Tom Jennissen
Digitale Gesellschaft e. V.
Groninger Str. 7
D - 13347 Berlin
(030) 450 840 18
info@digitalegesellschaft.de
www.digitalegesellschaft.de

Berlin, den 10.10.2023

IP-Adressen rechtssicher speichern und Kinder vor sexuellem Missbrauch schützen (BT-Drucksache 20/3687)

Stellungnahme der Digitalen Gesellschaft für den Rechtsausschuss des Deutschen Bundestages zum Antrag der CDU/CSU-Fraktion (BT-Drs. 20/3687).

Summary

Die Vorratsdatenspeicherung von IP-Adressen greift massiv in die durch Grundgesetz und Grundrechtecharta garantierten Rechte ein und ist – auch in der durch den Antrag BT-Drs. 20/3687 vorgeschlagenen Form unverhältnismäßig. Insbesondere ist sie nicht geeignet, sexualisierte Gewalt gegen Kinder zielführend und effektiv zu bekämpfen. Ein an dem Antrag orientiertes Gesetz würde den Maßgaben des Europäischen Gerichtshofs (EuGH) nicht gerecht und einer Prüfung nicht standhalten.

Das hoch emotionalisierte Thema der sexualisierten Gewalt gegen Kinder sollte nicht erneut gegen fundamentale Grundrechte ausgespielt werden, sondern in seine Komplexität erkannt und angegangen werden. Gerade in einer weitgehend digitalisierten Welt ist es wichtig, umfassend auf Aufklärung, Unterstützung und Prä-

vention zu setzen, statt mit einer allgemeinen Massenüberwachung das Vertrauen in staatliche Stellen weiter auszuhöhlen.

Sollte der Gesetzgeber sich zu einem weiteren Anlauf entscheiden, droht angesichts der Vielzahl von offenen rechtlichen Fragen eine weitere Hängepartie, die nicht nur zu Rechtsunsicherheit bei den Strafverfolgungsbehörden führen würde, sondern angesichts der damit einhergehenden anlasslosen Massenüberwachung auch geeignet ist, das Vertrauen der Bevölkerung in rechtsstaatliche Verfahren weiter zu untergraben.

Schon seit Jahrzehnten beflügelt die fortschreitende Digitalisierung die Fantasien von Politik und Strafverfolgung, da sie ungeahnte Möglichkeiten von massenhafter Überwachung technisch ermöglicht. Doch das Ausreizen dessen, was technisch möglich und verfassungsrechtlich gerade noch vertretbar ist, ist das Gegenteil einer den Grundrechten verpflichteten, zukunftsweisenden Politik.

Es ist an der Zeit die politisch und rechtlich vielfach begrabene Vorratsdatenspeicherung endlich ruhen zu lassen und den Schutz von Kindern ernsthaft und nachhaltig anzugehen.

Ausgangslage

Am 20. September 2022 hat der EuGH sein lange erwartetes Urteil zur deutschen Vorratsdatenspeicherung verkündet (berichtigt durch Beschluss vom 27. Oktober 2022, C-793 u. C-794). Wenig überraschend hat er seine langjährige Rechtsprechung bestätigt und die deutschen Regelungen für nicht mit europäischem Recht vereinbar erklärt. Die bisherigen Regelungen im Telekommunikationsgesetz (TKG) waren bereits seit 2017 ausgesetzt. Nachdem das Verwaltungsgericht Köln schon festgestellt hatte, dass die deutsche Regelung rechtswidrig ist, hatte das Bundesverwaltungsgericht (BVerwG) die Frage dem EuGH vorgelegt.

Dass der EuGH in Fortsetzung seiner ständigen Rechtsprechung die deutsche Regelung für europarechtswidrig erachten würde, war abzusehen. Dennoch wurde

– etwa bei der Novellierung des Telekommunikationsgesetzes (TKG) – an der anlasslosen Massenüberwachung festgehalten. Mit Urteil vom 14. August 2023 hat das BVerwG die entsprechenden §§ 175 Abs. 1 S. 1, 176 TKG nun endgültig für unanwendbar erklärt.

