DEUTSCHER RICHTERBUND
Bund der Richterinnen und Richter,
Staatsanwältinnen und Staatsanwälte

Stellungnahme

Nr. 23/2024
Dezember 2024

Stellungnahme des Deutschen Richterbundes zum Referentenentwurf eines Gesetzes zur Einführung einer Sicherungsanordnung für Verkehrsdaten in der Strafprozessordnung

Deutscher Richterbund
Haus des Rechts
Kronenstraße 73
10117 Berlin

T +49 30 206 125-0
F +49 30 206 125-25

info@drb.de
www.drb.de

Verfasser der Stellungnahme:
Dr. Oliver Piechaczek, Staatsanwalt
Mitglied des Präsidiums

A. Tenor der Stellungnahme

Aus Sicht des Deutschen Richterbundes leistet der Referentenentwurf eines Gesetzes zur Einführung einer Sicherungsanordnung für Verkehrsdaten in der Strafprozessordnung keinen werthaltigen Beitrag zur Verbesserung der Strafverfolgung. Die fünf großen Telekommunikationsdienste-Anbieter in Deutschland speichern Verkehrsdaten mangels Mindestspeicherfristen uneinheitlich und gegenwärtig maximal für einen Zeitraum von sieben Tagen. Das Quick-Freeze-Verfahren würde es den Strafverfolgungsbehörden daher lediglich ermöglichen, innerhalb dieses sehr kurzen Zeitraums Daten zu sichern, was wiederum voraussetzt, dass sie umgehend Kenntnis von entsprechenden Straftaten erlangen. Denn nach Ablauf der individuellen Speicherdauer der Provider liefe eine Sicherungsanordnung ins Leere, ein „Einfrieren“ der Daten wäre dann nicht mehr möglich.

Noch unbekannte Tatverdächtige könnten mit dem Quick-Freeze-Verfahren daher nicht identifiziert werden, sofern die relevanten Daten zum Zeitpunkt des Auskunftsersuchens nicht mehr oder nur noch lückenhaft gespeichert sind. In solchen Fällen – die absolute Mehrzahl in der Praxis – würde die Strafverfolgung daher massiv erschwert oder gar unmöglich gemacht. Ermittlungserfolge wären bisweilen vom Zufall abhängig. Das Quick-Freeze-Verfahren kann seine Wirksamkeit daher überhaupt nur für einen äußerst limitierten Teil der in der Strafverfolgungspraxis anfallenden Fällen entfalten. Es stellt insbesondere keine sinnvolle Alternative zur europarechtlich zulässigen allgemeinen und anlasslosen Speicherung von IP-Adressen dar.

Der Deutsche Richterbund spricht sich ferner gegen die im Referentenentwurf vorgesehene Festschreibung der jüngsten Rechtsprechung des 2. Strafsenats des Bundesgerichtshofs aus, wonach Funkzellenabfragen auf den Kreis der im Katalog der besonders schweren Straftaten aufgeführten Straftatbestände zu beschränken sind. Bei Umsetzung des Vorhabens würde beispielsweise das Deliktsfeld des sogenannten „Enkeltricks“ mit all seinen denkbaren Abwandlungen (etwa „Schockanrufe“, „falsche Polizeibeamte“, „falsche Bankmitarbeiter“, „falsche Staatsanwälte“ usw.) der zielgerichteten, erfolgversprechenden Strafverfolgung entzogen. Gerade diese Arten von Straftaten verursachen aber jedes Jahr erhebliche Schäden im dreistelligen Millionenbereich und sind geeignet, das Rechtsempfinden der Bevölkerung massiv zu beeinträchtigen, weil als Opfer gezielt ältere Menschen und damit schwächere Glieder der Gesellschaft ausgewählt werden.

