Generalstaatsanwaltschaft Frankfurt am Main
-Zentralstelle zur Bekämpfung der Internetkriminalität (ZIT)-

Oberstaatsanwalt Dr. Benjamin Krause

HESSEN

Stellungnahme zur öffentlichen Anhörung im Rechtsausschuss des Bundestages zum Antrag der Fraktion der CDU/CSU IP-Adressen rechtssicher speichern und Kinder vor sexuellem Missbrauch schützen (BT-Drs. 20/3687)

Frankfurt am Main, 9. Oktober 2023

I. Vorbemerkung

Die Zentralstelle zur Bekämpfung der Internetkriminalität (ZIT) der Generalstaatsanwaltschaft Frankfurt am Main ist im Jahr 2010 eingerichtet worden und hat die Aufgabe, durch die Führung herausgehobener Ermittlungsverfahren und die Weitergabe der gesammelten Erfahrungen im Wege der Aus- und Fortbildung bzw. Unterstützung anderer Dienststellen die Strafverfolgung von Internetkriminalität fortzuentwickeln. Dazu bearbeitet die ZIT sog. „Pilotverfahren, in denen erstmals neue technische Ermittlungsmaßnahmen angewendet werden oder rechtliche Fragestellungen auftreten, sowie „Massenverfahren“ gegen eine Vielzahl von unbekannten Tatverdächtigen bundesweit.

Neben den Kriminalitätsbereichen „Cybercrime und Underground Economy“, „Drogen- und Waffenhandel im Darknet“ sowie „Hate Speech in sozialen Netzwerken“ konzentriert sich die ZIT seit ihrer Einrichtung auf die Verfolgung und Bekämpfung der massenhaften Verbreitung von kinder- und jugendpornografischen Inhalten über E-Mail, Messenger und soziale Netzwerke sowie Plattformen im Internet oder Darknet. Ein wesentlicher Bestandteil ist dabei auch die Identifizierung von Tauschpartnern identifizierter Straftäter sowie die Erkennung und Aufklärung des mit der Verbreitung entsprechenden Bild- und Videomaterials verbundenen sexuellen Missbrauchs unbekannter Kinder und Jugendlicher. Erster polizeilicher Ansprechpartner der ZIT für die Bearbeitung entsprechender Verfahren ist das Bundeskriminalamt mit Sitz in Wiesbaden.

II. Stellungnahme

Mit dieser Stellungnahme möchte ich meine praktischen Erfahrungen als langjähriger Staatsanwalt der ZIT in die Diskussion einbringen. Dazu habe ich kürzlich einen Beitrag in der Zeitschrift für Rechtspolitik (ZRP) mit dem Titel „Vorratsdatenspeicherung oder ‚Quick Freeze‘?“ veröffentlicht und darin häufig gestellte Fragen beantwortet – quasi die FAQ.[1] Darauf aufbauend möchte ich auch im Rahmen dieser Stellungnahme typische Fragen aufwerfen und diese aus Sicht eines Staatsanwalts für Internetkriminalität beantworten.

Voranstellen möchte ich jedoch, dass ich mich ausdrücklich dafür ausspreche, den gesetzgeberischen Spielraum zu nutzen, den die Rechtsprechung des *EuGH*, des *BVerfG* und des *BVerwG* einräumt. Ich bin der Auffassung, dass die Einführung einer *EuGH*-konformen Speicherung von IP-Adressen die strafrechtlichen Ermittlungen zur Verfolgung von Kinderpornografie und sexuellen Kindesmissbrauch wesentlich vereinfachen und effektivieren würden – dies gilt im Übrigen auch für die Verfolgung von Darknet-Kriminalität. Denn IP-Adressen sind der werthaltigste Ermittlungsansatz zur Identifizierung unbekannter Tatverdächtiger von Internetkriminalität.

[1] *Krause* ZRP 2023, 169 ff.

- **Wie ist die Rechtslage?**

Der *EuGH*[2] hat auf Vorlagefrage des *BVerwG* entschieden, dass die deutschen Regelungen zur Vorratsdatenspeicherung nicht mit geltendem EU-Recht vereinbar sind. Die bislang vorgesehene – aber ausgesetzte[3] – anlasslose Speicherung von Verkehrs- und Standortdaten ist allein zum Schutz der nationalen Sicherheit vor einer aktuell oder vorhersehbar einzustufenden ernsten Bedrohung zulässig. Dagegen ist für die Verfolgung von schwerer Kriminalität nur eine gezielte Vorratsdatenspeicherung anhand von objektiven oder geografischen Kriterien, eine Vorratsspeicherung von IP-Adressen oder eine behördliche Anordnung zur Speicherung vorhandener und künftiger Daten bei einem konkreten Verdacht („Quick Freeze“) möglich. Zur Verfolgung übriger „nichtschwerer“ Kriminalität hat der *EuGH* auch eine Speicherung der Identitätsdaten bzw. Personendaten der Nutzer zugelassen.

