Universiteit Leiden
The Netherlands

Stellungnahme für den Rechtsausschuss des Deutschen Bundestages zum Antrag *IP-Adressen rechtssicher speichern und Kinder vor sexuellem Missbrauch schützen (BT-Drucksache 20/3687)*

Dr. Sabine K. Witting

Assistant Professor für Recht und Digitale Technologien, Universität Leiden

Adresse:

eLaw - Center for Law and Digital Technologies

Kamerlingh Onnes Building, Steenschuur 25, 2311 ES Leiden

E-Mail:

s.k.witting@law.leidenuniv.nl

Harare, 9. Oktober 2023

1. VORBEMERKUNG

Sexualisierte Gewalt gegen Kinder stellt eine schwere Kinderrechtsverletzung nach Art. 34 der UN-Kinderrechtskonvention (UN-KRK) dar. Sie findet im digitalen und analogen Raum nicht separat statt, sondern muss als miteinander verschränkt bekämpft werden. Sexualisierte Gewalt gegen Kinder kann daher im digitalen Raum nur dann effektiv adressiert werden, wenn sie im Zusammenspiel mit derartigen Kinderrechtsverletzungen im analogen Raum betrachtet wird. Dies wird daran deutlich, dass sich sexualisierte Gewalt gegen Kinder im digitalen Raum anbahnen, aber erst im analogen Raum manifestieren kann, und umgekehrt.

Die in BT-Drs. 20/3687 vorgeschlagene Vorratsdatenspeicherung von IP-Adressen zur Bekämpfung sexualisierter Gewalt gegen Kinder berührt allerdings nicht nur das Recht von Kindern auf Schutz vor sexualisierter Gewalt nach Art. 34 UN-KRK, sondern auch das Recht von Kindern auf Schutz der Privatsphäre und personenbezogener Daten, siehe Art. 16 UN-KRK. In diesem Zusammenhang führt der UN-Kinderrechtsausschuss aus:

> *„Die Privatsphäre ist für die Entscheidungsfreiheit, Würde und Sicherheit von Kindern sowie für die Ausübung ihrer Rechte von entscheidender Bedeutung. […] Jede digitale Überwachung von Kindern und die damit verbundene automatisierte Verarbeitung personenbezogener Daten sollten das Recht des Kindes auf Privatsphäre respektieren und nicht routinemäßig, wahllos […] durchgeführt werden […] und es sollte immer darauf geachtet werden, die am wenigsten in die Privatsphäre eingreifenden Mittel zu berücksichtigen, die zur Erfüllung des gewünschten Zwecks zur Verfügung stehen."*[1]

Staatliche Überwachungsmaßnahmen greifen also nicht nur in die Rechte von Erwachsenen, sondern auch in die Rechte von Kindern ein. Die Rechte von Kindern auf Schutz vor sexualisierter Gewalt, und die Rechte von Kindern und Erwachsenen auf Schutz der Privatsphäre und personenbezogener Daten werden oft gegeneinander ausgespielt und als gegensätzlich dargestellt, was jedoch nicht mit einem ganzheitlichen kinder- und menschenrechtlichen Ansatz im Einklang steht. Stattdessen sind eine Abwägung und Kontextualisierung von Maßnahmen unerlässlich, um das Wohl von Kindern zu wahren.

Vor diesem Hintergrund bewertet die vorliegende Stellungnahme die Vereinbarkeit der BT-Drs. 20/3687 mit der Rechtsprechung des Europäischen Gerichtshof (EuGH) und des Bundesverfassungsgerichts (BVerfG) und die Verhältnismäßigkeit der in BT-Drs. 20/3687 vorgeschlagenen Regelung, gefolgt von einer zusammenfassenden Bewertung.

