Stellungnahme des Arbeitskreises Vorratsdatenspeicherung zum Referentenentwurf des BMJ zur „Einführung einer IP-Adressspeicherung und Weiterentwicklung der Befugnisse zur Datenerhebung“

Überblick

Der Gesetzentwurf plant die Einführung einer dreimonatigen, anlasslosen Speicherung aller IP-Adressen und Portnummern. Der AK Vorrat hält diesen Entwurf für einen gefährlichen Rückschritt in die Massenüberwachung. Mit IP-Vorratsdatenspeicherung würde die Identität praktisch jeder Internetnutzung nachträglich feststellbar: welcher Anschluss hinter einem Posting, einer Suchanfrage, einem Forenbeitrag, dem Aufruf einer Beratungsstelle oder eines journalistischen Angebots steht. Der Arbeitskreis Vorratsdatenspeicherung lehnt eine solche anlasslose Massenspeicherung entschieden ab. Nicht zuletzt durch Einbeziehung von Portnummern und angesichts der niedrigen Hürden für den Datenabruf birgt der Gesetzentwurf massive rechtliche Risiken und bedroht die digitale Anonymität unbescholtener Bürger, ohne die Sicherheit messbar zu erhöhen, weil Straftäter einfach auf Anonymisierungsdienste ausweichen können.

Die Behauptung des Justizministeriums, eine IP-Adresse sei lediglich ein „digitales Kfz-Kennzeichen“, ist irreführend. Im Netz erfordert fast jede Interaktion eine IP-Verbindung und wird mit IP-Adresse in Logfiles protokolliert. Im wirklichen Leben entspräche dies einer Kombination aus ständig sichtbarem Kennzeichen und umfassender Bewegungs- und Leseprotokollierung: Als müssten alle Menschen ein Nummernschild um den Hals tragen und der Staat ließe anhand dieses Nummernschilds flächendeckend mitschreiben, wann wir welches Lokal, welche Arztpraxis, welche Beratungsstelle oder politische Versammlung aufsuchen und welche Zeitung wir wo gelesen haben – nicht nur bei Verdächtigen, sondern bei ausnahmslos allen. Eine solche lückenlose Protokollierung des Sozialverhaltens wäre in der physischen Welt in einer Demokratie undenkbar.

Die Auswirkungen: Eine solche Totalerfassung zerstört die digitale Anonymität und damit den vertraulichen Raum für Hilfesuchende, Presseinformanten und politische Aktivisten. Dieser „Chilling Effect“ führt dazu, dass Missbrauchsopfer aus Angst vor Registrierung keine Hilfe suchen und Whistleblower schweigen. Statt Kriminelle zu verfolgen (die sich technisch schützen können), schafft das Gesetz eine Infrastruktur der Überwachung, die tief in die Grundrechte unbescholtener Bürger eingreift und das Vertrauen in die freie Kommunikation nachhaltig beschädigt. Die anlasslose IP-Vorratsdatenspeicherung verstößt damit gegen den Grundsatz, dass Überwachung im Rechtsstaat die begründete Ausnahme bleiben muss – und nicht zum Normalzustand für alle werden darf.

I. Warum eine IP-Vorratsdatenspeicherung der Strafverfolgung mehr schadet als nützt

Entgegen der Darstellung des Ministeriums ist die anlasslose Internet-Vorratsdatenspeicherung kein Wundermittel der Kriminalitätsbekämpfung. Sie ist ineffektiv gegen Profis und kontraproduktiv für die Sicherheit im Netz:

