

Stellungnahme zum Entwurf eines Gesetzes zur Einführung einer Speicherpflicht für IP-Adressen und zur Anpassung weiterer digitaler Ermittlungsbefugnisse

1. Ausgangssituation

Das Bundesministerium der Justiz und für Verbraucherschutz beabsichtigt mit dem Gesetzentwurf die Effizienz der Strafverfolgung und der Gefahrenabwehr im digitalen Raum zu erhöhen. Ziel ist es, die Datenlage zu verbessern und sicherzustellen, dass digitale Beweismittel wie Internetprotokoll-Adressen (IP-Adressen) effizient und gleichzeitig in angemessenem Rahmen für die Strafverfolgung und Gefahrenabwehr nutzbar sind.

Dazu sieht der Gesetzentwurf eine Pflicht für Internetzugangsanbieter vor, IP-Adressen für einen Zeitraum von drei Monaten zu speichern, um eine verlässliche Identifikation von Anschlussinhabern zu ermöglichen. Damit sollen Strafverfolgungs-, Polizei- und andere Sicherheitsbehörden ein Instrument nutzen können, das es ihnen erlaubt, dem häufig einzigen, aber nahezu immer effizienten Ermittlungsansatz zu folgen, um digitale Spuren nachzuvollziehen, die bei Straftaten im Internet hinterlassen werden, beispielsweise bei der Verbreitung von Kinderpornografie, bei kriminellen Handelsplattformen, die Betäubungsmittel oder Cybercrime-as-a-Service anbieten, sowie bei echt wirkenden Onlineshops, die Waren verkaufen, die nicht existieren.

Ferner wird für Verkehrsdaten im Bereich der Strafverfolgung das Instrument der Sicherungsanordnung geschaffen. Damit können Strafverfolgungsbehörden die Sicherung von Verkehrsdaten veranlassen, sofern und solange die rechtlichen oder tatsächlichen Voraussetzungen einer Datenerhebung zu Zwecken der Strafverfolgung nicht vorliegen.

Schließlich soll es der Strafverfolgungspraxis wieder ermöglicht werden, bei Straftaten von erheblicher Bedeutung, insbesondere solchen nach § 100a Absatz 2 der Strafprozessordnung, eine Funkzellenabfrage durchzuführen.

Das Bundesministerium der Justiz und für Verbraucherschutz hat am 22. Dezember 2025 die Verbändebeteiligung zu dem Referentenentwurf eröffnet, die Aufforderung an betroffene Fachkreise sowie Organisationen versandt und um Rückmeldung bis zum 30. Januar 2026 gebeten. Diese Möglichkeit nutzt die Stiftung Digitale Chancen und gibt nachstehend Hinweise sowie Anregungen zu dem Entwurf. Dabei fokussieren wir insbesondere auf die Wahrung der Rechte von Kindern gemäß der UN-Kinderrechtskonvention, insbesondere ihren Schutz vor sexuellem Gewalt, gestützt auf unsere Expertise aus dem Projekt „Kinderschutz und Kinderrechte in der digitalen Welt“¹, und tragen zugleich dem Auftrag der Stiftung Digitale Chancen zur Förderung der Internetnutzung und Medienkompetenz und Berücksichtigung der Wahrung von Privatsphäre und Persönlichkeitsrechten sowie dem Schutz der persönlichen Integrität² aller Nutzenden digitaler Dienste Rechnung.

2. Kinderrechte im digitalen Umfeld

Mit der Allgemeinen Bemerkung Nr.25³ erläutert der Ausschuss für die Rechte des Kindes⁴ der Vereinten Nationen, wie deren Rechte auf Schutz, Förderung und Teilhabe im digitalen Umfeld gleichermaßen verwirklicht werden können. Dabei weisen die Ausschussmitglieder darauf hin, dass das digitale Umfeld eine enorme Bedeutung für junge Menschen und ihre Entwicklung hat u.a. auch

¹ Kinderschutz und Kinderrechte in der digitalen Welt. <https://www.kinderrechte.digital/projekt/> Abruf am 27.01.2026

² Krause, Torsten et al.: Zum Begriff der persönlichen Integrität im Jugendschutz. In: Recht der Jugend und des Bildungswesens (RdJB). Jahrgang 70 (2022). Heft 4. Seite 629-635

³ UN (2021): General Comment No. 25 (2021) on children's rights in relation to the digital environment.

https://www.childrens-rights.digital/fileadmin/kinderrechte.digital/Hintergrundmaterial/Englische_Downloads_pdf/General_comment_No.25.pdf
Abruf am 28.01.2026

⁴ Gemäß Artikel 1 UN-KRK gilt jeder Mensch, der das 18. Lebensjahr noch nicht vollendet hat als Kind.

zur Ausbildung der eigenen sexuellen Identität. Gerade vor diesem Hintergrund betonen sie die Notwendigkeit, Kinder und Jugendliche vor Risiken unter anderem in Zusammenhang mit Kontakten und Verhaltensweisen, wie sexualisierter Inhalte, aber auch sexueller Ausbeutung und sexueller Gewalt zu schützen, und verpflichten die Vertragsstaaten⁵, geeignete Maßnahmen zu ergreifen, um dies zu gewährleisten.