Seitdem wird rechtspolitisch[4] und wissenschaftlich[5] gestritten, ob von einer anlasslosen Speicherung ganz abgesehen und lediglich die Möglichkeit einer anlassbezogenen Sicherungsanordnung („Quick Freeze“) geschaffen werden soll oder ob zusätzlich eine anlasslose Speicherung von IP-Adressen notwendig ist.

Zuletzt hat das *BVerwG* die deutschen Regelungen zur Vorratsdatenspeicherung für unionsrechtswidrig erklärt, ohne jedoch weitergehende Anforderungen an eine unionsrechtskonforme Speicherung von IP-Adressen aufzustellen.[6]

---

[2] *EuGH* NJW 2022, 3135; vgl. dazu etwa *Beuckelmann/Heim* NJW-Spezial 2022, 664.
[3] Vgl. dazu etwa BeckOK StPO/*Bär*, 47. Ed., § 100g Rn. 66.
[4] Vgl. etwa *beck-aktuell* Buschmann legt Alternative zur Vorratsdatenspeicherung vor, becklink 2025120; *beck-aktuell* Faeser und Münch für verpflichtende Speicherung von IP-Adressen, becklink 2025386; *beck-aktuell* JuMiKo – Beschlüsse der Herbstkonferenz 2022, becklink 2025309; *Biesenbach/Strasser* DRiZ 2022, 302.
[5] Gegen eine Speicherung von IP-Adressen etwa *Roßnagel* ZD 2022, 650, 654; für eine Speicherung von IP-Adressen etwa *Benamor* VerfBlog, 2022/11/07, https://verfassungsblog.de/staatliche-schutzpflichten-im-kontext-der-vorratsdatenspeicherung/; *Fischer* FAZ-Einspruch vom 28.10.2022, https://www.faz.net/-irf-aytyi; *Gärditz* GSZ 2022, 292, 294; vgl. auch ZD-Aktuell 2023, 01264 zur Position des BfDI.
[6] *BVerwG* Urt. v. 14.08.2023 – 6 C 6.22, 6 C 7.22, https://www.bverwg.de/de/pm/2023/66. Die Entscheidungsgründe waren zum Zeitpunkt der Abgabe der Stellungnahme noch nicht veröffentlicht.

- **Was sind IP-Adressen?**

Vereinfacht gesagt ist die IP-Adresse die „Telefonnummer eines Computers.[7]“

IP-Adressen werden von den Internetzugangsanbietern den an das Internet angebundenen Geräten ihrer Kunden zugewiesen. Bei dem Aufrufen von Webseiten, dem Download einer Datei oder dem Einloggen in ein E-Mail-Postfach wird jeweils diese IP-Adresse übertragen, um einen Datenaustausch mit diesem Gerät zu ermöglichen. Während eine statische IP-Adresse einem bestimmten Anschlussinhaber dauerhaft fest zugewiesen wird, wird im Fall der dynamischen Adressierung dem Anschlussinhaber bei jeder neuen Aufnahme der Netzwerkverbindung eine IP-Adresse neu zugewiesen.[8]

Die „Telefonnummer des Computers“ ändert sich also ständig.

- **Warum ist die Speicherung von IP-Adressen für die Strafverfolgung notwendig?**

Bei im Internet begangenen Straftaten kann die IP-Adresse der zur Tatbegehung genutzten Internetverbindung der einzige vorliegende Ermittlungsansatz zur Identifizierung des unbekannten Täters sein. In diesen Fällen ist eine Aufklärung nur möglich, wenn über die IP-Adresse der Tatverdächtige identifiziert werden kann – das hat auch der *EuGH* ausdrücklich festgehalten.[9]

Aber auch wenn weitere Ermittlungsansätze zur Identifizierung eines unbekannten Cyber-Kriminellen vorliegen, ist die Zuordnung der zur Tatbegehung verwendeten oder ermittelten IP-Adressen zu den Anschlussinhabern mittels Bestandsdatenanfragen bei den Internetzugangsdiensten der effektivste Ermittlungsansatz.

