach Datenart, Erhebungsverfahren und Datenumfang haben allerdings jeweils einzelfallbezogene Gründe, die das Grundprinzip, dass die Abfrage retrograder Standortdaten nur gem. § 100g Abs. 3 S. 2 StPO zulässig ist, nicht in Frage stellen.

Der RefE will die Sicherung von Funkzellendaten generell unabhängig von der Datenart der Regelung gem. § 100g Abs. 6 S. 1 StPO-E unterstellen und damit die Erhebung derart gespeicherter Daten nach ausschließlich nach den neuen Anforderungen des § 100g Abs. 3 StPO-E zulassen. Dadurch würden die Beschränkungen durch § 100g Abs. 2 StPO wegfallen. Der Wegfall der engeren Eingriffsgrenzen

---

[20] BeckOK-StPO/Bär, StPO, 53. Ed. 2024, § 100g Rn. 3, 17; BGH, Beschluss vom 10.01.2024- 2 Str 171/23 zur Funkzellenabfrage.

[21] Zum Übereinkommen vgl. das deutsche Umsetzungsgesetz vom 05.11.2008, BGBl. II S. 1242; das 41. StrafrechtsÄndG vom 07.08.2007, (BGBl I 2007 S. 1786, sowie das TKÜ-Gesetz vom 21.12.2007, BGBl. I S. 3198; zum TKÜ-Gesetz vgl. Nichtigkeit der §§ 100g Abs. 1 S. 1 StPO, §§ 113a, 113b TKG gem. BVerfG, Urteil vom 02.03.2010 – 1 BvR 256/08, 1 BvR 263/08 und 1 BvR 586/08.

[22] Vgl. dazu auch das EuGH Urteil vom 06.10.2020 „La Quadrature du Net u. a.“, C-511/18, C-512/18 und C-520/18, Rz. 162.

[23] BGH, Beschluss vom 10.01.2024- 2 Str 171/23, BeckRS 2024, 10088; BGH, Beschl. v. 03.08.2017 – 1 BGs 237/17, NStZ 2018, 47.

[24] Für die Zulässigkeit nach geltendem Recht vgl. LG Stade, Beschl. v. 26.10.2018- 70 Qs 133/18, BeckRS 2018, 27043; LG Arnsberg, Beschluss vom 29.04.2019 - 2 Qs-410 UJs 254/19-43/19, BeckRS 2019, 8528; LG Regensburg, Beschl. v. 05.09.2024 – 8 Qs 30/24, BeckRS 2024, 22752.

sowie der erweiterte Zugriff auf retrograde Standortdaten widerspricht dem mit der gegenwärtigen Regelung verbundenem Grundrechtsschutz. Eine veränderte Gefahrenlage oder ein spezifisches Kriminalitätsbekämpfungsbedürfnis wird vom RefE nicht dargetan.

d) Hinsichtlich der Ermöglichung der Nachkontrolle der Datenverwendung ist zwar zu begrüßen, dass auch in Zukunft die gesicherten Daten zu kennzeichnen sind (§ 101a Abs. 3 StPO, § 174a Abs. 4 S. 5 TKG-E), um den Herkunftsnachweis aus einer Maßnahme gem. § 100g Abs. 6 StPO-E zu ermöglichen. Dagegen sollen die im geltenden Recht vorgesehenen Verwendungsbeschränkungen (§§ 101a Abs. 1, 100e Abs. 6 StPO, sowie gem. § 101a Abs. 4 und Abs. 5 StPO) entfallen. Wie der RefE selbst konstatiert, greift schließlich auch die Benachrichtigungspflicht gem. § 101 Abs. 4 S. 1 Nr. 3 StPO-E meist nicht, da Personen, deren Identität nicht aufgedeckt wurden, auch nicht benachrichtigt werden können (RefE S. 31, 33). Justizinterne Kontrollen, die an Vorgaben der §§ 100g Abs. 2 und 4, 101a Abs. 2, 4 und 5 StPO anknüpfen könnten, wären in diesem Fall ebenfalls wirkungslos, weil schon die Datenerhebung diese Vorgaben nicht mehr beachten müsste. Mithin fehlt es an objektiven Kontrollen für die Verwendung der erhobenen Daten durch die Strafverfolgungsbehörden.

