Stellungnahme des Arbeitskreises Vorratsdatenspeicherung zu dem Gesetzentwurf des Bundesjustizministeriums zur Vorratsdatenspeicherung

Der Gesetzentwurf des Bundesjustizministeriums zur Sicherung vorhandener Verkehrsdaten und Gewährleistung von Bestandsdatenauskünften im Internet sieht neben der als Alternative zur einer Vorratsdatenspeicherung zu begrüßenden schnellen Sicherung von Verkehrsdaten („Quick Freeze“) vor, Internet-Zugangsanbieter zu verpflichten, flächendeckend und ohne jeden Anlass aufzuzeichnen, wer wann mit welcher IP-Adresse das Internet genutzt hat (§ 113a TKG-E). In Verbindung mit anderen Informationen, die Internet-Diensteanbieter wie Google, Twitter oder Youtube speichern, würde so unsere gesamte Internetnutzung nachvollziehbar werden, also potenziell jede unserer Eingaben, jeder unserer Klicks, jeder unserer Downloads, jeder unserer Beiträge/Posts im Netz.

Aus den folgenden Gründen lehnen wir eine solche generelle und undifferenzierte Vorratsspeicherung unserer Identität im Internet entschieden ab:

1. **Eine generelle und undifferenzierte Vorratsspeicherung unserer Identität im Internet hätte unzumutbare Auswirkungen:** Sie würde das Ende der Anonymität im Internet bedeuten. Sie würde es unmöglich machen, das Internet frei vom Risiko staatlicher Beobachtung (z.B. auch wegen eines falschen Verdachts), missbräuchlicher Offenlegung durch Mitarbeiter des Anbieters (Telekom-Skandal) und versehentlichen Datenverlustes (z.B. T-Mobile-Datenverlust) zu nutzen. Dadurch hätte eine IP-Vorratsdatenspeicherung unzumutbare Folgen, wo Menschen nur im Schutz der Anonymität überhaupt bereit sind, sich in einer Notsituation beraten und helfen zu lassen (z.B. Opfer und Täter von Gewalt- oder Sexualdelikten), ihre Meinung trotz öffentlichen Drucks zu äußern oder Missstände bekannt zu machen (Presseinformanten, anonyme Strafanzeigen).
2. **Eine generelle und undifferenzierte Vorratsspeicherung unserer Identität im Internet stünde außer jedem Verhältnis zu ihrem möglichen Nutzen:** Schon heute werden Internetdelikte außergewöhnlich häufig aufgeklärt; die Einführung einer sechsmonatigen IP-Vorratsdatenspeicherung erhöhte diese Aufklärungsquote nicht. Eine flächendeckende Vorratsdatenspeicherung droht die Aufklärung von Straftaten umgekehrt sogar zu erschweren, weil sie ein verstärktes Ausweichen auf Anonymisierungstechniken und andere

Kommunikationskanäle nach sich zieht und dadurch selbst gezielte, verdachtsabhängige Überwachungsmaßnahmen vereitelt, wo sie heute noch möglich sind.

3. **Eine generelle und undifferenzierte Vorratsspeicherung unserer Identität im Internet wäre eine nicht zu rechtfertigende und technikfeindliche Diskriminierung von Internetnutzern** gegenüber Menschen, die weiterhin anonym telefonisch (z.B. Flatrate), postalisch oder unmittelbar kommunizieren und sich Informationen verschaffen können. In immer mehr Fällen können Menschen Informationen nur noch über das Internet beschaffen und nur noch über das Internet kommunizieren.