2. VEREINBARKEIT DER BT-DRS. 20/3687 MIT DER RECHTSPRECHUNG DES EUGH UND DES BVERFG

Die Voraussetzungen zur Speicherung von IP-Adressen, die auf Basis des europäischen Unionsrechts vom EuGH bereits in mehreren Entscheidungen[2] formuliert wurden, lassen

[1] UN-Kinderrechtsausschuss, 25. Allgemeine Bemerkung zu den Rechten der Kinder im digitalen Umfeld vom 02. März 2021, Vereinte Nationen CRC/C/GC/25, Rn. 74-75.

[2] EuGH, Urteil vom 22. September 2022, C-793/19 und C-794/19 – SpaceNet/Telekom; EuGH, Urteil vom 5. April 2022, C-140/20 - Commissioner of the Garda Síochána u.a.; EuGH, Urteil vom 6. Oktober 2020, C-511/18, C-512/18 und C-520/18 - La Quadrature du Net u. a.; EuGH, Urteil vom 21. Dezember 2016, C-203/15 und C-698/15 – Tele2 Sverige und Watson u.a.; EuGH, Urteil vom 08. April 2014, C-293/12 und C-594/12 – Digital Rights Ireland und Seitlinger u.a.

wichtige Fragen offen, deren Interpretation erhebliche Risiken für eine rechtssichere Regelung in den Mitgliedstaaten der EU schaffen.

2.1 SPEICHERUNG VON PORTNUMMERN ZUSÄTZLICH ZUR IP-ADRESSE

BT-Drs. 20/3687 sieht vor, dass zusätzlich zu den IP-Adressen „die Portnummern mitgespeichert werden, um eine rechtssichere Zuordnung der IP-Adresse auch dann zu ermöglichen, wenn Provider eine Adresse mehrfach vergeben haben“[3].

Es ist zwischen statischen und dynamischen IP-Adressen zu unterscheiden. Eine Vielzahl privater Internetuser*innen benutzen vornehmlich dynamische IP-Adressen. Um einzelne User*innen hinter einer dynamischen IP-Adresse zu identifizieren, sind aus technischer Sicht zusätzliche Daten notwendig, zum Beispiel die Portnummer, sowie das genaue Datum und die Uhrzeit der Verbindung (sog. Zeitstempel). Diese Informationen sind oft schwer zu erhalten, wenn die Network Address Translation (NAT)-Technologie verwendet wird. IP-Adressen, insbesondere dynamische IP-Adressen, werden aufgrund der weit verbreiteten Verwendung der NAT-Technologie häufig mehr als einem*einer User*in zugewiesen. Mithilfe von NAT könnten Tausende von User*innen mit einer einzigen öffentlichen IP-Adresse verknüpft sein, was es praktisch unmöglich macht, einen*eine konkrete*n User*in zu identifizieren, der*die für eine strafrechtliche Ermittlung von Interesse ist.[4] Deshalb ist die Speicherung von Portnummern zusätzlich zur IP-Adresse, wie auch in BT-Drs. 20/3687 angeführt[5], entscheidend, um eine rechtssichere Zuordnung der IP-Adresse auch dann zu ermöglichen, wenn der Provider eine Adresse mehrfach vergeben hat.

Der EuGH hingegen unterscheidet in seinen Ausführungen nicht zwischen statischen und dynamischen IP-Adressen und erwähnt auch Zusatzdaten wie die Portnummer nicht. Aus den Schlussanträgen des Generalanwalts Sánchez-Bordona zu *SpaceNet/Telekom* ergibt sich, dass sich der EuGH wohl absichtlich nicht zu dieser Frage geäußert hat, da das vorlegende Gericht, konkret das Bundesverwaltungsgericht, nicht ausdrücklich auf diese Problematik hingewiesen und diesbezüglich Aufklärung verlangt hatte.[6]

Allerdings könnte die in BT-Drs. 20/3687 geforderte zusätzliche Speicherung von Portnummern zu einer erhöhten Eingriffsintensität führen, da mit ihr eine noch genauere Profilbildung möglich ist. Es ist daher fraglich, ob Zusatzinformationen wie Portnummern, die zur eindeutigen Zuordnung einer dynamischen IP-Adresse notwendig sind, unter den EU-Mitgliedstaaten vom EuGH eingeräumten Regelungsspielraum zur Vorratsspeicherung von IP-Adressen fallen. Dies birgt das erhebliche rechtliche Risiko, dass eine entsprechende Regelung in diesem Punkt einer Überprüfung durch den EuGH nicht standhalten würde.

