Stellungnahme

Gewerkschaft der Polizei
Bundesvorstand

Stellungnahme der Gewerkschaft der Polizei (GdP)

zu einer Folgenabschätzung der
Europäischen Kommission zur

Vorratsdatenspeicherung durch Dienstanbieter für Strafverfahren

Berlin, 08.09.2025
Abt. II – jg, kj, mh

I. - Vorbemerkung

Die Gewerkschaft der Polizei (GdP) begrüßt ausdrücklich die Initiative der Europäischen Kommission zur Bewertung und möglichen Einführung eines Rechtsrahmens für eine Vorratsdatenspeicherung, um damit die Grundlage für eine europäische Harmonisierung zu schaffen. Für Polizei und Strafverfolgungsbehörden ist die Sicherung und der rechtzeitige Zugriff auf bestimmte, nicht inhaltsbezogene Kommunikationsdaten unverzichtbar, um Straftaten wirksam aufzuklären und die Sicherheit der Bürgerinnen und Bürger zu gewährleisten. Nationale Alleingänge und die derzeitige Rechtszersplitterung führen zu erheblichen praktischen Problemen für die Ermittlungsbehörden. Daher unterstützt die GdP nachdrücklich das Ziel, einen einheitlichen, europäisch abgestimmten Rechtsrahmen für die Vorratsdatenspeicherung zu schaffen. Insofern nehmen wir die Gelegenheit gerne wahr, als mit über 210.000 Mitgliedern größte Polizeigewerkschaft in Deutschland und als Mitglied im europäischen Dachverband EU.Pol, zu der Initiative der Europäischen Kommission Stellung zu nehmen.

II. - Sicherheitspolitische Relevanz

Die gegenwärtige Bedrohungslage verdeutlicht in besonderer Weise die Notwendigkeit einer verpflichtenden Vorratsdatenspeicherung. Kriminalität verlagert sich zunehmend in den digitalen Raum. Cybercrime stellt die am schnellsten wachsende Kriminalitätsform dar. Täterinnen und Täter agieren international, nutzen hochgradig arbeitsteilige Strukturen – häufig im Modell des sogenannten „Cybercrime-as-a-Service“. Parallel dazu nimmt die Verbreitung von Hasskriminalität und extremistischen Inhalten im Netz zu. Diese Entwicklungen stellen nicht nur eine Gefahr für die betroffenen Opfer dar, sondern bedrohen auch demokratische Prozesse und die gesellschaftliche Stabilität insgesamt. Besonders gravierend ist der Anstieg bei Darstellungen sexualisierter Gewalt gegen Kinder. Hier sind IP-Adressen oftmals die einzige Ermittlungsgrundlage. Ohne eine gesicherte Speicherung dieser Daten laufen zahlreiche Verfahren ins Leere, sodass Täter nicht identifiziert und Opfer nicht geschützt werden können. Hinzu kommt, dass Unternehmen in wachsendem Maße Ziel von massiven Cyberangriffen werden, die erhebliche wirtschaftliche Schäden verursachen und ganze Branchen oder kritische Infrastrukturen gefährden können.

Vor diesem Hintergrund ist eine wirksame Vorratsdatenspeicherung nicht nur ein kriminalistisches Werkzeug, sondern auch ein gesellschafts- und sicherheitspolitisches Erfordernis. Sie trägt entscheidend dazu bei, die Sicherheit der Bürgerinnen und Bürger zu gewährleisten, Opfer zu schützen und das Vertrauen in den Rechtsstaat zu stärken. In diesem Zusammenhang ist jedoch auch festzuhalten, dass nach wie vor **bestehende datenschutzrechtliche Hürden** zu einer faktischen Blockade digitaler Ermittlungsarbeit führen. Die GdP fordert daher insgesamt **eine kritische Überprüfung datenschutzrechtlicher Vorgaben** vorzunehmen, die in der Praxis Ermittlungsbehörden bei der Bekämpfung schwerster Kriminalität unverhältnismäßig einschränken. Gleichzeitig muss gewährleistet bleiben, dass rechtsstaatliche Grundsätze strikt beachtet werden. Nur durch eine klare Balance zwischen effektiver Strafverfolgung und dem Schutz individueller Grundrechte kann ein tragfähiger europäischer Rechtsrahmen geschaffen werden.