- **Ausweichbewegungen:** Kriminelle Akteure, insbesondere im Bereich der organisierten Kriminalität und der Verbreitung von Missbrauchsdarstellungen, reagieren technologisch. Eine Speicherpflicht führt zur massenhaften Nutzung von Anonymisierungsdiensten (VPNs, Tor, Proxy-Server). Auch wir werden dies zum Schutz unbescholtener Bürger öffentlich nachdrücklich empfehlen.
    - *Folge:* Die gespeicherte IP-Adresse führt dann im Fall einer strafrechtlichen Ermittlung lediglich zu einem VPN-Server im Ausland oder einem Tor-Exit-Node, nicht zum Täter. Wo bisher typischerweise sieben Tage lang noch eine Rückverfolgung anhand der IP-Adresse möglich war oder in Echtzeit zurückverfolgt werden konnte, ist bei Verwendung ausländischer Anonymisierungsdienste eine Rückverfolgung praktisch ausgeschlossen. Dadurch schadet die IP-Vorratsdatenspeicherung der Strafverfolgung insgesamt massiv und wirkt kontraproduktiv.
- **Historischer Beleg des Scheiterns:** Erfahrungen aus der Praxis widerlegen den Nutzen. Als 2009 in Deutschland die Vorratsdatenspeicherung von IP-Adressen in Kraft war, stieg die Aufklärungsquote bei Internetdelikten nicht an, sondern ging zurück. Auch in anderen EU-Ländern mit IP-Vorratsdatenspeicherung ist nicht bekannt, dass diese Maßnahme zu einem messbaren Anstieg der Aufklärungsquote bei Internetdelikten geführt hätte.
- **Hohe Aufklärungsquoten auch ohne Vorratsdatenspeicherung:** Die aktuelle BKA-Kriminalstatistik belegt auch ohne Speicherpflicht hohe Aufklärungsquoten (ca. 61,5 % bei Internetkriminalität allgemein, ca. 87,6 % bei Verbreitung pornografischer Inhalte).
    - *Fazit:* Der Ruf nach Massenspeicherung ignoriert, dass klassische Polizeiarbeit und bestehende Befugnisse bereits sehr effektiv sind.
- **Schaden durch „Chilling Effect“:** Die Speicherung zerstört das Vertrauen in die Vertraulichkeit digitaler Kommunikation. Wenn Bürger (z. B. Whistleblower, Missbrauchsopfer, Presseinformanten) fürchten müssen, dass ihre Spuren digital protokolliert werden, unterbleiben wichtige Hinweise an Beratungsstellen oder die Presse. Das Dunkelfeld wächst, die soziale Kontrolle nimmt ab.

II. Die europarechtliche Grauzone: Vorratsspeicherung von Portnummern

Der Entwurf geht über das vom EuGH Tolerierte hinaus, indem er auch Portnummern in die Speicherpflicht einbezieht:

- **EuGH-Rechtsprechung ignoriert:** Der Europäische Gerichtshof (EuGH) hat sich zur Zulässigkeit einer Vorratsdatenspeicherung auch von Portnummern bislang nicht geäußert. Er hat lediglich eine IP-Speicherung unter engen Voraussetzungen für möglich gehalten.
    - *Risiko:* Die Speicherung von Portnummern erhöht die Eingriffsintensität drastisch und könnte das Gesetz europarechtswidrig machen.
- **Gefahr der Profilbildung:** Portnummern sind mehr als technische Anhängsel. In Kombination mit IP-Adressen und Zeitstempeln ermöglichen sie Rückschlüsse auf charakteristische Nutzungsmuster und können etwa einen Rückschluss auf die abgerufenen Internetseiten zulassen.
    - *BfDI-Warnung:* Der Bundesdatenschutzbeauftragte warnt, dass aus diesen Daten auch ohne Inhaltsüberwachung präzise Rückschlüsse auf Lebensgewohnheiten gezogen werden können.
- **Technische Fehleranfälligkeit (Carrier-grade NAT):** Bei der dynamischen Zuweisung von Portnummern teilen sich hunderte Nutzer eine IP-Adresse.
    - *Gefahr:* Minimale Abweichungen bei Zeitstempeln (Server-Uhrzeiten vs. Provider-Logs) führen zwangsläufig zu falschen Zuordnungen. Unschuldige Bürger geraten so ins Visier von Hausdurchsuchungen, weil sie zur „falschen Zeit am falschen Port“ waren.
- **Unverhältnismäßige Datenmengen:** Der Aufruf einer einzigen modernen Webseite erzeugt hunderte Verbindungen mit verschiedenen Ports. Die zu speichernde Datenmenge explodiert, was hohe Kosten und Sicherheitsrisiken (Hacks der Datenbanken) bei den Providern verursacht.

III. Die IP-Adresse ist der Schlüssel: Zugriffsrechte europarechtswidrig und unverhältnismäßig

Sollte die Speicherung dennoch politisch durchgesetzt werden, darf die Nutzung dieser sensiblen Daten keinesfalls – wie vom Ministerium geplant – wie eine simple Adressabfrage behandelt werden. Die Speicherung kann nur dann unionsrechtskonform sein, wenn die Nutzung der Daten extrem streng reglementiert und auf wenige eng umrissene Zwecke beschränkt wird:

- **Der „Generalschlüssel“ zur Identität:** Die Zuordnung einer IP-Adresse zu einem Anschlussinhaber hebt die Anonymität von Onlineprofilen auf. In Kombination mit den Daten, die Plattformen wie Google, Meta oder X (Twitter) speichern, wird das gesamte digitale Leben einer Person transparent

(Suchverläufe, politische Äußerungen, Gesundheitsdaten, Bewegungsbilder). Im realen Leben ist unser Verhalten nicht anhand unseres Kfz-Kennzeichens nachvollziehbar. Die Abfrage einer auf Vorrat gespeicherten IP-Adresse muss deshalb rechtlich wie der Zugriff auf Verkehrsdaten behandelt werden.

