“Ich habe doch nichts zu verbergen!”

Irrtümer und Populismen zu Vorratsdatenspeicherung und Überwachung

Inhaltsverzeichnis

1 Worum geht es?

Der Streit um die Einführung bzw. Fortführung einer Vorratsdatenspeicherung währt nun schon seit einigen Jahren.

Kaum eine anderes innenpolitisches Thema hat es in den letzten Jahren zu einer derart breiten und anhaltenden Diskussion geführt, wie die Frage, ob es mit einer demokratischen Gesellschaft zu vereinbaren wäre, das (Tele-)Kommunikationsverhalten von allen diese Gemeinschaft bildenden Menschen ohne Anlaß und ohne Vorliegen von konkreten Anhaltspunkten digital zu erfassen und zu speichern.

Die Bürgerinitiative "Arbeitskreis Vorratsdatenspeicherung" steht mit ihrer grundsätzlich ablehnenden Haltung häufig am Pranger der von großen Parteien und Lobbygruppen dominierten Medienwelt.

Den häufig stereotyp vorgebrachten Vorwürfen und Kritiken möchten wir in diesem Heft begegnen und darlegen, auf welch tönernden Füßen diese häufig stehen[1].

1 Eine ständig aktualisierte Fassung dieser kritischen Beleuchtung der Argumente gibt es online unter http://www.vorratsdatenspeicherung.de/content/view/83/87/lang.de/

2 Was ist Vorratsdatenspeicherung?

Die Speicherung der Telekommunikations-Verbindungsdaten aller Menschen in Deutschland ohne konkreten Anlaß nennt man Vorratsdatenspeicherung.

Unter Telekommunikations-Verbindungsdaten versteht man:

- Telefon-Verbindungsdaten: Wer hat mit wem von welchem Telefonanschluss wie lange telefoniert bzw. versucht, jemand anderen anzurufen?

- Handy-Verbindungsdaten: Wer hat mit wem unter Verwendung welcher SIM-Karte wie lange telefoniert bzw. versucht, jemand anderen anzurufen. Auch jedes Versenden einer SMS wird (ohne ihren Inhalt) gespeichert.

- In diesem Zusammenhang wird zusätzlich gespeichert, welche Geräte dabei verwendet worden sind (IMEI-Identifikations-Nummern) und in welchen Funkzellen die Geräte während des Gesprächs eingeloggt waren. Letzteres ermöglicht abhängig von der konkreten Funkzellendichte zum Teil recht genaue Standortbestimmungen bzw. Bewegungsprofile alleine schon dadurch, dass sich ein Gesprächsteilnehmer während des Telefonats fortbewegt hat (Fahrrad, U-Bahn, Auto, Zug)

- Internet-Verbindungsdaten: Wer schrieb wem eine E-Mail, welche Internetseiten wurden von welchem Anschluß wann aufgerufen.

3 Populismen zur Vorratsdatenspeicherung

3.1 "Das Ende der Vorratsdatenspeicherung in Deutschland hat zu einer gefährlichen Sicherheitslücke geführt. Eine Vorratsspeicherung aller Verbindungsdaten ist zur Bekämpfung von Terrorismus und organisierter Kriminalität unverzichtbar."

Falsch. Die Zahl der aufgeklärten Straftaten ist ohne Vorratsdatenspeicherung ebenso hoch wie mit Vorratsdaten-speicherung. Eine Vorratsdatenspeicherung erhöht die Aufklärungs-quote nicht. Zur Kriminalitätsbekämpfung sind auch ohne eine Totalprotokollierung jeder Benutzung von Telefon, Handy, E-Mail und Internet **genügend Verbindungsdaten verfügbar**:

- Zu Abrechnungszwecken werden bestimmte Verbindungsdaten ohnehin gespeichert, in Deutschland bis zu sechs Monate lang.

- Darüber hinaus können die Sicherheitsbehörden bei Bedarf eine richterliche Anordnung beantragen, derzufolge die Verbindungsdaten bestimmter Verdächtiger aufzuzeichnen sind.

- Die terroristischen Anschläge in Madrid im Jahr 2004, die Taten der "Sauerland-Attentäter" 2006 und die Vorbereitungen der Düsseldorfer Quaida-Zelle 2011 konnten mit Hilfe von Verbindungsdaten aufgeklärt werden, die ohnehin verfügbar waren. Eine Vorratsdatenspeicherung war nicht erforderlich.

- Bis zum Beschluss der Vorratsspeicherungs-Richtlinie im Jahr 2006 gab es weltweit nur wenige Länder mit Vorratsspeicherungspflichten. In keinem Land gab es eine so umfassende Protokollierung wie in der EU-Richtlinie vorgesehen. Die weltweiten Sicherheitsbehörden sind stets ohne eine Totalprotokollierung der Telekommunikation ausgekommen.

- Nach einem Bericht[2] des Max-Planck-Instituts im Auftrag des Bundesjustizministerium waren Abfragen von Verbindungsdaten auch ohne Vorratsdatenspeicherung in 96% aller Fälle erfolgreich.

- Das Bundeskriminalamt nennt in einer Untersuchung[3] 880 Fälle, in denen den Ermittlungsbehörden Verbindungsdaten fehlten – gemessen an den 6 Mio. pro Jahr begangenen Straftaten eine verschwindend geringe Zahl von 0,01%. Keiner dieser Fälle wies einen Bezug zu Terrorismus auf, obwohl die Bekämpfung des Terrorismus immer wieder als Grund für die Vorratsdatenspeicherung vorgeschoben wird. Laut Bundeskriminalamt fehlen Verbindungsdaten im Wesentlichen nicht bei der Bekämpfung von Terrorismus und organisierte Kriminalität, sondern bei der Verfolgung des Austauschs von Kinderpornografie im Internet. Bei diesen Straftaten wird allerdings bereits ohne Vorratsdatenspeicherung mit die höchste Aufklärungsquote aller Straftaten erreicht.

Auch ohne Vorratsdatenspeicherung werden in Deutschland **80%** aller bekannt gewordener Internetdelikte erfolgreich aufgeklärt - von den sonstigen Straftaten nur 55%. Das Inkrafttreten einer

2 http://www.bmj.de/files/-/3045/MPI-GA-2008-02-13%20Endfassung.pdf

3 http://www.bundesrat.de/cln_179/DE/gremien-konf/fachministerkonf/imk/Sitzungen/10-11-19/anlage10,templateId=raw,property=publicationFile.pdf/anlage10.pdf

Internet-Vorratsdatenspeicherung im Jahr 2009 hat die Zahl der aufgeklärten Internetdelikte nicht erhöht (Aufklärungsrate 2008: 79,8%, 2009: 75,7%). Das Inkrafttreten der Telefon-Vorratsdatenspeicherung im Jahr 2008 hat die Zahl der insgesamt aufgeklärten Straftaten nicht erhöht (Aufklärungsrate 2007: 55,0%, 2008: 54,8%).

Eine Vorratsdatenspeicherung ist **gegen Terrorismus und organisierte Kriminalität wirkungslos**:

- Ernsthafte Kriminelle bleiben unentdeckt, weil sie Umgehungsstrategien einsetzen (z.B. wechselnde Benutzung unregistrierter Prepaid-Handykarten) oder auf andere Kommunikationskanäle ausweichen (z.B. Post, persönliche Treffen).
- Der Präsident des Europäischen Verbands der Polizei Heinz Kiefer warnt: "Für Kriminelle bliebe es einfach, mit relativ simplen technischen Mitteln eine Entdeckung zu verhindern, z.B. durch den Einsatz und häufigen Wechsel im Ausland gekaufter, vorausbezahlter Mobiltelefonkarten. Das Ergebnis wäre ein enormer Aufwand mit wenig mehr Wirkung auf Kriminelle und Terroristen, als sie etwas zu verärgern."