e) Änderungen für die Speicherung und den **Abruf von Nutzungsdaten**[25] in § 100k Abs. 1, 1a StPO-E sollen eine Aufteilung zwischen Nutzungsdaten und Standortdaten ermöglichen, für letztere soll eine Rückverweisung auf § 100g Abs. 1a StPO-E erfolgen. Auch hier ist die Absenkung der Voraussetzungen für den Abruf der Standortdaten problematisch.

f) Die Absenkung der Anforderungen an die Speicherung von Vorratsdaten und die anschließende Datenerhebung durch Strafverfolgungsbehörden unterliegt der schon zuvor geäußerten **Kritik** (vgl. dazu I.3.h). Die Mehrbelastung des einzelnen (unbeteiligten) Bürgers erfolgt ohne Abwägung der Verhältnismäßigkeit des Eingriffs. Auch stehen einer solchen Neuregelung keine Entlastungen durch Schaffung rechtlicher Freiräume, verbesserte Transparenz oder eines Zugewinns an Rechtschutz gegenüber. Der mit dem Quick-Freeze Modell verbundene Verzicht auf eingriffsbegrenzende Normen wird nicht anderweitig kompensiert. Betroffen wäre auch der Beratungs- und Schutzauftrag von zeugnisverweigerungsberechtigten Personen, insbesondere auch der Rechtsanwälte und Verteidiger, da das Quick-Freeze-Modell für Grund- und Menschenrechte sowie die Rechte von Zeugnisverweigerungsberechtigten keinen besonderen Schutz vorsieht und bestehende Hürden abgebaut werden. Weder soll der Freiraum höchstpersönlicher Lebensgestaltung sichergestellt werden, noch wird ein Betroffener durch rechtzeitige Information in die Lage versetzt, seine Rechte wahrzunehmen.

II.

1. Überblick

Der Entwurf eines „Gesetzes zur Einführung einer Mindestspeicherung von IP-Adressen für die Bekämpfung schwerer Kriminalität“ des Bundesrats vom 13.11.2024 (Bundestags-Drucksache 20/13748) auf Initiative des Bundeslands Hessen schlägt eine telekommunikationsrechtlich ausgestaltete Speicherpflicht von IP-Adressen für die Dauer von einem Monat vor. Außerdem sollen die damit verbundenen Daten über Anschlussinhaber und Benutzerkennung (§ 176 Abs. 1 TKG-E) gespeichert werden. Die Datenspeicherungspflicht wird mit einer allgemeinen Zweckbindung „für Zwecke der Bekämpfung schwerer Kriminalität“ gerechtfertigt und verändert im Wesentlichen die strafprozessualen Anforderungen an den Abruf der gespeicherten Daten nicht. Lediglich die

[25] Begriffsdefinition in § 2 Abs. 2 Nr. 2 TDDDG

Anforderungen für die Abfrage von Funkzellendaten sollen abgesenkt werden, indem die Bezugnahme auf die Anforderungen gem. § 100g Abs. 3 S. 2 StPO entfallen sollen.

2. Beurteilungsmaßstab

Beurteilungsmaßstab für den Gesetzgebungsvorschlag ist die oben unter I.2. zusammengefasste Rechtsprechung des BVerfG und des EuGH zur generellen, anlassunabhängigen Vorratsdatenspeicherung. Insbesondere hat der EuGH in den zitierten Entscheidungen[26] angenommen, dass eine Datenspeicherung zur Bekämpfung schwerer Kriminalität eingeführt werden kann, allerdings bedarf es nach dieser Rechtsprechung zum Schutz der Grundrechte außerdem aus Gründen der Verhältnismäßigkeit des Eingriffs ausreichend klarer und präziser Regeln für die Tragweite und die Anwendung der Maßnahme, ebenso wie die Aufstellung von Mindestanforderungen, so dass den Betroffenen Garantien für einen Schutz vor Missbrauch und vor einem unberechtigten Zugriff auf ihre Daten gewährt werden müssten. Letztlich ist auch die Verhältnismäßigkeit im engeren Sinne zu wahren, d.h. Regelungen sind auf das absolut Notwendige zu beschränkten, insbesondere sind Differenzierungen, Einschränkungen oder Ausnahmen zum Schutz der privaten Lebensverhältnisse vorzusehen.