Bereits im Jahr 2002 wurde auf europäischer Ebene das anlasslose Speichern von Telekommunikationsdaten durch einen entsprechenden Vorschlag der Ratspräsidentschaft zum ersten Mal aufgebracht. Seither wurden auf europäischer und nationaler Ebene verschiedene Anläufe für eine Vorratsdatenspeicherung unternommen, die regelmäßig vor den Gerichten scheiterten. Während die Forderung nach der Speicherung von Telekommunikationsdaten zunächst ganz überwiegend mit dem Kampf gegen den internationalen Terrorismus begründet wurde, kamen über die Jahrzehnte weitere Deliktsbereiche hinzu – derzeit verhandelt der EuGH etwa über eine französische Regelung zur Speicherung von IP-Adressen zum Zweck der Verfolgung von Urheberrechtsverletzungen.

Rechtliche Unsicherheit

Diese beharrlichen Versuche, eine Vorratsdatenspeicherung einzuführen, haben in der Bevölkerung nicht nur zu einer großen Unsicherheit über das Ausmaß staatlicher Überwachung geführt und sind damit geeignet das Vertrauen in die Wahrung zentraler Grundrechte zu erschüttern. Sie haben auch dazu beigetragen, dass die zuständigen Behörden mit großer Verzögerung überhaupt angefangen haben, die nötigen technischen und personellen Kompetenzen für zielgerichtete und den Anforderungen einer weitgehend digitalisierten Welt gerecht werdende Ermittlungsmethoden zu entwickeln.

Jeder weitere Versuch der Einführung einer anlasslosen Massenüberwachung wird unweigerlich erneut vor den Gerichten enden. Und da trotz der mittlerweile Jahrzehnte währenden politischen und rechtlichen Auseinandersetzung noch immer nicht alle Fragen von Bundesverfassungsgericht (BVerfG) und EuGH geklärt wurden, wird jeder entsprechende Versuch unweigerlich zu weiterer Rechtsunsicherheit für die Bürger*innen wie auch für die Ermittlungsbehörden führen. Denn

die anlasslose und massenhafte Speicherung der Kommunikationsdaten nahezu der gesamten Bevölkerung steht in einem notwendigen Widerspruch zu rechtsstaatlichen Grundlagen und den Werten einer offenen und freien Gesellschaft.

Insbesondere die im Antrag der CDU/CSU-Fraktion (BT-Drs. 20/3687) geforderten Leitlinien einer möglichen Gesetzgebung entsprechen nicht den Maßgaben des EuGH und würden neue rechtliche Fragen aufwerfen, die absehbar vor dem EuGH scheitern würden. Offenkundig liegt dem Antrag das seit vielen Jahren in der deutschen Innenpolitik etablierte und auch die Geschichte der Vorratsdatenspeicherung prägende Muster zugrunde, durch sehr weitgehende Gesetzgebung die Grenzen des verfassungsrechtlich gerade noch vertretbaren so weit als möglich auszureizen. Freiheitsrechte sind für eine derartige Politik nicht die Grundlage, sondern störende Grenzen, die verschoben werden sollten. Unfreiwillige aber nicht selten bewusst in Kauf genommene langjährige Rechtsunsicherheit sind die Folge.

Die Anforderungen des EuGH

Anders als der Antrag BT-Drs. 20/3687 suggeriert, hat der EuGH keineswegs Speicherung von IP-Adressen pauschal als mit der Grundrechtecharta vereinbar erklärt. Vielmehr stellt er ausdrücklich fest, „dass die allgemeine Speicherung der IP-Adressen der Quelle der Verbindung einen schweren Eingriff in die in den Art. 7 und 8 der Charta verankerten Grundrechte darstellt, da diese IP-Adressen es ermöglichen können, genaue Schlüsse auf das Privatleben des Nutzers des betreffenden elektronischen Kommunikationsmittels zu ziehen, und abschreckende Wirkung in Bezug auf die Ausübung der in Art. 11 der Charta garantierten Freiheit der Meinungsäußerung haben kann.“

Eine Speicherung von IP-Adressen ist daher laut EuGH nur unter äußerst engen Voraussetzungen rechtlich möglich.