---

[7] *BVerfG* NJW 2020, 2699, 2700.
[8] MüKoStPO/*Rückert*, StPO, 2. Aufl., § 100a Rn. 82.
[9] *EuGH* NJW 2022, 3135 Rn. 100 m.w.N.

Dies beruht darauf, dass E-Mail-Adressen, Kennungen bei Messenger-Diensten oder Profile in sozialen Netzwerken kostenlos und ohne Identitätskontrolle durch die Verwendung frei erfundener Personalien registriert werden können.[10] Diese durch die Strafverfolgungsbehörden abrufbaren Personendaten sind daher oftmals nicht werthaltig.[11] Die Internetzugangsdienste erheben dagegen verifizierte Personalien ihrer Kunden, um die Bezahlung der Dienstleitung sicherzustellen und Ansprüche notfalls gerichtlich durchzusetzen. Die Personendaten bei Internetzugangsdiensten sind für die Strafverfolgungsbehörden daher wesentlich werthaltiger zum Zwecke der Identifizierung unbekannter Tatverdächtiger.[12]

Diese Feststellung wird auch von einer kürzlich veröffentlichten Auswertung des Bundeskriminalamts (BKA) zur Bearbeitung von Hinweisen des U.S.-amerikanischen NCMEC[13] gestützt.[14] Danach sind Bestandsdatenabfragen zu IP-Adressen der effektivste Ermittlungsansatz zur Identifizierung unbekannter Nutzer von kinder- oder jugendpornografischem Material.[15]

Vor diesem Hintergrund hatte das FDP-geführte Bundesjustizministerium bereits im Jahr 2011 in einem Referentenentwurf zur Ermöglichung von „Quick Freeze“ eine begrenzte anlasslose Speicherung von IP-Adressen für sieben Tage als zwingend notwendig erachtet, um Bestandsdatenauskünfte zum Zwecke der Identifizierung unbekannter Internetnutzer zu ermöglichen.[16]

---

[10] Eine Pflicht zur Erhebung solcher Daten besteht gemäß nach § 172 Abs. 1 TKG für nummerngebundene interpersonelle Telekommunikationsdiente wie Telefon- oder Internetzugangsanbieter, wobei gemäß § 172 Abs. 2 TKG nur bei Prepaid-Mobilfunkverträgen die Daten zu verifizieren sind. Für nummernunabhängige Telekommunikationsdiente wie E-Mail- oder Messengerdienste besteht keine Speicherpflicht, sondern lediglich ein „Löschverbot“ nach § 172 Abs. 3 TKG. Für Telemediendienste wie Soziale Netzwerke, Foren oder Blogs besteht überhaupt keine Speicherpflicht, § 22 TTDSG.

[11] „Bestandsdaten“ gemäß § 100j Abs. 1 StPO in Verbindung mit §§ 172 Abs. 3, 174 Abs. 1 Satz 1, Abs. 3 TKG bzw. § 22 Abs. 1, 3 TTDSG.

[12] „Bestandsdaten“ gemäß § 100j Abs. 2, 5 StPO und §§ 172, 174 Abs. 1 Satz 3, Abs. 5 TKG.

[13] Vgl. zu dem „National Center for Missing and Exploited Children (NCMEC)“ etwa *Rörig* ZRP 2020, 228, 231.

[14] *Bundeskriminalamt* Positionspapier zu erforderlichen Speicherfristen von IP-Adressen, Stand: 21.07.2023, https://t1p.de/hcmun.

[15] Die Erfolgsquote von 75% in 1.000 händisch recherchierten Vorgängen beruht zu 41% auf der Zuordnung von IP-Adressen, zu 28% auf der Zuordnung von Telefonnummern und zu 6% auf der Zuordnung von E-Mail-Adressen.

[16] *Bundesministerium der Justiz* Diskussionsentwurf eines Gesetzes zur Sicherung vorhandener Verkehrsdaten und Gewährleistung von Bestandsdatenauskünften im Internet, https://t1p.de/vryh9; vgl. dazu *Arning/Moos* ZD 2012, 153 ff.

Aus Sicht der Strafverfolgungspraxis wäre eine Frist von sieben Tagen jedoch sehr knapp, da nicht jeder Fall wie im NCMEC-Prozess tagesaktuell den Strafverfolgungsbehörden gemeldet werden kann. Mit einer Speicherfrist von einem Monat könnten die Strafverfolgungsbehörden aber wohl leben.