Gleiches gilt auch für gefährliche Körperverletzungen, die im Einzelfall mit lebensgefährdenden und bleibenden Verletzungen einhergehen können. Auch im Bereich des Staatsschutzes wäre die effektive Strafverfolgung selbst von Straftaten, hinsichtlich derer wegen der besonderen Bedeutung eine Ermittlungszuständigkeit des Generalbundesanwalts begründet ist, bedroht. So wäre etwa die Maßnahme zur Aufklärung der Strukturen solcher krimineller Vereinigungen nicht mehr zulässig, deren Ziel die Begehung körperlicher Angriffe zum Nachteil des politischen Gegners oder von ethnischen und religiösen Minderheiten ist. Auch zur Aufklärung von Straftaten der (einfachen) geheimdienstlichen Agententätigkeit oder der verfassungsfeindlichen Sabotage – etwa bei mechanischer Einwirkung auf Gleise oder Versorgungsleitungen – mit teilweise erheblichen Auswirkungen auf die Infrastruktur und mit Millionenschäden wäre die Funkzellenabfrage nicht mehr zulässig.

Mit Blick auf diese nicht hinnehmbaren Verfolgungslücken sollten das für die Praxis unverzichtbare Ermittlungsinstrument der Verkehrsdatenspeicherung in der nächsten Legislaturperiode erneut aufgegriffen und die zweifelsfrei bestehenden europarechtlichen Spielräume für eine allgemeine und anlasslose Speicherung von IP-Adressen genutzt werden. Zwei Gesetzentwürfe des Bundesrates sowie der Fraktion von CDU/CSU im Deutschen Bundestag, die eine einmonatige bzw. eine dreimonatige Speicherfrist von IP-Adressen und eventuell vergebener Port-Nummern zum Zwecke der Bekämpfung schwerer Kriminalität vorsehen, sind daher ausdrücklich zu begrüßen.

B. Bewertung im Einzelnen

I. Inhalt und Bewertung des Referentenentwurfs

Mit dem Referentenentwurf eines Gesetzes zur Einführung einer Sicherungsanordnung für Verkehrsdaten in der Strafprozessordnung soll das Ermittlungsinstrument einer Sicherungsanordnung bereits vorhandener und künftig anfallender Verkehrsdaten geschaffen werden (sog. Quick-Freeze-Verfahren). Diese grundsätzlich unter Richtervorbehalt stehende Sicherungsanordnung soll zur rein anlassbezogenen Verfolgung von erheblichen Straftaten zulässig sein, sofern Verkehrsdaten für die Erforschung des Sachverhalts oder zur Ermittlung des Aufenthaltsortes eines Beschuldigten von Bedeutung sein können. Nur die bei den Anbietern von Telekommunikationsdiensten aus geschäftlichen Gründen ohnehin bereits vorhandenen und künftig anfallenden Verkehrsdaten sollen gesichert werden („Einfrieren"). Diese Daten sollen den Strafverfolgungsbehörden maximal drei Monate für eine spätere Erhebung und Auswertung zur Verfügung stehen, wobei die Nutzung derart gesicherter Daten dann einer erneuten richterlichen Anordnung bedürfte („Auftauen").

Zudem stellt der Referentenentwurf in Anknüpfung an eine Entscheidung des 2. Strafsenats des Bundesgerichtshofs vom 10.01.2024 (2 StR 171/23 = NJW 2024, S. 2336) klar, dass die Anordnung einer Funkzellenabfrage nach § 100g Abs. 3 Satz 1 StPO den Verdacht einer besonders schweren Straftat nach § 100g Abs. 2 Satz 2 StPO voraussetzt.

1. Das Quick-Freeze-Verfahren ist kein hinreichend effektives Ermittlungsinstrument zur Bekämpfung schwerer Kriminalität im digitalen Raum

Fraglos gibt es in der Praxis zahlreiche Anwendungsfälle für die mit dem Referentenentwurf vorgesehene Sicherungsanordnung nach § 100g Abs. 6 StPO-E. Es handelt sich dabei um Konstellationen, in denen der Anfangsverdacht einer erheblichen Straftat besteht, jedoch noch keine konkreten Hinweise auf Täter oder Teilnehmer vorliegen. Auf Basis der mit der Sicherungsanordnung generierten Verkehrsdaten könnten in der Praxis in sämtlichen Deliktsbereichen der Schwerkriminalität wie etwa des Mordes oder Totschlags, des Bandendiebstahls, der Betäubungsmittelkriminalität oder der Organisierten Kriminalität Täter und Tatbeteiligte ermittelt werden.

