

**Stellungnahme
des Arbeitskreises Vorratsdatenspeicherung**

zum

**Eckpunktepapier des Bundesjustizministeriums zur Sicherung
vorhandener Verkehrsdaten und Gewährleistung von
Bestandsdatenauskünften im Internet.**



www.vorratsdatenspeicherung.de

Zur uneingeschränkten Verbreitung.

Inhalt

Position zum Eckpunktepapier der Bundesregierung	2
Vorgebrachte Argumente.....	3
Forderungen zur Stärkung des Datenschutzes im Internet.....	5
Kontakt.....	6
Quellen.....	6



Position zum Eckpunktepapier der Bundesregierung

Das Eckpunktepapier 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. In Verbindung mit anderen Informationen, die Anbieter 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 Dambruch 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.



Vorgebrachte Argumente

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. **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.
3. **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.
4. **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).
5. **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 Vorratsdatenspeicherung 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.

6. **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.
7. **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, den Vorschlag einer generellen und undifferenzierten Vorratsspeicherung unserer Identität im Internet sofort zurückzuweisen und zurückzuziehen. Sinnvolle Vorschläge zum wirksameren Vorgehen gegen Internetdelikte haben wir bereits unterbreitet.^[7]



Forderungen zur Stärkung des Datenschutzes im Internet

Umgekehrt besteht ein dringender Bedarf, den Schutz unserer Privatsphäre im Internet vor staatlicher Überwachung zu stärken:

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 oder Telefonnummer 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 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 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.

Kontakt

Arbeitskreis Vorratsdatenspeicherung
c/o FoeBuD e.V.
Marktstr. 18, 33602 Bielefeld
Tel: 0521-175254

Email: kontakt@vorratsdatenspeicherung.de

Web: <http://www.vorratsdatenspeicherung.de>

Quellen

1. Beschluss der FDP-Bundestagsfraktion vom 09.11.2010, <http://bit.ly/eckpunktebmj>
2. BT-Drs. 16/8434, 78. <http://bit.ly/BTDRS-16-8434>
3. BT-Drs. 16/8434, 78. <http://bit.ly/BTDRS-16-8434>
4. infas-Umfrage im Oktober 2009, <http://bit.ly/VDS-infrasumfrage>
5. Mitteilung der Kommission vom 15.1.2011, Seite 3.
6. Kommission, Anhang I zum Jahresbericht 2009, Seite 18. <http://bit.ly/Kommission-Anhang1>
7. Sicherheit geht vor Sammelwut - Vorratsdatenspeicherung gefährdet Menschenleben, Oktober 2010, Seiten 18 ff. <http://bit.ly/SvorSammelwut>
8. Vgl. BGH, III ZR 146/10 vom 13.01.2011.

Aufklärungslücke bei der Verfolgung von Straftaten

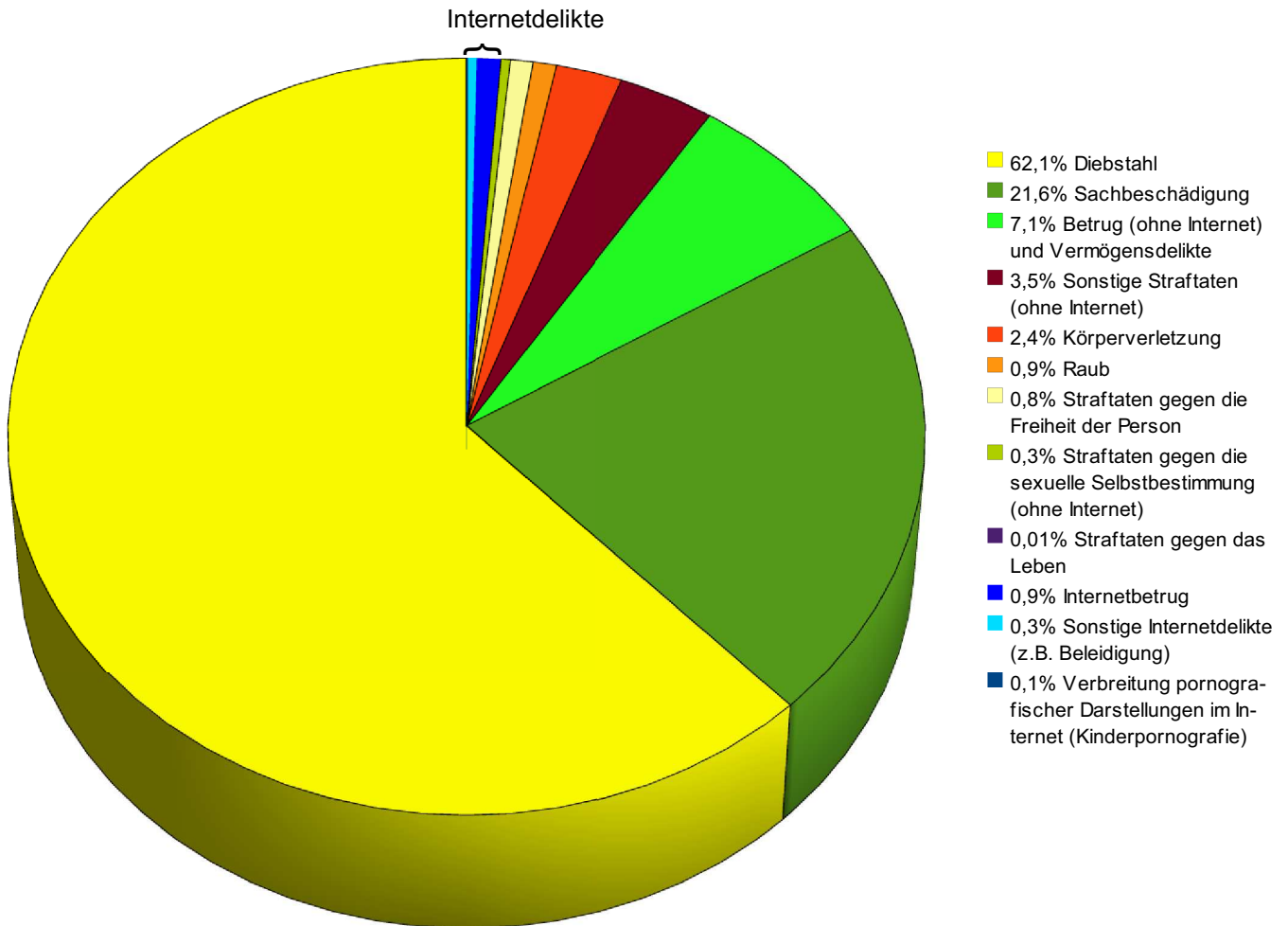


Bild 1: Aufklärungslücke ist die Zahl, um welche die Zahl der im jeweiligen Jahr aufgeklärten Straftaten eines Deliktsfeldes (berechnet aus der Aufklärungsquote) hinter der Zahl der in diesem Jahr registrierten Straftaten desselben Deliktsfeldes zurück bleibt. Datenquelle: Polizeiliche [Kriminalstatistik](#) des Bundeskriminalamts für 2008. Die Situation im Jahr 2008 ist mit der heutigen Situation vergleichbar, weil Internet-Zugangsanbieter nach einer [Intervention](#) des Bundesdatenschutzbeauftragten zugewiesene IP-Adressen nicht länger als 0-7 Tage speicherten und auch bereits [86%](#) der Internetnutzer eine Flatrate nutzten.

Es zeigt sich: Unter den polizeilich bekannten aber nicht aufgeklärten Straftaten ist nur ein Bruchteil (unter 2%) im Internet begangen oder handelt es sich gar um Verbreitung kinderpornografischer Darstellungen im Internet (0,1%). Nur jede 50. polizeilich bekannte aber nicht aufgeklärte Straftat wird im Internet begangen. Von 1.000 polizeilich bekannten aber nicht aufgeklärten Straftaten handelt es sich bei weniger als einer um die Verbreitung von Kinderpornografie im Internet.

Aufklärungslücke bei der Verfolgung von Straftaten

Deliktsfeld	Aufklärungs- lücke 2008	Anteil 2008	Aufklärungs- lücke 2009	Anteil 2009
Gesamt	2.759.884	100%	2.687.113	100%
Diebstahl	1.715.182	62,1%	1.638.124	61,0%
Sachbeschädigung	596.986	21,6%	581.660	21,6%
Betrug und Vermögensdelikte (ohne Internet)	194.762	7,1%	197.870	7,4%
Körperverletzung	66.852	2,4%	65.927	2,5%
Raub	23.558	0,9%	23.376	0,9%
Straftaten gegen die Freiheit einer Person (z.B. Nötigung)	22.372	0,8%	21.726	0,8%
Straftaten gegen die sexuelle Selbstbestimmung (ohne Internet)	9.498	0,3%	9.821	0,4%
Straftaten gegen das Leben (z.B. Mord)	253	0,01%	274	0,01%
Sonstige Straftaten (ohne Internet)	96.596	3,5%	98.057	3,6%
Internetdelikte insgesamt	33.825	1,2%	50.278	1,9%
Internetbetrug	23.758	0,9%	38.361	1,4%
Verbreitung pornografischer Darstellungen im Internet (Kinderpornografie)	1.290	0,1%	1.480	0,1%
Urheberrechtsverletzungen im Internet	708	0,03%	425	0,02%
Sonstige Internetdelikte (z.B. Beleidigung)	8.069	0,3%	10.012	0,4%

Tabelle 1: Aufklärungslücke ist die Zahl, um welche die Zahl der im jeweiligen Jahr aufgeklärten Straftaten eines Deliktsfeldes (berechnet aus der Aufklärungsquote) hinter der Zahl der in diesem Jahr registrierten Straftaten desselben Deliktsfeldes zurück bleibt. Datenquelle: Polizeiliche [Kriminalstatistik](#) des Bundeskriminalamts.

Erläuterung: Im Jahr 2008 waren – ebenso wie gegenwärtig – Internet-Zugangsanbieter nicht zu einer verdachtslosen Vorratsspeicherung von aller Internetkunden verpflichtet. Vom 01.01.2009-02.03.2010 waren Internet-Zugangsanbieter zu einer verdachtslosen Vorratsspeicherung von Daten aller Internetkunden verpflichtet. Während dieses Zeitraums vergrößerte sich die Aufklärungslücke im Internetbereich.

Aufklärungsquote bei Internetdelikten mit und ohne Vorratsdatenspeicherung

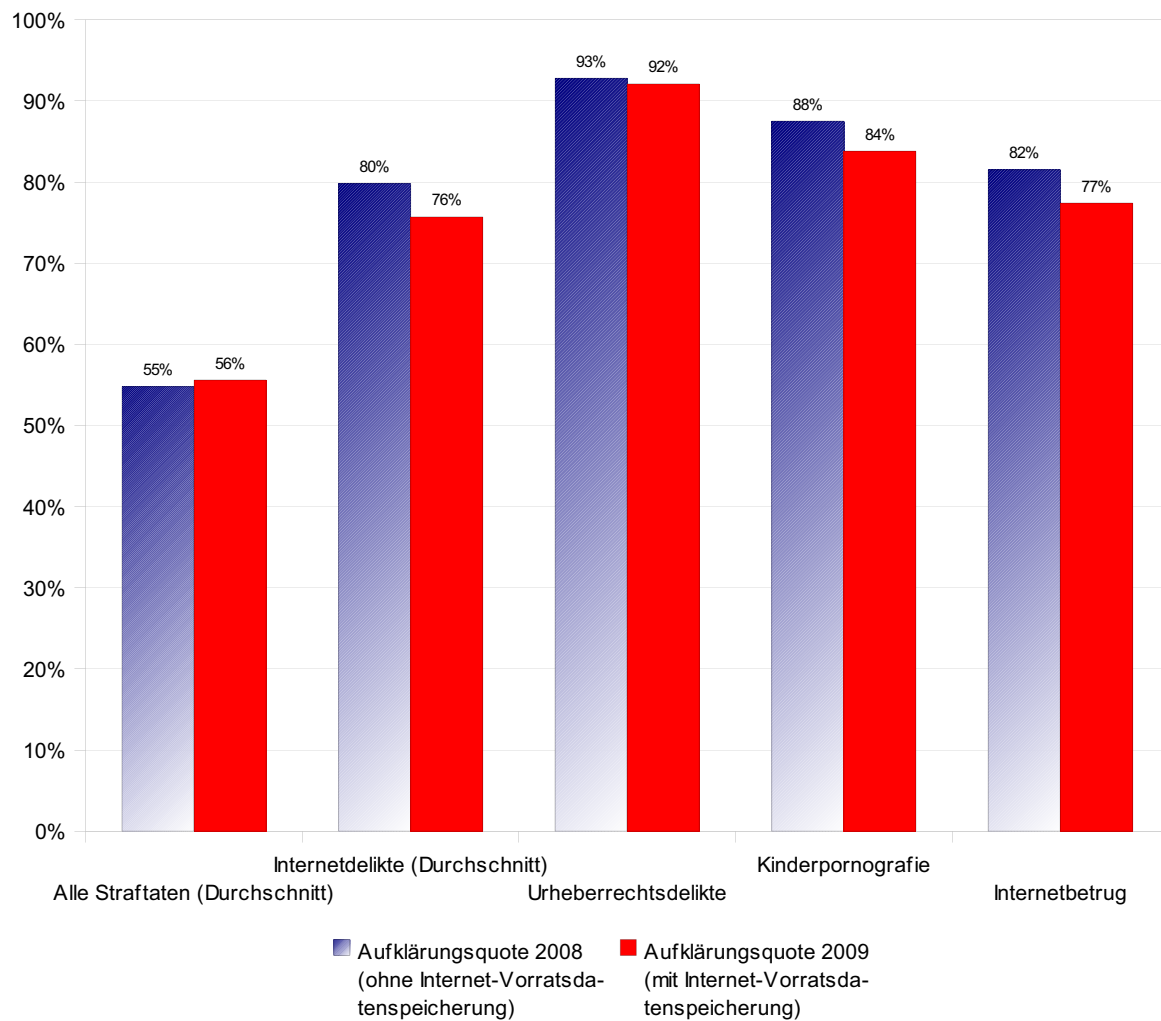


Bild 2: Im Internet begangene Straftaten werden zu einem weit höheren Anteil (76%) aufgeklärt als Straftaten allgemein (56%). Dies gilt auch für die Verbreitung kinderpornografischer Darstellungen im Internet (Aufklärungsquote: 84%). Vor Inkrafttreten der Internet-Vorratsdatenspeicherung am 01.01.2009 war die Aufklärungsrate bei Internetdelikten höher (2008: 80%) als unter Geltung der Internet-Vorratsdatenspeicherung (2009: 76%).

Vorratsdatenspeicherung und Aufklärung von Internet-Straftaten

Datenquelle: Kriminalstatistik des Bundeskriminalamts

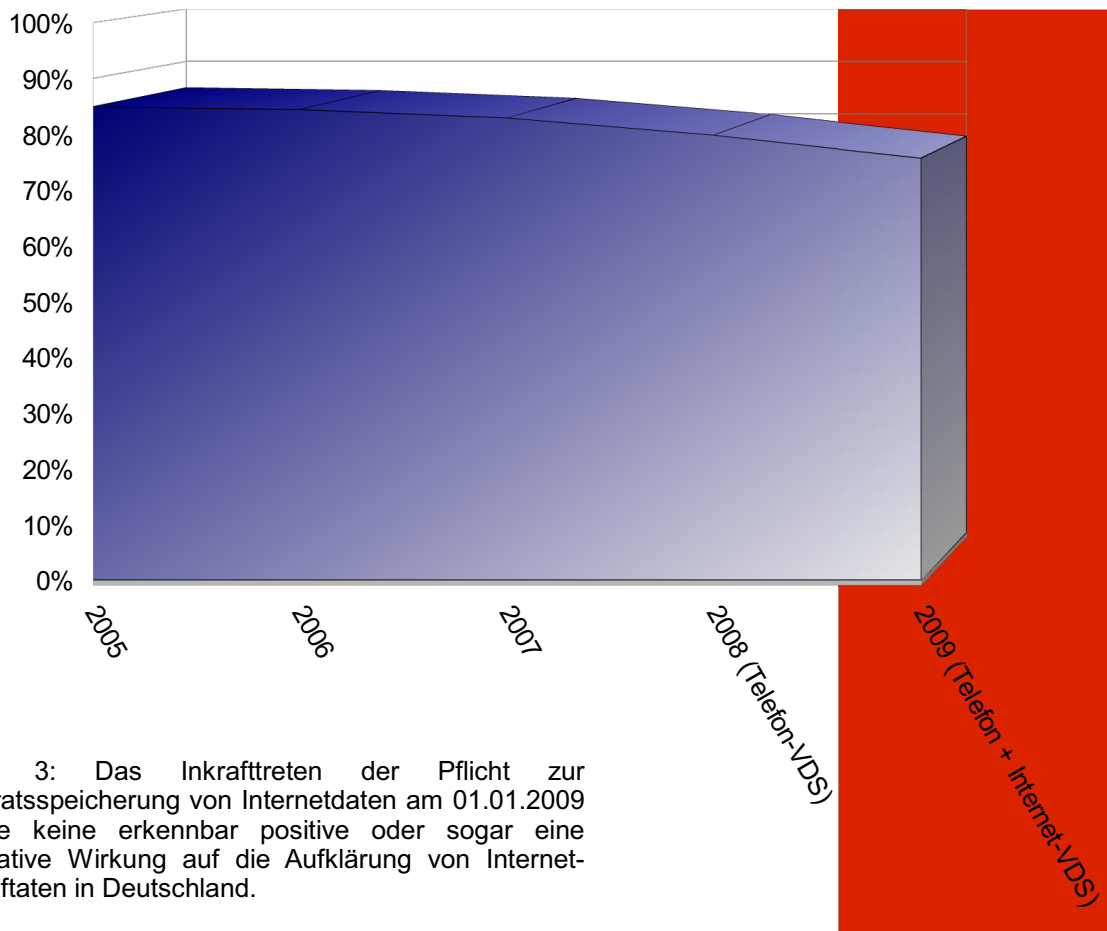


Bild 3: Das Inkrafttreten der Pflicht zur Vorratsspeicherung von Internetdaten am 01.01.2009 hatte keine erkennbar positive oder sogar eine negative Wirkung auf die Aufklärung von Internet-Straftaten in Deutschland.

