GESELLSCHAFT FÜR FREIHEITSRECHTE

10. Oktober 2023

Stellungnahme

zu dem Antrag der Fraktion der CDU/CSU „IP-Adressen rechtssicher speichern und Kinder vor sexuellem Missbrauch schützen“ (BT-Drs. 20/3687)

für die mündliche Anhörung im Rechtsausschuss des Deutschen Bundestags

am 11. Oktober 2023

von RA Dr. Bijan Moini M.A.,
Legal Director, Gesellschaft für Freiheitsrechte e.V.

A. Zusammenfassung

Eine sechsmonatige Vorratsspeicherung von IP-Adressen aller Internetnutzer*innen würde sie in ihren Grundrechten aus Art. 7, 8 und 11 der EU-Grundrechtecharta und in Art. 10 Grundgesetz verletzen. Mit Blick auf die Möglichkeiten zur Verschleierung von IP-Adressen würden viele Täter*innen nicht mit Hilfe der Vorratsspeicherung von IP-Adressen ermittelt werden können. Zielführender wären andere Maßnahmen, insbesondere die konsequente Löschung bekannter Kindesmissbrauchsdarstellungen im Internet und die Verhinderung von Kindesmissbrauch selbst.

Dem unzweifelhaft großen Gewicht, das die Aufklärung der Verbreitung von Kindesmissbrauchsdarstellungen im Internet hat, stünde zudem das noch größere Gewicht einer tiefgreifenden anlasslosen Massenüberwachung gegenüber. IP-Adressen sind höchst sensibel und

erlauben tiefe Einblicke in die Persönlichkeiten der Betroffenen. Unter diesen Betroffenen wären praktisch alle Menschen in Deutschland, obwohl so gut wie niemand von ihnen Anlass zur Speicherung ihrer IP-Adressen auf Vorrat geboten hat. So unverhältnismäßig es im analogen Leben wäre, monatelang zu speichern, welche Orte Menschen besuchen, wen sie dort treffen, was sie dort sagen oder tun, so wenig wäre es angemessen, das Verhalten unschuldiger Menschen im Netz auf diese Weise zu überwachen.

Aus der Rechtsprechung des EuGH und des Bundesverfassungsgerichts ergibt sich nicht mit der häufig vorgetragenen Sicherheit, dass eine Vorratsspeicherung von IP-Adressen vor Gericht Bestand hätte. Unabhängig davon ist Verfassungsrechtsprechung kein politisches Programm. Nur weil etwas ein Gerichtsverfahren überstehen könnte, ist es nicht legitim.

Die Gesellschaft für Freiheitsrechte rät deshalb davon ab, die beantragte gesetzliche Regelung zu treffen.

B. Antrag

Die CDU/CSU-Bundestagsfraktion fordert mit ihrem Antrag vom 27. September 2022 unter dem Titel „IP-Adressen rechtssicher speichern und Kinder vor sexuellem Missbrauch schützen“ (im Folgenden der „**Antrag**“) vom Deutschen Bundestag, die Bundesregierung dazu aufzufordern, einen Gesetzentwurf für eine Pflicht für Telekommunikationsdienste zur sechsmonatigen Speicherung von IP-Adressen vorzulegen. Der Entwurf soll auch eine praxistaugliche Regelung zur Speicherung von Portnummern, ein hohes Datenschutzniveau, sichere und schnelle Abrufverfahren und eine Eilzuständigkeit der Staatsanwaltschaft enthalten.

Zur Begründung führt der Antrag aus, „Jahr für Jahr“ könnten „abertausende nachweislich in Deutschland begangene Taten nicht aufgeklärt werden, weil die notwendigen IP-Adress-Daten zur Ermittlung der Täter mangels Speicherung nicht mehr verfügbar sind“. Wenn kinderpornografisches Material digital aufgespürt werde, sei die IP-Adresse häufig die einzige Spur zum Täter. Nur mit Hilfe dieser Identifikation, die einem Computer oder anderen Endgeräten beim Surfen vom Provider zugewiesen werde – „vergleichbar einem temporären digitalen Autokennzeichen“ –, ließen sich die Täter ermitteln.