Dies kann indes nur gelingen, wenn sich der für eine Sicherungsanordnung erforderliche Verdacht einer erheblichen Straftat binnen sehr kurzer Zeit ergibt. Denn gegenwärtig speichern die Telekommunikationsanbieter IP-Adressen lediglich zu eigenen Geschäftszwecken – etwa zum Zwecke der Abrechnung oder aus Gründen der IT-Sicherheit bzw. zur Störungsbeseitigung – für einen eng begrenzten Zeitraum. Die Bandbreite der aktuellen Speicher- und Auskunftspraxis von IP-Adressen der fünf großen Telekommunikationsanbieter in Deutschland reicht laut Eigenauskunft von null Tagen (Freenet) bis sieben Tagen (Deutsche Telekom AG, Vodafone, Telefonica, perspektivisch 1&1 Versatel); die polizeiliche Praxis berichtet partiell gar von deutlich kürzeren Speicherungszeiten (Positionspapier des BKA zu erforderlichen Speicherfristen von IP-Adressen, https://www.bka.de/SharedDocs/Kurzmeldungen/DE/Kurzmeldungen/230623_Mindestspeicherfristen_IP-Adressen.html).

Das Quick-Freeze-Verfahren würde es den Strafverfolgungsbehörden daher lediglich ermöglichen, innerhalb dieses sehr kurzen Zeitraums Daten zu sichern, was wiederum voraussetzt, dass sie umgehend Kenntnis von entsprechenden Straftaten erlangen. Denn nach Ablauf der individuellen Speicherdauer der Provider liefe eine Sicherungsanordnung ins Leere, ein „Einfrieren“ der Daten wäre dann nicht mehr möglich. Noch unbekannte Tatverdächtige könnten mit dem Quick-Freeze-Verfahren daher nicht identifiziert werden, sofern die relevanten Daten zum Zeitpunkt des Auskunftsersuchens nicht mehr oder nur noch lückenhaft gespeichert sind. In solchen Fällen – die absolute Mehrzahl in der Praxis – würde die Strafverfolgung daher massiv erschwert oder gar unmöglich gemacht. Ermittlungserfolge wären bisweilen vom Zufall abhängig. Das Quick-Freeze-Verfahren kann seine Wirksamkeit daher nur für einen äußerst limitierten Teil der in der Strafverfolgungspraxis anfallenden Fällen entfalten.

Die Annahme der Entwurfsbegründung, mit der Sicherungsanordnung würde den Strafverfolgungsbehörden ein „effektives Ermittlungsinstrument zur Bekämpfung schwerer Kriminalität im digitalen Raum an die Hand gegeben“ (Ref-E, S. 22), geht daher in dieser pauschalen Form an der Realität vorbei. Insbesondere stellt das Quick-Freeze-Verfahren keine sinnvolle Alternative zur allgemeinen und anlasslosen Speicherung von IP-Adressen dar (dazu II.). Es könnte zum Zwecke der Steigerung der Effizienz der Strafverfolgung allenfalls zusätzlich implementiert werden; insoweit stellte sich allerdings die Frage, ob Aufwand und Ertrag in einem angemessenen Verhältnis zueinander stünden.

2. Der vorgesehene Richtervorbehalt für das „Einfrieren“ von Verkehrsdaten ist nicht geboten und führt zu einer unnötigen Verfahrensverzögerung

Der Referentenentwurf sieht bereits für die Sicherung der Daten nach § 100g Abs. 6 StPO-E – das „Einfrieren“ – einen Richtervorbehalt vor, und führt zur Begründung aus, eine gerichtliche Entscheidung sei schon wegen der möglichen Breitenwirkung der Maßnahme, von der auch andere Personen als Beschuldigte und/oder Nachrichtenmittler betroffen sein können, im Sinne eines effektiven Grundrechtsschutzes geboten (Ref-E, S. 34). Dies ist jedoch aus Sicht des Deutschen Richterbundes weder europarechtlich noch verfassungsrechtlich geboten.

