VERBAND DER INTERNETWIRTSCHAFT E.V.

STELLUNGNAHME

zum Referentenentwurf des Bundesministeriums des Innern und für Heimat über den Gesetzesentwurf zur Neustrukturierung des Bundespolizeigesetzes und Änderung anderer Gesetze

Berlin, 08.06.2023

Mit der Novelle des Bundespolizeigesetzes (BPolG-E) soll für die Arbeit der Bundespolizei eine neue Rechtsgrundlage geschaffen werden, die eine umfassende Überarbeitung der Berechtigungen der Bundespolizei für den Einsatz ihrer Fähigkeiten und Kapazitäten unter Berücksichtigung des Urteils des Bundesverfassungsgerichts (BVerfG) von 2016 schaffen.

eco – Verband der Internetwirtschaft sieht jedoch insbesondere im Bereich der Telekommunikationsüberwachung durch den BPolG-E zentrale Fragestellungen aufgeworfen, die für die Internetwirtschaft relevant sind. Aus Sicht der Internetwirtschaft ist Vertrauen in digitale Technologien ein zentraler Faktor für die Digitalisierung, der in weiten Teilen durch die Vertraulichkeit der Kommunikation begründet wird. Das Fernmeldegeheimnis ist daher ein durch das Grundgesetz mit besonderem Schutz beachtetes Gut, welches Heute primär im Rahmen der Nutzung digitaler Dienste abgebildet wird. Staatliche Überwachungsbefugnisse und Eingriffe in die vertrauliche Kommunikation von Bürger:innen stehen daher in einem Spannungsverhältnis zum Grundgesetz und können das Vertrauen in digitale Technologien untergraben. Gleichzeitig erkennt eco an, dass Erkenntnisse aus digitaler Kommunikation einen wichtigen Beitrag zur Aufklärung von Verbrechen leisten können. Zur Auflösung dieses Konflikts hinterfragt eco die Aktivitäten in diesem Bereich kritisch. Eingriffe in das Fernmeldegeheimnis bedürfen eines besonderen Grundes und hoher rechtlicher Schranken. Dies gilt es auch bei der Novelle des BPolG zu berücksichtigen.

Im Einzelnen nimmt eco zu den nachstehenden Aspekten des BPolG wie folgt Stellung:

▪ Zu Paragraf 24 – Bestandsdatenauskunft

Der Paragraf 24 BPolG-E wurde im Vergleich zum Paragraf 22a des alten BPolG lediglich marginal überarbeitet. Die Klarstellungen beziehen sich darauf, dass eine Bestandsdatenauskunft nur bei solchen Telekommunikationsanbietern erfolgen kann, die diese geschäftsmäßig erbringen. Aus Sicht der Internetwirtschaft genügen die hier aufgeführten Gründe für die Rechtmäßigkeit der Bestandsdatenauskunft den Ansprüchen der Normenklarheit. Problematisch hingegen ist nach wie vor die Erfassung von Bestandsdaten von Telemediendiensten. Mit diesen ist es möglich, weitaus umfangreichere Erkenntnisse zu erlangen als mit einer

Bestandsdatenauskunft für einen nummerngebundenen Telekommunikationsdienst. Es bedarf daher einer Klarstellung, in welchem Umfang entsprechende Befugnisse für die jeweiligen Telemediendienste gelten sollen, beziehungsweise auf welche Datenarten sie sich beziehen (analog beispielsweise in §174 Abs. 1 TKG für Telekommunikationsdienste).

