Deutscher Bundestag **Drucksache 20/13366**

20. Wahlperiode 15.10.2024

Gesetzentwurf

der Fraktion der CDU/CSU

Entwurf eines Gesetzes zur Verbesserung der Verbrechensaufklärung – Einführung einer Mindestspeicherung von IP-Adressen und Wiederherstellung der Funkzellenabfragemöglichkeit

A. Problem

Bei Straftaten, die mittels Internet vorbereitet oder begangen werden, stellt die IP-Adresse des Täters häufig den einzigen, immer aber den ersten, effizientesten und schnellsten Ermittlungsansatz für die Strafverfolgungs- und Gefahrenabwehrbehörden dar. Ohne die Zuordnung der IP-Adresse zu einem Anschlussinhaber laufen die Ermittlungen oft ins Leere, wenn keine anderen Spuren vorhanden sind. Um diese Zuordnung sicher zu ermöglichen, bedarf es einer Regelung zur verbindlichen Speicherung von IP-Adressen durch die Internetzugangsanbieter, die die Spielräume nutzt, die der Europäische Gerichtshof (EuGH) in seinem Urteil vom 20. September 2022 – C-793/19 und C-794/19 – für die Verkehrsdatenspeicherung unbestreitbar eröffnet hat.

Darin hat der EuGH entschieden, dass die Vorschriften des deutschen Rechts zur Vorratsdatenspeicherung nicht mit dem Unionsrecht vereinbar sind. Die bislang vorgesehene – aber seit Jahren ausgesetzte – anlasslose Speicherung von Verkehrs- und Standortdaten ist danach nicht für die Verfolgung schwerer Kriminalität, sondern allein zum Schutz der nationalen Sicherheit vor einer aktuell oder vorhersehbar einzustufenden ernsten Bedrohung zulässig. Für die Verfolgung schwerer Kriminalität sowie zur Verhütung schwerer Bedrohungen der öffentlichen Sicherheit sind nach der Rechtsprechung des EuGH nur weniger eingriffsintensive Maßnahmen wie eine gezielte Vorratsdatenspeicherung anhand von objektiven oder geografischen Kriterien, eine behördliche Anordnung zur Speicherung vorhandener und künftiger Daten bei einem konkreten Verdacht („Quick Freeze“) oder eine allgemeine und unterschiedslose Speicherung von IP-Adressen in einem auf das absolut Notwendige begrenzten Zeitraum unionsrechtlich möglich.

Infolge dieses Urteils des EuGH hat das Bundesverfassungsgericht (BVerfG) mit Beschlüssen vom 14. Februar 2023 – 1 BvR 2845/16; 1 BvR 2683/16 – und vom 15. Februar 2023 – 1 BvR 141/16 – zwar mehrere Verfassungsbeschwerden gegen nationale Regelungen der Vorratsdatenspeicherung mangels Rechtsschutzbedürfnis nicht zur Entscheidung angenommen, aber gleichwohl festgestellt, dass die §§ 175, 176 des Telekommunikationsgesetzes (TKG) dem Unionsrecht widersprechen und deshalb innerstaatlich nicht mehr angewendet werden dürfen. Auch das Bundesverwaltungsgericht (BVerwG) hat infolge dieses Urteils des EuGH am 14. August 2023 – 6 C 6.22 und 6 C 7.22 – entschieden, dass die nationalen Regelungen zur Vorratsdatenspeicherung von Verkehrs- und Standortdaten in den §§ 175,

176 TKG unionsrechtswidrig sind und wegen des Anwendungsvorrangs des Unionsrechts nicht angewendet werden dürfen. Die §§ 175, 176 TKG in ihrer derzeitigen unionsrechtswidrigen Fassung sind daher zwingend zu ändern und an die Rechtsprechung des EuGH anzupassen.

Unstreitig kann bei im Internet begangenen Straftaten die IP-Adresse der zur Tatbegehung genutzten Internetverbindung der einzige vorliegende Ermittlungsansatz zur Identifizierung des unbekannten Täters oder Gefährders sein. Dies betrifft – so ausdrücklich auch der EuGH – insbesondere den Erwerb, die Verbreitung, die Weitergabe oder die Bereitstellung von Kinderpornografie im Internet. Ohne Mindestspeicherung von IP-Adressen hängt in diesen Fällen die Aufklärung und Verhütung der Straftat von dem Zufall ab, welchen Internetzugangsdienst der unbekannte Täter genutzt hat und ob dieser Internetzugangsdienst freiwillig die Zuordnung dieser IP-Adresse zu einer Benutzerkennung gespeichert hat.

Mit Urteil des EuGH vom 30. April 2024 – C-470/21 – hat der EuGH sowohl die unionsrechtliche Zulässigkeit als auch die Notwendigkeit und Verhältnismäßigkeit einer Mindestspeicherung von IP-Adressen noch einmal verdeutlicht. Er hat festgestellt, dass nationale Regelungen zur Speicherung von IP-Adressen zur Bekämpfung jeglicher Art von Straftaten unionsrechtlich grundsätzlich zulässig sind. Der EuGH hat damit seine Rechtsprechung zur Vorratsdatenspeicherung fortentwickelt und erachtet die Vorratsspeicherung von IP-Adressen aufgrund deren Bedeutung als oftmals einzigem Ermittlungsansatz für die Verfolgung und Verhinderung von Straftaten nunmehr sogar als zwingend erforderlich, um eine andernfalls drohende Gefahr der systemischen Straflosigkeit von Straftaten, die mithilfe des Internets begangen werden, zu vermeiden.

Der EuGH hat nunmehr in Abkehr von seiner bisherigen Rechtsprechung ausdrücklich festgestellt, dass nicht jede allgemeine und unterschiedslose Speicherung von IP-Adressen zwangsläufig einen schweren Eingriff in Grundrechte darstellt. Der EuGH hat zunächst noch einmal bekräftigt, dass bei online begangenen Straftaten der Zugang zu IP-Adressen die einzige Ermittlungsmaßnahme darstellen kann, die eine effektive Identifizierung der Person ermöglicht, der diese Adresse zugewiesen war, als die Tat begangen wurde (Rn. 117). Er hat aber auch betont, dass ohne eine entsprechende Speicherung eine Gefahr der systemischen Straflosigkeit von Straftaten droht, die online begangen oder vorbereitet werden (Rn. 119). Aber selbst in Fällen, in denen die IP-Adresse nicht die einzige mögliche Maßnahme zur Identifizierung des Tatverdächtigen darstellt, erachtet er eine Speicherung für notwendig. Denn anderenfalls wären umfangreiche Ermittlungen wie Internetrecherchen zu den Online-Aktivitäten der betreffenden Person (sog. OSINT) notwendig, insbesondere zu Aktivitäten in sozialen Netzwerken und zu Kontakten (Rn. 120). Solche Ermittlungsmaßnahmen können jedoch genaue Informationen über das Privatleben der Betroffenen offenbaren und stellen deswegen sogar einen schwereren Eingriff dar als die Speicherung und rein punktuelle Abfrage der IP-Adresse (Rn. 121).

Eine gesetzliche Pflicht zur allgemeinen und unterschiedslosen Speicherung von IP-Adressen sieht der EuGH nunmehr als verhältnismäßig an, wenn durch die Modalitäten der Speicherung ausgeschlossen ist, dass aus den IP-Adressen „genaue Schlüsse auf das Privatleben der Personen“ gezogen werden können (Rn. 83). Um dies sicherzustellen, muss durch klare und präzise Rechtsvorschriften „eine wirksame strikte Trennung der verschiedenen Kategorien auf Vorrat gespeicherter Daten gewährleistet“ sein (Rn. 84 f.). Hierzu formuliert der EuGH selbst vier Vorgaben an diese Gewährleistungsregelungen (Rn. 86 bis 89):

„Erstens müssen die in der vorstehenden Randnummer genannten nationalen Regeln sicherstellen, dass jede Kategorie von Daten, einschließlich der Identitätsda-

ten und der IP-Adressen, völlig getrennt von den übrigen Kategorien auf Vorrat gespeicherter Daten gespeichert wird.

Zweitens müssen diese Regeln gewährleisten, dass in technischer Hinsicht eine wirksame strikte Trennung zwischen den verschiedenen Kategorien auf Vorrat gespeicherter Daten, u. a. den Identitätsdaten, den IP-Adressen, den verschiedenen Verkehrsdaten außer den IP-Adressen und den verschiedenen Standortdaten durch eine abgesicherte und zuverlässige Datenverarbeitungseinrichtung stattfindet.

Drittens dürfen die Regeln, soweit sie die Möglichkeit vorsehen, die auf Vorrat gespeicherten IP-Adressen mit der Identität des Betroffenen zu verknüpfen, unter Beachtung der Anforderungen, die sich aus Art. 15 Absatz 1 der Richtlinie 2002/58 im Licht der Art. 7, 8 und 11 der Charta ergeben, eine solche Verknüpfung nur unter Verwendung eines leistungsfähigen technischen Verfahrens erlauben, das die Wirksamkeit der strikten Trennung dieser Datenkategorien nicht in Frage stellt.

Viertens muss die Zuverlässigkeit dieser strikten Trennung regelmäßig Gegenstand einer Kontrolle durch eine andere Behörde als die sein, die Zugang zu den von den Betreibern elektronischer Kommunikationsdienste auf Vorrat gespeicherten personenbezogenen Daten begehrt."

Werden sie eingehalten, „kann der Eingriff […] schon aufgrund der Struktur ihrer Speicherung nicht als ‚schwer' eingestuft werden" (Rn. 90). Eine Regelung zur Speicherung von IP-Adressen kann danach als zulässig gelten, wenn die Dauer der Speicherung auf das absolut Notwendige begrenzt ist, die materiellen und prozeduralen Voraussetzungen eingehalten werden und „die Betroffenen über wirksame Garantien zum Schutz vor Missbrauchsgefahren sowie vor jedem unberechtigten Zugang zu diesen Daten und jeder unberechtigten Nutzung verfügen" (Rn. 93).

Auch der aus dem Zugang zu den mit der IP-Adresse verbundenen Identifizierungsdaten resultierende Eingriff kann nach dem EuGH nicht als schwerwiegend eingestuft werden (Rn. 115). Wird eine IP-Adresse nur dazu genutzt, ihren Inhaber zu identifizieren, so betrifft der allein zu diesem Zweck dienende Zugang zu der IP-Adresse diese als Identitätsdatum und nicht als Verkehrsdatum (Rn. 101). Ein Zugang zu diesen Daten muss daher auch keiner vorherigen Kontrolle durch ein Gericht oder eine unabhängige, am Verfahren nicht beteiligte Verwaltungsstelle unterworfen werden, da es sich um keinen schwerwiegenden Eingriff handelt (Rn. 132 ff.). Insgesamt ist daher eine Speicherung von IP-Adressen und die Gewährung des Zugangs zu mit diesen IP-Adressen verbundenen Identitätsdaten auch zum Zwecke der Bekämpfung allgemeiner (nicht schwerer) Kriminalität unionsrechtlich zulässig.

Der Zugang staatlicher Behörden zu den Identitätsdaten zu IP-Adressen, um Straftaten im Allgemeinen zu verhüten, zu ermitteln und zu verfolgen, kann dann verhältnismäßig sein, wenn sie allein dazu dienen, Personen zu identifizieren, die im Verdacht stehen, Straftaten begangen zu haben (Rn. 96 ff., 122). Um diese Zweckbindung sicherzustellen, müssen Regelungen es den Bediensteten, die über einen solchen Zugang verfügen, untersagen, Informationen über den Inhalt der von den Inhabern der IP-Adressen konsultierten Dateien, außer zur Kommunikation mit der Staatsanwaltschaft, offenzulegen, die von diesen Personen besuchten Internetseiten nachzuverfolgen und die IP-Adressen zu anderen Zwecken als zu solchen Maßnahmen zu nutzen (Rn. 114 ff.).

Einer vorherigen gerichtlichen Kontrolle des Datenzugangs bedarf es zur Wahrung der Verhältnismäßigkeit nur, wenn dieser „Zugang die Gefahr eines schweren Eingriffs in die Grundrechte des Betroffenen in dem Sinne birgt, dass er es

der Behörde ermöglichen könnte, genaue Schlüsse auf sein Privatleben zu ziehen und gegebenenfalls sein detailliertes Profil zu erstellen“ (Rn. 132). Dies kann in atypischen Fällen möglich sein, z. B., wenn Titel urheberrechtlich geschützter Werke Informationen über Aspekte des Privatlebens offenbaren können (Rn. 135). Daher muss das Verfahren so gestaltet werden, dass eine vorherige gerichtliche Kontrolle möglich ist, bevor eine Verknüpfung von Identitätsdaten mit diesen Inhaltsdaten erfolgt (Rn. 141 ff.).

Schließlich erfordert der Schutz vor Missbrauch klare und präzise Regelungen, die eine regelmäßige Überprüfung der Integrität der verwendeten Datenverarbeitungssysteme durch eine unabhängige Stelle vorsehen (Rn. 156) und dem Betroffenen ausreichende prozessuale Garantien gewährleisten (Rn. 162).

Ziel des Gesetzes ist es daher, im Rahmen der Rechtsprechung des EuGH, des BVerfG und des BVerwG eine unionsrechtskonforme und rechtssichere Mindestspeicherung von IP-Adressen und eventuell vergebenen Port-Nummern bei Telekommunikationsunternehmen einzuführen, um den Strafverfolgungs- und Gefahrenabwehrbehörden zum Zwecke der Bekämpfung schwerer Kriminalität den Zugriff darauf zu ermöglichen.

Daneben soll es – ebenfalls unter Berücksichtigung der genannten Rechtsprechung – zur Verfolgung allgemeiner Kriminalität und zum Schutz der öffentlichen Sicherheit auch weiterhin möglich sein, dass Internetzugangsdienste mindestgespeicherte IP-Adressen für eine Bestandsdatenauskunft anhand einer zu einem bestimmten Zeitpunkt zugewiesenen IP-Adresse verwenden dürfen, um den Strafverfolgungs- und Gefahrenabwehrbehörden die Identitätsdaten des relevanten Anschlussinhabers zu übermitteln.

Die gesetzliche Regelung der Speicherpflicht von Telekommunikationsverkehrsdaten durch das Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG vom 21. Dezember 2007 (BGBl. I S. 3198) umfasste in § 113b Nummer 3 TKG a. F. auch eine Abrufbefugnis der Nachrichtendienste des Bundes und der Länder. Das BVerfG hat die Regelung in seinem Urteil vom 2. März 2010 insoweit auch verfassungsrechtlich nicht beanstandet (vgl. BVerfGE 125, 260/316). Seit der Neuregelung der Speicherpflicht durch das Gesetz zur Einführung einer Speicherpflicht und einer Höchstspeicherpflicht für Verkehrsdaten vom 10. Dezember 2015 (BGBl. I S. 2218) werden die Nachrichtendienste in § 177 Absatz 1 TKG (§ 113c Absatz 1 a. F.) aber nicht mehr ausdrücklich als abfragebefugte Behörden aufgeführt. Für einen Ausschluss der Nachrichtendienste lassen sich keine fachlichen Gründe anführen. Vielmehr deutet die jüngere Rechtsprechung des BVerfG (BVerfGE 162, 1) darauf hin, dass die „Vorratsdatenspeicherung“ – möglicherweise sogar primär – als Instrument der Nachrichtendienste in Betracht kommt.

Die Funkzellenabfrage ist bei bestimmten Delikten die einzige Möglichkeit einer Täterermittlung. Vor allem bei Serientaten (z. B. Sexualdelikten oder Schockanrufen) ergeben sich aus den Funkzellendaten oft wertvolle Hinweise auf den unbekannten Täter. Das Deliktsfeld SÄM-UT (Straftaten zum Nachteil älterer Menschen mit unbekannten Tätern, sog. „Enkeltrickbetrug“ lässt sich ohne Funkzellendaten nicht aufklären. Bundesweit werden die Schadenssummen bei derartigen Taten auf deutlich über 100 Millionen Euro geschätzt. Aufgrund einer Entscheidung des Bundesgerichtshofs ist eine Funkzellenabfrage derzeit aber bei derartigen Delikten nicht mehr möglich, so dass es keine Ermittlungsmöglichkeit mehr gibt.

Bisher war die Rechtsprechung davon ausgegangen, dass die Funkzellenabfrage gemäß § 100g Absatz 3 StPO den Anfangsverdacht einer Katalogtat nach § 100a Absatz 2 StPO erfordert. Der 2. Strafsenat des Bundesgerichtshofs hat in seiner

Entscheidung vom 10. Januar 2024 (Az. 2 StR 171/23) allerdings entschieden, dass die Funkzellenabfrage im Hinblick auf die regelmäßig miterfassten Standortdaten für die Anordnung jeder Funkzellenabfrage nur noch bei Vorliegen eines Verdachts einer besonders schweren Straftat nach § 100g Absatz 2 Satz 2 StPO zulässig ist. Damit steht die Funkzellenabfrage zur Aufklärung vieler gewichtiger Straftaten – insbesondere auch der bandenmäßig begangenen Betrugstaten – nicht mehr zur Verfügung.

B. Lösung

Mit diesem Gesetz werden die unionsrechtswidrigen nationalen Regelungen der Vorratsdatenspeicherung in den §§ 175, 176 TKG an die Rechtsprechung des EuGH, des BVerfG sowie des BVerwG angepasst und auf eine dreimonatige Speicherung von IP-Adressen samt eventuell vergebener Port-Nummern zum Zwecke der Bekämpfung schwerer Kriminalität und zur Verhütung schwerer Bedrohungen der öffentlichen Sicherheit begrenzt. Eine weitergehende und eingriffsintensivere Verpflichtung zur zusätzlichen Mindestspeicherung von Standortdaten bei mobiler Internetnutzung ist nicht vorgesehen.

Mit der vorgeschlagenen Anpassung verbunden sind lediglich einzelne redaktionelle Folgeänderungen, etwa in § 177 TKG durch den Entfall der Verwendung und des Abrufs anlasslos gespeicherter IP-Adressen zum Zwecke der Gefahrenabwehr sowie in § 180 TKG und in den §§ 100g, 101a der Strafprozessordnung (StPO) durch den Entfall der anlasslosen Speicherung von Standortdaten. Durch die Anpassung des § 176 TKG entfallen zudem einige Kostentatbestände in dem Justizvergütungs- und -entschädigungsgesetzes (JVEG), die ursprünglich für die unionsrechtswidrige anlasslose Speicherung verschiedener Arten von Verkehrs- und Standortdaten geschaffen worden waren.

Die jüngere höchstrichterliche Rechtsprechung zu den Datenerhebungsbefugnissen der Verfassungsschutzbehörden aufgreifend sieht der Gesetzentwurf die Schaffung einer Übermittlungsbefugnis der Telekommunikationsdiensteanbieter nicht nur an die Strafverfolgungsbehörden, sondern auch an die Verfassungsschutzbehörden von Bund und Ländern vor (§ 177 Absatz 1 Nummer 4 – neu – TKG). Korrespondierend hierzu ist auch eine entsprechende Abrufbefugnis des Bundesamts für Verfassungsschutz vorgesehen (§ 8a Absatz 1 Satz 3 – neu – BVerfSchG).

In § 100g StPO soll eine Klarstellung zur Funkzellenabfrage aufgenommen werden, so dass die Ermittlungsmöglichkeit der Funkzellenabfrage wiederhergestellt wird.

C. Alternativen

Eine Alternative bestünde in der ersatzlosen Streichung der Regelungen zur Vorratsdatenspeicherung in den §§ 175, 176 TKG. Jedoch würde dies angesichts der Flüchtigkeit elektronischer Daten bei der Beweissicherung dem Interesse an einer effektiven Strafverfolgung widersprechen, da digitale Kommunikation eine immer größere Bedeutung erlangt hat und in vielen Strafverfahren neben digitalen Spuren kaum weitere Ermittlungsansätze zur Verfügung stehen. Dies wurde auch in der öffentlichen Anhörung des Rechtsausschusses des Deutschen Bundestages im Oktober 2023 zu dem Antrag „IP-Adressen rechtssicher speichern und Kinder vor sexuellem Missbrauch schützen“ (BT-Drs. 20/3687) der CDU/CSU-Fraktion im Deutschen Bundestag, mit dem die Speicherung von IP-Adressen gefordert wurde, deutlich: Die Strafrechtspraxis hat diesen Antrag unterstützt und darauf hingewiesen, dass ohne IP-Speicherung insbesondere Kinderpornografie nicht aufgeklärt werden kann. Gerade bei diesem Delikt ist die IP-Adresse oftmals der

einzige Ermittlungsansatz. Dies bestätigt auch eine vom Bundeskriminalamt durchgeführte Analyse der Vorgänge des amerikanischen National Center for Missing & Exploited Children – also des NCMEC – das ihm gemeldete Kinderpornografie-Fälle an das Bundeskriminalamt als deutsche Zentralstelle weitergibt.

In nur 41 Prozent der Vorgänge konnte die IP-Adresse einem Nutzeranschluss für weitere Ermittlungen zugeordnet werden, während etwa 34 Prozent der angelieferten IP-Adressen beim TK-Anbieter nicht mehr gespeichert und weitere 24 Prozent aus anderen Gründen (etwa aufgrund einer zusätzlich zur Identifizierung erforderlichen, aber nicht gespeicherten Port-Nummer) nicht beauskunftbar waren. Im Jahr 2022 wurden etwa 20.000 strafrechtlich relevante NCMEC-Vorgänge mangels Möglichkeit der Identifizierung eines potentiellen Tatverdächtigen vom BKA zur Einstellung an die Zentralstelle zur Bekämpfung von Internetkriminalität übermittelt (vgl. insbesondere die Stellungnahme des Bundeskriminalamts: www.bundestag.de/resource/blob/970516/8bbf8a86fd621d3ec354ea92a849f9c0/Stellungnahme-Link_BKA.pdf).