Der Gerichtshof der Europäischen Union („**EuGH**“) eröffne mit seiner Rechtsprechung zur Vorratsspeicherung von Telekommunikationsdaten – zur deutschen Rechtslage in seinem Urteil vom 20. September 2022 in den verbundenen Rechtssachen C-793/19 (SpaceNet) und C-794/19

(Telekom Deutschland) – die Möglichkeit zu einer entsprechenden Regelung. Demgegenüber seien andere Vorschläge wie das Quick-Freeze-Verfahren „nach einhelliger Einschätzung der Ermittlungsbehörden untauglich".

C. Bewertung

I. Zweck des geforderten Gesetzes

Entgegen dem Titel des Antrags hätte eine Vorratsspeicherung von IP-Adressen nicht den primären Zweck, Kinder vor sexuellem Missbrauch zu schützen. Kinder werden weit überwiegend im sozialen Nahfeld missbraucht, zu dessen Aufklärung die IP-Adressen in der Regel keinen Beitrag leisten. Das angestrebte Gesetz soll vielmehr – wie sich trotz der irreführenden Zahlen im ersten Absatz des Antrags aus der weiteren Begründung ergibt – in erster Linie die Aufklärung von Straftaten nach §§ 184b, 184c StGB (Verbreitung, Erwerb und Besitz kinder- bzw. jugendpornographischer Inhalte) erleichtern. Auch dieser Zweck hat unzweifelhaft einen hohen Stellenwert.

Erreicht werden soll dies, indem eine Zuordnung von IP-Adressen, die im Zusammenhang mit solchen Straftaten ermittelt wurden, zu den Inhaber*innen der betreffenden Anschlüsse durch die Telekommunikationsunternehmen zuverlässiger gelingt und über einen längeren Zeitraum als bislang möglich bleibt.

II. Rechtliche Maßstäbe

Nach der Rechtsprechung des **EuGH** ist davon auszugehen, dass eine gesetzliche Pflicht zur Vorratsspeicherung von IP-Adressen in den Anwendungsbereich des Unionsrechts fiele, namentlich in den Geltungsbereich der Richtlinie 2002/58 („**ePrivacy-RL**")[1]. Dadurch beansprucht auch die Charta der Grundrechte der Europäischen Union („**Charta**") Geltung. Aus Art. 15 Abs. 1 der ePrivacy-RL sowie aus Art. 7 (Achtung des Privat- und Familienlebens), Art. 8 (Schutz personenbezogener Daten) und Art. 11 (Freiheit der Meinungsäußerung und Informationsfreiheit) hat der EuGH für die Vorratsspeicherung von Telekommunikationsdaten abgeleitet, dass sie nicht zur allgemeinen und unterschiedslosen Vorratsspeicherung von Verkehrs- und Standortdaten verpflichten darf.

Diese Daten könnten „Informationen über eine Vielzahl von Aspekten des Privatlebens der Betroffenen enthalten [ ], einschließlich sensibler Informationen wie sexuelle Orientierung,

[1] S. zuletzt EuGH, Urt. v. 20.09.2022 – Rs. 793/19 (SpaceNet) –, Rn. 48 m.w.N.

politische Meinungen, religiöse, philosophische, gesellschaftliche oder andere Überzeugungen sowie den Gesundheitszustand". Das erlaube sehr genaue Schlüsse auf das Privatleben der Personen, deren Daten gespeichert würden, einschließlich eines Profils der Betroffenen.[2] Außerdem begründe die Menge an gespeicherten Daten Gefahren des Missbrauchs und des rechtswidrigen Zugangs.[3] Auch für die Vorratsspeicherung von IP-Adressen erkennt der EuGH an, dass sie zur umfassenden Nachverfolgung der von einem Internetnutzer besuchten Internetseiten und infolgedessen seiner Online-Aktivität genutzt werden könne, sodass diese Daten die Erstellung eines detaillierten Profils dieses Nutzers ermöglichten.[4]