Jahr	Aufklärungsquote von Internet-Straftaten	Internet-Vorratsdatenspeicherung
2005	84,9%	keine
2006	84,4%	keine
2007	82,9%	keine
2008	79,8%	keine
2009	75,7%	Internet-Vorratsdatenspeicherung
2010	nicht bekannt	keine seit 02.03.2010

Anlässe für Auskünfte über Internetnutzer (IP-Adressen)

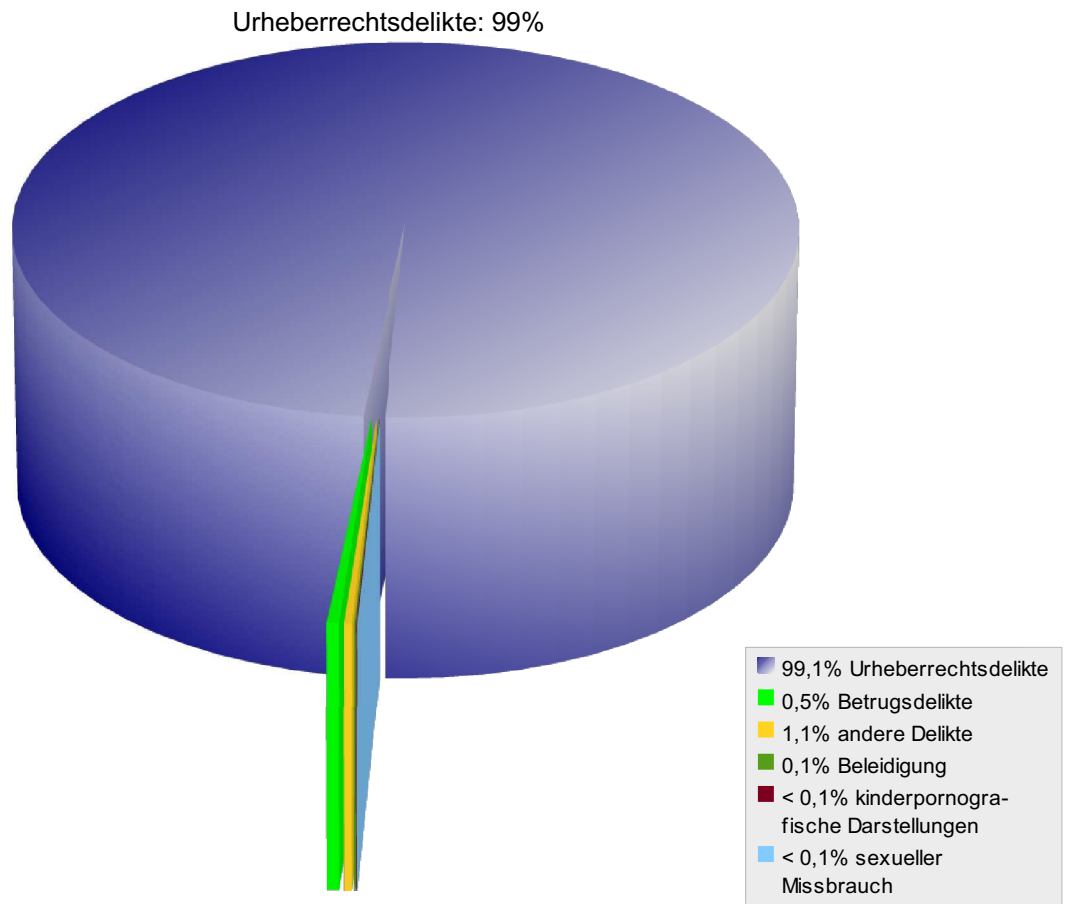


Bild 1: Auskünfte über Internetnutzer (IP-Adressen) werden fast ausschließlich an private Rechteinhaber zur Abmahnung von Urheberrechtsverstößen und nur zu einem geringen Bruchteil (0,1%) für strafrechtliche Ermittlungen wegen Austauschs kinderpornografischer Darstellungen im Internet erteilt.

	Anzahl 2010	Anteil
Auskünfte insgesamt	2.421.000	100%
Auskünfte an Rechteinhaber wegen Urheberrechtsverstößen	2.400.000	99,1%
Auskünfte an staatliche Stellen insgesamt	21.000	0,9%
• davon Betrug	11.432*	0,5%
• davon Beleidigung	1.300*	0,1%
• davon (kinder-)pornografische Darstellungen	662*	0,03%
• davon sexueller Missbrauch	275*	0,01%

Alle Zahlen beziehen sich auf Auskünfte der Deutschen Telekom AG (DTAG) im Jahr 2010. Quelle: Angaben der DTAG.

* Zur Aufschlüsselung des Zwecks der Auskünfte an staatliche Stellen wurde das Verhältnis der Anlässe zueinander aus dem Jahr 2005 zugrunde gelegt ([DTAG-Statistik](#), Seite 9), weil neuere Zahlen dazu nicht existieren.

Bundesministerin der Justiz
Mohrenstraße 37
10117 Berlin

17. Januar 2011

Sehr geehrte Frau Leutheusser-Schnarrenberger,

ein erfreulich klarer Beschluss der FDP aus dem vergangenen Jahr betont zum Thema „Vorgehen gegen Internetkriminalität“, es dürfe „nicht vom Grundsatz abgerückt werden, der für den Rechtsstaat konstitutiv ist, dass mit staatlicher Überwachung und Verfolgung nur derjenige rechnen muss, gegen den ein Verdacht vorliegt. Eine anlasslose Überwachung aller Bürgerinnen und Bürger unabhängig von einem Verdacht wie durch die Vorratsdatenspeicherung widerspricht diesem Grundsatz.“¹ „Die anlass- und verdachtsunabhängige Vorratsdatenspeicherung hat die FDP von Anfang an abgelehnt“, heißt es auch im Wahlprogramm der FDP aus dem Jahr 2009,² auf dessen Grundlage 14,6% der Wählerinnen und Wähler ihre Stimme der FDP gegeben haben.

In Umsetzung dieses Auftrags hat die FDP-Bundestagsfraktion am 09.11.2010 beschlossen: „Der Rechtsgrundsatz, dass 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, muss auch im digitalen Raum gelten. Wir lehnen daher die verdachts- und anlassunabhängige Speicherung personenbezogener Daten auf Vorrat ab.“³ Noch vor wenigen Tagen erklärte der Bundesvorsitzende Dr. Guido Westerwelle: „Wir sollten nicht ohne Anlass die Telefon- und Internetverbindungsdaten aller Bürger speichern.“⁴

Als Zusammenschluss von Bürgerrechtlern, Datenschützern und Internetnutzern teilen und begrüßen wir die Ablehnung einer Vorratsdatenspeicherung, für die Datenschutzbeauftragte, Zivilgesellschaft, Berufsverbände und freiheitsfreundliche Politiker gemeinsam werben.

1 Beschluss des 61. Ord. Bundesparteitages der FDP, Köln, 24.-25. April 2010: Liberale Rechtspolitik im Zeichen der Bürgerrechte, http://parteitag.fdp.de/files/47/BPT-Liberale_Rechtspolitik.pdf.

2 http://www.deutschlandprogramm.de/files/653/Deutschlandprogramm09_Endfassung.PDF.

3 http://www.fdp-fraktion.de/files/1228/Eckpunkte_Kriminalitaetsbekaempfung_Internet.pdf.

4 Hamburger Abendblatt vom 14.01.2011, <http://www.abendblatt.de/politik/deutschland/article1756560/Westerwelle-FDP-muss-zum-Schlussfaktor-werden.html>.

Mit Unverständnis und Bestürzen haben wir nun aber feststellen müssen, dass Sie mit dem Vorschlag einer einwöchigen Erfassung aller Internetverbindungen⁵ diesen Konsens verlassen. Die gesuchte „Alternative zur Vorratsdatenspeicherung“ kann nicht eine Vorratsdatenspeicherung sein, egal wie „klein“ oder „leicht“ sie angeblich erscheinen mag!

1. Jede Vorratsdatenspeicherung hat verheerende Folgen

Sie scheinen der Auffassung zu sein, eine einwöchige Vorratsdatenspeicherung sei ein weitaus geringerer Eingriff als eine sechsmonatige Vorratsdatenspeicherung. Wir sind anderer Meinung, und sehen kaum einen Unterschied. Eine Verkürzung des Speicherzeitraums würde im Grundsatz nichts an den fatalen Wirkungen und Risiken jeder verdachtslosen Totalspeicherung ändern:

In einer Informationsgesellschaft wird der Zugang zum Internet zunehmend Voraussetzung für Recherche, Meinungsbildung, Meinungsäußerung und Meinungsaustausch. Anders als bei persönlichen Recherchen, direkten Gesprächen und postalischem Meinungsaustausch trägt man im Internet jedoch eine Identifikationskennziffer (IP-Adresse) offen bei sich. Verbreitet wird diese Kennziffer zusammen mit Informationsabrufen und Veröffentlichungen protokolliert und mit E-Mails versandt. Dadurch kann sich unser gesamtes Informations- und Kommunikationsverhalten im Internet nachträglich rekonstruieren und rückverfolgen lassen, wie es außerhalb des Internets undenkbar wäre. Das vom Bundesgerichtshof geforderte „Recht des Internetnutzers auf Anonymität“⁶ lässt vor diesem Hintergrund nur gewährleisten, wenn die Zuordnung von IP-Adressen möglichst verhindert wird.

Als Zusammenschluss von Bürgerrechtlern, Datenschützern und Internetnutzern sähen wir eine inakzeptable Diskriminierung der Internetnutzer darin, deren Verhalten ohne Anlass erfassen zu lassen, während vergleichbare Verhaltensweisen außerhalb des Internet anonym möglich bleiben: Warum soll ein anonym per E-Mail versandtes Dokument rückverfolgbar bleiben, wenn dasselbe Schreiben per Post anonym versandt werden kann? Warum soll die Lektüre eines politischen Artikels im Internet nachverfolgbar bleiben, wenn man sich den Abdruck des Artikels anonym in der Buchhandlung kaufen kann? Wie rechtfertigt sich die Ungleichbehandlung von Internet-Telefonie und Telefon-Flatrates, von Twitter-Nutzung und SMS-Flatrates? Aus unserer Sicht ist es unerträglich und mit einer modernen Netzpolitik unvereinbar, gerade Internetnutzer unter einen Generalverdacht stellen zu wollen, indem man ihr Verhalten ohne Anlass erfassen lässt.

Jede allgemeine Aufzeichnung der Zuordnung von Internetadressen setzt vertrauliche Tätigkeiten und Kontakte etwa zu Journalisten, Beratungsstellen oder Geschäftspartnern dem ständigen Risiko eines Bekanntwerdens durch Datenpannen und -missbrauch aus. Daneben schafft die Aufzeichnung von Verbindungsdaten das permanente Risiko, unschuldig einer Straftat verdächtigt, einer Wohnungsdurchsuchung oder Vernehmung unterzogen oder abgemahnt zu werden, denn Verbindungsdaten lassen nur auf den Inhaber eines Anschlusses rückschließen und nicht auf dessen Benutzer.

5 Süddeutsche Zeitung vom 16.01.2011, <http://www.sueddeutsche.de/politik/justizministerin-im-sz-gespraech-es-darf-nicht-uferlos-gespeichert-werden-1.1047230>.

6 BGHZ 181, 328.

Das ständige Risiko von Nachteilen infolge von Kommunikationsprotokollen entfaltet eine enorme Abschreckungswirkung und würde eine unbefangene Internetnutzung in sensiblen Situationen zu vereiteln drohen (z.B. anonyme Information von Journalisten per E-Mail, anonyme Meinungsäußerung im Internet, vertraulicher Austausch von Geschäftsgeheimnissen, vertrauliche Koordinierung politischer Proteste, psychologische, medizinische und juristische Beratung und Selbsthilfegruppen von Menschen in besonderen Situationen wie Notlagen und Krankheiten). Wenn gefährliche oder gefährdete Menschen nicht mehr ohne Furcht vor Nachteilen Hilfe suchen können, verhindert dies eine sinnvolle Prävention und kann sogar Leib und Leben Unschuldiger gefährden.

Jede massenhafte Erfassung des Informations- und Kommunikationsverhalten vollkommen Unschuldiger verstößt gegen die EU-Grundrechtecharta und die Europäische Menschenrechtskonvention. Der EU-Gerichtshof, der Europäische Gerichtshof für Menschenrechte und der Rumänische Verfassungsgerichtshof haben flächendeckende Veröffentlichungen, Erfassungen oder Aufzeichnungen persönlicher Daten bereits als unverhältnismäßig verworfen. Das Bundesverfassungsgericht hat in seiner Entscheidung zur Vorratsdatenspeicherung nur das Grundgesetz angewandt, nicht aber die ebenfalls zu beachtende EU-Grundrechtecharta und Europäische Menschenrechtskonvention geprüft.

2. Dammbbruch auf dem Weg in die Überwachungsgesellschaft

Die Zulassung einer Vorratsdatenspeicherung wäre ein Dammbbruch auf dem Weg in die Überwachungsgesellschaft. Die globale Speicherung von Daten allein für eine mögliche künftige staatliche Verwendung würde allmählich alle Lebensbereiche erfassen, denn die vorsorgliche Protokollierung personenbezogener Daten ist für den Staat stets und in allen Bereichen nützlich. Wenn dem Staat die permanente Aufzeichnung des Verhaltens sämtlicher seiner Bürger ohne Anlass gestattet würde, würden schrittweise sämtliche Lebensbereiche in einer Weise registriert werden, wie es selbst unter früheren totalitären Regimes wie der DDR undenkbar war. Sicherlich wollen Sie nicht, dass der Staat „kurzfristig“ erfassen lässt, welche Bücher Sie lesen und mit wem Sie den Tag über sprechen und verkehren?

Wenn Sie eine einwöchige Erfassung aller Internetverbindungen für gerechtfertigt erachten, können Sie beispielsweise nicht begründen, warum nicht auch eine zweiwöchige, sechswöchige oder sechsmonatige Aufbewahrung der Daten gerechtfertigt sein soll. Das Bundeskriminalamt behauptet schon heute, eine einwöchige Vorratsdatenspeicherung würde „nicht annähernd den polizeilichen Bedarf decken. Selbst in einem noch so engen Zeitfenster von Ereigniszeitpunkt, polizeilicher Kenntniserlangung, Prüfung und Auskunftersuchen sind wenige Tage in der Regel nicht ausreichend.“⁷

Wenn Sie eine Erfassung aller Internetverbindungen für gerechtfertigt erachten, können Sie auch nicht begründen, warum Telefonverbindungen nicht erfasst werden dürften. Schließlich nimmt die Zahl der Telefon-Flatrates zu. Hängt der polizeiliche Bedarf davon ab, ob ein Amoklauf im Internet

7 Bundeskriminalamt, Auswirkungen des Urteils des Bundesverfassungsgerichts zu Mindestspeicherungsfristen, http://www.bundesrat.de/cln_179/DE/gremien-konf/fachministerkonf/imk/Sitzungen/10-11-19/anlage10.templateId=raw.property=publicationFile.pdf/anlage10.pdf.

oder telefonisch angedroht wird? Sie führen Ihre eigene, ansonsten prinzipielle Argumentation gegen eine Vorratsdatenspeicherung ad absurdum, wenn Sie selbst eine Vorratsdatenspeicherung vorschlagen.

Eine Internet-Vorratsdatenspeicherung schaffte genau den Präzedenzfall für eine flächendeckende, unterschiedslose Erfassung des Verhaltens unschuldiger Menschen, den wir zum Erhalt unserer freien Gesellschaft verhindern müssen.

3. Strafverfolgung braucht keine Vorratsdatenspeicherung

Ausgangspunkt Ihrer Überlegungen ist die Tatsache, dass nicht gespeicherte Verbindungsdaten nicht an den Staat herausgegeben oder für diesen „eingefroren“ werden können. Dies ist indes kein Nachteil der aktuellen Rechtslage, sondern - wie oben gezeigt - ihr entscheidender Vorteil.

Leider übernehmen Sie mit Ihrem Vorschlag unbesehen die Behauptung maßloser Innenpolitiker, man brauche insbesondere bei Pauschaltarifen („Flatrates“) eine Protokollierung jeder Verbindung, um Straftaten verfolgen zu können. Die Behauptung, dass sich Straftaten ohne Vorratsspeicherung von Verbindungsdaten über das Verbindungsende hinaus nicht verfolgen ließen, ist ebenso falsch wie die Behauptung, ein Verfahren zur schnellen Sicherung von Verkehrsdaten („Quick Freeze“) setze eine 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, mit wem wir geredet, wo wir uns aufgehalten oder worüber wir informiert haben. Wie gelingt Strafverfolgung bei unbekannten Tätern?

- Teilweise werden Straftäter noch auf frischer Tat festgehalten und identifiziert. Dies ist auch im Internet möglich: Straftäter können während der bestehenden Verbindung auch ohne Vorratsdatenspeicherung „auf frischer Tat“ identifiziert werden. Zurzeit dauert es allerdings noch viel zu lange, bis die Anzeige eines Internetdelikts zu einem sachkundigen Polizeibeamten gelangt und die erforderlichen Ermittlungsmaßnahmen vorgenommen werden.
- Teilweise werden Straftäter mithilfe von Spuren ausfindig gemacht. Im Internet ist das auch ohne Vorratsdatenspeicherung möglich. Beispielsweise handelt es sich bei 82% der polizeilich registrierten Internetdelikte um Betrug. Hier kann man oftmals erfolgreich der Spur des erschwindelten Geldes bzw. der bestellten Waren folgen.
- Teilweise werden Straftäter ertappt, wenn sie 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). Beispielsweise konnte das Bundeskriminalamt auf diese Weise einen Mann, der in einem Internetchat über einen Kindesmissbrauch berichtet hatte, im März 2010 dingfest machen, obwohl der genutzte Zugangsanbieter Verbindungsdaten nicht verdachtslos auf Vorrat speicherte.

Politisch muss entscheidend sein, dass im Internet keine rechtsfreien Räume entstehen und Internetdelikte ebenso wirksam aufgeklärt werden können wie außerhalb des Internets begangene Delikte. Dies ist bereits gegenwärtig und auch ohne Erfassung jeder Internetverbindung gewährleistet. Die Verfolgung von Straftaten wird durch das Internet nicht erschwert, sondern enorm erleichtert. Ohne Totalerfassung sämtlicher Verbindungen werden Internetdelikte sehr viel häufiger aufgeklärt (zu über 70%) als sonstige Straftaten (zu etwa 55%). Solange dies so ist, besteht überhaupt kein Anlass für eine Erfassung jeder Internetverbindung völlig unschuldiger Menschen ins Blaue hinein. Die äußerst hohen Aufklärungsraten bei Internetdelikten ohne Vorratsdatenspeicherung wurden übrigens zuletzt im Jahr 2008 erzielt, als schon 86% der Deutschen eine Internet-Flatrate nutzen. Dies beweist, dass eine wirksame Strafverfolgung auch bei Pauschaltarifen („Flatrates“) ohne verdachtslose Aufzeichnung jeder Verbindung möglich ist. Um Ihr eigenes Ministerium zu zitieren: „Zur Kriminalitätsbekämpfung sind auch ohne die pauschale und anlasslose Speicherung jeder Benutzung von [...] Internet genügend Verbindungsdaten verfügbar“.⁸

Es ist nicht nachzuweisen, dass eine Internet-Vorratsdatenspeicherung überhaupt einen statistisch signifikanten Beitrag zu der Zahl der aufgeklärten Straftaten leistete. Dabei ist zunächst zu berücksichtigen, dass überhaupt nur 3% aller Straftaten im Internet begangen werden. Die vielfältigen Umgehungsmöglichkeiten, die bei Einführung einer Vorratsspeicherung von Internet-Verbindungsdaten noch stärker genutzt würden, stellen den vermeintlichen Nutzen einer solchen Maßnahme grundlegend in Frage. Bereits 2009 gaben 46,4% der Bürgerinnen und Bürger an, bei der Internetnutzung einen Anonymisierungsdienst zu benutzen oder benutzen zu wollen.⁹ Mit Internet-Cafés, offenen WLAN-Internetzugängen, internationalen Anonymisierungsdiensten und unregistrierten Handykarten stehen gerade im Internetbereich so viele und kostengünstige Umgehungsmöglichkeiten zur Verfügung, dass sich eine intelligente Sicherheitspolitik nicht ernsthaft einen nennenswerten Zusatznutzen von einer Erfassung jeder Internetverbindung versprechen kann.