In der Entscheidung des EuGH vom 30.04.2024[27] hat der EuGH die grundsätzliche Zulässigkeit der Speicherung von IP-Adressen für den Nachweis von Urheberrechtsverletzungen durch die französische HADOPI erlaubt, deren Aufgaben seit dem 1.1.2022 durch die französische Regulierungsbehörde ARCOM durchgeführt werden.[28] In der genannten Entscheidung hat der EuGH der HADOPI allerdings ebenfalls bestimmte Vorgaben gemacht, indem die Daten zu Bedingungen und unter technischen Modalitäten gespeichert werden, die gewährleisten müssen, dass *„… es ausgeschlossen ist, dass aus der Vorratsspeicherung genaue Schlüsse auf das Privatleben der Inhaber der IP-Adressen, zB durch Erstellung ihres detaillierten Profils, gezogen werden können. …“* Zudem muss die Gesamtnutzung verschiedener Daten, die auf Persönlichkeit und Lebenswandel der Person schließen lassen, durch geeignete Maßnahmen verhindert und die Dauer der Speicherung auf das absolut notwendige Maß beschränkt sein. Der EuGH geht noch weiter, indem auch der Zugang einer Behörde zu den gespeicherten Daten ausschließlich für die Identifikation von Personen ermöglicht werden darf, die schon im Verdacht einer Straftat stehen. Auch darf mit den Daten keine Profilerstellung ermöglicht werden. Schließlich hat sich der EuGH in der Entscheidung gehen automatisierte IT-Routinen ausgesprochen, die etwaige auf diesem Weg erlangte Daten mit anderen Daten verknüpfen könnten, die sich im Besitz der Behörden befinden oder über andere Maßnahmen erlangt worden sind. Daher sei es auch weiterhin verboten, durch Datenanalysen oder Verknüpfungen beliebiger Verbindungs- und Nutzungsdaten „… Schlüsse auf das Privatleben der Person zu ziehen, deren IP-Adresse für Aktivitäten genutzt wurde, die möglicherweise Urheberrechte oder verwandte Schutzrechte verletzen. …“ Schließlich verlangt der EuGH auch eine regelmäßige Revision der Integrität der Datenverarbeitungssysteme der Behörden.

[26] EuGH, Urteil vom 08.04.2014 – verb. Rs C-293/12 und C-594/12 (Digital Rights Ireland, Vorlage Österreich) NJW 2014, 2169, Rn. 37-40.

[27] Vgl. oben Fn. 3, EuGH, Urteil vom 30.04.2024, Rs. C-470/21, La Quadrature du Net u. a. & lutte contre la contrefaçon, ZD 2024, 569.

[28] Vgl. dazu bspw. *Mathieu Pollet* übersetzt von Charles Szumski: French government creates new online antipiracy body. (https://www.euractiv.com/section/digital/news/french-government-creates-new-online-antipiracy-body) In: Euractiv. 26. Oktober 2021; vgl. auch Krempl, EuGH-Gutachter für Vorratsdatenspeicherung im Kampf gegen Urheberrechtsverstöße, heise-online, 28.09.2023;

3. Zum strafprozessualen Eingriff

a) Der Gesetzesentwurf sieht keine wesentlichen Änderungen an den strafprozessualen Eingriffsbefugnissen vor. Lediglich die Funkzellenabfrage soll ausgeweitet werden, indem die Anbindung an den Straftatenkatalog sowie an die erhöhten Eingriffsvoraussetzungen des § 100g Abs. 2 StPO gelöst werden, so dass zugleich diejenigen Vorgaben entfallen, die Grundrechte des Einzelnen sichern, nämlich das partielle Verwertungsverbot, die Verwendungsbeschränkungen, die besonderen Kennzeichnungspflichten sowie die Sicherung des Kernbereichs der persönlichen Lebensgestaltung (§§ 100g Abs. 2 und 4, 101a Abs. 2, 4 und 5 StPO).