---

[3] Antrag der Fraktion der CDU/CSU, IP-Adressen rechtssicher speichern und Kinder vor sexuellem Missbrauch schützen, BT-Drs. 20/3687, 27. September 2022, S. 1.
[4] Adam Juszczak/Elisa Sason, Recalibrating Data Retention in the EU: The Jurisprudence of the Court of Justice of the EU on Data Retention - Is This the End or Is This Only the Beginning?, eucrim - The European Criminal Law Associations' Forum, 8. September 2021.
[5] Antrag der Fraktion der CDU/CSU, IP-Adressen rechtssicher speichern und Kinder vor sexuellem Missbrauch schützen, BT-Drs. 20/3687, 27. September 2022, S. 2.
[6] Schlussanträge Generalanwalt Sánchez-Bordona vom 18. November 2021, C-793/19 und C-794/19, Rn. 83.

2.2 „AUF DAS ABSOLUT NOTWENDIGE BEGRENZTER ZEITRAUM“

In seiner *SpaceNet/Telekom* Entscheidung betont der EuGH wiederholt, dass eine allgemeine und unterschiedslose Vorratsspeicherung von IP-Adressen zur Bekämpfung von schwerer Kriminalität nur für einen auf das absolut Notwendige begrenzten Zeitraum zulässig ist.[7]

BT-Drs. 20/3687 sieht eine Speicherfrist von sechs Monaten vor, ohne jegliche Begründung oder empirische Grundlage für diesen Zeitraum zu nennen. Nach der Rechtsprechung des EuGH ist freilich eine evidenzbasierte, überprüfbare Begründung unentbehrlich, da der stark limitierte zeitliche Rahmen ein Kernelement der engen Ausnahmemöglichkeiten ist, die der EuGH überhaupt zu akzeptieren bereit ist. Auch das Bundesverfassungsgericht hat in seiner Entscheidung zur Vorratsdatenspeicherung von 2010 festgestellt, dass eine Speicherung von Telekommunikationsdaten für einen Zeitraum von sechs Monaten “sehr lang und […] an der Obergrenze dessen [liegt], was unter Verhältnismäßigkeitserwägungen rechtfertigungsfähig ist“.[8] Angesichts des derzeit verfügbaren Wissensstandes gibt es erhebliche Zweifel an der Angemessenheit einer Speicherungsfrist von sechs Monaten. Das Bundeskriminalamt (BKA) selbst hat im Ausschuss für Familie, Senioren, Frauen und Jugend als geeignete Speicherungsfrist für NCMEC Cybertipps[9] einen Zeitraum von lediglich zwei Wochen angegeben.[10] In diesem Zusammenhang ist anzumerken, dass solche Angaben des BKA als Exekutivbehörde allein nicht genügen können, weil eine Begründung zur Festsetzung des Zeitraums aus Transparenzgründen und aufgrund der Schwere des Eingriffs in das Recht auf Schutz der Privatsphäre und personenbezogener Daten auf einer unabhängig überprüfbaren Evidenzgrundlage beruhen sollte.

Demzufolge muss ein Antrag wie jener in BT-Drs. 20/3687 eine umfängliche Begründung für den gewählten Speicherungszeitraum enthalten. Ob diese Begründung dann der rechtlichen Überprüfung durch den EuGH standhalten wird, ist aktuell aufgrund fehlender expliziter Interpretation des Begriffs “auf das absolut Notwendige begrenzter Zeitraum“ in der Rechtsprechung des EuGH mit erheblichen rechtlichen Risiken behaftet.