Wirklich nützlich für die Arbeit der Sicherheitsbehörden wären **andere** Maßnahmen, etwa verbesserte Zugriffsmöglichkeiten auf ausländische Verbindungsdaten. Sicherheitsbehörden klagen, dass Auskünfte über Verbindungsdaten aus anderen EU-Staaten nur sehr langsam, aus Nicht-EU-Staaten überhaupt nicht zu erlangen sind. Dies beeinträchtige ihre Arbeit viel stärker als das Fehlen von Verbindungsdaten im Inland. Etwa 80% der Ermittlungen im Bereich Terrorismus und organisierte Kriminalität weisen internationale Bezüge auf[4].

4 Siehe auch: "Vorratsdatenspeicherung: Nützlichkeit ist nicht gleich Sicherheit" -

3.2 "Wenn auch nur ein schweres Verbrechen verhindert werden kann, rechtfertigt dies schon die gesamte Datensammlung."

Falsch. Eine freie und offene Kommunikation ist für unsere Gesellschaft wichtiger als der Versuch, möglichst jede Straftat zu verhindern.

Zunächst einmal wird es kaum jemals vorkommen, dass mithilfe von Verbindungsdaten eine Straftat verhindert werden kann; höchstens können bereits begangene Straftaten aufgeklärt werden.

Selbst, wenn im Ausnahmefall einmal die Verhinderung einer Straftat gelingen könnte, rechtfertigt dies nicht die Aufzeichnung der Kommunikation der gesamten Bevölkerung. Würde die Verhinderung eines Verbrechens jegliche Maßnahme rechtfertigen, müssten wir die Grundrechte aufgeben, auch das Folterverbot und den Schutz der Menschenwürde. All diese **Menschen- und Bürgerrechte** können der Verbrechensbekämpfung nämlich im Einzelfall im Weg stehen. Insgesamt dienen die Grundrechte aber der Erhaltung einer freien Gesellschaft und einer lebendigen Demokratie, letztlich also dem Wohl der gesamten Bevölkerung. Diese Werte sind für uns wichtiger als der Versuch, möglichst jede Straftat zu verhindern.

Wer jede Straftat verhindern will, müsste konsequenterweise auch für ein Verbot des Straßenverkehrs, des Rauchens und des Alkoholkonsums eintreten. All diese Maßnahmen könnten die **Anzahl von Todesfällen** erheblich senken. Wer dagegen eine "Bevormundung" der Bürger ablehnt und deswegen Verkehrsopfer und Krebstote in Kauf nimmt, kann nicht glaubwürdig jedes einzelne "Verbrechen" verhindern wollen.

---

https://www.vorratsdatenspeicherung.de/content/view/249/79/lang,de/

Falsche Prioritätensetzung

Wer ständig mehr Sicherheit fordert, lenkt von den Versäumnissen und der **falschen Prioritätensetzung der Politik** ab. Während die Politik versucht, durch eine lückenlose Überwachung und Kontrolle der Bevölkerung möglichst auch noch den letzten Straftäter zu bestrafen, nimmt sie bewusst in Kauf, dass tausende von Menschen jedes Jahr an den Folgen z.B. von Tabak, Alkohol und Verkehrsunfällen sterben. Zugunsten des Profits einzelner Wirtschaftszweige (Tabakindustrie, Brauereien, Autoindustrie) bleibt die Politik untätig, wo sie Krankheit und Tod unzähliger Menschen leicht verhindern könnte und müsste. Auch bei der Bekämpfung von Armut – eine der wichtigsten Sorgen der Menschen – hat die herrschende Politik in den letzten Jahren beständig versagt, wie die Statistiken zeigen.

Die Auswirkungen von Kriminalität sind im Vergleich zu diesen Problemen ungleich geringer:

- Eurostat zufolge **sterben weniger als 0,002%** der Europäer jährlich als Opfer einer Straftat, terroristische Anschläge eingeschlossen.

- Der Weltgesundheitsorganisation zufolge beruht der Verlust gesunder Lebenszeit für Westeuropäer zu 92% auf Krankheiten, zu 2% auf Verkehrsunfällen, zu 1% auf Stürzen, zu 1,7% auf Suizid und **nur zu 0,2% auf Gewalt und Straftaten**. Die großen Gesundheitsrisiken sind andere als Kriminalität: Bluthochdruck, Tabak, Alkohol, Cholesterin, Übergewicht, Fehlernäherung und Bewegungsmangel sind die Hauptrisikofaktoren. Auch dass uns Lebensrisiken wie Armut, Arbeitslosigkeit oder Naturkatastrophen treffen, ist weitaus wahrscheinlicher als das Risiko, Opfer einer Straftat zu werden.

- Würde man z.B. den Tabakkonsum nur um 2% reduzieren, dann würde man der Gesundheit der Bevölkerung einen größeren Dienst erweisen als durch die Verhinderung sämtlicher Gewalttaten einschließlich Terrorismus.

Wer ständig neue Maßnahmen zur Kriminalitätsbekämpfung fordert, verfehlt damit die **wirklichen Probleme** der Menschen, mit denen sie täglich zu kämpfen haben. Die Kriminalitätsrate hat schon immer in der gleichen Größenordnung wie heute gelegen, ohne unsere Gesellschaft dadurch ernsthaft zu gefährden.

Nachteile

Wer die einzelne, schreckliche Straftat in den Mittelpunkt stellt, ignoriert, dass die **Nachteile einer Totalprotokollierung** deren Nutzen bei weitem überwiegen. Weil die Nachteile einer generellen Kommunikationsprotokollierung für unsere Gesellschaft deren Vorteile bei weitem überwiegen, ist eine Vorratsdatenspeicherung **unverhältnismäßig**. Selbst der Schutz vor Verbrechen rechtfertigt keine unverhältnismäßigen Maßnahmen.

- Eine Vorratsspeicherung schreckt **Informanten von Journalisten** davon ab, wichtige Informationen über Missstände per Telefon, Fax oder Internet weiterzugeben. Informanten müssten ständig damit rechnen, dass ihr Kontakt mithilfe von Verbindungsdaten aufgedeckt werden kann.

- Wer bei einem Anwalt, einem Arzt oder einer Beratungsstelle (z.B. Eheberatung, Suchtberatung, Telefonseelsorge) Rat sucht, muss bedenken, dass der Kontakt Rückschlüsse auf sein **persönliches Problem** (z.B. Ermittlungsverfahren, Krankheit, Ehekrise, Suchtproblem) zulassen kann und im Fall des Bekanntwerdens Nachteile

drohen. Für Prominente, denen die Sensationspresse auf Schritt und Tritt nachspioniert, ist dies eine besondere Gefahr.

- Vertrauliche Verhandlungen in der Wirtschaft über Großaufträge oder Fusionen würden behindert, weil die Beteiligten mit **Wirtschaftsspionage** rechnen müssten. Konkurrenzunternehmen können auf Verbindungsdaten zugreifen, um Aufträge "wegzuschnappen" oder Zusammenschlüsse zu verhindern.

- **Politiker werden erpressbar**, weil ihre Kontakte zu umstrittenen Personen (z.B. Lobbyisten, Industrielle) nachvollziehbar werden.

- Die Arbeit von **politischen Aktivisten** (z.B. Globalisierungskritiker, Castorgegner) wird behindert, weil sie mit einer - auch nachträglichen - Aufdeckung ihrer Netzwerke durch den Verfassungsschutz rechnen müssten.

Insgesamt geht die **Unbefangenheit** weiter Teile der zwischenmenschlichen Kommunikation verloren, und zwar spätestens, sobald der erste Missbrauchsfall an das Licht der Öffentlichkeit gelangt. Abhörskandale hat es bereits in Griechenland und Italien gegeben. In den USA können Verbindungsdaten käuflich erworben werden. In Deutschland hat die Deutsche Telekom missbräuchlich 250.000 Telefonverbindungsdaten und Handy-Positionsdaten von Journalisten sowie von Arbeitnehmer-

Aufsichtsräten und Managern des Unternehmens ausgewertet[5], um undichte Stellen im Unternehmen zu ermitteln. Außerdem hat ein Mitarbeiter von T-Mobile die Daten von 17 Mio. Kunden - darunter geheimer Nummern und Privatadressen von bekannten Politikern, Ministern, Ex-Bundespräsidenten, Wirtschaftsführern, Milliardären und Glaubensvertretern - verkauft[6], die nun in kriminellen Kreisen kursieren. Dass auch vorratsgespeicherte Kommunikationsdaten missbraucht werden, ist nur eine Frage der Zeit - und der Geldsumme, die z.B. einem Telekom-Mitarbeiter für eine Auskunft angeboten wird.