- **Gilt die Notwendigkeit auch für die Verfolgung von Darknet-Kriminalität?**

Entgegen vereinzelter Äußerungen[17] wäre eine anlasslose Speicherung von IP-Adressen auch geeignet, die Strafverfolgung im Darknet zu verbessern.[18]

Auch wenn die Internetverbindungen im Darknet unter Nutzung etwa des TOR-Browsers mehrfach verschlüsselt sind und keine sog. „Klar-IP-Adressen" übertragen werden, ist die Zuordnung von IP-Adressen zu Anschlussinhabern ein wichtiger Ermittlungsansatz. In dem Ermittlungsverfahren der ZIT gegen die Betreiber der kinderpornografischen Darknet-Plattformen „Elysium[19]" und „BoysTown[20]" sind Betreiber nur deswegen identifiziert und verurteilt worden, weil die IP-Adresse, mit der er sich auf einen Server der Tätergruppierung angemeldet hatte, im Rahmen einer Server-Überwachung festgestellt und bei dem Internetdienstanbieter einem Anschlussinhaber zugeordnet werden konnte. Bei der Nutzung anderer Internetdienstanbieter seitens der Beschuldigten wäre eine Identifizierung mangels Speicherung nicht möglich gewesen. Die Identifizierung ist insofern von der Zufälligkeit abhängig, welchen Internetdienstanbieter die Täter verwenden. Dies ist insbesondere vor dem Hintergrund problematisch, dass jeweils bei einzelnen identifizierten Betreibern der Darknet-Plattformen „Elysium" und „BoysTown" auch schwerer sexueller Missbrauch von Kindern aufgeklärt werden konnte. Vergleichbare Identifizierungserfolge sind auch in anderen Ermittlungsverfahren der ZIT gegen Betreiber krimineller Darknet-Plattformen erzielt worden.[21]

---

[17] Vgl. etwa Bundesjustizminister *Buschmann* (FDP), https://www.tagesschau.de/inland/interview-ta-gesschau24-buschmann-101.html.
[18] Vgl. dazu etwa *Krause* NJW 2018, 678.
[19] *LG Limburg* BeckRS 2019, 34315; *BGH* BeckRS 2020, 8432.
[20] *LG Frankfurt am Main* becklink 2025585.
[21] Vgl. etwa *LG Karlsruhe* BeckRS 2018, 40013 („Deutschland im Deep Web"); *BGH* NStZ 2023, 503 („Wall Street Market").

- **Ist nicht bereits in über 90% aller Fälle eine Aufklärung über die IP-Adresse möglich?**

In diesem Zusammenhang wird häufig auf eine Mitteilung der Bundesregierung im Januar 2022 abgestellt, wonach in den Jahren 2017 bis 2021 von über 300.000 Hinweisen des U.S.-amerikanischen NCMEC[22] zu Kinderpornographie im Internet etwa 19.000 Fälle nicht aufgeklärt werden konnten, weil die IP-Adresse mangels Speicherung nicht mehr abfragbar war.[23] Der Umkehrschluss, dass in über 90% aller Fälle eine Aufklärung über die IP-Adresse möglich war, ist zwar naheliegend[24] – aber nicht zutreffend.

Denn diese Statistik bezieht sich einerseits ausschließlich auf nicht abfragbare IP-Adressen und nicht etwa auch auf Fälle, in denen eine IP-Adresse erfolglos abgefragt worden ist. Andererseits sind in der Statistik nur solche Fälle erfasst worden, in denen als einziger Identifizierungsansatz ausschließlich diese eine IP-Adresse vorlag und nicht etwa weitere Ermittlungsansätze wie E-Mail-Adressen, bei denen eine Abklärung der IP-Adressen ebenfalls zur Aufklärung hätte führen können. Das BKA hat vielmehr klargestellt, dass in dem genannten NCMEC-Prozess trotz tagesaktueller Abfrage der mitgeteilten IP-Adressen nur 41% einem Nutzeranschluss zugeordnet werden konnten.[25] Durch weitere und wesentlich aufwändigere Ermittlungen wie etwa im Hinblick auf ebenfalls mitgeteilte E-Mail-Adressen oder Mobilrufnummern erreichte das BKA zwar eine Erfolgsquote von insgesamt etwa 75% – die übrigen 25% der Meldungen müssen mangels Ermittlungsansätzen durch die Staatsanwältinnen und Staatsanwälte der ZIT eingestellt werden.