3. VERHÄLTNISMÄßIGKEIT DER VORGESCHLAGENEN REGELUNG

Die in BT-Drs. 20/3687 vorgeschlagene Regelung muss dem Grundsatz der Verhältnismäßigkeit entsprechen, also einen legitimen Zweck verfolgen, geeignet, erforderlich und angemessen sein.

In diesem Zusammenhang ist zunächst erneut auf die **Eingriffsintensität** der vorgeschlagenen Regelung hinzuweisen. Der EuGH hat festgehalten, dass eine Vorratsspeicherung von IP-Adressen einen schweren Eingriff in die Grundrechte von Internetuser*innen aus Art. 7 (Achtung des Privat- und Familienlebens) und Art. 8 (Schutz personenbezogener Daten) der EU-Grundrechtecharta darstellt. Für die Bewertung der Eingriffsintensität auf nationaler Ebene kommt es zudem auf eine Gesamtschau der existierenden Überwachungsmaßnahmen an, die je

[7] EuGH, Urteil vom 22. September 2022, C-793/19 und C-794/19 – SpaceNet/Telekom, Rn. 131.
[8] BVerfG, 02.März 2010 - 1 BvR 256/08, 1 BvR 263/08, 1 BvR 586/08, Rn. 215.
[9] Aufgrund eines Bundesgesetzes sind US-amerikanische Provider verpflichtet, Hinweise auf Darstellungen sexualisierter Gewalt gegen Kinder an die Nichtregierungsorganisation „National Center for Missing and Exploited Children“ (NCMEC) weiterzuleiten. Alle beim NCMEC eingehenden Hinweise werden dort gesichtet und münden in standardisierten Berichten (sogenannte „CyberTipps"), die an das BKA als deutsche Zentralstelle für weitere Ermittlungen weitergegeben werden.
[10] Ausschuss für Familie, Senioren, Frauen und Jugend, Wortprotokoll der 41. Sitzung am 21. Juni 2023, Protokoll-Nr. 20/41, S. 10-11.

nach EU-Mitgliedsstaat verschieden ausfallen kann. Eine Überwachungsgesamtrechnung ist daher dringend notwendig, um festzustellen, welchem Maß an Überwachung die Bürger*innen insgesamt bereits ausgesetzt sind, und um bewerten zu können, wie sich die Einführung einer generellen und anlasslosen Speicherung von IP-Adressen in Zusammenschau mit bereits bestehenden Maßnahmen auf die Eingriffsintensität auswirkt.

Während die vorgeschlagene Regelung einen **legitimen Zweck** verfolgt, namentlich den Schutz von Kindern vor sexualisierter Gewalt, ist bereits fraglich, ob sie **geeignet** ist, den verfolgten Zweck zu erreichen. In diesem Zusammenhang ist darauf hinzuweisen, dass die IP-Adresse allein nicht einen*r bestimmte*n Internetuser*in identifizieren kann, sondern allenfalls den*die Anschlussinhaber*in. Ein typisches Beispiel für die Wichtigkeit von Zusatzdaten wie der Portnummer ist hierbei der Zugang zum Internet über das WLAN-Netzwerk eines Hotels. Mit der IP-Adresse kann zwar der Anschlussinhaber, also das Hotel, ermittelt werden, doch nur mit der Portnummer auch der*die User*in einer bestimmten Website. Die Annahme in BT-Drs. 20/3687 ist fragwürdig, relevante Straftaten könnten nicht aufgeklärt werden, weil die notwendigen IP-Adressen nicht mehr zur Verfügung stünden. Denn selbst beim Vorhandensein der IP-Adresse kommt es aufgrund der limitierten Aussagekraft der IP-Adressen nicht automatisch zu einem Ermittlungserfolg.