Eine weitere Alternative bestünde in der Einführung einer Sicherungsanordnung („Quick Freeze“). Die Möglichkeit einer anlassbezogenen Sicherungsanordnung wird indes von der Mehrheit in der Strafrechtspraxis als ineffizient betrachtet. Auch in der oben genannten öffentlichen Anhörung im Rechtsausschuss des Deutschen Bundestages wurde ein solches „Quick Freeze“-Verfahren als untauglich abgelehnt Daher ist die Einführung einer Sicherungsanordnung („Quick Freeze“) keine Alternative zur Einführung einer Mindestspeicherung von IP-Adressen, sondern kann allenfalls ergänzend dazu eingeführt werden.

Auch die ebenfalls diskutierte Möglichkeit der anlassbezogenen Erhebung von Login-IP-Adressen durch eine sogenannte „Login-Falle“ stellt keine Alternative dar. Ein solche Maßnahme ist bereits nach den §§ 100g, 100k StPO möglich. Auch durch eine weitergehende Ausgestaltung im Rahmen einer nationalen Regelung könnten ausländische Internetdienstanbieter jedenfalls nicht zur entsprechenden Kooperation verpflichtet werden. Insofern bedürfte es einer europäischen bzw. internationalen Regelung.

D. Haushaltsausgaben ohne Erfüllungsaufwand

Keine.

E. Erfüllungsaufwand

E.1 Erfüllungsaufwand für Bürgerinnen und Bürger

Keiner.

E.2 Erfüllungsaufwand für die Wirtschaft

Für die betroffenen Telekommunikationsdienste-Anbieter entsteht durch die Einführung einer Mindestspeicherung von IP-Adressen – sowohl gegenüber der ursprünglich vorgesehenen Vorratsdatenspeicherung als auch gegenüber der Einführung einer Sicherungsanordnung („Quick Freeze“) – kein wesentlicher Mehraufwand gegenüber der bereits überwiegend durchgeführten freiwilligen Speicherung der IP-Adressen von bis zu sieben Tagen. Im Übrigen entsteht für die Wirtschaft kein Erfüllungsaufwand.

Davon Bürokratiekosten aus Informationspflichten

Keine.

E.3 Erfüllungsaufwand der Verwaltung

Für die Strafverfolgungsbehörden des Bundes und der Länder entsteht durch die Einführung einer Mindestspeicherung von IP-Adressen sowohl ein Mehraufwand durch die damit verbundene weitergehende Möglichkeit zur Abfrage gespeicherter IP-Adressen in Ermittlungsverfahren als auch ein Minderaufwand durch eine Verringerung ergebnislos verlaufender Auskunftsersuchen und den Entfall anderer alternativer, nicht gleichsam effektiver Ermittlungsmaßnahmen insbesondere zur Identifizierung unbekannter Tatverdächtiger. In der Gesamtbetrachtung ist zu erwarten, dass der Mehr- und Minderaufwand sich annähernd ausgleichen wird. Bei der Bundesnetzagentur entsteht durch die Einführung einer Mindestspeicherung von IP-Adressen zwar ein zusätzlicher Kontrollaufwand und Mehraufwand bei der Anwendung der Bußgeldtatbestände. Jedoch ist sowohl gegenüber der ursprünglich vorgesehenen Vorratsdatenspeicherung als auch und insbesondere gegenüber der Einführung einer Sicherungsanordnung („Quick Freeze“) von einer erheblichen Entlastung auszugehen.

F. Weitere Kosten

Durch das Erfordernis eines Gerichtsbeschlusses für die einzelfallbezogene Anordnung der Herausgabe mindestgespeicherter IP-Adressen ist von einem geringfügigen Mehraufwand für die Justiz auszugehen. Auch insoweit ist jedoch sowohl gegenüber der ursprünglich vorgesehenen Vorratsdatenspeicherung als auch und insbesondere gegenüber der Einführung einer Sicherungsanordnung („Quick Freeze“) von einer erheblichen Entlastung auszugehen. Von weiteren Kosten ist nicht auszugehen. Auswirkungen auf Einzelpreise und das allgemeine Preisniveau, insbesondere auf das Verbraucherpreisniveau für Telekommunikationsdienste, sind im Übrigen nicht zu erwarten.

Entwurf eines Gesetzes zur Verbesserung der Verbrechensaufklärung – Einführung einer Mindestspeicherung von IP-Adressen und Wiederherstellung der Funkzellenabfragemöglichkeit

Vom …

Der Bundestag hat das folgende Gesetz beschlossen:

Artikel 1

Änderung des Telekommunikationsgesetzes

Das Telekommunikationsgesetz in der Fassung der Bekanntmachung vom 23. Juni 2021 (BGBl. I S. 1858), das zuletzt durch … geändert worden ist, wird wie folgt geändert:

1. § 175 Absatz 1 Satz 1 wird wie folgt gefasst:

   „Verpflichtungen zur Speicherung von Verkehrsdaten, zur Verwendung der Daten und zur Datensicherheit nach den §§ 176 bis 181 beziehen sich auf Anbieter öffentlich zugänglicher Internetzugangsdienste für Endnutzer."

2. § 176 wird wie folgt geändert:

   a) Absatz 1 wird wie folgt gefasst:

      „(1) Die in § 175 Absatz 1 Genannten sind verpflichtet,

      1. die dem Endnutzer für eine Internetnutzung zugewiesene Internetprotokoll-Adresse der Quelle einer Verbindung,
      2. eine eindeutige Kennung des Anschlusses, über den die Internetnutzung erfolgt, eine zugewiesene Benutzerkennung sowie eine gegebenenfalls zugewiesene Port-Nummer, sofern diese für die Identifikation des Endnutzers erforderlich ist, und
      3. Datum und Uhrzeit von Beginn und Ende der Internetnutzung unter der zugewiesenen Internetprotokoll-Adresse unter Angabe der zugrunde liegenden Zeitzone

      zum Zwecke der Bekämpfung schwerer Kriminalität sowie zur Verhütung schwerer Bedrohungen der öffentlichen Sicherheit für drei Monate im Inland zu speichern."

   b) Die Absätze 2 bis 4 werden aufgehoben.

   c) Absatz 5 wird Absatz 2.

   d) Absatz 6 wird aufgehoben.

   e) Die Absätze 7 und 8 werden die Absätze 3 und 4.

   f) Folgender Absatz 5 wird angefügt:

      „(5) Das Grundrecht des Fernmeldegeheimnisses (Artikel 10 Absatz 1 des Grundgesetzes) wird insoweit eingeschränkt."

3. § 177 Absatz 1 wird wie folgt geändert:

   a) In Nummer 3 werden die Wörter „öffentlich zugänglicher Telekommunikationsdienste“ durch die Wörter „öffentlich zugänglicher Internetzugangsdienste für Endnutzer“ und der Punkt am Ende durch ein Semikolon ersetzt.

   b) Folgende Nummer 4 wird angefügt:

      „4. an die Verfassungsschutzbehörden des Bundes und der Länder übermittelt werden, soweit diese die Übermittlung unter Berufung auf eine gesetzliche Bestimmung verlangen, die ihnen eine Erhebung der in § 176 genannten Daten wenigstens unter den Voraussetzungen des § 3 Absatz 1 des Artikel 10-Gesetzes erlauben.“

4. In § 180 Absatz 3 Satz 3 werden die Wörter „§ 176 Absatz 7 und 8“ durch die Wörter „§ 176 Absatz 3 und 4“ ersetzt.

5. In § 228 Absatz 2 Nummer 57 wird die Angabe „Absatz 8“ durch die Angabe „Absatz 4“ ersetzt.

Artikel 2

Änderung der Strafprozessordnung

Die Strafprozessordnung in der Fassung der Bekanntmachung vom 7. April 1987 (BGBl. I S. 1074, 1319), die zuletzt durch … geändert worden ist, wird wie folgt geändert:

1. § 100g wird wie folgt geändert:

   a) Absatz 3 Satz 1 erster Halbsatz wird wie folgt gefasst:

      „Die Erhebung aller in einer Funkzelle angefallenen Verkehrsdaten, einschließlich der Standortdaten (Funkzellenabfrage), ist nur zulässig,“.

   b) Absatz 3 Satz 2 wird aufgehoben.

   c) In Absatz 4 Satz 1 werden die Wörter „auch in Verbindung mit Absatz 3 Satz 2,“ gestrichen.

2. § 101a wird wie folgt geändert:

   a) In Absatz 1 Satz 2 werden die Wörter „, auch in Verbindung mit § 100g Absatz 3 Satz 2,“ gestrichen.

   b) In Absatz 4 Satz 1 in dem Satzteil vor Nummer 1 und in Nummer 1 werden jeweils die Wörter „oder Absatz 3 Satz 2“ gestrichen.

   c) In Absatz 5 werden die Wörter „, auch in Verbindung mit Absatz 3 Satz 2,“ gestrichen.

Artikel 3

Änderung des Justizvergütungs- und -entschädigungsgesetzes

Anlage 3 zum Justizvergütungs- und -entschädigungsgesetz vom 5. Mai 2004 (BGBl. I S. 718, 776), das zuletzt durch … geändert worden ist, wird wie folgt geändert:

1. In den Nummern 202 und 301 werden jeweils in der Spalte 2 die Wörter „§ 176 Absatz 2 bis 4 TKG“ durch die Angabe „§ 176 Absatz 1 TKG“ ersetzt.

2. Die Nummern 304 und 307 werden aufgehoben.

3. In Nummer 309 werden in der Spalte 2 die Wörter „und für die Auskunft muss auf Verkehrsdaten nach § 176 Absatz 2 bis 4 TKG zurückgegriffen werden“ gestrichen.

4. Die Nummern 310 bis 314 werden wie folgt gefasst:

„310	Auskunft über gespeicherte Verkehrsdaten in Fällen, in denen lediglich Ort und Zeitraum bekannt sind: Die Abfrage erfolgt für einen bestimmten, durch eine Adresse bezeichneten Standort ..... Die Auskunft erfolgt für eine Fläche:	60,00 €
311	– Die Entfernung der am weitesten voneinander entfernten Punkte beträgt nicht mehr als 10 Kilometer: Die Pauschale 310 beträgt	190,00 €
312	– Die Entfernung der am weitesten voneinander entfernten Punkte beträgt mehr als 10, aber nicht mehr als 25 Kilometer: Die Pauschale 310 beträgt	490,00 €
313	– Die Entfernung der am weitesten voneinander entfernten Punkte beträgt mehr als 25, aber nicht mehr als 45 Kilometer: Die Pauschale 310 beträgt	930,00 €
	Liegen die am weitesten voneinander entfernten Punkte mehr als 45 Kilometer auseinander, ist für den darüber hinausgehenden Abstand die Entschädigung nach den Nummern 311 bis 313 gesondert zu berechnen.	
314	Die Auskunft erfolgt für eine bestimmte Wegstrecke: Die Pauschale 310 beträgt für jeweils angefangene 10 Kilometer Länge	110,00 €“.

5. Die Nummern 315 bis 319 und 401 werden aufgehoben.

Artikel 4

Änderung des Bundesverfassungsschutzgesetzes

Dem § 8a Absatz 1 des Bundesverfassungsschutzgesetzes vom 20. Dezember 1990 (BGBl. I S. 2954, 2970), das zuletzt durch ... geändert worden ist, wird folgender Satz angefügt:

„Eine Auskunft zu den in § 176 des Telekommunikationsgesetzes genannten Daten darf nur unter den Voraussetzungen des § 3 Absatz 1 des Artikel 10-Gesetzes eingeholt werden.“

Artikel 5

Einschränkung eines Grundrechts

Durch Artikel 1 und Artikel 4 wird das Fernmeldegeheimnis (Artikel 10 Absatz 1 des Grundgesetzes) eingeschränkt.

Artikel 6

Inkrafttreten

Dieses Gesetz tritt am ... [einsetzen: Datum des ersten Tages des dritten auf die Verkündung folgenden Monats] in Kraft.

Berlin, den 15. Oktober 2024

Friedrich Merz, Alexander Dobrindt und Fraktion

Begründung

A. Allgemeiner Teil

I. Zielsetzung und Notwendigkeit der Regelungen

Eine anlasslose und umfassende Speicherung der Verkehrsdaten bei Telefonaten und Internet-Nutzung für sechs Monate wurde erstmals mit dem Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG vom 21. Dezember 2007 (BGBl. I S.3198) mit Wirkung ab 1. Januar 2008 eingeführt und war bußgeldbewehrt ab 1. Januar 2009 umzusetzen. Nachdem das Bundesverfassungsgericht (BVerfG) mit einstweiligen Anordnungen vom 11. März 2008 und 28. Oktober 2008 den Abruf entsprechender Daten stark eingeschränkt hatte, erklärte es mit Urteil vom 2. März 2010 – 1 BvR 256/08 – die §§ 113a und 113b des Telekommunikationsgesetzes (TKG) und auch § 100g Absatz 1 Satz 1 der Strafprozessordnung (StPO), soweit danach Verkehrsdaten nach § 113a TKG erhoben werden durften, wegen Verstoßes gegen Art. 10 Absatz 1 GG für nichtig.

Mit dem Gesetz zur Einführung einer Speicherpflicht und einer Höchstspeicherpflicht für Verkehrsdaten vom 10. Dezember 2015 (BGBl. I S. 2218) wurden in den §§ 113a bis 113g TKG differenzierte Regelungen zur anlasslosen Speicherung von Telefon- und Internetverbindungen für zehn Wochen sowie Standortdaten von Mobiltelefonen für vier Wochen eingeführt. Diese Speicherpflicht war an sich ab dem 1. Juli 2017 zu erfüllen. Nachdem das BVerfG mit Beschlüssen vom 8. Juni 2016 – 1 BvQ 42/15 und 1 BvR 229/16 – und 26. März 2017 – 1 BvR 141/16 1 BvR 3156/15 – noch den Erlass einstweiliger Anordnungen abgelehnt hatte, mit denen diese Speicherverpflichtungen vorläufig außer Kraft gesetzt werden sollten, entschied das Oberverwaltungsgericht Münster mit Beschluss vom 22. Juni 2017 – 13 B 238/17 – im Rahmen des einstweiligen Rechtsschutzes, dass die Telekommunikationsdiensteanbieter bis zum rechtskräftigen Abschluss des Hauptsacheverfahrens keine Speicherpflicht trifft. Daraufhin erklärte die Bundesnetzagentur am 28. Juni 2017 keine Anordnungen und sonstige Maßnahmen zur Durchsetzung der Speicherverpflichtung zu ergreifen und damit nicht aufsichtsrechtlich gegen die Telekommunikationsdiensteanbieter vorzugehen, welche die „Vorratsdatenspeicherung“ nicht umsetzen. Seitdem ist die Vorratsdatenspeicherung de facto ausgesetzt (vgl. dazu etwa BeckOK StPO/Bär, 50. Ed., § 100 g Rn. 65 ff.; Roßnagel, in: Geppert/Schütz/, TKG, 5. Aufl, § 175 Rn. 43 ff.).

In der Hauptsache hat das im Wege der Sprungrevision angerufene Bundesverwaltungsgericht (BVerwG) mit Beschluss vom 25. September 2019 – 6 C 12/18 – dem EuGH im Rahmen eines Vorabentscheidungsersuchens die Rechtsfrage vorgelegt, ob die Speicherpflicht der §§ 113a, 113b TKG europarechtskonform ist. Zwischenzeitlich wurden mit dem Telekommunikationsmodernisierungsgesetz vom 23. Juni 2021 (BGBl. I S. 1858) die Regelungen der §§ 113a bis 113g TKG inhaltlich unverändert in den §§ 175 bis 181 TKG übernommen.

Mit Urteil vom 20. September 2022 – C-793/19 und C-794/19 – hat der EuGH zunächst seine Rechtsprechung zu nationalen Regelungen der Vorratsdatenspeicherung bekräftigt und u. a. festgehalten, dass die Richtlinie 2002/58/EG (ePrivacy-RL) den Grundsatz des Verbots der Speicherung von sich auf Teilnehmer und Nutzer beziehenden Verkehrsdaten durch Dritte regele (Rn. 56). Art. 15 Absatz 1 ePrivacy-RL sehe zwar die Möglichkeit vor, die sich im Übrigen aus der Richtlinie ergebenden Rechte und Pflichten der Betreiber elektronischer Kommunikationsdienste zu dem Gemeinwohl dienenden Zwecken zu beschränken (Rn. 57), sofern diese für die nationale Sicherheit, die Landesverteidigung, die öffentliche Sicherheit sowie die Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten oder des unzulässigen Gebrauchs von elektronischen Kommunikationssystemen in einer demokratischen Gesellschaft notwendig, angemessen und verhältnismäßig ist. Nationale Regelungen zur Beschränkung der in der ePrivacy-RL vorgesehenen Rechte und Pflichten seien jedoch nur dann zu rechtfertigen, wenn die verfolgte, dem Gemeinwohl dienende Zielsetzung in einem angemessenen Verhältnis zur Schwere des Eingriffs steht (Rn. 68). Eine Speicherung der Verkehrsdaten stelle zudem – unabhängig davon, ob sie später verwendet werden oder nicht – einen Eingriff in die Grundrechte der Bürgerinnen und Bürger auf Achtung des Privatlebens und auf den Schutz personenbezogener Daten dar, die in den Art. 7 und 8 der Charta der Grundrechte der Europäischen Union (GRCh) verankert sind (Rn. 60). Aus der Gesamtheit dieser Daten könnten sehr genaue Schlüsse auf das Privatleben der Personen gezogen werden, deren Daten gespeichert wurden (Rn. 61), was in Abhängigkeit von Menge und Vielfalt der auf Vorrat gespeicherten Daten auch dazu führen könne, dass die Nut-

zer elektronischer Kommunikationsmittel von der Ausübung ihrer durch Art. 11 GRCh gewährleisteten Freiheit der Meinungsäußerung abgehalten würden (Rn. 62). Diese Rechte der Bürgerinnen und Bürger könnten jedoch nach Art. 52 Absatz 1 GRCh durch eine gesetzliche Regelung, die den Wesensgehalt dieser Rechte achtet und den Grundsatz der Verhältnismäßigkeit wahrt, eingeschränkt werden (Rn. 63). Die Ausnahmen vom Schutz personenbezogener Daten und dessen Einschränkungen müssten sich jedoch auf das absolut Notwendige beschränken (Rn. 67).

Ausgehend von diesen Grundsätzen hat der EuGH ausgeführt, dass eine allgemeine und unterschiedslose Vorratsdatenspeicherung aller Verkehrsdaten allein mit dem Schutz der nationalen Sicherheit als bedeutendstem Zweck gerechtfertigt werden kann, wenn sich der betreffende Mitgliedstaat einer als real und aktuell oder vorhersehbar einzustufenden ernsten Bedrohung für die nationale Sicherheit gegenübersieht, die Anordnung einer wirksamen gerichtlichen Kontrolle unterliegt und nur für einen auf das absolut Notwendige begrenzten Zeitraum ergeht (Rn. 72). Hinsichtlich des Ziels der Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten, könne allein die Bekämpfung schwerer Kriminalität und die Verhütung ernster Bedrohungen der öffentlichen Sicherheit eine Speicherverpflichtung für Verkehrsdaten im Einklang mit dem Grundsatz der Verhältnismäßigkeit rechtfertigen (Rn. 73). Eine allgemeine und unterschiedslose Vorratsdatenspeicherung von allen Verkehrsdaten komme zur Verwirklichung dieses Ziels nicht in Betracht (Rn. 75). Zum Zwecke der Bekämpfung schwerer Kriminalität und der Verhütung ernster Bedrohungen der öffentlichen Sicherheit hält der EuGH allgemein folgende Maßnahmen für zulässig (Rn. 75): (1) eine gezielte Vorratsspeicherung von Verkehrs- und Standortdaten auf der Grundlage objektiver und nicht diskriminierender Kriterien anhand von Kategorien betroffener Personen oder mittels eines geografischen Kriteriums für einen auf das absolut Notwendige begrenzten, aber verlängerbaren Zeitraum; (2) eine allgemeine und unterschiedslose Vorratsspeicherung der IP-Adressen, die der Quelle einer Verbindung zugewiesen sind, für einen auf das absolut Notwendige begrenzten Zeitraum; (3) eine allgemeine und unterschiedslose Vorratsspeicherung der die Identität der Nutzer elektronischer Kommunikationsmittel betreffenden Daten; (4) eine Verpflichtung der Betreiber elektronischer Kommunikationsdienste mittels einer Entscheidung der zuständigen Behörde, die einer wirksamen gerichtlichen Kontrolle unterliegt, während eines festgelegten Zeitraums die ihnen zur Verfügung stehenden Verkehrs- und Standortdaten umgehend zu sichern („Quick Freeze“). Vor diesem Hintergrund hat der EuGH entschieden, dass die 2015 eingeführte Pflicht zur anlasslosen Vorratsdatenspeicherung von Telekommunikations-Verkehrsdaten in den §§ 113a bis 113g TKG a. F. (§§ 175 bis 181 TKG n. F.) nicht auf Art. 15 ePrivacy-RL gestützt werden kann und somit nicht mit dem Unionsrecht vereinbar ist. Denn die deutschen Vorschriften sähen eine Vorratsspeicherung von Verkehrs- und Standortdaten vor, die nahezu alle die Bevölkerung bildenden Personen betreffe, ohne dass diese sich auch nur mittelbar in einer Lage befänden, die Anlass zur Strafverfolgung geben könnte. Ebenso schrieben sie die anlasslose, flächendeckende und personell, zeitlich und geografisch undifferenzierte Vorratsspeicherung eines Großteils der Verkehrs- und Standortdaten vor (Rn. 83). Die deutschen Vorschriften könnten daher nicht als gezielte Vorratsdatenspeicherung im Sinne der Rechtsprechung des EuGH angesehen werden (Rn. 84). Ferner würden auch die vorgesehenen kurzen Speicherfristen die Eingriffsintensität nicht durchgreifend mindern, da selbst die Speicherung einer begrenzten Menge von Verkehrs- oder Standortdaten oder die Speicherung dieser Daten über einen kurzen Zeitraum geeignet seien, sehr genaue Informationen über das Privatleben des Nutzers eines elektronischen Kommunikationsmittels zu liefern (Rn. 87 ff.). Dasselbe gelte auch für die strengen Regelungen zum Schutz der gespeicherten Daten vor Missbrauch, da die Vorratsspeicherung dieser Daten und der Zugang zu ihnen unterschiedliche Eingriffe in die in den Art. 7 und 11 GRCh garantierten Grundrechte darstellen, die eine gesonderte Rechtfertigung nach Art. 52 Absatz 1 GRCh erfordern (Rn. 91).