Der EuGH hält vor diesem Hintergrund eine Vorratsdatenspeicherung nur für grundrechtskonform, wenn sie zur Bekämpfung schwerer Kriminalität und zur Verhütung schwerer Bedrohungen der öffentlichen Sicherheit

- 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 eine gezielte Vorratsspeicherung von Verkehrs- und Standortdaten vorsehen;
- **für einen auf das absolut Notwendige begrenzten Zeitraum eine allgemeine und unterschiedslose Vorratsspeicherung der IP-Adressen, die der Quelle einer Verbindung zugewiesen sind, vorsehen**;
- eine allgemeine und unterschiedslose Vorratsspeicherung der die Identität der Nutzer elektronischer Kommunikationsmittel betreffenden Daten vorsehen;
- vorsehen, dass den Betreibern elektronischer Kommunikationsdienste mittels einer Entscheidung der zuständigen Behörde, die einer wirksamen gerichtlichen Kontrolle unterliegt, aufgegeben werden kann, während eines festgelegten Zeitraums die ihnen zur Verfügung stehenden Verkehrs- und Standortdaten umgehend zu sichern (quick freeze).[5]

Zu berücksichtigen sind weiter die Grundrechte des deutschen Grundgesetzes, wenn man richtigerweise nicht von einer Vollharmonisierung des „Rechts der Vorratsdatenspeicherung" durch die ePrivacy-RL ausgehen möchte. Eine nationale Regelung, die unionsrechtlich nicht voll determiniert ist, überprüft das **Bundesverfassungsgericht** (primär) am Maßstab des

[2] EuGH, Urt. v. 20.09.2022 – Rs. 793/19 (SpaceNet) –, Rn. 61 m.w.N.
[3] EuGH, Urt. v. 20.09.2022 – Rs. 793/19 (SpaceNet) –, Rn. 62 m.w.N.
[4] EuGH, Urt. v. 20.09.2022 – Rs. 793/19 (SpaceNet) –, Rn. 79 m.w.N.
[5] EuGH, Urt. v. 20.09.2022 – Rs. 793/19 (SpaceNet) –, Rn. 75 m.w.N.

Grundgesetzes.[6] Das Bundesverfassungsgericht hat sich in seinem Urteil vom 2. März 2010 – 1 BvR 256/08 u.a. – ausführlich mit der Vorratsdatenspeicherung befasst. Danach hält es die Vorratsdatenspeicherung nur unter engen Voraussetzungen für verfassungsgemäß.[7]

Das Gericht hat in seinem Urteil auch die besondere **Bedeutung und Aussagekraft von IP-Adressen** herausgestellt. Da der Inhalt von Internetseiten anders als das beim Telefongespräch gesprochene Wort elektronisch fixiert und länger wieder aufrufbar sei, lasse sich mit ihr vielfach verlässlich rekonstruieren, mit welchem Gegenstand sich der Kommunizierende auseinandergesetzt habe. Die Individualisierung der IP-Adresse als der „Telefonnummer des Internet" gebe damit zugleich Auskunft über den Inhalt der Kommunikation. Die für das Telefongespräch geltende Unterscheidung von äußerlichen Verbindungsdaten und Gesprächsinhalten löse sich hier auf. Werde der Besucher einer bestimmten Internetseite mittels der Auskunft über eine IP-Adresse individualisiert, wisse man nicht nur, mit wem er Kontakt gehabt habe, sondern **kenne in der Regel auch den Inhalt des Kontakts**.[8]

Gleichwohl könne der Gesetzgeber zur Gewährleistung einer verlässlichen Zuordnung der IP-Adressen über einen gewissen Zeitraum die Vorhaltung der entsprechenden Daten beziehungsweise einen weitgehenden Rückgriff auf insoweit vorgehaltene Daten seitens der Diensteanbieter vorsehen.[9] Zugleich betonte das Bundesverfassungsgericht jedoch, dass die Vorratsdatenspeicherung nicht auch die Kommunikationsinhalte erfassen dürfe und dass auch die Speicherung der von ihren Kunden aufgerufenen Internetseiten durch kommerzielle Diensteanbieter grundsätzlich untersagt sei.[10]

III. Eingriffstiefe

Die Vorratsspeicherung von IP-Adressen greift tief in Grundrechte ein. Sowohl der EuGH als auch das Bundesverfassungsgericht erkennen das zwar an, ziehen daraus aber nur unzureichende Konsequenzen. Die oben zusammengefasste Rechtsprechung ist von der Vorstellung geprägt, IP-Adressen hätten insbesondere gegenüber Verkehrs- und Standortdaten ein geringeres Gewicht.