Speicherfrist

Ihre Speicherung kann – wie bereits aus dem Leitsatz des Urteils ersichtlich ist – nur für einen auf das für das verfolgte Ziel absolut Notwendige beschränkten Zeitraum rechtmäßig sein. Allerdings benennt der EuGH selbst keinen konkreten Zeitraum. Jedenfalls kann dieser Zeitraum nicht willkürlich gewählt werden, sondern muss durch den Gesetzgeber evidenzbasiert begründet werden. Aus dem Antrag BT-Drs 20/3687 wird in keiner Weise ersichtlich, weshalb der Zeitraum von sechs Monaten gewählt wurde und es sind auch keine Daten bekannt, auf die sich ein solcher Zeitraum stützen könnte. Insbesondere liegen keine unabhängigen Untersuchungen vor, die einen Zusammenhang zwischen Speicherdauer und Ermittlungserfolg zum Thema haben. Und selbst das BKA fordert auf Grundlage seiner eigenen Analysen bezüglich der Meldungen des US-amerikanischen National Centers for Missing and Exploited Children (NCMEC) lediglich eine Speicherung von mehreren Wochen.

Portnummern

Der Europäische Gerichtshof hat ausdrücklich nur die Speicherung von IP-Adressen bewertet. Der Antrag BT-Drs. 20/3687 geht jedoch weit darüber hinaus, indem er zugleich die Speicherung von Portnummern fordert. Hintergrund ist, dass bei dynamischen IP-Adressen angesichts des beschränkten IPv4-Adressraums IP-Adressen mehrfach vergeben werden. Mittels Netzwerkadressübersetzung (Network Address Translation – NAT) ist es möglich, dieselbe IP-Adresse mehreren Nutzer*innen zuzuweisen. Eine Identifizierung ist in diesem Fall nur über die Portnummer (und einen genauen Zeitstempel) möglich.

Zum einen stellen sich rein technische Fragen, etwa ob die Strafverfolgungsbehörden selbst über die entsprechenden für eine Abfrage beim Anbieter nötigen Daten verfügen. Auch sollte nicht verkannt werden, dass selbst geringe Abweichungen im Zeitstempel nicht nur zur Unbrauchbarkeit der Daten führen können, sondern sogar die Gefahr besteht, dass Unschuldige aufgrund vermeintlich eindeutiger technischer Daten Ziel von Strafverfolgung werden.

Vor allem aber wirft die Speicherung von Portnummern bislang in der Rechtsprechung nicht geklärte Fragen auf, insbesondere inwiefern die Speicherung von Daten aus der Transportebene des Internets (nach ISO) einen schwerwiegenderen Eingriff in die Grundrechte darstellt, als eine Speicherung der IP-Adressen. Jedenfalls wäre allein die Menge der gespeicherten Daten erheblich höher und könnte weitgehendere Rückschlüsse zulassen, als die bloße Speicherung der IP-Adresse. Während auch eine dynamische IP-Adresse für einen längeren Zeitraum zugewiesen bleibt (üblicherweise über die Dauer einer Netzwerkverbindung bzw. mehr oder weniger regelmäßige Zuweisungen etwa nach 24 Stunden), kann allein das Aufrufen einer einzigen Website – angesichts der komplexen Struktur moderner Seiten – mehrere Hundert Sessions mit je unterschiedlichen Portnummern generieren. Allein aus der Analyse dieser Daten kann auch ohne Zugriff oder Rückverfolgung der Kommunikationsinhalte selbst ein sehr präzises Bild des Nutzungsverhaltens und weitreichende Rückschlüsse auf die Lebensgewohnheiten der Betroffenen gezogen werden. Gerade angesichts der Möglichkeiten moderner automatisierter Datenauswertung würde bereits die Speicherung dieser gigantischen Datenmengen eine erhebliche Gefahr darstellen. Die Schwere des Eingriffs ist jedenfalls nicht mit der Speicherung von IP-Adressen gleichzusetzen sondern in ihrer Intensität mit der einer Speicherung von Verkehrs- und Standortdaten vergleichbar.