4. **Eine generelle und undifferenzierte Vorratsspeicherung unserer Identität im Internet wäre ein Dammbruch mit weitreichenden Folgen:** Eine IP-Vorratsdatenspeicherung stellte den Präzedenzfall einer Aufgabe des rechtsstaatlichen Grundsatzes dar, wonach „grundrechtsrelevante Maßnahmen im Rahmen der Strafverfolgung oder der Gefahrenabwehr nur unter der Voraussetzung erfolgen, dass ein ausreichender Verdacht oder Anlass für diese Maßnahme gegeben ist“.[1] Wird eine generelle und undifferenzierte Vorratsdatenspeicherung erstmals als legitimes Mittel anerkannt, droht schrittweise (z.B. als Ergebnis von Koalitionsverhandlungen) nicht nur eine noch sehr viel weiter reichende Erfassung von Telekommunikationsdaten, sondern auch von Flugreisedaten und weiteren Daten über das alltägliche Verhalten vollkommen unbescholtener Bürgerinnen und Bürger. Das Prinzip einer rein prophylaktischen Erfassung des Verhaltens wahlloser Bürger führt in den Überwachungsstaat.

Die zur Begründung vorgebrachten Argumente rechtfertigen den Vorstoß nicht:

1. **Internetnutzer werden keineswegs „insbesondere zum Vorgehen gegen Kinderpornografie“ identifiziert, schon gar nicht in 80% der Fälle.** Eine solche Zahl kann allenfalls für das Bundeskriminalamt zutreffen, das sich speziell mit solchen Fällen befasst. Insgesamt betrachtet aber erfolgen nach einer Untersuchung des Max-Planck-Instituts für ausländisches und internationales Strafrecht weniger als 5% der staatlichen IP-Auskunftsersuchen wegen eines Verdachts des Austauschs kinder- oder jugendpornografischer Darstellungen über das Internet.[2] Auch nach der polizeilichen Kriminalstatistik betreffen weniger als 3% der polizeilichen Ermittlungen wegen Internetdelikten Fälle des Austauschs kinder- oder jugendpornografischer Darstellungen im Internet.[3] Solche Ermittlungen waren schon vor Inkrafttreten einer IP-Vorratsdatenspeicherung zum 01.01.2009 überdurchschnittlich erfolgreich (Aufklärungsrate 2008: 80%), sogar etwas erfolgreicher als nach Inkrafttreten einer IP-Vorratsdatenspeicherung am 01.01.2009 (Aufklärungsrate 2009: 76%).

2. **Eine generelle und undifferenzierte Vorratsspeicherung unserer Identität im Internet zieht durchaus das vom Bundesverfassungsgericht angesprochene diffus bedrohliche Gefühl des Beobachtetseins nach sich.** Sie erfasst nämlich Internetverbindungen, die unter der Erwartung von Anonymität hergestellt werden. 2009 gaben 46% der Bürger an, einen Internet-Anonymisierungsdienst zu nutzen oder nutzen zu wollen,[4] was sich nur durch den Wunsch erklären lässt, dem Risiko einer Aufdeckung der eigenen Internetnutzung zu entgehen.

3. **Eine generelle und undifferenzierte Vorratsspeicherung unserer Identität im Internet ermöglicht die Erstellung aussagekräftiger Persönlichkeits- und Bewegungsprofile praktisch jeden Bürgers in noch höherem Maße als Telefon-Verbindungsdaten**: Die Kenntnis der Identität eines Internetnutzers macht in Verbindung mit „Logfiles" der Diensteanbieter potenziell unsere gesamte Internetnutzung nachvollziehbar – nicht nur, mit wem wir in Verbindung standen (wie bei Telefon-Verbindungsdaten), sondern sogar die Inhalte, für die wir uns im Netz interessiert haben (gelesene Internetseiten, eingegebene Suchbegriffe usw.). Aus der IP-Adresse lässt sich auch der Aufenthaltsort ableiten - nach neuen Forschungsergebnissen sogar, ob sich der Nutzer zuhause, auf der Arbeit oder unterwegs befindet.

4. **Eine siebentägige statt sechsmonatige Vorratsdatenspeicherung beseitigt das Risiko von Datenmissbrauch, Datenpannen und falschem Verdacht nicht**, sondern begrenzt erst, nachdem die Offenlegung bereits passiert ist, das Ausmaß des Schadens. Im Fall anmeldepflichtiger Internetdienste (z.B. Google Mail, Facebook, Twitter) und bei Einsatz von „Cookies" ermöglicht es die Offenlegung der Identität des Nutzers, dessen Internetnutzung weit länger als sieben Tage zurückzuverfolgen.