Die **Geeignetheit** der Vorratsdatenspeicherung wurde bereits im Jahr 2011 in einer Studie des Max-Planck-Instituts bezweifelt. Die Studie stellte fest, es gebe keine belastbaren Hinweise, dass Schutzmöglichkeiten durch den Wegfall der Vorratsdatenspeicherung reduziert worden wären, was insbesondere auch für den Bereich der sog. 'Kinderpornografie' gelte.[11] Zwar haben das BKA und einige Strafverfolgungsbehörden immer wieder betont, dass eine Speicherung von IP-Adressen unentbehrlich sei, um sexualisierte Gewalt gegen Kinder aufklären zu können,[12] allerdings lediglich für Fälle von NCMEC Cybertipps. Eine Einschätzung zur Effektivität einer IP-Vorratsdatenspeicherung fehlt bislang gänzlich für Fälle des Verbreitens von Darstellungen sexualisierter Gewalt gegen Kinder, die nicht auf NCMEC Cybertipps beruhen.

Diese Einschätzung der Strafverfolgungsbehörden ist aufgrund der praktischen Erfahrungswerte in die **Prüfung der Geeignetheit** der vorgeschlagenen Regelung miteinzubeziehen. Gemessen an der hohen Eingriffsintensität der vorgeschlagenen Regelung kann jedoch eine solche lediglich erfahrungsgesättigte Praxiseinschätzung eine unabhängige, empirische Studie zur Wirksamkeit der Vorratsspeicherung von IP-Adressen nicht ersetzen, zumal sich auch aus dem Bereich der Strafverfolgungsbehörden Stimmen mehren, die eine solche Maßnahme für nicht effektiv halten.[13] Auch hat Generalanwalt Villalón in seinen Schlussanträgen zu *Digital Rights Ireland* die Beweislast klar dem Gesetzgeber zugeordnet, bei der Vorratsdatenspeicherung eine regelmäßige Neubewertung der Umstände vorzunehmen, welche die durch die vorgeschlagene Regelung entstandene Einschränkung der Ausübung des Rechts auf Achtung des Privatlebens rechtfertigen könnte.[14] Die Beweislast für die Effektivität der vorgeschlagenen IP-Vorratsdatenspeicherung ist

---

[11] Max-Planck-Institut für ausländisches und internationales Strafrecht, Schutzlücken durch Wegfall der Vorratsdatenspeicherung? Eine Untersuchung zu Problemen der Gefahrenabwehr und Strafverfolgung bei Fehlen gespeicherter Telekommunikationsverkehrsdaten, Freiburg 2011, S. 220-221.

[12] BKA, Erforderliche Speicherfristen für IP-Adressen, Stand: 05. Juli 2023.

[13] Generalstaatsanwaltschaft Köln, Zentral- und Ansprechstelle Cybercrime Nordrhein-Westfalen, Stellungnahme zu der öffentlichen Anhörung des Ausschusses für Digitales des Deutschen Bundestags zur „Chatkontrolle" am 1. März 2023, Ausschussdrucksache 20(23)131 vom 22. Februar 2023, S. 17-18.

[14] Schlussanträge Generalanwalt Villalón vom 12. Dezember 2013, C-293/12, Rn. 139.

damit in der Gesetzesbegründung zu erbringen, sowohl hinsichtlich der Notwendigkeit des Erlasses der Maßnahme selbst als auch hinsichtlich der Notwendigkeit, eine Maßnahme aufrechtzuerhalten. Eine solche Begründung fehlt in BT-Drs. 20/3687 vollständig.

Obwohl bereits die Geeignetheit der vorgeschlagenen Regelung bezweifelt werden kann, bestehen auch erhebliche Bedenken im Bereich der **Erforderlichkeit**. Denn es gibt jedenfalls eine Vielzahl milderer, gleich wirksamer Mittel.

