

**Stellungnahme des Arbeitskreises  
Vorratsdatenspeicherung zum Entwurf eines  
Gesetzes zur Erhöhung der Sicherheit  
informationstechnischer Systeme (IT-  
Sicherheitsgesetz), BT-Drucksache 18/4096**



Zu den Auswirkungen des Gesetzentwurfs auf den Datenschutz bei Telekommunikations- und Internetdiensten nehmen wir wie folgt Stellung:

**1. Der Arbeitskreis Vorratsdatenspeicherung begrüßt, dass der Regierungsentwurf nicht mehr vorsieht, unter dem Deckmantel der „Störungsbeseitigung“ eine Ermächtigung zur verdachtslosen Aufzeichnung des Surfverhaltens im Internet in das Telemediengesetz aufzunehmen.** Dabei muss es auch bleiben. Zur Begründung verweisen wir auf unsere Pressemitteilung vom 20.08.2014<sup>1</sup> und auf unsere Stellungnahme vom 7. Mai 2009 an den Innenausschuss<sup>2</sup>.

**2. Der Arbeitskreis Vorratsdatenspeicherung fordert – wie auch der Bundesrat –, die im Gesetzentwurf vorgesehene Ausweitung des § 100 Abs. 1 TKG (Verkehrsdatenspeicherung zur „Störungserkennung“) zu streichen. Umgekehrt bedarf die Vorschrift dringend einer Eingrenzung, um eine anlasslose Vorratsdatenspeicherung auszuschließen.**

De facto speichern viele Anbieter unter Berufung auf § 100 Abs. 1 TKG tage- oder wochenlang Informationen über alle Telefonverbindungen, Standorte und Internetverbindungen ihrer Kunden auf Vorrat. So wird bis zu sechs Monate lang gespeichert, von wem man angerufen wurde, obwohl die Anrufannahme in aller Regel nicht kostenpflichtig ist. Die Mobilfunk-Netzbetreiber zeichnen außerdem die Position der Handynutzer und die Geräteerkennung auf, ohne dass dies abrechnungsrelevant wäre. Viele Internetzugangsanbieter praktizieren eine IP-Vorratsdatenspeicherung.

---

1 „Bundesinnenminister plant verdachtslose Aufzeichnung des Surfverhaltens im Internet“, <http://www.vorratsdatenspeicherung.de/content/view/748/79/lang.de/>

2 Stellungnahme zum Entwurf eines „Gesetzes zur Stärkung der Sicherheit in der Informationstechnik des Bundes“, [http://webarchiv.bundestag.de/archive/2009/0626/ausschuesse/a04/anhoerungen/Anhoerung\\_21/Stellungnahmen\\_SV/Stellungnahme\\_07.pdf](http://webarchiv.bundestag.de/archive/2009/0626/ausschuesse/a04/anhoerungen/Anhoerung_21/Stellungnahmen_SV/Stellungnahme_07.pdf)

Auf dieser Grundlage wirft der Arbeitskreis Vorratsdatenspeicherung der deutschen Telekommunikationsbranche vor, systematisch betrieblich nicht erforderliche Informationen über die Telekommunikation aufzuzeichnen und damit eine verbotene Vorratsdatenspeicherung zu praktizieren.<sup>3</sup> Dass auf diese Weise ein großer Teil der verfassungswidrigen staatlich angeordneten Vorratsdatenspeicherung (§ 113 a TKG a. F.) von den Telekommunikationsunternehmen unter anderem Vorzeichen fortgesetzt wird, ist ein nicht akzeptabel.

Die betrieblichen Vorratsdaten werden tatsächlich nicht zur „Störungsbeseitigung“, sondern unter Durchbrechung der Zweckbindung genutzt, um Internet-Anschlussinhaber wegen angeblicher Urheberrechtsverletzungen millionenfach abzumahnen (über 700.000 IP-Auskünfte alleine der Deutschen Telekom zur Verfolgung von Urheberrechtsverletzungen im Jahr 2014) und um tausendfach Auskünfte an Eingriffsbehörden zu erteilen (z.B. Funkzellenabfragen, Bestandsdatenauskünfte). Folge sind immer wieder auch polizeiliche Ermittlungen gegen Unschuldige. Die Vorratsspeicherung von Kommunikations- und Bewegungsdaten durch die deutsche Telekommunikationsbranche bringt Millionen von Menschen in die Gefahr strafrechtlicher Ermittlungen, weil sie zufällig am falschen Ort waren oder mit der falschen Person telefoniert haben (Beispiel: Funkzellenabfragen). Die Datenberge schaffen auch die permanente Gefahr von Datenpannen, Datenverkauf<sup>4</sup> und einer Aufdeckung der Quellen von Journalisten.<sup>5</sup> Nur nicht gespeicherte Daten sind sichere Daten. Die „freiwillige Vorratsdatenspeicherung“ der Telekommunikationsanbieter ist für die Freiheit der Telekommunikation und die Sicherheit unserer Daten genauso schädlich wie eine staatlich erzwungene Vorratsdatenspeicherung; sie unterliegt zudem nicht den Auflagen einer staatlich angeordneten Vorratsdatenspeicherung betreffend Datensicherheit, Datenspeicherung und Datenverwendung.