[6] BVerfG, Urt. v. 06.11.2019 – 1 BvR 16/13 –, Ls. 1 (Recht auf Vergessen I).
[7] BVerfG, Urt. v. 2.03.2010 – 1 BvR 256/08 –, Rn. 220 ff.
[8] BVerfG, Urt. v. 2.03.2010 – 1 BvR 256/08 –, Rn. 259.
[9] BVerfG, Urt. v. 2.03.2010 – 1 BvR 256/08 –, Rn. 260.
[10] BVerfG, Urt. v. 2.03.2010 – 1 BvR 256/08 –, Rn. 218.

Diese Annahme ist unzutreffend. **IP-Adressen sind** – insbesondere in Zusammenhang mit den im Antrag ebenfalls in den Blick genommenen Portnummern – **höchst sensible Daten**. Sie erlauben nachzuvollziehen, was Internetnutzer*innen gelesen, gehört, gesehen oder gesucht haben, welchen Meinungsbeitrag sie veröffentlicht, welche Datei sie heruntergeladen, welche Produkte, Dienstleistungen und Applikationen sie betrachtet oder bestellt bzw. in Anspruch genommen haben. Es sind also im Kern Inhaltsdaten, die über die IP-Adresse einer*m Anschlussinhaber*in zugeordnet werden. Insgesamt ist das Überwachungspotenzial von IP-Adressen größer als z.B. das von Telefonverbindungsdaten: über die allermeisten Menschen lässt sich durch ihre Bewegungen im Internet sehr viel mehr erfahren als durch ihre Telefonkontakte: politische Überzeugungen, sexuelle Präferenzen, religiöse, philosophische, gesellschaftliche oder andere Überzeugungen, der Gesundheitszustand usw.

Die **Sensibilität** der Speicherung von IP-Adressen hat sich in den vergangenen Jahren zudem dadurch **weiter erhöht**, dass die Nutzung des Internets in diesem Zeitraum stark zugenommen hat. Während im Jahr 2010 – zum Zeitpunkt des oben referierten Urteils des Bundesverfassungsgerichts – nur 72 % der Menschen in Deutschland das Internet nutzten, waren es im Jahr 2022 bereits 93 %. Unter den 14-49-Jährigen sind es nahezu alle.[11] Noch signifikanter ist die *Dauer* der Internetnutzung gestiegen: Allein zwischen 2015 und 2022 wuchs sie von 40 auf 65 Stunden pro Woche an.[12] Damit korrespondieren die von Sicherheitsbehörden vorgetragenen gestiegenen Zahlen von festgestellten Straftaten nach §§ 184b f. StGB mit dem Tatmittel Internet.

Durch die gestiegenen Zahlen der Nutzer*innen und der jeweiligen Nutzungsdauer ist die Quantität und – weil sich zugleich immer wesentlichere Teile des Lebens ins Netz verlagern – die Sensibilität der potentiell mit IP-Adressen verknüpfbaren Internetkommunikation in einem Maße gestiegen, die in folgerichtiger Anwendung der vom EuGH aufgestellten Maßstäbe, wonach insbesondere die Menge der gespeicherten Daten die Eingriffsintensität verstärkt, zu einer Neubewertung der angeblich geringeren Eingriffstiefe der Vorratsspeicherung von IP-Adressen zwingt.