Hinsichtlich der allgemeinen und unterschiedslosen Vorratsspeicherung der „Quellen-IP-Adressen“ hat der EuGH in dem Urteil vom 20. September 2022 – C-793/19 und C-794/19 – ergänzend ausgeführt, dass eine solche Speicherung zwar einen schweren Eingriff in die in den Art. 7 und 8 der GRCh verankerten Grundrechte darstelle, da IP-Adressen es ermöglichen könnten, genaue Schlüsse auf das Privatleben des Nutzers des betreffenden elektronischen Kommunikationsmittels zu ziehen, und damit abschreckende Wirkung in Bezug auf die Ausübung der in Art. 11 GRCh garantierten Freiheit der Meinungsäußerung zu haben (Rn. 100). Allerdings sei auch zu berücksichtigen, dass im Fall einer im Internet begangenen Straftat und insbesondere im Fall des Erwerbs, der Verbreitung, der Weitergabe oder der Bereitstellung im Internet von Kinderpornografie die IP-Adresse der einzige Anhaltspunkt sein könne, der es ermögliche, die Identität der Person zu ermitteln, der diese Adresse zugewiesen war, als die Tat begangen wurde (Rn. 100). Unter diesen Umständen treffe es zwar zu, dass eine Vorratsspeicherung der IP-Adressen aller natürlichen Personen, denen ein Endgerät gehört, von dem aus ein Internetzugang möglich ist, Personen erfassen würde, die prima facie keinen Zusammenhang mit den verfolgten Zielen der Maßnahme

aufwiesen (Rn. 101). Auch treffe es zu, dass die Internetnutzer aufgrund Art. 7 und 8 GRCh erwarten dürften, dass ihre Identität grundsätzlich nicht preisgegeben werde (Rn. 101). Gleichwohl verstöße eine Rechtsvorschrift, die eine allgemeine und unterschiedslose Vorratsspeicherung allein der IP-Adressen der Quelle einer Verbindung vorsieht, grundsätzlich nicht gegen Art. 15 Absatz 1 ePrivacy-RL im Licht der Art. 7, 8 und 11 sowie von Art. 52 Absatz 1 GRCh, sofern diese Möglichkeit von der strikten Einhaltung der materiellen und prozeduralen Voraussetzungen abhängig gemacht werde, die die Nutzung dieser Daten regeln müsse (Rn. 101). Angesichts der Schwere des mit dieser Vorratsdatenspeicherung verbundenen Eingriffs in die Grundrechte der Art. 7 und 8 GRCH seien neben dem Schutz der nationalen Sicherheit jedoch nur die Bekämpfung schwerer Kriminalität und die Verhütung schwerer Bedrohungen der öffentlichen Sicherheit geeignet, diesen Eingriff zu rechtfertigen (Rn. 102). Außerdem dürfe die Dauer der Speicherung das im Hinblick auf das verfolgte Ziel absolut Notwendige nicht überschreiten (Rn. 102). Schließlich müsse eine derartige Maßnahme strenge Voraussetzungen und Garantien hinsichtlich der Auswertung dieser Daten, insbesondere in Form einer Nachverfolgung, in Bezug auf die Online-Kommunikationen und -Aktivitäten der Betroffenen vorsehen (Rn. 102).

Daneben hat der EuGH in dem Urteil vom 20. September 2022 – C-793/19 und C-794/19 – festgestellt, dass auch die Vorratsspeicherung der die Identität der Nutzer elektronischer Kommunikationsmittel betreffenden Daten („Identitätsdaten“) zur Bekämpfung schwerer Kriminalität beitragen kann, sofern diese Daten es ermöglichen, die Personen zu identifizieren, die solche Kommunikationsmittel im Zusammenhang mit der Vorbereitung oder Begehung einer zur schweren Kriminalität zählenden Tat verwendet haben (Rn. 98). Eine allgemeine Vorratsdatenspeicherung von „Identitätsdaten“ sei bereits für die Zwecke der Bekämpfung der Kriminalität im Allgemeinen zulässig (Rn. 99).

Infolge dieses Urteils des EuGH hat das BVerfG mit Beschlüssen vom 14. Februar 2023 – 1 BvR 2845/16; 1 BvR 2683/16 – und vom 15. Februar 2023 – 1 BvR 141/16 – zwar mehrere Verfassungsbeschwerden gegen nationale Regelungen der Vorratsdatenspeicherung mangels Rechtsschutzbedürfnis nicht zur Entscheidung angenommen, aber gleichwohl festgestellt, dass §§ 175, 176 TKG dem Unionsrecht widersprechen und deshalb innerstaatlich nicht mehr angewendet werden dürfen. Auch das BVerwG hat infolge dieses Urteils des EuGH am 14. August 2023 – 6 C 6.22 und 6 C 7.22 – entschieden, dass die nationalen Regelungen zur Vorratsdatenspeicherung von Verkehrs- und Standortdaten in den §§ 175, 176 TKG unionsrechtswidrig sind und wegen des Anwendungsvorrangs des Unionsrechts nicht angewendet werden dürfen.

Mit Urteil des EuGH vom 30. April 2024 – C-470/21 – hat der EuGH sowohl die unionsrechtliche Zulässigkeit als auch die Notwendigkeit und Verhältnismäßigkeit einer Mindestspeicherung von IP-Adressen noch einmal verdeutlicht. Er hat festgestellt, dass nationale Regelungen zur Speicherung von IP-Adressen zur Bekämpfung jeglicher Art von Straftaten unionsrechtlich grundsätzlich zulässig sind. Der EuGH hat damit seine Rechtsprechung zur Vorratsdatenspeicherung fortentwickelt und erachtet die Vorratsspeicherung von IP-Adressen aufgrund deren Bedeutung als oftmals einzigem Ermittlungsansatz für die Verfolgung und Verhinderung von Straftaten nunmehr sogar als zwingend erforderlich, um eine andernfalls drohende Gefahr der systemischen Straflosigkeit von Straftaten, die mithilfe des Internets begangen werden, zu vermeiden.

Der EuGH hat nunmehr in Abkehr von seiner bisherigen Rechtsprechung ausdrücklich festgestellt, dass nicht jede allgemeine und unterschiedslose Speicherung von IP-Adressen zwangsläufig einen schweren Eingriff in Grundrechte darstellt. Der EuGH hat zunächst noch einmal bekräftigt, dass bei online begangenen Straftaten der Zugang zu IP-Adressen die einzige Ermittlungsmaßnahme darstellen kann, die eine effektive Identifizierung der Person ermöglicht, der diese Adresse zugewiesen war, als die Tat begangen wurde (Rn. 117). Er hat aber auch betont, dass ohne eine entsprechende Speicherung eine Gefahr der systemischen Straflosigkeit von Straftaten droht, die online begangen oder vorbereitet werden (Rn. 119). Aber selbst in Fällen, in denen die IP-Adresse nicht die einzige mögliche Maßnahme zur Identifizierung des Tatverdächtigen darstellt, erachtet er eine Speicherung für notwendig. Denn anderenfalls wären umfangreiche Ermittlungen wie Internetrecherchen zu den Online-Aktivitäten der betreffenden Person (sog. OSINT) notwendig, insbesondere zu Aktivitäten in sozialen Netzwerken und zu Kontakten (Rn. 120). Solche Ermittlungsmaßnahmen können jedoch genaue Informationen über das Privatleben der Betroffenen offenbaren und stellen deswegen sogar einen schwereren Eingriff dar als die Speicherung und rein punktuelle Abfrage der IP-Adresse (Rn. 121).

Eine gesetzliche Pflicht zur allgemeinen und unterschiedslosen Speicherung von IP-Adressen sieht der EuGH nunmehr als verhältnismäßig an, wenn durch die Modalitäten der Speicherung ausgeschlossen ist, dass aus den IP-Adressen „genaue Schlüsse auf das Privatleben der Personen“ gezogen werden können (Rn. 83). Um dies sicherzustellen, muss durch klare und präzise Rechtsvorschriften „eine wirksame strikte Trennung der verschie-

denen Kategorien auf Vorrat gespeicherter Daten gewährleistet“ sein (Rn. 84 f.). Hierzu formuliert der EuGH selbst vier Vorgaben an diese Gewährleistungsregelungen (Rn. 86 bis 89):

„Erstens müssen die in der vorstehenden Randnummer genannten nationalen Regeln sicherstellen, dass jede Kategorie von Daten, einschließlich der Identitätsdaten und der IP-Adressen, völlig getrennt von den übrigen Kategorien auf Vorrat gespeicherter Daten gespeichert wird.

Zweitens müssen diese Regeln gewährleisten, dass in technischer Hinsicht eine wirksame strikte Trennung zwischen den verschiedenen Kategorien auf Vorrat gespeicherter Daten, u. a. den Identitätsdaten, den IP-Adressen, den verschiedenen Verkehrsdaten außer den IP-Adressen und den verschiedenen Standortdaten durch eine abgesicherte und zuverlässige Datenverarbeitungseinrichtung stattfindet.

Drittens dürfen die Regeln, soweit sie die Möglichkeit vorsehen, die auf Vorrat gespeicherten IP-Adressen mit der Identität des Betroffenen zu verknüpfen, unter Beachtung der Anforderungen, die sich aus Art. 15 Absatz 1 der Richtlinie 2002/58 im Licht der Art. 7, 8 und 11 der Charta ergeben, eine solche Verknüpfung nur unter Verwendung eines leistungsfähigen technischen Verfahrens erlauben, das die Wirksamkeit der strikten Trennung dieser Datenkategorien nicht in Frage stellt.

Viertens muss die Zuverlässigkeit dieser strikten Trennung regelmäßig Gegenstand einer Kontrolle durch eine andere Behörde als die sein, die Zugang zu den von den Betreibern elektronischer Kommunikationsdienste auf Vorrat gespeicherten personenbezogenen Daten begehrt.“

Werden sie eingehalten, „kann der Eingriff […] schon aufgrund der Struktur ihrer Speicherung nicht als ‚schwer‘ eingestuft werden“ (Rn. 90). Eine Regelung zur Speicherung von IP-Adressen kann danach als zulässig gelten, wenn die Dauer der Speicherung auf das absolut Notwendige begrenzt ist, die materiellen und prozeduralen Voraussetzungen eingehalten werden und „die Betroffenen über wirksame Garantien zum Schutz vor Missbrauchsgefahren sowie vor jedem unberechtigten Zugang zu diesen Daten und jeder unberechtigten Nutzung verfügen“ (Rn. 93).

Auch der aus dem Zugang zu den mit der IP-Adresse verbundenen Identifizierungsdaten resultierende Eingriff kann nach dem EuGH nicht als schwerwiegend eingestuft werden (Rn. 115). Wird eine IP-Adresse nur dazu genutzt, ihren Inhaber zu identifizieren, so betrifft der allein zu diesem Zweck dienende Zugang zu der IP-Adresse diese als Identitätsdatum und nicht als Verkehrsdatum (Rn. 101). Ein Zugang zu diesen Daten muss daher auch keiner vorherigen Kontrolle durch ein Gericht oder eine unabhängige, am Verfahren nicht beteiligte Verwaltungsstelle unterworfen werden, da es sich um keinen schwerwiegenden Eingriff handelt (Rn. 132 ff.). Insgesamt ist daher eine Speicherung von IP-Adressen und die Gewährung des Zugangs zu mit diesen IP-Adressen verbundenen Identitätsdaten auch zum Zwecke der Bekämpfung allgemeiner (nicht schwerer) Kriminalität unionsrechtlich zulässig.

Der Zugang staatlicher Behörden zu den Identitätsdaten zu IP-Adressen, um Straftaten im Allgemeinen zu verhüten, zu ermitteln und zu verfolgen, kann dann verhältnismäßig sein, wenn sie allein dazu dienen, Personen zu identifizieren, die im Verdacht stehen, Straftaten begangen zu haben (Rn. 96 ff., 122). Um diese Zweckbindung sicherzustellen, müssen Regelungen es den Bediensteten, die über einen solchen Zugang verfügen, untersagen, Informationen über den Inhalt der von den Inhabern der IP-Adressen konsultierten Dateien, außer zur Kommunikation mit der Staatsanwaltschaft, offenzulegen, die von diesen Personen besuchten Internetseiten nachzuverfolgen und die IP-Adressen zu anderen Zwecken als zu solchen Maßnahmen zu nutzen (Rn. 114 ff.).

Einer vorherigen gerichtlichen Kontrolle des Datenzugangs bedarf es zur Wahrung der Verhältnismäßigkeit nur, wenn dieser „Zugang die Gefahr eines schweren Eingriffs in die Grundrechte des Betroffenen in dem Sinne birgt, dass er es der Behörde ermöglichen könnte, genaue Schlüsse auf sein Privatleben zu ziehen und gegebenenfalls sein detailliertes Profil zu erstellen“ (Rn. 132). Dies kann in atypischen Fällen möglich sein, z. B., wenn Titel urheberrechtlich geschützter Werke Informationen über Aspekte des Privatlebens offenbaren können (Rn. 135). Daher muss das Verfahren so gestaltet werden, dass eine vorherige gerichtliche Kontrolle möglich ist, bevor eine Verknüpfung von Identitätsdaten mit diesen Inhaltsdaten erfolgt (Rn. 141 ff.).

Schließlich erfordert der Schutz vor Missbrauch klare und präzise Regelungen, die eine regelmäßige Überprüfung der Integrität der verwendeten Datenverarbeitungssysteme durch eine unabhängige Stelle vorsehen (Rn. 156) und dem Betroffenen ausreichende prozessuale Garantien gewährleisten (Rn. 162).

Seit der Neuregelung der Speicherpflicht durch das Gesetz zur Einführung einer Speicherpflicht und einer Höchstspeicherpflicht für Verkehrsdaten vom 10. Dezember 2015 (BGBl. I S. 2218) werden die Nachrichtendienste in § 177 Absatz 1 TKG (§ 113c Absatz 1 a. F.) nicht mehr ausdrücklich als abfragebefugte Behörden aufgeführt.

Für einen Ausschluss der Nachrichtendienste lassen sich keine fachlichen Gründe anführen, denn die Nachrichtendienste haben seit dem Terrorismusbekämpfungsgesetz vom 9. Januar 2002 (BGBl. I S. 361) die Befugnis, bei Telekommunikationsdiensteanbietern auch Verkehrsdaten abzufragen (vgl. § 8 Absatz 8 BVerfSchG a. F.; heute § 8a Absatz 2 Satz 1 Nummer 4 BVerfSchG). Auf dieser Grundlage können auch Verkehrsdaten über bereits vor der Abfrage erfolgte Telekommunikationsverbindungen abgefragt werden, sofern die Daten bei den Telekommunikationsdiensteanbietern für Zwecke der Abrechnung noch gespeichert sind. Damit hängt aber die Abfragemöglichkeit von der Abrechnungspraxis des jeweiligen Anbieters und damit letztlich vom Zufall ab (vgl. hierzu BT-Drucksache 18/5088, S. 1, 21). Es gibt keinen Grund, die Abfragemöglichkeit der Nachrichtendienste vom Zufall abhängen zu lassen, die der anderen Sicherheitsbehörden aber durch eine Mindestspeicherfrist abzusichern. Vielmehr deutet die jüngere Rechtsprechung des BVerfG darauf hin, dass die „Vorratsdatenspeicherung" – möglicherweise sogar primär – als Instrument der Nachrichtendienste in Betracht kommt: Zwar hat das Gericht die Abrufbefugnis des Bayerischen Landesamtes für Verfassungsschutz in Artikel 15 Absatz 3 BayVSG a. F. für nichtig erklärt, dies jedoch nur deshalb, weil der Bundesgesetzgeber nach dem Modell der „Doppeltür" keine entsprechende Übermittlungsbefugnis im TKG eröffnet hat (BVerfGE 162, 1 Rn. 333 ff.). Obwohl es darauf nicht mehr entscheidungserheblich ankam, hat der erkennende Senat aber in diesem Zusammenhang seine frühere Aussage relativiert (BVerfGE 125, 260/331 f.), dass beim Abruf von gespeicherten Telekommunikationsverkehrsdaten für Polizei und Nachrichtendienste dieselben verfassungsrechtlichen Anforderungen gelten (BVerfGE 162, 1 Rn. 172 f.). Vielmehr rechtfertige der Umstand, dass eine Verfassungsschutzbehörde nicht über eigene operative Anschlussbefugnisse verfüge, es im Grundsatz, die ihr zur Wahrnehmung ihrer Beobachtungsaufgaben eingeräumten Datenerhebungsbefugnisse im Vergleich zu den Befugnissen einer Polizeibehörde wegen des geringeren Eingriffsgewichts an modifizierte Eingriffsschwellen zu knüpfen (BVerfGE 162, 1 Rn. 156 ff.).

Die Funkzellenabfrage ist bei bestimmten Delikten die einzige Möglichkeit einer Täterermittlung. Vor allem bei Serientaten (z. B. Sexualdelikten oder Schockanrufen) ergeben sich aus den Funkzellendaten oft wertvolle Hinweise auf den unbekannten Täter. Das Deliktsfeld SÄM-UT (Straftaten zum Nachteil älterer Menschen mit unbekannten Tätern, sog. „Enkeltrickbetrug" lässt sich ohne Funkzellendaten nicht aufklären. Bundesweit werden die Schadenssummen bei derartigen Taten auf deutlich über 100 Millionen Euro geschätzt. Aufgrund einer Entscheidung des Bundesgerichtshofs ist eine Funkzellenabfrage derzeit aber bei derartigen Delikten nicht mehr möglich, so dass es keine Ermittlungsmöglichkeit mehr gibt.

Bisher war die Rechtsprechung davon ausgegangen, dass die Funkzellenabfrage gemäß § 100g Absatz 3 StPO den Anfangsverdacht einer Katalogtat nach § 100a Absatz 2 StPO erfordert. Der 2. Strafsenat des Bundesgerichtshofs hat in seiner Entscheidung vom 10. Januar 2024 (Az. 2 StR 171/23) allerdings entschieden, dass die Funkzellenabfrage im Hinblick auf die regelmäßig miterfassten Standortdaten für die Anordnung jeder Funkzellenabfrage nur noch bei Vorliegen eines Verdachts einer besonders schweren Straftat nach § 100g Absatz 2 Satz 2 StPO zulässig ist. Damit steht die Funkzellenabfrage zur Aufklärung vieler gewichtiger Straftaten – insbesondere auch der bandenmäßig begangenen Betrugstaten – nicht mehr zur Verfügung.

II. Wesentlicher Inhalt des Entwurfs

Mit diesem Entwurf werden die gegen das Unionsrecht verstoßenden Regelungen der Vorratsdatenspeicherung in den §§ 175, 176 TKG im Hinblick auf die Rechtsprechung des EuGH, des BVerfG sowie des BVerwG angepasst und auf eine dreimonatige Speicherung von IP-Adressen samt eventuell vergebener Port-Nummern zum Zwecke der Bekämpfung schwerer Kriminalität und zur Verhütung schwerer Bedrohungen der öffentlichen Sicherheit begrenzt. Eine weitergehende und eingriffsintensivere Verpflichtung zur zusätzlichen Mindestspeicherung von Standortdaten bei mobiler Internetnutzung ist nicht vorgesehen.

Unter Berücksichtigung der Rechtsprechung des BVerfG zu dem sogenannten Doppeltürmodell (Beschluss vom 24. Januar 2012 – 1 BvR 1299/05 – Rn. 123) können die Verpflichtungen zur Verwendung und Übermittlung der Daten („1. Tür") sowie zur Datensicherheit nach den §§ 177 bis 181 TKG, die sich dann nur noch auf die begrenze Speicherpflicht nach den §§ 175, 176 TKG weitgehend fortbestehen.

Fortbestehen kann auch die Abrufregelung („2. Tür“) zum Zwecke der Bekämpfung schwerer Kriminalität in § 100g Absatz 2 StPO, da darüber nur in Fällen abschließend benannter besonders schweren Straftaten und ausschließlich nach Anordnung durch das Gericht zugegriffen werden darf und über § 101a StPO auch strenge Verwendungsbeschränkungen gelten. Auch die mittelbaren Abrufregelungen zu Bestandsdatenauskünften nach § 100j Absatz 2 StPO und verschiedenen Fachgesetzen bedürfen keiner Änderung (dazu nachfolgend 3.).