Aus den Schlussanträgen des Generalanwalts zum Verfahren SpaceNet/Telekom geht hervor (Rn. 83), dass spezifische Fragen um statische und dynamische IP-Adressen bereits Teil der mündlichen Verhandlung, jedoch angesichts der Vorlagefragen und der klaren Rechtswidrigkeit der deutschen Vorratsdatenspeicherung nicht entscheidungserheblich waren. Es ist aber mehr als zweifelhaft, ob die Speicherung von Portnummern angesichts der Schwere des Eingriffs vor den Gerichten Bestand haben würde.

Schwere Kriminalität

Eine Speicherung von IP-Adressen kommt im Rahmen der Strafverfolgung nach Maßgabe des EuGH nur zur Verfolgung schwerer Kriminalität in Betracht.

In den letzten Jahren werden die Forderungen nach flächendeckenden Überwachungsmaßnahmen verstärkt mit dem Schutz von Kindern begründet. Sexualisierte Gewalt gegen Kinder ist ein schwerwiegendes soziales Problem und die Verbreitung von Kindesmissbrauchsdarstellungen kann, auch nach Einschätzung des EuGH, schwere Kriminalität darstellen. Fraglich ist allerdings, ob eine anlasslose Speicherung der IP-Adressen überhaupt geeignet wäre, diese Formen der schweren Kriminalität wirksam zu bekämpfen.

Denn die Speicherung der eigenen IP-Adresse lässt sich durch die Täter ohne weiteres umgehen. Bereits das simple Nutzen von Proxy-Servern oder ein Virtual Private Network (VPN) lässt die Speicherung der Nutzerkennung in der Regel ins Leere laufen. Erwachsene Täter, insbesondere solche, die strategisch bzw. mit Unrechtsbewusstsein handeln, würden sich – auch ohne besondere technische Kenntnisse – voraussichtlich schnell darauf einstellen, gerade da damit zu rechnen ist, dass die Nutzung von VPNs sich durch die Einführung einer Vorratsdatenspeicherung schnell verbreiten dürfte.

Bereits jetzt wird ein großer Anteil der Ermittlungsverfahren nach §§ 184b, 184c StGB laut Polizeilicher Kriminalstatistik (PKS)* gegen Kinder und Jugendliche geführt. So haben mehr als die Hälfte der Tatverdächtigen nach § 184b StGB das 21. Lebensjahr noch nicht vollendet, 13 % waren noch nicht einmal strafmündig.

Die gegenwärtige Rechtslage, insbesondere die Ausgestaltung der §§ 184b und 184c StGB differenziert nicht ausreichend zwischen Darstellungen, die aus schwersten Gewaltprozessen entstehen und dem auch unter Kindern und Jugendlichen teilweise verbreiteten Sexting. Hinzu kommt, dass angesichts der Ausgestaltung von §§ 184b Abs. 3 und § 184c Abs. 3 StGB (Besitz ohne Verbreitungsabsicht, regelmäßig gut die Hälfte der Fallzahlen der §§ 184b, 184c StGB in der PKS), sich bereits sämtliche Teilnehmer etwa eines Klassenchats strafbar machen können, wenn sie das automatische Herunterladen von Medieninhalten nicht ausgeschaltet haben und entsprechende Darstellungen innerhalb des Chats versendet werden. Auch wenn derartigen Fallkonstellationen regelmäßig strafbare Hand-

* Zahlen nach PKS 2021, da sich auch der zu behandelnden Antrag BT-Drs. 20/3687 auf diese bezieht.

lungen zugrunde liegen, ist es doch mehr als zweifelhaft, ob sie als schwere Kriminalität im Sinne des EuGH zu werten sind.

