Stellungnahme zum Entwurf eines Gesetzes zur Einführung einer IP-Adressspeicherung und Weiterentwicklung der Befugnisse zur Datenerhebung im Strafverfahren

Neue
Richter*innenvereinigung
Greifswalder Str. 4
10405 Berlin
Telefon 030 420223 49
Mobil 0176567 996 48
bb@neuerichter.de
www.neuerichter.de

02.02.2026

Sehr geehrte Damen und Herren,

die Neue Richter*innenvereinigung (NRV) bedankt sich für die Gelegenheit, zum Referentenentwurf eines Gesetzes zur Einführung einer IP-Adressspeicherung und Weiterentwicklung der Befugnisse zur Datenerhebung im Strafverfahren Stellung nehmen zu können.

I. Einleitung

Die Zielsetzung des vorliegenden Gesetzesentwurfs ist es, den Ermittlungsbehörden künftig die Möglichkeit zu eröffnen, Telekommunikationsanbieter zu verpflichten, IP-Adressen samt zugehöriger Portnummern zu speichern, um auf diese Weise den Anschlussinhaber eindeutig identifizieren zu können. Es soll damit einem kriminalpolitisch artikulierten Bedürfnis Rechnung getragen werden, wobei zu berücksichtigen ist, dass bereits in der Vergangenheit eine Vielzahl von Straftaten in Bezug auf Kinderpornographie und sexuellen Missbrauches trotz fehlender Speicherpflicht aufgeklärt werden konnten (https://beck-online.beck.de/Dokument?vpath=bibdata%2Freddok%2Fbecklink%2F2037003.htm&pos=14&hlwords=on).

Weiterhin soll es im Hinblick auf dynamische Verkehrsdaten ermöglicht werden, eine Sicherungsanordnung zu erlassen, um diese Daten vorsorglich zu sichern, sofern die rechtlichen und tatsächlichen Voraussetzungen für eine Datenerhebung noch nicht vorliegen.

Schließlich soll die bisher bereits zulässige Ermittlungsmaßnahme der Funkzellenabfrage im Einklang mit der Entscheidung des Bundesgerichtshofs vom 10. Januar 2024 (2 StR 171/23) wieder zur Anwendung kommen, wobei diese in Bezug auf den Tatverdacht höhere Anforderungen stellt. Aus Sicht der NRV bestehen keine Bedenken hinsichtlich der Einführung einer besonders hohen Eingriffsschwelle für schwerste Straftaten, um den höchstrichterlichen Anforderungen Genüge zu genügen.

II. Kritik

Zunächst ist festzustellen, dass Telekommunikationsanbieter IP-Adressen bereits speichern, jedoch ausschließlich zu zweckgebundenen, nicht zur allgemeinen Bevorratung von Ermittlungsdaten. Die geplante Erweiterung der Speicherbefugnisse zugunsten der Ermittlungsbehörden ist unter der Annahme einer technisch nicht eingrenzbaren Speicherung der Daten weiterhin abzulehnen, da sie den verfassungsrechtlichen Anforderungen nicht genügt.

Daher bedarf der der Gesetzesentwurf im Übrigen grundlegender Kritik. Es fehlt an der hinreichenden Darstellung der Notwendigkeit der Maßnahme. Denn unter Berücksichtigung der dargestellten Rechtsprechung der vergangenen Jahre im Blick auf die beabsichtigten Regelungen zur Vorratsdatenspeicherung, soll nunmehr eine leicht angepasste Regelung eingeführt werden, die den angeblich bestehenden kriminalpolitischen Bedürfnissen entsprechen würde, ohne dass diese empirisch hinterlegt sind. Bereits die aktuellen Regelungen der §§ 100a ff. StPO ermöglichen eine Überwachung der Kommunikation in Echtzeit oder retrograd oder den Abruf von Bestandsdaten von (verdächtigen) Personen, anhand derer eine Vielzahl von Straftaten aufgeklärt werden können. Eine spezifische Lücke, die durch die IP-Adressenspeicherung geschlossen werden müsste, ist für die Erforderlichkeit des Gesetzes nicht dargelegt.