Strafverfolgungsbehörden beklagen – zu Recht – ein strukturelles Verfolgungsdefizit durch unzureichende technische und personelle Ausstattung. Ermittlungen in Fällen sexualisierter Gewalt gegen Kinder, vor allem bei Vorliegen digitaler Beweismittel, sind langwierig und komplex. Diese Komplexität der Ermittlungen, in Kombination mit der allgemeinen Ressourcenknappheit, hat schwerwiegende Auswirkungen auf die Ermittlungsfähigkeit der Strafverfolgungsbehörden. Dies führt laut einer aktuellen Studie etwa zu der Zwangslage, dass sich Strafverfolgungsbehörden aufgrund fehlender Ressourcen zwischen Betroffenenidentifizierung, Tataufklärung oder Löschung von Darstellungen sexualisierter Gewalt gegen Kinder entscheiden müssen.[15] Ein verbesserter Wissens- und Personalaufbau ist damit ein unabdingbarer Schritt, um sexualisierte Gewalt gegen Kinder im digitalen und analogen Raum tatsächlich wirksam zu bekämpfen. Ein Positivbeispiel hierfür ist die personelle Verstärkung und das Errichten einer auf sexualisierte Gewalt gegen Kinder spezialisierten Abteilung bei der Zentral- und Ansprechstelle Cybercrime Nordrhein-Westfalen (ZAC NRW). Durch diese institutionelle Stärkung konnte die ZAC NRW die Zahl der Verfahren im Bereich der Straftaten gegen die sexuelle Selbstbestimmung gegen bekannte Straftäter im Jahresvergleich 2021 zu 2022 bereits mehr als verdoppeln und die gegen unbekannte Täter gar versechsfachen.[16] Eine solche umfassende Investition in die den Strafverfolgungsbehörden zur Verfügung stehenden Ressourcen würde damit nicht nur der Ermittlung von NCMEC Cybertipps zugutekommen, sondern dem gesamten rechtlichen Kampf gegen sexualisierte Gewalt gegen Kinder. Dies ist vor allem deshalb wichtig, weil sich ein Großteil der Taten von sexualisierter Gewalt gegen Kinder im Nahbereich abspielt.

Eine andere, grundrechtsschonendere Maßnahme ist das konsequente Löschen von Darstellungen sexualisierter Gewalt gegen Kinder. Aus Sicht von Überlebenden ist das Löschen essenziell, da jedes weitere Teilen solcher Darstellungen zu einer Retraumatisierung führen kann. Konsequentes Löschen würde zudem der weiteren Verbreitung von Darstellungen sexualisierter Gewalt gegen Kinder entschieden vorbeugen und ist mit verhältnismäßig geringem Aufwand möglich. In einem Versuch sammelten Journalisten binnen weniger Stunden rund 80.000 Links zu im Clearweb gespeicherten Darstellungen sexualisierter Gewalt gegen Kinder, um sie anschließend bei den entsprechenden Speicherdiensten zu melden. Nach Meldung bei in- und ausländischen Speicherdiensten waren diese Darstellungen spätestens nach zwei Tagen gelöscht, nachdem sie zuvor bis zu sechs Jahre lang online gewesen waren.[17] In einem Gespräch mit den Journalisten begründet das BKA die mangelnde Priorisierung des Löschens von Inhalten vor allem mit fehlenden Ressourcen. Primäres Ziel der Strafverfolgungsbehörden sei die Ermittlung der Täter*innen. Auf eine kleine Anfrage der Fraktion DIE LINKE, ob der Bund verpflichtet sei,

---

[15] World Vision Deutschland e.V., Sexualisierte Gewalt gegen Kinder im digitalen Raum, 2023, S. 36.
[16] Generalstaatsanwaltschaft Köln, Zentral- und Ansprechstelle Cybercrime Nordrhein-Westfalen, Stellungnahme zu der öffentlichen Anhörung des Ausschusses für Digitales des Deutschen Bundestags zur „Chatkontrolle“ am 1. März 2023, Ausschussdrucksache 20(23)131 vom 22. Februar 2023, S. 10-11.
[17] Tagesschau, Kindesmissbrauch: Warum löscht die Polizei die Bilder nicht?, 2. Dezember 2021.