Eine Aufklärungsrate von über 90% wäre in dem NCMEC-Prozess jedoch erreichbar, wenn es eine einmonatige Speicherpflicht für IP-Adressen gäbe.[26]

---

[22] Siehe oben Fußnote 13.
[23] BT-Drs. 20/534, S. 27 f.
[24] So etwa *Roßnagel* ZD 2022, 650, 654.
[25] *Bundeskriminalamt* Positionspapier zu erforderlichen Speicherfristen von IP-Adressen, Stand: 21.07.2023, https://t1p.de/hcmun: Etwa 34% der angelieferten IP-Adressen waren beim Internetdienstanbieter nicht mehr gespeichert und weitere 24% nicht beauskunftbar.
[26] *Bundeskriminalamt* Positionspapier zu erforderlichen Speicherfristen von IP-Adressen, Stand: 21.07.2023, https://t1p.de/hcmun.

- **Besagen nicht Studien, dass die Vorratsdatenspeicherung wirkungslos ist?**

Im Juli 2011 haben Wissenschaftler des Max-Planck-Instituts für ausländisches und internationales Strafrecht die Studie „Schutzlücken durch Wegfall der Vorratsdatenspeicherung?“ im Auftrag des Bundesjustizministeriums veröffentlicht. Die Wissenschaftler kamen zu der Erkenntnis, dass der Wegfall der Vorratsdatenspeicherung im Jahre 2010 nicht als Ursache für Veränderungen bei der Aufklärungsquote gelten könne.[27] Dies habe die Untersuchung von Aufklärungsquoten für den Zeitraum 1987 bis 2010 in Deutschland sowie der Vergleich von Aufklärungsquoten im Ausland gezeigt. Dieses Ergebnis wurde zwar vielfach dahingehend kommentiert, dass die Vorratsdatenspeicherung wirkungslos sei und keinen Nutzen für die Strafverfolgung habe.[28] Bereits zuvor hatten im Jahr 2007 der Arbeitskreis Vorratsdatenspeicherung, das Netzwerk Neue Medien e.V. und die Neue Richtervereinigung e.V. in einer Stellungnahme festgestellt, dass die Erhöhung der Aufklärungsquote von Straftaten durch die Vorratsdatenspeicherung gerade einmal 0,006% betrage.[29]

Für die heutige Diskussion um eine Speicherpflicht für IP-Adressen haben diese Studien jedoch nur eine geringe Aussagekraft. Denn untersucht wurden jeweils die Auswirkungen einer umfassenden 6-monatigen Vorratsdatenspeicherung von Telefonie-Verkehrsdaten und IP-Adressen. Die rechtspolitische Diskussion wird heute jedoch nur um die Speicherung von IP-Adressen geführt. Zudem hat sich seit den Jahren 2007 bzw. 2011 das gesellschaftliche Leben und damit einhergehend auch die Kriminalität immer weiter ins Internet verlagert. Während die Straftaten der Polizeilichen Kriminalstatistik (PKS) zwischen 2015 bis 2022 um über 11% zurückgegangen sind, sind „digitale“ Straftaten gegen den allgemeinen Trend stark gestiegen. Beispielsweise ist der Besitz und die Verbreitung kinder- und jugendpornografische Inhalte über das Tatmittel Internet von knapp 6.500 Fällen im Jahr 2015 auf knapp 45.000 Fälle im Jahr 2022 gestiegen.[30]

---

[27] Studie, Schlussfolgerung 2.9, Seite 219.
[28] Vgl. etwa https://www.zeit.de/digital/datenschutz/2012-01/vorratsdatenspeicherung-studie.
[29] *Redaktion beck-aktuell* becklink 1018722.
[30] *Bundeskriminalamt* Polizeiliche Kriminalstatistik (PKS), abrufbar unter www.bka.de.

- **Was beabsichtigt der „Quick Freeze“-Ansatz?**

Ziel von „Quick Freeze“ ist es, eine anlasslose Speicherung von Verkehrsdaten aller Bürgerinnen und Bürger zu verhindern und stattdessen nur eine anlassbezogene Speicherung in Bezug auf tatrelevante Kennungen zu ermöglichen. Dazu sollen mittels einer gerichtlichen Anordnung die bei den Dienstanbietern vorhandenen und künftig anfallenden Verkehrsdaten zu tatrelevanten Festnetz- oder Mobilrufnummern bzw. IP-Adressen „eingefroren“ werden, um eine Löschung zu verhindern. Diese Datenbestände können Strafverfolgungsbehörden bei Vorlage einer erneuten gerichtlichen Anordnung erheben und auswerten.[31]