1. Mindestspeicherung von Quellen-IP-Adressen und Port-Nummern

Zur Einführung einer Mindestspeicherung von Quellen-IP-Adressen und Port-Nummern wird zunächst der Kreis der verpflichteten Telekommunikationsunternehmen in § 175 StPO auf Internetzugangsdienste für Endnutzer beschränkt und der Umfang der zu speichernden Verkehrsdaten in § 176 TKG auf IP-Adressen, die der Quelle einer Verbindung zugewiesen sind (Quellen-IP-Adressen) und eventuell vergebener Port-Nummern begrenzt (vgl. zur Funktionsweise von IP-Adressen bei der Internetnutzung etwa Wildberg/Lee-Wunderlich, CCZ 2023, 281). Auch die Speicherung von korrespondierenden Benutzer- und Anschlusskennungen sowie von Datum und Uhrzeit in Bezug auf Beginn und Ende der Internetnutzung unter der zugewiesenen Quellen-IP-Adresse bleibt in § 176 TKG weiterhin notwendig. Eine Speicherung der im Internet aufgerufenen Adressen (Uniform Ressource Locator – URL – bzw. IP-Adresse des Ziels) ist nicht vorgesehen.

Diese Regelungen stehen bereits im Einklang mit den Anforderungen aus der Rechtsprechung des EuGH aus dem Urteil vom 20. September 2022 – C-793/19 und C-794/19–:

So stellt die Speicherung von „Quellen-IP-Adressen“ für einen Zeitraum von drei Monaten zwar laut der EuGH-Entscheidung vom 20. September 2022 einen schweren Eingriff in die in den Art. 7 und 8 der GRCh verankerten Grundrechte dar, da auch solche IP-Adressen es ermöglichen könnten, genaue Schlüsse auf das Privatleben des Nutzers des betreffenden elektronischen Kommunikationsmittels zu ziehen, und damit abschreckende Wirkung in Bezug auf die Ausübung der in Art. 11 GRCh garantierten Freiheit der Meinungsäußerung zu haben (EuGH a. a. O. Rn. 100). Die Bekämpfung schwerer Kriminalität stellt jedoch einen legitimen Zweck dar, um diesen Eingriff zu rechtfertigen (EuGH a. a. O. Rn. 102).

Zudem hat der EuGH in seiner Entscheidung vom 30. April 2024 hervorgehoben, dass nicht jede allgemeine und unterschiedslose Vorratsspeicherung eines unter Umständen umfangreichen Bestands der von einer Person innerhalb eines bestimmten Zeitraums genutzten statischen und dynamischen IP-Adressen zwangsläufig einen schweren Eingriff in die durch die Art. 7, 8 und 11 der Charta garantierten Grundrechte darstellt. Die den Betreibern elektronischer Kommunikationsdienste durch eine Rechtsvorschrift im Sinne von Art. 15 Absatz 1 der Richtlinie 2002/58 auferlegte Pflicht, die allgemeine und unterschiedslose Vorratsspeicherung der IP-Adressen sicherzustellen, kann gegebenenfalls durch das Ziel der Bekämpfung von Straftaten im Allgemeinen gerechtfertigt sein, wenn tatsächlich ausgeschlossen ist, dass diese Speicherung schwere Eingriffe in das Privatleben des Betroffenen zur Folge haben kann, die darauf beruhen, dass insbesondere durch eine Verknüpfung dieser IP-Adressen mit einem von den Betreibernebenfalls gespeicherten Satz von Verkehrs- oder Standortdaten die Möglichkeit besteht, genaue Schlüsse in Bezug auf ihn zu ziehen.

Die Speicherung von „Quellen-IP-Adressen“ für einen Zeitraum von drei Monaten ist zudem zur Bekämpfung schwerer Kriminalität geeignet. Die Speicherung solcher IP-Adressen sowie der die Identität der Nutzer elektronischer Kommunikationsmittel betreffenden Daten kann zur Bekämpfung schwerer Kriminalität beitragen, da diese Daten es ermöglichen, die Personen zu identifizieren, die solche Kommunikationsmittel im Zusammenhang mit der Vorbereitung oder Begehung einer zur schweren Kriminalität zählenden Tat verwendet haben (EuGH vom 20. September 2022, a. a. O. Rn. 98). Zusätzlich zur Speicherung der IP-Adresse wird aber in bestimmten Fällen noch die sogenannte Port-Nummer benötigt. Da der Adressbereich der IPv4-Adressen weitgehend ausgeschöpft ist, werden durch die Internetzugangsdienste den Kunden oft keine öffentlichen IPv4-Adressen zugeordnet. Hier findet dann das sogenannte „Natting“ (NAT = Network Address Translation) statt. Dabei wird beim Internetzugangsdienst einem Kunden nur temporär eine öffentliche IP-Adresse zugeteilt (vgl. dazu BeckOK StPO/Bär, 50. Ed., § 100g Rn. 11). Eine Zuordnung einer IP-Adresse zu einem Anschlussinhaber ist dann nur mitsamt der Port-Nummer möglich (Bundesbeauftragter für den Datenschutz und die Informationsfreiheit, Stellungnahme zu BT-Drs. 20/3687, S. 3; Witting, Stellungnahme zu BT-Drs. 20/3687, S. 2). Ohne Speicherung auch der Port-Nummer wären die gespeicherten IP-Adressen in vielen Fällen nur bedingt zur Identifizierung der Anschlussinhaber geeignet (Bundeskriminalamt, Stellungnahme zu BT-Drs. 20/3687, S. 1). Das Merkmal der EuGH-Rechtsprechung „IP-Adresse der Quelle einer Verbindung“ ist deswegen – nicht zuletzt im Hinblick auf die faktische Vorgehensweise der Internetzugangsdienste – als partiell ausfüllungsbedürftige technische Leerstelle zu

verstehen und belässt gesetzgeberische Gestaltungsspielräume zur Speicherverpflichtung auch der Port-Nummer (Gutmann/Wollenschläger, GSZ 2023, 249, 255 m. w. N.).

Eine Mindestspeicherung von IP-Adressen ist zudem auch für die Bekämpfung schwerer Kriminalität im Darknet geeignet, insbesondere in Bezug auf schweren sexuellen Missbrauch von Kindern und die Verbreitung kinderpornografischer Inhalte. Obwohl 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. Den Ermittlungsbehörden gelingt es – wenn auch mit hohem Aufwand in Form personeller und technischer Ermittlungsmaßnahmen – selbst im Darknet regelmäßig, Täter aus der Anonymität zu holen und IP-Adressen zu ermitteln (Deutscher Richterbund, Stellungnahme zu BT-Drs. 20/3687, S. 3 ff.). In den Ermittlungsverfahren gegen die Betreiber der kinderpornografischen Darknet-Plattformen „Elysium " (LG Limburg, Urteil vom 7. März 2019 – 1 KLs 3 Js 73019/18 –; BGH, Beschluss vom 15. Januar 2020 –2 StR 321/19) und „BoysTown" (LG Frankfurt a. M., Urteil vom 6. Dezember 2022 – 5/08 KLs 4881 Js 250066/21) sind Betreiber nur deswegen identifiziert und verurteilt worden, weil IP-Adressen, mit der sie sich auf Servern der Tätergruppierung angemeldet hatten, im Rahmen einer Server-Überwachung festgestellt und bei dem Internetdienstanbieter einem Anschlussinhaber zugeordnet werden konnten. Auch einzelne Betreiber der Darknet-Plattform „WallStreet Market" konnten nur auf diesem Weg identifiziert und wegen bandenmäßigen Handeltreibens mit Betäubungsmitteln verurteilt werden (LG Frankfurt a. M., Urteil vom 2. Juli 2021 – 5/08 KLs 5240 Js 257463/19; BGH, Beschluss vom 2. Juni 2022 – 2 StR 12/22). Bei der Nutzung anderer Internetzugangsdienst ohne entsprechende Speicherung wäre eine Identifizierung der Betreiber und eine Aufklärung von Fällen des schweren sexuellen Missbrauchs von Kindern bzw. des bandenmäßigen Handeltreibens mit Betäubungsmitteln nicht möglich gewesen (Krause, Stellungnahme zu BT-Drs. 20/3687, S. 6).

Eine Speicherung von „Quellen-IP-Adressen" und eventuell vergebener Port-Nummern für einen Zeitraum von drei Monaten ist zur Bekämpfung schwerer Kriminalität auch erforderlich, da kein milderes, zur Zielerreichung gleich geeignetes Mittel vorliegt. In Fällen einer im Internet begangenen Straftat, bei denen die IP-Adresse der einzige Anhaltspunkt zur Identifizierung der tatverdächtigen Person sein kann, ist es notwendig, über die den Strafverfolgungsbehörden bekannten IP-Adressen – und gegebenenfalls die Port-Nummer – den Anschlussinhaber des zur Tatbegehung genutzten Internetzugangs zu ermitteln, um darüber die tatverdächtige Person identifizieren zu können (EuGH vom 20. September 2022, a. a. O. Rn. 100). Für eine solche Identifizierung einer noch unbekannten tatverdächtigen Person bietet das „Quick-Freeze"-Verfahren aus Sicht der Strafverfolgungspraxis keinen Nutzen, sofern die relevanten Daten zum Zeitpunkt des Auskunftsersuchens nicht mehr oder unvollständig gespeichert sind, da entsprechende Daten bei Telekommunikations-Anbietern nur zu bekannten Anschlussinhabern eingefroren werden können (vgl. Bund Deutscher Kriminalbeamter, Stellungnahme zu BT-Drs. 20/3687, S. 2; Bundeskriminalamt, Stellungnahme zu BT-Drs. 20/3687, S. 2; Deutscher Richterbund, Stellungnahme zu BT-Drs. 20/3687, S. 5; Krause, ZRP 2023, 169). Zu diesem Ergebnis ist auch im Jahr 2020 veröffentlichte Studie der Europäischen Kommission zur Speicherung nichtinhaltsbezogener elektronischer Kommunikationsdaten für Strafverfolgungszwecke gekommen (European Commission, Study on the retention of electronic communications non-content data for law enforcement purposes, 2020, S. 20).

Dementsprechend hat eine Abfrage auf EU-Ebene im Dezember 2021 ergeben, dass lediglich ein Mitgliedsstaat das „Quick-Freeze"-Verfahren ins nationale Recht umgesetzt hat. Dieser Mitgliedsstaat hat diesen Ansatz indes als nicht erfolgreich bewertet. Auch aus den übrigen Mitgliedsstaaten gab es massive Bedenken, weil sich die Strafverfolgung bei einem „Quick-Freeze"-Mechanismus abhängig von dem Speicherverhalten der Provider macht. Die Daten könnten damit nur erfasst werden, wenn und soweit sie bei den Betreibern beispielsweise zu Abrechnungszwecken noch vorhanden seien, so dass ein einheitlicher europaweiter Ansatz damit nicht gewährleistet werden könne (vgl. Drahtbericht BRUEEU_2021-12-23_64957). Mithin musste die Bundesregierung im Oktober 2022 einräumen, dass das Quick Freeze-Verfahren innerhalb der Europäischen Union nur in Österreich existiert (vgl. Antwort auf die schriftliche Frage, BT-Drs. 20/3987).

Letztlich besteht auch unionsrechtlich kein Vorrang des „Quick-Freeze"-Verfahrens gegenüber einer Speicherung von IP-Adressen (EuGH vom 20. September 2022, a. a. O. Rn. 75, 121). In Fällen, in denen die IP-Adresse der einzige Anhaltspunkt zur Identifizierung der tatverdächtigen Person ist, sind auch keine anderen – gleichwohl individuell eingriffsintensiveren – Maßnahmen wie eine Überwachung der Telekommunikation nach den §§ 100a, 100g, 100k StPO oder gar eine Online-Durchsuchung gemäß § 100b StPO möglich. In diesen Fällen ist die Straftat nur aufklärbar, wenn die tatrelevante IP-Adresse bei dem Internetzugangsanbieter einem Anschlussinhaber zugeordnet werden kann (Bundeskriminalamt, Stellungnahme zu BT-Drs. 20/3687, S. 2).

Im Hinblick auf die Begrenzung der zu speichernden Daten und der Notwendigkeit der Speicherung von „Quellen-IP-Adressen“ zum Zwecke der Bekämpfung schwerer internetbezogener Kriminalität wie insbesondere der Bekämpfung des Kindesmissbrauchs steht eine Speicherung der „Quellen-IP-Adressen“ für eine Dauer von drei Monaten in einem angemessenen Verhältnis zur Schwere des Eingriffs und überschreitet nicht das im Hinblick auf das verfolgte Ziel absolut Notwendige (vgl. EuGH vom 20. September 2022, a. a. O. Rn. 59, 63, 68). Dabei sind in einer Gesamtabwägung – neben den bereits genannten widerstreitenden Rechten und berechtigten Interessen im Zusammenhang mit einer Vorratsdatenspeicherung – insbesondere folgende Gesichtspunkte berücksichtigt worden (vgl. dazu auch Gutmann/Wollenschläger, GSZ 2023, 249, 257; Puschke, GSZ 2024, 23, 26 f, jeweils m. w. N.):

- Bei der Schwere des Eingriffs ist festzuhalten, dass die Speicherpflicht auf „Quellen-IP-Adressen“ beschränkt ist und von einer wesentlich eingriffsintensiveren anlasslosen Speicherung der Standortdaten von Mobilfunkendgeräten abgesehen wird. Eine solche Speicherung alleine der „Quellen-IP-Adressen“ ist weniger zur abstrakten Gefährdung des Privatlebens geeignet und insofern mit einer geringeren Eingriffsintensität verbunden als die Speicherung sonstiger Verkehrsdaten. So hat der EuGH in seinem Urteil vom 6. Oktober 2020 – C-511/18, C-512/18 und C-520/18547 – festgehalten, dass IP-Adressen zwar zu den Verkehrsdaten gehörten, aber ohne Anknüpfung an eine bestimmte Kommunikation erzeugt würden und in erster Linie dazu dienten, über die Betreiber elektronischer Kommunikationsdienste die natürliche Person zu ermitteln, der ein Endgerät gehört, von dem aus eine Kommunikation über das Internet stattfindet (Rn. 152). Sofern im Bereich von E-Mail und Internettelefonie nur die „Quellen-IP-Adressen“ gespeichert würden und nicht die des Adressaten einer Kommunikation, ließe sich diesen Adressen als solchen keine Information über die Dritten entnehmen, mit denen die Person, von der die Kommunikation ausging, in Kontakt stand (Rn. 152). Diese Kategorie von Daten weise daher einen geringeren Sensibilitätsgrad auf als die übrigen Verkehrsdaten (Rn. 152). Damit kann allein auf Grundlage der zu speichernden Internetdaten nicht das gesamte „Surfverhalten“ von Internetnutzern nachvollzogen werden (so ausdrücklich Roßnagel, in: Geppert/Schütz, TKG, 5. Aufl., § 176 Rn. 24).

- Um auch hinsichtlich der zusätzlichen Speicherung der Port-Nummern den Eingriff so gering wie möglich zu halten, wird die Speicherpflicht auf die Fälle begrenzt, in denen eine zusätzlich zu einer mehrfach vergebenen IPv4 eine Port-Nummer vergeben worden ist und diese auch zur Identifizierung des Endkunden erforderlich ist (so ausdrücklich Bundesbeauftragter für den Datenschutz und die Informationsfreiheit, Stellungnahme zu BT-Drs. 20/3687, S. 3; vgl. auch Witting, Stellungnahme zu BT-Drs. 20/3687, S. 2). Durch eine solche Reduzierung des Speicherumfangs bleibt eine unmittelbare Protokollierung des Surfverhaltens der Internetnutzer, etwa von Daten über aufgerufene Internetseiten oder Diensten elektronischer Post, weiterhin ausgeschlossen. Ihr zusätzlich generierter Informationswert ist vielmehr von der Ebene des Datentransports abhängig, auf der die gegenständliche Port-Nummer zugewiesen und Gegenstand der Mindestspeicherung wird (vgl. ausführlich zur Frage der Eingriffsintensität der zusätzlichen Speicherung von Port-Nummern Gutmann/ Wollenschläger, GSZ 2023, 249, 254 ff.).

- Soweit als Beleg für die behauptete Unwirksamkeit einer Verkehrsdatenspeicherung die Studie des Max-Planck-Instituts für ausländisches und internationales Strafrecht aus dem Jahre 2011 „Schutzlücken durch Wegfall der Vorratsdatenspeicherung?“ herangezogen wird, ist darauf hinzuweisen, dass diese Studie durchgreifender wissenschaftlicher Kritik ausgesetzt ist. Das Ergebnis der Studie, dass der Wegfall der Vorratsdatenspeicherung im Jahre 2010 nicht als Ursache für Veränderungen bei der Aufklärungsquote gelten könne, geht von falschen Voraussetzungen aus. Bei der Beurteilung der Auswirkungen des Wegfalls der Verkehrsdatenspeicherung im Jahre 2010 auf die Aufklärungsquote ist zu berücksichtigen, dass die Pflicht zur Speicherung für den Bereich der Internetzugangsanbieter zu keinem Zeitpunkt in dem gesetzlich vorgesehenen Umfang zum Tragen gekommen ist, weil die erste einstweilige Anordnung des BVerfG vom 11. März 2008 (NStZ 2008, 290) bereits vor Geltung der Verkehrsdatenspeicherung für die Internetprovider ab dem 01. Januar 2009 die Verwendung der Daten eingeschränkt hatte. Nach dem genannten Beschluss des BVerfG war die Übermittlung der allein nach § 113a TKG auf Vorrat gespeicherten Verkehrsdaten an die Strafverfolgungsbehörden bis zur Entscheidung in der Hauptsache auf die Fälle des § 100g Absatz 1 Satz 1 Nr. 1 StPO, also auf die Fälle der „Straftat von erheblicher Bedeutung“, beschränkt. Das bedeutet: Für das Feld der Internetkriminalität hat sich die Verkehrsdatenspeicherung nie in vollem Umfang positiv auswirken können. Dies bedingt zwangsläufig, dass ihr Wegfall auch nicht wesentlich negativ bei den Aufklärungsquoten zu Buche schlagen konnte. Hinzu kommt, dass sich in den vergangenen Jahren das gesellschaftliche Leben und damit einhergehend auch die Kriminalität immer weiter ins Internet verlagert hat. Während die

Straftaten der Polizeilichen Kriminalstatistik (PKS) zwischen 2015 bis 2022 insgesamt um über 11 Prozent zurückgegangen sind, sind „digitale“ Straftaten wie etwa Straftaten unter Nutzung des Tatmittels Internet, Computerkriminalität bzw. Cybercrime, Hasspostings oder die Verbreitung pornografischer Inhalte gegen den allgemeinen Trend stark gestiegen (Bundeskriminalamt, Stellungnahme zu BT-Drs. 20/3687, S. 2). Bei der Frage der Erforderlichkeit einer Speicherung von IP-Adressen ist daher nicht alleine auf die messbaren Zahlen der PKS und die feststellbare Aufklärungsrate als sog. „Hellfeld“ abzustellen. Vielmehr muss die Gesamtentwicklung der internetbezogenen Kriminalität und der Verlagerung der Kriminalität in den digitalen Raum in den Blick genommen werden. Denn nach repräsentativen Opferbefragungen ist von einem wesentlich höheren „Dunkelfeld“ nicht angezeigter Straftaten auszugehen. So sind nach einer im Januar 2024 veröffentlichten Studie des Branchenverbandes BITKOM e. V. insgesamt 67 Prozent der Internetnutzerinnen und -nutzer in Deutschland im Jahr 2023 Opfer von Cyberkriminalität geworden. Und nach einer im September 2023 veröffentlichten Studien des Branchenverbandes BITKOM e. V. sehen sich 52 Prozent der befragten Unternehmen durch Cyberattacken in ihrer Existenz bedroht. In einer im Februar 2024 veröffentlichten empirische Studien des Kompetenznetzwerks gegen Hass im Netz gaben 15 Prozent der Befragten an, selbst schon von Hass im Netz betroffen gewesen zu sein – darunter knapp jede dritte Frau im Alter von 16 bis 24 Jahren. Im Rahmen einer im November 2022 veröffentlichen Studie der Landesanstalt für Medien Nordrhein-Westfalen zu „Cybergrooming“ haben ein Viertel der repräsentativ befragten Kinder und Jugendlichen angegeben, bereits im Netz von Erwachsenen zu einer Verabredung aufgefordert worden zu sein.