Der Europäische Gerichtshof hat in seiner Rechtsprechung – soweit ersichtlich – bislang keine Aussage darüber getroffen, ob der effektive Grundrechtsschutz im Rahmen des Quick-Freeze-Verfahrens beim „Einfrieren“ nur durch einen Richtervorbehalt gewährleistet werden kann. Auch verfassungsrechtlich liegt diese Annahme nicht eben nahe. Ohne Zweifel geht mit der zweiten Stufe des Quick-Freeze-Verfahrens – dem „Auftauen“ – ein nicht unerheblicher Grundrechtseingriff einher. Erst mit diesem Schritt werden die Daten einer Person bekannt und unterliegen tatsächlich dem staatlichen Zugriff. Folgerichtig sieht der Referentenentwurf für das „Auftauen“ einen Richtervorbehalt vor. Beim bloßen „Einfrieren“ hingegen – gewissermaßen der ersten Stufe des Quick-Freeze-Verfahrens – werden die Telekommunikationsdienste-Anbieter lediglich dazu verpflichtet, die Daten für einen längeren Zeitraum als denjenigen vorrätig zu halten, der für betriebliche Zwecke erforderlich ist.

In Ansehung der vergleichsweise geringen Eingriffstiefe ist eine staatsanwaltschaftliche Anordnung für das „Einfrieren“ der Daten ohne weiteres verfassungsrechtlich zulässig und ausreichend – auch ohne das Vorliegen von Gefahr im Verzug. Denn Staatsanwälte stehen Richtern mit Blick auf ihre fachliche Qualifikation, der gesetzlich gebotenen Pflicht zur Objektivität gemäß § 160 Abs. 1 und 2 StPO und ihrer Bindung an Recht und Gesetz nach Art. 20 Abs. 3 GG gleich. Die Staatsanwaltschaft fungiert als unabhängige Instanz im Ermittlungsverfahren. Vor diesem Hintergrund und nicht zuletzt, da das Bundesverfassungsgericht der Staatsanwaltschaft die Rolle als „Wächter des Gesetzes“ zuschreibt (BVerfG, NJW 2013, S. 1058 Rn. 93), ist ein Richtervorbehalt für das bloße „Einfrieren“ der Daten nicht erforderlich.

Die seitens des Europäischen Gerichtshofs mit seinem Urteil vom 20.09.2022 in den verbundenen Rechtssachen C-793/19 (SpaceNet) und C-794/19 (Telekom Deutschland) geforderte „wirksame gerichtliche Kontrolle“ einer staatsanwaltschaftlichen Anordnung könnte durch das Erfordernis einer gerichtlichen Bestätigung gewährleistet werden.

Für ein Absehen von der Verankerung eines Richtervorbehalts für das „Einfrieren“ sprechen neben rechtlichen auch rechtstatsächliche Gründe. Denn angesichts der ohnehin sehr kurzen Speicherdauer von Verkehrsdaten müssten äußerst kurzfristig gerichtliche Anordnungen getroffen werden, wobei sich der Gesetzgeber vor Augen halten sollte, dass ein nächtlicher richterlicher Bereitschaftsdienst in Deutschland nicht flächendeckend eingerichtet ist.

3. Die mit dem Referentenentwurf beabsichtigte Beschränkung der Funkzellenabfrage auf den Kreis der im Katalog der besonders schweren Straftaten aufgeführten Straftatbestände ist abzulehnen

Mit Beschluss vom 10.01.2024 hat der 2. Strafsenat des Bundesgerichtshofs eine für die Strafverfolgungspraxis durchaus folgenschwere Entscheidung (2 StR 171/23 = NJW 2024, S. 2336) getroffen. Das Gericht führt in diesem Beschluss aus, die Anordnung einer Funkzellenabfrage gemäß § 100g Abs. 3 StPO sei nur dann zulässig, wenn der Verdacht einer besonders schweren Straftat im Sinne des § 100g Abs. 2 Satz 2 StPO vorliegt. Nach Auffassung des 2. Strafsenats des Bundesgerichtshofs sei die in § 100g Abs. 3 Satz 1 Nr. 1 StPO enthaltene Verweisung auf § 100g Abs. 1 Satz 1 Nr. 1 StPO dergestalt auszulegen, dass diese zugleich die Anordnungsvoraussetzungen des § 100g Abs. 1 Satz 3 erfasse. Sofern bei einer Funkzellenabfrage kein Verdacht für eine Katalogtat im Sinne des § 100g Abs. 2 Satz 2 StPO bestehe, sei von einem Beweisverwertungsverbot auszugehen.

