WIR GESTALTEN DAS INTERNET.

Verband der deutschen Internetwirtschaft e.V.

Auf dem Prüfstand: Gesetzesentwurf zur Vorratsdatenspeicherung

Stand: 20.05.2015

Das Bundesministerium für Justiz und Verbraucherschutz (BMJV) hat am 15. Mai einen Referentenentwurf für ein Gesetz zur Vorratsdatenspeicherung vorgelegt. Der Gesetzesentwurf setzt die im April 2015 vorgestellten Leitlinien zur Einführung einer Speicherpflicht und Höchstspeicherfrist für Verkehrsdaten um. Gesetzesentwurf und Leitlinien werden als „Kompromiss“ in der insbesondere seit den Urteilen von BVerfG und EuGH politisch hochumstrittenen Debatte um die Wiedereinführung der Vorratsdatenspeicherung präsentiert. Das Gesetz soll noch vor der Sommerpause in Kraft treten. Sowohl Leitlinien als auch Gesetzesentwurf werfen im Detail viele rechtliche und technische Fragen auf, die der Gesetzgeber auflösen muss.

1. Ist die geplante Regelung verfassungsgemäß?

Das Bundesverfassungsgericht (BVerfG) hat in seinem Urteil vom März 2010 die anlasslose Sammlung von Verkehrsdaten zum Zwecke des Zugriffs durch Strafverfolgungsbehörden (Vorratsdatenspeicherung) zwar nicht als grundsätzlich verfassungswidrig eingestuft. Gleichwohl setzt das Urteil dem Gesetzgeber angesichts der Schwere der Grundrechtseingriffe enge Grenzen für die Ausgestaltung einer solchen Regelung. Der Gesetzesentwurf zeigt, dass sich das BMJV im Rahmen des vom BVerfG vorgegebenen rechtlichen Spielraums bewegen möchte. Speicherdauer und Umfang der gespeicherten Daten fallen wesentlich geringer aus als in § 113a TKG a.F., der vom BVerfG 2010 für verfassungswidrig erklärt wurde. Gleichzeitig sieht der Gesetzesentwurf aber weiterhin vor, die Daten aller Nutzer elektronischer Kommunikation „anlasslos“, d.h. pauschal und ohne Verdacht auf die Verwicklung in eine Straftat, zu speichern. Dies ist problematisch, weil es gegen das Grundprinzip der Unschuldsvermutung verstößt und einen massiven Eingriff in die Privatsphäre darstellt.

Das Bundesverfassungsgericht stellt in seinem Urteil vom 2. März 2010 hohe Anforderungen an eine verfassungsgemäße Regelung zur Vorratsdatenspeicherung. Unter anderem fordern die Richter eine asymmetrische Verschlüsselung des gesamten Datenbestands. Das Bundesjustizministerium fordert in seinen Leitlinien und im Gesetzesentwurf lediglich den „Einsatz eines besonders sicheren Verschlüsselungsverfahrens“. Sollte der Gesetzestext derart vage bleiben, ergäben sich demnach verfassungsrechtliche Probleme. Eine asymmetrische Verschlüsselungstechnik, die gleichzeitig praktikabel für die Verwaltung der zu erwartenden hohen Datenaufkommen ist, existiert allerdings derzeit nicht.

eco
Verband der deutschen
Internetwirtschaft e.V.
Lichtstraße 43h
50825 Köln

Tel.: +49 (0) 221-70 00 48-0
Fax: +49 (0) 221-70 00 48-111
E-Mail: info@eco.de
www.eco.de

Hauptstadtbüro
Französische Straße 48
10117 Berlin
Tel.: +49 (0) 30-20 21 567-0
Fax: +49 (0) 30-20 21 567-11
E-Mail: berlin@eco.de

Vorstand:
Prof. Michael Rotert
(Vorsitzender)
RA Oliver J. Süme
(Stellv. Vorsitzender)
Thomas von Bülow
Felix Höger
Klaus Landefeld
Geschäftsführer:
Harald A. Summa

Bankverbindung:
Sparkasse KölnBonn
Kto.-Nr. 129 629 73
BLZ 370 501 98
SWIFT CODE:
COLSDE33
IBAN:
DE29 3705 0198 0012 9629 73

Deutsche Bank Köln
Kto.-Nr. 195 1474
BLZ 370 700 60

Vereinsregister Köln 14478
VAT-ID DE 182676944

2. Welche Herausforderungen ergeben sich aus rechtlicher und technischer Sicht mit der neuen Regelung zur Speicherung von IP-Adressen