„Datenschutz“

Nicht ganz nachvollziehbar ist, dass der Antrag BT-Drs. 20/3687 ein hohes Datenschutzniveau einfordert. Da die geforderten Maßnahmen selbst massiv in die informationelle Selbstbestimmung eingreifen und geeignet sind diese zu verletzen, ist nicht ersichtlich, inwiefern ein hohes Datenschutzniveau erreicht werden kann. Bezüglich der „sicheren und schnellen“ Abrufverfahren, die – so wird suggeriert – im Widerspruch zum Datenschutzniveau stehen, sei darauf verwiesen, dass der EuGH ausdrücklich die „Möglichkeit [einer IP-Adressspeicherung] von der strikten Einhaltung der materiellen und prozeduralen Voraussetzungen abhängig [macht], die die Nutzung dieser Daten regeln müssen“. Inwiefern die strafprozessualen Regelungen zum Abruf und zur Nutzung diesen Anforderungen entsprechen, lag dem EuGH bislang noch nicht zur Entscheidung vor. Jedenfalls dürfte auch hier noch Potential für einige Jahre juristischer Auseinandersetzung liegen.

Im Übrigen sei darauf verwiesen, dass mit der Menge der gespeicherten Daten nicht nur das Missbrauchspotential steigt sondern auch die Begehrlichkeiten böswilliger Akteure geweckt werden können. Sowohl die Speicherung bei den Anbietern als auch Abrufverfahren bieten zahlreiche Angriffsvektoren. Die zuverlässigste Form der Sicherheit vertraulicher personenbezogener Daten ist, sie nicht dauerhaft zu speichern.

Verhältnismäßigkeit

Eine Vorratsdatenspeicherung, insbesondere wie sie der Antrag BT-Drs. 20/3687 vorsieht, wäre unverhältnismäßig. Bereits 2011 hat das Max-Planck-Institut für ausländisches und internationales Strafrecht („Schutzlücken durch Wegfall der Vorratsdatenspeicherung?“, Freiburg 2011) festgestellt, dass keine belastbaren

Hinweise darauf bestehen, dass durch den Wegfall der 2010 für verfassungswidrig befundenen Regelung zur Vorratsdatenspeicherung Schutzlücken entstanden seien. Auch seinerzeit hatten die Strafverfolgungsbehörden darauf bestanden, dass angesichts des größer werdenden Deliktsfelds der Internetkriminalität eine Vorratsdatenspeicherung unabdinglich sei. Eine solche Notwendigkeit ist auch heute nicht ersichtlich.

Laut PKS lag die Aufklärungsquote 2021 in Fällen des § 184b StGB bei 92,3 % und damit sehr hoch. Insbesondere ist aber fraglich, ob die – von den beteiligten Nationalstaaten auch vor dem EuGH vielbeschworenen – Fälle die Regel sind, dass Darstellungen sexualisierter Gewalt gegen Kinder aufgrund einer fehlenden IP-Adressspeicherung nicht verfolgt werden können.

Der EuGH rechtfertigt eine mögliche Ausnahme von seiner Ablehnung der allgemeinen Speicherung von IP-Adressen mit jenen Fällen, in denen „die IP-Adresse der einzige Anhaltspunkt sein kann, der es ermöglicht, die Identität der Person zu ermitteln, der diese Adresse zugewiesen war, als die Tat begangen wurde“ (C-793, Rn. 100). Laut Antwort der Bundesregierung auf die schriftliche Anfrage des Bundestagsabgeordneten de Vries vom Januar 2022 (BT-Drs. 20/534, S. 27f) konnte aber lediglich in ca. 3 % aller im im Jahr vom US-amerikanischen National Centers for Missing and Exploited Children (NCMEC) gemeldeten, strafrechtlich relevanten Fälle ein Täter nicht identifiziert werden, weil als einziger Ermittlungsansatz die IP-Adresse bekannt und diese nicht mehr abfragbar waren. Im Übrigen ist auch nicht klar, inwiefern die IP-Adresse als einziger Ermittlungsansatz ausgereicht hätte, einen Täter zu ermitteln oder was das Ergebnis der Ermittlungen gewesen wäre.