Dies bestätigt die Erfahrung: In Deutschland wurde vor Beginn der Vorratsspeicherung aller Internet-Verbindungsdaten sogar ein größerer Anteil der Internetdelikte aufgeklärt (79,8%) als nach Inkrafttreten der Internet-Vorratsdatenspeicherung im Jahr 2009 (75,7%). Zu erklären ist dieser erstaunliche Befund mit den kontraproduktiven Wirkungen einer Totalerfassung aller Verbindungen. Werden sämtliche Verbindungen erfasst, wächst das Bewusstsein der Rückverfolgbarkeit jeder Internetnutzung und werden in zunehmendem Maß Umgehungsmöglichkeiten (z.B. Internet-Cafés, offene WLAN-Internetzugänge, Anonymisierungsdienste, unregistrierte Handykarten) genutzt, die dann selbst bei Verdacht einer Straftat keine gezielten Ermittlungen mehr zulassen, wo sie ohne Vorratsdatenspeicherung noch möglich gewesen wären. „Dadurch entfaltet eine Vorratsdatenspeicherung auf Gefahrenabwehr und Strafverfolgung kontraproduktive Wirkungen und verkehrt den erhofften Nutzen der Maßnahme möglicherweise sogar in sein Gegenteil“, so auch der Zusammenschluss von Richterinnen und Richtern, Staatsanwältinnen und Staatsanwälten e.V.¹⁰

8 http://www.bmj.bund.de/enid/Strafverfahren/Vorratsdatenspeicherung_1f6.html.

9 Infas: Der überwachte Bürger zwischen Apathie und Protest vom Oktober 2009, <http://www.vorratsdatenspeicherung.de/images/infas-umfrage.pdf>.

10 http://www.vorratsdatenspeicherung.de/images/NRV_Brief_2011-01-05.pdf.

In befreundeten Staaten wie Österreich, Schweden, Norwegen oder Kanada gilt schon lange ein striktes Verbot der Vorratsspeicherung von Verbindungsdaten,¹¹ ohne dass das Internet dort deswegen ein „rechtsfreier Raum“ wäre.

4. Kommunikationsfreiheit politisch klug verteidigen

Ihr Vorschlag fällt in die Zeit einer europäischen Debatte über den Grundansatz einer Vorratsspeicherung von Telekommunikationsdaten. Wir teilen Ihren Ausgangspunkt, dass auf europäischer Ebene ein Gegenmodell zur Vorratsdatenspeicherung gebraucht wird. Schon seit Monaten wirbt die Zivilgesellschaft europaweit und insbesondere bei der EU-Kommission für ein solches Gegenmodell.

Wir fordern dabei nicht die ersatzlose Streichung der Richtlinie zur Vorratsdatenspeicherung, weil dies die nationalen Gesetze zur Vorratsdatenspeicherung nicht stoppen würde. Gemeinsam mit 100 Organisationen europaweit fordern wir vielmehr die „Abschaffung der EU-Vorgaben zur Vorratsdatenspeicherung zugunsten eines Systems zur schnellen Sicherstellung und gezielten Aufzeichnung von Verkehrsdaten, wie es in der Cybercrime-Konvention des Europarats vereinbart worden ist“. Wir fordern also ein Verfahren zur schnellen Sicherstellung und gezielten Aufzeichnung von Verkehrsdaten, verbunden mit einem europaweiten Verbot einer verdachtslosen und flächendeckenden Totalspeicherung. Das ist unser Gegenmodell zur Vorratsdatenspeicherung.

Auch für den Fall, dass dieses Modell nicht europaweit durchzusetzen sein sollte, liegt ein Vorschlag auf dem Tisch: Danach würde die EU wenigstens den nationalen Volksvertretern und Verfassungsgerichten die Wahl überlassen, ob sie sich für eine (möglichst eingeschränkte) Vorratsdatenspeicherung oder aber für das bewährte Verfahren gezielter Aufbewahrungsanordnungen entscheiden. Wenn sich mehrere Mitgliedsstaaten für dieses Modell aussprechen und es im Europaparlament auf Akzeptanz stößt, bestehen durchaus Realisierungschancen. Das verfehlte Grundprinzip einer anlasslosen Totalerfassung muss dazu nicht akzeptiert werden.

Gerade vor dem Hintergrund der europäischen Debatte wäre es kontraproduktiv, wenn Deutschland als bisheriger Kritiker einer Vorratsdatenspeicherung nun selbst eine solche einführt. Sie könnten dann auf europäischer Ebene nicht mehr glaubwürdig für ein anlassbezogenes Verfahren als Alternative zu einer globalen und pauschalen Verbindungserfassung eintreten, sondern müssten sich auf bloße Diskussionen über die Modalitäten einer Vorratsdatenspeicherung (Datenarten, Aufbewahrungsdauer) beschränken.

5. Appell

Sehr geehrte Frau Leutheusser-Schnarrenberger, wir schätzen Ihren persönlichen langjährigen und konsequenten Einsatz für die Grund- und Freiheitsrechte sehr und haben großen Respekt davor. Im Hinblick auf die große Verantwortung, die Sie als Bundesjustizministerin tragen, appellieren wir an Sie, die Idee einer einwöchigen Vorratsspeicherung aller Internetverbindungen aufzugeben und entsprechend der Linie Ihrer Partei jeder verdachtsunabhängigen Speicherung von

11 Siehe Urteil des österreichischen Obersten Gerichtshofs vom 14.7.2009, Az. 4 Ob 41/09x.

Kommunikations- und Verbindungsdaten, die der grundgesetzlich geschützten Sphäre privater Lebensführung zuzurechnen sind, unabhängig von der Dauer der Speicherung entschieden entgegen zu treten.

Gerade in der jetzigen politischen Situation brauchen wir Ihre Unterstützung bei unserer Werbung für das Modell einer gezielten Strafverfolgung, das sich neben Deutschland auch in vielen weiteren Staaten wie Österreich, Schweden, Griechenland und Kanada bewährt hat. Bitte fallen Sie uns bei unserem europaweiten Werben für gezielte Strafverfolgung nicht zur Unzeit in den Rücken, sondern unterstützen Sie unsere europaweite Koalition gegen Vorratsdatenspeicherung nach Kräften.

Seien Sie sich unserer Unterstützung versichert, wenn es um die Entwicklung von und Werbung für Alternativen zu einer globalen und pauschalen Erfassung unserer Kommunikation geht.

Mit freundlichem Gruß,

Arbeitskreis Vorratsdatenspeicherung

Video: FDP-Pressekonferenz zur Vorratsdatenspeicherung (19.01.2011)

Die FDP-Politiker Ahrendt, Piltz und Leutheusser-Schnarrenberger nahmen gestern zu dem **untragbaren Eckpunktepapier** des Bundesjustizministeriums Stellung, das unter II. eine Erfassung jeder Internetverbindung auf Vorrat vorsieht, und kündigten noch weiter reichende Kompromisse in den anstehenden Verhandlungen mit CDU/CSU an (14 min.):



Anmerkungen:

- Falsch ist die Aussage der Bundesjustizministerin, die vorgeschlagene Speicherung von Daten über jede Internetnutzung gehe nicht über die bisherige Praxis der Anbieter hinaus. Bisher kann man Anbieter nutzen, die nicht auf Vorrat speichern (**z.B. Arcor/Vodafone, Versatel**), was der vorgeschlagene Speicherzwang verhindern würde. Außerdem hat erst letzte Woche der Bundesgerichtshof **entschieden**, dass die von einigen Internet-Zugangsanbietern zurzeit praktizierte mehrtägige Vorratsdatenspeicherung, soweit sie nicht technisch zwingend erforderlich ist, unzulässig ist.
- Falsch ist auch die Aussage der Bundesjustizministerin, sie schlage keine "Vorratsdatenspeicherung light" vor und Verkehrsdaten sollten nur anlassbezogen gespeichert werden. In Wahrheit sieht das **Eckpunktepapier** unter Punkt II. vor, dass für jede Internetverbindung jedes Internetnutzers in Deutschland ohne Anlass protokolliert werden soll, wann wer mit welcher IP-Adresse online war, was in Verbindung mit den Nutzungsprotokollen der Anbieter die Rekonstruktion unserer gesamten Internetnutzung ermöglichen würde. Die zu speichernden Daten sind sehr wohl Verkehrsdaten, die auf Vorrat gespeichert werden sollen.
- Siehe auch das **Interview der Bundesjustizministerin mit dem ZDF**, in dem sie ankündigt, die in ihrem Vorschlag vorgesehenen Fristen und Ausgestaltungen seien mit CDU und CSU verhandelbar. Die Union will sogar eine sechsmonatige Erfassung jeder Nutzung von Telefon, Handy, E-Mail und Internet erreichen. Bei einem **heutigen Ministertreffen** und am morgigen Donnerstag im Koalitionsausschuss soll ein Kompromiss ausgehandelt werden. Was dabei heraus kommt, ist offen; wir müssen das Schlimmste befürchten.



+++ Der Arbeitskreis Vorratsdatenspeicherung bittet heute alle Internetnutzer, sich für einen Anruf bei FDP-Bundestagsabgeordneten 5 Minuten Zeit zu nehmen, um die geplante Vorratsspeicherung jeder Internetverbindung in Deutschland zu verhindern +++

Schon anlässlich des heutigen Treffens des Koalitionsausschusses am Abend könnten CDU, CSU und FDP die Wiedereinführung einer Vorratsdatenspeicherung in Deutschland vereinbaren, befürchten die im AK Vorrat zusammen geschlossenen Bürgerrechtler, Datenschützer und Internetnutzer. Um dies zu verhindern, sollen besorgte Internetnutzer heute telefonisch eine Sperrminorität von mindestens 21 FDP-Bundestagsabgeordneten überzeugen, öffentlich zuzusichern, dass sie - wie von der FDP wiederholt beschlossen - der Wiedereinführung einer Vorratsdatenspeicherung unter keinen Umständen zustimmen werden, auch nicht der von der Bundesjustizministerin vorgeschlagenen Internet-Vorratsdatenspeicherung.

Nach einem „Eckpunktepapier“ von Bundesjustizministerin Leutheusser-Schnarrenberger (FDP) soll künftig für die gesamte Bevölkerung auf Vorrat protokolliert werden, wer wann mit welcher Kennung (IP-Adresse) im Internet gesurft hat. In Verbindung mit anderen Informationen, die Anbieter wie Google, Twitter oder Youtube speichern, würde so potenziell unsere gesamte Internetnutzung nachvollziehbar werden, also jede unserer Eingaben, jeder unserer Klicks, jeder unserer Downloads, jeder unserer Beiträge/Posts im Netz. Dies bedroht die Informationsfreiheit im Internet, weil man Nachteile durch den Aufruf "potenziell verdächtiger" Seiten oder die Verwendung "potenziell verdächtiger" Suchwörter befürchten müsste. Der Vorschlag würde weitgehend das Ende der Möglichkeit anonymer Kommunikation und Publikation im Internet bedeuten. Damit steht auch der Schutz kranker, ratsuchender oder bedrohter Menschen auf dem Spiel, die oftmals nur im Schutz der Anonymität bereit sind, sich im Internet zu informieren oder helfen zu lassen.

Nach dem Vorschlag der Ministerin könnte die Polizei Internetnutzer noch nach Tagen (bis zu sieben Tage lang) ermitteln, und zwar „für die Aufklärung aller Straftaten“, selbst bei Verdacht von Bagatelldelikten wie Beleidigung oder Filesharing, und zwar ohne richterliche Prüfung oder Genehmigung. Zulässig wäre auch ein präventiver Datenzugriff ohne Tatverdacht, Zugriffe durch Geheimdienste (§ 113 TKG) und eine Namhaftmachung gegenüber Abmahnanwälten (§ 101 UrhG). Selbst an 29 ausländische Staaten einschließlich der USA wären die Daten auf Anfrage herauszugeben.

Mit einer Zustimmung zu diesem Vorschlag würde die FDP ihr Wort brechen, das sie vor der Bundestagswahl in ihrem Wahlprogramm gegeben und in vielen späteren Beschlüssen und Aussagen stets wiederholt hatte: „Die anlass- und verdachtsunabhängige Vorratsdatenspeicherung hat die FDP von Anfang an abgelehnt“^[1] und: „Der Rechtsgrundsatz, dass 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, muss auch im digitalen Raum gelten. Wir lehnen daher die verdachts- und anlassunabhängige Speicherung personenbezogener Daten auf Vorrat ab.“^[2]

Die Vorratsdatenspeicherung steht auf der Tagesordnung der Sitzung des Koalitionsausschusses im Kanzleramt am heutigen Abend. FDP-Spitzenpolitiker sind bislang bereit, einen Kompromiss mit CDU und CSU auszuhandeln. Die Union will in den Verhandlungen sogar noch eine sehr viel weiter reichende Vorratsprotokollierung auch unserer Telefon-, Handy-, E-Mail- und Anonymisierungsdienstnutzung für eine Dauer von sechs Monaten durchsetzen. Was als Ergebnis beschlossen würde, ist offen; der AK Vorrat befürchtet das Schlimmste. Die innenpolitische Sprecherin der FDP Gisela Piltz erklärte am Dienstag, rote Linie bei den Verhandlungen sei lediglich die „Einhaltung der Kernaussagen des Bundesverfassungsgerichts“, wonach bekanntlich eine sechsmonatige Vorratsspeicherung von Telefon-, Handy-, E-Mail-, Internet- und Anonymisierungsdienstnutzung mit dem Grundgesetz vereinbar sei. Auch die Bundesjustizministerin will sich auf einen „Kompromiss“ mit CDU/CSU einlassen und ist bereit, über „Fristen“ und „die einzelnen Punkte“ zu sprechen.

Vor diesem Hintergrund sollen heute zahlreiche Telefonanrufe die FDP-Bundestagsabgeordneten an ihre Zusage erinnern, jede „anlassunabhängige Speicherung personenbezogener Daten auf Vorrat“ abzulehnen. Im AK Vorrat-Wiki gibt es dazu eine **Liste der Telefonnummern der Abgeordneten der FDP-Fraktion** und eine **Handreichung für das Gespräch mit den**

Abgeordneten. Wenn nur 21 der 93 FDP-Abgeordneten überzeugt werden, Wort zu halten, ist jeder Kompromiss blockiert, weil laut Koalitionsvertrag „wechselnde Mehrheiten ausgeschlossen“ sind. Jeder kann an dieser Aktion teilnehmen und mithelfen!

Die Aktionsseite im AK Vorrat-Wiki lautet:

http://wiki.vorratsdatenspeicherung.de/Wort_halten_FDP



Uns ist die Beschwerdeschrift zugespielt worden, mit der Frau Leutheusser-Schnarrenberger (FDP-Bundesjustizministerin), Frau Piltz (FDP-MdB), Herr Vogel (FDP-MdB), Herr Dr. Solms (FDP-MdB) und andere FDP-Größen vor drei Jahren gegen die Vorratsdatenspeicherung vor das Bundesverfassungsgericht gezogen sind. Und siehe da - die jetzt von Frau Leutheusser-Schnarrenberger vorgeschlagene flächendeckende Erfassung aller Internetverbindungen auf Vorrat wäre damals als "unverhältnismäßig" und gar als Verstoß gegen die Würde des Menschen eingestuft worden.

Der folgende Text ist wörtlich aus Aussagen der **FDP-Beschwerdeschrift** zusammen gestellt - und liest sich wie ein Plädoyer gegen das aktuelle "**Kompromissangebot**" der FDP-Bundesjustizministerin:

- *Bei Kontakten über das Internet werden die dynamischen IP-Adressen gespeichert, unter denen der Nutzer im Netz "surft" und die es u. U. ermöglichen, die vom Nutzer im Internet aufgerufene Seite zu ermitteln. Die Neuregelung weitet auch den Umfang der bisher gespeicherten Daten erheblich aus, auf die der Staat zugreifen möchte. Dazu gehören die Telekommunikationsdaten der Internet-Dienste und die Verbindungsdaten über prepaid-Karten oder die mit einer Pauschale - Flatrate - bezahlt werden. **Dabei sollen nun aber zu den zu übermittelnden Bestandsdaten auch die dynamisch auf Zeit zugeteilten IP-Adressen gehören, mit denen man die Kommunikationsverbindungen der Internetnutzer im einzelnen nachvollziehen kann.***
- *Die angefochtene Neuregelung ist keine Kleinigkeit einer bloß geringfügigen Erweiterung ohnehin schon bestehender Kontrollmöglichkeiten. **Sie ist eine prinzipielle Veränderung, die weitere Folgen und Forderungen nach sich ziehen wird, wenn sie erst einmal verwirklicht worden ist.** Das hat schon angefangen. So hat der Bundesrat bei der Einbringung und der Zustimmung zum Gesetz am 30. 11. 2007 auf Vorschlag seines Rechtsausschusses gefordert, auch zivilrechtliche Auskunftsrechte gegenüber Internet-Providern zur Durchsetzung urheberrechtlicher Ansprüche einzuführen, eine Forderung, die die Bundesregierung wegen der „beachtlichen Gründe für bedenkenswert“ gehalten hat. Zweifellos werden sich alsbald weitere Anliegen für eine Überwachung und Nutzung der doch ohnehin schon gespeicherten, also verfügbaren Daten finden.*
- ***Der entscheidende Unterschied liegt eben darin, daß die Speicherung selbst als gegeben und [...] streitlos gestellt erscheint, sodaß dann nur noch über Details einer weiteren Anwendung der Datensammlung entschieden werden wird.***
- *Der bisher in § 3 a BDSG verankerte Grundsatz, Datensammlungen möglichst zu vermeiden, wird in sein Gegenteil verkehrt. **Die entscheidende Veränderung, die das angefochtene Gesetz bewirkt, liegt darin, daß jeder Einwohner als potentieller Straftäter, Gefährder oder Extremist behandelt wird.** Die Neuregelung trifft jeden Nutzer der Telekommunikation, also jeden Bürger, der an ihr und damit an der Gesellschaft teilnehmen möchte, die von ihr geprägt wird.*
- ***Die Vorratsdatenspeicherung stellt jeden Einwohner der Republik unter potentiellen Verdacht.** Sonst wäre sie sinnlos. Man legt sich einen Vorrat nicht aus Spaß an, sondern weil man ihn nutzen will. Der Nutzer weiß bei jedem elektronisch vermittelten Kontakt mit anderen oder bei jedem Aufruf des Internet, daß seine Daten zusammengeführt und gespeichert werden, auch wenn dafür nicht die geringste Veranlassung besteht. Er kann dieser Speicherung nicht ausweichen, ohne besondere konspirative Vorkehrungen zu treffen.*
- *Die massiven öffentlichen Reaktionen auf dieses Gesetz zeigen, daß vielen Nutzern das keineswegs gleichgültig ist und ihr Kommunikationsverhalten verändern kann - und das aus guten und nachvollziehbaren Gründen. Denn niemand kann wissen, wer die Verbindungsdaten schließlich zur Kenntnis bekommt und ob sich aus den jeweiligen privaten, beruflichen oder politischen Kontakten Schlüsse auf den Inhalt der Kommunikation ergeben, die zu irgendwelchen nachteiligen beruflichen, politischen oder persönlichen Folgen führen könnten. Jede freie Kommunikation steht und fällt mit der Überzeugung, selbst bestimmen zu können, ob sie vertraulich bleibt oder nicht. **Wenn der Staat in die Möglichkeit einer freien Kommunikation ohne zwingenden Grund eingreift, dann zerstört er eine der wesentlichsten Grundlagen einer freien und demokratischen Gesellschaft.***
- ***Es gibt keine freie Gesellschaft ohne das Vertrauen des Bürgers in eine vertrauliche Kommunikation,** bei der er weiß oder selbst bestimmen kann, wer von ihr Kenntnis erlangt. Dem Bürger muß ein Kernbereich der persönlichen Lebensführung belassen bleiben, in dem er das Recht hat und darauf vertrauen kann, von staatlicher*

Beobachtung, Kontrolle oder Beeinflussung frei zu sein und zu bleiben. Das gilt auch dann, wenn er kritische, unliebsame Gedanken hat und äußern will, so lange es nicht darum geht, eine konkrete Straftat vorzubereiten, zu verabreden oder zu begehen. Es ist das Wesen einer freien Gesellschaft, daß der unbefangene Austausch von Gedanken möglich sein muß und der Bürger auf eine solche staatsfreie Kommunikation vertrauen kann. Dieses Recht wird nicht im Interesse eigenbrötlerischer Individualisten gefordert. Es ist die unverzichtbare Grundlage einer freien Gesellschaft, die ohne ein solches Recht in ihrer Gesamtheit und in ihrem Kern verändert wird.