Zur Beseitigung von Störungen ist eine dauerhafte rein vorsorgliche Verkehrsdatenverarbeitung allenfalls während der Dauer einer Verbindung zu rechtfertigen, um etwa aufgetretene Störungen bzw. Fehler protokollieren zu können, nicht dagegen eine Protokollierung auch der ohne Störungen und Fehler abgewickelten Verbindungen.<sup>6</sup> Ein nur in einzelnen Fällen bestehendes Speicherinteresse rechtfertigt nicht die generelle Speicherung eines Datentyps bei allen Verbindungen.<sup>7</sup> Gleichwohl wird § 100 Abs. 1 TKG verbreitet als Ermächtigung zur einer anlasslosen Vorratsdatenspeicherung ausgelegt und so angewandt.

3 Anzeige des AK Vorrat bei der Bundesnetzagentur,

[http://www.vorratsdatenspeicherung.de/images/anzeige\\_verkehrsdatenspeicherung\\_anon.pdf](http://www.vorratsdatenspeicherung.de/images/anzeige_verkehrsdatenspeicherung_anon.pdf)

4 Diebe klauten 17 Millionen T-Mobile-Kundendatensätze,

<http://www.spiegel.de/wirtschaft/telekom-skandal-diebe-klauten-17-millionen-t-mobile-kundendatensaetze-a-581938.html>

5 Telekom-Chef Obermann "zutiefst erschüttert" über Spionage-Skandal,

<http://www.spiegel.de/wirtschaft/management-bespitzelung-telekom-chef-obermann-zutiefst-erschuettert-ueber-spionage-skandal-a-555162.html>

6 Königshofen/Ulmer, Datenschutzhandbuch Telekommunikation, 2006, § 100 TKG, Rdnr. 9; Arndt/Fetzer, in: Berliner TKG-Kommentar, § 100 TKG Rdnr. 8; Wittern, in: Beck'scher TKG-Kommentar, § 100 TKG, Rdnr. 7; Breyer, MMR 2011, 578 m. w. Nachw.

7 Vgl. BVerfGK 9, 399 = NJW 2007, 3055 Rdnr. 31.

Der Regierungsentwurf eines IT-Sicherheitsgesetzes lässt diese Mängel des § 100 Abs. 1 TKG nicht nur fortbestehen, er soll die darin vorgesehene Datenspeicherung sogar noch ausweiten – mit nicht absehbaren Folgen. Künftig sollen hochsensible Verbindungs- und Bewegungsdaten schon dann gespeichert werden dürfen, wenn Maßnahmen Verfügbarkeitsbeeinträchtigungen oder unerlaubte Zugriffe nach sich ziehen „können“ (Artikel 5 Nr. 2 des Gesetzentwurfs). Ein konkreter Anlass oder eine Beschränkung auf den Einzelfall, eine maximale Aufbewahrungsdauer oder Benachrichtigung der Nutzer, ein Richtervorbehalt oder eine strikte Zweckbindung der Daten ist nicht vorgesehen. Die erlaubte „Verwendung“ von Telekommunikationsdaten würde sogar deren Weitergabe an Dritte ermöglichen.

Bei der damit einzuführenden Speicherbefugnis handelt es sich – so auch der Bundesrat – im Kern um eine weitreichende Vorratsdatenspeicherung, die zu keiner Verbesserung der Informationssicherheit führt, sondern umgekehrt zu einer weiteren Gefahrenquelle werden könnte. Schadsoftware oder Spam rechtfertigen es nicht, das Recht auf Anonymität im Netz generell zu zerstören, anstatt anlassbezogen gegen Verursacher vorzugehen.

Die vage neue Formulierung dürfte mit dem Bestimmtheitsgebot unvereinbar sein. Sie dürfte auch unverhältnismäßig sein, denn ihr fehlt jegliche Höchstfrist und wirksame Zweckbindung der Daten. Außerdem dürfte sie mit der EU-Richtlinie 2002/58 über den Datenschutz in der Telekommunikation unvereinbar sein, die vom Grundsatz der Verkehrsdatenlöschung mit Verbindungsende nur sehr enge Ausnahmen zulässt (siehe Erwägungsgrund 29).