Aufgrund der Sensibilität von IP-Adressdaten ist der **Vergleich**, den der Antrag **zwischen IP-Adressen und Kfz-Kennzeichen** zieht, nicht nur schief, sondern er liegt quer: Der

[11] Zitiert nach Statista, online abrufbar unter https://de.statista.com/statistik/daten/studie/13070/umfrage/entwicklung-der-internetnutzung-in-deutschland-seit-2001/ (Stand: 9.10.2023).
[12] Zitiert nach Statista, online abrufbar unter https://de.statista.com/statistik/daten/studie/875957/umfrage/dauer-der-internetnutzung-pro-woche-in-deutschland/ (Stand: 9.10.2023).

Vorratsspeicherung von IP-Adressen würde es im realen Leben von Kfz-Fahrer*innen entsprechen, über mehrere Monate einen Abgleich zu ermöglichen zwischen allen Kfz-Kennzeichen und jenen Orten, die Fahrzeuge mit diesen Kennzeichen besucht haben: die Arztpraxis, die Strafrechtskanzlei, die politische Veranstaltung, die Affäre usw. Das Pendant zur Vorratsspeicherung von IP-Daten wäre also die deutschlandweite Nachvollziehbarkeit aller Bewegungen von Kraftfahrzeugen auf Vorrat, nicht die Speicherung der Kfz-Kennzeichen beim Kraftfahrbundesamt. Anders als im Bereich des Individualverkehrs per Kfz, der sich durch Rad, Bus, Bahn oder – je nach Entfernung – durch Zufußgehen oder Flugzeug ersetzen lässt, gibt es außerdem im Netz für technisch Unversierte keine Alternative zur Nutzung von IP-Adressen.

Die **Gefahren** aus der Vorratsspeicherung von IP-Adressen sind vielfältig. Denkbar ist eine abschreckende Wirkung für die freie Nutzung des Internets, wenn alle damit rechnen müssen, dass ihre Bewegungen im Netz monatelang rückverfolgt werden können (Chilling Effect). IP-Adressdaten können aber auch versehentlich oder absichtlich zweckentfremdet oder von Kriminellen oder Nachrichtendiensten entwendet und zur Schädigung der Betroffenen eingesetzt werden. Gerade heute, da Instrumente zur KI-gestützten Massendatenverarbeitung sowie zur zunehmend ebenfalls KI-gestützten Ausnutzung der erworbenen Erkenntnisse für Erpressungen und Betrugsmaschen immer leichter verfügbar sind, ist die Gefahr, die von zweckentfremdeten IP-Adressdaten ausgeht, nicht zu überschätzen.

Umgekehrt ist nicht zu unterschätzen die Erhöhung der Gefahr von **falschen Verdächtigungen** und damit zusammenhängenden Folgemaßnahmen, die sich gegen die Falschen richten. Schon heute bezieht sich ein großer Teil der Verdachtsfälle, die deutsche Behörden über NCMEC erreichen, auf Kommunikation von Minderjährigen, die häufig straflos ist. Gerade über Chatgruppen, in denen z.B. Bilder geteilt werden, können sehr viele Personen rasch zu Unrecht inkriminiert werden, worüber in der Regel nicht bereits die IP-Adresse Aufschluss gibt. Schon die Aufklärung des falschen Verdachts kann die Betroffenen schwer belasten, durch polizeiliche Vorladungen, die Beschlagnahme von Smartphones oder gar Hausdurchsuchungen. Mit einer Steigerung der Fälle von IP-basierten Ermittlungen würde das Risiko für solche Belastungen steigen. Das gälte erst recht, sollte es auf EU-Ebene tatsächlich zu der sogenannten Chatkontrolle kommen, also einer Pflicht u.a. von Messengerdiensten, die Verbreitung vermeintlich strafbarer Kindesmissbrauchsdarstellungen an die Strafverfolgungsbehörden zu melden.

IV. Verhältnismäßigkeit

Mit Blick auf das hohe Eingriffsgewicht wäre eine gesetzliche Pflicht zur sechsmonatigen Speicherung von IP-Adressen durch Telekommunikationsdienste unverhältnismäßig. Der Mehrwert für die Aufklärung von internetbasierten Fällen von Straftaten nach §§ 184b, 184c StGB steht in keinem Verhältnis zur Eingriffstiefe einer Vorratsspeicherung von IP-Adressen.