Die IP-Adresse ist das sensibelste Datum im Internet. Die IP-Adresse dient zur Identifizierung eines Geräteanschlusses, eines/r Nutzer*in oder einer Website und mit ihrer Hilfe kann eine Verbindung zwischen dem Standort, der Nutzer und ihrem Surfverhalten im Internet hergestellt werden. Die berechtigte Intention mit Hilfe dieser Daten schwere Straftaten wie das Verbreiten von

*www.neuerichter.de
Neue Richter*innenvereinigung e.V. | Bundesbüro | Greifswalder Str. 4 | 10405 Berlin | Tel: 030-4202 2349
Mobil 0176 567 996 48 | bb@neuerichter.de | www.neuerichter.de
Sprecher der Fachgruppe: Dr. Simon Pschorr, Staatsanwalt, Staatsanwaltschaft Regensburg

Kinderpornographie aufklären zu können, darf aber nicht um jeden Preis erfolgen. Denn anhand der erhobenen IP-Adressen und Portnummern mit Zeitstempeln können umfassende Nutzerprofile im Hinblick auf die persönliche Lebensgestaltung, das Surfverhalten oder sensible Gesundheits- oder Bankinformation erstellt werden. Dies gilt umso mehr, weil es bislang technisch nicht möglich ist die zu speichernden Daten auf verdächtige Personendaten einzugrenzen und unbeteiligte Personen von der Datenerhebung auszuschließen. Es werden daher auch Daten von Personen gespeichert, die keinerlei Anlass für strafrechtliche Ermittlungen gegeben haben. Der aufgrund dieser Massenüberwachung erfolgende Eingriff in das Fernmeldegeheimnis des Art. 10 GG ist nicht zu rechtfertigen.

So führte auch der europäische Gerichtshof in einem Urteil aus Oktober 2020 (La Quadrature du Net) zur Sensibilität von IP-Daten aus:

„Da die IP-Adressen jedoch insbesondere zur umfassenden Nachverfolgung der von einem Internetnutzer besuchten Internetseiten und infolgedessen seiner Online-Aktivität genutzt werden können, ermöglichen sie die Erstellung eines detaillierten Profils dieses Nutzers. Die für eine solche Nachverfolgung erforderliche Vorratsspeicherung und Analyse der IP-Adressen stellen daher schwere Eingriffe in die Grundrechte des Internetnutzers aus den Art. 7 und 8 der Charta dar und können abschreckende Wirkungen wie die in Rn. 118 des vorliegenden Urteils dargelegten entfalten.“

In diesem Kontext ist es bedenklich, dass im Referentenentwurf (S. 22) lediglich von einer Identifizierung des Nutzers durch die IP-Adresse die Rede ist, ohne die umfassenden Folgen einer vollständigen Profilerstellung zu berücksichtigen. Die Speicherung von IP-Adressen unter der Maßgabe einer vollständigen Zuordnung von Internetaktivitäten zu einem bestimmten Anschlussinhaber setzt zwangsläufig die Erstellung eines Nutzerprofils in Gang, was einen erheblichen Grundrechtseingriff darstellt. Die zusätzliche Speicherung der Portnummer (§ 100g Abs. 5 Nr. 3 Ref-E) liefert zu der IP-Adresse den Zeitstempel des Verbindungsaufbaus und -abbruchs sowie die konkrete Zeitzone, sodass die erhobene IP-Adresse mit weiteren zusätzlichen notwendigen Informationen versehen ist. Solange dynamische IP-Adressen von mehreren Personen gleichzeitig genutzt werden können, kann erst mit diesen Informationen ein Bezug zu einer konkreten Straftat hergestellt werden. Gleichzeitig kann anhand dieser Daten ein noch weit umfassenderes Nutzerprofil erstellt werden.

Verfassungsrechtlich muss der Eingriff in das Fernmeldegeheimnis des Art. 10 GG hohen Anforderungen genügen. Aufgrund der Erheblichkeit des Eingriffs darf bei der Vorratsdatenspeicherung von IP-Adressen und vergleichbaren technischen Ermittlungsmaßnahmen ein Verdacht für eine auch im Einzelfall erhebliche Straftat nicht genügen. Zudem mangelt es den aktuellen Ermächtigungsgrundlagen der §§ 100a ff. StPO häufig an hinreichend klaren Regelungen, sodass die Unübersichtlichkeit der Vorschriften dazu führt, dass Staatsanwaltschaften und Ermittlungsgerichte häufig den § 100a Abs. 1 StPO als Ermächtigungsgrundlage anwenden, ohne dessen Voraussetzungen im Einzelfall vollumfänglich zu prüfen. Ob die Maßnahme tatsächlich auf die Überwachung einer Kommunikation abzielt und dabei die Anforderungen an den einfachgesetzlichen Kommunikationsbegriff erfüllt sind oder ob es sich nicht um eine Maßnahme eigener Art handelt, für die es aktuell an einer ausreichenden Ermächtigung fehlt, wird nur selten im Einzelfall geprüft.