Folgte man dieser Rechtsauffassung, nähme man den Strafverfolgungsbehörden ein für die Aufklärung seriell begangener Einbruchstaten außerhalb von Wohnräumen sowie bei gewerbsmäßigen Betrugstaten (unter anderem dem sogenannten „Enkeltrick“) essenzielles Ermittlungsinstrument. Auch in Fällen von gefährlicher Körperverletzung, schwerer Körperverletzung und Körperverletzung mit Todesfolge sowie des Raubs oder zahlreicher Straftaten gegen die sexuelle Selbstbestimmung (etwa der Vergewaltigung durch einen Einzeltäter) wäre – legt man die

vorskizzierte Rechtsauffassung zugrunde – keine Funkzellenabfragen mehr möglich.

Die Rechtsauffassung des 2. Strafsenats des Bundesgerichtshofs ist keinesfalls unumstritten. Denn § 100g Abs. 3 Satz 1 Nr. 3 StPO verweist ausschließlich auf § 100g Abs. 1 Satz 1 Nr. 1 StPO und gerade nicht auf § 100g Abs. 1 Satz 3 StPO. Sie ist auch unter Wertungsgesichtspunkten kritisch zu betrachten. Denn der Katalog des § 100g Abs. 2 Satz 2 StPO ist eng umrissen, insbesondere enger als derjenige des § 100a Abs. 2 StPO, und benennt eine Vielzahl von erheblichen Straftaten nicht. Die Folge: Nunmehr können bei Vorliegen einiger Tatvorwürfe zwar eingriffsintensivere Telekommunikationsmaßnahmen erfolgen, die Einholung der Funkzellendaten zur Erlangung der benötigten Rufnummern soll indes nicht mehr möglich sein.

Die Rechtsauffassung des 2. Strafsenats des Bundesgerichtshofs ist bislang nicht durch Entscheidungen anderer Senate des Bundesgerichtshofs bestätigt worden. Von einer gefestigten Rechtsprechung kann daher (noch) nicht die Rede sein. Vielmehr haben sich beispielsweise das Landgericht Hamburg (Beschluss vom 06.06.2024 – 621 Qs 32/24, BeckRS 2024, 14227) sowie das Landgericht Dortmund (Beschluss vom 03.07.2024 – 36 Qs- 520 UJs 61/24-21/24) der jüngsten Rechtsprechung des 2. Strafsenats des Bundesgerichtshofs nicht angeschlossen. Beide Beschlüsse hatten Taten des banden- und gewerbsmäßigen Betrugs nach dem modus operandi des falschen Polizeibeamten zum Gegenstand. Das Landgericht Hamburg begründet seine Entscheidung damit, dass sich das Erfordernis einer Katalogtat gemäß § 100g Abs. 2 Satz 2 StPO weder im Wortlaut noch in der Systematik des Gesetzes wiederfinde und auch keine Stütze in der historischen oder der teleologischen Auslegung finde (vgl. LG Hamburg, Beschluss vom 06.06.2024 – 621 Qs 32/24, BeckRS 2024, 14227, Rn. 15 ff.).

Entsprechend hat auch die Justizministerkonferenz am 28. November 2024 den Bundesminister der Justiz aufgefordert, auf eine Anpassung des §100g StPO hinzuwirken, durch die klargestellt werde, dass das Vorliegen einer Katalogtat nach § 100g Abs.2 StPO keine zusätzliche Voraussetzung für die Anordnung einer Funkzellenabfrage nach §100g Abs. 3 Satz1 StPO darstellt.

Der Referentenentwurf schränkt nun die Möglichkeit von Funkzellenabfragen im Sinne der Rechtsprechung des 2. Strafsenats des Bundesgerichtshofs im Wege der Anpassung des Gesetzeswortlauts ein und verweist in seiner

Begründung – insoweit vergleichsweise oberflächlich – auf die „bisherige Rechtslage“, wobei als Referenz einzig die vorbezeichnete Entscheidung des 2. Strafsenats des Bundesgerichtshofs genannt wird (Ref-E, S. 28).

Der Deutsche Richterbund lehnt – wie die Justizministerkonferenz – diese Beschränkung der Funkzellenabfrage auf den Kreis der im Katalog der besonders schweren Straftaten im Sinne des § 100g Abs. 2 Satz 2 StPO aufgeführten Straftatbestände aufgrund der bereits benannten Wertungswidersprüche ab. Zudem sollten die Folgen einer solcher Beschränkung für die Strafverfolgungspraxis und das Vertrauen der Bürger in eine effektive Strafverfolgung nicht außer Acht gelassen werden.