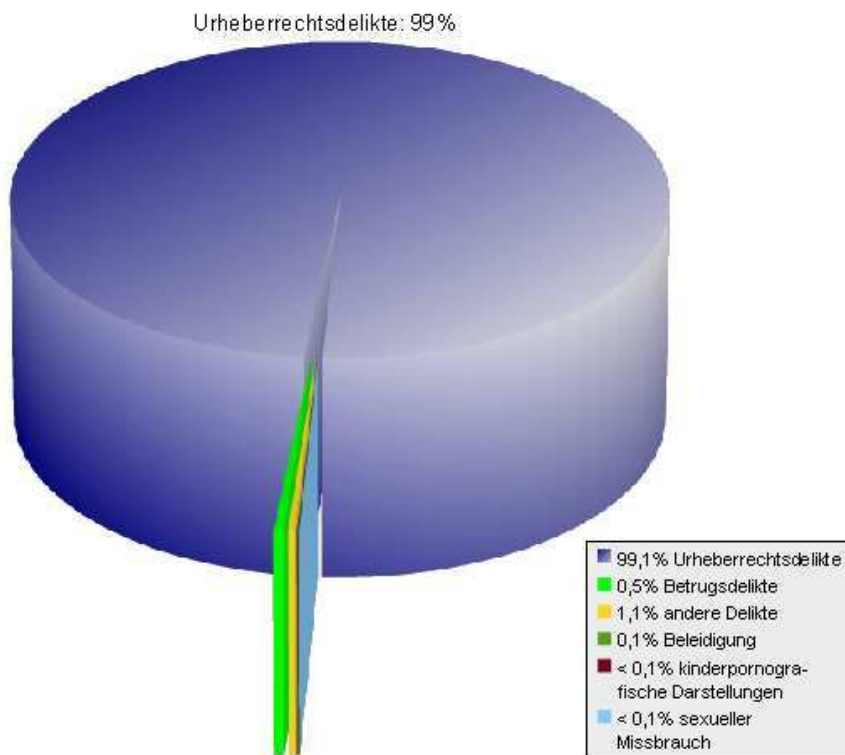
- **Der Staat muß den seinem Schutz anvertrauten Bürger in seiner Würde ernst nehmen.** Er darf ihn nicht als bloßes Objekt und nicht wie einen potentiellen Straftäter behandeln, als ein im Prinzip gefährliches Objekt, das unabhängig von individuellem Handeln allein schon durch seine Existenz gefährlich ist und daher vorsorglich - sozusagen auf Vorrat - überwacht und kontrolliert werden sollte.
- **Der Bürger ist nicht schon dadurch gefährlich und polizeipflichtig, daß er mit anderen Menschen kommuniziert und daß er sich dafür auch technischer Hilfsmittel bedient, eines Telefons, eines Handys oder eines Computers, den er ans Internet anschließt.** In einer freien Gesellschaft können das keine Anknüpfungspunkte für staatliches Handeln und staatliche Kontrolle sein.
- Schließlich ist die Verhältnismäßigkeit dieses Eingriffs nicht gegeben. **Denn die Tiefe des Eingriffs steht in keinem Verhältnis zu dem durch ihn erzielten Nutzen.**
- Im übrigen weise [laut Max-Planck-Institut] „die Aktenanalyse selbst unter den heutigen (d.h. den bisherigen) rechtlichen Bedingungen nur für etwa 2 % der Abfragen nach, daß sie wegen Löschungen ins Leere gehen“, sich also auf Daten richteten, die vom Provider nicht oder nicht mehr benötigt wurden. **Man kann aus dieser Aussage erkennen, daß sich aus einer Speicherung, die über die heute geregelte hinausgeht, kein nennenswerter zusätzlicher Gewinn für die Kriminalitätsbekämpfung ergeben wird.**
- Es ist zwar zutreffend, daß sich die Mittel der elektronischen Kommunikation in den letzten zwanzig Jahren dramatisch verbreitet haben und daß sie ebenso wie andere Mittel auch zur - generell und tendentiell sinkenden - Kriminalität benutzt werden. Es ist auch richtig, daß Strafverfolgungsbehörden und Polizei bei der Bekämpfung schwerer Kriminalität die Möglichkeit haben müssen, mutmaßliche Straftäter auch über die Nutzung der Kommunikation zu ermitteln und zu überführen. **Aber es ist in einer freien und demokratisch verfaßten Gesellschaft undenkbar und nicht hinnehmbar, daß jedes Kommunikationsmittel wie ein gefährliches Werkzeug überwacht und jeder Bürger, der ein solches gefährliches Werkzeug besitzt, wie ein potentieller Straftäter in seiner Kommunikation [...] vorsorglich verdatet und gespeichert wird.**
- **Es verstößt gegen den rechtlichen Grundkonsens unserer Gesellschaft, wenn der Staat ohne jeden Unterschied und ohne jede äußere Veranlassung jeden Kontakt der beschriebenen Art vorsorglich erfaßt und verdatet.** Er ermittelt nicht nur "ins Blaue" hinein, sondern er richtet eine Infrastruktur ein, die das Vertrauen der Bürger in eine freie Kommunikation zerstört und zukünftig schon bei minimalen Veränderungen der Zugriffsberechtigungen, der Zweckbestimmungen oder der Speicherdauer weitere maximale Überwachungen ermöglichen wird.
- Das Grundrecht aus Art. 1 GG wird damit bereits durch die anlaßlose Speicherung der Kommunikationsdaten verletzt. **Diese auf Dauer angelegte Regelung verstößt gegen die in Art. 1 und 20 GG niedergelegten Grundsätze der Menschenwürde und eines demokratischen Rechtsstaats.**

Internet-Vorratsdatenspeicherung gegen Kinderpornografie nutzlos (25.01.2011)



Nach dem "Kompromissvorschlag" von Bundesjustizministerin Leutheusser-Schnarrenberger zur Vorratsdatenspeicherung soll künftig für jede unserer Internetverbindungen auf Vorrat gespeichert werden, wer wann mit welcher IP-Adresse im Netz gesurft, publiziert oder gemailt hat, um "insbesondere zum Vorgehen gegen Kinderpornografie solche Bestandsdatenauskünfte zu **ermöglichen**". Eine **Berechnung (pdf)** des AK Vorrat zeigt nun aber, dass Auskünfte über Internetnutzer kaum einmal der Verfolgung des Besitzes kinderpornografischer Darstellungen dienen, sondern zu einem Anteil von über 95% der Abmahnung von Urheberrechtsvergehen (z.B. Tauschbörsennutzung). Allein die Deutsche Telekom AG legte zu diesem Zweck gegenüber privaten Rechteinhabern 2009 die Identität von 2,7 Mio. Internetnutzern offen.

Anlässe für Auskünfte über Internetnutzer (IP-Adressen)



Nach dem Vorschlag der Bundesjustizministerin sollen private Rechteinhaber zwar wohl keinen direkten Zugriff auf vorratsgespeicherte IP-Adressen erhalten. Sie könnten aber Strafanzeige erstatten und durch anschließende Akteneinsicht die Zuordnung der IP-Adresse in Erfahrung bringen.

Die Bundesjustizministerin hat bei der **Pressekonferenz** zur Vorratsdatenspeicherung in der vergangenen Woche erklärt, ihr Vorstoß zur Einführung einer Internet-Vorratsdatenspeicherung beziehe sich "gerade auf mögliche Straftaten im Zusammenhang mit Kinderpornografie. Die Fachleute sagen, 80% der Daten, die da immer so gerne benutzt werden wollen, beziehen sich genau hierauf, nämlich auf Vorgehen gegen Kinderpornografie." Die Zahl von 80% stammt allerdings aus einem **umstrittenen Bericht** des Bundeskriminalamts und ist nicht korrekt, weil die BKA-Untersuchung nur einen sehr kleinen und nicht repräsentativ ausgewählten Teil der Ermittlungsverfahren mit Internetbezug im Untersuchungszeitraum zum Gegenstand hatte.

Eine korrekte Gesamtbetrachtung zeigt: An staatliche Behörden erteilte Auskünfte über Internetnutzer **dienen** zu 54% Ermittlungen wegen Betrugs und zu 6% Ermittlungen wegen Beleidigung. Nur 3% der Auskünfte an staatliche Stellen werden zur Verfolgung des Besitzes kinderpornografischer Darstellungen erteilt. Ermittlungen wegen mutmaßlichen Besitzes kinderpornografischer Darstellungen waren aber schon im Jahr 2008 ohne Internet-Vorratsdatenspeicherung zu **87,5%** erfolgreich - weit häufiger als sonstige Ermittlungsverfahren (durchschnittliche Aufklärungsquote 2008: **54,8%**). Nach Inkrafttreten einer Internet-

Vorratsdatenspeicherung im Jahr 2009 erhöhte sich die hohe Aufklärungsquote im Bereich kinderpornografischer Darstellungen nicht, sondern sie fiel um 3,7% auf **83,8%** ab.

Eine Vorratsdatenspeicherung senkt die Aufklärungsquote erfahrungsgemäß, weil sie Straftäter zur verstärkten Nutzung von Verschleierungstechniken und anderen Kanälen veranlasst. Nach Einführung der Internet-Vorratsdatenspeicherung im Jahr 2009 gaben bereits **46,4%** der Bürgerinnen und Bürger an, bei der Internetnutzung einen Anonymisierungsdienst zu benutzen oder benutzen zu wollen. Wer die Ermittlung von Besitzern kinderpornografischer Darstellungen erleichtern will, muss deswegen eine Vorratsdatenspeicherung gerade ablehnen, die ohnehin gerade im Internetbereich durch einfache und kostengünstige Mittel jederzeit problemlos umgangen werden kann.

Untersuchung: Vorratsdatenspeicherung ist ineffektiv (26.01.2011)



Einer heute veröffentlichten **Untersuchung** der deutschen polizeilichen Kriminalstatistik zufolge ist eine Vorratsspeicherung von Telekommunikationsdaten bei der Verfolgung schwerer Straftaten nicht von Nutzen.

Eine EU-Richtlinie aus dem Jahr 2006 sieht vor, dass Telekommunikationsunternehmen verpflichtet werden sollen, Informationen über die Verbindungen ihrer sämtlichen Kunden aufzubewahren, um die "Ermittlung, Feststellung und Verfolgung von schweren Straftaten, wie sie von jedem Mitgliedstaat in seinem nationalen Recht bestimmt werden", zu erleichtern. Deutschland setzte die Richtlinie mit Wirkung ab 2008 um. Nach einer einstweiligen Anordnung des Bundesverfassungsgerichts konnten Strafverfolger auf Vorrat gespeicherte Verbindungsdaten für Ermittlungen wegen schwerer Straftaten abrufen. Ferner konnten sie zur Aufklärung jeglicher Straftat Internetnutzer mithilfe von Vorratsdaten identifizieren lassen. 2010 hob das Bundesverfassungsgericht die deutschen Regelungen zur Vorratsdatenspeicherung auf, weil sie unverhältnismäßig tief in die Grundrechte eingriffen.

Eine heute vom Arbeitskreis Vorratsdatenspeicherung veröffentlichte Analyse^[1] der einschlägigen Tatbestände der polizeilichen Kriminalstatistik des Bundeskriminalamts offenbart nun, dass die Vorratsdatenspeicherung, solange sie in Kraft war, die Aufklärung schwerer Straftaten nicht verbesserte. So registrierte die Polizei in der Zeit der Vorratsdatenspeicherung mehr schwere Straftaten (2009: 1.422.968) als zuvor (2007: 1.359.102), die zudem seltener aufgeklärt wurden (2009: 76.3%) als noch vor Beginn der anlasslosen Kommunikationsprotokollierung (2007: 77.6%). Als 2009 auch Internetdaten auf Vorrat gespeichert werden mussten, stieg die Zahl der registrierten Internetstraftaten von 167.451 im Jahr 2008 auf 206.909 im Jahr 2009 stark an, während die Aufklärungsrate bei Internetstraftaten von 79,8% im Jahr 2008 auf 75,7% im Jahr 2009 zurückging.

Dem AK Vorrat zufolge lassen sich diese kontraproduktive Wirkungen einer Vorratsdatenspeicherung mit Verhaltensanpassungen erklären. Um der ausufernden Erfassung sensibler Kommunikationsdaten zu entgehen, werden unter Geltung einer Vorratsdatenspeicherung verstärkt Internetcafés, öffentliche WLAN-Zugänge, Anonymisierungsdienste, öffentliche Telefone und nicht-elektronische Kommunikation genutzt. Solche Vermeidungsmaßnahmen können nicht nur Vorratsdaten die Aussagekraft nehmen, sondern zugleich gezielte Überwachungsmaßnahmen vereiteln, wie sie ohne Vorratsdatenspeicherung noch möglich gewesen wären. Insgesamt kann eine Vorratsdatenspeicherung dadurch der Verfolgung von Straftaten abträglich sein, indem sie einige Ermittlungen erleichtert, weit mehr Ermittlungen aber vereitelt.

Da die Europäische Kommission derzeit die Richtlinie zur Vorratsdatenspeicherung evaluiert, fordern über 100 europäische Bürgerrechts-, Datenschutz- und Menschenrechtsorganisationen ebenso wie Telefonseelsorge- und Notrufvereine, Berufsverbände, Gewerkschaften, Verbraucherzentralen und Wirtschaftsverbände von der EU-Kommission, "die Aufhebung der EU-Vorgaben zur Vorratsdatenspeicherung zugunsten eines Systems zur schnellen Sicherstellung und gezielten Aufzeichnung von Verkehrsdaten vorzuschlagen".^[2] Das deutsche Beispiel beweist, dass solche gezielten Ermittlungen insgesamt effektiver sein können als wahllos Daten über das Kommunikations-, Bewegungs- und Internetnutzungsverhalten der gesamten Bevölkerung anzuhäufen. In mehreren EU-Staaten wird die Verhältnismäßigkeit der Vorratsdatenspeicherung zurzeit vor Gericht angefochten. Der Europäische Gerichtshof wird dazu voraussichtlich 2012 eine Entscheidung fällen.

Unterstützung erhalten die Kritiker der EU-Richtlinie nun auch von der deutschen Bundesjustizministerin Sabine Leutheusser-Schnarrenberger, die sich ebenfalls für eine Änderung der Richtlinie dahin ausgesprochen hat, dass Daten nur noch in konkreten Verdachtsfällen gespeichert werden. Leutheusser-Schnarrenberger sagte auf einer Pressekonferenz vergangene Woche: "Es haben sechs Mitgliedsstaaten insgesamt diese Richtlinie seit Inkrafttreten nicht umgesetzt. Damit ist die Kommission ein Stück weit gescheitert in ihrem Vorhaben, innerhalb der Europäischen Union einheitliche Standards zu Wettbewerbszwecken zu bekommen, denn das ist ja die Grundlage dafür gewesen, dass diese Richtlinie überhaupt verabschiedet werden konnte. Sie ist nicht auf der Grundlage der dritten Säule zu Zwecken der Strafverfolgung verabschiedet worden, weil es dazu keine Einstimmigkeit gegeben hat. Und deshalb muss die Kommission ein ganz großes Interesse daran haben, bei der Evaluierung zu sehen, wie man den Mitgliedsstaaten mehr Spielräume eröffnen kann. Denn sechs Staaten haben die Richtlinie nicht umgesetzt,

Schweden und Österreich sind schon zweimal verurteilt worden. [...] Dies zeigt, dass das nicht ein Erfolgsprojekt der Europäischen Kommission und der Europäischen Union ist."^[3]

Justiz-Staatssekretär Dr. Max Stadler bekräftigte nach einem informellen Treffen der Europäischen Justiz- und Innenminister letzte Woche: "Zum Schutz der Grundrechte gehört es auch, dass wir bei Maßnahmen der Strafverfolgung nur so weit in die Privatsphäre der Bürgerinnen und Bürger eingreifen, als es unbedingt erforderlich ist. Die derzeitige EU-Richtlinie zur Vorratsdatenspeicherung geht unserer Meinung nach über dieses Ziel hinaus.

Selbstverständlich brauchen Strafverfolgungsbehörden Daten, um Beweise zu erheben.

Deswegen ist es in einem bestimmten Umfang gerechtfertigt, wenn Telekommunikationsdaten gespeichert werden, aber unserer Meinung nach nicht ohne Anlass. Es ist sehr erfreulich, dass Justizkommissarin Viviane Reding diesen Vorschlag der deutschen Bundesjustizministerin [zur Einführung eines Quick-Freeze-Verfahrens] als 'vielversprechenden Lösungsansatz' bezeichnet hat."^[4]

Registrierte schwere Straftaten in Deutschland

Quelle: Kriminalstatistik des Bundeskriminalamts

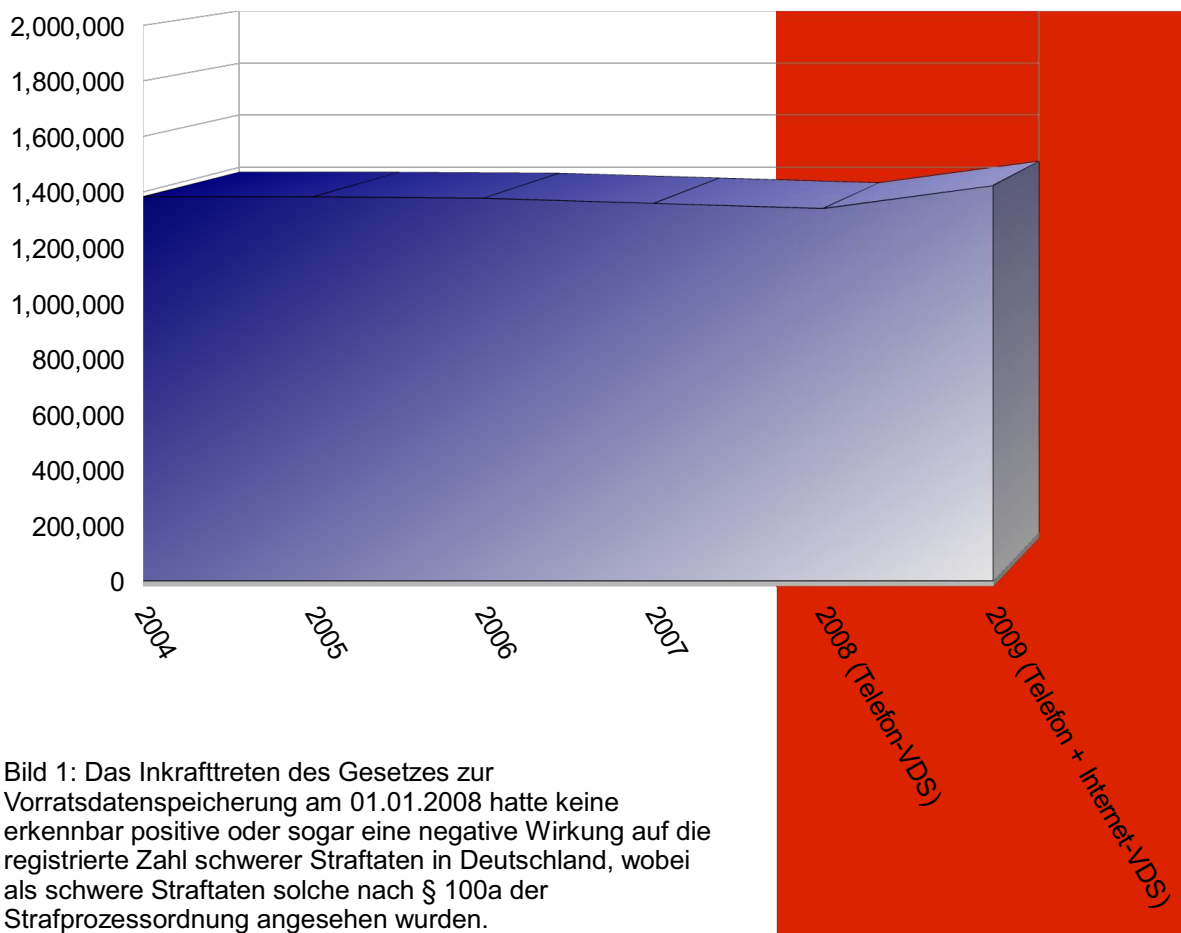


Bild 1: Das Inkrafttreten des Gesetzes zur Vorratsdatenspeicherung am 01.01.2008 hatte keine erkennbar positive oder sogar eine negative Wirkung auf die registrierte Zahl schwerer Straftaten in Deutschland, wobei als schwere Straftaten solche nach § 100a der Strafprozessordnung angesehen wurden.