dafür zu sorgen, dass Darstellungen sexualisierter Gewalt gegen Kinder gelöscht werden, antwortete die Bundesregierung, dass es dem BKA an einer Rechtsgrundlage zur Anordnung der Löschung von rechtswidrigen Inhalten fehle.[18] Es ist daher zu empfehlen, neben einer erheblichen Investition in die personellen und technischen Ressourcen der Strafverfolgungsbehörden vorrangig die Schaffung einer Rechtsgrundlage zum proaktiven Löschen illegaler Darstellungen von sexualisierter Gewalt gegen Kinder in Erwägung zu ziehen.

Als weitere Maßnahme ist die vom Bundesministerium der Justiz in einem Referentenentwurf vorgeschlagene Sicherungsanordnung für Verkehrsdaten zu erwähnen (sog. Quick-Freeze-Verfahren). Im Gegensatz zu der in BT-Drs. 20/3687 vorgeschlagenen anlasslosen und allgemeinen Vorratsspeicherung der IP-Adressen umfasst das Quick-Freeze-Verfahren die anlassbezogene Sicherung von Verkehrsdaten für einen festgelegten Zeitraum aufgrund richterlicher Anordnung. Relevante Verkehrsdaten können laut Referentenentwurf auf richterliche Anordnung „eingefroren" werden, wenn dies zur Verfolgung erheblicher Straftaten erforderlich ist. Diese stehen dann den Strafverfolgungsbehörden für einen begrenzten Zeitraum zur Verfügung und können zur Auswertung mit richterlicher Anordnung "aufgetaut" werden. „Eingefroren" werden könnten Verkehrsdaten bereits in einem frühen Stadium der Ermittlungen. Die Sicherungsanordnung kann sich sowohl auf die Verkehrsdaten von Beschuldigten erstrecken als auch auf Personen, bei denen auf Grund bestimmter Tatsachen anzunehmen ist, dass sie für den*die Beschuldigte*n bestimmte oder von ihm*ihr herrührende Mitteilungen entgegennehmen oder weitergeben. Eine spätere Erhebung und Auswertung gesicherter Daten ist nur bei Personen zulässig, gegen die ein konkreter Tatverdacht vorliegt oder die als Nachrichtenmittler anzusehen sind. Der EuGH hat ein solches Verfahren in mehreren Urteilen für zulässig erachtet, solange durch klare und präzise Regeln sichergestellt wird, dass die materiellen und prozessualen Voraussetzungen eingehalten werden und Betroffene über wirksame Garantien zum Schutz vor Missbrauchsrisiken verfügen.[19] Es handelt sich – unabhängig von einer detaillierten rechtlichen Bewertung – ersichtlich um ein deutlich datensparsameres Datensicherungsverfahren, das zudem einem Richtervorbehalt unterliegt.

Maßnahmen wie Investitionen in personelle und technische Ressourcen, die Priorisierung und das Schaffen einer rechtlichen Grundlage für das Löschen von Darstellungen sexualisierter Gewalt gegen Kinder, sowie das Quick-Freeze-Verfahren stellen damit grundrechtsschonendere und zugleich wirksamere Maßnahmen zur Bekämpfung von sexualisierter Gewalt gegen Kinder dar. Die generelle und anlasslose Speicherung von IP-Adressen zur Verfolgung von Straftaten der sexualisierten Gewalt gegen Kinder ist weder geeignet noch erforderlich und daher grundrechtlich unverhältnismäßig.