– Eine messbare Steigerung der Kriminalität über das Tatmittel Internet ist insbesondere im Zusammenhang mit dem Besitz und der Verbreitung kinder- und jugendpornografische Inhalte festzustellen. Veränderungen im Online-Kommunikationsverhalten haben in den letzten Jahren zu einer massenhaften Verbreitung der einschlägigen Inhalte beigetragen. Kinderpornografische Inhalte werden häufig über Messenger-Dienste, soziale Plattformen und audiovisuelle Plattformen verbreitet. Die in der PKS erfassten Fälle sind von knapp 6.500 im Jahr 2015 auf knapp 45.000 im Jahr 2022 gestiegen, wobei über 20.000 zusätzliche, trotz intensiver Ermittlungen nicht aufklärbare Fälle mit Deutschlandbezug bereits keinen Eingang in die PKS finden konnten (Bundeskriminalamt, Stellungnahme zu BT-Drs. 20/3687, S. 4). Die Hauptursache für den deutlichen Anstieg der Fallzahlen ist ein gestiegenes Hinweisaufkommen U.S.-amerikanischer Internetdienstanbieter über das U.S.-amerikanische National Center for Missing & Exploited Children (NCMEC). Insgesamt gingen im Jahr 2022 beim Bundeskriminalamt ca. 136.450 Hinweise auf kinderpornografische Inhalte durch das NCMEC ein. Rund zwei Drittel dieser Meldungen (ca. 89.850 Hinweise) waren nach deutschem Recht strafrechtlich relevant und enthielten in der Regel die zur Tatbegehung genutzte IP-Adresse sowie ggf. weitere Ermittlungsansätze wie z. B. Telefonnummern oder E-Mail-Adressen. Vergleichbare Hinweise deutscher oder europäischer Internetdienstanbieter für E-Mail, Messenger oder Cloud-Speicherung liegen dagegen nicht vor, so dass auch die erschreckend hohen NCMEC-Zahlen nur einen Ausschnitt des tatsächlich vorkommenden Straftataufkommens abbilden können und auch insofern von einem wesentlich höheren „Dunkelfeld“ auszugehen ist. Um dieser steigenden digitalen Kriminalität effektiv zu begegnen, ist eine Mindestspeicherung von „Quellen-IP-Adressen“ und eventuell vergebener Port-Nummern unumgänglich.

– Ohne Mindestspeicherung von IP-Adressen kann den Strafverfolgungsbehörden in Fällen, in denen die IP-Adresse der einzige Anhaltspunkt zur Identifizierung der tatverdächtigen Person und zur Aufklärung der Straftat ist, das einzige Mittel zur Identifizierung de facto vorenthalten werden, was zu einer systemischen Straflosigkeit führen kann (so ausdrücklich Generalanwalt beim EuGH, Schlussantrag vom 28. September 2023 – C-470/21 – Rn. 80 m. w. N.). Nach einer Mitteilung der Bundesregierung aus Januar 2022 konnten in den Jahren 2017 bis 2021 von über 300.000 Hinweisen des U.S.-amerikanischen NCMEC zu Kinderpornografie im Internet etwa 19.000 Fälle nicht aufgeklärt werden, in denen die IP-Adresse der einzige Ermittlungsansatz war und die IP-Adresse mangels Speicherung nicht abfragbar war (BT-Drs. 20/534, S. 27 f.). Der Umkehrschluss, dass in über 90 Prozent aller Fälle eine Aufklärung über die IP-Adresse möglich ist (so etwa Roßnagel, ZD 2022, 650, 654), ist nicht zutreffend. Nicht umfasst waren bei dieser Angabe die – mangels zusätzlicher Informationen wie etwa der Port-Nummer – „nicht beauskunftbaren“ IP-Adressen (Bundeskriminalamt, Stellungnahme zu BT-Drs. 20/3687, S. 5; Krause, Stellungnahme zu BT-Drs. 20/3687, S. 7). Die Quote der nicht aufklärbaren Fälle liegt also noch höher.

– Tatrelevante bzw. ermittlungsrelevante IP-Adressen können ohne Mindestspeicherung derzeit überwiegend nicht erfolgreich abgefragt und damit Straftaten nicht aufgeklärt werden. Das Bundeskriminalamt hat im Rahmen einer händischen Auswertung zu 1.000 strafrechtlich relevanten NCMEC-Vorgängen vielmehr klargestellt, dass bei den Internetzugangsdiensten nur 41 Prozent der IP-Adressen einem Nutzeranschluss zuge-

ordnet werden konnten, obwohl in dem NCMEC-Prozess die Meldungen tagesaktuell in Bearbeitung genommen werden, die Strafbarkeitsprüfung durch das BKA ohne größeren Zeitverzug durchgeführt und die Bestandsdatenanfrage bei hinreichender Erfolgswahrscheinlichkeit unmittelbar gestellt wird. Etwa 34 Prozent der angelieferten IP-Adressen waren bei den Internetzugangsdiensten trotzdem bereits nicht mehr gespeichert und weitere 24 Prozent aus anderen Gründen, etwa aufgrund einer zusätzlich zur Identifizierung erforderlichen, aber nicht gespeicherten Port-Nummer, nicht beauskunftbar (Bundeskriminalamt, Stellungnahme zu BT-Drs. 20/3687, S. 3 ff.).

– Bei dieser Statistik ist zusätzlich zu berücksichtigen, dass in dem NCMEC-Prozess des Bundeskriminalamts die tatrelevanten IP-Adressen automatisiert durch die Internetdienstanbieter erhoben und an die Polizeibehörden weitergeleitet sowie dort tagesaktuell abgefragt werden. In allen anderen Ermittlungsverfahren, in denen tatrelevante IP-Adressen erst später polizeilich bekannt werden oder durch (zeit-)aufwändige Maßnahmen zunächst ermittelt werden müssen, ist angesichts des unvermeidlichen Zeitablaufs von einer noch wesentlich geringeren Aufklärungsrate als 41 Prozent auszugehen (Bundeskriminalamt, Stellungnahme zu BT-Drs. 20/3687, S. 5).

– Diese geringe Aufklärungsrate von IP-Adressen beruht darauf, dass Internetzugangsdienste die an ihre Kunden vergebenen IP-Adressen nur für maximal sieben Tage speichern. Gemäß § 9 Absatz 1 Satz 1 TTDSG und § 12 Absatz 1 und 4 TTDSG dürfen zwar Verkehrsdaten zur Entgeltabrechnung sowie zur Störungsbeseitigung und zur Missbrauchsbekämpfung gespeichert werden. Jedoch sind erhobene Daten nach § 9 Absatz 1 Satz 2, § 12 Absatz 2 TTDSG unverzüglich zu löschen, sobald sie für die vorgenannten Zwecke nicht mehr erforderlich sind. Wie lange IP-Adressen gespeichert werden dürfen, unterscheidet sich danach, auf welcher Rechtsgrundlage entsprechende Daten erhoben und gespeichert werden können. Für Abrechnungszwecke dürfen Verkehrsdaten gemäß § 10 Absatz 2 Satz 2 TTDSG bis zu sechs Monate nach Versendung der Rechnung gespeichert werden. Bei den mittlerweile im Bereich der Festnetzanschlüsse und der Mobilfunktelefonie zum Regelfall gewordenen Tarifen mit Pauschalvergütung („Flatrate“, vgl. dazu Bundesnetzagentur, Nutzung von OTT-Kommunikationsdiensten in Deutschland, Bericht 2020) besteht aber bereits keine Notwendigkeit für die Dienstanbieter, IP-Adressen zu Abrechnungszwecken zu speichern (BeckOK StPO/Bär, 50. Ed., TTDSG § 9 Rn. 8). Dies macht regelmäßig eine Löschung der IP-Adressen unmittelbar nach dem Ende der Verbindung erforderlich. Auch bei volumenbegrenzten Verträgen werden aus Gründen des Datenschutzes nur Datenvolumen und Nutzerkennung, nicht aber IP-Adressen gespeichert (vgl. zum Ganzen Bundesbeauftragter für Datenschutz und Informationssicherheit, Leitfaden für datenschutzgerechte Speicherung von Verkehrsdaten, Stand: 30. September 2022). Zum Zwecke der Störungsbeseitigung werden dagegen gemäß § 12 Absatz 1 und 4 TTDSG Kennung der beteiligten Anschlüsse, Beginn und Ende der jeweiligen Verbindung gespeichert – bei mobilen Anschlüssen auch Standortdaten. In diesem Zusammenhang besteht für Internetzugangsdienste die Möglichkeit, die vergebenen IP-Adressen und die Verknüpfungen zu den Benutzerkennungen für einen kurzen Zeitraum von bis zu sieben Tagen zum Zwecke der Erkennung, Eingrenzung und Beseitigung von Störungen zu speichern (vgl. BGH NJW 2014, 2500: sieben Tage; OLG Köln BeckRS 2016, 898: vier Tage). Danach sind diese Daten unverzüglich zu löschen. Eine solche unternehmensinterne Speicherung wird von einigen Internetzugangsanbietern bei Festnetzanschlüssen für maximal sieben Tage durchgeführt; andere Anbieter speichern kürzer, nicht alle Verbindungen oder gar nicht (Bundeskriminalamt, Stellungnahme zu BT-Drs. 20/3687, S. 2). Zudem unterbleibt insbesondere im Mobilfunkbereich häufig das Hinzuspeichern der vergebenen Port-Nummer zur IP-Adresse, die jedoch erforderlich ist, um eine Identifizierung des Anschlussinhabers zu ermöglichen (Bundeskriminalamt, Stellungnahme zu BT-Drs. 20/3687, S. 1).

– Zudem ist eine Speicherung von IP-Adressen für die Bekämpfung schwerer Kriminalität nicht nur notwendig, um ausschließlich die IP-Adresse der unmittelbar zur Tatbegehung verwendeten Internetverbindung aufzuklären. Ohne automatisierte Erfassung und Weiterleitung dieser tatrelevanten IP-Adressen durch Internetdienstanbieter – wie in dem beschriebenen NCMEC-Prozess des Bundeskriminalamts – liegen diese IP-Adressen zum Zwecke der Ermittlungen schlichtweg nicht vor, da Opfer entsprechender Kriminalität diese IP-Adressen nicht erheben oder speichern. In diesen Fällen sind umfangreiche weitere Ermittlungen zur Identifizierung der unbekannten Tatverdächtigen erforderlich, wie etwa in Bezug auf in sozialen Netzwerken oder in Messengern verwendete Kennungen, auf verwendete E-Mail-Adressen, Kennungen bei Messenger-Diensten, Profile in sozialen Netzwerken oder Mobilrufnummern und die mit den jeweiligen Nutzerkonten verbundenen Identitätsdaten. Im Rahmen der Abwägung ist daher durchaus zu berücksichtigen, dass tatverdächtige Personen schwerer internetbezogener Kriminalität theoretisch auch mit anderen Mitteln identifiziert

werden könnten. Bei solchen kann es jedoch erforderlich sein, die Online-Aktivitäten des Internetnutzers zu untersuchen werden, so dass solche Ermittlungen individuell zu einer größeren Eingriffstiefe führen können, als die Abfrage einer tatrelevanten IP-Adresse (so ausdrücklich Generalanwalt beim EuGH, Schlussantrag vom 28. September 2023 – C-470/21 – Rn. 83 f.).

– Auch diese weitergehenden Ermittlungen zur Identifizierung unbekannter Tatverdächtiger über E-Mail-Adressen, Kennungen bei Messenger-Diensten oder Profilen in sozialen Netzwerken sind oftmals erfolglos. Dies beruht darauf, dass diese Nutzerprofile kostenlos und ohne Identitätskontrolle durch die Verwendung frei erfundener Personalien registriert werden können. Nach § 172 Absatz 1 TKG besteht zwar eine Pflicht zur Erhebung solcher Daten für nummerngebundene interpersonelle Telekommunikationsdiente wie Telefon- oder Internetzugangsanbieter, wobei gemäß § 172 Absatz 2 TKG nur bei Prepaid-Mobilfunkverträgen die Daten zu verifizieren sind. Für nummernunabhängige Telekommunikationsdiente für E-Mail oder Messenger besteht dagegen keine Speicherpflicht, sondern lediglich ein „Löschverbot“ nach § 172 Absatz 3 TKG. Für Telemediendienste wie Soziale Netzwerke, Foren oder Blogs besteht gemäß § 22 TTDSG überhaupt keine Speicherverpflichtung. Diese durch die Strafverfolgungsbehörden gemäß § 100j Absatz 1 StPO in Verbindung mit § 172 Absatz 3, § 174 Absatz 1 Satz 1, Absatz 3 TKG bzw. § 22 Absatz 1, 3 TTDSG abrufbaren Bestandsdaten sind daher oftmals nicht werthaltig. Die Internetzugangsdienste erheben dagegen verifizierte Personalien ihrer Kunden, um die Bezahlung der Dienstleitung sicherzustellen und Ansprüche notfalls gerichtlich durchzusetzen. Die Bestandsdaten bei Internetzugangsdiensten gemäß § 100j Absatz 2, 5 StPO und §§ 172, 174 Absatz 1 Satz 3, Absatz 5 TKG sind für die Strafverfolgungsbehörden daher wesentlich werthaltiger zum Zwecke der Identifizierung unbekannter Tatverdächtiger (Krause, Stellungnahme zu BT-Drs. 20/3687, S. 4 f.). Das zeigt sich auch an einer Statistik des Bundeskriminalamts, wonach in dem NCMEC-Prozess durch weitere und wesentlich aufwändigere Ermittlungen im Hinblick auf ebenfalls mitgeteilte Mobilrufnummern oder E-Mail-Adressen – zusätzlich zu den über die tatrelevante IP-Adresse aufgeklärten Fällen – insgesamt 34 Prozent der bis dahin noch nicht aufgeklärten NCMEC-Vorgänge der weiteren Strafverfolgung zugeführt werden konnten (Bundeskriminalamt, Stellungnahme zu BT-Drs. 20/3687, S. 3 ff.).

– Mangels Mindestspeicherung von „Quellen-IP-Adressen“ und eventuell vergebener Port-Nummern sind in dem NCMEC-Prozess des Bundeskriminalamts auch in Bezug auf weitergehende Ermittlungen insgesamt 25 Prozent der Meldungen nicht aufklärbar – trotz automatisierter Erhebung der tatrelevanten IP-Adressen durch die Internetdienstanbieter und Weiterleitung an die Strafverfolgungsbehörden nahezu in Echtzeit, trotz tagesaktueller Strafbarkeitsprüfung, unmittelbarer Abfrage der IP-Adressen und somit insgesamt größtmöglicher Anstrengungen des Bundeskriminalamts. Über 20.000 strafrechtlich relevante NCMEC-Meldungen mussten daher im Jahr 2022 mangels fortbestehender Ermittlungsansätze durch die zuständige Staatsanwaltschaft eingestellt werden (Bundeskriminalamt, Stellungnahme zu BT-Drs. 20/3687, S. 3 ff.). Auch insoweit ist zu berücksichtigen, dass in allen anderen Ermittlungsverfahren, in denen tatrelevante IP-Adressen erst später polizeilich bekannt werden oder durch (zeit-)aufwändige Maßnahmen zunächst ermittelt werden müssen, angesichts des unvermeidlichen Zeitablaufs von einer noch wesentlich geringeren Aufklärungsrate auszugehen ist (Bundeskriminalamt, Stellungnahme zu BT-Drs. 20/3687, S. 5).

– Diese Zahlen nicht aufklärbarer Fälle internetbezogener Kriminalität, sind eindeutig zu hoch und können nicht weiter hingenommen werden. In einer Vielzahl dieser Fälle der Verbreitung von Kinderpornografie kommt es zum Realmissbrauch oder dauert ein solcher Missbrauch gar an. Jeder Realmissbrauch – gerade auch der schwere sexuelle Missbrauch von Kleinkindern – ist ein schweres Verbrechen, das in den Grenzen rechtsstaatlich zulässiger Instrumente maximal effektiv verfolgt werden muss (Deutscher Richterbund, Stellungnahme zu BT-Drs. 20/3687, S. 5). Schließlich hat der EuGH in dem Urteil vom 20. September 2022 – C-793/19 und C-794/19 – festgehalten, dass bei dem Gesichtspunkt der wirksamen Bekämpfung von Straftaten, deren Opfer u. a. Minderjährige und andere schutzbedürftige Personen sind, auch zu berücksichtigen sei, dass sich aus Art. 3, 4 und 7 GRCh auch positive Verpflichtungen der Behörden im Hinblick auf den Erlass rechtlicher Maßnahmen zum Schutz u. a. der körperlichen und geistigen Unversehrtheit der Menschen sowie des Privat- und Familienlebens ergeben können (EuGH a. a. O. Rn. 64 – vgl. zu entsprechenden „Schutzpflichten“ etwa Gutmann/Wollenschläger, GSZ 2023, 249, 250 f.). Zudem sei die Bekämpfung schwerer Kriminalität von größter Bedeutung für die Gewährleistung der öffentlichen Sicherheit und ihre Wirksamkeit in hohem Maß von der Nutzung moderner Ermittlungstechniken abhängig (EuGH a. a. O. Rn. 123).

- Auch für die Abwägung eines angemessenen Speicherzeitraums, deren Ausgangspunkt fachliche Erfordernisse sind (Gutmann/Wollenschläger, GSZ 2023, 249, 257), kann nicht alleine auf die messbaren Zahlen der PKS und die feststellbare Aufklärungsrate bzw. die Strafverfolgungsstatistik und die feststellbare Verurteilungsquote als sog. „Hellfeld“ abgestellt werden. Vielmehr muss die Gesamtentwicklung der internetbezogenen Kriminalität und der Verlagerung der Kriminalität in den digitalen Raum samt „Dunkelfeld“ in den Blick genommen. Wie bereits beschrieben konnten im Jahr 2022 alleine über 20.000 Hinweise auf strafbare kinderpornografische Inhalte bei deutschen Internetnutzern aus dem NCMEC-Prozess des Bundeskriminalamts mangels Beauskunftung der zur Tatbegehung genutzten IP-Adresse durch die Internetzugangsdienste und trotz intensiver Ermittlungen nicht aufgeklärt werden, so dass diese keinen Eingang in die PKS finden konnten (Bundeskriminalamt, Stellungnahme zu BT-Drs. 20/3687, S. 4). Würden nur diese 20.000 Fälle in der PKS eine Berücksichtigung finden, fiele die Aufklärungsquote von 89,1 Prozent auf knapp 60 Prozent und würde damit trotz größtmöglicher Anstrengungen des Bundeskriminalamts und der Länderpolizeien etwa der Aufklärungsquote von Straftaten mit dem Tatmittel Internet insgesamt entsprechen, bei deren Verfolgung jedoch kein vergleichbar hoher Aufwand zur Aufklärung betrieben werden kann. Jedenfalls ist die Aufklärungsquote in der PKS in diesem Kontext nur eingeschränkt aussagekräftig (Bundeskriminalamt, Stellungnahme zu BT-Drs. 20/3687, S. 4).
- Zur Beantwortung der Frage, welche Erfolgsquote im NCMEC-Prozess erreicht werden könnte, wenn eine einheitliche Speicherverpflichtung für IP-Adressen und gegebenenfalls vergebene Port-Nummern umgesetzt würde, hat das BKA eine technische Auswertung von etwa 66.000 strafrechtlich relevanten NCMEC-Vorgängen aus dem Jahr 2022 durchgeführt und hat das Alter der IP-Adressen in diesen Vorgängen in Relation zu einer hypothetischen Speicherverpflichtungen für Internetzugangsdienste von IP-Adressen und Port-Nummern gesetzt. Dabei konnte festgestellt werden, dass die Erfolgsquote im NCMEC-Prozess durch eine einheitliche gesetzliche Speicherverpflichtung erheblich gesteigert werden könnte, wobei der Effekt in den ersten Wochen besonders signifikant wäre. So würde die Erfolgsquote der Gewinnung von Identifizierungsansätzen allein anhand der IP-Adressen bei einer einheitlichen Speicherverpflichtung für 14 Tage von 41 Prozent auf über 80 Prozent gestiegen. Bei einer einmonatigen Speicherpflicht würde die Aufklärungsrate der IP-Adressen auf über 90 Prozent steigen (Bundeskriminalamt, Stellungnahme zu BT-Drs. 20/3687, S. 7). In einem Rechtsstaat sollte bei tatrelevanten IP-Adressen besonders in einem Prozess, in dem wie in dem NCMEC-Prozess zivilgesellschaftliche und staatliche Stellen mit größtmöglichen Anstrengungen zusammenarbeiten, eine größtmögliche Aufklärungsrate das zu erstrebende Ziel sein.
- Zudem hat das Bundeskriminalamt – wie bereits beschrieben – darauf hingewiesen, dass die Erfolgsquoten aus dem NCMEC-Verfahren in anderen Prozessen nicht erreicht werden können, bei denen tatrelevante IP-Adressen erst später bekannt werden oder zunächst aufwändig ermittelt werden müssen. Dies betrifft etwa schwere Kriminalität im Bereich Cybercrime, Organisierter Kriminalität oder komplexer Ermittlungsverfahren im Bereich des sexuellen Missbrauchs von Kindern und Jugendlichen, in denen tatrelevante IP-Adressen erst später polizeilich bekannt werden oder durch (zeit-)aufwändige Maßnahmen zunächst ermittelt werden müssen (Bundeskriminalamt, Stellungnahme zu BT-Drs. 20/3687, S. 7). In diesen Prozessen ist angesichts des unvermeidlichen Zeitablaufs auch bei einer einmonatigen Mindestspeicherung von IP-Adressen und gegebenenfalls vergebener Port-Nummern von einer noch wesentlich geringeren Aufklärungsrate auszugehen.