So zeigt eine zuletzt ergangene Eilentscheidung des BVerfG, bei der sich ein Telekommunikationsanbieter gegen die Anordnung eines DNS-Monitoring wehrt, dass anhand einer Folgenabwägung eine flächendeckende Überwachung von IP-Adressen vorläufig nicht möglich sein soll (BVerfG, Einstweilige Anordnung vom 25. November 2025 – 1 BvR 2317/25 -). Insbesondere die § 100g StPO (Erhebung von Verkehrsdaten) und § 100j StPO (Erhebung von Bestandsdaten) zeigen, dass die Erhebung bestimmter Daten ermöglicht werden soll, aber die Art und Weise der Erhebung nicht näher konkretisiert wird. Um einen Grundrechtseingriff vollumfänglich prüfen zu können, bedarf es aber zu jeder Datenerhebung auch einer klaren Umgrenzung der möglichen Art und Weise der Datenerhebung. Dies belegt auch die Maßnahme des „IP-Catching“ (https://netzpolitik.org/2025/ip-catching-die-ueberwachungs-massnahme-die-geheim-bleiben-soll/). Der Fall zeigt, dass die zuständigen Institutionen mit der Anwendung der bestehenden einfachgesetzlichen Vorschriften teilweise herausgefordert sind und die technischen Anforderungen der Maßnahme nur selten vollumfänglich verstanden werden.

Aus rechtsstaatlicher Perspektive stellt dies einen erheblichen Mangel dar, da es sich zumeist um heimliche Maßnahmen handelt und die Betroffenen erst nachträglich darüber informiert werden, ohne dass ihnen gegen die Anordnung der Maßnahme effektiver Rechtsschutz zur Seite steht. Des Weiteren ist zu berücksichtigen, dass es den Ermittlungsbehörden, bei der Vielzahl der erhobenen Nutzerdaten, in der täglichen Praxis kaum möglich sein wird alle Betroffenen von der Maßnahme zu informieren, sodass sie niemals von ihrer eigenen Betroffenheit erfahren. Zunächst ist es deshalb erforderlich die Ermittlungsbehörden personell und technisch auf eine Weise

auszustatten, dass eine massenhafte Erhebung von Daten nicht erforderlich ist, sondern dass die Maßnahmen, sollten sie in Kraft treten, mit in einer effizienten Vorgehensweise punktuell und zielgerichtet für strafrechtliche Ermittlungen nutzbar gemacht und verarbeitet werden können.

Darüber hinaus können mit der fortschreitenden Digitalisierung und der Nutzung von Künstlicher Intelligenz (KI) durch die Ermittlungsbehörden neue Probleme auftreten. Algorithmen, die zur Auswertung der gesammelten Daten eingesetzt werden, könnten zu Lasten des Beschuldigten wirken, indem sie entlastende Beweise übersehen oder nicht berücksichtigen. Zudem könnte die Datenerhebung von privaten, kommerziellen Anbietern oder ausländischen Systemen in einem Maße erfolgen, dass eine staatliche Kontrolle und die Wahrung des Datenschutzes nicht mehr gewährleistet werden können.

Sollte der Gesetzgeber dennoch an dem Entwurf festhalten wollen, erscheint es möglicherweise sinnvoll, bei der zulässigen Speicherdauer von IP-Adressen nach Straftaten zu differenzieren, da verschiedene Straftaten zur Nachermittlung einer unterschiedlichen Speicherdauer bedürfen. Eine Differenzierung, bezogen auf die Notwendigkeit des Speicherzeitraums für eine effektive Strafverfolgung, könnte zur Verfassungsgemäßheit der Regelung beitragen.

III. Die Sicherungsanordnung

Besonders problematisch erscheint die in § 100g Abs. 7 Ref-E vorgesehene Möglichkeit, eine Sicherungsanordnung zur vorläufigen Speicherung von Verkehrsdaten zu erlassen, obwohl die tatsächlichen oder rechtlichen Voraussetzungen noch nicht gegeben sind. Eine solche Maßnahme, die den Tatverdacht vorzeitig aufgreift und damit den strafrechtlichen Kontext der Maßnahme aufweicht, stellt eine unzulässige Grundlage für eine anlasslose Massenüberwachung dar. Sie birgt die Gefahr einer flächendeckenden Datensammlung ohne konkrete Verdachtsmomente und führt zu einer praktischen Überforderung der Ermittlungsbehörden aufgrund der enormen Datenmengen, die anschließend aufgrund der unzureichenden personellen und technischen Ressourcen nicht zielgerichtet verarbeitet werden können. Wenngleich nach dem Ref-E (S. 33) eine Erhebung, gemeint sein dürfte eher ein Abruf durch die Ermittlungsbehörden, erst erfolgen soll, wenn sich die Anhaltspunkte zu einem qualifizierten Tatverdacht verdichtet haben, werden diese Daten bereits bei dem Verdacht auf eine Straftat von auch im Einzelfall erheblicher Bedeutung durch die Diensteanbieter erhoben.