5 http://www.daten-speicherung.de/index.php/faelle-von-datenmissbrauch-und-irrtuemern/#Deutschland_3
6 http://www.spiegel.de/wirtschaft/0,1518,581938,00.html

3.3 "Nach dem Ende der Vorratsdatenspeicherung ist das Internet ein rechtsfreier Raum."

Falsch. Auch ohne Vorratsdatenspeicherung werden 80% aller bekannt gewordenen Internetdelikte aufgeklärt (2008: 79,8%[7]). Zum Vergleich: Nur 55% der außerhalb des Internets begangenen Straftaten werden aufgeklärt (2009: 55.6%[8]).

Während Internet-Verbindungsdaten in Deutschland auf Vorrat gespeichert wurden, stieg die vorher hohe Aufklärungsquote nicht, sondern sie ging sogar zurück (2009: 75.7%[9]), vermutlich weil verstärkt Gegenmaßnahmen (z.B. ausländische Anonymisierungsdienste) eingesetzt wurden. Die Vorratsdatenspeicherung schadet also der Strafverfolgung, weil sie zum Einsatz von Umgehungsmaßnahmen führt, deren Anonymität selbst im Verdachtsfall nicht mehr aufgehoben werden kann.

Die Sicherheitsbehörden vieler Staaten Europas und weltweit arbeiten bis heute erfolgreich ohne verdachtslose Vorratsdatenspeicherung (z.B. Österreich, Griechenland, Norwegen, Rumänien, Schweden, Australien, Kanada, Japan). Niemand kann ernsthaft behaupten, in diesen Staaten sei das Internet ein "rechtsfreier Raum".

Die Aufklärung von Internet-Straftaten gelingt auch ohne Vorratsdatenspeicherung zu 80%, weil Internetverbindungen in Zeiten von Pauschaltarifen (Flatrates) lange aufrecht erhalten werden und die Behörden entsprechend lange Zeit haben, um einen Internetnutzer noch während der bestehenden Verbindung zu identifizieren. Wo dies nicht gelingt, ist eine Fangschaltung möglich: Der Verdächtige wird dann bei seiner nächsten Verbindung mit dem entsprechenden Dienst identifiziert.

7 http://www.bka.de/pks/pks2008/download/pks-jb_2008_bka.pdf
8 http://www.bka.de/pks/pks2009/download/pks2009_imk_kurzbericht.pdf

3.4 "Wegen der Zunahme von Flatrates stehen den Ermittlungsbehörden heute weniger Verbindungsdaten zur Verfügung als vor Einführung der Vorratsdatenspeicherung."

Falsch. Den Ermittlungsbehörden stehen von Jahr zu Jahr mehr Verbindungsdaten zur Verfügung.

Hauptsächlich Internetverbindungen werden verbreitet pauschal tarifiert. 2008, vor Inkrafttreten der Pflicht zur Vorratsspeicherung von Internetverbindungen, nutzten jedoch bereits 86%[10] der Internetnutzer eine Flatrate. Dieser Anteil ist heute nicht wesentlich höher.

Vor Inkrafttreten der Pflicht zur Vorratsdatenspeicherung im Internetbereich am 01.01.2009 speicherten Internet-Zugangsanbieter die Zuordnung der von ihren Kunden genutzten Internetadressen nicht oder höchstens wenige Tage lang (bis 7 Tage[11]). Nicht anders verhält es sich auch gegenwärtig wieder (Übersicht[12]). Übrigens fielen bis zur Einführung digitaler Vermittlungsstellen in den 90er Jahren keinerlei Verbindungsdaten an, ohne dass dies eine Strafverfolgung unmöglich gemacht hätte.

Tatsächlich nimmt die Anzahl der verfügbaren Kommunikationsspuren im Informationszeitalter zu und nicht ab, weil an die Stelle persönlicher Gespräche und Briefe zunehmend elektronische Kommunikation tritt. Selbst wenn in einzelnen Fällen die Verfügbarkeit von Verkehrsdaten abgenommen hat, ist dieser Effekt klein im Vergleich zu der rapide anwachsenden Informationsmenge, auf die der Staat insgesamt Zugriff hat.[13]

9 http://www.bka.de/pks/pks2009/download/pks-jb_2009_bka.pdf

3.5 "Kommunikationsinhalte werden nicht gespeichert."

Das ist für sich genommen zwar richtig, aber **irreführend**. In vielen Fällen lässt sich der Kommunikationsinhalt nämlich anhand der Verbindungsdaten rekonstruieren.

Schon die Person des Gesprächspartners lässt oft **Rückschlüsse auf den Gesprächsinhalt** zu. Es liegt auf der Hand, weshalb jemand eine Ehe- oder Drogenberatungsstelle anruft, einen auf Geschlechtskrankheiten spezialisierten Arzt, einen Fachanwalt für Steuerstrafrecht oder eine Telefonsexnummer. Bei Politikern können Kontakte zu Lobbyisten oder zu Prostituierten von Interesse sein.

In einem Versuch[14] des US-amerikanischen Forschungszentrums MIT wurden Telekommunikations-Verbindungsdaten und auf 10m genaue Standortdaten von 100 Versuchspersonen erhoben. Mithilfe dieser Daten gelang es mit einer 90%igen Genauigkeit, die Arbeitskollegen, Bekannten und Freunde einer jeden Person zu identifizieren. Ferner waren umfangreiche Vorhersagen möglich. Anhand der Bewegungsdaten einer Person während eines Monats konnte mit einer 95%igen Genauigkeit vorhergesagt werden, wann sich die Person am Arbeitsplatz, zu Hause oder an einem anderen Ort aufhalten würde. Weiter konnte mit einer 90%igen Genauigkeit vorhergesagt werden, ob sich zwei Personen innerhalb der nächsten Stunde begegnen würden. Anhand der Aktivitäten einer Person während der ersten 12 Stunden eines Tages konnten die Aktivitäten während der verbleibenden 12 Stunden mit etwa 80% Genauigkeit vorhergesagt werden. Auch die Zufriedenheit am Arbeitsplatz konnte anhand der Daten vorhergesagt werden.

10 http://www.ard-zdf-onlinestudie.de/fileadmin/Onlineo8/Fisch_I.pdf
11 http://www.heise.de/newsticker/meldung/Datenschuetzer-haelt-siebentaegige-Speicherung-von-Verbindungsdaten-fuer-angemessen-150197.html
12 http://wiki.vorratsdatenspeicherung.de/Speicherdauer
13 Weitere Informationen: https://www.vorratsdatenspeicherung.de/images/schriftsatz_2008-03-17.pdf

Bei der Nutzung des **Internet** werden die abgerufenen Inhalte, die Klicks und Suchwörter des Nutzers oft von dem Anbieter freiwillig mitprotokolliert ("Server-Logfiles"). Hier genügen schon die Verbindungsdaten des Internet-Zugangsanbieters (IP-Adresse), um die Kommunikationsinhalte minuziös nachvollziehen zu können.

Es besteht die Gefahr, dass die Vorratsdatenspeicherung in Zukunft auf Kommunikationsinhalte **ausgedehnt** wird. In Italien werden beispielsweise SMS bereits gespeichert. Mit dem Argument, dass die Daten zur Strafverfolgung benötigt werden, lässt sich in Zukunft durchaus auch eine Inhaltsspeicherung rechtfertigen.