Jahr	Registrierte schwere Straftaten	Vorratsdaten-speicherung
2004	1.382.118	keine
2005	1.381.750	keine
2006	1.377.824	keine
2007	1.359.102	keine
2008	1.340.560	Telefondaten-speicherung
2009	1.422.968	Telefon- und Internetdaten-speicherung
2010	nicht bekannt	keine seit 02.03.2010

Aufklärung schwerer Straftaten in Deutschland

Quelle: Kriminalstatistik des Bundeskriminalamts

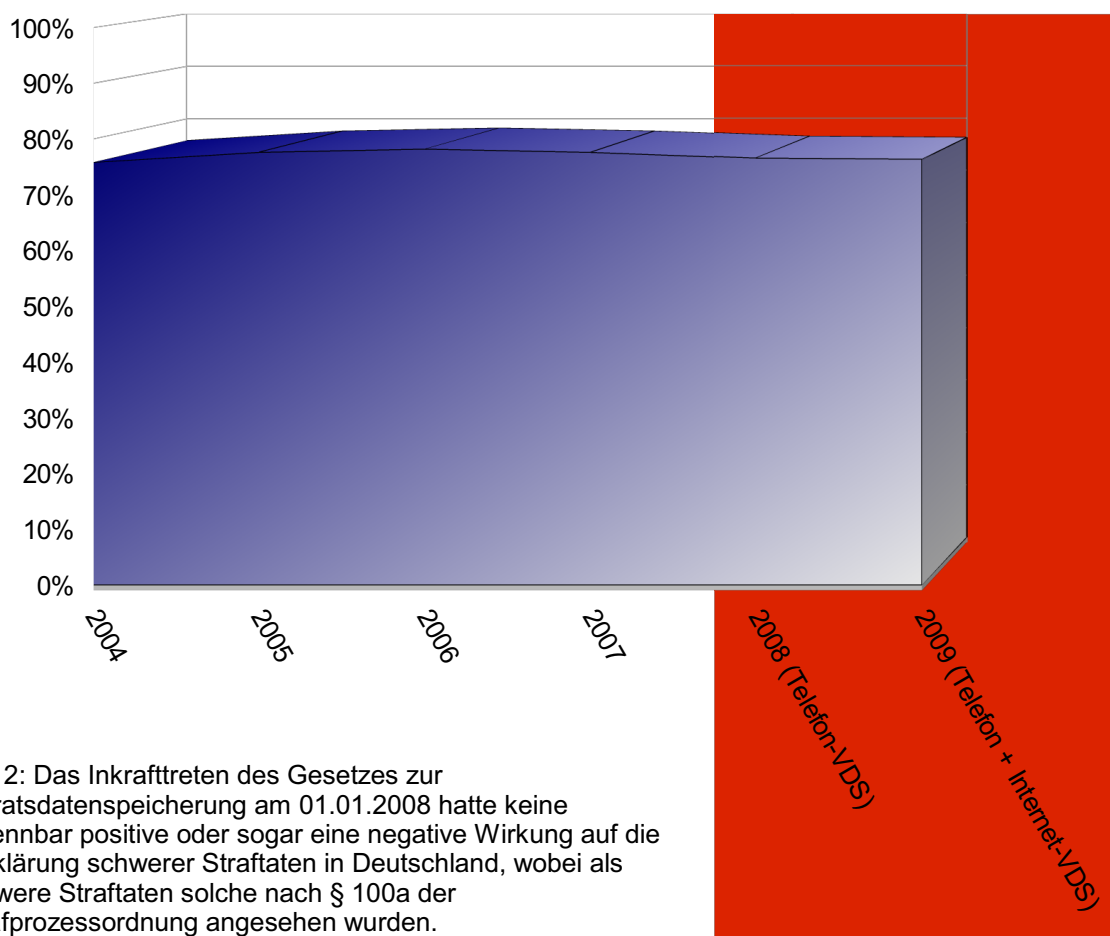


Bild 2: Das Inkrafttreten des Gesetzes zur Vorratsdatenspeicherung am 01.01.2008 hatte keine erkennbar positive oder sogar eine negative Wirkung auf die Aufklärung schwerer Straftaten in Deutschland, wobei als schwere Straftaten solche nach § 100a der Strafprozessordnung angesehen wurden.

Jahr	Aufklärungs- quote schwerer Straftaten	Vorratsdaten- speicherung
2004	75,8%	keine
2005	77,6%	keine
2006	78,2%	keine
2007	77,6%	keine
2008	76,5%	Telefondaten- speicherung
2009	76,3%	Telefon- und Internetdaten- speicherung
2010	nicht bekannt	keine seit 02.03.2010

Registrierte Internet-Straftaten in Deutschland

Quelle: Kriminalstatistik des Bundeskriminalamts

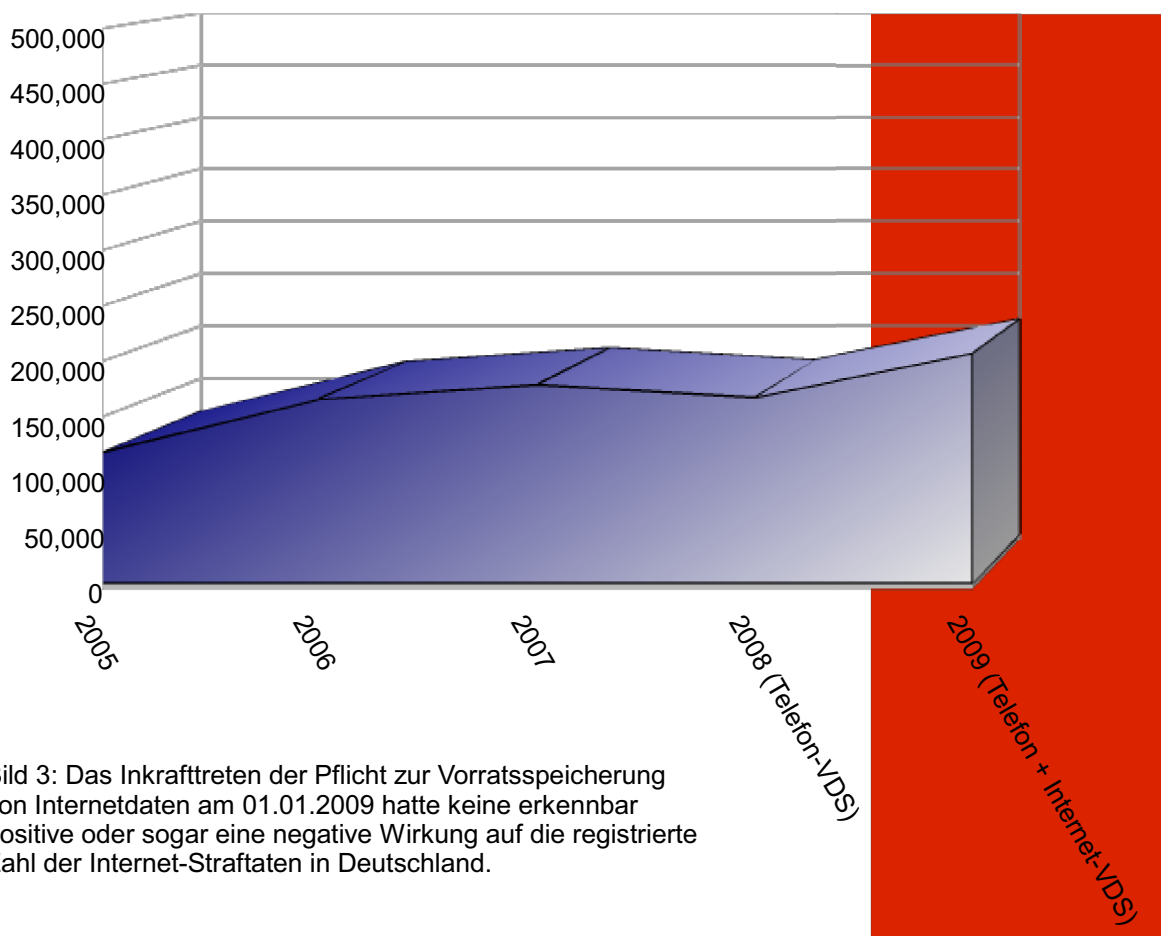


Bild 3: Das Inkrafttreten der Pflicht zur Vorratsspeicherung von Internetdaten am 01.01.2009 hatte keine erkennbar positive oder sogar eine negative Wirkung auf die registrierte Zahl der Internet-Straftaten in Deutschland.

Jahr	Registrierte Internet-Straftaten	Internet-Vorratsdatenspeicherung
2005	118.036	keine
2006	165.720	keine
2007	179.026	keine
2008	167.451	keine
2009	206.909	Internet-Vorratsdatenspeicherung
2010	nicht bekannt	keine seit 02.03.2010

Aufklärung von Internet-Straftaten in Deutschland

Quelle: Kriminalstatistik des Bundeskriminalamts

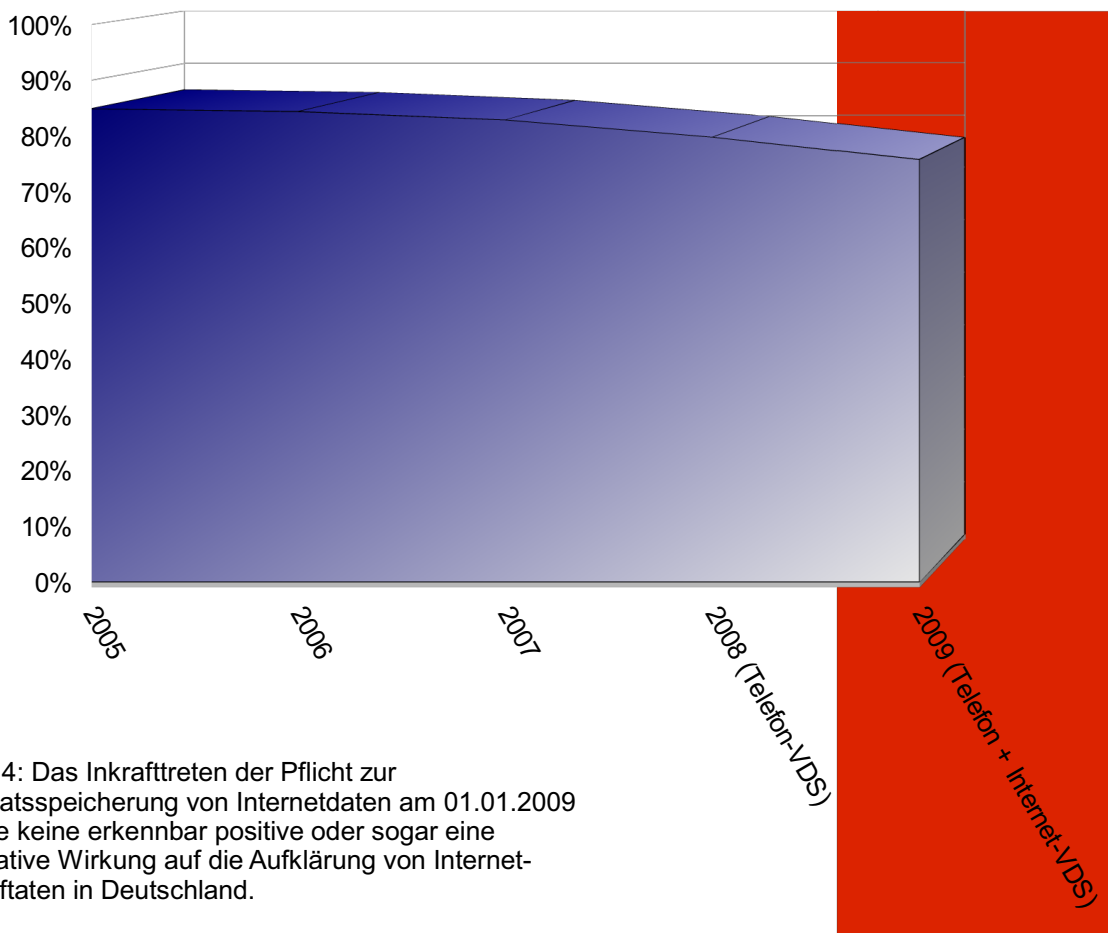


Bild 4: Das Inkrafttreten der Pflicht zur Vorratsspeicherung von Internetdaten am 01.01.2009 hatte keine erkennbar positive oder sogar eine negative Wirkung auf die Aufklärung von Internet-Straftaten in Deutschland.

Jahr	Aufklärungsquote von Internet-Straftaten	Internet-Vorratsdatenspeicherung
2005	84,9%	keine
2006	84,4%	keine
2007	82,9%	keine
2008	79,8%	keine
2009	75,7%	Internet-Vorratsdatenspeicherung
2010	nicht bekannt	keine seit 02.03.2010

Note: While data retention was in effect in Germany, retained data could be used for the prosecution of serious crime and for the identification of suspects of Internet crime.

Vorratsdatenspeicherung: Die Kinderporno-Lüge (31.01.2011)



Das Bundesjustizministerium will wegen vermeintlicher Lücken beim Vorgehen gegen Kinderpornografie im Internet eine Vorratsdatenspeicherung. Doch von 1.000 nicht aufgeklärten Straftaten handelt es sich bei weniger als einer um Kinderpornografie im Internet.

Nach einem "**Kompromissvorschlag**" von Bundesjustizministerin Leutheusser-Schnarrenberger zur Vorratsdatenspeicherung soll künftig für jede unserer Internetverbindungen auf Vorrat gespeichert werden, wer wann mit welcher IP-Adresse im Netz gesurft, publiziert oder gemailt hat, um "*insbesondere zum Vorgehen gegen Kinderpornografie solche Bestandsdatenauskünfte zu ermöglichen*". Die Bundesjustizministerin **erklärte**, ihr Vorstoß beziehe sich "*gerade auf mögliche Straftaten im Zusammenhang mit Kinderpornografie. Die Fachleute sagen, 80% der Daten, die da immer so gerne benutzt werden wollen, beziehen sich genau hierauf, nämlich auf Vorgehen gegen Kinderpornografie.*"

Ein Blick in die einschlägigen Statistiken ergibt allerdings ein vollkommen anderes **Bild**:

- Von 1.000 polizeilich bekannten aber nicht aufgeklärten Straftaten handelt es sich bei weniger als einer um Verbreitung oder Verschaffung von Kinderpornografie im Internet (unter 0,1%).
- Nicht einmal jede 50. polizeilich bekannte aber nicht aufgeklärte Straftat wird überhaupt im Internet begangen (unter 2%).
- Auskünfte über Internetnutzer (IP-Adressen) werden fast ausschließlich (zu 95,4%) an private Rechteinhaber zur Abmahnung von Urheberrechtsverstößen und nur zu einem geringen Bruchteil (0,1%) für strafrechtliche Ermittlungen wegen Austauschs kinderpornografischer Darstellungen im Internet erteilt.
- Im Internet begangene Straftaten werden zu einem weit höheren Anteil (2009: 76%) aufgeklärt als Straftaten allgemein (2009: 56%). Dies gilt auch für die Verbreitung kinderpornografischer Darstellungen im Internet (Aufklärungsquote 2009: 84%).
- Vor Inkrafttreten der Internet-Vorratsdatenspeicherung zum 01.01.2009 war die Aufklärungsrate bei Internetdelikten höher (2008: 80%) als unter Geltung der Internet-Vorratsdatenspeicherung (2009: 76%).

Insgesamt zeigt sich: Es gibt auch ohne Vorratsspeicherung von Internetadressen keine signifikante Aufklärungslücke im Internet, schon gar nicht bei Ermittlungen wegen Kinderpornografie im Internet. Umgekehrt werden Internetdelikte häufiger aufgeklärt als außerhalb des Internet begangene Straftaten.

Die vom Justizministerium offenbar übernommene Behauptung des Bundeskriminalamts, **72,82%** nicht beantworteter Auskunftersuchen beträfe "die Straftatbestände Verbreitung, Erwerb oder Besitz kinder- und jugendpornographischer Schriften", ist auf abenteuerliche Art und Weise zustande gekommen: Beispielsweise lagen 209 der vom BKA ergebnislos angefragten Internetverbindungen länger als 10 Tage zurück, die Anfragen waren wegen der dem BKA bekannten, kürzeren Speicherfristen der Provider von vornherein sinnlos. 147 weitere angefragte Internetverbindungen lagen sogar länger als sechs Monate in der Vergangenheit! Auf Nachfrage **teilte** uns das Bundesinnenministerium mit, dort sei nicht bekannt, ob das Bundeskriminalamt die öffentlich beklagte Zahl erfolgloser Verbindungsdatenabfragen durch erkennbar aussichtslose Ersuchen in die Höhe getrieben habe. Nach einer ausführlichen **Analyse** unsererseits sind die BKA-Zahlen "irrelevant" und belegen "keine blinde Flecken in der Verbrechensbekämpfung oder Schutzlücken". Auch Dr. Michael Kilchling vom Max-Planck-Institut für ausländisches und internationales Strafrecht in Freiburg **kritisierte**: "Für eine seriöse wissenschaftliche Stellungnahme fehlt jede Basis". Dennoch ist ausgerechnet die Bundesjustizministerin dem unhaltbaren, vom Bundesinnenminister im Rahmen einer politischen **Kampagne** in Auftrag gegebenen BKA-Bericht aufgesessen.

Weiter heißt es in dem **Eckpunktepapier** des Bundesjustizministeriums zur Rechtfertigung der vorgeschlagenen Internet-Vorratsdatenspeicherung, die Zuordnung von IP-Adressen ermöglichen "die Erstellung aussagekräftiger Persönlichkeits- und Bewegungsprofile praktisch jeden Bürgers" nicht. Tatsächlich ist genau dies der Fall: 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.).