4. ZUSAMMENFASSENDE BEWERTUNG

Nach bald zwei Jahrzehnten Streit um die Vorratsdatenspeicherung ist es dringend geboten, endlich Rechtssicherheit für die Strafverfolgungsbehörden zu schaffen. Die in BT-Drs. 20/3687 vorgeschlagene anlasslose und allgemeine Vorratsspeicherung von IP-Adressen ist hierbei

[18] Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Anke Domscheit-Berg u.a. und der Fraktion DIE LINKE. – BT-Drs. 20/729 – Löschen statt sperren – Entfernung digitaler Darstellungen sexualisierter Gewalt an Kindern, BT-Drs. 20/1128, 17. März 2022, S. 9.
[19] EuGH, Urteil vom 22. September 2022, C-793/19 und C-794/19 – SpaceNet/Telekom, Rn. 75; EuGH, Urteil vom 6. Oktober 2020, C-511/18, C-512/18 und C-520/18 - La Quadrature du Net u. a., Rn. 168.

allerdings kein zukunftsfähiger Weg, da die vorgeschlagene Regelung mit einem erheblichen Rechtssicherheitsrisiko verbunden und unverhältnismäßig ist. Es stehen zahlreiche evidenzbasierte, grundrechtsschonendere Maßnahmen zur Verfügung, die aus grundrechtlicher Sicht priorisiert werden müssen, um Kinder effektiv vor sexualisierter Gewalt zu schützen.

Hingewiesen sei auf die anhaltenden Diskussionen zum Verordnungsentwurf der EU-Kommission zur Prävention und Bekämpfung des sexuellen Missbrauchs von Kindern (sog. „Chatkontrolle"). [20] Auch in diesem Verordnungsentwurf wird suggeriert, dass technisch unterstütze Maßnahmen wie Aufdeckungsanordnungen, die schwerwiegend in das Recht auf Privatsphäre von Kindern und Erwachsenen eingreifen, nötig seien, um Kinder im digitalen Bereich zu schützen. Bei diesem Verordnungsentwurfs stehen allerdings auch grundrechtsschonendere Maßnahmen zur Verfügung, die die digitalen Diensteanbieter stärker in die Prävention und Bekämpfung von sexualisierter Gewalt gegen Kinder einbinden könnten. Denkbar wären hier Rahmenvorschriften zur kinderfreundlichen Gestaltung von Community Guidelines oder kinderfreundliche Meldemechanismen. Zudem könnten die Sorgfaltspflichten für digitale Diensteanbieter derart erweitert werden, dass sie zu den speziellen Risiken für die Rechte von Kindern, insbesondere dem Recht auf Schutz vor sexualisierter Gewalt, Stellung beziehen und entsprechende grundrechtsschonende Risikominimierungsmaßnahmen ergreifen müssen. Derartige Maßnahmen würden auch der Charakterisierung des Verordnungsentwurfs als *lex specialis* zur Digitalen-Dienste-Verordnung gerecht.

Das Thema sexualisierte Gewalt gegen Kinder emotionalisiert, und das zu Recht – denn was Kindern von Eltern, Vertrauenspersonen, Lehrer*innen, Trainer*innen oder Dritten durch sexualisierte Gewalt angetan wird, kann sie ein Leben lang verfolgen. Daher ist die Priorisierung des Themas im politischen Diskurs begrüßenswert, denn es gilt, dem Kampf gegen diese Form von Gewalt endlich die notwendigen personellen, technischen und politischen Ressourcen zu widmen. Es ist es allerdings umso wichtiger, sich nicht in Diskussionen um punktuelle, technische (Schein-)Lösungen zu verlieren. Denn diese lenken oftmals von den grundlegenden, systematischen Interventionen ab, die notwendig sind, um das gesamtgesellschaftliche, strukturelle Problem von sexualisierter Gewalt gegen Kinder tatsächlich wirksam anzugehen und nicht nur symbolische Gesetzgebungsvorhaben zu verfolgen, die absehbar keine positiven Effekte haben werden.

---

gez. Dr. Sabine K. Witting

---

[20] Verordnungsentwurf der EU-Kommission zur Prävention und Bekämpfung des sexuellen Missbrauchs von Kindern, COM(2022) 209 final, 11. Mai 2022.