DEUTSCHER RICHTERBUND
Bund der Richterinnen und Richter,
Staatsanwältinnen und Staatsanwälte

Stellungnahme

Nr. 25/23
Oktober 2023

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

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

Der Deutsche Richterbund begrüßt das mit dem Antrag der CDU/CSU-Fraktion „IP-Adressen rechtssicher speichern und Kinder vor sexuellem Missbrauch schützen“ (in der Folge: „der Antrag“) verfolgte Ziel ausdrücklich. Denn aus Sicht der Strafverfolgungspraxis besteht das Bedürfnis, den vom Europäischen Gerichtshof eingeräumten gesetzgeberischen Spielraum auszunutzen und eine allgemeine und unterschiedslose Vorratsdatenspeicherung von IP-Adressen bei schwerer Kriminalität zu ermöglichen. Dies gilt in besonderem Maße für die Verfolgung des sexuellen Missbrauchs von Kindern sowie der Kinderpornographie. Das in dem Referentenentwurf des Bundesministeriums der Justiz aus dem Jahr 2022 vorgeschlagene Quick-Freeze-Verfahren stellt keine Alternative zur allgemeinen und unterschiedslosen Vorratsdatenspeicherung von IP-Adressen dar.

B. Bewertung im Einzelnen

I. Nach der Rechtsprechung des Europäischen Gerichtshofs ist eine allgemeine und anlasslose Vorratsspeicherung von IP-Adressen unter gewissen Voraussetzungen möglich.

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, 3135)).

In der Strafprozessordnung findet sich ein Katalog von Straftaten der schweren Kriminalität. Anpassungen wären damit allenfalls im Bereich des Telekommunikationsgesetzes erforderlich, um eine Speicherung von IP-Adressen in Einklang mit dem Unionsrecht möglich zu machen (vgl. dazu Krause, ZRP 2023, 169, 171).

II. In der Praxis der Strafverfolgung besteht ein Bedürfnis für eine allgemeine und anlasslose Vorratsspeicherung von IP-Adressen.

Die Bekämpfung des Deliktsbereiches Cybercrime stellt einen Schwerpunkt der Strafverfolgungspraxis dar. Die Anzahl solcher Delikte hat sich laut Statistiken des Bundeskriminalamtes seit dem Jahr 2015 beinahe verdoppelt, wobei die tatsächlichen Zahlen angesichts des hohen Dunkelfeldes deutlich höher liegen dürften.

Für den Bereich der Kinder- und Jugendpornographie weist die Polizeiliche Kriminalstatistik etwa für das Jahr 2021 im Vergleich zum Vorjahr gar eine Verdoppelung der Fallzahlen aus. Auch Delikte, die unter den Überbegriff „Hass und Hetze im Netz“ gefasst werden, nehmen enorm zu. Daraus wird

ersichtlich: 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 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 weit 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.

Gegenwärtig speichern die Telekommunikationsanbieter IP-Adressen allerdings 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

0 Tagen (Freenet) bis 7 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, abrufbar unter https://www.bka.de/SharedDocs/Kurzmeldungen/DE/Kurzmeldungen/230623_Mindestspeicherfristen_IP-Adressen.html).

Als Ermittlungsansatz taugt die IP-Adresse daher nur dann, wenn die Telekommunikationsanbieter gesetzlich dazu verpflichtet würden, eine Speicherung der IP-Adressen durchzuführen.

Die Relevanz dieses Ermittlungsansatzes für die Strafverfolgungspraxis darf aus Sicht des Deutschen Richterbundes nicht unterschätzt werden.

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.

Das Bundeskriminalamt hat zudem in einem kürzlich veröffentlichen Positionspapier aufgezeigt, dass die Erfolgsquote im NCMEC-Prozess im Falle einer einheitlichen gesetzlichen Speicherverpflichtung von IP-Adressen (inkl. Portnummern) erheblich gesteigert werden könnte, wobei der Effekt in den ersten Wochen besonders signifikant wäre (Positionspapier des BKA zu erforderlichen Speicherfristen von IP-Adressen, abrufbar unter https://www.bka.de/SharedDocs/Kurzmeldungen/DE/Kurzmeldungen/230623_Mindestspeicherfristen_IP-Adressen.html).

Im Bereich der Bekämpfung von Kinderpornographie sind – was in der rechtspolitischen Debatte bisweilen nicht hinreichend berücksichtigt wird – hohe Aufklärungsquoten, die ohne Täteridentifizierung mittels IP-Adresse erreicht werden, aus Sicht des Deutschen Richterbundes kein belastbares Argument. 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.

III. Das in der rechtspolitischen Debatte seitens des Bundesministeriums der Justiz derzeit favorisierte Quick-Freeze-Verfahren stellt keine Alternative zur allgemeinen und anlasslosen Vorratsspeicherung von IP-Adressen dar.

Das Bundesministerium der Justiz hat im vergangenen Jahr im Anschluss an die Entscheidung des Europäischen Gerichtshofs einen Referentenentwurf eines Gesetzes zur Einführung einer Sicherungsanordnung für Verkehrsdaten der Strafprozessordnung vorgelegt. Diesem Entwurf zufolge ist beabsichtigt, die gegen europäisches Recht verstoßenden Regelungen der §§ 175-181 des Telekommunikationsgesetzes (TKG) sowie § 100g Abs. 2 StPO aufzuheben. Demgegenüber soll § 100g Abs. 5 StPO neu gefasst und damit das Ermittlungsinstrument einer Sicherungsanordnung bereits vorhandener und künftig anfallender Verkehrsdaten geschaffen werden (sog. „Quick-Freeze-Verfahren“). Diese grundsätzlich unter Richtervorbehalt stehende Sicherungsanordnung soll zur anlassbezogenen Verfolgung von erheblichen Straftaten zulässig sein, sofern die 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 dürfen („Einfrieren“). Diese Daten sollen den Strafverfolgungsbehörden für eine begrenzte Zeit für eine spätere Erhebung und Auswertung zur Verfügung stehen, wobei dies dann einer erneuten richterlichen Anordnung bedürfte („Auftauen“).

Eine solche „Quick-Freeze-Regelung“ stellt keine Alternative zur allgemeinen und anlasslosen Vorratsspeicherung von IP-Adressen dar.

Wie bereits erläutert, speichern die fünf großen Telekommunikationsanbieter in Deutschland die IP-Adressen gegenwärtig maximal für einen Zeitraum von 7 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 sehr früh Kenntnis von entsprechenden Straftaten erlangen. Nach Ablauf der individuellen Speicherdauer der Provider hingegen liefe eine Sicherungsanordnung ins Leere, ein „Einfrieren“ der Daten ist dann nicht mehr möglich. Noch unbekannte Tatverdächtige können mit dem Quick-Freeze-Verfahren daher nicht identifiziert werden, sofern die relevanten Daten zum Zeitpunkt des Auskunftsersuchens nicht mehr oder lückenhaft

gespeichert sind. In solchen Fällen, die die absolute Mehrzahl der Praxis bilden, würde die Strafverfolgung im Bereich von schwerer Kriminalität, wie etwa dem sexuellen Missbrauch von Kindern, daher massiv erschwert.

Der Deutsche Richterbund ist mit mehr als 17.500 Mitgliedern in 25 Landes- und Fachverbänden (bei bundesweit mehr als 25.000 Richtern und Staatsanwälten insgesamt) der mit Abstand größte Berufsverband der Richterinnen und Richter, Staatsanwältinnen und Staatsanwälte in Deutschland.