5. **Dass bereits heute einige Internet-Zugangsanbieter rechtswidrig eine Vorratsspeicherung unserer Identität im Internet praktizieren, ist mit den Auswirkungen eines generellen Speicherzwangs nicht zu vergleichen.** Denn bisher ermöglicht die unterschiedliche Speicherpraxis gerade Personen, die auf eine anonyme Internetnutzung angewiesen sind, die Wahl eines Internet-Zugangsanbieters, der keine Vorratsdatenspeicherung vornimmt (z.B. Arcor, Freenet, Versatel, Vodafone).

6. **Eine generelle und undifferenzierte Vorratsspeicherung unserer Identität im Internet beseitigt das Risiko eines mit Sanktionen verbundenen EU-Vertragsverletzungsverfahrens nicht**, denn Sanktionen nach Art. 260 Abs. 3 AEUV beantragt die EU-Kommission auch, „wenn sich die mitgeteilten Umsetzungsmaßnahmen [...] nur auf einen Teil der Richtlinie beziehen".[5] Die Meldung einer Teilumsetzung kann bereits bei Einführung eines reinen Quick-Freeze-Verfahrens erfolgen. Ohnehin ist eine Entscheidung des Europäischen Gerichtshofs über eine Klage wegen Vertragsverletzung nicht vor Ablauf eines Jahres zu erwarten. Es ist vollkommen offen, ob und in welcher Form die EG-Richtlinie zur

Vorratdatenspeicherung in einem Jahr noch existiert. Übrigens sind ständig ca. 20 Vertragsverletzungsverfahren gegen Deutschland vor dem Europäischen Gerichtshof anhängig.[6] Vor allem hat die Bundesregierung die Möglichkeit, aus wichtigen Gründen des Grundrechtsschutzes eine Befreiung von der Pflicht zur Umsetzung der Richtlinie zur Vorratsdatenspeicherung zu beantragen und dies nötigenfalls einzuklagen (Art. 114 Abs. 4 AEUV). Dadurch kann eine Verurteilung wegen Vertragsverletzung auf absehbare Zeit ausgeschlossen werden.

7. **Eine generelle und undifferenzierte Vorratsspeicherung unserer Identität im Internet ändert nichts daran, dass CDU- und CSU-Politiker die FDP als Sicherheitsrisiko und Vertragsverletzer diffamieren**, wie die aktuelle Debatte zeigt.

8. **Straftaten lassen sich auch ohne Vorratsspeicherung von Verbindungsdaten über das Verbindungsende hinaus verfolgen; auch ein Verfahren zur schnellen Sicherung von Verkehrsdaten („Quick Freeze“) setzt keine Vorratsdatenspeicherung voraus.** Schon der Blick auf unser tägliches Leben zeigt, dass die meisten (ca. 55%) dem Staat bekannt gewordenen Straftaten aufgeklärt werden können, obwohl niemand mitschreibt, wer wir sind, mit wem wir geredet, wo wir uns aufgehalten und worüber wir uns informiert haben. Strafverfolgung gelingt bei unbekannten Tätern beispielsweise, indem sie noch auf frischer Tat festgehalten und identifiziert werden. Dies ist im Internet besonders lange möglich, weil Internetverbindungen im Zeitalter von Flatrates typischerweise länger aufrecht erhalten werden als sich ein Täter sonst am Tatort aufhalten würde. Teilweise werden unbekannte Straftäter auch mithilfe von Spuren ausfindig gemacht. Im Internet kann man bei Betrugsdelikten oftmals erfolgreich der Spur des erschwindelten Geldes bzw. Gutes folgen. Bei 82% der polizeilich registrierten Internetdelikte handelt es sich um Betrug. Teilweise werden unbekannte Straftäter ertappt, wenn sie an den Tatort zurück kehren. Im Internet funktioniert dies beispielsweise, wenn sich der Straftäter erneut bei dem Dienst anmeldet, über den er seine Straftat begangen oder bekannt gegeben hat (z.B. Auktionshaus, Chat-Dienst, E-Mail-Konto). So konnte das Bundeskriminalamt auf diese Weise einen Mann, der in einem Internetchat über einen Kindesmissbrauch berichtet hatte, im März 2010 dingfest machen lassen, obwohl der genutzte Zugangsanbieter Verbindungsdaten nicht verdachtslos auf Vorrat speicherte. Es ist nicht nachzuweisen, dass eine Internet-Vorratsdatenspeicherung überhaupt einen statistisch signifikanten Beitrag zu der Zahl der aufgeklärten Straftaten leistete, nachdem selbst die sechsmonatige Vorratsdatenspeicherung im Jahr 2009 die Aufklärungsquote nicht gesteigert hat.