Die individuelle Signatur jedes Internetanschlusses kann heute nicht mehr ohne Weiteres einem bestimmten Nutzer zugeordnet werden. Bei den Internetdienst-anbietern hat die Knappheit von IPv4-Adressen dazu geführt, dass hinter einer öffentlichen IP-Adresse ein eigener IP-Adressraum aufgebaut worden ist. Das heißt, eine IP-Adresse wird für mehrere Geräte genutzt. Um einen Nutzer eindeutig zu identifizieren, braucht die Strafverfolgungsbehörde also nicht nur die IP-Adresse, sondern auch den sogenannten Port, über den sich der Nutzer verbunden hat sowie einen hochgenauen Zeitstempel. Das bedeutet nicht nur deutlichen Mehraufwand für den Internetdienstanbieter (derzeit wird dieses Merkmal nur selten gespeichert, da es für die Abrechnung nicht benötigt wird), insgesamt wird auch die Zuordnung zum User sehr viel schwieriger. Der Provider muss letztendlich aufzeichnen welche Internetverbindung von wann bis wann welchen Port mit welcher IP-Adresse (intern bzw. auch extern) genutzt hat. Das heißt, die Anbieter bauen damit eine Datenbank über sämtliche Kommunikationsverbindungen auf, deren Auswertung umfangreiche Nutzerprofile ergeben würde. Dies verstößt das Grundgesetz und könnte auch Begehrlichkeiten beispielsweise bei ausländischen Geheim- und Spionagediensten wecken.

3. Wie wird das Berufsträgergeheimnis geschützt?

Daten von telefonischen Seelsorgediensten sollen grundsätzlich von der Speicherung ausgenommen sein, während Daten von Berufsgeheimnisträgern wie Ärzten, Anwälten, Abgeordneten und Journalisten zwar gespeichert - aber nicht abgerufen werden dürfen. Unklar ist, wie diese Regelung umgesetzt werden soll. Bislang werden Berufsstand oder die Tätigkeit von Nutzern nicht von den Internet- und Telekommunikationsanbieter erfasst. Das heißt, entweder werden die Daten von Berufsgeheimnisträgern automatisch mit abgerufen (und dann ggf. erst von den zuständigen Strafverfolgungsbehörden nach Prüfung aussortiert), oder die Unternehmen müssen eine entsprechende Datenbank über Berufsgeheimnisträger aufbauen, die politisch nicht gewünscht ist.

4. Welche wirtschaftlichen Folgen ergeben sich für Internet- und Telekommunikationsunternehmen?

Für die verpflichteten Unternehmen wird sich der Aufwand für die Implementierung der Speicherverpflichtung im Vergleich zur alten Regelung noch erhöhen. Denn um den Vorgaben des BVerfG zu entsprechen, werden

den Unternehmen hohe Anforderungen, insbesondere für den Umgang mit den gespeicherten Daten, auferlegt.

Ein Mehraufwand bei den TK-Unternehmen könnte dabei:

- durch die Umsetzung der Verpflichtung zur Differenzierung der Speicherfristen von Standortdaten (Mobilfunk) und den übrigen Verkehrsdaten (Rufnummer, Zeitpunkt und Dauer des Anrufs, IP-Adressen mit Zeitpunkt und Dauer der Vergabe, Anschlusskennung sowie zugewiesene Benutzerkennung),
- durch Verpflichtung zur Gewährleistung der Sicherheit der Daten (besonders gesichertes Verschlüsselungsverfahren, Speicherung in gesonderten Speichereinrichtungen mit hohem Schutz vor Angriffen, revisionssichere Protokollierung des Zugriffs unter Gewährleistung des Vier-Augen-Prinzips),
- sowie durch strenge Löschpflichten entstehen.

Die Systeme zur früheren Vorratsdatenspeicherung sind abgeschaltet und können für die neue Regelung schon aufgrund der neuen technischen Anforderungen nicht mehr verwendet werden. Alle betroffenen Provider müssen also neue Infrastrukturen schaffen, die deutlich komplexer als die bisherigen Systeme sind. Die Kosten könnten sich nach ersten Schätzungen von eco auf rund 600 Millionen Euro belaufen.

5. Was bedeutet die geplante Regelung für die Rechts- und Innovationssicherheit der betroffenen Unternehmen?

Fraglich bleibt, wie sich das Vorhaben im weiteren Gesetzgebungsverfahren entwickeln wird, etwa in Bezug auf den Umfang der zu speichernden Daten. Schon jetzt fordern Politiker längere Speicherfristen oder die Einbeziehung von Messenger-Diensten bzw. sogenannten „Over-the-Top“-Angeboten wie WhatsApp in die Speicherverpflichtung. Gegner der anlasslosen Speicherung haben bereits Klagen gegen die geplanten Regelungen angekündigt. Die betroffenen Unternehmen werden daher erst nach einem erneuten Verfahren vor dem BVerfG, dass jetzt schon absehbar ist, endgültige rechtliche Klarheit über die Verfassungsmäßigkeit bekommen. Dies erschwert rechtssichere Entscheidungen im Hinblick auf die Implementierung der Speicherinfrastruktur. Der Gesetzesentwurf sieht aktuell eine sehr kurze Umsetzungsfrist von sechs Monaten vor. Hier muss die Bundesregierung etwa durch eine Verlängerung der Umsetzungsfristen sicherstellen, dass die Unternehmen nicht wieder überflüssige Investitionen tätigen.