III. - Bedeutung der Vorratsdatenspeicherung für die Strafverfolgung

Digitale Spuren spielen heute in nahezu jedem Verfahren eine Rolle. Gerade bei Delikten, die sich im digitalen Raum abspielen, etwa bei Cyberkriminalität, sexualisierter Gewalt im Internet, Hasskriminalität, organisierter Kriminalität oder auch terroristischen Aktivitäten, sind IP-Adressen und Portnummern oftmals der einzige Ansatzpunkt, um Tatverdächtige überhaupt identifizieren zu können. In Fällen des sexuellen Missbrauchs von Kindern, die häufig über Hinweise internationaler Organisationen wie dem National Center for Missing & Exploited Children (NCMEC) an die Strafverfolgungsbehörden herangetragen werden, bilden IP-Adressen oft die einzige Spur zu den Tätern. Problematisch ist dabei, dass es derzeit keine Speicherpflicht gibt. Viele Anbieter bewahren Daten ausschließlich für eigene Zwecke auf. In Deutschland werden solche Daten meist nur für einen Zeitraum von höchstens sieben Tagen gespeichert, Portnummern häufig gar nicht. Für komplexere Ermittlungen, in denen IP-Adressen oftmals erst nach einer gewissen Zeit bekannt werden, sind diese kurzen Speicherfristen völlig unzureichend.

Die Konsequenz ist gravierend: Ermittlungen scheitern, Täter bleiben anonym und die Opfer erhalten nicht den Schutz, den sie dringend benötigen.

IV. - Rechtliche Rahmenbedingungen und europäische Harmonisierung

Die derzeitige Rechtslage innerhalb der Europäischen Union ist durch eine Vielzahl unterschiedlicher oder fehlender Regelungen zur Vorratsdatenspeicherung geprägt. Während einige Mitgliedstaaten keine Speicherpflichten vorsehen, existieren in anderen Ländern sehr unterschiedliche Vorgaben hinsichtlich der Dauer oder des Umfangs der Speicherung. Dieses Auseinanderdriften führt zu erheblichen Schwierigkeiten für die Strafverfolgung.
Einerseits entsteht für Anbieter digitaler Kommunikationsdienste, die europaweit tätig sind, ein unübersichtliches und belastendes Regelungsgefüge, das Rechtsunsicherheit schafft und zusätzliche Kosten verursacht. Andererseits wird die grenzüberschreitende Zusammenarbeit der Strafverfolgungsbehörden massiv erschwert, weil in einem Mitgliedstaat noch vorhandene Daten in einem anderen bereits gelöscht sein können. Für Bürgerinnen und Bürger bedeutet diese Uneinheitlichkeit, dass Straftaten unterschiedlich effektiv verfolgt werden.

Eine einheitliche europäische Regelung würde diese Probleme lösen. Sie würde Rechtssicherheit für Anbieter schaffen und die Zusammenarbeit der Strafverfolgungsbehörden erleichtern. Vor allem aber würde sie den Ermittlungsbehörden verlässlichere Möglichkeiten eröffnen, Straftaten aufzuklären und damit die Sicherheit der Bevölkerung zu stärken. Die GdP sieht deshalb in einer EU-weiten Harmonisierung nicht nur einen rechtspolitisch, sondern auch einen kriminalpolitisch zwingend notwendigen Schritt.

V. - Anforderungen an eine Vorratsdatenspeicherung

Aus Sicht der GdP müssen an eine europäische Regelung zur Vorratsdatenspeicherung klare Anforderungen gestellt werden:

- Im Zentrum steht die Einführung einer verbindlichen Mindestspeicherfrist für IP-Adressen und Portnummern. Diese Daten sind in den meisten Fällen der einzige Ermittlungsansatz. **Eine Speicherdauer von mindestens drei Monaten ist erforderlich, besser jedoch sechs**

Monate, um auch komplexere und länger andauernde Ermittlungen, etwa im Bereich organisierter Kriminalität, Cyberkriminalität oder Terrorismus, wirksam führen zu können. Kürzere Fristen reichen in der Praxis häufig nicht aus, da IP-Adressen oftmals erst mit zeitlicher Verzögerung in Ermittlungen relevant werden.