Wir verlangen vor diesem Hintergrund, die Vorschrift zur generellen und undifferenzierten Vorratsspeicherung unserer Identität im Internet (§ 113a TKG-E) sofort aus dem Gesetzentwurf zu streichen. Sinnvolle Vorschläge zum wirksameren Vorgehen gegen Internetdelikte haben wir bereits unterbreitet.[7]

<u>Umgekehrt besteht ein dringender Bedarf, den Schutz von Internetnutzern vor Überwachung und Beobachtung zu stärken:</u>

1. Durch Änderung des § 100 TKG muss auch eine aus Providersicht **freiwillige, anlassunabhängige Vorratsspeicherung von Verkehrsdaten klar ausgeschlossen** werden.[8] 96,2% der im Rahmen einer Umfrage befragten Internetnutzer/innen ist dies wichtig, 86,7% sogar sehr wichtig. Die nach § 100 TKG gesammelte Datenhalde geht sowohl hinsichtlich der protokollierten Informationen wie bezüglich der Datenverwendung (z.B. millionenfache Datennutzung zur Auskunfterteilung an Private nach § 101 UrhG) noch weit über die im Eckpunktepapier vorgeschlagene verpflichtende Vorratsdatenspeicherung hinaus. Daneben muss auch das vor Einführung der Vorratsdatenspeicherung bestehende Recht, die unverzügliche Löschung von Abrechnungsdaten zu verlangen (§ 97 TKG a.F.), wieder eingeführt werden.

2. Die **Identität des Nutzers einer IP-Adresse darf künftig nur noch mit richterlichem Beschluss**, nur zur Verfolgung schwerer Straftaten oder zur Abwehr schwerer Gefahren und nicht für Geheimdienste offengelegt werden (§§ 112, 113 TKG und § 100k StPO-E ändern). 92,4% der Internetnutzer/innen ist dies wichtig.

3. Behörden dürfen **Auskünfte über Nutzer von Internetdiensten und ihre Internetnutzung künftig nur noch unter den Voraussetzungen verlangen, die für Auskünfte über Nutzer von Telekommunikationsdiensten und deren Verbindungen gelten** (nur auf richterliche Anordnung, nur zur Verfolgung schwerer Straftaten oder zur Abwehr schwerer Gefahren). Die §§ 14, 15 des Telemediengesetzes müssen entsprechend geändert werden. 92,4% der Internetnutzer/innen ist dies wichtig.

4. Eine in die Zukunft gerichtete „Quick-Freeze"-Anordnung auf „Zuruf" zur **Speicherung zukünftiger Verkehrsdaten muss außer Kraft treten, wenn sie nicht binnen drei Werktagen gemäß § 100g StPO richterlich bestätigt wird**. Quick-Freeze-Anordnungen müssen die Rufnummer oder eine andere Kennung des zu überwachenden Anschlusses oder des Endgerätes bezeichnen. Ohne richterliche Anordnung eingefrorene Daten müssen spätestens nach sieben Tagen gelöscht werden, weil innerhalb dieser Zeitspanne ausreichend Gelegenheit besteht, eine richterliche Anordnung zur Herausgabe der Daten zu bewirken. 91,4% der Internetnutzer/innen ist eine derartige Gestaltung des geplanten Quick-Freeze-Verfahrens wichtig.