- **Zwingender Richtervorbehalt:** Wegen der enormen Sensibilität darf die Abfrage einer auf Vorrat gespeicherten IP-Adresse **niemals** automatisiert oder als simple Bestandsdatenauskunft erfolgen. Da die Abfrage einer IP-Adresse genaue Schlüsse auf das Privatleben ermöglichen kann (siehe oben) und der Strafverfolgung dient, muss sie laut EuGH (EuGH, 30.04.2024 - C-470/21) zwingend „von einer Kontrolle durch ein Gericht oder eine unabhängige Verwaltungsstelle abhängig gemacht“ werden, wobei die Strafverfolgungsorgane keine unabhängige Verwaltungsstelle in diesem Sinne sind (Rn. 126). Der EuGH sieht eine besondere Sensibilität etwa dann, wenn mit einer IP-Abfrage die Kontakte oder der Standort einer Zielperson ermittelt werden soll (a.a.O., Rn. 101) oder wenn sie der Nachverfolgung der von ihrem Inhaber besuchten Internetseiten dient (a.a.O., Rn. 115).
    - *Forderung:* Wie bei anderen Verkehrsdatenzugriffen muss vor jeder Abfrage einer IP-Adresse ein unabhängiger Richter prüfen, ob der Eingriff im Einzelfall verhältnismäßig ist.
- **Beschränkung auf Strafverfolgung europarechtlich geboten:** Der Gesetzentwurf will die Verwendung auf Vorrat gespeicherter IP-Adressen unter denselben Voraussetzungen erlauben wie eine beliebige Bestandsdatenauskunft (§ 174 TKG), also für unzählige Zwecke und nahezu allen nur denkbaren Stellen. Das ist politisch inakzeptabel und europarechtlich nicht haltbar.
    - *Politische Forderung:* Weil IP-Abfragen die Rekonstruktion des Inhalts der Internetnutzung ermöglichen, fordern wir, sie auf den Katalog schwerer Straftaten nach § 100a StPO zu beschränken (wie Telekommunikations- und Internetüberwachung).
    - *Rechtliche Mindestanforderung:* Europarechtlich kann die anlasslose Vorratsspeicherung und Abfrage von IP-Adressen laut EuGH gerechtfertigt sein, um „Straftaten im Allgemeinen zu verhüten, zu ermitteln, festzustellen und zu verfolgen“ (EuGH, 30.04.2024 – C-470/21, Rn. 92, 95). Daneben kann die Verhütung schwerer Bedrohungen der öffentlichen Sicherheit eine Vorratsdatenspeicherung rechtfertigen (EuGH a.a.O., Rn. 95). § 174 TKG geht aber weit darüber hinaus. So setzen Zugriffe durch BfV, MAD, BND und BSI weder einen Tatverdacht noch eine konkrete Gefahr voraus. Das ist europarechtswidrig. Zugriffe zu rein präventiven Zwecken ohne konkrete Gefahr und ohne Tatverdacht (etwa durch Nachrichtendienste oder BSI) sind auszuschließen.

IV. Grundrechtsschonende Alternativen zur Vorratsdatenspeicherung

Statt alle Bürger unter Generalverdacht zu stellen, sollten zielgerichtete Instrumente gewählt werden:

- **Sicherungsanordnung (Anlassbezogene Speicherung):** Bei einem konkreten Anfangsverdacht werden Daten bei den Providern „eingefroren“ (gesichert), aber erst nach richterlicher Prüfung herausgegeben.
    - *Vorteil:* Dies respektiert die Unschuldsvermutung und ist grundrechtskonform.
- **Login-Falle bei Wiederholungsgefahr:** Kann ein Täter bei einer Tat nicht identifiziert werden (z. B. wegen fehlender Daten), wird der Provider verpflichtet, bei der *nächsten* Einwahl des betreffenden Accounts die Daten zu sichern.
    - *Praxis:* Bisher werden NCMEC-Hinweise (Cybertipline) oft weggelegt, wenn die IP-Adresse nicht mehr gespeichert ist, anstatt den Account für die Zukunft zu überwachen.
- **Lückenhafte NCMEC-Meldungen:** US-Diensteanbieter nehmen in ihre Verdachtsmeldungen (NCMEC-Reports) oft keine Portnummern und Ziel-IP-Adressen auf. In diesen Fällen (NAT) scheitert eine Identifizierung – ob mit oder ohne IP-Vorratsdatenspeicherung.
- **Löschen statt Speichern:** Das BKA muss die Aufgabe erhalten, im Zuge von Ermittlungen festgestellte illegale Inhalte (insb. Missbrauchsdarstellungen) den Hostern zu melden, statt nur Darknet-Foren zu schließen und die weitere Zirkulation der dort verlinkten Missbrauchsdarstellungen zu dulden.

V. Bundesregierung muss EU-Plänen zur „Vorratsdatenspeicherung 2.0“ eine klare Absage erteilen

Parallel zu diesem Gesetzgebungsverfahren arbeitet die EU-Kommission an Vorgaben zur „Vorratsdatenspeicherung 2.0“, die weit über den Koalitionsvertrag und eine IP-Vorratsdatenspeicherung hinausgehen. Dass die Bundesregierung diesen Plänen im EU-Rat bisher keine klare Absage erteilt hat, ist inakzeptabel.

Konkret droht auf EU-Ebene:

1. **Mogelpackung „gezielte Vorratsdatenspeicherung“:** Erwogen wird die "gezielte" Vorratsspeicherung der Verbindungsdaten und Standorte sämtlicher Personen in Gebieten mit „überdurchschnittlicher Kriminalität“ oder “wohlhabenden Wohngebieten”. Da dies auf fast jede Großstadt zutrifft, geraten Millionen unschuldiger Bürger und Pendler allein durch ihren Wohn- oder Aufenthaltsort unter Generalverdacht. Von weiteren "Zielen" betroffen sein könnten Touristen, Benutzer öffentlicher Verkehrsmittel oder Fahrer an

Mautstellen. Erwogen wird zudem, Informationen über Menschen in Kirchen, Schulen, Einkaufszentren und sogar bei Protestmärschen zu sammeln.

2. **Dammbruch bei Messengern und Chats:** Erstmals soll eine Pflicht zur Vorratsdatenspeicherung auch für sogenannte Over-the-Top-Dienste (OTT) eingeführt werden. Damit müssten auch Anbieter von **Messengern (z. B. WhatsApp, Signal), E-Mail-Diensten und Videokonferenzen** protokollieren, wer wann mit wem kommuniziert. Dies tiefer in die Privatsphäre ein als die von EuGH gekippte Richtlinie zur Vorratsdatenspeicherung.
3. **Angriff auf die Anonymität:** Geplant sind auch Identifizierungspflichten für diese Dienste. Dies würde das Recht auf anonyme Kommunikation im Netz faktisch abschaffen und den Schutzraum für Whistleblower, Presseinformanten und Hilfesuchende zerstören.

Unsere Forderung: Die Bundesregierung muss im EU-Rat ihr Schweigen brechen und diese noch weit über den Koalitionsvertrag hinaus gehenden Pläne zu einer Vorratsdatenspeicherung 2.0 **aktiv und eindeutig ablehnen**. Die Zeit drängt, weil die EU-Kommission ihren Vorschlag bald vorlegen will.

06.02.2026

Arbeitskreis Vorratsdatenspeicherung

Der Arbeitskreis Vorratsdatenspeicherung (AK Vorrat) ist ein bundesweiter Zusammenschluss, der sich gegen die ausufernde Überwachung im Allgemeinen und gegen die Vollprotokollierung der Telekommunikation und anderer Verhaltensdaten im Besonderen einsetzt. Mitglieder des Arbeitskreises sind Bürgerrechtler, Datenschützer und Internetnutzer, aber auch Verbände, Organisationen und Initiativen. Sie engagieren sich gegen die anlasslose Speicherung persönlicher Daten, für mehr Datenschutz, für das Recht auf Privatheit, für unbeobachtete Kommunikation und für den Respekt vor der Menschenwürde, besonders für das Recht auf informationelle Selbstbestimmung.

Homepage und Kontakt: https://www.vorratsdatenspeicherung.de