- Darüber hinaus muss es möglich sein**, Verkehrs- und Standortdaten sowohl allgemein als auch anlassbezogen zu speichern, wenn eine Bedrohung der nationalen Sicherheit vorliegt.** Gerade in Fällen schwerwiegender Gefahrenlagen wie terroristischer Bedrohungen oder großangelegter Cyberangriffe kann nur durch den Zugriff auf solche Daten ein umfassendes Lagebild erstellt und wirksam reagiert werden.
- Zugleich ist klar, dass eine **Speicherung immer an rechtsstaatliche Standards gebunden** sein muss. Der Zugang zu den gespeicherten Daten darf nur unter strengen Voraussetzungen und nach klar geregelten Verfahren erfolgen. So wird sichergestellt, dass die Verhältnismäßigkeit gewahrt bleibt und der Grundrechtsschutz der Bürgerinnen und Bürger nicht untergraben wird.

Der vielfach diskutierte Gegenvorschlag des sogenannten „Quick-Freeze“-Verfahrens stellt in diesem Zusammenhang keine echte Lösung bzw. Alternative dar. Quick-Freeze setzt voraus, dass ein Anschlussinhaber bereits identifiziert ist. Genau diese Identifizierung ist jedoch in der überwiegenden Zahl der Fälle nur mithilfe zuvor gespeicherter IP-Daten möglich. Ohne Vorratsdatenspeicherung bleibt Quick-Freeze daher ein wirkungsloses Instrument, das den Ermittlungsbehörden nicht die notwendige Handlungsfähigkeit verleiht.

VI. - Rolle der EU-Institutionen und Agenturen

Die GdP betont, dass der Erfolg einer europäischen Vorratsdatenspeicherung nicht allein von der nationalen Umsetzung abhängt, sondern wesentlich von der **klaren Rolle und Koordination der europäischen Institutionen** bestimmt wird. Neben einer einheitlichen Rechtsgrundlage bedarf es eines gemeinsamen Verständnisses für die sicherheitspolitische Relevanz digitaler Verkehrsdaten im gesamten Rechtsraum der EU.

Gerade die Institutionen der Europäischen Union – die Europäische Kommission, der Rat und das Europäische Parlament – tragen eine zentrale Verantwortung dafür, die Voraussetzungen für eine effektive und grundrechtskonforme Vorratsdatenspeicherung zu schaffen. Sie müssen nicht nur den rechtlichen Rahmen harmonisieren, sondern auch die **grenzüberschreitende Zusammenarbeit der Ermittlungsbehörden koordinieren** und absichern.

Eine besondere Rolle kommt dabei **Europol** zu. Als EU-Agentur mit operativer und analytischer Zuständigkeit für schwere und organisierte Kriminalität kann Europol künftig eine wichtige Schnittstelle bei der **Verarbeitung und Verknüpfung digitaler Spuren über Ländergrenzen hinweg** darstellen. Um diese Rolle auszufüllen, muss Europol jedoch über einen **gesetzlich abgesicherten Zugriff auf verkehrsdatenbezogene Informationen** verfügen – und mit ausreichend Ressourcen ausgestattet sein, um Ermittlungen mit hohem Datenaufkommen zu unterstützen. Hier beruft sich die GdP insbesondere auf das Versprechen der Kommission in ihrer ProtectEU Strategie für die Innere Sicherheit, Europol in eine wirklich operative Polizeibehörde zur Unterstützung der Mitgliedstaaten zu verwandeln.

Das Mandat von und Europols Kontrolle durch den europäischen Datenschutzbeauftragten darf dabei nicht der erfolgreichen Strafverfolgung und der Entwicklung von innovativen Tools für die Datenspeicherung, -verarbeitung und -analyse im Wege stehen.

Die GdP fordert daher:

- eine **klare rechtliche Verankerung der Rolle von Europol** bei der Auswertung und Koordination digitaler Ermittlungsdaten im Rahmen der Vorratsdatenspeicherung,
- die **Bereitstellung finanzieller und personeller Mittel** auf EU-Ebene, um technische Schnittstellen, Analysekapazitäten und Ausbildungsprogramme zu stärken,
- sowie die **Einbindung von EU-Agenturen in die Umsetzung und Kontrolle** der künftigen Speicherregelung, insbesondere zur Gewährleistung einheitlicher Standards in den Mitgliedstaaten.
- Eine **Revision des Kontrollmandats des europäischen Datenschutzbeauftragten** gegenüber Europol, bzw. die Einführung einer Berufungsinstanz im Falle eines negativen Assessments durch den Datenschutzbeauftragten von innovativen Europol-Tools.

Nur wenn die europäischen Institutionen hier konsequent handeln, kann die Vorratsdatenspeicherung ihren Beitrag zur inneren Sicherheit in einem offenen, digitalen Europa leisten.