IP-Adressen sind zu dem verfolgten Zweck schon nur begrenzt geeignet. Die **Verschleierung von IP-Adressen** ist heute nicht nur bei der Nutzung des sog. Darknets einfacher denn je. Es liegt auf der Hand, dass Menschen, die mit einer entsprechenden kriminellen Energie Kindesmissbrauchsdarstellungen verbreiten oder erwerben, spätestens mit Einführung einer Vorratsspeicherung von IP-Adressen Dienste zu deren Verschleierung nutzen werden. Schon jetzt tauschen Pädokriminelle „Sicherheitstipps" aus, die darauf gerichtet sind, keine Datenspuren zu hinterlassen, die als Ermittlungsansätze dienen könnten.[13] Ins Netz gingen den Ermittler*innen damit viele Unbedarfte wie zum Beispiel Minderjährige, während zugleich massenhaft völlig unbescholtene Menschen mit der Vorratsspeicherung ihrer IP-Adressen belastet würden.

Zu bedenken sind weiter die **Alternativen zur Vorratsspeicherung von IP-Adressen**, die zum Schutz von Kindern vor Missbrauch ergriffen werden könnten. Es fehlt hier der Raum, auf diese im Einzelnen einzugehen. Sehr effektiv wäre etwa das konsequente Löschen von Kindesmissbrauchsdarstellungen im Internet, die den Ermittlungsbehörden bereits bekannt sind. Mit Blick auf die Strafverfolgung sind das Quick-Freeze-Verfahren und die Login-Falle zu nennen, die die Grundrechte deutlich mehr schonen als die Vorratsdatenspeicherung. Wesentlich wirksamer wären aber insbesondere jene Maßnahmen, die das Übel an der Wurzel packen, also den dargestellten Missbrauch von Kindern selbst angehen: Die Stärkung der klassischen Polizeiarbeit, effektivere Führungsaufsicht für Straftäter*innen, die Erstellung von Schutzkonzepten in Einrichtungen wie Schulen, Kindertagesstätten, Heimen, Sportvereinen, Kliniken oder Kirchengemeinden, die zuverlässige Bearbeitung von Verdachtsmeldungen durch Vereine, Schulen und Ärzt*innen, die Beratung von Betroffenen oder die Präventionsarbeit mit Pädophilen. Das wäre aufwendiger, verspräche aber größeren Erfolg.

Die anlasslose **Vorratsspeicherung von IP-Adressen** wäre aber auch unabhängig davon **unangemessen**. Sie ist nicht Überwachung light, sondern bedeutet eine Massenüberwachung aller Internetnutzer*innen. Nahezu keine*r dieser Internetnutzer*innen hat Anlass für die

[13] Moßbrucker, Direkt vor unseren Augen, Droemer Verlag, München 2023, S. 220.

Vorratsspeicherung seiner IP-Adressen gegeben, weil unter ihnen nur ein verschwindend geringer Anteil an Täter*innen ist. Trotzdem wären alle Menschen gleichermaßen von der monatelangen Vorratsspeicherung sehr sensibler Daten und von den oben beschriebenen Missbrauchsgefahren betroffen. So unverhältnismäßig es im analogen Leben wäre, aufzuzeichnen und monatelang zu speichern, welche Orte Menschen besuchen, wen sie dort treffen, was sie dort sagen oder tun, so wenig wäre es angemessen, das Verhalten unschuldiger Menschen im Netz auf diese Weise zu überwachen.