5. Das **Fernmeldegeheimnis muss auf die Nutzung von Internetdiensten erstreckt** werden („Telemedien-Nutzungsgeheimnis"). 89,5% der Internetnutzer/innen ist dies wichtig.

6. **Für rechtswidrig erteilte Auskünfte über Nutzer von Internetdiensten muss ein Verwertungsverbot** eingeführt werden, unter anderem damit ausländische Anbieter nicht länger ohne Vorliegen der deutschen Schutzvorschriften „freiwillig“ Auskünfte über Internetnutzer erteilen. 87,6% der Internetnutzer/innen ist dies wichtig.

7. Anbietern von Internetdiensten muss die **Erstellung von Nutzerprofilen ohne Einwilligung des Nutzers verboten** werden; das bisherige Widerspruchsrecht reicht nicht (§ 15 TMG ändern). 86,7% der Internetnutzer/innen ist dies wichtig.

8. Die **Ermächtigung des Bundesamts für Sicherheit in der Informationstechnik zur Aufzeichnung von Surfprotokollen muss aufgehoben** werden (§ 5 BSIG). 84,8% der Internetnutzer/innen ist dies wichtig.

9. Behörden dürfen **Passwörter zu E-Mail-Konten und SIM-PINs nur unter den Voraussetzungen der dadurch ermöglichten Telekommunikationsüberwachung** verlangen (§ 113 I 2 TKG ändern). 82,9% der Internetnutzer/innen ist dies wichtig.

10. **Internet-Zugangsanbieter müssen verpflichtet werden, auf Wunsch die dynamische Zuteilung einer neuen IP-Adresse bei jedem Einwahlvorgang anzubieten**. Im Zeitalter von IPv6 wird sonst eine Nachverfolgung unserer Internetnutzung nicht nur bis zu eine Woche lang, sondern monate- oder jahrelang möglich sein. 79,1% der Internetnutzer/innen ist dies wichtig. Dynamisch zugeteilte IP-Adressen müssen auch im Zeitalter von IPv6 so aufgebaut sein, dass der Internet-Zugangsanbieter mit ihnen nach Verbindungsende keine Rückverfolgung mehr vornehmen kann. „Semipermanente“ IP-Adressen erfüllen diese Anforderung nicht. Wegen der zunehmend dauerhaft verbundenen Geräte (z.B. Telefonmodems, TV-Modems) muss auf Wunsch auch die Neuzuteilung einer IP-Adresse spätestens alle 24 Stunden angeboten werden. Internet-Zugangsanbieter müssen Neukunden bei Vertragsschluss diese Wahlrechte anbieten.

11. Es muss gesetzlich festgelegt werden, dass die **Bereitstellung von Diensten nicht von der Angabe einer DeMail-Adresse abhängig gemacht werden** darf. 75,2% der Internetnutzer/innen ist dies wichtig.

Nachweise:

1. Beschluss der FDP-Bundestagsfraktion vom 09.11.2010, http://www.fdp-fraktion.de/files/1228/Eckpunkte_Kriminalitaetsbekaempfung_Internet.pdf
2. BT-Drs. 16/8434, 78.
3. BT-Drs. 16/8434, 78.
4. infas-Umfrage im Oktober 2009, http://www.vorratsdatenspeicherung.de/images/infas-umfrage.pdf.
5. Mitteilung der Kommission vom 15.1.2011, Seite 3.
6. Kommission, Anhang I zum Jahresbericht 2009, http://ec.europa.eu/eu_law/docs/docs_infringements/annual_report_27/statannex_1-3_en.pdf, Seite 18.
7. Sicherheit geht vor Sammelwut - Vorratsdatenspeicherung gefährdet Menschenleben, Oktober 2010, http://wiki.vorratsdatenspeicherung.de/images/Bericht_Sicherheit-vor-Sammelwut.pdf, Seiten 18 ff.
8. Vgl. BGH, III ZR 146/10 vom 13.01.2011.

04.03.2012

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