- **Zu Paragraf 25 – Erhebung von Verkehrs- und Nutzungsdaten**

Mit der Schaffung einer Rechtsgrundlage für die Erhebung von Verkehrs- und Nutzungsdaten durch die Neueinführung eines Paragrafen 25 im BPolG-E wird für die Internetwirtschaft prinzipiell mehr Klarheit darüber geschaffen, unter welchen Rahmenbedingungen welche Informationen durch die Bundespolizei erhoben werden dürfen. Analog zu den Regelungen in Paragraf 24 bleibt jedoch für den Komplex der Nutzungsdaten unklar, in welchem Umfang dies erfolgen kann und welche Abgrenzungen zu Inhaltsdaten bestehen sollen. Dies sollte in §25 Abs. 4 Nr. 3 sowie in §25 Abs. 5 Nr. 3 daher explizit als Teil des Umfangs der jeweiligen Maßnahme gefordert werden, da bei Telemediendiensten der ansonsten im täglichen Gebrauch von Anordnungen gegenüber Telekommunikationsdiensten übliche Passus der Ausleitung „aller sonstigen Daten“ überbordend wäre.

Unklar bleibt bei diesem Passus zudem, wie genau die von den Betreibern digitaler Dienste zu beauskunftenden Verkehrsdaten erhoben werden sollen bzw. wie diese an die berechtigte Stelle ausgeleitet werden. Aus Sicht der Internetwirtschaft wäre hier eine weitere Präzisierung z.B. im Rahmen einer Verordnungsermächtigung analog zu den Regelungen der TR-TKÜV erforderlich, so dass für Betreiber digitaler Dienste keine Sicherheitsrisiken durch die Übertragung entstehen. Die Herausgabe entsprechender Informationen darf unter keinen Umständen zu einer Kompromittierung von deren Sicherheit auf dem Transportweg oder bei der Speicherung bei den Ermittlungsbehörden führen.

- **Zu Paragraf 38 – Überwachung der Telekommunikation**

Die in Paragraf 38 BPolG-E dargelegte Rechtsgrundlage zur Überwachung der Telekommunikation wirft aus der Sicht von eco Fragen auf. Die dargelegten Überwachungsziele legen analog zum Bundeskriminalamtgesetz umfassenden Eingriffe in das Fernmeldegeheimnis und in den Bereich der persönlichen Lebensführung nahe. Grundsätzlich sollte im Gesetzgebungsverlauf erörtert werden, ob die Aufgreifschwellen für die Überwachung der Telekommunikation hinreichend präzise formuliert sind, um ein Untergraben des Vertrauens in den Einsatz digitaler Technologien zu vermeiden.

- **Zu Paragraf 39 – Identifizierung und Lokalisierung von Mobilfunkkarten und -endgeräten**

Mit Paragraf 39 BPolG-E wird eine neue Rechtsgrundlage für die Bestimmung des Standortes von Mobilfunkkarten und -geräten durch die Bundespolizei geschaffen.. Als Voraussetzung sollen die selben Bestimmungen für den Einsatz der Maßnahmen wie in Paragraf 38 BPolG-E gelten. Aus Sicht der Internetwirtschaft sind gerade bei sensiblen Daten, die dazu geeignet sind, Profile von Personen zu bilden und so umfassende Einblicke in ihre private Lebensgestaltung zu gewinnen, möglichst konkret gefasste Aufgreifschwellen zu definieren, um durch unklare Formulierung einen ausufernden Einsatz entsprechender Maßnahmen zu vermeiden. Da auch Betreiber von Telekommunikationsdiensten in diese Maßnahmen mit einbezogen werden sollen, sind die weiteren Modalitäten einer entsprechenden Abfrage weiter zu konkretisieren.

Zwar geht die vorliegende Regelung augenscheinlich davon aus, dass Maßnahmen nur zulässig sein sollten, wenn die Überwachung nach Paragraf 38 grundsätzlich möglich wäre. Dies unterstellt aber eine gerichtliche Genehmigung aus § 38 Abs. 2. Das Verhältnis von Anordnungen nach § 39 in Korrelation mit Verbindungsdaten und die hieraus ableitbaren Erkenntnisse, welche beispielsweise durch den BND als „wichtiger als der Inhalt der Kommunikation selbst“ bezeichnet werden, sind hingegen nicht berücksichtigt. Hier sollte in §39 Abs. 3 mindestens neben § 38 Abs. 2, Abs. 4 und Abs. 5 auch Abs. 3 mit der sich daraus ergebenden Begründung (Abs. 3, Nr. 3, 4. und 5.) aufgenommen werden, um eine problematische Kollusion von verschiedenen Formen der Datenerhebung zu vermeiden.