14 http://reality.media.mit.edu/dyads.php

3.6 "Verbindungsdaten wurden schon immer gespeichert; sie sollen künftig nur länger aufbewahrt werden."

Das ist **falsch**.

Ohne Vorratsdatenspeicherung dürfen Telekommunikationsanbieter nur die Verbindungsdaten speichern, von denen die **Rechnungshöhe** abhängt (§ 97 Absatz 3 Telekommunikationsgesetz[15]). Deswegen dürfen etwa eingehende Verbindungen (z.B. ankommende Anrufe), Handy-Standortdaten (Wer hat wo telefoniert?) und E-Mail-Verbindungsdaten (Wer hat wem eine E-Mail geschickt?) nicht gespeichert werden. Auch die beim Internet-Surfen genutzte Kundenkennung (IP-Adresse) dürfen Anbieter nicht speichern. Bei Pauschaltarifen ("flatrates") dürfen keinerlei Verbindungsdaten gespeichert werden, weil dies nicht zur Abrechnung erforderlich ist[16].

Es werden somit derzeit sehr viel weniger Verbindungsdaten gespeichert als mit einer Vorratsdatenspeicherung. Außerdem lässt sich die Speicherung von Verbindungsdaten zurzeit insgesamt verhindern (Flatrate), was eine Vorratsdatenspeicherung ändern würde. Nach Schätzungen führte eine Vorratsdatenspeicherung zur Speicherung 100-mal so vieler Verkehrsdaten wie bisher. Es kann daher keine Rede davon sein, dass sich nichts Wesentliches ändere.

15 http://bundesrecht.juris.de/tkg_2004/__97.html
16 http://www.heise.de/newsticker/meldung/80614

3.7 "Der Zugriff auf die gespeicherten Daten wird nur unter engen Voraussetzungen (z.B. richterliche Anordnung) zugelassen."

Falsch. Verbindungs- und Standortdaten werden schon heute in **tausenden[17] von Strafverfahren jährlich** abgefragt, die Identität von Telefon-, Handy-, E-Mail- und Internetnutzern (Bestandsdaten) wird sogar mehrere Millionen Mal jährlich abgefragt (4,5 Mio.[18] mal im Jahr 2009 oder über 10.000mal am Tag). Die Vorratsdatenspeicherung hat die Zahl der Abfragen noch einmal sprunghaft ansteigen lassen. In Anbetracht dessen kann keine Rede davon sein, dass der Zugriff auf die gespeicherten Daten engen Voraussetzungen unterliege.

- In Deutschland sind Zugriffe auf Verbindungsdaten **bei jedem Verdacht** einer "erheblichen" oder einer "mittels Telekommunikation begangenen" Straftat gesetzlich zugelassen (§ 100g StPO). Zugriff erhalten zu diesem Zweck die Staatsanwaltschaft und die Polizei, aber auch **ausländische Staaten** wie die USA, Albanien, Azerbaijan und Russland im Rahmen von Rechtshilfeübereinkommen (§ 59 IRG[19]). Was mit den Daten im Ausland geschieht, ist nicht kontrollierbar. Bei Abfragen zur Verfolgung von Straftaten ist eine **richterliche Anordnung** erforderlich (§ 100g StPO), aber auch hier überprüft der Richter nur das Vorliegen der gesetzlichen Voraussetzungen. Sind diese gegeben, muss er den Zugriff genehmigen.

- **Nachrichtendienste** dürfen ohne richterliche Genehmigung Verbindungsdaten abfragen (§ 8a BVerfSchG,

17 http://www.bundesjustizamt.de/cln_101/nn_1635504/DE/Themen/Justizstatistik/Telekommunikations_C3_BCberwachung/downloads/_C3_9Cbersicht_20Vd_C3_BC_202008,templateId=raw,property=publicationFile.pdf/%C3%9Cbersicht%20Vd%C3%BC%202008.pdf

§ 10 MAD-G, § 8 Abs. 3a BND-G). Auf Vorrat gespeicherte Verbindungsdaten dürfen aufgrund des jetzt beschlossenen Gesetzes noch nicht an Nachrichtendienste übermittelt werden. Es bedarf dazu eines weiteren Gesetzes.

- Zugriff auf die Identität von Telefon-, Handy-, E-Mail- und Internetnutzern (Name, Anschrift, Geburtsdatum) haben nach § 113 TKG 1.000 verschiedene Behörden (z.B. Polizei, Staatsanwaltschaft, Geheimdienste, Zoll, Behörden zur Bekämpfung von Schwarzarbeit). Schon die Verfolgung von Ordnungswidrigkeiten (z.B. Falschparken) werden Zugriffe in einem **direkten Online-Abrufverfahren** zugelassen (§ 112 TKG). In keinem dieser Fälle ist eine richterliche Anordnung erforderlich.

- Auch die **Film- und Musikindustrie** und andere "Rechteinhaber" dürfen Auskunft über die Identität von Telefon-, Handy-, E-Mail- und Internetnutzern verlangen, etwa um die Benutzung von Tauschbörsen im Internet verfolgen zu können (§ 101 UrhG[20]). Hier ist zwar eine richterliche Anordnung erforderlich, aber der Richter überprüft nur das Vorliegen der gesetzlichen Voraussetzungen. Sind diese gegeben, muss er den Zugriff genehmigen.

Eine Untersuchung[21] über das Abhören von Telefonen hat im Übrigen gezeigt, dass das Erfordernis eines "richterlichen Beschlusses" **keine wirksame Kontrolle** gewährleistet: In sehr vielen Fällen wurde eine Blankoerlaubnis erteilt, ohne dass auch nur die eingereichten Schriftstücke näher begutachtet und bei

18 http://www.bundesnetzagentur.de/cae/servlet/contentblob/152206/publicationFile/6683/Jahresbericht2009Id18409pdf.pdf

19 https://www.vorratsdatenspeicherung.de/content/view/154/79/

Fehlen der rechtlichen Voraussetzungen Anträge abgelehnt wurden[22]. Der "richterliche Beschluss" konnte auch nicht verhindern, dass die Anzahl von Telefonüberwachungen seit Jahren immer weiter ansteigt - aufgrund einer Verwässerung der Voraussetzungen für Überwachungsmaßnahmen, nicht etwa aufgrund eines entsprechend starken Anstiegs der Verbrechensanzahl. Dass nur die Einrichtung der Überwachung, nicht aber deren weitere Durchführung der richterlichen Kontrolle unterliegt, wird dabei ebenfalls immer wieder von Datenschützern bemängelt[23].

Abgesehen davon zeigt nicht nur die Mautbrückendiskussion[24], wie unsicher rechtlich geschützte Datensammlungen auf Dauer sind. Zugriffsbeschränkungen, die heute noch gesetzlich vorgesehen sind, können morgen schon **durch Gesetzesänderungen verwässert** oder aufgehoben werden. Dieser Mechanismus ist immer wieder zu beobachten. Beispielsweise war der Zugriff auf Bankkonten-Stammdaten ursprünglich nur zur Bekämpfung des Terrorismus eingeführt worden. Heute haben Finanzämter, Sozialämter und viele mehr Zugriff auf diese Daten.

All diese Aspekte sind Grund genug, an der dauerhaften Sicherheit der Daten vor **Missbrauch** sowie dem Zugriff nichtstaatlicher Stellen zu zweifeln. Das Aushebeln gesetzlicher Schutzmechanismen (z.B. Mautzweckbindung), Gummiparagraphen (sehr unscharfe Gesetze), menschliches Versagen (z.B. fehlerhafte richterliche Kontrolle) und die fortschreitende Auslagerung von Staatsaufgaben an die private Wirtschaft (Datenzugriff von "Rechteinhabern") lassen kaum erwarten, dass gerade bei vorratsgespeicherten Daten mit besonderer Gewissenhaftigkeit

20 http://www.gesetze-im-internet.de/urhg/__101.html
21 http://www.bmj.bund.de/files/-/136/Abschlussbericht.pdf
22 http://www.heise.de/newsticker/meldung/33558
23 http://www.heise.de/newsticker/meldung/72439
24 http://www.heise.de/newsticker/meldung/76391

vorgegangen wird.