3. Schutz der persönlichen Integrität

Der Bundesgesetzgeber hat mit Reform des Jugendschutzgesetzes 2021 das Schutzziel der persönlichen Integrität neu eingeführt. Dieser im Jugendschutzrecht neu etablierte Begriff⁶ ist geeignet, nicht nur in Bezug auf Kinder und Jugendliche, sondern vielmehr auf alle Nutzenden digitaler Dienste Anwendung zu finden. Darunter ist – so Krause et.al. – sowohl der Schutz der physischen und psychischen Integrität als auch in Bezug auf das digitale Umfeld der Schutz der Privatsphäre, das heißt der Integrität von Daten Betroffener im Einklang mit der DSGVO zu verstehen. Die hier in Frage stehende gesetzliche Regelung ist in diesem Kontext zu bewerten.

4. Einführung einer Speicherpflicht für IP-Adressen und Anpassung weiterer digitaler Ermittlungsbefugnisse

Mit der Einführung einer Speicherpflicht für IP-Adressen und der Anpassung weiterer digitaler Ermittlungsbefugnisse will das Bundesministerium der Justiz und für Verbraucherschutz die Effizienz der Strafverfolgung und der Gefahrenabwehr im digitalen Raum zu erhöhen.

4.1. Allgemeine Bewertung

Die Stiftung Digitale Chancen unterstützt das Anliegen des Bundesministeriums der Justiz und für Verbraucherschutz, die Effizienz der Strafverfolgung und der Gefahrenabwehr im digitalen Raum zu erhöhen. Es ist nachvollziehbar und geboten, für Strafverfolgungs-, Polizei- und andere Sicherheitsbehörden eine gesetzliche Grundlage zu schaffen, die es erlaubt, zur Bekämpfung schwerer Straftaten, eine verlässliche Identifikation von Anschlussinhabern digitaler Dienste zu durchzuführen.

4.2. Begründeter Verdacht der Begehung einer besonders schweren Straftat

Der Gesetzentwurf sieht als Grundlage der Erhebung von Verkehrsdaten nach § 100g in Absatz 1 den Verdacht der Begehung oder im Falle dessen Strafbarkeit auch des Versuchs der Begehung oder der Vorbereitung einer Straftat von auch im Einzelfall erheblicher Bedeutung, insbesondere einer in § 100a Absatz 2 bezeichneten Straftat vor. Die geregelte Erforderlichkeit der Erhebung von Verkehrsdaten für die Erforschung des Sachverhalts oder zur Ermittlung des Aufenthaltsorts des Beschuldigten ist nach Einschätzung der Stiftung Digitale Chancen zielführend zur Bekämpfung von Straftaten gegen die sexuelle Selbstbestimmung insbesondere in Bezug auf Kinder und Jugendliche gemäß StPO § 100a (2) 1. lit. f sowie in Bezug auf die Verbreitung von sogenanntem kinder- und jugendpornographischem Material gem. StPO § 100a (2) 1. lit. g. Das geforderte angemessene Verhältnis der Erhebung der Verkehrsdaten zur Bedeutung der Sache ist aus unserer Sicht geeignet, eine über das Maß hinausgehende Datenerhebung zu verhindern.

Die Geltung von Satz 1, d. h. die Zulässigkeit der Erhebung von Verkehrsdaten auch bei Personen, „bei denen auf Grund bestimmter Tatsachen anzunehmen ist, dass sie für den Beschuldigten bestimmte oder von ihm herrührende Mitteilungen entgegennehmen“, sehen wir kritisch insofern als die Entgegennahme von Mitteilungen eines Beschuldigten durch eine andere Person unwillentlich – im Sinne einer aufgedrängten Information – erfolgen kann, z.B. im Falle der Übermittlung von

⁵ Staaten, die sich gegenüber den Vereinten Nationen zur Umsetzung eines Vertrages verpflichten, gelten als Vertragsstaaten. Für die Kinderrechtskonvention trifft dies auf alle Staaten mit Ausnahme der Vereinigten Staaten von Amerika zu.