Dies ermöglicht die Auswertung der Daten mittels automatischer Analysen zur Erstellung von Nutzerprofilen über einen längeren Zeitraum, ohne dass dafür ein konkretes strafprozessuales Bedürfnis erkannt werden kann. Wenn in der Praxis jedes technische Gerät, das in einer Funkzelle eingewählt ist, bereits als „Spur" für Ermittlungsbehörden angelegt werden kann, könnten umfassende Verdachtsbilder zu unmittelbaren Tatverdächtigen wie auch zu Unbeteiligten entstehen.

b) Die Absenkung von Kontrollen und Rechtsgarantien für den einzelnen Bürger ist abzulehnen, weil sie der Rechtsprechung des EuGH widerspricht (vgl. bereits oben I.3.h), I.4.c)).

4. Zur telekommunikationsrechtlichen Speicherpflicht

Der Gesetzentwurf zielt im Kern auf eine telekommunikationsrechtliche Einführung der anlassunabhängigen, unterschiedslosen Speicherpflicht für IP-Daten, Benutzer- und Anschlusskennungen sowie Portdaten auf die Dauer von einem Monat vor. Zwar ist anzuerkennen, dass einige Unternehmen, die Telekommunikationsdienstleistungen in Deutschland erbringen, ohnehin für wenige Tage zu technischen Zwecken auf vertraglicher Basis IP-Adressen speichern, aber auch eine 30tägige Speicherpflicht bedeutet für diese eine besondere Belastung.

Der EuGH hat zwar die Speicherung von IP-Daten dem Grunde nach zugelassen, zugleich aber Grenzen gesetzt. So entspricht die schematische Frist von „*einem Monat*" nicht der Anforderung des EuGH, die Speicherung „*für einen auf das absolut Notwendige begrenzten Zeitraum*" zuzulassen. Der EuGH will zudem nur erlauben, dass die Ermittlung von Internetzugängen (IP-Adressen) und den Namen des Nutzers, der die IP-Adresse verwendet, ermöglicht werden soll.[29] Außerdem darf nicht übersehen werden, dass die Speicherung auch von Portnummern für die Persönlichkeitsrechte der Nutzer eine höhere Belastung bedeuten, ebenso auch eine technische und finanzielle Belastung für die Unternehmen, die dann massiv erhöhte Datenmengen zu speichern haben.

Zusammenfassend führt der EuGH in seinem Urteil aus:[30] *„Aus der Rechtsprechung des Gerichtshofs ergibt sich, dass der Zugang zu personenbezogenen Daten nur dann mit dem in Art. 15 Abs. 1 der Richtlinie 2002/58 aufgestellten Erfordernis der Verhältnismäßigkeit vereinbar sein kann, wenn die Rechtsvorschriften, die ihn gestatten, klare und präzise Regeln enthalten, die vorsehen, dass die für den Zugang geltenden materiellen und prozeduralen Voraussetzungen eingehalten werden und dass die Betroffenen über wirksame Garantien zum Schutz vor den Gefahren eines missbräuchlichen oder unberechtigten Zugangs zu den Daten und ihrer missbräuchlichen oder unberechtigten Nutzung verfügen".*

[29] EuGH, Urteil vom 30.04.2024 – Rz. 133; EuGH Urteil vom 06.10.2020, Rn. 157 und 158.

[30] EuGH, Urteil vom 30.04.2024 – Rz. 152; EuGH, Urteil vom 06.10.2020, Rn. 132 und 173; EuGH Urteil vom 02.03.2021, Prokuratuur [Voraussetzungen für den Zugang zu Daten über die elektronische Kommunikation], C 746/18, Rn. 49 und die dort angeführte Rechtsprechung

Zur Speicherpflicht von IP-Daten hat der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) in einer Sachverständigenanhörung des Deutschen Bundestags (Stellungnahme vom 16.10.2023)[31] zur Problematik einer Speicherung von IP-Adressen u.a. zutreffend auf folgendes hingewiesen:

> „… . Dabei sollte evaluiert werden, inwiefern hier eine ausreichend zuverlässige Zuordnung überhaupt möglich ist, etwa durch Ungenauigkeiten bei Zeitangaben und inwiefern die erforderliche umfangreiche Speicherung bei dynamischer Zuweisung der Ports zu einer deutlichen Erhöhung der Eingriffsintensität führen kann, etwa, weil charakteristische Verhaltensweisen von Websites Rückschlüsse auf die Internetnutzung ermöglichen könnten. Auch wenn der Europäische Gerichtshof der Speicherung von IP-Adressen keinen endgültigen Riegel vorgeschoben hat, stellt sich die grundsätzliche Frage, wie nützlich dieses Instrument überhaupt ist. Denn gerade diese Nützlichkeit ist abzuwägen mit dem erheblichen Grundrechtseingriff, der mit einer Speicherung einhergeht. Dies gilt insbesondere vor dem Hintergrund möglicher Umgehungsmöglichkeiten durch Täter und Tätergruppierungen in Form der Nutzung von VPN oder bestimmter Browser, die die IP-Adresse verschleiern und damit wiederum eine anonyme Nutzung des Internets ermöglichen, und so eine Vorratsdatenspeicherung von IP-Adressen konterkarieren.
>
> Die professionell organisierten Täterstrukturen können auch durch die Speicherung der IP-Adresse nicht ermittelt werden. Es ist vorauszusehen, dass gerade durch die Einführung eines neuen Gesetzes derartige Gruppierungen der organisierten Kriminalität sich weiterhin dem Zugriff staatlicher Strafverfolgungsbehörden entziehen können und werden. … Vor neuen gesetzgeberischen Aktivitäten im Bereich einer Vorratsdatenspeicherung von IP-Adressen sollte eine umfassende, unabhängige Evaluation bzw. die von dem BVerfG auch geforderte „Überwachungsgesamtrechnung“ vorgenommen werden. Wer zu weitgehend, zu pauschal oder "ins Blaue hinein" neue Speicherbefugnisse fordert, ist weiterhin dem Risiko ausgesetzt, unverhältnismäßig zu handeln. …“

Tatsächlich fehlt es bisher an einer solchen gesamthaften und ausgewogenen Bewertung von Eingriffen und grundrechtssichernden Maßnahmen.[32] Einer anlassunabhängigen Speicherpflicht steht jedenfalls entgegen, dass dem Einzelnen dadurch eine erhebliche Belastung durch staatliche Überwachung zugemutet wird, die nicht am rechtsstaatlichen Verhältnismäßigkeitsgrundsatz ausgerichtet ist. Solange kein Ausgleich durch neu zu schaffende Freiräume, erweiterte Transparenz und effektiven Rechtschutz vorgesehen ist, kann dem Gesetzentwurf nicht zugestimmt werden.

III.

Ergänzend zu der Beurteilung der beiden Gesetzesvorhaben fehlt es einer überzeugenden Abwägung der Verhältnismäßigkeit der vorgesehenen Eingriffe gegenüber den Grundrechten und Verfahrensrechten, insbesondere von Beschuldigten, Opfern und unbescholtenen Dritten, sowie den Rechten zeugnisverweigerungsberechtigter Personen, insbesondere von Rechtsanwälten und Verteidigern.

---

[31] https://www.bfdi.bund.de/SharedDocs/Downloads/DE/DokumenteBfDI/Stellungnahmen/2023/StgN_IP-Adressen-Rechtsausschuss.pdf

[32] Ebenso auch Roßnagel, ZD 2022, 650, 655.