Deswegen ist ein Speicherzeitraum für IP-Adressen und gegebenenfalls vergebene Port-Nummern von drei Monaten angemessen, um das Ziel der Bekämpfung schwerer internetbezogener Kriminalität zu realisieren und überschreitet angesichts der hohen Gesamtzahlen schwerer internetbezogener Kriminalität, der nur kurzen und unvollständigen freiwilligen Speicherung der Internetzugangsdiensten und der daraus folgenden niedrigen Aufklärungsrate von tatrelevanten IP-Adressen nicht das im Hinblick auf das verfolgte Ziel absolut Notwendige. Gerade außerhalb des NCMEC-Bereichs sind nämlich im Einzelfall sehr bedeutende Verfahren wegen Kinderpornografie und sexuellem Missbrauch von Kindern betroffen. Hier besteht bei einer Mindestspeicherfrist von weniger als drei Monaten die erhebliche Gefahr, dass die IP-Adressen nicht mehr vorhanden sind – etwa infolge von zunächst erforderlichen, gegebenenfalls aufwändigen Rechtshilfemaßnahmen oder in Fällen, in denen die Täter unter Einsatz von Verschleierungstechniken operieren (etwa im Darknet oder mit VPN-Diensten). Einen Leerlauf der vorgesehenen Mindestspeicherpflicht gilt es jedoch gerade vor dem Hintergrund der erforderlichen effektiven Verfolgung von Kinderpornografie und sexuellem Missbrauch von Kindern zu verhindern. Deswegen hat auch die Ständige Konferenz der Innenminister und -senatoren der Länder mit Beschluss vom 16. Juni 2023 unter TOP 25 (dort unter Ziffer 3) gestützt auf den Bericht einer unter anderem zu diesem Zweck eingesetzten Bund-Länder-Projektgruppe eine Speicherfrist von sogar sechs Monaten für erforderlich erachtet.

Eine weitergehende und eingriffsintensivere Verpflichtung zur zusätzlichen Mindestspeicherung von Standortdaten bei mobiler Internetnutzung ist nicht vorgesehen, da eine nicht gezielte Speicherung und Übermittlung solcher Verkehrsdaten nach dem Urteil des EuGH vom 20. September 2022 – C-793/19, C-794/19 – zum Zwecke der Bekämpfung schwerer Kriminalität unionsrechtlich nicht möglich ist (Rn. 131).

2. Datenverwendungs- und Übermittlungsregelungen („1. Tür“)

Die Verpflichtungen zur Verwendung der Daten und zur Datensicherheit nach den §§ 177 bis 181 TKG, die sich dann nur noch auf die begrenze Speicherpflicht nach den §§ 175, 176 TKG beziehen, können – mit Ausnahme einzelner rein redaktioneller Änderungen – ganz überwiegend fortbestehen.

Diese Regelungen der §§ 177 bis 181 TKG erfüllen die aus dem Urteil des EuGH vom 20. September 2022 – C-793/19 und C-794/19 – folgenden Anforderungen, wonach nationale Rechtsvorschriften für eine allgemeine und unterschiedslose Vorratsspeicherung der IP-Adressen, die der Quelle einer Verbindung zugewiesen sind, durch klare und präzise Regeln sicherstellen müssten, dass bei der Speicherung der fraglichen Daten die für sie geltenden materiellen und prozeduralen Voraussetzungen eingehalten würden und dass die Betroffenen über wirksame Garantien zum Schutz vor Missbrauchsrisiken verfügten (EuGH a. a. O Rn. 75, 101). Diese Feststellung hatte auch das BVerwG in seinem Vorlagebeschluss vom 25. September 2019 – 6 C 12.18 – getroffen und ausgeführt, dass durch die Vorgaben der §§ 113d ff. TKG a. F. (§§ 178 ff. TKG n. F.) ein wirksamer Schutz der auf Vorrat gespeicherten Daten vor Missbrauchsrisiken sowie vor jedem unberechtigten Zugang gewährleistet sei (Rn. 29).

Dies betrifft insbesondere die Verwendungs- und Übermittlungsregelung in § 177 Absatz 1 Nr. 1 TKG, die den Abruf der zu einem Anschlussinhaber anlasslos gespeicherten Quellen-IP-Adressen zum Zwecke der Verfolgung schwerer Kriminalität gemäß § 100g Absatz 2 StPO ermöglicht.

Umstritten ist lediglich, ob die Rechtsprechung des EuGH so auszulegen ist, dass auch die Verwendungsregelung in § 177 Absatz 1 Nr. 3 TKG bestehen bleiben kann, wonach die gemäß § 176 TKG mindestgespeicherten Daten für eine Bestandsdatenauskunft nach § 174 Absatz 1 Satz 3 TKG anhand einer zu einem bestimmten Zeitpunkt zugewiesenen IP-Adresse (automatisiert) verwendet werden dürfen. Seit dem Urteil des EuGH vom 20. September 2022 – C-793/19 und C-794/19 – wird darüber diskutiert, ob eine solche mittelbare Verwendung von IP-Adressen durch Internetzugangsdiensten zur Ermöglichung der Beauskunftung von Identitätsdaten nur zum Schutz der nationalen Sicherheit, zum Zwecke der Bekämpfung schwerer Kriminalität und zur Verhütung schwerer Bedrohungen der öffentlichen Sicherheit möglich sei (Rn. 102, 131) oder ob sich die Zulässigkeit nach der Verwendung von „Identitätsdaten“ richte, die bereits für die Zwecke der Bekämpfung der Kriminalität und zum Schutz der öffentlichen Sicherheit im Allgemeinen zulässig sei (Rn. 99, 131). In dem Referentenentwurf des Bundesministeriums der Justiz (BMJ) für ein „Gesetz zur Einführung einer Sicherungsanordnung für Verkehrsdaten in der Strafprozessordnung“ sollte diese Möglichkeit durch eine Streichung der §§ 176 bis 181 TKG entfallen. Vertreter der Strafverfolgungspraxis haben sich jedoch für einen Erhalt ausgesprochen (Krause, ZRP 2023, 169, 171; ders. Stellungnahme zu BT-Drs. 20/3687, S. 13 f.).

Das BVerwG hat sich in den nicht tragenden Gründen seiner Urteile vom 14. August 2023 – 6 C 6.22 und 6 C 7.22 – zwar dahingehend geäußert, dass die Regelung in § 177 Absatz 1 Nr. 3, § 174 Absatz 1 Satz 3 TKG diese strengen unionsrechtlichen Anforderungen verfehle, da diese eine Beschränkung auf die Bekämpfung schwerer Kriminalität nicht vorsehe (Rn. 43) und eine unionsrechtskonforme Auslegung wegen des vom EuGH hervorgehobenen Grundsatzes der Bestimmtheit und Normenklarheit nicht in Betracht komme (Rn. 45).

Dabei ist jedoch zu berücksichtigen, dass diese von dem BVerwG in Bezug genommene Anforderung von dem EuGH in Bezug auf nationale Regelungen entwickelt worden ist, die den Zugang zu allen Verkehrs- und Standortdaten der Nutzer in Bezug auf sämtliche von ihnen genutzten elektronischen Kommunikationsmittel oder zumindest in Bezug auf die Festnetz- und Mobiltelefonie identifizierter Nutzer ermöglichten. Die Schwere des mit einer – von § 177 Absatz 1 Nr. 3, § 174 Absatz 1 Satz 3 TKG ermöglichten – Verknüpfung von Identitätsdaten mit einer IP-Adresse verbundenen Eingriffs ist jedoch weitaus geringer als die Schwere des Eingriffs, der sich aus dem Zugang zu sämtlichen Verkehrs- und Standortdaten einer Person ergibt, da diese Verknüpfung keine Anhaltspunkte liefert, die genaue Schlüsse auf das Privatleben der Zielperson zulassen (so ausdrücklich Generalanwalt beim EuGH, Schlussantrag vom 28. September 2023 – C-470/21 – Rn. 69, 71). Die anlasslose Speicherung der IP-Adressen hat den Zweck, die gespeicherten IP-Adressen zu einer tatrelevanten Benutzerkennung in Gänze an die Strafverfolgungsbehörden auszuliefern, um durch einen Abruf und eine entsprechende Auswertung nicht nur zukünftiger, sondern gerade auch zurückliegender Verbindungen einen „Blick in die Vergangenheit“ (Priebe,

EuZW 2017, 136) zu ermöglichen. Dieser schwerwiegende Eingriff kann – so der EuGH – nur für die Strafverfolgung schwerer Kriminalität zulässig sein. Bei einer Auskunft nach § 177 Absatz 1 Nr. 3, § 174 Absatz 1 Satz 3 TKG betrifft die Verwendung aber nur die Zuordnung und Übermittlung der Bestandsdaten („Identitätsdaten"), die mit einer durch die Strafverfolgungs-bzw. Sicherheitsbehörden mitgeteilten IP-Adresse verbunden sind. Die Übermittlung der einem Anschlussinhaber zu bestimmten Zeitpunkten zugewiesenen IP-Adressen ist dagegen nicht zulässig. Hinsichtlich der Eingriffstiefe der Verwendung muss daher zwischen der Verwendung und Übermittlung der Gesamtheit der gespeicherten Verkehrsdaten zu einer Person im Sinne des § 177 Absatz 1 Nr. 1 TKG und einer Verwendung einer einzelnen IP-Adresse zum Zwecke der Zuordnung und Übermittlung von Identitätsdaten gemäß § 177 Absatz 1 Nr. 3 TKG unterschieden werden (Krause, ZRP 2023, 169, 171).

Diese Unterscheidung entspricht auch der ständigen Rechtsprechung des BVerfG, wonach 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. Auch bedürfe es für entsprechende Bestandsdatenabfragen weder eines begrenzenden Rechtsgüter- oder Straftatenkatalogs noch eines Richtervorbehalt. Mit Beschluss vom 27. Mai 2020 – 1 BvR 1873/13, 1 BvR 2618/13 – hat das BVerfG ausgeführt, dass die Behörden bei einer Bestandsdatenauskunft unter Zuordnung dynamischer IP-Adressen keine Kenntnis der Verkehrsdaten erhielten, sondern lediglich personenbezogene Auskünfte über den Inhaber eines bestimmten Anschlusses, der von den Diensteanbietern unter Rückgriff auf die (anlasslos gespeicherten) Verkehrsdaten sowie gegebenenfalls weitere Daten wie etwa der Port-Nummer ermittelt worden sei. Da die Verwendung der Verkehrsdaten allein zu der Auskunft führe, welcher Anschlussinhaber unter einer den Sicherheitsbehörden bereits bekannten IP-Adresse zu einem bestimmten Zeitpunkt im Internet angemeldet war, bleibe ihr Erkenntniswert punktuell. Ausforschungen über einen längeren Zeitraum oder die Erstellung von Persönlichkeits- und Bewegungsprofilen ließen sich allein auf Grundlage solcher Auskünfte gerade nicht verwirklichen (Rn. 169, 171). Anders als für Abrufregelungen, die den Abruf der Gesamtheit bevorratend gespeicherter Verkehrsdaten ermöglichen und für die ein Richtervorbehalt grundsätzlich notwendig sei, bedürfe es für eine Auskunft über einen Anschlussinhaber, der unter nur punktueller und mittelbarer Verwendung von Verkehrsdaten ermittelt wurde, keiner zusätzlichen Sicherungen in Form einer vorbeugenden unabhängigen Kontrolle (Rn. 254). Auf diese Rechtsprechung hatte das BVerwG in seinem Vorlagebeschluss vom 25. September 2019 – 6 C 12.18 – noch selbst Bezug genommen (Rn. 30).

Entscheidend für eine Auslegung der EuGH-Rechtsprechung im hiesigen Sinne spricht jedoch, dass diese auch von dem Generalanwalt beim EuGH vertreten wird. In seinem Schlussantrag vom 28. September 2023 – C-470/21 – hat dieser sich für eine Verfeinerung der Rechtsprechung des EuGH zur Speicherung von Daten wie IP-Adressen, die mit Identitätsdaten verknüpft sind, und zum Zugang zu ihnen ausgesprochen (Rn. 78). Er hat die Ansicht vertreten, dass die Rechtsprechung des EuGH zur Schwere des durch die Speicherung von IP-Adressen und den Zugang zu ihnen verursachten Eingriffs in die Grundrechte nicht dahin ausgelegt werden sollte, dass ein solcher Eingriff immer ein schwerwiegender Eingriff sei, sondern dahin, dass er nur dann schwerwiegend sei, wenn die IP-Adressen zu einer umfassenden Nachverfolgung der Online-Aktivität des Internetnutzers führen und sehr genaue Schlüsse auf sein Privatleben zulassen könnten (Rn. 55). Diese Rechtsprechung des EuGH sei in Bezug auf nationale Regelungen entwickelt worden, die den Zugang zu allen Verkehrs- und Standortdaten der Nutzer in Bezug auf sämtliche von ihnen genutzten elektronischen Kommunikationsmittel oder zumindest in Bezug auf die Festnetz- und Mobiltelefonie identifizierter Nutzer ermögliche (Rn. 69). Die Schwere des Eingriffs bei einer Verknüpfung von Identitätsdaten mit einer IP-Adresse sei jedoch weitaus geringer als die Schwere des Eingriffs, der sich aus dem Zugang zu sämtlichen Verkehrs- und Standortdaten einer Person ergibt, da diese Verknüpfung keine Anhaltspunkte liefere, die genaue Schlüsse auf das Privatleben der Zielperson zulasse (Rn. 71). Die Rechtsprechung des EuGH sei daher dahingehend auszulegen, dass sie nationalen Regelungen zu einer Verpflichtung der Betreiber elektronischer Kommunikation zur Vorratsspeicherung von IP-Adressen und den dazugehörigen Identitätsdaten und dem Zugriff darauf durch eine Verwaltungsbehörde zum Schutz von Urheberrechten gegen Urheberrechtsverletzungen im Internet nicht entgegenstehe (Rn. 90). Nach diesem Verständnis der Rechtsprechung des EuGH und des BVerfG ist die von § 177 Absatz 1 Nr. 3 TKG eröffnete Möglichkeit der mittelbaren Verwendung von IP-Adressen durch Internetzugangsdienste zur Ermöglichung der Beauskunftung von Identitätsdaten bereits für die Bekämpfung der Kriminalität und zum Schutz der öffentlichen Sicherheit im Allgemeinen zulässig und setzt nicht etwa die Bekämpfung schwerer Kriminalität voraus (vgl. dazu BeckOK StPO/Ferner, 50. Ed., TKG § 174 Rn. 35.1 ff. m. w. N.).

Der EuGH hat in seiner Entscheidung vom 30. April 2024 ausgeführt (Rn. 101, 115), dass die nationale Regelung klare und präzise Regeln vorsehen muss, mit denen sichergestellt werden kann, dass die unter Beachtung der

Richtlinie 2002/58 auf Vorrat gespeicherten IP-Adressen nur zur Identifizierung der Person genutzt werden können, der eine bestimmte IP-Adresse zugewiesen wurde, während sie eine Nutzung ausschließen, die es ermöglicht, mittels einer oder mehrerer IP-Adressen die Online-Aktivität dieser Person zu überwachen. Wird eine IP-Adresse somit nur dazu genutzt, ihren Inhaber im Rahmen eines spezifischen Verwaltungsverfahrens, das zu seiner strafrechtlichen Verfolgung führen kann, zu identifizieren, und nicht zu Zwecken, die etwa darauf abzielen, seine Kontakte oder seinen Standortherauszufinden, so betrifft der allein zu diesem Zweck dienende Zugang zu der IP-Adresse diese als Identitätsdatum und nicht als Verkehrsdatum. Sofern eine nationale Regelung diese Voraussetzungen erfüllt, ermöglichen die einer Behörde übermittelten IP-Adressen somit keine Nachverfolgung der von ihrem Inhaber besuchten Internetseiten; dies spricht dafür, dass der mit dem Zugang dieser Behörde zu den im Ausgangsverfahren in Rede stehenden Identifizierungsdaten verbundene Eingriff nicht als schwerwiegend eingestuft werden kann.

3. Abrufregelungen („2. Tür“)

Gleiches gilt für die Abrufregelung zum Zwecke der Verfolgung schwerer Kriminalität nach § 100g Absatz 2 StPO, da darüber nur in Fällen abschließend benannter besonders schweren Straftaten und ausschließlich nach Anordnung durch das Gericht zugegriffen werden darf und über § 101a StPO auch strenge Verwendungsbeschränkungen gelten. Da sowohl § 100g Absatz 2 und 3 StPO als auch § 101a Absatz 1, 3 und 5 StPO allgemein auf § 176 TKG verweisen, können diese ebenfalls ganz überwiegend bestehen bleiben. Erforderlich sind lediglich einzelne redaktionelle Folgeänderungen in den §§ 100g, 101a StPO durch den Entfall der anlasslosen Speicherung von Standortdaten.

Auch dies entspricht den Anforderungen aus der Rechtsprechung des EuGH aus dem Urteil vom 20. September 2022 – C-793/19 und C-794/19 –. Danach stelle der Zugang zu auf Vorrat gespeicherten IP-Adressen einen eigenständigen, rechtfertigungsbedürftigen Eingriff dar und bedürfe ebenfalls der gesetzlichen Regelung (Rn. 91). In seinem Urteil vom 6. Oktober 2020 – C-511/18 u. a. – hat der EuGH diesbezüglich zudem ausgeführt, dass diese nationalen Abrufregelungen mit bindender Wirkung im nationalen Recht versehen sein sowie Angaben zu Umständen und Voraussetzungen von Maßnahmen der Datenverarbeitung enthalten müssten, sodass Eingriffe auf das absolut Notwendige beschränkt werden (Rn. 132). Diese Regelungen müssten ebenfalls die strikte Einhaltung materieller und prozeduraler Voraussetzungen der Datennutzung sicherstellen und strenge Voraussetzungen und Garantien hinsichtlich der Datenauswertung, insbesondere in Form einer Nachverfolgung in Bezug auf die Online-Kommunikation und -aktivitäten der Betroffenen normieren (Rn. 155 f., 160 ff.). Insbesondere erfüllt der Katalog der besonders schweren Straftaten des § 100g Absatz 2 StPO die Anforderungen des EuGH an den qualifizierten Zweck der Bekämpfung schwerer Kriminalität. Der EuGH hat im Kontext der Vorratsdatenspeicherung noch keinen Katalog der hiervon erfassten Straftaten definiert oder abstrakte Vorgaben für deren Bestimmung aufgestellt In der bisherigen Rechtsprechung des EuGH sind aber jedenfalls die Bekämpfung der organisierten Kriminalität und des Terrorismus sowie des sexuellen Missbrauchs von Kindern sowie die Kinderpornografie darunter gefasst worden (Gutmann/Wollenschläger, GSZ 2023, 249, 254). Dem nationalen Gesetzgeber verbleibt insofern ein eigenständiger Ermessenspielraum, der durch die Wahl des restriktiven Katalogs des § 100g Absatz 2 StPO jedenfalls nicht überschritten wird.

Auch die mittelbare Abrufregelung zu Bestandsdatenauskünften nach § 100j Absatz 2 StPO in Verbindung mit § 174 Absatz 1 Satz 3, § 177 Absatz 1 Nr. 3 TKG kann bestehen bleiben. Dies gilt ebenso für mittelbare Abrufregelungen verschiedener Fachgesetze, wie z. B. § 22a Absatz 3 des Bundespolizeigesetzes, § 5c Absatz 2 Satz 1 des BSI-Gesetzes, § 10 Absatz 3 Satz 1, § 40 Absatz 1 und Absatz 4 Satz 1 des Bundeskriminalamtgesetzes oder § 10 Absatz 3 Satz 1, § 30 Absatz 4 Satz 1 des Zollfahndungsdienstgesetzes. Wie bereits dargestellt ist die Rechtsprechung des EuGH und des BVerfG so auszulegen, dass die mittelbare Verwendung von IP-Adressen durch Internetzugangsdienste zur Ermöglichung der Beauskunftung von Identitätsdaten bereits für die Zwecke der Bekämpfung der Kriminalität und zum Schutz der öffentlichen Sicherheit im Allgemeinen zulässig ist und nicht etwa die Bekämpfung schwerer Kriminalität voraussetzt (vgl. vorstehend unter 2.). Dies Erwägungen gelten auch für die entsprechenden Abrufregelungen.

Durch die Beschränkung des § 176 TKG und den Entfall der anlasslosen Speicherung und Übermittlung sowie der Möglichkeit des Abrufs verschiedener Arten von Verkehrs- und Standortdaten folgt, dass auch entsprechende Kostentatbestände in dem Justizvergütungs- und -entschädigungsgesetzes (JVEG) aufzuheben sind.

Die Abrufregelungen zur Verhütung schwerer Kriminalität als Teil der Bekämpfung schwerer Kriminalität sowie zur Verhütung schwerer Bedrohungen der öffentlichen Sicherheit bleiben bis auf wenige Ausnahmen den Landesgesetzgebern vorbehalten.

4. Übermittlung gespeicherter Verkehrsdaten an die Verfassungsschutzbehörden

Die jüngere höchstrichterliche Rechtsprechung zu den Datenerhebungsbefugnissen der Verfassungsschutzbehörden aufgreifend sieht der Gesetzentwurf die Schaffung einer Übermittlungsbefugnis der Telekommunikationsdiensteanbieter nicht nur an die Strafverfolgungsbehörden, sondern auch an die Verfassungsschutzbehörden von Bund und Ländern vor (§ 177 Absatz 1 Nummer 4 – neu – TKG). Korrespondierend hierzu ist auch eine entsprechende Abrufbefugnis des Bundesamts für Verfassungsschutz vorgesehen (§ 8a Absatz 1 Satz 3 – neu – BVerfSchG). Als Eingriffsschwelle für den Datenabruf wurde als Mindestvoraussetzung die vom Bundesverfassungsgericht als verfassungsgemäß erachtete (BVerfGE 30, 1 ff.) Eingriffsschwelle für Maßnahmen nach § 1 Absatz 1 Nummer 1 des Artikel 10-Gesetzes gewählt (§ 3 Absatz 1 des Artikel 10-Gesetzes), so dass für den Abruf gespeicherter Verkehrsdaten die gleichen Voraussetzungen gelten, wie für eine Telekommunikationsüberwachung durch den Verfassungsschutz. Dies erscheint sachgerecht, weil Verkehrsdaten nicht schützenswerter als die Inhalte der Telekommunikation sind. Das Eingriffsgewicht des Abrufs von Verkehrsdaten, die vom Telekommunikationsanbieter aufgrund einer gesetzlichen Verpflichtung gespeichert wurden, ist zwar höher zu bewerten, als der Abruf von (nicht verpflichtend gespeicherten) Verkehrsdaten, jedoch niedriger als bei Maßnahmen der Wohnraumüberwachung oder der Online-Datenerhebung, für die nach der verfassungsgerichtlichen Rechtsprechung die Eingriffsschwelle der „konkretisierten“ bzw. „dringenden“ Gefahr gilt (BVerfGE 162, 1 Rn. 168 f.).