§ 100 Abs. 1 TKG verfehlt in alter wie geplanter neuer Fassung die verfassungsrechtlichen Anforderungen bei weitem:<sup>8</sup> Danach darf eine automatisierte Datenerfassung „nicht anlasslos erfolgen oder flächendeckend durchgeführt werden“. Begriffe wie „erforderlich“ oder „sachdienlich“ stellen keine hinreichende Eingriffsschwelle dar.<sup>9</sup> Das „strikte Verbot der Sammlung personenbezogener Daten auf Vorrat“ ist zu gewährleisten.<sup>10</sup> Eine „enge und konkrete Zweckbindung“ muss gesetzlich angeordnet werden.<sup>11</sup> Dem Bundesverfassungsgericht liegt aktuell eine Verfassungsbeschwerde wegen § 100 TKG vor.<sup>12</sup>

---

8 Näher Breyer, RDV 2004, 147 und MMR 2011, 573.

9 BVerfG, MMR 2008, 308, 308; BVerfG, NVwZ 2007, 688, 691.

10 BVerfG, MMR 2006, 531.

11 BVerfGE 100, 313, 385 f.

12 <http://www.ndr.de/nachrichten/Klage-gegen-Daten-Sammelwut-der-Telekom,telekom236.html>

**Bitte setzen Sie sich dafür ein, dass die Ausweitung der Vorratsdatenspeicherung zur „Störungserkennung“ unterbleibt und die bestehende Regelung des § 100 Abs. 1 TKG beschränkt wird auf eine Datenspeicherung „im Einzelfall“. Formuliert werden könnte die Vorschrift beispielsweise wie folgt:**

*„Liegen dem Diensteanbieter im Einzelfall zu dokumentierende tatsächliche Anhaltspunkte vor, dass bestimmte Nutzer seine zur Bereitstellung seines Dienstes genutzten technischen Einrichtungen stören, darf er die Verkehrsdaten dieser Nutzer über das Ende der Verbindung hinaus nur erheben, speichern und nutzen, soweit dies zur Beseitigung der Störung erforderlich ist. Eine Verwendung der Daten für andere Zwecke ist unzulässig. Die Maßnahme kann auch durchgeführt werden, wenn Dritte unvermeidbar mitbetroffen werden. Der Diensteanbieter hat die Daten unverzüglich zu löschen, wenn die Voraussetzungen nach Satz 1 nicht mehr vorliegen oder die Daten zur Störungsbeseitigung nicht mehr benötigt werden. Nach Satz 3 gespeicherte Daten sind spätestens nach 24 Stunden zu löschen. Der betroffene Nutzer ist zu unterrichten, sobald dies ohne Gefährdung des mit der Maßnahme verfolgten Zweckes möglich ist.“*

Die Formulierung würde dafür Sorge tragen, dass eine Protokollierung nicht permanent, generell und ohne Anlass erfolgt, sondern nur wenn „im Einzelfall“ tatsächlich konkrete Anhaltspunkte für eine Störung durch bestimmte Nutzer eines Dienstes vorliegen. Die Weitergabe der Daten an Dritte wäre ausgeschlossen. Satz 2 des hier unterbreiteten Formulierungsvorschlags würde eine Verwendung der hochsensiblen Daten zu ganz anderen Zwecken ausschließen. Satz 3 würde dem Umstand Rechnung tragen, dass es aus technischen Gründen unvermeidbar sein kann, neben den mutmaßlichen Störern auch andere Nutzer mitzuerfassen. Jedoch müssen die Daten der mutmaßlichen Störer dann unverzüglich ermittelt und die übrigen Aufzeichnungen spätestens nach 24 Stunden gelöscht werden (Satz 5). Dies dient dem Schutz der überwältigenden Mehrheit rechtstreuer Nutzer, die keinen Anlass für eine Aufzeichnung ihres Telekommunikationsverhaltens gegeben haben.

04.05.2015

Anlagen:

- Fachbeitrag [„\(Un-\)Zulässigkeit einer anlasslosen, siebentägigen Vorratsdatenspeicherung nach geltendem Recht“](#), MMR 2011, 573
- Fachbeitrag [„Illegale Vorratsdatenspeicherung in der Telekommunikationsbranche?“](#), NJW Heft 1-2/2012, 14

### **Arbeitskreis Vorratsdatenspeicherung**

Der Arbeitskreis Vorratsdatenspeicherung (AK Vorrat) ist ein deutschlandweiter Zusammenschluss, der sich gegen die ausufernde Überwachung im Allgemeinen und gegen die Vollprotokollierung der Telekommunikation und anderer Verhaltensdaten im Besonderen einsetzt.

Homepage und Kontakt: <http://www.vorratsdatenspeicherung.de>