In einer ganzen Reihe von Fällen sind Telekommunikationsdaten in Deutschland (z.B. Telekom-Skandal[25]), Italien, Griechenland, Lettland, Bulgarien, der Slowakei und Ungarn missbraucht worden oder verloren gegangen. Telekommunikationsunternehmen wie die Deutsche Telekom oder Vodafone ist es immer wieder nicht gelungen, gespeicherte Verbindungsdaten zu schützen. Solche Daten wurden gestohlen, verkauft und missbraucht. Der Bundesdatenschutzbeauftragte stellte[26] 2009 schwere Mängel bei der damaligen Vorratsdatenspeicherung fest: Der Zugriff auf die Daten war nicht nachvollziehbar, es wurden mehr Daten gespeichert als erlaubt (z.B. Standortdaten und E-Mail-Daten) und die Daten wurden nicht nach sechs Monaten gelöscht.

25 http://de.wikipedia.org/wiki/%C3%9Cberwachungsaff%C3%A4re_der_Deutschen_Telekom

26 https://www.vorratsdatenspeicherung.de/images/vb_bfdi_schreiben_2009-11-24_1-bvr-256-08.pdf

3.8 "Deutschland ist verpflichtet, die europäische Richtlinie zur Vorratsdatenspeicherung umzusetzen und wieder eine Vorratsdatenspeicherung einzuführen."

Falsch. Deutschland muss und darf die europäische Richtlinie zur Vorratsdatenspeicherung nicht umsetzen.

Artikel 114 (4) AEUV gibt Deutschland das Recht, trotz der EG-Richtlinie das aktuelle Verbot der Vorratsdatenspeicherung (§ 96 Telekommunikationsgesetz) wegen wichtiger Erfordernisse des

Grundrechtsschutzes beizubehalten[27]. Die Bundesjustizministerin braucht der Europäischen Kommission nur die beibehaltenen Bestimmungen des deutschen Rechts zu melden und die Gründe für deren Beibehaltung mitzuteilen.

Die EG-Richtlinie 2006/24 zur Vorratsdatenspeicherung ist wegen der Verletzung der 2009 in Kraft getretenen **EU-Grundrechtecharta** rechtswidrig. Der Europäische Gerichtshof wird auf Vorlage[28] eines irischen Gerichts über die Rechtmäßigkeit der Richtlinie zu entscheiden haben.

Die E**uropäische Menschenrechtskonvention**, zu deren Einhaltung Deutschland verpflichtet ist, verbietet die Umsetzung der Richtlinie zur Vorratsdatenspeicherung. Eine Vorratsdatenspeicherung verstößt[29] gegen mehrere Artikel dieser Konvention. Dies hat der Rumänische Verfassungsgerichtshof bereits entschieden[30].

Das Urteil des **Bundesverfassungsgerichts** ändert an dieser Rechtslage nicht. Das Bundesverfassungsgericht hat nur über die Vereinbarkeit einer Vorratsdatenspeicherung mit dem deutschen Grundgesetz entschieden, nicht aber mit der EU-Grundrechtecharta und der Europäischen Menschenrechtskonvention.

27 http://www.daten-speicherung.de/index.php/keine-eu-pflicht-zur-wiedereinfuehrung-einer-vorratsdatenspeicherung/
28 https://www.vorratsdatenspeicherung.de/content/view/366/79/
29 http://www.tkg-verfassungsbeschwerde.de/data_retention_and_human_rights_essay.pdfß
30 https://www.vorratsdatenspeicherung.de/content/view/342/79/

3.9 "Durch die Vorratsdatenspeicherung werden Bürgerrechte nicht beschnitten."

Diese Behauptung, die Bundesjustizministerin Brigitte Zypries (SPD) 2006 vor dem Deutschen Bundestag aufgestellt[31] hat, ist **falsch**.

Am schwersten wiegt die **Verletzung des Fernmeldegeheimnisses**: Ohne jeden Verdacht einer Straftat werden sensible Informationen über die sozialen Beziehungen (einschließlich Geschäftsbeziehungen), die Bewegungen und die individuelle Lebenssituation (z.B. Kontakte mit Ärzten, Rechtsanwälten, Psychologen, Beratungsstellen) von über 80 Millionen Bundesbürgerinnen und Bundesbürgern gesammelt. Damit höhlt die Vorratsdatenspeicherung Anwalts-, Arzt-, Seelsorge-, Beratungs- und andere Berufsgeheimnisse aus und begünstigt Wirtschaftsspionage. Sie untergräbt den Schutz journalistischer Quellen und beschädigt damit die Pressefreiheit im Kern. Es werden Berge von Spuren und Beweismaterial gegen jeden gesammelt, ohne dass der geringste Verdacht gegen die Betreffenden vorliegt. Das steht in klarem Widerspruch zur Europäischen Menschenrechtskonvention.

Man vergleiche die Vorratsdatenspeicherung einmal mit dem Versenden von Briefen, bei denen man auf dem Umschlag nicht einmal den Absender angeben muss. Eine **"Vorratsdaten-speicherung für Briefe"** würde bedeuten, dass der Staat registrieren lässt, wer wem wann einen Brief geschickt hat. Eine "Vorratsdatenspeicherung für Gespräche" würde bedeuten, dass staatliche Spitzel überall mitschreiben, wer wann mit wem geredet hat. An diesen Beispielen wird deutlich, dass eine Vorratsdatenspeicherung der Stasi würdig ist, nicht aber einem demokratischen Rechtsstaat.

31 http://www.heise.de/newsticker/meldung/74493

3.10 "Laut Bundesverfassungsgericht ist die Vorratsdatenspeicherung mit den Grundrechten vereinbar."

Falsch. Das Bundesverfassungsgericht hat sich nur zur Vereinbarkeit einer Vorratsdatenspeicherung mit den Grundrechten des Grundgesetzes geäußert, nicht aber mit den Grundrechten der Europäischen Menschenrechtskonvention und der EU-Grundrechtecharta. Mit den zuletzt genannten Grundrechtskatalogen ist eine Vorratsdatenspeicherung unvereinbar.

Die Vorratsdatenspeicherung verletzt die 2009 in Kraft getretene **EU-Grundrechtecharta**. Der Europäische Gerichtshof wird darüber auf

Vorlage[32] eines irischen Gerichts aus dem Jahr 2010 zu entscheiden haben. Das Bundesverfassungsgericht hat sich dazu nicht geäußert und ist dafür auch nicht zuständig.

Die **Europäische Menschenrechtskonvention**, zu deren Einhaltung Deutschland verpflichtet ist, verbietet ebenfalls die Einführung einer Vorratsdatenspeicherung. Dies hat der Rumänische Verfassungsgerichtshof bereits entschieden[33]. Das Bundesverfassungsgericht hat sich zu der Europäischen Menschenrechtskonvention nicht geäußert, sondern nur zu dem Grundgesetz.

Der **Europäische Gerichtshof für Menschenrechte** entschied[34] im Jahr 2008, "dass die umfassende und wahllose Befugnis zur Speicherung von Fingerabdrücken, Zellproben und DNA-Profilen von verdächtigten, aber nicht verurteilten Personen [...] keinen gerechten Ausgleich zwischen den widerstreitenden öffentlichen und privaten Interessen trifft und der belangte Staat in dieser Hinsicht jeden akzeptablen Ermessensspielraum überschritten hat. Die umstrittene Speicherung begründet daher einen unverhältnismäßigen Eingriff in das Recht der Beschwerdeführer auf Achtung des Privatlebens, der nicht als notwendig in einer demokratischen Gesellschaft angesehen werden kann." Nichts anderes kann für die Vorratsdatenspeicherung gelten, die sogar die gesamte Bevölkerung treffen soll.