5. Wiederherstellung der Möglichkeit der Funkzellendatenabfrage

In § 100g StPO soll eine Klarstellung zur Funkzellenabfrage aufgenommen werden, so dass die Ermittlungsmöglichkeit der Funkzellenabfrage wiederhergestellt wird.

III. Alternativen

1. Ersatzlose Streichung der §§ 175, 176 TKG

Eine Alternative bestünde in der ersatzlosen Streichung der Regelungen zur Vorratsdatenspeicherung in den §§ 175, 176 TKG. Jedoch würde dies angesichts der dargestellten Flüchtigkeit elektronischer Daten bei der Beweissicherung dem Interesse an einer effektiven Strafverfolgung widersprechen, da digitale Kommunikation eine immer größere Bedeutung erlangt hat und in vielen Strafverfahren neben digitalen Spuren kaum weitere Ermittlungsansätze zur Verfügung stehen.

2. Einführung einer Sicherungsanordnung („Quick Freeze“)

Eine weitere Alternative bestünde in der Einführung einer Sicherungsanordnung („Quick Freeze“), die Gegenstand eines Ende des Jahres 2022 bekannt gewordenen Referentenentwurfs des Bundesministeriums der Justiz (BMJ) für ein „Gesetz zur Einführung einer Sicherungsanordnung für Verkehrsdaten in der Strafprozessordnung“ ist. Mit diesem Entwurf soll von einer anlasslosen Speicherung ganz abgesehen und lediglich die Möglichkeit einer anlassbezogenen Sicherungsanordnung („Quick Freeze“) geschaffen werden.

Dieser Entwurf befindet sich seit ca. zwei Jahren in der Ressortabstimmung der Bundesregierung und ist vielfach aus Ablehnung gestoßen. So hat u. a. die Ständige Konferenz der Innenminister und -senatoren der Länder in ihrer 221. Sitzung vom 19. bis 21. Juni 2024 den Beschluss „Praxistaugliche Umsetzung der Vorgaben des EuGH zur Regelung der Vorratsdatenspeicherung im Lichte der jüngsten Erleichterungen“ gefasst und darin festgestellt, dass ein „Quick Freeze“-Verfahren unzureichend sei. Sie hat die Bitte an das BMI bekräftigt, sich innerhalb der Bundesregierung weiterhin dafür einzusetzen, eine den Regelungsspielraum der Urteile des EuGH vom 20. September 2022 (Rs. C-793/19 und Rs. C-794/19) und vom 30. April 2024 (Rs. C-470/21) ausschöpfende Neuregelung herbeizuführen und sich auch auf europäischer Ebene für eine entsprechende Regelung einzusetzen. Sie fordert die Bundesregierung insbesondere weiterhin auf, unverzüglich einen Gesetzentwurf zur Novellierung der §§ 176, 177 TKG und der entsprechenden Fachgesetze vorzulegen, um die elementare Tätigkeit der Gefahrenabwehr- und Strafverfolgungsbehörden, aber auch des Verfassungsschutzes, zu effektivieren. Ebenso haben sich die Praktiker im Rahmen einer öffentlichen Anhörung im Rechtsausschuss des Deutschen Bundestages im Oktober 2023 – BT-Drs. 20/9527 – zu dem Antrag „IP-Adressen rechtssicher speichern und Kinder vor sexuellem Missbrauch schützen“ der Fraktion der CDU/CSU – BT-Drs. 20/3687, mit dem die IP-Speicherung gefordert wurde, für diesen Antrag ausgesprochen und das vom Bundesjustizministerium favorisierte „Quick-Freeze“-Verfahren abgelehnt. Die geladenen Sachverständigen der Strafverfolgungspraxis haben sich einhellig für die Notwendigkeit

einer anlasslosen Speicherung von IP-Adressen zum Zwecke der Verfolgung schwerer Kriminalität ausgesprochen. Für die Identifizierung unbekannter tatverdächtiger Person über IP-Adressen bietet das „Quick-Freeze"-Verfahren aus Sicht der Strafverfolgungspraxis keinen Nutzen, sofern die relevanten Daten zum Zeitpunkt des Auskunftsersuchens nicht mehr oder unvollständig gespeichert sind, da entsprechende Daten bei Telekommunikations-Anbietern nur zu bekannten Anschlussinhabern eingefroren werden können (vgl. Bund Deutscher Kriminalbeamter, Stellungnahme zu BT-Drs. 20/3687, S. 2; Bundeskriminalamt, Stellungnahme zu BT-Drs. 20/3687, S. 2; Deutscher Richterbund, Stellungnahme zu BT-Drs. 20/3687, S. 5; Krause, ZRP 2023, 169). Eine gesetzliche Pflicht zur Speicherung von IP-Adressen besteht aber gerade nicht.

Internetzugangsanbieter können auch nicht frei entscheiden, ob und wie lange Verkehrsdaten zu geschäftlichen Zwecken vorgehalten werden. Dies ist gemäß § 9 Absatz 1 Satz 1 TTDSG zwar insbesondere zur Entgeltabrechnung sowie gemäß § 12 Absatz 1 und 4 TTDSG zur Störungsbeseitigung und zur Missbrauchsbekämpfung möglich. Jedoch sind erhobene Daten nach § 9 Absatz 1 Satz 2, § 12 Absatz 2 TTDSG unverzüglich zu löschen, sobald sie für die vorgenannten Zwecke nicht mehr erforderlich sind. Wie lange IP-Adressen „zum Einfrieren" vorliegen würden, unterscheidet sich danach, auf welcher Rechtsgrundlage entsprechende Daten erhoben und gespeichert werden können.

Für Abrechnungszwecke dürfen Verkehrsdaten gemäß § 10 Absatz 2 Satz 2 TTDSG bis zu sechs Monate nach Versendung der Rechnung gespeichert werden. Bei den mittlerweile im Bereich der Festnetzanschlüsse und der Mobilfunktelefonie zum Regelfall gewordenen Tarifen mit Pauschalvergütung („Flatrate", vgl. dazu Bundesnetzagentur, Nutzung von OTT-Kommunikationsdiensten in Deutschland, Bericht 2020) besteht aber bereits keine Notwendigkeit für die Dienstanbieter, IP-Adressen zu Abrechnungszwecken zu speichern (BeckOK StPO/Bär, 50. Ed., TTDSG § 9 Rn. 8). Dies macht regelmäßig eine Löschung der IP-Adressen unmittelbar nach dem Ende der Verbindung erforderlich. Bei anderen Vertragsmodellen oder Prepaid-Produkten werden zwar im Bereich der Telefondienste Verkehrsdaten bis zu drei Monate nach Rechnungsstellung gespeichert. Bei Internetzugangsdiensten werden auch bei volumenbegrenzten Verträgen aus Gründen des Datenschutzes nur Datenvolumen und Nutzerkennung, nicht aber IP-Adressen gespeichert (vgl. zum Ganzen Bundesbeauftragter für Datenschutz und Informationssicherheit, Leitfaden für datenschutzgerechte Speicherung von Verkehrsdaten, Stand: 30. September 2022).

Zum Zwecke der Störungsbeseitigung werden dagegen gemäß § 12 Absatz 1 und 4 TTDSG Rufnummer oder Kennung der beteiligten Anschlüsse, Beginn und Ende der jeweiligen Verbindung gespeichert – bei mobilen Anschlüssen auch Standortdaten. In diesem Zusammenhang besteht für Internetzugangsdienste die Möglichkeit, die vergebenen IP-Adressen und die Verknüpfungen zu den Benutzerkennungen für einen kurzen Zeitraum von bis zu sieben Tagen zum Zwecke der Erkennung, Eingrenzung und Beseitigung von Störungen zu speichern (vgl. BGH, Urteil vom 3. Juli 2014 – III ZR 391/13). 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 (Bundeskriminalamt, Stellungnahme zu BT-Drs. 20/3687, S. 2).

Daher ist die Einführung einer Sicherungsanordnung („Quick Freeze") keine Alternative zu einer zur Einführung einer Mindestspeicherung von IP-Adressen, sondern kann allenfalls ergänzend dazu eingeführt werden.

Auch das BVerfG hatte bereits in seinem Urteil zur Vorratsdatenspeicherung vom 2. März 2010 – 1 BvR 256/08 – die Existenz weniger einschneidender Mittel mit ebenso weitreichenden Aufklärungsmöglichkeiten verneint und geurteilt, dass das „Quick-Freeze"-Verfahren der Speicherung von IP-Adressen nicht vorgehe, da ein solches Verfahren, das Daten aus der Zeit vor der Anordnung ihrer Speicherung nur erfassen kann, soweit sie noch vorhanden sind, nicht ebenso wirksam sei wie eine kontinuierliche Speicherung, die das Vorhandensein eines vollständigen Datenbestandes gewährleiste (Rn. 208).

Diese Notwendigkeit einer Speicherung von IP-Adressen zusätzlich zu einem „Quick-Freeze"-Verfahren hatte das Bundesjustizministerium bereits im Jahr 2011 in einem Diskussionsentwurf eines Gesetzes zur Sicherung vorhandener Verkehrsdaten und Gewährleistung von Bestandsdatenauskünften im Internet ausdrücklich anerkannt (vgl. dazu Arning/Moos ZD 2012, 153).

Letztlich würde durch die Einführung einer Sicherungsanordnung („Quick Freeze") ein völlig neues Speichersystem und Beauskunftungsmodell eingerichtet werden, was mit großem Ressourceneinsatz und Erfüllungsaufwand sowohl für die Telekommunikationsunternehmen als auch für die Strafverfolgungsbehörden verbunden wäre. Für die Beauskunftung von gespeicherten IP-Adressen bestehen dagegen bereits praxiserprobte elektronische Schnitt-

stellen und gesicherte Auskunftssysteme zwischen Telekommunikationsunternehmen und Strafverfolgungsbehörden.

3. Login-Falle

Neben diesem Referentenentwurf zur Einführung einer Sicherungsanordnung („Quick-Freeze“) wird auch die Einführung einer Login-Falle diskutiert. Dieser Vorschlag ist auch Gegenstand des Koalitionsvertrags der Ampel-Koalition aus dem Jahr 2021 (S. 87: „Mit der Login-Falle wollen wir grundrechtsschonende und freiheitsorientierte Instrumente schaffen, um die Identifizierung der Täterinnen und Täter zu erreichen“.). Ein Gesetzesentwurf liegt nicht vor.

Mit der Login-Falle sollen nach der Meldung von strafrechtlich relevanten Handlungen des Nutzers eines Internet-Dienstanbieters diese Internet-Dienstanbieter dazu verpflichtet werden, für dieses Nutzerprofil die Login-Falle zu aktiviert. Dies soll dazu führen, dass bei einer erneuten Verbindungsaufnahme dieses Nutzerprofils die verwendete IP-Adresse einmalig registriert und an die Strafverfolgungsbehörden übermittelt wird, so dass über eine Personenauskunft zu einer dynamischen IP-Adresse eine Identifizierung des Anschlussinhabers erfolgen kann (vgl. näher zur Login-Falle Brodowski StV 2022, 413).

Eine solche Login-Falle ist bereits nach den §§ 100g, 100k StPO möglich (MüKoStPO/Rückert, 2. Aufl., § 100g Rn. 127). Da diese Ermittlungsmaßnahme aber erst nach einer begangenen Tat ansetzt und einen weiteren Login der Straftäter voraussetzt, können davon solche Straftaten nicht aufgeklärt werden, bei denen sich Straftäter nach der Tatbegehung nicht mehr in das Nutzerprofil einloggen. Aber auch wenn ein erneuter Login stattfindet und eine Weiterleitung der erhobenen IP-Adresse an Strafverfolgungsbehörden sattfindet, ist davon auszugehen, dass die damit erzielbaren Aufklärungsquoten etwa dem beschriebenen NCMEC-Prozess des Bundeskriminalamts entsprechen dürften, da auch dort tagesaktuell IP-Adressen mitgeteilt und abgefragt werden (vgl. BeckOK StPO/Bär, 50. Ed., § 100g Rn. 71b).

Gegen eine Login-Falle als Alternative für eine Mindestspeicherung von Quellen-IP-Adressen spricht zudem, dass mit rein nationalen Regelungen wie §§ 100g, 100k StPO ausländische Internetdienstanbieter nicht verpflichtet werden können. Insofern würde es einer europäischen bzw. internationalen Regelung bedürfen (vgl. dazu etwa Frank, MMR 2022, 1026).

IV. Gesetzgebungskompetenz

Die Gesetzgebungskompetenz des Bundes folgt aus Artikel 73 Absatz 1 Nummer 7 und Nummer 10b in Verbindung mit Artikel 87 Absatz 1 Satz 2 des Grundgesetzes (Telekommunikation, Verfassungsschutz, betrifft Artikel 1 und 4) und Artikel 74 Absatz 1 Nummer 1 des Grundgesetzes (gerichtliches Verfahren, Strafrecht, betrifft Artikel 2 und 3 dieses Gesetzes).

V. Vereinbarkeit mit dem Recht der Europäischen Union und völkerrechtlichen Verträgen

Der Gesetzentwurf ist mit dem Recht der Europäischen Union und mit völkerrechtlichen Verträgen, die die Bundesrepublik Deutschland abgeschlossen hat, vereinbar.

Insbesondere ist die Änderung und Begrenzung der §§ 175, 176 TKG zwingende Folge des Urteils des EuGH vom 20. September 2022 – C-793/19 und C-794/19 –, der befunden hat, dass diese nationalen Vorschriften gegen das Unionsrecht verstoßen. Infolge dieses Urteils des EuGH hat das BVerwG am 14. August 2023 – 6 C 6.22 und 6 C 7.22 – entschieden, dass die nationalen Regelungen zur Vorratsdatenspeicherung von Verkehrs- und Standortdaten in den §§ 175, 176 TKG unionsrechtswidrig sind und wegen des Anwendungsvorrangs des Unionsrechts nicht angewendet werden dürfen.

Die vorgeschlagene Regelung einer Mindestspeicherung von Quellen-IP-Adressen samt gegebenenfalls vergebener Port-Nummern zum Zwecke der Bekämpfung schwerer Kriminalität in den §§ 175, 176 TKG steht dagegen im Einklang mit den diesbezüglichen Anforderungen des EuGH.

VI. Gesetzesfolgen

1. Rechts- und Verwaltungsvereinfachung

Aspekte der Rechts- und Verwaltungsvereinfachung sind durch den Entwurf nicht betroffen.

2. Nachhaltigkeitsaspekte

Der Entwurf steht im Einklang mit den Leitgedanken der Bundesregierung zur nachhaltigen Entwicklung im Sinne der Deutschen Nachhaltigkeitsstrategie.

3. Haushaltsausgaben ohne Erfüllungsaufwand

Haushaltsausgaben ohne Erfüllungsaufwand sind für Bund, Länder und Gemeinden durch den Entwurf nicht zu erwarten.

4. Erfüllungsaufwand

a) Erfüllungsaufwand für Bürgerinnen und Bürger

Für die Bürgerinnen und Bürger entsteht oder entfällt kein Erfüllungsaufwand.

b) Erfüllungsaufwand für die Wirtschaft

Für die betroffenen Telekommunikationsdienste-Anbieter entsteht durch die Einführung einer Mindestspeicherung von IP-Adressen kein wesentlicher Mehraufwand gegenüber der bereits überwiegend durchgeführten freiwilligen Speicherung der IP-Adressen von bis zu sieben Tagen (vgl. BT-Drs. 19/25891 sowie Bundeskriminalamt, Stellungnahme zu BT-Drs. 20/9527, S. 1), zumal bereits praxiserprobte elektronische Schnittstellen und gesicherte Auskunftssysteme zwischen Telekommunikationsunternehmen und Strafverfolgungsbehörden eingerichtet sind. Sowohl gegenüber der ursprünglich vorgesehenen Vorratsdatenspeicherung als auch gegenüber der Einführung einer Sicherungsanordnung („Quick Freeze“) ist von einer erheblichen Entlastung auszugehen.

Im Übrigen entsteht für die Wirtschaft kein Erfüllungsaufwand.

c) Erfüllungsaufwand der Verwaltung

Für die Strafverfolgungsbehörden des Bundes und der Länder entsteht durch die Einführung einer Mindestspeicherung von IP-Adressen sowohl ein Mehraufwand durch die damit verbundene weitergehende Möglichkeit zur Abfrage gespeicherter IP-Adressen in Ermittlungsverfahren als auch ein Minderaufwand durch eine Verringerung ergebnislos verlaufender Auskunftsersuchen und den Entfall anderer alternativer, nicht gleichsam effektiver Ermittlungsmaßnahmen insbesondere zur Identifizierung unbekannter Tatverdächtiger. In der Gesamtbetrachtung ist zu erwarten, dass der Mehr- und Minderaufwand sich annähernd ausgleichen wird.

Bei der Bundesnetzagentur entsteht durch die Einführung einer Mindestspeicherung von IP-Adressen zwar ein zusätzlicher Kontrollaufwand und Mehraufwand bei der Anwendung der Bußgeldtatbestände. Jedoch ist sowohl gegenüber der ursprünglich vorgesehenen Vorratsdatenspeicherung als auch und insbesondere gegenüber der Einführung einer Sicherungsanordnung („Quick-Freeze“) von einer erheblichen Entlastung auszugehen.

5. Weitere Kosten

Durch das Erfordernis eines Gerichtsbeschlusses für die einzelfallbezogene Anordnung der Herausgabe mindestgespeicherter IP-Adressen ist von einem geringfügigen Mehraufwand für die Justiz auszugehen. Auch insoweit ist jedoch sowohl gegenüber der ursprünglich vorgesehenen Vorratsdatenspeicherung als auch und insbesondere gegenüber der Einführung einer Sicherungsanordnung („Quick-Freeze“) von einer erheblichen Entlastung auszugehen. Von weiteren Kosten ist nicht auszugehen. Auswirkungen auf Einzelpreise und das allgemeine Preisniveau, insbesondere auf das Verbraucherpreisniveau für Telekommunikationsdienste, sind im Übrigen nicht zu erwarten.

6. Weitere Gesetzesfolgen

Die Regelungen sind inhaltlich geschlechtsneutral und betreffen alle Menschen ungeachtet ihrer sexuellen und geschlechtlichen Identität. Im Übrigen werden die Regelungen des Entwurfs keine Auswirkungen auf Verbrau-

cherinnen und Verbraucher haben. Demografische Auswirkungen oder Auswirkungen auf die Gleichwertigkeit der Lebensverhältnisse in Deutschland sind ebenfalls nicht zu erwarten.

VII. Befristung; Evaluation

Eine Befristung der vorgeschlagenen Gesetzesänderungen kommt nicht in Betracht. Sie betreffen den Kernbereich des Strafverfahrensrechts sowie des Verfassungsschutzrechts und des dazugehörigen Telekommunikationsrechts und sind auf Dauer angelegt. Eine Evaluierung würde die Strafverfolgungsbehörden nur unnötig belasten.

B. Besonderer Teil

Zu Artikel 1 (Änderung des **Telekommunikationsgesetzes**)

Zu Nummer 1 (Änderung des § 175)

Nach § 175 Absatz 1 TKG betrafen die Verpflichtungen zur Speicherung von Verkehrsdaten, zur Verwendung der Daten und zur Datensicherheit nach den §§ 176 bis 181 TKG bislang die Anbieter öffentlich zugänglicher Telekommunikationsdienste für Endnutzer, bei denen es sich nicht um nummernunabhängige interpersonelle Telekommunikationsdienste handelt.

Dieser Kreis der speicherpflichtigen Anbieter wird wegen der beabsichtigten Beschränkung der Mindestspeicherung auf Quellen-IP-Adressen sowie gegebenenfalls vergebene Port-Nummern (§ 176 Absatz 1 TKG n. F.) auf Anbieter öffentlich zugänglicher Internetzugangsdienste für Endnutzer beschränkt. Diese sind in § 3 Nr. 23 TKG definiert.

Begrenzt bleibt die Speicherpflicht auf Diensteanbieter für Endnutzer. Hierbei handelt es sich entsprechend der Begriffsbestimmung in § 3 Nr. 13 TKG um Kunden, die Internetzugangsdienste – gleichgültig ob als Privathaushalt oder als Unternehmen – für eigene Zwecke nutzen. Die Eigenschaft als Endnutzer geht damit weiterhin nur dann verloren, soweit Dienste auch Dritten angeboten werden (BeckOK StPO/Bär, 50. Ed., TKG § 175 Rn. 5).