6. Können die Unternehmen die in den Leitlinien geforderten Sicherheitsanforderungen realisieren?

Die in den Leitlinien formulierten Sicherheitsanforderungen, die die betroffenen Unternehmen erfüllen sollen, sind teilweise noch sehr vage formuliert und werfen Fragen hinsichtlich ihrer technischen Umsetzbarkeit auf. Die Maßnahmen umfassen insbesondere:

1. den Einsatz eines besonders sicheren Verschlüsselungsverfahrens

Es ist unklar, wie die Vorgaben des BVerfG in die Praxis umgesetzt werden können, z.B. ist jeder Index in eine verschlüsselte Datei von Metadaten selbst wieder eine Metadatensammlung. Völlig unklar ist, wie die Vorgabe für Massenabfragen wie z.B. die Funkzellenabfrage realisiert werden soll.

2. die Speicherung mit einem hohen Schutz vor dem Zugriff aus dem Internet auf vom Internet entkoppelten Rechnern

Diese Anforderung ist faktisch nicht umsetzbar, da alle Systeme im Internet . vernetzt sind, die Daten werden in Systemen im Netz erhoben, werden durch ein einheitliches Netz transportiert und wieder in Systemen verarbeitet, welche ebenfalls online sind. Auch das VPN der Bedarfsträger ist ein internetbasiertes System und muss mit dem Auskunftssystem zwangsläufig verbunden werden.

3. die notwendige Mitwirkung von mindestens zwei Personen beim Zugriff auf die Daten, die dazu durch den Verpflichteten besonders ermächtigt worden sind

Diese Anforderung ist für die Masse der kleine Provider, welche nur eine Handvoll Mitarbeiter beschäftigen, faktisch nicht umsetzbar.

Forderungen der deutschen Internetwirtschaft

1. Rechtssicherheit für Unternehmen gewährleisten

Mit der geplanten Wiedereinführung der Vorratsdatenspeicherung drohen erneut Investitions- und Rechtsunsicherheit für die betroffenen Unternehmen. Spätestens seit dem Urteil des Bundesverfassungsgericht von 2010 ist klar, dass eine verfassungskonforme Umsetzung der Vorratsdatenspeicherung in Deutschland kaum möglich ist. Mit dem geplanten Gesetz ist ein neues Verfahren vor dem Bundesverfassungsgericht praktisch vorprogrammiert. Es ist Aufgabe des Gesetzgebers, bei einem erneuten Gesetzgebungsprozess zur Vorratsdaten-speicherung beispielsweise durch lange Umsetzungsfristen sicherzustellen, dass die betroffenen Internet- und Telekommunikationsunter-

nehmen nicht wieder auf hohen Kosten zur Umsetzung einer wertlosen gesetzlichen Regelung sitzenbleiben.

2. Vorratsdatenspeicherung aufgeben und Vertrauen schaffen

eco lehnt die anlass- und verdachtsunabhängige Vorratsdatenspeicherung aus grundsätzlichen Erwägungen ab. Die anlasslose Speicherung sämtlicher Verkehrsdaten der Nutzer elektronischer Kommunikation ist weder verhältnismäßig noch gerechtfertigt. Die mit der Speicherung verbundenen Eingriffe in die Grundrechte der Bürger und Unternehmen stehen in keinem Verhältnis zum behaupteten, aber nicht belegten Effektivitätsgewinn bei der Strafverfolgung.
Zahlreiche zivilgesellschaftliche und wirtschaftliche Errungenschaften der letzten Jahre basieren auf dem Internet. Sein Erfolg basiert auf dem Vertrauen der Nutzer in elektronische Kommunikationstechnologien, das durch die jüngsten Enthüllungen um die Abhörpraktiken von Geheimdiensten erschüttert wurde. Es ist auch Aufgabe der Bundesregierung, dieses Vertrauen ins Internet wiederherzustellen. Eine Wiedereinführung der Vorratsdatenspeicherung ist hierzu sicher nicht geeignet.

3. Entschädigungsregelung für betroffene Unternehmen

Anbieter elektronischer Kommunikation sehen sich immer weitergehenden und umfassenden regulatorischen Verpflichtungen, etwa in der IT-Sicherheit, ausgesetzt und sind zusätzlich angehalten durch eigene Investitionen die Grundlagen für die zukünftige digitale Infrastruktur zu sichern. Alle weiteren Verpflichtungen werden sich negativ auf die Investitionsmöglichkeiten der betroffenen Unternehmen auswirken. Der Gesetzgeber sollte daher den Rahmen des wirtschaftlich Zumutbaren in seine Erwägungen miteinfließen lassen. eco fordert klare und konkrete Entschädigungsregelungen, die sich an realistischen ökonomischen Parametern orientieren und grundsätzlich für alle betroffenen Unternehmen gelten

4. Schutzlücken und Effektivität prüfen und belegen

Ob und inwieweit tatsächlich Schutzlücken in Bereich der Strafverfolgung vorliegen, ist empirisch bislang nicht belegt. Der positive Effekt der Vorratsdatenspeicherung für die Verhinderung oder Verfolgung von Straftaten ist ebenfalls nicht belegt. Wir fordern die Bundesregierung deshalb dazu auf, zunächst einen Nachweis für den Nutzen und die Effektivität der Vorratsdatenspeicherung zu erbringen, bevor ein erneutes gesetzliches Verfahren eröffnet wird.