Angesichts der einfachen Umgehungsmöglichkeiten einer IP-Adressenspeicherung mittels VPN durch strategisch handelnde Täter und dem sehr hohen Anteil von Kindern und Jugendlichen als Täter*innen, ist davon auszugehen, dass der Anteil der Verfahren schwerer Kriminalität, die allein deshalb nicht aufzuklären ist, weil eine IP-Adresse nicht mehr abrufbar ist, in einem Bereich liegt, der einen generellen, schwerwiegenden Eingriff in die Grundrechte nahezu der gesamten Bevölkerung nicht rechtfertigen kann.

Alternativen

Gegenüber dem massiven Eingriff in die Grundrechte nahezu der gesamten Bevölkerung durch das massenhafte, anlasslose Speichern von personenbezogenen Daten stehen eine ganze Bandbreite von milderen und deutlich effektiveren Mitteln zur Bekämpfung von sexualisierter Gewalt gegen Kinder zur Verfügung.

Seit Jahren werden Alternativen diskutiert, die jedoch nicht zuletzt durch den Fokus auf die Vorratsdatenspeicherung weiter auf ihre Umsetzung warten. So wäre ein durchdachtes und grundrechtsorientiertes Quick-Freeze-Verfahren geeignet, zielgerichtet Ermittlungen zu führen ohne die gesamte Bevölkerung unter Generalverdacht zu stellen. Das konsequente Löschen bereits bekannten Materials im Internet würde die Verbreitung von Darstellungen eindämmen und insbesondere den Opfern sexualisierter Gewalt helfen. Und nicht zuletzt sind ein angemessener Personal- und Wissensaufbau sowie die Schaffung effizienter Strukturen in den Strafverfolgungsbehörden sicherzustellen, um effektive, zielgerichtete und rechtsstaatliche Ermittlungen sicherzustellen.

Grundlegende Voraussetzung für einen wirksamen Kinderschutz wäre allerdings, dass sexualisierte Gewalt gegen Kinder nicht lediglich als Problem der Strafverfolgung erachtet werden darf. Derartige Gewalt ist ein komplexes soziales Problem, in dem die Verbreitung von Bildmaterial nur die sichtbarste Ausprägung ist. Zu versuchen, diese Verbreitung durch vermeintlich einfache technische Lösungen in den Griff zu bekommen erweist sich gerade dort als kontraproduktiv, wo das als bedrohlich wahrgenommene Internet als Tatort identifiziert wird und aus dem Blick gerät, dass sexualisierte Gewalt in der Regel weiterhin im sozialen Nahbereich ausgeübt wird und auch die Online-Gewalt sich nicht nur im digitalen Raum abspielt, sondern einen ganz physischen Hintergrund hat.

Trotz einer deutlichen Erhellung des Dunkelfelds in den vergangenen Jahren und trotz hoher Aufklärungsquoten und der Verschärfung des Strafrechts wird ersichtlich, dass ein weitgehend auf Strafverfolgung ausgerichteter Umgang mit sexualisierter Gewalt gegen Kinder nicht zielführend ist. Der Fokus auf das Internet als Tatort verschleiert, dass die Aufnahmen zumeist im sozialen Nahfeld entstehen und in diesem auch verbreitet werden. Betroffene werden weiterhin allzu oft allein

gelassen. An verbindlichen Strukturen, etwa durch verpflichtende Schutzkonzepte in Schulen und Jugendvereinen mangelt es eklatant, während Jugendämter und soziale Arbeit chronisch unterfinanziert sind. Und die Aufklärung über einen sicheren und verantwortungsvollen Umgang mit modernen Kommunikationsmitteln ist auch im Jahr 2023 noch allzu oft vom Elternhaus oder vom Zufall einzelner engagierter und sachkundiger Lehrkräfte abhängig.

All diese Maßnahmen wurden in der Vergangenheit massiv vernachlässigt. Auch wenn aufgrund zahlreicher Fälle in den letzten Jahren das Thema breiter öffentlich diskutiert wird, sind doch behäbige Strukturen und die mangelnde Bereitschaft auch finanziell massiv in den Aufklärungs- und Schutzstrukturen zu investieren ein weitaus größeres Hemmnis für einen effektiven Kinderschutz als mangelnde Möglichkeiten der Massenüberwachung.