***www.neuerichter.de**
Neue Richter*innenvereinigung e.V. | Bundesbüro | Greifswalder Str. 4 | 10405 Berlin | Tel: 030-4202 2349
Mobil 0176 567 996 48 | bb@neuerichter.de | www.neuerichter.de
Sprecher der Fachgruppe: Dr. Simon Pschorr, Staatsanwalt, Staatsanwaltschaft Regensburg

Die Sicherungsanordnung soll nach dem Ref-E auf Anordnung der Staatsanwaltschaft und bei Gefahr im Verzug durch ihre Ermittlungspersonen erfolgen dürfen. Dies ist aufgrund der Erheblichkeit des Grundrechtseingriffs bedenklich, nur unter einem Richtervorbehalt genügt die Anordnung verfassungsrechtlichen Maßstäben. Die §§ 100a ff. StPO sehen grundsätzlich die Anordnung einer Maßnahme durch einen Richter vor. Weshalb in den Fällen der Sicherungsanordnung eine Ausnahme geschaffen werden soll, erscheint nicht plausibel. Wenigstens sollte eine richterliche Bestätigung der Maßnahme binnen weniger Tage, vergleichbar zu § 98 Abs. 2 S. 1 StPO, eingeholt werden.

Vorkehrungen hinsichtlich einer Wahrung der Datensicherheit bei der Erhebung der Daten durch die Telekommunikationsanbieter sind dem Gesetzesentwurf nur bedingt zu entnehmen. Es fehlt an Anordnungen dazu, auf welchen Servern Daten gespeichert und verarbeitet werden dürfen, um nicht Gefahr zu laufen die Datenhoheit zu verlieren und für die Daten der Nutzer*innen möglicherweise einen irreparabler Schaden herbeizuführen.

Auch nach der Verordnung (EU) 2023/1543 sollen *„erlangte personenbezogene Daten nur verarbeitet werden, wenn dies erforderlich ist, und die Verarbeitung sollte so erfolgen, dass sie für den Zweck der Prävention, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Vollstreckung strafrechtlicher Sanktionen und der Ausübung des Rechts auf Verteidigung verhältnismäßig ist. Insbesondere sollten die Mitgliedstaaten sicherstellen, dass für die Übermittlung personenbezogener Daten von den jeweiligen Behörden an die Diensteanbieter für die Zwecke dieser Verordnung geeignete Datenschutzvorkehrungen und -maßnahmen gelten, unter anderem Maßnahmen zur Wahrung der Datensicherheit. Die Diensteanbieter sollten sicherstellen, dass für die Übermittlung personenbezogener Daten an die jeweiligen Behörden dieselben Garantien gelten. Der Zugang zu Informationen mit personenbezogenen Daten sollte befugten Personen vorbehalten sein, wofür durch Authentifizierungsverfahren gesorgt werden kann.“*

IV. Schlussfolgerung

Die beabsichtigten Regelungen zur Speicherung von IP-Adressen bleiben auch nach dem nunmehr vorgelegten Entwurf verfassungsrechtlich bedenklich.

***www.neuerichter.de**
Neue Richter*innenvereinigung e.V. | Bundesbüro | Greifswalder Str. 4 | 10405 Berlin | Tel: 030-4202 2349
Mobil 0176 567 996 48 | bb@neuerichter.de | www.neuerichter.de
Sprecher der Fachgruppe: Dr. Simon Pschorr, Staatsanwalt, Staatsanwaltschaft Regensburg

Sollte der Gesetzgeber die Einführung einer IP-Adressspeicherung dennoch für erforderlich erachten, bedürften sie einer Ermächtigungsgrundlage, die verfassungsrechtlichen Anforderungen im Hinblick auf einen Verdacht schwerster Straftaten („Eingriffszweck"), einer präzisen Maßnahmenbeschreibung im Hinblick auf die Erhebung bestimmter Daten sowie einer differenzierten zeitlichen Begrenzung der Speicherpflicht gerecht wird.

Schließlich soll darauf hingewiesen werden, dass es aus Sicht der NRV im Bereich der technischen Ermittlungsmaßnahmen, dies belegen die Diskussionen um Maßnahmen wie das DNS-Monitoring oder IP-Catching eindrücklich, dringend geboten erscheint ein hinreichend klares Schutzsystem zu entwickeln, das die Rechte der Betroffenen wahrt und rechtsstaatlichen Anforderungen genügt.

Dr. Sven Kersten
Für die Fachgruppe Strafrecht der NRV

***www.neuerichter.de**
Neue Richter*innenvereinigung e.V. | Bundesbüro | Greifswalder Str. 4 | 10405 Berlin | Tel: 030-4202 2349
Mobil 0176 567 996 48 | bb@neuerichter.de | www.neuerichter.de
Sprecher der Fachgruppe: Dr. Simon Pschorr, Staatsanwalt, Staatsanwaltschaft Regensburg