Ein gerichtlich angeordnetes „Einfrieren“ von Verkehrsdaten wird aber nur dann möglich sein, wenn diese bei dem jeweiligen Dienstanbieter vorhanden sind. Eine Pflicht zur Erhebung und Speicherung besteht aber nicht.[32] Dienstanbieter können auch nicht frei entscheiden, ob und wie lange Verkehrsdaten zu geschäftlichen Zwecken vorgehalten werden. Dies ist zwar insbesondere zur Entgeltabrechnung[33] sowie zur Störungsbeseitigung und zur Missbrauchsbekämpfung[34] möglich. Jedoch sind erhobene Daten unverzüglich zu löschen, sobald sie für die vorgenannten Zwecke nicht mehr erforderlich sind.[35]

- **Wie lange würden Verkehrsdaten „zum Einfrieren“ vorliegen?**

Das unterscheidet sich danach, auf welcher Rechtsgrundlage entsprechende Daten erhoben und gespeichert werden können.

---

[31] *Bundesministerium der Justiz*, Referentenentwurf eines Gesetzes zur Einführung einer Sicherungsanordnung für Verkehrsdaten in der Strafprozessordnung, https://t1p.de/lltr0; vgl. dazu etwa BeckOK StPO/*Bär*, 47. Ed., § 100g Rn. 71a; *Seyda/Zurawski* ZD-Aktuell 2023, 12.
[32] BeckOK StPO/*Bär*, 47. Ed., TTDSG § 9 Rn. 7.
[33] § 9 Abs. 1 Satz 1 TTDSG.
[34] § 12 Abs. 1 und 4 TTDSG.
[35] §§ 9 Abs. 1 Satz 2, 12 Abs. 2 TTDSG.

Für **Abrechnungszwecke** dürfen Verkehrsdaten bis zu sechs Monate nach Versendung der Rechnung gespeichert werden.[36] Bei den mittlerweile im Bereich der Festnetzanschlüsse und der Mobilfunktelefonie zum Regelfall[37] gewordenen Tarifen mit Pauschalvergütung („Flatrate“) besteht aber bereits keine Notwendigkeit für die Dienstanbieter, Telefondaten oder IP-Adressen zu Abrechnungszwecken zu speichern.[38] Dies macht regelmäßig eine Löschung der Verkehrsdaten unmittelbar nach dem Ende der Verbindung erforderlich. Bei anderen Vertragsmodellen oder Prepaid-Produkten werden im Bereich der Telefondienste Verkehrsdaten bis zu drei Monate nach Rechnungsstellung gespeichert.[39] Bei Internetzugangsdiensten werden auch bei volumenbegrenzten Verträgen aus Gründen des Datenschutzes nur Datenvolumen und Nutzerkennung, nicht aber IP-Adressen gespeichert.[40]

Zum Zwecke der **Störungsbeseitigung** werden dagegen Rufnummer oder Kennung der beteiligten Anschlüsse, Beginn und Ende der jeweiligen Verbindung gespeichert – bei mobilen Anschlüssen auch Standortdaten.[41] In diesem Zusammenhang besteht für Internetzugangsdienste die Möglichkeit, die vergebenen IP-Adressen und die Verknüpfungen zu den Benutzerkennungen für einen kurzen Zeitraum von wenigen Tagen zum Zwecke der Erkennung, Eingrenzung und Beseitigung von Störungen zu speichern.[42] Danach sind diese Daten unverzüglich zu löschen. Eine solche unternehmensinterne Speicherung wird von einigen Internetzugangsanbietern wie etwa der Deutschen Telekom bei Festnetzanschlüssen für maximal sieben Tage durchgeführt; andere Anbieter speichern kürzer, nicht alle Verbindungen oder gar nicht. Es ist daher nicht zutreffend, dass die Speicherdauer für IP-Adressen derzeit durchschnittlich sieben Tagen beträgt. Im Bereich des mobilen Internetzugangs, bei dem einzelne IP-Adressen im Format IPv4 mehreren Kunden

---

[36] § 10 Abs. 2 Satz 2 TTDSG.
[37] *Bundesnetzagentur*, Nutzung von OTT-Kommunikationsdiensten in Deutschland, Bericht 2020, https://t1p.de/73elo.
[38] BeckOK StPO/*Bär*, 47. Ed., TTDSG § 9 Rn. 8.
[39] Bundesbeauftragter für Datenschutz und Informationssicherheit, Leitfaden für datenschutzgerechte Speicherung von Verkehrsdaten, Stand: 30.09.2022, https://t1p.de/nopne.
[40] Bundesbeauftragter für Datenschutz und Informationssicherheit, Leitfaden für datenschutzgerechte Speicherung von Verkehrsdaten, Stand: 30.09.2022, https://t1p.de/nopne.
[41] § 12 Abs. 1 und 4 TTDSG.
[42] Vgl. zu § 100 TKG a.F. *BGH* NJW 2014, 2500: 7 Tage; *OLG Köln* BeckRS 2016, 898: 4 Tage.