32 https://www.vorratsdatenspeicherung.de/content/view/366/79/
33 https://www.vorratsdatenspeicherung.de/content/view/342/79/
34 http://www.menschenrechte.ac.at/docs/08_6/08_6_14

3.11 "Vertrauensberufe wie Strafverteidiger, Seelsorger und Bundestagsabgeordnete werden von der Vorratsdatenspeicherung ausgenommen."

Falsch. Auch Kontakte von und zu diesen Personen sowie deren Handy-Positionsdaten wurden auf Vorrat gespeichert.

Nur die Abfrage dieser Daten wurde den Strafverfolgern untersagt. Das Verbot galt aber erstens nur, wenn die Daten unter das Berufsgeheimnis fallen. Es galt zweitens nicht, wenn der Berufsgeheimnisträger selbst im Verdacht stand, an einer Straftat beteiligt zu sein. Drittens weiß die Polizei bei der Abfrage von Verbindungs- oder Bewegungsdaten oftmals nicht, ob der Betroffene oder seine Gesprächspartner Berufsgeheimnisträger sind. Das Erhebungsverbot ist also weitgehend wirkungslos. Viertens gilt die Zugriffsbeschränkung nur für Zugriffe der Strafverfolger, nicht aber für Nachrichtendienste und präventive Zugriffe von Polizeibehörden.

3.12 "Die Entscheidung des Bundesverfassungsgerichts führt zu einem angemessenen Kompromiss."

Richtig. Nach dem Urteil des Bundesverfassungsgerichts ist nur noch die gezielte Überwachung Verdächtiger zulässig und nicht mehr eine Speicherung der Verbindungsdaten von Millionen völlig Unbeteiligter. Dieses Verfahren stellt einen angemessenen Kompromiss dar, der sich in vielen Staaten weltweit bewährt hat.

Mit Urteil vom 2. März 2010 hat das Bundesverfassungsgericht die deutschen Vorschriften zur Vorratsdatenspeicherung **für nichtig erklärt**. Zur Begründung hat es ausgeführt, die Vorratsdatenspeicherung verstoße in ihrer bisherigen Ausgestaltung gegen das Grundgesetz. Eine Vorratsdatenspeicherung könne allerdings ohne Verstoß gegen das Grundgesetz wieder eingeführt werden, wenn die Daten sicherer gespeichert würden, wenn sie nur unter höheren Voraussetzungen an den Staat weiter geleitet würden und wenn Vertrauensbeziehungen besonders geschützt würden. Auch eine solche "Vorratsdatenspeicherung 2.0" wäre indes inakzeptabel: Im Zuge einer solchen Vorratsdatenspeicherung würden wieder ohne jeden Verdacht einer Straftat sensible Informationen über die sozialen Beziehungen (einschließlich Geschäftsbeziehungen), die Bewegungen und die individuelle Lebenssituation (z.B. Kontakte mit Ärzten, Rechtsanwälten, Betriebsräten, Psychologen, Beratungsstellen) von über 80 Millionen Bundesbürgerinnen und Bundesbürgern gesammelt. Damit höhlte die Vorratsdatenspeicherung Anwalts-, Arzt-, Seelsorge-, Beratungs- und andere Berufsgeheimnisse aus und begünstigte Datenpannen und -missbrauch. Sie würde den Schutz journalistischer Quellen untergraben und damit die Pressefreiheit im Kern beschädigen. Sie beeinträchtigte insgesamt die Funktionsbedingungen unseres freiheitlichen demokratischen Gemeinwesens.

3.13 "Quick Freeze läuft ohne Vorratsdatenspeicherung leer. Was nicht gespeichert ist, kann auch nicht eingefroren werden."

Falsch. Ein Verfahren zur schnellen Sicherung von Verkehrsdaten ("Quick Freeze") setzt keine Vorratsdatenspeicherung voraus.

Eine Aufbewahrungsanordnung ermöglicht es Ermittlern, vorhandene Verkehrsdaten im Verdachtsfall sichern zu lassen, die andernfalls möglicherweise gelöscht würden. Herausgegeben werden die "eingefrorenen" Daten an die Ermittlungsbehörde erst, wenn die gesetzlichen Voraussetzungen dafür vorliegen. Beispielsweise kann eine richterliche Genehmigung gefordert werden.

Eine Aufbewahrungsanordnung ist erstens während der Dauer der jeweiligen Verbindung möglich. Während einer laufenden Verbindung kann eine Rückverfolgung auch ohne Vorratsdatenspeicherung erfolgen. Da pauschal tarifierte Internetverbindungen typischerweise lange aufrecht erhalten werden, kann eine schnelle Identifizierung im Internet sogar leichter möglich sein als bei sonstigen Straftaten. Lange nach Begehung eines Internetdelikts kann der Täter noch festgestellt werden, wo er sonst den Tatort schon lange verlassen hätte.

Eine Aufbewahrungsanordnung ist zweitens auch nach Verbindungsende möglich, wo Verkehrsdaten aus betrieblichen Gründen, insbesondere zu Abrechnungszwecken, ohnehin gespeichert werden. Dies erfolgt in Deutschland bis zu sechs Monate lang.

Richtig ist, dass nicht gespeicherte Verbindungsdaten nicht an den Staat herausgegeben oder für diesen "eingefroren" werden können. Dies ist indes kein Nachteil, sondern unabdingbare Voraussetzung für die Gewährleistung der Vertraulichkeit und Unbefangenheit der Kommunikation von zu 99,9% vollkommen unbescholtener Menschen.

3.14 "Das Bundesverfassungsgericht hat Quick Freeze als Alternative zur Vorratsdatenspeicherung verworfen."

Falsch. Das Bundesverfassungsgericht hat Quick Freeze als Alternative zur Vorratsdatenspeicherung keineswegs verworfen.

Das Bundesverfassungsgericht hat festgestellt, der Gesetzgeber dürfe nach dem Grundgesetz eine sechsmonatige Speicherung aller Telekommunikationsverkehrsdaten als erforderlich beurteilen, weil eine gezielte Aufbewahrung nicht in jedem Einzelfall so wirksam sei wie eine globale und pauschale Vorratsdatenspeicherung. Die verfassungsrechtliche Hürde der "Erforderlichkeit" ist allerdings äußerst niedrig: Schon eine einzige Bagatellstraftat, die nur durch Vorratsdatenspeicherung aufzuklären ist, verhilft der radikalen Vorratsdatenspeicherung über die Erforderlichkeitshürde, selbst wenn insgesamt betrachtet ohne Vorratsdatenspeicherung sogar mehr Straftaten aufgeklärt werden können, wie es im Bereich der Internetkriminalität der Fall war.

Für die politische Debatte über die Notwendigkeit und Verhältnismäßigkeit einer globalen und pauschalen Vorratsdatenspeicherung kann das minimale verfassungsrechtliche Erforderlichkeitsgebot nicht maßgeblich sein. Politisch ist vielmehr entscheidend, dass im Internet keine rechtsfreien Räume entstehen und Internetdelikte ebenso wirksam aufgeklärt werden können wie außerhalb des Internet begangene Delikte. Dies ist, wie oben erläutert, auch ohne Vorratsdatenspeicherung gewährleistet.

3.15 "Eine ein- oder zweiwöchige Vorratsdatenspeicherung ("Quick Freeze Plus") wäre ein angemessener Kompromiss."

Falsch. Eine kürzere Speicherdauer würde nichts an den fatalen Wirkungen jeder allgemeinen und unterschiedslosen Totaldatenspeicherung ändern:

Jede allgemeine Verbindungsdatenaufzeichnung 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.

Das ständige Risiko von Nachteilen infolge von Kommunikationsprotokollen entfaltet eine enorme Abschreckungswirkung und vereitelt eine unbefangene Telefon- und Internetnutzung in sensiblen Situationen (z.B. anonyme Information von Journalisten, 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.

Die Zulassung einer Vorratsdatenspeicherung wäre ein Dammbruch 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.

