

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