gleichzeitig zugewiesen und nur über den sog. „Port“ unterschieden werden können,[43] erfolgt derzeit bei keinem Anbieter eine entsprechende Speicherung, da der Speicheraufwand und die Datenmenge aufgrund der Komplexität des Zuweisungsprozesses und der großen Anzahl der pro Nutzer vergebenen Ports zu hoch ist. Die Identifizierung eines konkreten Anschlusses mittels einer Portnummer ist in diesen Fällen nicht möglich.

- **Wäre „Quick Freeze“ eine Alternative für die Strafverfolgungsbehörden?**

Das hängt insbesondere davon ab, ob und wie lange bei den Dienstanbietern Daten zum „Einfrieren“ vorhanden sind, damit „Quick Freeze“ nicht ins Leere läuft.

Im Bereich der **Telefonie** sind Rufnummern regelmäßig einem konkreten Endgerät und einem bekannten Anschlussinhaber zugeordnet. Zudem sind sowohl Verbindungsdaten zu Gesprächen und Nachrichten als auch Standortdaten von Mobiltelefonen bei den Dienstanbietern jedenfalls für einen gewissen Zeitraum vorhanden. Aufgrund dieses verfügbaren Datenbestands kann „Quick Freeze“ eine Alternative zur Vorratsdatenspeicherung sein.

Im Bereich der **Internetnutzung** werden IP-Adressen den Anschlussinhabern ständig dynamisch neu zugewiesen. Für ein „Einfrieren“ von Daten muss daher zunächst der tatrelevante Anschluss der Betroffenen über eine Zuordnung der IP-Adresse zu einem Kunden identifiziert werden. Ist diese Zuordnung jedoch nicht gespeichert, können auch keine Verkehrsdaten zu dem jeweiligen Tatverdächtigen „eingefroren“ werden.[44] „Quick Freeze“ kann daher eine anlasslose Speicherung von IP-Adressen nicht ersetzen.

---

[43] Bei dem „Network-Adress-Port-Translation“-Verfahren (NAPT)“ wird eine IP-Adresse zeitgleich mehreren Geräten zugewiesen und eine Unterscheidung ist nur durch interne Ports möglich; vgl. dazu BeckOK StPO/*Bär*, 47. Ed., § 100g Rn. 11; § 101a Rn. 18; KK-StPO/*Henrichs/Weingast*, 9. Aufl., § 100j Rn. 4.

[44] So auch *European Commission* Study on the retention of electronic communications non-content data for law enforcement purposes, 2020, S. 20, https://t1p.de/ids5n.

Nicht zu unterschätzen ist dabei auch, dass mit „Quick Freeze“ ein völlig neues Speichersystem und Beauskunftungsmodell eingerichtet werden soll, was mit großem Ressourcenaufwand sowohl für die Telekommunikationsunternehmen als auch für die Strafverfolgungsbehörden verbunden wäre. Für die Bestandsdatenabfragen zu IP-Adressen bestehen jedoch bereits praxiserprobte elektronische Schnittstellen und gesicherte Auskunftssysteme zwischen Telekommunikationsunternehmen und Strafverfolgungsbehörden.

- **Wie könnte eine *EuGH*-konforme Speicherung von IP-Adressen ausgestaltet werden?**

Der *EuGH* hat unmissverständlich festgehalten, dass eine anlasslose Speicherung zum Zwecke der Strafverfolgung nur bei schwerer Kriminalität möglich ist.[45] Dies hat der *EuGH* damit begründet, dass in einer anlasslosen Speicherung von IP-Adressen ein schwerer Grundrechtseingriff liegt, weil die IP-Adressen bei Abruf durch die Strafverfolgungsbehörden zur umfassenden Nachverfolgung der von einem Internetnutzer besuchten Internetseiten und seiner Online-Aktivität genutzt werden können und dadurch abschreckende Wirkung für alle Internetnutzer haben.[46]

Vor diesem Hintergrund wäre eine geringfügige Anpassung der §§ 175, 176 TKG als „Speicherregelungen“ erforderlich. Denn auch dort ist bereits geregelt, wie verpflichtete Dienstanbieter Verkehrsdaten zu speichern haben und in welchen Fällen diese Daten wie an die Strafverfolgungsbehörden herauszugeben sind (§ 176 Abs. 1 und Abs. 3 TKG). Diese Regelungen müssten auf Internetzugangsdienstanbieter sowie auf die Speicherung von IP-Adressen begrenzt und hinsichtlich des Speicherzwecks beschränkt werden.