⁶ Krause, Torsten et al.: Zum Begriff der persönlichen Integrität im Jugendschutz. In: Recht der Jugend und des Bildungswesens (RdJB). Jahrgang 70 (2022). Heft 4. Seite 629-635

inkriminiertem Bildmaterial an eine dem Beschuldigten bekannte E-Mail-Adresse in der Absicht, die diese Adresse innehabende Person zu kompromittieren. Daher wäre u. E. bei inkriminiertem Material zwischen der potenziell unwillentlichen Entgegennahme einerseits und der willentlichen Entgegennahme andererseits zu differenzieren, wobei die Weiterleitung grundsätzlich in beiden Fällen als strafrechtlich relevant zu erachten ist.

Gemäß § 100g Absatz 2 soll die Erhebung von Verkehrsdaten nach Absatz 1 Satz 1 Nummer 1 auch dann zulässig sein, wenn kein Verdacht hinsichtlich einer Straftat von auch im Einzelfall erheblicher Bedeutung besteht, aber die Erforschung des Sachverhalts auf andere Weise aussichtslos oder wesentlich erschwert wäre. Diese Regelung ist aus Sicht der Stiftung Digitale Chancen sinnvoll und erforderlich, insbesondere zur Aufdeckung von Fällen sexueller Handlungen an oder gegenüber sehr jungen Kindern. Kleinkinder, die entweder noch nicht sprechfähig sind oder in einem familialen Abhängigkeitsverhältnis zur Tatperson stehen, sind aufgrund dessen meist nicht in der Lage zu Äußerungen über mögliche strafrechtlich relevante sexuelle Handlungen; ebenso sind Personen im sozialen Umfeld der Gewaltausübung nur selten in der Lage, Verdachtsmomente gegenüber den Strafverfolgungsbehörden zu äußern. Die Identifikation, der die strafrechtlich relevanten sexuellen Handlungen ausübenden Person(en) durch die Erhebung von Verkehrsdaten, d. h. hier der genutzten IP-Adressen, ist daher in diesem Fall notwendig, um den Sachverhalt zu erforschen und das betroffene Kind ggf. der Tatsituation zu entziehen, um es vor weiteren sexuellen Handlungen zu schützen.

Die angestrebten Handlungsbefugnisse erachten wir im Kontext schwerer Straftaten, wie sie im geltenden Recht definiert sind, als angemessen und nachvollziehbar. Eine Ausdehnung der Befugnisse auf de facto jeglichen Verdachtsfall einer Straftat mittels Telekommunikation sehen wir hingegen kritisch und hinsichtlich der Eingriffstiefe in die Privatsphäre als nicht verhältnismäßig sowie nicht in Einklang mit dem Urteil des EuGH vom 06.10.2020⁷.

Die nach § 100g Abs. 7 StPO, vorgesehene Sicherungsanordnung für Verkehrsdaten, wenn ein Anfangsverdacht für die Begehung von regelmäßig besonders schweren Straftaten besteht, ist insbesondere im Kontext von Straftaten gegenüber Minderjährigen sinnvoll und erforderlich. Vorausgesetzt, dass der Abruf dieser Daten nach § 175 TKG durch die Strafverfolgungsbehörden nur und erst dann erfolgt, wenn der Tatverdacht sich bestätigt oder zumindest erhärtet hat, ist damit eine aus unserer Sicht angemessene Wahrung des Schutzes der Daten von potenziell tatverdächtigen Personen gegeben.

Entsprechend erachten wir die in § 100j Absatz 3 vorgesehenen Einschränkungen der Bestandsdatenauskunft auf Fälle, in denen „die gesetzlichen Voraussetzungen für die Nutzung der Daten vorliegen“ oder die gesetzlichen Voraussetzungen für die Nutzung von als Bestandsdaten erhobenen Passwörtern oder anderen Daten, mittels derer der Zugriff auf Endgeräte oder auf Speichereinrichtungen geschützt wird, vorliegen, zur Verfolgung von besonders schweren Straftaten für sinnvoll und geeignet.

Auch die in § 101a Absatz 1 Nr. 1 lit. a und b vorgesehenen Maßgaben der eindeutigen Angabe der zu übermittelnden Daten und des Zeitraums, für den sie übermittelt werden sollen, sowie die bei Funkzellenabfrage räumlich und zeitlich eng begrenzte und hinreichend bestimmte Bezeichnung der Telekommunikation sind u. E. geeignet, einer übermäßigen Datenerhebung entgegenzuwirken.

Die in § 160a unverändert beibehaltenen Maßnahmen, die das Zeugnisverweigerungsrecht von berechtigten Berufsgeheimnisträgern respektieren, sind aus Sicht der Stiftung Digitale Chancen geeignet, die Vertraulichkeit der Kommunikation zwischen Berufsgeheimnisträgern und deren Klienten oder möglichen Informanten zu wahren.