Vor allem in Fällen des äußerst praxisrelevanten Tatbestands des gewerbs- und bandenmäßigen Betrugs wären keine Funkzellenabfragen mehr möglich. Als in der Öffentlichkeit wahrscheinlich geläufigstes und damit auch plakativstes Beispiel fällt hierunter der sogenannte „Enkeltrick“ mit all seinen denkbaren Abwandlungen (etwa „Schockanrufe“, „falsche Polizeibeamte“, „falsche Bankmitarbeiter“, „falsche Staatsanwälte“ usw.). In all diesen Fällen sind Funkzellenabfragen häufig der einzige Ansatzpunkt für weitere Ermittlungen, weil über die Einholung retrograder Verbindungsdaten ausgehend vom Anschluss des jeweiligen Opfers hinaus kaum weitere Ermittlungsansätze gewonnen werden können. Zudem handelt es sich bei den Opfern üblicherweise um ältere Mitbürgerinnen und Mitbürger, die teilweise in ihren kognitiven Fähigkeiten deutlich eingeschränkt sind, insgesamt sehr unsicher sind und von den Tätern auch genau deshalb ausgesucht werden. Es handelt sich durchweg um Zeugen, die die „Abholer“ nur unzureichend beschreiben können und denen ein Wiedererkennen in den seltensten Fällen möglich ist. Ein „Abholer“ konnte deshalb häufig nur durch Funkzellendaten mit der Tat in Verbindung gebracht bzw. der Tat überführt werden.

Mit einer gesetzlichen Festschreibung der in der Entscheidung des 2. Strafsenats des Bundesgerichtshofs zum Ausdruck kommenden Rechtsauffassung würde ein Deliktsfeld, in dem jedes Jahr erhebliche Schäden entstehen (allein in Bayern belief sich der Schaden im Jahr 2023 auf 26,3 Millionen Euro; bundesweit werden die Schadenssummen auf deutlich über 100 Millionen Euro pro Jahr geschätzt) und das geeignet ist, das Rechtsempfinden der Bevölkerung massiv zu beeinträchtigen, weil als Opfer gezielt ältere Menschen und damit schwächere Glieder der Gesellschaft ausgewählt werden, einer zielgerichteten, erfolgversprechenden Strafverfolgung entzogen.

II. Ausblick

Aus Sicht des Deutschen Richterbundes ist es dringend geboten, das Thema Verkehrsdatenspeicherung erneut aufzugreifen und die Spielräume auszunutzen, die der Europäische Gerichtshof für die allgemeine und anlasslose Speicherung von IP-Adressen eingeräumt hat. Denn die allgemeine und anlasslose Speicherung von IP-Adressen ist ein für die Strafverfolgungspraxis unverzichtbares Ermittlungsinstrument.

Zudem wäre aus Sicht der Strafverfolgungspraxis eine gesetzgeberische Klarstellung zu den Voraussetzungen einer Funkzellenabfrage nach § 100g Abs. 3 StPO wünschenswert, die dem Erfordernis einer effektiven Strafverfolgung Rechnung trägt.

Zwei aktuelle Gesetzentwürfe des Bundesrates sowie der Fraktion von CDU/CSU im Deutschen Bundestag greifen diese Anliegen der Strafverfolgungspraxis auf.

1. Die allgemeine und anlasslosen Speicherung von IP-Adressen ist ein für die Strafverfolgungspraxis besonders werthaltiges Ermittlungsinstrument

Die Bekämpfung der Deliktsbereiche Cybercrime, sexueller Kindesmissbrauch, Kinder- und Jugendpornographie sowie von Delikten, die unter den Überbegriff „Hass und Hetze im Netz“ gefasst werden, stellt einen Schwerpunkt der Strafverfolgungspraxis dar. Die enormen und stetig ansteigenden Fallzahlen in den genannten Deliktsfeldern zeigen: Straftaten werden zunehmend im oder über das Internet begangen.