Trotz der oben skizzierten Rechtsprechung besteht mindestens Unsicherheit darüber, dass nicht auch der **EuGH und das Bundesverfassungsgericht** in konsequenter Anwendung der oben skizzierten Rechtsprechungsmaßstäbe zu der Unangemessenheit einer Vorratsspeicherung von IP-Adressen kämen. Der EuGH hat sich zu dieser Form der Vorratsdatenspeicherung nur flüchtig geäußert, wohl auch unter dem Druck, seine als zu streng empfundene Rechtsprechung zu lockern. Weil es auf seine Erwägungen zur Vorratsspeicherung von IP-Adressen in den jeweiligen Verfahren nicht entscheidend ankam, sind sie sehr kurz geblieben. Eine genauere Prüfung könnte den EuGH dazu führen, vor dem Hintergrund des immer weiter steigenden Eingriffsgewichts einer Vorratsspeicherung von IP-Adressen seine für Verkehrs- und Standortdaten formulierten Beschränkungen auch auf IP-Adressen zu übertragen. Zu einer ähnlichen Einschätzung könnte auch das Bundesverfassungsgericht kommen, zumal es selbst anerkennt, dass die Zuordnung von IP-Adressen zu bestimmten Kommunikationsvorgängen im Internet diese faktisch zu Inhaltsdaten macht. Außerdem wäre das Bundesverfassungsgericht bei einer nicht unionsrechtlich geprägten Vorratsdatenspeicherung deutlich freier in seiner Beurteilung als bei seinem Urteil von 2010, das vor dem Hintergrund der Richtlinie 2006/24/EG zur Vorratsdatenspeicherung erging.

Unangemessen wäre in jedem Fall die im Antrag vorgesehene **Speicherdauer von sechs Monaten**. Der EuGH stellt nur in den Raum, dass IP-Adressen ggf. über einen auf das „absolut Notwendige begrenzten Zeitraum" auf Vorrat gespeichert werden könnten (s. oben II.). Das Bundeskriminalamt geht bei einer 7-tätigen Speicherfrist davon aus, dass drei Viertel aller Zuordnungsversuche erfolgreich wären, bei einer Speicherfrist von 26 Tagen über 90 %.[14] Unterstellt, dass diese Zahlen tatsächlich richtig sind, wäre der Mehrwert einer um ein Vielfaches längeren Speicherfrist unangemessen gering.

[14] Präsentation der Vizepräsidentin des Bundeskriminalamts Martina Link vor dem Familienausschuss des Deutschen Bundestags am 21.06.2023, S. 7, online abrufbar unter: https://cdn.netzpolitik.org/wp-upload/2023/06/2023-06-21_BKA_Bedeutung-IP-Adresse.pdf (Stand: 9.10.2023).

V. Begehrlichkeiten

Ein eher rechtspolitisches Argument, das es aber bei der Bewertung der Vorratsspeicherung von IP-Adressen zu berücksichtigen gilt, ist das Wecken von Begehrlichkeiten für einmal bevorratete IP-Adressdaten aller Menschen in Deutschland. Es ist absehbar, dass der Zugriff auf diese Daten sich nicht lange auf die Verfolgung der im Antrag genannten Straftaten begrenzen, sondern dass der **Katalog bald erweitert** würde. Wahrscheinlich ist auch, dass es rasch nicht mehr nur um Strafverfolgung, sondern **auch** um **Gefahrenabwehr** ginge, schließlich sogar um **nachrichtendienstliche Aufklärung**, für die wiederum der Zugriff auf Daten generell unter geringeren Voraussetzungen zulässig ist als zur Strafverfolgung und Gefahrenabwehr. Dadurch würden schrittweise der Kreis der auskunftsberechtigten Stellen, die Anzahl von Abfragen und das Risiko für Missbrauch und unberechtigte Folgemaßnahmen erheblich steigen. Etablierte sich die Vorratsspeicherung von IP-Adressen, stünde mittelfristig auch die Vorratsspeicherung weiterer Daten zur Debatte.

Ein Verzicht auf die Vorratsspeicherung von IP-Adressen wäre also auch eine Absage an eine Entwicklung, die unter Ausnutzung der Errungenschaften des Internets die Menschen immer umfassender und intensiver erfasst und durchleuchtet.

Gesellschaft für Freiheitsrechte e.V.
Boyenstraße 41
10115 Berlin

info@freiheitsrechte.org
Amtsgericht Berlin-Charlottenburg
Registernummer VR 34505 B

GLS Gemeinschaftsbank eG
IBAN · DE 88 4306 0967 1182 9121 00
BIC · GENODEM1GLS