3.16 "Die Ablehnung jeder Vorratsdatenspeicherung ist eine fundamentalistische Extremposition."[35]

Falsch. Umgekehrt wäre die Forderung einer flächendeckenden Vorratsspeicherung sämtlicher Verbindungsdaten aller Bürger ohne jeden Anlass eine radikale Extremposition.

Das Grundgesetz erlaubte ursprünglich keinerlei staatliche Eingriffe in die Vertraulichkeit des Fernmeldeverkehrs. Infolge der Notstandsgesetze konnten Richter und bei Gefahr im Verzug auch die Staatsanwaltschaft die Aufzeichnung der Telekommunikationsverbindungen von Personen verlangen, die im Verdacht standen, eine Straftat begangen zu haben. Die Idee einer "Vorratsdatenspeicherung" sieht vor, dass **ohne Verdacht und Anordnung** für die **gesamte Bevölkerung** aufgezeichnet wird, wer wann mit wem in Verbindung stand, wo sein Handy nutzte und unter welcher Kennung das Internet nutzte. Eine solche Totaldatenspeicherung wäre ebenso extrem und radikal wie ein komplettes Verbot jeder Aufzeichnung von Verbindungsdaten. Dass Gerichte und Staatsanwaltschaften zur Verfolgung von Straftaten nur im Bedarfsfall die Verbindungen Tatverdächtiger aufzeichnen lassen können, ist ein seit Jahrzehnten praktizierter rechtsstaatlicher Kompromiss und keine "fundamentalistische Extremposition"

35 http://www.heise.de/ct/artikel/Kommentar-Bei-der-Vorratsdatenspeicherung-gibt-es-nicht-nur-Schwarz-und-Weiss-1337311.html

3.17 "Das Zusammenleben in einer demokratischen Gesellschaft verlangt differenzierte Betrachtungen."[36]

Richtig, deswegen ist eine undifferenzierte Vorratsspeicherung sämtlicher Verbindungsdaten in einer demokratischen Gesellschaft nicht akzeptabel.

36 http://www.heise.de/ct/artikel/Kommentar-Bei-der-Vorratsdatenspeicherung-gibt-es-nicht-nur-Schwarz-und-Weiss-1337311.html

3.18 "Die Ablehnung jeder Vorratsdatenspeicherung ohne konstruktive Gegenvorschläge ist nicht sinnvoll."[37]

Falsch, unsere Freiheitsrechte sind nicht verhandelbar.
Als Gegner einer anlasslosen Vorratsdatenspeicherung unterbreiten wir im Übrigen seit langem Vorschläge[38], die tatsächlich zur Verbesserung der Strafverfolgung beitragen könnten, etwa in den Bereichen schnelle Datensicherung, bessere Ausbildung und Ausstattung, Kriminalprävention durch Datenschutz und Kriminalprävention durch Verbraucherschutz. Wer Straftaten wirklich wirksamer verfolgen will, müsste solche **organisatorischen und gesetzlichen Maßnahmen ergreifen**, anstatt eine Symboldebatte zum Thema „Vorratsdatenspeicherung" zu führen, die von den wahren Versäumnissen bei dem Schutz der Bürger abzulenken droht.

37 http://www.heise.de/ct/artikel/Kommentar-Bei-der-Vorratsdatenspeicherung-gibt-es-nicht-nur-Schwarz-und-Weiss-1337311.html

3.19 "Ein europaweites Verbot jeder Vorratsdatenspeicherung ist nicht mehrheitsfähig."[39]

Falsch. Solange die EU-Kommission kein europaweites Verbot jeder Vorratsdatenspeicherung vorschlägt, lässt sich nicht sagen, ob sich dafür eine Mehrheit finden würde oder nicht.
Selbst wenn es keine Mehrheit für ein europaweites Verbot jeder Vorratsdatenspeicherung geben sollte, folgt daraus nicht die Erforderlichkeit eines europaweiten Zwangs zur anlasslosen Vorratsdatenspeicherung. Vielmehr könnte es die EU – wie bis 2006 – den nationalen Parlamenten und Verfassungsgerichten überlassen, ob sämtliche Telekommunikationsdaten ohne jeden Anlass aufgezeichnet werden sollen oder nicht. Eine solche Vorgehensweise haben eine Reihe zivilgesellschaftlicher Organisationen bereits vorgeschlagen[40].

38 http://wiki.vorratsdatenspeicherung.de/images/Bericht_Sicherheit-vor-Sammelwut.pdf#page=18
39 http://www.moenikes.de/ITC/2011/09/05/stand-vorratsdatenspeicherung/

3.20 "Schon jetzt speichern Telekommunikationsanbieter Daten teilweise deutlich länger, als es bestimmte Vorschläge zur Wiedereinführung einer Vorratsdatenspeicherung vorsehen."[41]

Richtig, aber entscheidend ist das Wort **„teilweise"**.

Nach geltendem Recht kann jeder eine Erfassung seiner Verkehrsdaten verhindern, indem er einen Pauschaltarif wählt. Diese Wahlmöglichkeit ist für viele Menschen, die aus persönlichen oder beruflichen Gründen auf absolut vertrauliche Telekommunikation angewiesen sind oder denen ihre Privatsphäre wichtig ist, von hoher Bedeutung.

40 http://www.daten-speicherung.de/data/joint_position_15-07-2011.pdf
41 http://www.moenikes.de/ITC/2011/09/05/stand-vorratsdatenspeicherung/

3.21 " 'Quick-Freeze' eröffnet den Ermittlungsbehörden in der Praxis die Möglichkeit, stets alle Daten auf Verdacht sichern zu lassen, da der Verlauf und Ausgang von Ermittlungsverfahren nicht voraussehbar ist."[42]

Falsch. Quick-Freeze-Anordnungen müssen die Kennung des Anschlusses bezeichnen, dessen Daten eingefroren werden sollen. Damit scheidet die Möglichkeit, sämtliche Daten sichern zu lassen, aus.

Nach § 100j[43] Abs. 2 S. 3 StPO-E in Verbindung mit § 100b Abs. 2 StPO soll jede Quick-Freeze-Anordnung "die Rufnummer oder eine andere Kennung des zu überwachenden Anschlusses oder des Endgerätes" angeben müssen (siehe auch Seite 23[44] der Begründung). Außerdem sollen für jeden Anschluss, dessen Daten gesichert werden, mindestens 30 Euro an den Anbieter zu zahlen sein. All dies verhindert ausufernde Sicherungsanordnungen.

42 http://www.moenikes.de/ITC/2011/09/05/stand-vorratsdatenspeicherung/

3.22 "Damit überhaupt etwas auf Zuruf eingefroren werden kann, müssen verdachtsunabhängig laufend Verkehrsdaten mit Bestandsdaten verknüpft werden."[45]

Falsch. Eine Datensicherung ist ohne vorsorgliche Datenverknüpfung möglich.

Internet-Zugangsanbieter müssen während einer bestehenden Verbindung schon aus technischen Gründen wissen, welchem Internetanschluss welche IP-Adresse zugewiesen ist. Um diese Information im Verdachtsfall sichern zu können, ist eine flächendeckende vorsorgliche Datenverknüpfung nicht erforderlich. „Quick Freeze" umfasst nur eine Sicherung von "bei der Nutzung des Dienstes bereits erzeugten oder verarbeiteten sowie künftig anfallenden Verkehrsdaten" (§ 100j[46] StPO-E). Soweit eine Sicherung mangels Datenspeicherung nicht möglich ist, muss einer entsprechenden Anordnung auch nicht Folge geleistet werden.