1. Beschuldigte dürfen nicht zum Objekt der Strafverfolgung werden

Beschuldigte sind keine Gegenstände oder Objekte der Strafverfolgung, sondern Subjekte eines rechtsstaatlich geordneten Verfahrens. Die strafprozessualen Eingriffsbefugnisse zur Erhebung und Bevorratung von Verbindungs-, Standort- und Nutzerdaten sind bereits nach geltendem Recht empfindliche Eingriffe in die oben (I.2.) genannten Grundrechte ein, die nur aufgrund bestimmter, einzelfallbezogener Tatbestandsvoraussetzungen gerechtfertigt sein können. Durch die Abfrage der Verbindungs-, Standort- und Nutzerdaten werden Grundrechte der Familienangehörigen, der Opfer und des sozialen Lebensumfelds erfasst, deren Verhalten analysiert und Verdachtshypothesen zugeführt werden kann. Eine umfassende Bevorratung von Daten kann erheblich in den Schutz von Rechten von Kindern, Jugendlichen und Heranwachsenden eingreifen, die bei Rückgriff auf derart umfassend gespeicherte Daten durch IT-Routinen unberechtigterweise erheblich stigmatisiert werden können. Wie gezeigt erfolgt auch bei dem im RefE skizzierten Quick-Freeze-Modell keine die Eingriffsintensität hinreichend begrenzende qualitative wie quantitative Beschränkung des Speicherumfangs und der Speicherdauer.

Auch deren Vertrauensverhältnisse zu zeugnisverweigerungsberechtigen Personen, d.h. Geistlichen, Ärzten, Verteidigern und Rechtsanwälten, Journalisten und Abgeordneten, sind zu schützen. Der Schutz der Grundrechte, die Privatheit der persönlichen Lebensumgebung ist bei jeglicher Variante einer Vorratsdatenspeicherung durch unabhängig von staatlichen Strafverfolgungs- und Sicherheitsorganen eingerichtete Stellen zu gewährleisten, insbesondere wenn die abgefragten Daten zur Erstellung von Persönlichkeits- und Bewegungsprofilen verwendet werden können oder auch nur ein Kontakt zu einem Vertrauensträger offenbart wird.

Zu beachten ist in diesem Zusammenhang, dass in Umsetzung der zitierten Rechtsprechung zur Begrenzung der Eingriffsintensität bzw. zum Schutz. des dem Menschenwürdegebots unterliegenden absoluten Kernbereichs privater Lebensgestaltung eine Aussonderung solcher Daten erforderlich ist, die diesem Kernbereich unterfallen. Dazu zählen auch Kontakte zu bzw. Korrespondenzen mit den genannten Vertrauenspersonen - insbesondere zu Rechtsanwälten. Eine solche Aussonderung wird indes praktisch kaum ohne deren vorherige Offenbarung und mithin nicht ohne Beeinträchtigung des allgemeinen Persönlichkeitsrechts bzw. nicht ohne Verletzung des absoluten Kernbereichs – mithin der Menschenwürde - möglich sein.

2. Schutzlücke bei Zeugnisverweigerungsrechten aus beruflichen Gründen

a) Indem für das Quick-Freeze-Modell nach dem RefE der Anwendungsbereich des § 100g Abs. 2 und 4, sowie die Anwendung der bislang bestehenden Schutzvorschriften gem. § 100e Abs. 6 sowie § 101a Abs. 4 und 5 StPO entfallen sollen, würde auf eine objektive Grundrechtskontrolle verzichtet, die aus rechtstaatlichen Gründen erforderlich ist, um die Gefahr einer beliebigen Ausnutzung der Daten, mithin auch der Daten von zeugnisverweigerungsberechtigten Personen zu verhindern.

b) In Bezug auf Zeugnisverweigerungsrechte aus beruflichen Gründen (§ 53 StPO) verweist der RefE des BMJ (S. 27, 28) ausdrücklich auf einen Schutz gem. § 160a StPO. Der RefE geht davon aus, dass damit ausreichend dem Schutz der sozialen, medizinischen, rechtlichen, kirchlichen, journalistischen und politischen Bezüge von Beschuldigten Rechnung getragen werde, ebenso wie dem Schutz der Verfahrensrechte der Zeugnisverweigerungsberechtigten. Das sich im Quick-Freeze-Modell ein Eingriff deutlich weitergehend auch auf Betroffene und deren Kommunikation mit den Zeugnisverweigerungsberechtigten bezieht, die durch § 160a StPO nicht umfassend geschützt ist, wird dabei ausgeblendet. Mithin fehlt es an ausreichenden Abwägungen der Verhältnismäßigkeit einer