All diesen Deliktsbereichen ist gemein, dass die Taten durch anonym agierende Täter im Netz begangen werden. Bei solchen im Internet begangenen Straftaten ist die IP-Adresse der zur Tatbegehung verwendeten Internetverbindung häufig der einzig tragfähige, in jedem Falle aber der schnellste und effizienteste Ermittlungsansatz, um die unbekannten Täter zu identifizieren.

Dieser Ermittlungsansatz spielt ganz besonders bei der Bekämpfung des sexuellen Missbrauchs von Kindern sowie der Kinderpornographie eine zentrale Rolle. Denn der Austausch von kinderpornographischen Inhalten findet weit überwiegend im Internet statt. Bilder und Videos werden zum Teil

in versteckten Foren, zum Teil auch öffentlich gehandelt und getauscht. Die ganz überwiegende Anzahl von Hinweisen wird dem Bundeskriminalamt durch das National Center for Missing and Exploited Children (NCMEC) übermittelt; es handelt sich hierbei um eine gemeinnützige US-amerikanische Organisation, die sich für die Belange vermisster und ausgebeuteter Kinder einsetzt. Das NCMEC wiederum erhält seine Daten von großen Internetkonzernen wie beispielsweise Google oder Facebook, die auf ihren Plattformen solche inkriminierten Inhalte festgestellt haben.

Das Bundeskriminalamt erhält auf diese Weise in der Regel den Accountnamen, zuweilen auch die E-Mail-Adresse, sowie die verwendete IP-Adresse. Ermittlungen zu den Accountnamen und E-Mail-Adressen gehen regelmäßig ins Leere, da die Dienste keine Identitätskontrollen durchführen und ohne Entgelt genutzt werden können. Nutzer können sich daher mit Alias-Daten oder Fantasienamen registrieren, ohne Zahlungsdaten hinterlegen zu müssen. Der einzig brauchbare Ermittlungsansatz ist dann die IP-Adresse.

Dieser Ermittlungsansatz verspricht allerdings nur dann Aussicht auf Erfolg, wenn eine bekannt gewordene IP-Adresse durch eine Anfrage bei dem Internet-Zugangsanbieter einem konkreten Anschlussinhaber zuzuordnen ist.

Die Relevanz dieses Ermittlungsansatzes für die Strafverfolgungspraxis ist enorm. 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 Klar-IP-Adressen zu ermitteln.

Allerdings verkennt die rechtspolitische Debatte, dass im Bereich der Bekämpfung von Kinderpornographie hohe Aufklärungsquoten, die ohne Täteridentifizierung mittels IP-Adresse erreicht werden, kein belastbares Argument gegen die Notwendigkeit der allgemeinen und anlasslosen Speicherung von IP-Adressen darstellen können. Angesichts des enormen Fallzahlenaufkommens sind in realen Zahlen mehrere tausende Fälle pro Jahr nicht aufklärbar, weil die übermittelte IP-Adresse als einziger Ermittlungsansatz aufgrund der fehlenden IP-Adressen-Speicherung bei den Providern keinem Nutzer zugeordnet werden kann. In einer Vielzahl dieser Fälle 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.

Trotz der besonderen Bedeutung dieses Ermittlungsinstruments fehlt im deutschen Recht bislang eine Regelung zur allgemeinen und anlasslosen Speicherung von IP-Adressen.

Der Deutsche Richterbund spricht sich daher für eine entsprechende gesetzliche Regelung zur Mindestspeicherung von IP-Adressen aus, die durch vergleichsweise moderate Anpassungen im Telekommunikationsgesetz möglich wäre.

2. Die Rechtsprechung des Europäischen Gerichtshofs ermöglicht eine rechtssichere Ausgestaltung der anlasslosen Speicherung von IP-Adressen zum Zwecke der Bekämpfung von internetbezogener Kriminalität

Der Europäische Gerichtshof hat mit seinem Urteil vom 20.09.2022 in den verbundenen Rechtssachen C-793/19 (SpaceNet) und C-794/19 (Telekom Deutschland) nicht lediglich festgestellt, dass die deutschen Regelungen zur Vorratsdatenspeicherung nicht mit europäischem Recht vereinbar sind. Vielmehr hat der Europäische Gerichtshof in seiner Entscheidung zugleich deutlich gemacht, welche Rechtsvorschriften im Einklang mit europäischen Grundrechten stehen könnten und damit positiv möglich wären.

