VERBAND DER INTERNETWIRTSCHAFT E.V.

Info-Papier

zum Gesetzentwurf der Bundesregierung zur Modernisierung des Bundespolizeigesetzes

Berlin, 16.12.2025

Mit dem Entwurf zur Modernisierung des Bundespolizeigesetzes (BPolG) legt die Bundesregierung erstmals seit den 1990er-Jahren eine umfassende Neufassung des Gesetzes vor. Ziel ist es, die Befugnisse der Bundespolizei an veränderte technische, gesellschaftliche und sicherheitspolitische Rahmenbedingungen anzupassen. Ausgangspunkt sind dabei insbesondere die zunehmende Digitalisierung von Kommunikation, der verbreitete Einsatz von Ende-zu-Ende-Verschlüsselung sowie neue Arbeitsweisen organisierter Kriminalität. Zugleich reagiert der Gesetzgeber auf mehrere Entscheidungen des Bundesverfassungsgerichts, die bestehende Sicherheitsgesetze, etwa das BKA-Gesetz, wegen unzureichender Begrenzungen und Schutzmechanismen für Grundrechte beanstandet haben.

Gerade im Bereich der Telekommunikationsüberwachung geht der Entwurf jedoch deutlich weiter als eine bloße Fortschreibung bestehender Instrumente. Der neu gefasste § 40 BPolG-E erweitert die Möglichkeiten der Bundespolizei erheblich und wirft grundlegende Fragen sowohl nach Verhältnismäßigkeit und technischer Sicherheit als auch nach den mittelbaren Folgen für digitale Infrastrukturen auf. Vor allem folgende Punkte dürfen in der weiteren Debatte um eine Modernisierung des Bundespolizeigesetzes nicht unberücksichtigt bleiben:

1. Ausweitung der Telekommunikationsüberwachung

Der neue § 40 BPolG-E schafft eine eigenständige, umfassende Rechtsgrundlage für die Überwachung der Telekommunikation durch die Bundespolizei im Bereich der Gefahrenabwehr. Er orientiert sich zwar formal an bestehenden Regelungen im BKA-Gesetz, überträgt diese Logik aber auf ein deutlich breiteres Einsatzspektrum der Bundespolizei. Besonders problematisch ist, dass die Norm nicht nur klassische Telekommunikationsüberwachung adressiert, sondern faktisch auch den Einsatz von Quellen-TKÜ ermöglicht.

Aus Sicht der Internetwirtschaft ist diese Entwicklung kritisch zu bewerten. Bei der Quellen-TKÜ wird die Kommunikation nicht auf der Leitung, sondern direkt auf dem Endgerät überwacht. Die geschieht regelmäßig mithilfe sogenannter Staatstrojaner. Das Bundesverfassungsgericht hat hierfür enge verfassungsrechtliche Grenzen gezogen und insbesondere betont, dass derartige Maßnahmen nur bei schwersten Gefahren und unter strikten Voraussetzungen zulässig sind. Der vorliegende Entwurf bleibt hier zu unbestimmt und verlagert zentrale Abwägungen in die Anwendungspraxis, anstatt sie klar gesetzlich einzugrenzen.

Hinzu kommt ein ungelöster technischer Zielkonflikt. Der Einsatz von Staatstrojanern erfolgt in der Regel unter der Ausnutzung von IT-Sicherheitslücken. Zwar hat die Koalition in Aussicht gestellt, deren Zugang zu regeln, jedoch zeigen sich im Lichte des NIS2UmsuCG noch offene Fragen hinsichtlich der weiteren Ausgestaltung. Mit der Ausnutzung von Sicherheitslücken wird die IT-Sicherheit insgesamt geschwächt, nicht nur für potenzielle Zielpersonen, sondern für Millionen

Bürger:innen und Unternehmen. Der Staat darf jedoch nicht selbst zum Risiko für die digitale Sicherheit werden. Eine Sicherheitsarchitektur, die auf dem systematischen Ausnutzen von Schwachstellen beruht, steht im Widerspruch zu einem ganzheitlichen Verständnis von Cybersicherheit.