- **Zu Paragraf 42 – Zweckbindung, Grundsatz der hypothetischen Datenneuerhebung**

Aus dem neuen Paragraf 42 Abs. 2 BPolG-E soll eine Änderung der Verarbeitungsgrundlage von durch die Bundespolizei selbst oder durch eine andere öffentliche oder nichtöffentlich Stelle erhobenen Daten unter dem Oberbegriff einer „hypothetischen Datenneuerhebung“ zulässig sein. Diese Regelung umfasst somit alle personenbezogenen Daten, unabhängig davon, unter welcher Rechtsgrundlage sie von welcher Stelle zu welchem Zweck erhoben wurden. eco sieht die Zulässigkeit der Änderung kritisch, da diese auch Zufallsfunde oder Weiterleitungen von Kommunikationsinhalten umfasst.

Abgrenzungen wie beispielsweise eine Beschränkung auf Kommunikationsdaten oder ein Verbot der Nutzung von Daten bestehen nicht oder greifen nicht durch. So ist der Versuch einer Beschränkung des Datenzugriffs, wie er in Paragraf 42 Abs. 3 BPolG-E unternommen wird, für alle durch privatwirtschaftliche Unternehmen im Kundenauftrag erhobenen und weitergeleiteten Daten wirkungslos.

- **Zusammenfassung und Fazit:**

Mit dem vorliegenden BPolG-E werden zahlreiche, im Vorfeld aufgeworfene Kritikpunkte wie der Einsatz von Trojanern und der Quellen-Telekommunikationsüberwachung werden nicht mehr explizit im BPolG-E aufgegriffen. Für das BPolG-E gilt insbesondere, dass es sich bei der Bundespolizei um eine Polizei des Bundes mit begrenztem Aufgabenspektrum (z.B. Schutz von Bahnhöfen, Flughäfen und der Landesgrenze) handelt. eco befürwortet die Entscheidung des Gesetzgebers. Denn mit dem Einsatz von Trojanern und der Quellen-TKÜ sind erhebliche Risiken verbunden. Staatstrojaner sind weder durch die sie einsetzenden Sicherheitsbehörden beherrschbar noch durch deren Kontrollorgane bzw. Gerichte kontrollierbar. Trojaner schwächen die IT-Sicherheit massiv, da sie in der Regel unter Ausnutzung von Lücken in Massensoftware eingesetzt werden. Dazu müssten solche Lücken geheim gehalten werden, anstatt sie unverzüglich zu schließen. Dies widerspricht der Schutzpflicht des Staates und gefährdet die Sicherheit informationstechnischer Systeme. Es setzt Bürger, Unternehmen und Staat einem unkalkulierbaren Sicherheitsrisiko aus. Derartige Spähsoftware kann nicht zuletzt erheblichen Schaden an Netzen und Diensten der Unternehmen anrichten und das Vertrauen in die Digitalisierung untergraben.

Problematisch bleiben indes die Aufgreifschwellen der in den §§ 25, 38 und 39 aufgeführten Befugnisse für Maßnahmen der Telekommunikationsüberwachung. Auch die Erhebungsfiktion gem. § 42 für personenbezogene Daten bedarf einer gründlichen Überprüfung. Die Internetwirtschaft sieht in den für Ihre Arbeit relevanten Teilen des Gesetzes Konkretisierungsbedarf, was die Rechtsgrundlagen für entsprechende Eingriffe anbetrifft. Weitere Schädigung des Vertrauens von Bürger:innen in digitale Dienste durch staatliche Stellen dürfen nicht eintreten. Dies würde letzten Endes auch das Vertrauen in die Demokratie untergraben. eco plädiert daher dafür, an den genannten Stellen weiter zu präzisieren und so Rechtsklarheit für Ermittlungsbehörden, Diensteanbieter und Bürger:innen herzustellen.