Konkret hält der europäische Gerichtshof zur Bekämpfung schwerer Kriminalität „für einen auf das absolut Notwendige begrenzten Zeitraum eine allgemeine und unterschiedslose Vorratsspeicherung der IP-Adressen, die der Quelle einer Verbindung zugewiesen sind“ sowie eine Speicherung „der die Identität der Nutzer elektronischer Kommunikationsmittel betreffenden Daten“ für mit Unionsrecht vereinbar (EuGH (Große Kammer) Urteil vom 20.9.2022 – C-793/19, C-794/19 (BRD/SpaceNet AG bzw. Telekom Deutschland GmbH, in: NJW 2022, S. 3135).

Mit seinem Urteil in der Rechtssache C-470/21 vom 30.04.2024 (La Quadrature du Net ua/ Premier ministre ua, NJW 2024, S. 2099) hat der Europäische Gerichtshof diese Rechtsprechung präzisiert und zugleich gelockert: Die allgemeine und unterschiedslose Speicherung von IP-Adressen soll unter gewissen materiellen wie prozeduralen Voraussetzungen auch zur Bekämpfung allgemeiner, internetbezogener Straftaten zulässig sein. Seine

Entscheidung begründet der Europäische Gerichtshof unter anderem damit, dass die IP-Adresse bisweilen der einzige Anhaltspunkt sein kann, die Identität eines Täters zu ermitteln; bei einem unterschiedslosen Verbot jeglicher Vorratsdatenspeicherung drohe im Falle von internetbezogenen Straftaten eine systemische Straflosigkeit.

Aus alledem wird ersichtlich: Der Europäische Gerichtshof hat nicht zuletzt in seiner jüngsten Rechtsprechung den Weg für eine anlasslose Speicherung von IP-Adressen zum Zwecke der Bekämpfung von schwerer und internetbezogener Kriminalität geebnet.

3. Zu zwei aktuellen Gesetzentwürfen des Bundesrates sowie der Fraktion von CDU/CSU im Deutschen Bundestag

Ende September 2024 hat der Bundesrat auf eine Initiative der Hessischen Landesregierung hin einen Gesetzentwurf beschlossen, der eine einmonatige Speicherfrist von IP-Adressen und eventuell vergebener Port-Nummern zum Zwecke der Bekämpfung schwerer Kriminalität vorsieht; eine weitergehende Speicherung von Standortdaten ist nicht vorgesehen (BR-Drucksache 180/24).

Die CDU/CSU-Fraktion im Deutschen Bundestag hat Mitte Oktober 2024 einen insoweit weitgehend identischen Gesetzentwurf vorgelegt, der einen zentralen Unterschied aufweist: IP-Adressen und gegebenenfalls Port-Nummern sollen für die Dauer von drei Monaten gespeichert werden können (BT-Drucksache 20/13366).

Beide Gesetzesentwürfe sind aus Sicht der Strafverfolgungspraxis ausdrücklich zu begrüßen. Da beispielsweise die Generierung von IP-Adressen bei der Sicherstellung einer Plattform aus dem Bereich Cybercrime mitunter mehrere Wochen in Anspruch nehmen kann, erscheint eine dreimonatige Speicherfrist vorzugswürdig.

Der Gesetzentwurf der CDU/CSU-Fraktion im Deutschen Bundestag mindert überdies die nach Maßgabe der Rechtsprechung des 2. Strafsenats des Bundesgerichtshofs bestehende Gefahr einer stark begrenzten Möglichkeit zur Funkzellenabfrage. Der Entwurf sieht daher in Reaktion auf diese Rechtsprechung eine gesetzgeberische Klarstellung vor, wonach Funkzellenabfragen auch im Hinblick auf die regelmäßig miterfassten Standortdaten nur von den in § 100g Abs. 3 Satz 1 StPO ausdrücklich

genannten Voraussetzungen abhängen und keine Katalogtat im Sinne des § 100g Abs. 2 Satz 2 StPO erfordern.

Der Deutsche Richterbund ist mit mehr als 18.000 Mitgliedern in 25 Landes- und Fachverbänden der mit Abstand größte Berufsverband der Richterinnen und Richter, Staatsanwältinnen und Staatsanwälte in Deutschland.