Internetdienste im In- und Ausland protokollieren verbreitet jeden unserer Klicks und jede unserer Eingaben auf Vorrat. Das Bundesverfassungsgericht **meinte** 2010 noch, eine Internet-Vorratsdatenspeicherung laufe nicht darauf hinaus, "eine allgemein umfassende Datensammlung zur weitestmöglichen Rekonstruierbarkeit jedweder Aktivitäten der Bürger zu schaffen", weil das deutsche Telemediengesetz verhindere, "dass die Internetnutzung inhaltlich in allgemeinen kommerziellen Datensammlungen festgehalten wird und damit rekonstruierbar bleibt." Das Gericht übersah dabei aber, dass ein deutsches Gesetz für die größten Diensteanbieter im Internet mit Sitz im Ausland von vornherein nicht gilt. Allein Google speichert jeden unserer Klicks **neun Monate** lang auf Vorrat und gibt **jeden Tag dreimal** solche Surfprotokolle an deutsche Behörden heraus – ohne richterliche Anordnung, auch präventiv und selbst an Nachrichtendienste. Vor dem Hintergrund solcher Surfprotokolle ist es gerade die Zuordnung der genutzten IP-Adresse, die Polizei und Geheimdiensten die "Erstellung aussagekräftiger Persönlichkeitsprofile" über uns **ermöglicht**. Aus der IP-Adresse lässt sich auch der Aufenthaltsort ableiten - **neuerdings** sogar, ob man von zuhause, auf der Arbeit oder unterwegs surft.

Das Bundesjustizministerium schreibt schließlich, das vom Bundesverfassungsgericht anerkannte "diffus bedrohliche Gefühl des Beobachtetseins" entstehe bei einer Internet-Vorratsspeicherung nicht. Tatsächlich kündigten 2009 aber schon **46%** der Bürger an, einen Anonymisierungsdienst zu nutzen oder nutzen zu wollen – ganz ohne Sorge vor Beobachtung? Nach Inkrafttreten der Vorratsdatenspeicherung wurde uns **berichtet**, politische Themen würden in Chats und Internetforen gemieden, intime Themen nicht mehr recherchiert, E-Mails nur noch zurückhaltend versandt. Eine Internetnutzerin schrieb: *"Letztes Jahr habe ich einige Hilfeseiten von Missbrauchsoffern umgesehen und mir hier und da Rat und Hilfe gesucht, auch konnte ich sicher sein, dass meine Geschichte zu meiner realen Person nicht zugeordnet werden konnte. Bei dem Gedanken, dass jemand über meine IP dann meinen Namen meine Adresse und meine Geschichte haben könnte, wird mir ziemlich übel. Deshalb habe ich mich aus diversen Foren und Chats zurück gezogen und somit leider auch keine Möglichkeit mehr, mich mit anderen anonymen Opfern auszutauschen."*

Vorratsdatenspeicherung: Politische Einflussnahme auf unliebsame Forscher? (01.02.2011)



+++ Das Bundesjustizministerium verlangte 2007 "Nachbesserungen" an einem unliebsamen Forschungsbericht zur Vorratsdatenspeicherung - doch welche Änderungen verlangt wurden, soll auch heute noch unter Verschluss bleiben. +++

Im Jahr 2004 forderte der Bundestag die Bundesregierung auf, bis zum 30.06.2007 einen Erfahrungsbericht über die Nutzung von Telekommunikationsdaten zur Strafverfolgung vorzulegen. Im Juli 2007 lag der entsprechende Bericht des Max-Planck-Instituts für internationales und ausländisches Strafrecht dem Bundesjustizministerium vor, das damals wegen des Gesetzentwurfs zur Vorratsdatenspeicherung massiv unter öffentlicher Kritik stand. Auf Wunsch des Ministeriums **wurde** der Bericht im September 2007 von den Forschern "nachgebessert". Das Bundesamt für Justiz "prüfte" die neue Fassung, versah sie mit "Anmerkungen" und leitete sie an das Bundesjustizministerium weiter.

Im Ministerium wurde eine Vorlage an Ministerin Brigitte Zypries erstellt, welche einen "Vorschlag zum weiteren Vorgehen" unterbreitete und die "Annahmefähigkeit" des Berichts feststellte. Der Forschungsbericht wurde trotzdem erst nach Beschluss des Gesetzes zur Vorratsdatenspeicherung am 9. November 2007 **veröffentlicht** - angeblich, weil *"zum damaligen Zeitpunkt eine Abnahme des Gutachtens kurzfristig nicht zu finalisieren war"*. In ihrem Bericht waren die Forscher zu einem politisch brisanten Ergebnis gekommen: *"Doch weist die Aktenanalyse selbst unter den heutigen rechtlichen Bedingungen nur für etwa 2% der Abfragen nach, dass sie wegen Löschungen ins Leere gehen."* Und: *"Die Aktenanalyse führt somit zu dem Ergebnis, dass im Untersuchungszeitraum die Löschung im Zusammenhang mit der Ausführung der Verkehrsdatenabfrage jedenfalls keine erhebliche Rolle spielt."*

Welche "Nachbesserungen" hat das Bundesjustizministerium damals von den unbequemen Forschern verlangt? Und warum wurde der "annahmefähige" Bericht unseren Volksvertretern vorenthalten, als sie über das verfassungswidrige Gesetz zur Vorratsdatenspeicherung abstimmten?

Mit einem Antrag nach dem Informationsfreiheitsgesetz hat ein AK Vorrat-Mitglied "Übersendung aller bei dem BMJ vorhandener Unterlagen bezüglich des Forschungsprojekts 'Rechtswirklichkeit der Auskunftserteilung über Telekommunikationsverbindungsdaten nach §§ 100g, 100h StPO' des Max-Planck-Instituts für ausländisches und internationales Strafrecht" verlangt. Doch das Bundesjustizministerium, inzwischen von Frau Leutheusser-Schnarrenberger (FDP) geführt, lehnte den Antrag ab: Die ursprüngliche Fassung des Forschungsberichts sei urheberrechtlich geschützt. Und die Anmerkungen des Ministeriums dazu unterfielen dem "Kernbereich exekutiver Eigenverantwortung".

Der daraufhin eingeschaltete Bundesbeauftragte für Datenschutz und Informationsfreiheit fand dazu deutliche Worte: Die Befürchtung einer Urheberrechtsverletzung *"kann ohne Belege von mir nicht akzeptiert werden."* Es müsse näher geprüft werden, *"ob hier tatsächlich ein vom Gesetz anerkannter Hinderungsgrund besteht"*. Auch dass die Unterlagen *"dem Kern exekutiver Eigenverantwortung zuzuordnen und deshalb nicht zugänglich zu machen sind, wird von mir nicht geteilt."*

Nach den deutlichen Worten des BfDI überprüft das Ministerium nun seit Wochen seine Position. Gleichzeitig schlägt es, nachdem das Bundesverfassungsgericht den damaligen Gesetzentwurf des Ministeriums für im Kern verfassungswidrig erklärt hat, bereits eine neue Vorratsdatenspeicherung vor.

Sicherheit geht vor Sammelwut - Vorratsspeicherung gefährdet Menschenleben

Dieser Bericht erläutert, warum eine ungezielte Protokollierung jeder Verbindung den Schutz von Kindern und Menschenleben gefährdet, warum eine Vorratsdatenspeicherung die Ermittlung von Straftätern nicht erleichtert, warum die EU Deutschland nicht zur Vorratsdatenspeicherung verpflichtet und welcher Verbesserungen die Strafverfolgung wirklich bedürfte.

1 Einführung

1.1 Traditionelle Vertraulichkeit von Gesprächen

Wenn wir miteinander sprechen oder einander Briefe schreiben, können wir sicher sein, dass unsere privaten und geschäftlichen Kontakte vertraulich bleiben. Niemand fertigt Aufzeichnungen darüber an, und wir müssen niemandem Rechenschaft darüber ablegen, mit wem wir gesprochen haben, wo wir gewesen sind oder was wir gelesen haben. Nicht anders ist dies seit jeher bei Telefongesprächen und Internetverbindungen gewesen: Telefongespräche wurden bis in die 80er Jahre analog vermittelt. Aufzeichnungen darüber wurden nur auf richterliche Anordnung erstellt. Mit der Einführung digitaler Vermittlungstechnik wurde dann erstmals die elektronische Erfassung jedes Telefongesprächs möglich. Die Telekommunikationsgesellschaften durften aber nur die zur Abrechnung erforderlichen Informationen erfassen. Kunden konnten die verkürzte Erfassung der gewählten Rufnummern und die Löschung aller Aufzeichnungen mit Rechnungsversand verlangen. Durch Nutzung von Pauschaltarifen konnten sie die Erfassung ihrer Verbindungen insgesamt verhindern. Im Verdachtsfall konnten die zuständigen Behörden Abrechnungsdaten einsehen und zukünftige Verbindungen aufzeichnen lassen.

1.2 Einführung einer Vorratsdatenspeicherung zum 01.01.2008

Trotz verbreiteter Proteste von Bürgern und Experten wurde zum 01.01.2008 erstmals die verdachtsunabhängige Erfassung und sechsmonatige Speicherung sämtlicher Telefon- und Handyverbindungen in Deutschland eingeführt. Bei jedem Handytelefonat und jeder versandten oder eingegangenen SMS wurde der Standort des Handynutzers erfasst. Zum 01.01.2009 musste dann auch jede Internetverbindung erfasst werden. In Verbindung mit anderen Daten konnte sechs Monate lang festgestellt werden, was wann über unseren Internetanschluss getan wurde.

1.3 Ende der Vorratsdatenspeicherung am 04.03.2010

34.000 Bürgerinnen und Bürger reichten gegen das Gesetz zur Vorratsdatenspeicherung Verfassungsbeschwerde ein. Am 04.03.2010 erklärte das Bundesverfassungsgericht die Vorschriften zur Vorratsdatenspeicherung für verfassungswidrig und hob sie auf. Seither gilt wieder die bewährte Regel, dass unsere Verbindungen nur ausnahmsweise erfasst werden dürfen, wenn dies zur Rechnungsstellung nötig ist.

1.4 Kampagne zur Wiedereinführung

Im Oktober 2010 wurde [bekannt](#), dass CDU und CSU eine „öffentliche Kampagne“ eingeleitet haben, um die FDP zu einem neuen Gesetz zur Erfassung aller Verbindungsdaten zu bewegen. Die FDP hat eine solche Vorratsdatenspeicherung immer wieder als unverhältnismäßig abgelehnt; Bundesjustizministerin Leutheusser-Schnarrenberger war dagegen sogar vor das Bundesverfassungsgericht gezogen. Bundesinnenminister de Maizière (CDU) und der Präsident des nachgeordneten Bundeskriminalamts wollen nun aber am 08.10.2010 „anhand möglichst spektakulärer Fälle“ belegen, dass es wegen der aktuell fehlenden Speicherpflicht „blinde Flecken in der Verbrechensbekämpfung“ gebe. Das Bundeskriminalamt hat dazu einen Bericht über die Auswirkungen des Endes der Vorratsdatenspeicherung am 04.03.2010 erstellt.

Der Arbeitskreis Vorratsdatenspeicherung als Zusammenschluss von Bürgerrechtlern, Datenschützern und Internetnutzern legt mit diesem Bericht eine eigene Expertise über die Forderung nach Erfassung aller Verbindungen vor.

2 Vorratsdatenspeicherung gefährdet den Schutz von Kindern und Menschenleben

Eine Erfassung sämtlicher Telefongespräche und Verbindungen hat schwerwiegende unerwünschte Nebenwirkungen auf unser Leben und auf unsere Gesellschaft:

2.1 Eine Erfassung sämtlicher Telefongespräche und Verbindungen gefährdet den Schutz von Kindern und kann Menschenleben kosten

Das Leben und die Gesundheit potenzieller Opfer von Gewalttaten kann in vielen Fällen nur durch anonyme Beratung geschützt werden (z.B. Telefonseelsorge, Hotlines). Viele Täter sind nur im Schutz der Anonymität bereit, sich helfen zu lassen, wobei sie vielfach von geplanten Gewalttaten abgebracht oder von der Notwendigkeit einer Behandlung überzeugt werden können. Viele Opfer können sich nur im Rahmen anonymer Beratung entschließen, Täter anzuzeigen. Eine Erfassung sämtlicher Telefongespräche und Verbindungen gefährdet die Bereitschaft von Tätern und Opfern zur Inanspruchnahme von Beratung und gefährdet damit Menschenleben.

Beispiel 1: Im Jahr 2007 konnte ein bei der Telefonseelsorge in Bayern tätiger Pfarrer einen Jugendlichen überzeugen, einen geplanten Amoklauf in seiner Schule zu unterlassen. Wäre der Anruf rückverfolgbar gewesen, hätte der Jugendliche wohl nie über sein Vorhaben gesprochen.

Beispiel 2: Im Jahr 2010 erwägt ein betrogener Ehemann, seine Ehefrau oder ihren Liebhaber zu töten. Die Telefonseelsorge kann ihn davon abbringen. Wäre der Anruf rückverfolgbar gewesen, hätte der Mann wohl nie über sein Dilemma gesprochen.

Beispiel 3: Eine akut krebserkrankte Patientin vermeidet wegen der Vorratsdatenspeicherung, sich per Telefon oder E-Mail nach einer Behandlungsmöglichkeit für ihre Tumorerkrankung zu erkundigen und vereinbart stattdessen einen persönlichen Gesprächstermin in einem Berliner Klinikum. Das Abwarten verzögert den Behandlungsbeginn. In der Zwischenzeit wächst der Tumor weiter, die Prognose der Patientin verschlechtert sich.

Nach einer [Vorgabe](#) des Bundesverfassungsgerichts muss für bestimmte, auf besondere Vertraulichkeit angewiesene Telekommunikationsverbindungen ein „grundsätzliches Übermittlungsverbot“ an staatliche Stellen gelten. Dies lässt aber erstens Ausnahmen zu, so dass im Fall einer Anrufererfassung weiterhin eine Aufdeckung gegenüber staatlichen Stellen drohen würde. Zweitens ließe ein Übermittlungsverbot das Risiko illegaler oder versehentlicher Offenlegung der erfassten Kontakte durch Telekommunikationsunternehmen, ihre Mitarbeiter

oder Hacker bestehen. Dieses Risiko hat sich in der Vergangenheit bereits mehrfach realisiert. Drittens kann nicht angenommen werden, dass sich Menschen in Notsituationen an den Feinheiten gesetzlicher Regelungen orientieren. Für ihre Bereitschaft zur Kontaktaufnahme ist entscheidend, ob ihre Rufnummer erfasst wird oder nicht. Dies zeigt die folgende Untersuchung:

Eine repräsentative [Umfrage](#) unter 1.002 Bundesbürgern am 27./28. Mai 2008 hat ergeben, dass mehr als die Hälfte der Deutschen wegen der Vorratsdatenspeicherung davon absehen würden, per Telefon, E-Mail oder Handy Kontakt zu einer Eheberatungsstelle, einem Psychotherapeuten oder einer Drogenberatungsstelle aufzunehmen, wenn sie deren Rat benötigten. Dies betrifft über 40 Mio. Menschen in Deutschland.

2.2 Eine Erfassung sämtlicher Telefongespräche und Verbindungen begünstigt Korruption

Korruption und andere öffentliche Missstände werden oftmals erst dann wirksam aufgeklärt und angegangen, wenn die Medien darüber öffentlich berichten. Wer Journalisten von solchen Fällen als Insider berichtet, riskiert aber oftmals seine Anstellung oder muss sogar mit einem Strafverfahren wegen Geheimnisverrats rechnen. Wichtige Missstände und Skandale melden Informanten der Presse daher nur im Schutze absoluter Vertraulichkeit. Eine Erfassung sämtlicher Telefongespräche und Verbindungen gefährdet die Bereitschaft von Informanten, mit Journalisten zu sprechen, und begünstigt damit Korruption und andere Missstände im Verborgenen.

Beispiel 1: Der Journalist Philipp Kunze (Name geändert) aus Nordrhein-Westfalen befasst sich im Rahmen seiner Arbeit unter anderem mit Menschenrechtsverletzungen der EU-Grenzagentur Frontex. Bereits kurz nach Inkrafttreten der Vorratsdatenspeicherung lehnen zwei Kontaktpersonen den Informationsaustausch via E-Mail ab.

Beispiel 2: Die Drehbuchautorin Maria Urner (Name geändert) aus Bayern recherchierte den Wismut-Skandal, in dessen Rahmen ca. 2.800 ehemaligen Uranerz-Bergmänner der DDR durch Radioaktivität in den Stollen Krebserkrankungen bekamen und nun keine Unfallrente erhalten. Nach dem 1.1.2008 bekommt Frau Urner bei telefonischen Recherchen, besonders in der ehemaligen DDR, nur noch zögerlich oder gar keine Auskünfte zu dem Thema mehr.

Beispiel 3: Der Sportjournalist Florian Schröder (Name geändert) aus Hamburg ist nach Inkrafttreten der Vorratsdatenspeicherung damit konfrontiert, dass viele Informanten nicht nur Fragen am Telefon oder per E-Mails ablehnten, sondern auch direkte Gespräche und Treffen. Für seine Arbeit etwa beim Thema Doping sind die Auswirkungen katastrophal.

In einer [Umfrage](#) unter 1.489 deutschen Journalisten aus dem Jahr 2008 erklärte jeder vierzehnte Journalist, das Bewusstsein, dass Kommunikationsdaten auf Vorrat gespeichert werden, habe sich bereits negativ auf die Kommunikation mit seinen Informanten ausgewirkt. Damit beeinträchtigte die Vorratsdatenspeicherung die Arbeit von hochgerechnet mindestens 3.000 Journalisten in Deutschland.

2.3 Eine Erfassung sämtlicher Telefongespräche und Verbindungen gefährdet die Wissenschaft

Wissenschaftliche Forschung setzt in vielen Bereichen die Bereitschaft von Menschen voraus, anonym über ihre Persönlichkeit und ihr Leben Auskunft zu geben. Werden alle Kontakte erfasst, können Forschungsprojekte an der fehlenden Bereitschaft zur Mitwirkung an Umfragen scheitern.

Beispiel: Leon Schulz (Name geändert) arbeitet in der universitären Onlineforschung an einem Lehrstuhl für Persönlichkeitspsychologie. Für seine psychologischen Studien über die menschliche Persönlichkeit sind oft sehr intime Fragen nötig. Diese Fragen werden von den Versuchsteilnehmern nach Inkrafttreten der Vorratsdatenspeicherung nicht mehr beantwortet, wodurch die Forschung im Bereich Psychologie sehr leidet.

2.4 Eine Erfassung sämtlicher Telefongespräche und Verbindungen setzt Arbeitsplätze aufs Spiel

Geschäftsbeziehungen und Vertragsverhandlungen sind oft äußerst vertraulich. Eine Erfassung telefonischer oder elektronischer Kontakte schafft das Risiko, dass Geschäftsgeheimnisse bekannt werden (z.B. durch Wirtschaftsspionage), was großen Schaden nach sich ziehen kann. Deswegen verzichten Wirtschaftsunternehmen teilweise lieber ganz auf Kontakte als das Risiko unbefugter Offenlegung einzugehen. Dadurch können Unternehmen Aufträge verlieren, was Arbeitsplätze kosten kann.