Beschränkung der Grundrechte durch die staatliche Wahrheitsermittlungspflicht.[33] Dies wird der Rechtsprechung des EuGH und des BVerfG zur Verhältnismäßigkeit staatlich vorgesehener Grundrechtseingriffe und zu den rechtsstaatlichen Anforderungen an die Eingriffstiefe nicht gerecht. Im Mindesten sollte in § 100 g Abs. 4 StPO ein Anwendungsverweis auch auf Fälle der Sicherungsanordnung gemäß § 100 g Abs. 6 StPO erfolgen. Entsprechend sollte in den § 100e Abs. 6 sowie § 101a Abs. 4 und 5 StPO verfahren werden.

c) Vom Entwurf nicht länger vorgesehen ist die ursprünglich von den Koalitionsparteien vereinbarte und in der Vorgängerversion des Entwurfs noch enthaltene Streichung der gegenwärtig in §§ 175 – 181 TKG enthaltenen Regelungen zur Vorratsdatenspeicherung. Diese werden nach der Entwurfsbegründung aufgrund der hierzu ergangenen Rechtsprechung des EuGH und des BVerwG für nicht anwendbar erachtet („totes Recht“). Die Beibehaltung der klar europa- und verfassungsrechtswidrigen Regelungen zur Vorratsdatenspeicherung in § 176 TKG ist indes (neben den immanenten inhaltlichen Vorbehalten) aus Gründen der Bestimmtheit und Rechtsklarheit abzulehnen.

Im Vergleich zur vorigen Entwurfsversion zu begrüßen sind die nun in § 174a Abs. 3 S. 1 TKG-E für das Quick-Freeze-Modell grundsätzlich vorgesehenen Sicherungsmechanismen. Deren Tauglichkeit kann allerdings erst nach erfolgter Ausgestaltung abschließend bewertet werden. In ihrer jetzigen Form sind sie nicht hinreichend bestimmt, um einen angemessenen Grundrechtsschutz sicher zu gewährleisten.

Die BRAK hatte in ihrer Stellungnahme 52/2022 zur vorigen Entwurfsversion Absicherungen zum Schutz vor Offenbarungen von Mandatskontakten angemahnt. Solche sind weiterhin dringend erforderlich und nicht in ausreichendem Maß vorhanden. Insoweit wird zwar in der Entwurfsbegründung des RefE des BMJ darauf verwiesen, dass § 160a StPO einen hinreichenden Schutz gewährleiste. Das ist aber nur bedingt der Fall. Die in § 174a Abs. 3 S. 1 TKG-E vorgesehenen technisch-organisatorischen Maßnahmen gegen unbefugte Kenntnisnahmen der gespeicherten Daten sind unbestimmt und nicht geeignet, den fehlenden Schutz zu kompensieren. Insbesondere wird darin kein schonender grundrechtsschonender Aussonderungsmechanismus beschrieben. Ein solcher erscheint auch schwerlich möglich, da jede Aussonderung zunächst die Erkennung und damit einen gewissen Grad an Offenbarung voraussetzt. Daher muss die Einführung eines Quick-Freeze-Modells (und erst recht die einer anlasslosen IP-Vorratsspeicherung) unterbleiben, Im Mindesten sollten aber konkrete Vorgaben für ein möglichst schonendes Aussonderungsverfahren gemacht werden. Denkbar – wenn auch nicht ausreichend – wären u. a. die Aufnahme von auszusondernden Telekommunikationsdaten in eine Liste analog zu § 174 II TKG-E i.V.m. § 11 V und VI TDDSG (dann mit einer Erstreckung auf § 203 Abs. 1 Nr. 3 StPO) sowie ein frühzeitiger automatisierte Abgleich mit dem BRAV. Die BRAK erneuert an dieser Stelle ihr Gesprächsangebot zu diesem Thema.

- - -

[33] BVerfG, Urt. v. 02.03.2010 – 1 BvR 256/08, Rz. 238; BVerfG, Beschl. v. 12.10.2011 – 2 BvR 236/08, Rz. 268.