2. Risiken für IT-Sicherheit und Vertrauen in digitale Infrastrukturen

Der Gesetzentwurf berücksichtigt die sicherheitspolitischen Folgewirkungen solcher Eingriffsbefugnisse nur unzureichend. Gerade im Zuständigkeitsbereich der Bundespolizei (Grenzschutz, Verkehrsinfrastrukturen, kritische Knotenpunkte) ist Vertrauen in sichere digitale Kommunikation essenziell. Werden staatliche Stellen ermächtigt, technische Schutzmechanismen gezielt zu unterlaufen, entsteht ein strukturelles Misstrauen gegenüber digitalen Diensten.

Aus Sicht des eco ist zudem die Verhältnismäßigkeit fraglich. Aktuelle Zahlen zeigen, dass der tatsächliche Einsatz von Staatstrojanern auf wenige Dutzend Fälle pro Jahr begrenzt ist. Demgegenüber steht das Risiko für die Cybersicherheit von rund 90 Millionen Menschen und Unternehmen. Eine solche Relation lässt Zweifel aufkommen, ob mildere, technisch weniger invasive Mittel ausreichend geprüft und priorisiert wurden.

Notwendig wären stattdessen verbindliche Regeln zum staatlichen Schwachstellenmanagement, klare Transparenz- und Berichtspflichten sowie eine gesetzliche Priorisierung von IT-Sicherheit vor punktuellen Zugriffsinteressen. Diese Elemente fehlen im § 40 BPolG-E bislang.

3. Drohende Chatkontrolle

Besonders kritisch beurteilt eco die Gefahr, dass § 40 BPolG-E mittelbar den Weg für Formen der Chatkontrolle ebnet. Auch wenn der Entwurf formal keine anlasslose Massenüberwachung privater Kommunikation vorsieht, schafft er doch eine Infrastruktur, die genau dafür genutzt werden könnte. Die Debatten auf EU-Ebene zur CSAM-Verordnung zeigen, wie schnell aus punktuellen Eingriffsbefugnissen allgemeine Scan-Pflichten werden können.

Eine Aufweichung sicherer Verschlüsselung, sei es durch Client-Side-Scanning oder durch staatliche Zugriffe auf Endgeräte, ist nicht nur grundrechtswidrig und technisch fehlgeleitet, sondern auch sicherheitspolitisch gefährlich. Anlassloses oder breit angelegtes Scannen privater Kommunikation verletzt das Fernmeldegeheimnis und führt zu hohen Fehlerrisiken. Es schafft eine Infrastruktur zur Massenüberwachung, die weit über den ursprünglichen Zweck hinaus genutzt werden kann.

Zudem ist die Wirksamkeit solcher Ansätze begrenzt. Sie verhindern keinen laufenden Missbrauch, identifizieren kaum neue Täterkreise und binden erhebliche Ressourcen, die bei Prävention, Opferschutz und internationaler Strafverfolgung besser eingesetzt wären. Gerade für kleine und mittlere Anbieter digitaler Dienste drohen unverhältnismäßige technische und finanzielle Belastungen.

Über eco: Mit rund 1.000 Mitgliedsunternehmen ist eco (www.eco.de) der führende Verband der Internetwirtschaft in Europa. Seit 1995 gestaltet eco maßgeblich das Internet, fördert neue Technologien, schafft Rahmenbedingungen und vertritt die Interessen seiner Mitglieder gegenüber der Politik und in internationalen Gremien. eco hat Standorte in Köln, Berlin und Brüssel. eco setzt sich in seiner Arbeit vorrangig für ein leistungsfähiges, zuverlässiges und vertrauenswürdiges Ökosystem digitaler Infrastrukturen und Dienste ein.