Beispiel: Hans Grunwald aus Bayern arbeitet in der Industrieproduktion. Sein Unternehmen, in dem acht Mitarbeiter tätig sind, fertigt für potenzielle Kunden aus ganz Europa Prototypen, wofür technische Zeichnungen oder sonstige sicherheitsrelevante Beschreibungen der Geschäftspartner benötigt werden. Nach Inkrafttreten der Vorratsdatenspeicherung weigern sich mehrere Kunden, die erforderlichen Unterlagen per Email oder Telefax zu versenden. Dadurch verliert das Unternehmen einen Großkunden und muss zwei Arbeitnehmer entlassen.

2.5 Eine Erfassung sämtlicher Telefongespräche und Verbindungen lässt politische Kritiker abtauchen

Die Vorbereitung spektakulärer Protestaktionen gegen Gentechnik, gegen Atomenergie usw. bedarf oft absoluter Vertraulichkeit. Viele Menschen sind nicht zu einem Engagement in politisch kritischen Gruppen bereit, wenn sie damit rechnen müssen, in das Raster des Verfassungsschutzes zu geraten.

Beispiel 1: Patrick Schuhmacher (Name geändert) engagiert sich antifaschistisch und befürchtet mit Inkrafttreten der Vorratsdatenspeicherung, dass seine Daten besonders geprüft werden. Auf Telefongespräche und Internetkorrespondenz, die nicht unbedingt notwendig sind, verzichtet er daher.

Beispiel 2: Katharina Gärtner aus Baden-Württemberg ist in einer Attac-Gruppe aktiv. Seit Inkrafttreten der Vorratsdatenspeicherung wirken die Diskussionsbeiträge im Internetforum der Gruppe wie zensiert, die Diskussionsteilnehmer trauen sich nicht mehr, ihre Meinung zu äußern.

2.6 Eine Erfassung sämtlicher Telefongespräche und Verbindungen verhindert die Ermittlung von Straftätern

Eine verdachtsunabhängige Erfassung jedes Telefonats und jeder Verbindung gräbt sich in das Bewusstsein Unschuldiger wie Schuldiger ein. Eine Vorratsdatenspeicherung erhöht daher die Entwicklung und Nutzung anderer Kommunikationskanäle. Viele Menschen gehen dazu über, Gespräche nicht mehr telefonisch zu führen, wechselnde Handys zu benutzen oder mit ausländischen Anonymisierungsdiensten im Internet zu surfen. Dies verschließt den Ermittlern selbst im Fall eines konkreten Verdachts die Möglichkeit einer Überwachung und Aufklärung schwerster Straftaten.

Beispiel: Ein anonymen Nutzer kündigt im Polizisten-Forum Copzone einen Amoklauf an und bedroht dabei eine Arbeitsvermittlerin massiv. Weil er einen internationalen Anonymisierungsdienst nutzt, ist eine Identifizierung nicht möglich. Stattdessen wird versehentlich der Betreiber des Dienstes verhaftet.

In einer [infas-Umfrage](#) aus dem Jahr 2009 erklärten schon 12,8% der Befragten, einen Anonymisierungsdienst einzusetzen, 6,4%, sie seien zu einem Provider ohne Vorratsdatenspeicherung gewechselt, und 5,1%, dass sie Internet-Cafés benutzten. Eine jederzeitige Rückverfolgbarkeit durch Vorratsdatenspeicherung dürfte diese Entwicklung erheblich beschleunigen.

2.7 Eine Erfassung sämtlicher Telefongespräche und Verbindungen führt zur Verfolgung Unschuldiger

Verbindungsdaten können die Ermittlung eines Anschlussinhabers ermöglichen, geben aber nicht an, wer das entsprechende Telefon oder Handy oder den Internetanschluss konkret genutzt hat. Durch Verbindungsdaten geraten daher viele Menschen zu Unrecht in einen falschen Verdacht, z.B. wegen eines Zahlendrehers, wegen eines verkauften Handys, wegen eines offenen Internetzugangs. Dies zieht immer wieder Überwachungsmaßnahmen, Hausdurchsuchungen oder sogar Festnahmen Unschuldiger nach sich und hat schon das Leben von Menschen ruiniert.

Beispiel 1: Die Wohnung eines deutschen Professors wurde durchsucht und seine Computer beschlagnahmt, weil er Kinderpornografie über das Internet verbreitet haben soll. Tatsächlich hatte sein Internet-Zugangsanbieter der Polizei eine falsche Auskunft erteilt.

Beispiel 2: Im Dezember 2008 stürmte das Spezialeinsatzkommando (SEK) die Wohnung eines 38jährigen Mannes in Recklinghausen. Die Polizei hatte von einer Amokdrohung erfahren. Erst später stellte sich heraus, dass ein Nachbar die Drohung über das offene Funknetz des Mannes versandt hatte.

2.8 Eine Erfassung sämtlicher Telefongespräche und Verbindungen führt zum Bekanntwerden vertraulichster Beziehungen

Beinahe wöchentlich werden immer neue Fälle von Missbrauch, Verkauf, Verlust, Veröffentlichung von und Zugang zu persönlicher Daten bekannt. Heutzutage sind nur nicht erfasste Daten sichere Daten. Eine Erfassung sämtlicher Telefongespräche und Verbindungen führt dazu, dass weit mehr Menschen unter dem Missbrauch, dem Verkauf, dem Verlust, der Veröffentlichung von und dem missbräuchlichen Zugang zu ihren vertraulichen Kontakten und Aufenthaltsorten leiden als sonst.

Beispiel 1: Die Deutsche Telekom AG kontrolliert über einen Zeitraum von insgesamt anderthalb Jahren die Telefonverbindungen von Journalisten sowie von Arbeitnehmer-Aufsichtsräten, Managern und Betriebsräten des Unternehmens. Da keine Vorratsdatenspeicherung erfolgt, sind die Verbindungen von Menschen mit Pauschaltarifen vor missbräuchlicher Aufdeckung ihrer Kontakte geschützt.

Beispiel 2: Im Jahr 2006 verkaufte ein Mitarbeiter von T-Mobile die Daten der 17 Mio. Kunden des Mobilfunkunternehmens. Darunter befinden sich Privatanschriften und -nummern vieler Prominenter aus Kultur und Gesellschaft sowie eine erstaunliche Anzahl geheimer Nummern und Privatadressen von bekannten Politikern, Ministern, Ex-Bundespräsidenten, Wirtschaftsführern, Milliardären und Glaubensvertretern, für die eine Verbreitung ihrer Kontaktdaten in kriminellen Kreisen eine Bedrohung ihrer Sicherheit darstellt (etwa von Charlotte Knobloch, Präsidentin des Zentralrats der Juden). Das Bundeskriminalamt erstellt eine Gefährdungsanalyse, um Betroffene schützen zu können. Zur Aufklärung des Datenlecks verletzte T-Mobile erneut das Fernmeldegeheimnis und überprüfte illegal auf eigene Faust Verbindungsdaten.

3 Eine Erfassung sämtlicher Telefongespräche und Verbindungen verbessert die Ermittlung von Straftätern nicht

Der vom Bundeskriminalamt veröffentlichten Polizeilichen [Kriminalstatistik](#) zufolge hat die Erfassung aller Internetverbindungen im Jahr 2009 weder von Straftaten abgeschreckt, noch den Anteil der aufgeklärten Straftaten erhöht. Obwohl im Internetbereich Verbindungsdaten teilweise der einzige Ermittlungsansatz sind, konnte ohne Vorratsdatenspeicherung sogar eine höhere Aufklärungsrate erzielt werden.

Im Jahr 2008, in dem Internet-Einwahlen und E-Mails von den Anbietern allenfalls [kurzfristig](#) protokolliert wurden, wurden danach 167.451 Internet-Straftaten registriert, die zu 79,8% aufgeklärt werden konnten. Im Jahr 2009, in dem alle Internet-Einwahlen und E-Mails für sechs Monate protokolliert wurden, registrierte die Polizei demgegenüber 206.909 begangene Internet-Straftaten, und ihre Aufklärung gelang nur zu 75,7%.

Internetdelikte wurden ohne Vorratsdatenspeicherung weit häufiger aufgeklärt (79,8%) als sonstige Straftaten (54,8%). Das gilt übrigens auch für die Verbreitung von Kinderpornografie im Internet (87,5%). Von einem rechtsfreien Raum kann keine Rede sein. Andere Staaten auf der ganzen Welt (z.B. Österreich, Griechenland, Schweden, Rumänien, Norwegen, Australien, Kanada, Japan) ermitteln schon immer erfolgreich ohne Vorratsdatenspeicherung.

3.1 Die Zahlen des Bundeskriminalamts belegen keinen Bedarf

Ein aktuell diskutierter [Bericht](#) des Bundeskriminalamts über die „Auswirkungen des Urteils des Bundesverfassungsgerichts zu Mindestspeicherungsfristen“ belegt keinen Bedarf nach einer neuerlichen Erfassung sämtlicher Telefongespräche und Verbindungen.

3.1.1 Die mitgeteilte Zahl ergebnisloser Auskunftersuchen ist irrelevant

Für den Bericht wertete das Bundeskriminalamt Auskunftersuchen an Telekommunikationsfirmen zu 1.157 Anschlüssen im Zeitraum 2. März bis 17. September 2010 aus. 85% dieser Auskunftersuchen betrafen Inhaber von Internetadressen. Zu 880 der erfragten Anschlüsse (76%) sei dem Bundeskriminalamt keine Auskunft erteilt worden. Die Auskunftersuchen zu Internetadressen seien zu 16% erfolgreich gewesen, die Auskunftersuchen zu Telefonen und Handys zu 86%.

Aus den folgenden Gründen belegen diese Zahlen keine „blinde Flecken in der Verbrechensbekämpfung“ oder „Schutzlücken“:

1. **Wären im Fall einer Vorratsdatenspeicherung nicht ebenso viele Auskünfte unterblieben?** Das Bundeskriminalamt liefert keine Vergleichswerte für die Zeit, als in Deutschland alle Verbindungen auf Vorrat erfasst wurden (2009). Deswegen belegen die Zahlen nicht, dass gegenwärtig weniger Auskünfte erteilt würden. 147 der ergebnislosen Auskunftersuchen des BKA betrafen beispielsweise Internetverbindungen, die im Zeitpunkt der Anfrage (25.05.2010) bereits länger als sechs Monate zurück lagen (Zeitstempel: 29.05.2009-11.09.2009) und deswegen auch im Fall einer sechsmonatigen Vorratsdatenspeicherung ergebnislos geblieben wären. Das Bundeskriminalamt liefert auch keine Vergleichswerte für die Zeit vor Einführung der Vorratsdatenspeicherung. Deswegen belegen die Zahlen nicht, dass gegenwärtig weniger Auskünfte erteilt würden als seit jeher.
2. **Wäre im Fall der Auskunfterteilung eine Identifizierung des Verdächtigen möglich gewesen?** Das Bundeskriminalamt beantwortet diese Frage nicht. Deshalb kann nicht davon ausgegangen werden, dass weitere Auskünfte zur Identifizierung weiterer Straftäter geführt hätten. In vielen Fällen verwenden Straftäter Internet-Cafés, offene Internetzugänge (WLAN), Anonymisierungsdienste, öffentliche Telefone, unregistrierte Handykarten usw. Eine Auskunft über den Anschlussinhaber ermöglicht eine Identifizierung des Nutzers in diesen Fällen nicht.
3. **Wäre es im Fall der Auskunfterteilung zur Verurteilung des Verdächtigen gekommen?** Das Bundeskriminalamt beantwortet diese Frage nicht. Deshalb kann nicht davon ausgegangen werden, dass Auskünfte letztlich zur Verurteilung von Straftätern geführt hätten. Nach einer Untersuchung des Max-Planck-Instituts im Auftrag des Bundesjustizministeriums kam es in 72% der Verfahren mit erfolgreicher Verbindungsdatenabfrage gleichwohl zu keiner Verurteilung.
4. **Hat das Bundeskriminalamt Auskünfte angefordert, obwohl es von vornherein wusste, dass sie nicht erteilt werden können?** Das Bundeskriminalamt beantwortet diese Frage nicht. Es liegt nahe, dass das Bundeskriminalamt die Zahl erfolgloser Auskunftersuchen durch erkennbar aussichtslose Anfragen in die Höhe getrieben hat. Dem Bundeskriminalamt liegt eine Liste [vor](#), wie lange welches Unternehmen Verbindungsdaten aufbewahrt (maximal eine Woche). Dennoch lagen 209 der ergebnislos angefragten Internetverbindungen länger als 10 Tage zurück, 147 weitere Internetverbindungen lagen sogar länger als sechs Monate in der Vergangenheit. In Anbetracht dieser von vornherein aussichtslosen Anfragen sind die vom Bundeskriminalamt ermittelten Zahlen manipuliert und wertlos. Dass die Untersuchung des

Bundeskriminalamts von vornherein auf ein feststehendes Ergebnis abzielte, zeigt schon die Bezeichnung der verwendeten Erhebungsbögen: *„Erhebungsbogen zur Begründung des polizeilichen Bedarfs der Auskunft über längerfristig gespeicherte Verkehrsdaten“*

5. **In wie vielen Fällen kann das Bundeskriminalamt generell Täter mangels Spuren nicht identifizieren?** Ohne eine Antwort auf diese Frage muss davon ausgegangen werden, dass physisch anwesende Täter oder Absender von Briefen seltener identifizierbare Spuren hinterlassen als Täter von Telefon- oder Internetdelikten. Es ist nicht einzusehen, warum Telefon und Internet gläserner sein sollten als persönliche Kontakte und die Post. Tatsächlich wurden Internetdelikte auch ohne Vorratsdatenspeicherung zuletzt zu 79% aufgeklärt, während sonstige Straftaten nur zu 55% aufgeklärt wurden. Während vier Fünftel aller im Internet begangenen Straftaten aufgeklärt werden, bleibt etwa jeder zweite Raub unaufgeklärt.

3.1.2 Auswirkungen auf die Strafverfolgung sind nicht belegt

Dem Bericht des Bundeskriminalamts zufolge gelang in 636 der 1157 untersuchten Fälle (55%), in denen das Bundeskriminalamt nach Telekommunikationsdaten fragte, die Aufklärung der Straftat nicht oder nicht vollständig.

Aus den folgenden Gründen belegt dies keine „blinde Flecken in der Verbrechensbekämpfung“ oder „Schutzlücken“:

1. **Welche Aufklärungsquote ergibt sich bei einer statistisch repräsentativen Stichprobe?** Die Zahlen des Bundeskriminalamts betreffen lediglich 1.157 „Auskunftsersuchen des BKA, die im Zeitraum vom 02.03. bis 17.09.2010 gestellt und erfasst wurden“. Es ist bereits ungeklärt, welche Auskunftsersuchen des BKA für die Auswertung erfasst wurden und nach welchen Kriterien die Auswahl erfolgte. 70% der für die Studie ausgewerteten Auskunftsersuchen betrafen zudem die Verbreitung von Kinderpornografie. Tatsächlich handelte es sich bei den 206.909 Straftaten, die 2009 im Internet begangen und polizeilich registriert wurden, aber zu 82% um Betrugsdelikte und nur zu 3% um die Verbreitung kinderpornographischer Schriften. Von den 6 Mio. Straftaten, die 2009 insgesamt registriert wurden, betrafen sogar nur 0,1% die Verbreitung kinderpornographischer Schriften. Die Zahlen des Bundeskriminalamts betreffen mithin nur einen sehr kleinen Teil der strafrechtlichen Ermittlungsverfahren, weil das Bundeskriminalamt dafür nur ausnahmsweise zuständig ist (§ 4 Abs. 2 BKAG). Die Zahlen des Bundeskriminalamts betreffen außerdem einen nicht repräsentativen Teil der Deliktsformen, nämlich vorwiegend die Verbreitung

kinderpornographischer Schriften, obwohl diese tatsächlich nur einen sehr kleinen Teil der Kriminalitätswirklichkeit ausmacht. Die Zahlen des Bundeskriminalamts lassen daher keinen Rückschluss auf die Frage zu, ob das Ende der Vorratsdatenspeicherung Auswirkungen auf die Strafverfolgung insgesamt hatte.

2. **Wie sind die Zahlen des Bundeskriminalamts mit der hohen Aufklärungsquote vor Geltung einer Vorratsdatenspeicherung in Deutschland in Einklang zu bringen?** Internetdelikte wurden im Jahr 2008 auch ohne Vorratsdatenspeicherung zu fast 80% aufgeklärt, während sonstige Straftaten zu 55% aufgeklärt wurden. Warum diese Aufklärungsquoten nicht auch heute wieder erreicht werden sollen, erklärt das Bundeskriminalamt nicht schlüssig. Der Hinweis des Bundeskriminalamts auf die zunehmende Verbreitung von Flatrates verfängt nicht. Denn schon 2008, als Internetanbieter nicht auf Vorrat speicherten, nutzten [86%](#) der Deutschen eine Internet-Flatrate und wurden gleichwohl [79%](#) der registrierten Internetdelikte aufgeklärt. Deshalb ändern die Zahlen des Bundeskriminalamts nichts daran, dass auch gegenwärtig ohne Vorratsdatenspeicherung vermutlich eine weit überdurchschnittliche Aufklärungsquote bei Internetdelikten erzielt wird.
3. **Wäre im Fall einer Vorratsdatenspeicherung ein größerer Teil der vom Bundeskriminalamt verfolgten Straftaten aufgeklärt worden?** Das Bundeskriminalamt beantwortet diese Frage nicht. Deshalb kann nicht davon ausgegangen werden, dass weitere Auskünfte zur Aufklärung weiterer Straftaten geführt hätten. Das Bundeskriminalamt teilt etwa nicht mit, wie viele Ermittlungsverfahren trotz erteilter Auskunft eingestellt werden mussten. Das Bundeskriminalamt liefert ferner keine Vergleichswerte für die Zeit, als in Deutschland alle Verbindungen auf Vorrat erfasst wurden (2009). Deswegen belegen die Zahlen nicht, dass gegenwärtig weniger Straftaten aufgeklärt würden als bei Geltung einer Vorratsdatenspeicherung. Das Bundeskriminalamt liefert schließlich keine Vergleichswerte für die Zeit vor Einführung der Vorratsdatenspeicherung. Deswegen belegen die Zahlen nicht, dass gegenwärtig weniger Straftaten aufgeklärt würden als seit jeher.
4. **Wären im Fall einer Vorratsdatenspeicherung mehr Täter verurteilt worden?** Das Bundeskriminalamt beantwortet diese Frage nicht. Deshalb kann nicht davon ausgegangen werden, dass weitere Auskünfte letztlich zur Verurteilung weiterer Straftäter geführt hätten. Nach einer [Untersuchung](#) des Max-Planck-Instituts im Auftrag des Bundesjustizministeriums kam es in 72% der Verfahren mit erfolgreicher Verbindungsdatenabfrage gleichwohl zu keiner Verurteilung.

3.2 Die Fallberichte des Bundeskriminalamts belegen keinen Bedarf

Die vom Bundeskriminalamt im Einzelnen geschilderten Straftaten belegen ebensowenig „blinde Flecken in der Verbrechensbekämpfung“ oder „Schutzlücken“:

3.2.1 „Ermordung eines Hamas-Funktionärs“

Im Zusammenhang mit der Ermordung eines Funktionärs der paramilitärischen Terrororganisation Hamas in Dubai im Januar 2010 lief ein Ermittlungsverfahren gegen einen Beschuldigten in Deutschland wegen des Verdachts geheimdienstlicher Agententätigkeit. Über einen Mobilfunkanschluss wurden Gespräche des Komplotts rückwirkend noch mehrere Monate abgerechnet. Dadurch wollte das BKA Kontaktpersonen identifizieren und Ansätze für weitere Ermittlungen gewinnen.