⁷ EuGH, 06.10.2020 - C-511/18, C-512/18, C-520/18

4.3. Speicherpflicht und Verwendungsbefugnis von Verkehrsdaten zur Identifizierung von Anschlussinhabern

Aus Sicht der Stiftung Digitale Chancen ist die nach §176 Absatz 1 vorgesehene Verpflichtung zur Speicherung von IP-Adressen für einen Zeitraum von drei Monaten kritisch zu hinterfragen. Nach unserer Kenntnis erachten Mitarbeitende verschiedener LKÄ ebenso wie des BKA eine Speicherfrist von zwei Wochen bereits als ausreichend, um in Verdachtsfällen einen hohen Prozentsatz von Ermittlungserfolgen zu erzielen. Insbesondere bei der Priorisierung von Verdachtsfällen könnte sich eine längere Speicherfrist sogar kontraproduktiv auswirken und im Falle von strafrechtlich relevanten sexuellen Handlungen an und vor Minderjährigen notwendige und schnell umzusetzende Ermittlungsmaßnahmen ggf. verzögern. Wir regen daher an, die in §176 Absatz 1 vorgesehene Speicherfrist auf **maximal vier Wochen** zu reduzieren. Diese Fristsetzung stünde auch im Verhältnis mit einer technischen Auswertung des BKA, wonach „bei einer einmonatigen Speicherpflicht die Aufklärungsrate der IP-Adressen in dem NCMEC-Prozess auf über 90% steigen“ würde.⁸

Entsprechend wäre die in Absatz 2, Nr. 4 vorgesehene irreversible Löschung der gespeicherten Daten vier Wochen nach dem Zeitpunkt der Zuweisung der IP-Adresse vorzunehmen. Diese Anregungen stützen sich zudem auf das Urteil des EuGH zur Vorratsdatenspeicherung vom 06.10.2020⁹, mit dessen Vorgaben die hier zu kommentierende vorgesehene gesetzliche Regelung u. E. unbedingt in Einklang stehen sollte.

Die in Absatz 3 vorgesehene Verwendung der Daten für die Erfüllung einer Europäischen Herausgabeanordnung oder einer Europäischen Sicherungsanordnung zur Erlangung von Teilnehmerdaten gemäß der Verordnung (EU) 2023/1543 mit der Einschränkung, dass die Daten nicht für andere Zwecke verwendet werden dürfen, halten wir für europarechtlich notwendig und sinnvoll.

4.4. Bußgeldvorschriften gem. § 228

Aus Sicht der Stiftung Digitale Chancen läuft die Bewertung von vorsätzlicher oder fahrlässiger Nichteinhaltung der Maßgaben der geänderten gesetzlichen Regelungen als Ordnungswidrigkeit der Absicht des Gesetzesvorhabens zur Erhöhung der Gefahrenabwehr im digitalen Raum zuwider. Die in Absatz 7 vorgesehenen Bußgelder in Höhe von 500.00 resp. 300.00 EUR erscheinen zudem zu niedrig, um die beabsichtigte Erhöhung der Gefahrenabwehr zu bewirken.

4.5. Begriffsverwendungen

Wie bereits in früheren Stellungnahmen weisen wir darauf hin, dass die Begriffe der Kinderpornografie sowie des sexuellen Missbrauchs im Zusammenhang mit sexueller Gewalt gegenüber Kindern abzulehnen sind.¹⁰ Die Stiftung Digitale Chancen empfiehlt vor diesem Hintergrund erneut, die Benennung von Straftaten in diesem Kontext zu prüfen und auf Basis der Terminology Guidelines zu revidieren.

5. Über die Stiftung Digitale Chancen

Die Stiftung Digitale Chancen ist eine gemeinnützige, operativ tätige Stiftung mit Sitz in Berlin. Seit 2002 erforscht sie die gesellschaftlichen Folgen der Digitalisierung und setzt sich für den chancengleichen Zugang aller Menschen zum Internet ein. Mit zahlreichen Projekten auf nationaler

⁸ Hessisches Ministerium der Justiz und für den Rechtsstaat (2023): Fakten zur IP-Adressspeicherung. 19. April 2023. <https://justizministerium.hessen.de/sites/justizministerium.hessen.de/files/2024-04/Factsheet%20IP-Adressdatenspeicherung%20%28Presse%29.pdf> Abruf am 28.01.2026

⁹ EuGH, 06.10.2020 - C-511/18, C-512/18, C-520/18

¹⁰ ECPAT Deutschland (2025): Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse. 2. Edition. März 2025. https://www.kinderrechte.digital/fileadmin/user_upload/Second-Edition-Terminology-Guidelines-final.pdf Abruf am 28.01.2026

und europäischer Ebene verfolgt die Stiftung das Ziel der digitalen Inklusion, Teilhabe und Chancengerechtigkeit und wirkt so einer digitalen Spaltung der Gesellschaft entgegen.

Berlin, 28. Januar 2026