Zu Nummer **2 (Änderung des § 176)**

In § 176 TKG n. F. wird die Pflicht zur Mindestspeicherung der Quellen-IP-Adressen sowie gegebenenfalls vergebener Port-Nummern eingeführt und auf einen Zeitraum von drei Monaten zur Bekämpfung schwerer Kriminalität sowie zur Verhütung schwerer Bedrohungen der öffentlichen Sicherheit beschränkt.

Zu Buchstabe a

In § 176 Absatz 1 TKG n. F. wird die bisherige Speicherverpflichtung für Internetzugangsdienste aus § 176 Absatz 3 TKG übernommen, ausdrücklich auf den Zweck der Bekämpfung schwerer Kriminalität sowie zur Verhütung schwerer Bedrohungen der öffentlichen Sicherheit bezogen und in Nr. 1 und Nr. 2 erweitert:

- In § 176 Absatz 1 Nr. 1 TKG n. F. wird im Hinblick auf das Urteil des EuGH vom 20. September 2022 – C-793/19 und C-794/19 – ergänzend zu der ausdrücklichen Regelung in § 176 Absatz Absatz 5 TKG (§ 176 Absatz Absatz 2 TKG n. F.) nochmals klargestellt, dass die Speicherplicht nur die zugewiesene Internetprotokoll-Adresse der Quelle einer Verbindung („Quellen-IP-Adresse“) betrifft (EuGH a. a. O. Rn. 97, 101 ff., 131). Derzeit ist in § 176 Absatz Absatz 3 Nr. 1 TKG nur allgemein von „Internetprotokoll-Adressen“ die Rede. Mit der Klarstellung soll verdeutlicht werden, dass die Speicherverpflichtung gerade nicht die IP-Adressen der aufgerufenen Ziele oder Dienste betrifft (vgl. zur Funktionsweise von IP-Adressen bei der Internetnutzung etwa Wildberg/Lee-Wunderlich, CCZ 2023, 281).
- In § 176 Absatz 1 Nr. 2 TKG n. F. wird die bislang von § 176 Absatz 3 Nr. 2 TKG vorgesehene Speicherung von korrespondierenden Benutzer- und Anschlusskennungen übernommen und klarstellend um die Pflicht zur Speicherung einer gegebenenfalls zugewiesenen Port-Nummer ergänzt, sofern diese für die Identifikation des Endnutzers erforderlich ist. Die Speicherung der Port-Nummer wird zusätzlich zur Speicherung der IP-Adresse dann zur Bestimmung des Anschlussinhabers benötigt, wenn Internetzugangsdienste einzelne öffentliche IP-Adressen mehreren Kunden im Rahmen des sogenannten „Natting“ (NAT = Network Address Translation) gleichzeitig zuweisen. Eine Zuordnung einer IP-Adresse zu einem Anschlussinhaber ist dann nur mitsamt der Port-Nummer möglich (Bundesbeauftragter für den Datenschutz und die Informationsfreiheit, Stel-

lungnahme zu BT-Drs. 20/3687, S. 3). Bislang findet aber keine einheitliche Speicherung der Port-Nummer seitens der Internetzugangsdienste statt (Bundeskriminalamt, Stellungnahme zu BT-Drs. 20/3687, S. 1). Um auch hinsichtlich der zusätzlichen Speicherung der Port-Nummern den Eingriff so gering wie möglich zu halten, wird die Speicherpflicht auf die Fälle begrenzt, in denen zusätzlich zu einer mehrfach vergebenen IPv4-Adresse eine Port-Nummer vergeben worden ist und diese auch zur Identifizierung des Endkunden erforderlich ist (so ausdrücklich Bundesbeauftragter für den Datenschutz und die Informationsfreiheit, Stellungnahme zu BT-Drs. 20/3687, S. 3; vgl. ausführlich zur Frage der Eingriffsintensität der zusätzlichen Speicherung von Port-Nummern Gutmann/Wollenschläger, GSZ 2023, 249, 254 ff.).

– In § 176 Absatz 1 Nr. 3 TKG n. F. wird die bislang von § 176 Absatz 3 Nr. 3 TKG vorgesehene Pflicht zur Speicherung von Datum und Uhrzeit in Bezug auf Beginn und Ende der Internetnutzung unter der zugewiesenen IP-Adresse unverändert übernommen.

Die Begrenzung der Speicherung auf den Zweck der Bekämpfung schwerer Kriminalität sowie zur Verhütung schwerer Bedrohungen der öffentlichen Sicherheit entspricht den Anforderungen aus dem Urteil des EuGH vom 20. September 2022 – C-793/19 und C-794/19 –, wonach eine allgemeine und unterschiedslose Vorratsspeicherung der IP-Adressen, die der Quelle einer Verbindung zugewiesen sind, zum Schutz der nationalen Sicherheit, zur Bekämpfung schwerer Kriminalität und zur Verhütung schwerer Bedrohungen der öffentlichen Sicherheit für einen auf das absolut Notwendige begrenzten Zeitraum mit Unionsrecht vereinbar sei (EuGH a. a. O. Rn. 131). Der Begriff der schweren Kriminalität wird nicht in § 176 Absatz 1 TKG n. F. definiert, sondern ergibt sich mittelbar aus der (unverändert fortbestehenden) Abrufregelung in § 100g Absatz 2 StPO und dem dortigen Katalog schwerer Straftaten (vgl. zur Konkretisierung der schweren Kriminalität als Eingriffszweck Gutmann/Wollenschläger, GSZ 2023, 249, 254).

Nach der Rechtsprechung des EuGHs (vgl. Urteil vom 20. September 2022 – C-793/19, Rn. 73, 75) umfasst die Bekämpfung schwerer Kriminalität nicht nur die Verfolgung von solchen Straftaten, sondern bereits deren Verhütung. Die Verhütung von Straftaten meint im Gefahrenabwehrrecht der Länder regelmäßig die vorbeugende Bekämpfung von Straftaten. Insoweit stellen die vorgesehenen Änderungen diesen Befund ausdrücklich klar und eröffnen den Ländern sowie dem Bund, soweit er die vorbeugende Bekämpfung von Straftaten betreibt, die Möglichkeit, entsprechende Abrufregelungen im Gefahrenabwehrrecht zu schaffen. Gerade im Kampf gegen Kindesmissbrauch benötigt die Polizei die Befugnis, diesen auch vorbeugend bekämpfen zu können soweit die Gefährder das Tatmittel Internet nutzen.

Die Speicherpflicht wird zudem auf einen Zeitraum von drei Monaten beschränkt. Aus dem Urteil des EuGH vom 20. September 2022 – C-793/19 und C-794/19 – ergibt sich insoweit keine feste zeitliche Vorgabe. Vielmehr müsse sich die Speicherpflicht auf einen auf das absolut Notwendige begrenzten Zeitraum beschränken (EuGH a. a. O. Rn. 131). Nach der unter A. II. 1. beschriebenen, umfassenden Abwägung ist ein Speicherzeitraum für IP-Adressen und gegebenenfalls vergebener Port-Nummern von drei Monaten angemessen, um das Ziel der Bekämpfung schwerer internetbezogener Kriminalität zu realisieren und überschreitet angesichts der hohen Gesamtzahlen schwerer internetbezogener Kriminalität, der nur kurzen und unvollständigen freiwilligen Speicherung der Internetzugangsdiensten und der daraus folgenden niedrigen Aufklärungsrate von tatrelevanten IP-Adressen nicht das im Hinblick auf das verfolgte Ziel absolut Notwendige.

Zu Buchstabe b

Die beabsichtigte Streichung von § 176 Absatz 2 bis 4 TKG beruht auf der beschriebenen Beschränkung der Mindestspeicherpflicht auf Quellen-IP-Adressen bei Internetzugangsdiensten in § 176 Absatz 1 TKG n. F.

Insbesondere soll auf eine weitergehende Verpflichtung zur zusätzlichen Mindestspeicherung von Standortdaten bei mobiler Internetnutzung verzichtet werden, die bislang in § 176 Absatz 4 TKG geregelt ist. Der EuGH hat in seinem Urteil vom 20. September 2022 – C-793/19 und C-794/19 – bekräftigt, dass eine allgemeine und unterschiedslose Vorratsspeicherung von Verkehrs- und Standortdaten, deren Vertraulichkeit von entscheidender Bedeutung für das Recht auf Achtung des Privatlebens sei, nicht mit dem Ziel der Bekämpfung schwerer Kriminalität gerechtfertigt werden könne (EuGH a. a. O. Rn. 74). Die Speicherung von Verkehrs- oder Standortdaten, die Informationen über die Kommunikationen des Nutzers eines elektronischen Kommunikationsmittels oder über den Standort der von ihm verwendeten Endgeräte liefern können, sei jedem Fall schwerwiegend, unabhängig von der Länge des Speicherzeitraums und von der Menge oder Art der gespeicherten Daten, sofern der Datensatz geeignet sei, sehr genaue Schlüsse auf das Privatleben der betroffenen Person bzw. der betroffenen Personen zuzulassen (EuGH a. a. O. Rn. 88).

Zu Buchstabe c

Aufgrund der beabsichtigten Streichung von § 176 Absatz 2 bis 4 TKG wird die Regelung in § 176 Absatz 5 TKG ohne inhaltliche Änderung in § 176 Absatz 2 TKG n. F. übernommen.

Zu Buchstabe d

Über § 176 Absatz 6 TKG und die Verweisung auf § 11 Absatz 5 TTDSG wird geregelt, dass Verbindungen zu bestimmten sozialen oder kirchlichen Einrichtungen in einem Einzelverbindungsnachweis nicht aufgeführt werden dürfen, damit eine Inanspruchnahme solcher Dienste durch Endnutzer grundsätzlich anonym bleibt und es nicht zu einer Offenbarung solcher Kontaktaufnahmen kommt, die regelmäßig mit den Kernbereich privater Lebensgestaltung im Zusammenhang stehen (vgl. BeckOK StPO/Bär, 50. Ed., TTDSG § 11 Rn. 11). Durch die Beschränkung der Speicherpflicht auf Quellen-IP-Adressen ist diese Ausnahmeregelung zukünftig nicht mehr notwendig.

Zu Buchstabe e

Aufgrund der beabsichtigten Streichung von § 176 Absatz 2 bis 4 TKG wird die Regelung in § 176 Absatz 7 TKG ohne inhaltliche Änderung in § 176 Absatz 3 TKG n. F. übernommen. Gleiches gilt für die Regelung in § 176 Absatz 8 TKG, die ohne inhaltliche Änderung in § 176 Absatz 4 TKG n. F. übernommen wird.

Zu Buchstabe f

Nach Artikel 19 Absatz 1 Satz 2 des Grundgesetzes muss ein Gesetz, das ein Grundrecht einschränkt, dieses Grundrecht unter Angabe des Artikels nennen. Dieses Zitiergebot soll sicherstellen, dass keine unbeabsichtigten Grundrechtseingriffe erfolgen. Der Gesetzgeber soll sich über die Auswirkungen seiner Regelungen für die betroffenen Grundrechte im Klaren sein und die Grundrechtseinschränkung kenntlich machen. Ein entsprechender Vermerk soll unmittelbar nach der einschränkenden Vorschrift angebracht werden.

Zu Nummer 3 (Änderung des § 177)

Die Verwendungsregelungen in § 177 Absatz 1 Nr. 1 bis Nr. 3 TKG können fortbestehen. Dies betrifft insbesondere die Verwendungs- und Übermittlungsregelung in § 177 Absatz 1 Nr. 1 TKG, die den Abruf der zu einem Anschlussinhaber anlasslos gespeicherten Quellen-IP-Adressen zum Zwecke der Verfolgung schwerer Kriminalität gemäß § 100g Absatz 2 StPO ermöglicht.

Zu Buchstabe a

Wie unter A. II. 2. beschrieben, ist nach zutreffendem Verständnis der Rechtsprechung des EuGH und des BVerfG ist die von § 177 Absatz 1 Nr. 3 TKG eröffnete Möglichkeit der mittelbaren Verwendung von IP-Adressen durch Internetzugangsdienste zur Ermöglichung der Beauskunftung von Identitätsdaten bereits für die Bekämpfung der Kriminalität und zum Schutz der öffentlichen Sicherheit im Allgemeinen zulässig und setzt nicht etwa die Bekämpfung schwerer Kriminalität voraus.

Die Ersetzung der Wörter „öffentlich zugänglicher Telekommunikationsdienste“ durch „öffentlich zugänglicher Internetzugangsdienste für Endnutzer“ ist eine Folgeänderung zur Beschränkung des § 175 TKG n. F.

Zu Buchstabe b

Die Regelung dient der Schaffung einer Übermittlungsbefugnis der Telekommunikationsdiensteanbieter an die Verfassungsschutzbehörden von Bund und Ländern (§ 177 Absatz 1 Nummer 4 TKG) und schafft damit die Voraussetzungen für die von der Rechtsprechung geforderte sog. „1. Tür“.

Zu Nummer 4 (Änderung des § 180)

Die beabsichtigte Änderung ist eine rein redaktionelle Anpassung an die Neunummerierung der Absätze in § 176 TKG n. F.

Zu Nummer 5 (Änderung des § 228)

Die beabsichtigte Änderung ist eine rein redaktionelle Folgeänderung der Umnummerierung des § 176 Absatz 8 TKG in § 176 Absatz 4 TKG n. F. ohne inhaltliche Änderung (Artikel 1 Nummer 2 Buchstabe e).

Zu Artikel 2 (Änderung der Strafprozessordnung)

Mit der Anpassung der §§ 175, 176 TKG und der Einführung einer Pflicht zur Mindestspeicherung der Quellen-IP-Adressen sowie gegebenenfalls vergebener Port-Nummern sind nahezu keine Änderungen der Strafprozessordnung verbunden.

Dies gilt insbesondere für § 100g Absatz 2 StPO als Abrufregelung der zu einem Anschlussinhaber anlasslos gespeicherten Quellen-IP-Adressen zum Zwecke der Verfolgung schwerer Kriminalität, da darüber nur in Fällen abschließend benannter besonders schweren Straftaten und ausschließlich nach Anordnung durch das Gericht zugegriffen werden darf und über § 101a StPO auch strenge Verwendungsbeschränkungen gelten. Da sowohl § 100g Absatz 2 und 3 StPO als auch § 101a Absatz 1, 3 und 5 StPO allgemein auf § 176 TKG verweisen, können diese ebenfalls ganz überwiegend bestehen bleiben. Insbesondere erfüllt der Katalog der besonders schweren Straftaten des § 100g Absatz 2 StPO die Anforderungen des EuGH an den qualifizierten Zweck der Bekämpfung schwerer Kriminalität.

Auch die mittelbare Abrufregelung zu Bestandsdatenauskünften nach § 100j Absatz 2 StPO in Verbindung mit § 174 Absatz 1 Satz 3, § 177 Absatz 1 Nr. 3 TKG kann bestehen bleiben. Wie unter A. II. 2. und 3. beschrieben, ist die Rechtsprechung des EuGH und des BVerfG so auszulegen, dass die mittelbare Verwendung von IP-Adressen durch Internetzugangsdienste zur Ermöglichung der Übermittlung von Identitätsdaten bereits für die Zwecke der Bekämpfung der Kriminalität und zum Schutz der öffentlichen Sicherheit im Allgemeinen zulässig ist und nicht etwa die Bekämpfung schwerer Kriminalität voraussetzt. Dies gilt ebenso für mittelbare Abrufregelungen verschiedener polizeilicher Fachgesetze, Mit dem Entfall der anlasslosen Speicherung von Standortdaten sind daher lediglich einige Folgeänderungen in den §§ 100g, 101a StPO erforderlich.

Zu Nummer 1 (Änderung des § 100g)

Zu Buchstabe a (Änderung des § 100g Absatz 3 Satz 1)

Mit der Einfügung der Wörter „einschließlich der Standortdaten“ soll klargestellt werden, dass Funkzellenabfragen auch im Hinblick auf die regelmäßig miterfassten Standortdaten nur von den in § 100g Absatz 3 Satz 1 StPO ausdrücklich genannten Voraussetzungen abhängen und keine Katalogtat im Sinne des § 100g Absatz 2 Satz 2 StPO erfordern. Damit wird auf die Entscheidung des 2. Strafsenats des Bundesgerichtshofs vom 10. Januar 2024 (Az. 2 StR 171/23) reagiert.

Zu Buchstabe b (Änderung des § 100g Absatz 3 Satz 2)

Die beabsichtigte Streichung von § 100g Absatz 3 Satz 2 StPO ist eine Folgeänderung zur intendierten Aufhebung des § 176 Absatz 4 TKG (Artikel 1 Nummer 2 Buchstabe b) und beruht darauf, dass zukünftig keine Pflicht mehr zur Speicherung der genutzten Funkzellen bei mobilen Telefon- und Internetdiensten bestehen soll.

Zu Nummer1 Buchstabe c und Nummer 2 (Änderung von § 100g Absatz 4, § 101a)

Es handelt sich um Folgeänderungen durch die beabsichtigte Aufhebung von § 100g Absatz 3 Satz 2 StPO (Artikel 2 Nummer 2 und Artikel 1 Nummer 2 Buchstabe b).

Zu Artikel 3 (Änderung des Justizvergütungs- und -entschädigungsgesetzes)

Durch die beabsichtigte Beschränkung des § 176 TKG und den Entfall der Möglichkeit des Abrufs verschiedener Arten von anlasslos gespeicherten Verkehrs- und Standortdaten folgt, dass auch entsprechende Kostentatbestände in dem Justizvergütungs- und -entschädigungsgesetzes (JVEG) aufzuheben sind.

Zu Nummer 1

Dabei handelt es sich rein redaktionelle Folgeänderungen durch die Begrenzung der Speicherpflicht in § 176 Absatz 1 TKG n. F.

Zu Nummer 2

Das Entfallen von Nummer 304 ist eine Folgeänderung der beabsichtigten Begrenzung der anlasslosen Speicherung auf IP-Adressen und des damit verbundenen Wegfalls der Pflicht zur Speicherung der Telefon-Verbindungsdaten für eine Zielwahlsuche.

Das Entfallen von Nummer 307 ist eine Folgeänderung zur beabsichtigten Aufhebung des § 176 Absatz 4 TKG und des Wegfalls der Pflicht zur Speicherung der genutzten Funkzellen bei mobilen Telefon- und Internetdiensten (Artikel 1 Nummer 2 Buchstabe b).

Zu den Nummern 3, 4 und 5

Das Entfallen von Nummern 309 und 401 ist eine Folgeänderung zur beabsichtigten Aufhebung des § 176 Absatz 4 TKG und des Wegfalls der Pflicht zur Speicherung der genutzten Funkzellen bei mobilen Telefon- und Internetdiensten (Artikel 1 Nummer 2 Buchstabe b).

Das Entfallen von Nummern 311, 315 bis 319 ist eine Folgeänderung zur Begrenzung der anlasslosen Speicherung auf Quellen-IP-Adressen in § 176 Absatz 1 TKG n. F. und des damit verbundenen Entfalls der Auskunft über gespeicherte Verkehrsdaten in Fällen, in denen lediglich Ort und Zeitraum bekannt sind.

Zu Artikel 4 (Änderung des Bundesverfassungsschutzgesetzes)

Korrespondierend zur Übermittlungsbefugnis der Telekommunikationsdiensteanbieter wird auch eine entsprechende Abrufbefugnis des Bundesamts für Verfassungsschutz vorgesehen (§ 8a Absatz 1 Satz 3 – neu – BVerfSchG) – sog. „2. Tür“. Als Eingriffsschwelle für den Datenabruf wurde als Mindestvoraussetzung die vom Bundesverfassungsgericht als verfassungsgemäß erachtete (BVerfGE 30, 1 ff.) Eingriffsschwelle für Maßnahmen nach § 1 Absatz 1 Nummer 1 des Artikel 10-Gesetzes gewählt (§ 3 Absatz 1 des Artikel 10-Gesetzes), so dass für den Abruf gespeicherter Verkehrsdaten die gleichen Voraussetzungen gelten wie für eine Telekommunikationsüberwachung durch den Verfassungsschutz. Dies erscheint sachgerecht, weil Verkehrsdaten nicht schützenswerter als die Inhalte der Telekommunikation sind. Das Eingriffsgewicht des Abrufs von Verkehrsdaten, die vom Telekommunikationsanbieter aufgrund einer gesetzlichen Verpflichtung gespeichert wurden, ist zwar höher zu bewerten als der Abruf von (nicht verpflichtend gespeicherten) Verkehrsdaten, jedoch niedriger als bei Maßnahmen der Wohnraumüberwachung oder der Online-Datenerhebung, für die nach der verfassungsgerichtlichen Rechtsprechung die Eingriffsschwelle der „konkretisierten“ bzw. „dringenden“ Gefahr gilt (BVerfGE 162, 1 Rn. 168 f.).

Zu Artikel 5 (Einschränkung eines Grundrechts)

Die Vorschrift entspricht dem Zitiergebot, da das Grundrecht aus Artikel 10 GG durch die Regelungen in Artikel 1 und Artikel 4 eingeschränkt wird.

Zu Artikel 6 (Inkrafttreten)

Die Bestimmung regelt das Inkrafttreten des Gesetzes.

Gesamtherstellung: H. Heenemann GmbH & Co. KG, Buch- und Offsetdruckerei, Bessemerstraße 83–91, 12103 Berlin, www.heenemann-druck.de
Vertrieb: Bundesanzeiger Verlag GmbH, Postfach 10 05 34, 50445 Köln, Telefon (02 21) 97 66 83 40, Fax (02 21) 97 66 83 44, www.bundesanzeiger-verlag.de
ISSN 0722-8333