Es ist nicht belegt und liegt fern, dass Verbindungsdaten hier weiter geführt hätten. Hamas-Mitglieder werden geschickt genug sein, um nur mit Handys zu telefonieren, die nicht auf ihren Namen registriert sind. Deswegen belegt der Fall nicht, dass eine Erfassung sämtlicher Verbindungen weiter geführt hätte.

3.2.2 „Wer verlinkte das Terror-Video?“

In einem Internetforum wurde am 12. April 2010 eine Videoverlautbarung einer terroristischen Vereinigung über verschiedene Links zur Verfügung gestellt. Einer davon stammte von einer unbekannten Person, deren E-Mail-Adresse einen Tag zuvor registriert worden war. Das BKA fragte am 20. April bei der Deutschen Telekom Kundendaten zu der IP-Adresse (Computeradresse im Internet) für den Registrierungstag (11. April) ab. Der Konzern teilte daraufhin mit, dass die Speicherfrist von sieben Tagen bereits abgelaufen sei und verwies auf das Verfassungsgerichtsurteil. Fazit des BKA: Aufklärung unmöglich.

Es ist nicht belegt und liegt fern, dass Verbindungsdaten hier weiter geführt hätten. Es kann nicht ernsthaft angenommen werden, dass ein Terrorvideo vom Heimanschluss eines Unterstützers verlinkt wird. Wahrscheinlich hätten Verbindungsspuren nur zu einem Internetcafé oder einem offenen Internetzugang (WLAN) geführt und damit nichts zu der Ermittlung beigetragen.

3.2.3 „Terrorandrohung gegen Schulen“

Ein Unbekannter versandte seit Dezember 2009 über ein Briefzentrum mehr als 100 Briefe, in denen er Sprengstoffanschläge androhte. Adressaten waren Schulen, Universitäten und Bürger. Falls sie eine gewisse Geldsumme nicht zahlten, sollten sie getroffen werden. Der Täter kontaktierte per E-Mail am 22. April eine Geschädigte über deren Profil bei „studiVZ“. Zwar bekam das BKA von

dem Netzwerk die IP-Adresse des Absenders und fand den dahinter stehenden Anbieter Vodafone. Doch der teilte mit, dass er solche Daten nicht speichere. Fazit des BKA: Aufklärung unmöglich.

Es ist nicht belegt und liegt fern, dass Verbindungsdaten hier weiter geführt hätten. Es kann nicht ernsthaft angenommen werden, dass der Urheber von 100 Bombendrohungen eine Vodafone-Internetkarte nutzt, die auf seinen Namen registriert ist. Sinnvollerweise wird „studiVZ“ eine Fangschaltung einrichten: Wenn sich der Täter wieder anmeldet, wird seine Kennung der Polizei übermittelt. Während der bestehenden Internetverbindung kann Vodafone die Anschlussdaten auch ohne Vorratsdatenspeicherung feststellen.

3.2.4 „Mafiamord in Leverkusen“

Ein italienischer Staatsbürger wurde am 15. Januar 2010 in Leverkusen ermordet. Als der 43-jährige noch lebte, hatte er sich unangemeldet in Köln aufgehalten. Das BKA erfuhr von italienischen Behörden, dass das Mordopfer der Mafia nahe gestanden haben soll. Dem BKA gelang es, den möglichen Tatort und vier Verdächtige zu ermitteln. Für ein Ermittlungsverfahren wäre laut des BKA jedoch die Auswertung von Telefondaten erforderlich gewesen. Aber einen solchen Antrag lehnte die Staatsanwaltschaft Köln ab. Fazit des BKA: Die Aufklärung des Mordes sei zumindest „wesentlich erschwert“.

Offensichtlich konnte der Fall auch auf anderem Wege aufgeklärt werden. Im Übrigen steht in den Sternen, ob Verbindungsdaten weiter geführt hätten. In Mafiakreisen liegt dies fern.

3.2.5 „Polizistenmord“

In Brandenburg wurde am 23. November 2009 der Mord an dem 46-jährigen Polizeihauptkommissar Steffen M. bekannt. Der oder die Täter flüchteten mit dem Auto des Opfers. Dieses wurde laut BKA abgestellt und eine andere „Beförderungsmöglichkeit“ per Handy angefordert. Am 18. Februar erging beim Amtsgericht Cottbus ein Beschluss, dass die Daten abgefragt werden dürfen. D2 Vodafone teilte dem BKA daraufhin am 9. März 2010 mit, dass für das betreffende Handy am 7. März keine Verkehrsdaten mehr vorliegen würden. Fazit des BKA: Aufklärung unmöglich.

Es ist nicht belegt und liegt fern, dass Verbindungsdaten hier weiter geführt hätten. Wenn der Täter einen Komplizen angerufen hat, wird dieser geschickt genug gewesen sein, mit einem Handy zu telefonieren, das nicht auf seinen Namen registriert war. Deswegen belegt der Fall nicht, dass eine Erfassung sämtlicher Verbindungen weiter geführt hätte.

3.2.6 „Hinweise auf Kindesmissbrauch“

Das BKA erhielt am 14. Mai 2010 die Meldung über einen Kindesmissbrauch. In einem Internetforum fand sich ein Hinweis vom 6. Mai darüber, dass ein Stiefvater seinen Sohn missbraucht und ihn deswegen sogar teilweise mit Medikamenten ruhig stellt. Der Nutzernamen war anonym und ausschließlich die IP-Adresse sichtbar. Das BKA forschte noch am 14. Mai nach, bekam aber keine Auskunft. Aus dem Inhalt des Textes konnten keine Hinweise auf die Identität des Nutzers gezogen werden. Fazit des BKA: Aufklärung unmöglich.

Es ist nicht belegt und liegt fern, dass Verbindungsdaten hier weiter geführt hätten. Es kann nicht ernsthaft angenommen werden, dass der Betroffene über einen auf seinen Namen angemeldeten Anschluss über seine Straftaten berichtet hat. Sinnvollerweise wird der Betreiber des Forums eine Fangschaltung einrichten: Wenn sich der Täter wieder anmeldet, wird seine Kennung der Polizei übermittelt. Während der bestehenden Internetverbindung kann der Internet-Zugangsanbieter die Anschlussdaten auch ohne Vorratsdatenspeicherung feststellen.

Selbst wenn dieser Kindesmissbrauch hätte beendet werden können, hätte eine Vorratsdatenspeicherung den Schutz einer weit größeren Anzahl von Kindern vereitelt: Nicht rückverfolgbare, anonyme Beratung ist zum Schutz unzähliger Kindern und Erwachsener unverzichtbar. Anonymen Telefonberatungsstellen gelingt es immer wieder, Täter von Kindesmissbrauch und Pädophile zu überzeugen, sich in Behandlung zu begeben. Gewalttätige Ehemänner werden überzeugt, sich in Therapie zu begeben. HIV-Infizierte werden überzeugt, andere nicht weiter durch ungeschützten Geschlechtsverkehr mit der lebensbedrohenden Krankheit anzustecken. Die Gesundheit Unschuldiger steht und fällt mit der Verfügbarkeit nicht rückverfolgbarer Beratung.

3.2.7 „Botnetz“

Ein Ermittlungsverfahren in Luxemburg ergab nach der Auswertung eines beschlagnahmten Computerservers als Teil eines illegalen Botnetzes, dass dieser zur „Verschleierung der Täterkommunikation“ und zur „Erlangung der digitalen Identität“ von Nutzern diente. Es wurden 218.703 deutsche IP-Adressen, die auf den Server zugegriffen, mit „Zeitstempel November 2009“ an das BKA übermittelt. Die Fahnder wollten über die Länderpolizeien die Computerbesitzer in Deutschland informieren. Doch das Auskunftersuchen wurde weitgehend abgelehnt. Das betraf allein in Nordrhein-Westfalen und Hessen 169.964 IP-Adressen. Fazit des BKA: Aufklärung unmöglich.

Es ist nicht die Aufgabe der Polizei, Computerbenutzer über eine Infektion ihres Computers zu informieren. Dies ist in erster Linie Aufgabe des Nutzers selbst. In zweiter Linie tun dies die Internet-Zugangsanbieter im Rahmen ihrer Anti-

Botnetz-Initiative, ganz ohne Vorratsdatenspeicherung. In dritter Linie wäre es sinnvoll, die Hersteller gebrauchsfertiger Computersysteme zu verpflichten, Computer nur noch mit vorinstalliertem Virenschanner auszuliefern.

3.2.8 „Kontakte einer radikal-islamischen Untergrundorganisation“

Das BKA wollte nach Hinweisen von amerikanischen und libanesischen Sicherheitsbehörden Mitglieder der sunnitischen radikal-islamischen Untergrundorganisation Fatah al-Islam in Deutschland aufspüren und identifizieren. Das gelang bei einem Mann, weil er falsche Ausweispapiere hatte und gegen ihn ein libanesischer Haftbefehl vorlag. Nach der Festnahme befindet sich der Mann in Auslieferungshaft. Das BKA konnte aber keine Kontaktpersonen ermitteln. Der Grund: Die Telekommunikationsfirmen gaben Telefon- und Internetverbindungsdaten nicht oder nur unvollständig heraus. Fazit des BKA: „Somit konnte keine vollständige Aufhellung der Szene erfolgen“.

Es ist nicht belegt und liegt fern, dass weitere Verbindungsdaten die „Szene“ hier „vollständig erhellt“ hätten. Es kann nicht ernsthaft angenommen werden, dass Mitglieder einer Untergrundorganisation über auf ihren eigenen Namen registrierte Telefon- oder Internetanschlüsse miteinander kommunizierten. Wahrscheinlich hätten Verbindungsspuren nur zu einem Internetcafé oder einem offenen Internetzugang (WLAN) geführt und damit nichts zu der Ermittlung beigetragen.

4 Die EU verpflichtet Deutschland nicht zur Vorratsdatenspeicherung

Die EU-Richtlinie 2006/24/EG zur Vorratsdatenspeicherung verpflichtet Deutschland nicht zu einer Erfassung sämtlicher Verbindungen. Die EU-Verträge (Art. 114 Abs. 4 AEUV) erlauben es Deutschland, aus wichtigem Grund von solchen Richtlinien abzuweichen und abweichende Gesetze beizubehalten. Der Schutz Unschuldiger und ihrer Grundrechte ist Bestandteil der öffentlichen Ordnung Deutschlands und rechtfertigt eine Abweichung von der EU-Richtlinie zur Vorratsdatenspeicherung. Die Bundesregierung muss dazu lediglich eine entsprechende Anzeige bei der EU-Kommission machen.

Allerdings überprüft die EU-Kommission derzeit ohnehin, ob die EU-Richtlinie 2006/24/EG verhältnismäßig ist. Sowohl EU-Innenkommissarin Cecilia Malmström wie auch EU-Justizkommissarin Viviane Reding hatten damals gegen die Richtlinie gestimmt. Die EU-weite Vorgabe einer Erfassung aller Verbindungsdaten wird voraussichtlich schon deshalb geändert werden müssen, weil der Verfassungsgerichtshof Rumäniens entschieden hat, dass eine Vorratsdatenspeicherung mit der Europäischen Menschenrechtskonvention generell unvereinbar ist.

Vor einigen Monaten hat der irische High Court in Dublin bereits [angekündigt](#), dem Europäischen Gerichtshof die Frage vorzulegen, ob die EU-Richtlinie zur Speicherung aller Verbindungsdaten gegen die Ende 2009 in Kraft getretene EU-Grundrechtecharta verstößt und unwirksam ist. „Es ist klar, dass Überwachungsmaßnahmen gerechtfertigt sein müssen und in der Regel gezielt erfolgen sollten“, heißt es in dem Urteil vom 05.05.2010. Ob die EU-Richtlinie aus dem Jahr 2006 überhaupt Bestand haben wird oder ob sie der Europäische Gerichtshof - wie zuvor die Verfassungsgerichte Rumäniens und Deutschlands - aufheben wird, bleibt abzuwarten.

5 Die Strafverfolgung bedarf Verbesserungen ganz anderer Art

Wirklich nützlich zur Verbesserung der Strafverfolgung wären ganz andere Maßnahmen als eine Erfassung aller Verbindungsdaten:

5.1 Schnelle Datensicherung, bessere Ausbildung und Ausstattung

National und international wäre es hilfreich, wenn in rechtsstaatlichem Rahmen eine unverzügliche, schnelle und möglichst unbürokratische Sicherung ohnehin gespeicherter Computer- und Verkehrsdaten für nachfolgende Übermittlungsersuchen veranlasst werden könnte. Wenn auf der Straße ein Verdächtiger noch am Tatort angetroffen wird, kann er festgehalten und seine Identität festgestellt werden. Ebenso wäre es im Internet wichtig, dass ein Tatverdächtiger während der noch bestehenden Internetverbindung durch seinen Internet-Zugangsanbieter auf Ersuchen der Polizei identifiziert wird und die Daten für ein nachfolgendes Ermittlungsverfahren verfügbar gehalten werden. Zurzeit dauert es viel zu lange, bis eine Strafanzeige zu einem sachkundigen Polizeibeamten gelangt; außerdem existiert dann kein Verfahren, in dem der Polizeibeamte die unverzügliche Identifizierung des Verdächtigen durch dessen Internet-Zugangsanbieter anordnen kann.

Der Bund deutscher Kriminalbeamter [fordert](#) dementsprechend beispielsweise die Einrichtung von leistungsfähigen Spezialdienststellen zur Bekämpfung der Computerkriminalität, die Entwicklung eines Berufsbildes „Computerkriminalist“ mit eigenen Aus- und Fortbildungsgängen, die zusätzliche Einstellung von Experten mit abgeschlossenen Studiengängen der Informatik, Mathematik und Betriebswirtschaft und Fortbildung zum Kriminalisten, die Entwicklung standardisierter Sachbearbeitungsverfahren für häufige Arbeitsweisen der Computerkriminalität, die Entwicklung internationaler Standards für IT-Forensik und die Benennung von Schwerpunktstaatsanwaltschaften für Computerkriminalität.

Die Bundesjustizministerin [fordert](#) ebenfalls eine bessere Ausstattung der Ermittler: „Wenn sich in Hamburg 1450 Kripobeamte 50 Rechner mit Internetzugang teilen müssen, wird es schon schwierig mit der Aufklärung. Wenn das BKA nur 30 Experten hat, um gegen Kinderpornografie vorzugehen, ebenfalls. Wenn im gleichen Deliktfeld die personellen Kapazitäten fehlen, Computer-Festplatten hinreichend auszuwerten, dann ist doch klar: Es gibt Vollzugsdefizite, die behoben werden müssen.“

5.2 Kriminalprävention durch Datenschutz

Die häufigste Internet-Straftat ist Betrug, der oft durch Verwendung fremder Identitäten oder Zahlungsdaten begangen wird. Zur Verhütung von Identitätsdiebstahl und sonstigem Datenmissbrauch muss die Verfügbarkeit persönlicher Daten für Straftaten reduziert werden.

1. Dazu muss die Erfassung, Aufbewahrung und Weiterstreuung persönlicher Informationen von Internetnutzern reduziert werden:

- Anbietern von Internetdiensten muss untersagt werden, die Bereitstellung von Internetdiensten von der Angabe personenbezogener Daten abhängig zu machen, die zur Bereitstellung des Dienstes nicht erforderlich sind („Koppelungsverbot“)
- Schutz der Nutzer vor unangemessenen Datenverarbeitungs-Einwilligungsklauseln, indem klargestellt wird, dass derartige Klauseln einer gerichtlichen Kontrolle unterliegen
- Verbot der Erstellung von Nutzerprofilen ohne Einwilligung des Nutzers
- Erstreckung des Fernmeldegeheimnisses auf Anbieter von Internetdiensten
- Schaffung von Rechtssicherheit durch Klarstellung, dass der gesetzliche Datenschutz auch für Internet-Protocol-Adressen gilt
- Anbieter kommerzieller Internetdienste müssen persönliche Daten nach dem jeweiligen Stand der Technik schützen
- Anbieter kommerzieller Internetdienste müssen ihre Nutzer über die Dauer der Aufbewahrung ihrer Daten und über die getroffenen technischen Vorkehrungen zum Schutz ihrer Daten informieren

2. Außerdem muss die Durchsetzung der Gesetze zum Schutz persönlicher Informationen im Internet verbessert werden:

- Wettbewerber, Verbraucherzentralen und Datenschutzverbände müssen das Recht erhalten, Datenschutzverstöße kommerzieller Anbieter von Internetdiensten abzumahn
- Der Verlust persönlicher Daten durch Anbieter von Internetdiensten muss einen Anspruch der Betroffenen auf pauschale Entschädigung nach sich ziehen (z.B. 200 Euro pro Person)
- Privacy by design: Kommerzielle informationstechnische Produkte zur Verarbeitung personenbezogener Daten dürfen nicht so voreingestellt sein, dass der Verwender gegen deutsches Datenschutzrecht verstößt

5.3 Kriminalprävention durch Verbraucherschutz

Security by default: Gebrauchsfertige Geräte zur Internetnutzung sowie kommerzielle Internetdienste müssen von ihrem Hersteller bzw. Anbieter so voreingestellt und bereit gestellt werden, dass die Vertraulichkeit, Verfügbarkeit und Unversehrtheit der Nutzerdaten dauerhaft nach den anerkannten Regeln der Technik gewährleistet ist (z.B. automatische Sicherheitspatches, Firewall, Schadprogrammerkennung). Der Nutzer muss dabei stets die volle Kontrolle über Vorkehrungen zu seinem Schutz behalten und diese auch abschalten können.

„Beipackzettel“: Gebrauchsfertigen Geräten zur Internetnutzung sollten einfache Hinweise zur Vorbeugung vor häufigen Internetdelikten und zur richtigen Reaktion darauf beigelegt werden.

Opfern von Schadprogrammen sollte kostenfreie Unterstützung bei deren Beseitigung zur Verfügung stehen (z.B. Hotline).

6 Ergebnis

Im Ergebnis zeigt sich, dass die gegenwärtig verfügbaren Kommunikationsdaten ganz regelmäßig zur effektiven Aufklärung von Straftaten ausreichen und dass Menschen in allen Bereichen der Gesellschaft auf die Möglichkeit angewiesen sind, telefonische und elektronische Gespräche ebenso vertraulich und spurlos führen zu können wie persönliche Gespräche. Die Erfahrung mit einer Vorratsdatenspeicherung in Deutschland zeigt, dass bei Erfassung sämtlicher Verbindungen nicht mehr Straftaten aufgeklärt oder verhindert wurden als ohne eine solche Vorratsdatenspeicherung; etwas anderes ergibt sich auch nicht aus Berichten des Bundeskriminalamts. Selbst wenn aber in vereinzelten Ermittlungen eine Erfassung aller Verbindungsdaten nützlich wäre, so stünde jedem erhofften Erfolg die Unaufklärbarkeit vieler anderer Straftaten und die Gefährdung von Menschenleben infolge einer Vorratsdatenspeicherung gegenüber.

Insgesamt betrachtet ist eine anlass- und verdachtslose Aufzeichnung jeder Telefon-, Handy-, E-Mail- und Internetverbindung für die Strafverfolgung nutzlos und zudem völlig unverhältnismäßig. Wer Straftaten wirklich wirksamer verfolgen will, müsste ganz andere organisatorische und gesetzliche Maßnahmen ergreifen, wie sie in diesem Bericht vorgeschlagen werden. Die Symboldebatte zum Thema „Vorratsdatenspeicherung“ droht von den wahren Versäumnissen bei dem Schutz der Bürger abzulenken.

23.12.2010