[45] *EuGH* NJW 2022, 3135 Rn. 102.
[46] *EuGH* NJW 2022, 3135 Rn. 79; zuvor bereits *EuGH* EuZW 2021, 209 Rn. 153, 156.

Einen Katalog entsprechender Straftaten der schweren Kriminalität sieht die Strafprozessordnung schon jetzt etwa in § 100g Abs. 2 StPO vor. Die sog. „Abrufregelungen“ zur Vorratsdatenspeicherung in §§ 100g Abs. 2 StPO, 101a Abs. 1 StPO müssten daher nicht zwingend geändert werden, um eine *EuGH*-konforme Speicherung von IP-Adressen zu ermöglichen.

- **Können anlasslos gespeicherte IP-Adressen auch für minderschwere Kriminalität genutzt werden?**

Die anlasslose Speicherung der IP-Adressen hat den Zweck, bei schwerer Kriminalität die gespeicherten IP-Adressen zu einer tatrelevanten Benutzerkennung in Gänze an die Strafverfolgungsbehörden auszuliefern. Durch einen Abruf und eine entsprechende Auswertung nicht nur zukünftiger, sondern gerade auch zurückliegender Verbindungen wird ein „Blick in die Vergangenheit[47]“ möglich. Dieser schwerwiegende Eingriff kann nur für die Strafverfolgung schwerer Kriminalität zulässig sein.

Erforderlich für eine effektive Aufklärung und Verfolgung von Internetkriminalität ist aber regelmäßig nur, dass eine (!) den Strafverfolgungsbehörden bereits bekannte IP-Adresse durch die Internetzugangsanbieter dem jeweiligen Anschlussinhaber zugeordnet werden kann. Bei einer entsprechenden Bestandsdatenanfrage nach § 100j Abs. 2 StPO zu dieser IP-Adresse sind die Internetzugangsdienste gemäß §§ 177 Abs. 1 Nr. 3, 174 Abs. 1 Satz 3 TKG verpflichtet, intern auch auf den anlasslos gespeicherten Gesamtdatenbestand von IP-Adressen zuzugreifen, so den zu der mitgeteilten IP-Adresse verknüpften Abschlussinhaber zu identifizieren und anschließend ausschließlich die entsprechenden Personendaten an die Strafverfolgungsbehörden herauszugeben. Eine solche Auskunft ist nach der Rechtsprechung des *EuGH* nicht als schwerer Eingriff einzustufen, so dass dieser auch mit der Verfolgung minderschwerer Straftaten gerechtfertigt werden kann[48].

---

[47] *Benamor* VerfBlog, 2022/11/07, https://verfassungsblog.de/staatliche-schutzpflichten-im-kontext-der-vorratsdatenspeicherung/; *Priebe* EuZW 2017, 136.

[48] *EuGH* NJW 2022, 3135 Rn. 99

Es muss also zwischen dem Eingriff der anlasslosen Speicherung der Daten und dem Zugriff auf sowie die Verwendung der anlasslos gespeicherten Daten unterschieden werden.

Diese Unterscheidung zwischen Herausgabe aller IP-Adressen und lediglich punktuellem internem Zugriff der Internetzugangsdienste hat auch das *BVerfG* anerkannt und ausdrücklich festgehalten, dass bei einer Zuordnung von IP-Adressen durch anlasslos gespeicherte Verkehrsdaten verfassungsrechtlich nicht die für die unmittelbare Verwendung der Gesamtheit der vorsorglich gespeicherten Verkehrsdaten geltenden besonders strengen Voraussetzungen gegeben sein müssen.[49] Auch bedarf es nach dem *BVerfG* für entsprechende Bestandsdatenabfragen weder einen begrenzenden Rechtsgüter- oder Straftatenkatalog noch einen Richtervorbehalt.[50]

Das Urteil des *EuGH* steht dieser Rechtsprechung des *BVerfG* nicht entgegen, so dass auch § 100j Abs. 2 StPO sowie §§ 174 und 177 TKG bestehen bleiben könnten.

gez. Dr. Krause
Oberstaatsanwalt

[49] *BVerfG* NJW 2020, 2699 Rn. 175.
[50] *BVerfG* NJW 2020, 2699 Rn. 177, 254.