43 http://wiki.vorratsdatenspeicherung.de/images/DiskE_.pdf
44 http://wiki.vorratsdatenspeicherung.de/images/DiskE_.pdf#page=23
45 http://www.moenikes.de/ITC/2011/01/18/quick-freeze-%E2%80%93-der-wolf-im-schafspelz/

4 Falschbehauptungen zur IP-Vorratsdatenspeicherung

4.1 "Eine IP-Vorratsdatenspeicherung ist ein geringfügiger Grundrechtseingriff, denn nach einer konkreten Straftat können Ermittlungsbehörden einzig herausfinden, wem der Internet-Anschluss gehört, von dem die Straftat ausging."[47]

Falsch. Eine IP-Vorratsdatenspeicherung würde in Verbindung mit Aufzeichnungen der Diensteanbieter (einschließlich staatlicher Internetportale) die Nachverfolgbarkeit potenziell jedes Klicks und jeder Eingabe, jeder gelesenen Seite und jeder geäußerten Meinung im Internet bedeuten - ein massiver Eingriff in das Recht auf unbefangene Information, Meinungsäußerung und Kommunikation über das Internet.

Die Identifizierung von Internetnutzern zur Strafverfolgung setzt nach geltendem Recht (§ 113 TKG) nicht voraus, dass eine Straftat begangen worden ist. Es genügt der Verdacht, dass eine Straftat begangen worden sein könnte. Der Inhaber der zu identifizierenden IP-Adresse muss zudem nicht im Verdacht stehen, die Tat begangen zu haben. Es genügt, dass seine Identifizierung zur "Erforschung des Sachverhalts" erforderlich ist. Ganz ohne Verdacht einer Straftat ist eine Identifizierung von Internetnutzern „zur Abwehr von Gefahren" und für Aufklärungszwecke der Geheimdienste zugelassen. Kein Richter kontrolliert vor der Identifizierung, ob ihre gesetzlichen Voraussetzungen vorliegen. Internet-Zugangsanbieter identifizieren jährlich über 3 Mio. Internetnutzer gegenüber Staat und Urheberrechtsinhabern.

46 http://wiki.vorratsdatenspeicherung.de/images/DiskE_.pdf
47 http://blog.odem.org/2011/01/quick-freeze-ip-phobie.html

Mithilfe von Aufzeichnungen (Logfiles) von Internetanbietern wie Google, Youtube oder Twitter können Behörden im Fall einer IP-Vorratsdatenspeicherung nicht nur lange nach Abschluss der Internetsitzung herausfinden, über welche Anschlüsse vermeintlich verdächtige Internetseiten gelesen, ungewöhnliche Videos betrachtet oder auffällige Meinungen geäußert wurden. Mithilfe von Referer, Cookies, Identifier oder Benutzerkonten kann nach einer Identifizierung oft auch festgestellt werden, was der Betroffene sonst noch im Internet getan hat, teilweise über Wochen oder Monate hinweg. Die jeweils genutzten IP-Adressen ermöglichen dann auch die Erstellung eines ungefähren Bewegungsprofils. Mithilfe von IP-Adressen können zudem vermeintlich anonyme E-Mails rückverfolgt und vermeintlich anonyme Benutzerkonten zugeordnet werden.

Insgesamt würde schon die ernsthafte Sorge vor Nachteile infolge einer jederzeitigen Identifizierbarkeit in vielen Situationen eine unbefangene, freie Kommunikation unmöglich machen (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 oder Selbsthilfegruppen von Menschen in besonderen Situationen wie Notlagen und Krankheiten).

Weitere Informationen:

- Die drohende IP-Vorratsdatenspeicherung[48]
- Quiz: IP-Vorratsdatenspeicherung[49]

48 http://www.vorratsdatenspeicherung.de/content/view/481/186/lang,de/

4.2 "Durch eine IP-Vorratsdatenspeicherung können keine Kontakte aufgedeckt werden."

Falsch. Durch eine IP-Vorratsdatenspeicherung können Kommunikationspartner einer Person aufgedeckt werden.

In den meisten E-Mails ist die IP-Adresse des Absenders enthalten. Darüber konnten im Fall einer IP-Vorratsdatenspeicherung selbst vermeintlich anonym versandte E-Mails zurückverfolgt werden.

49 http://akvorrat.de/s/IP-Wissensquiz

4.3 “Durch eine IP-Vorratsdatenspeicherung können keine Bewegungsprofile erstellt werden.”

Falsch. Durch eine IP-Vorratsdatenspeicherung können unter Umständen durchaus Bewegungsprofile erstellt werden.

Gelingt es Behörden über die IP-Adresse, ein vermeintlich anonymes Benutzerkonto zu identifizieren, können sie sich von dem Diensteanbieter die von dem Nutzer in der Vergangenheit genutzten IP-Adressen mitteilen lassen. Mit deren Hilfe lässt sich gerade im Fall der mobilen Internetnutzung ein ungefähres Bewegungsprofil erstellen.

4.4 "Durch eine IP-Vorratsdatenspeicherung ist nicht herauszufinden, auf welchen Seiten man im Internet gesurft hat."

Falsch. Durch eine IP-Vorratsdatenspeicherung kann ermittelt werden, auf welchen Seiten man im Internet gesurft hat.

Gelingt es Behörden über die IP-Adresse, einen vermeintlich anonymen Nutzer zu identifizieren, können sie sich von den Diensteanbietern mithilfe von Referer, Cookies, Identifier oder Benutzerkonten oftmals mitteilen lassen, was der Betroffene sonst noch im Internet getan hat, gegebenenfalls über Wochen oder Monate hinweg.

4.5 "Laut Bundesverfassungsgericht stellt eine Vorratsspeicherung von IP-Adressen nur einen sehr geringen Grundrechtseingriff dar."[50]

Falsch. Laut Bundesverfassungsgericht stellt die Identifizierung von Internetnutzern einen Grundrechtseingriff von "erheblichem Gewicht" dar (Abs. 258[51]).

Zwar hat das Bundesverfassungsgericht ausgeführt, eine Speicherung allein der Zuordnung dynamischer IP-Adressen hätte ein erheblich weniger belastendes Gewicht als eine nahezu vollständige Speicherung der Daten sämtlicher Telekommunikationsverbindungen. Dass eine auf den Internetbereich beschränkte Vorratsdatenspeicherung weniger eingriffsintensiv ist als eine Vorratsspeicherung auch von Telefon-, Handy- und E-Mail-Verbindungen, ist aber eine Selbstverständlichkeit. Das Bundesverfassungsgericht erkennt in seiner Entscheidung an, dass die Zuordnung einer IP-Adresse nicht mit der Identifizierung einer Telefonnummer gleichgesetzt werden kann. Da der Inhalt von Internetseiten anders als das beim Telefongespräch gesprochene Wort elektronisch fixiert und länger wieder aufrufbar sei, lasse sich mit ihr vielfach verlässlich rekonstruieren, mit welchem Gegenstand sich der Kommunizierende auseinander gesetzt hat. Werde der Besucher einer bestimmten Internetseite mittels der Auskunft über eine IP-Adresse individualisiert, wisse man nicht nur, mit wem er Kontakt hatte, sondern kenne in der Regel auch den Inhalt des Kontakts.

Weitere Argumente des Bundesverfassungsgerichts zu IP-Adressen

50 http://www.heise.de/ct/artikel/Kommentar-Bei-der-Vorratsdatenspeicherung-gibt-es-nicht-nur-Schwarz-und-Weiss-1337311.html

sind von Datenschützern[52] und auch von dem Bundesdatenschutzbeauftragten[53] kritisiert worden. Laut Schaar stehen die Aussagen des Bundesverfassungsgerichts zu IP-Adressen unter Prämissen, die der Realität „immer weniger entsprechen". Das Gericht sei davon ausgegangen, dass die Abrufe von Internetseiten nicht registriert werden. Nur in diesem Fall sei die IP-Adresse „verhältnismäßig unsensibel". Die Praxis sei aber die, „dass die IP-Adresse gespeichert wird". Selbst wenn man nicht angemeldet sei, speichere Google beispielsweise 9 Monate lang, mit welcher IP-Adresse welche Suchanfragen vorgenommen werden. Vor diesem Hintergrund seien IP-Zuordnungen „höchst sensibel".

Weitere Informationen:

- Die drohende Internet-Vorratsdatenspeicherung[54]

51 http://www.bverfg.de/entscheidungen/rs20100302_1bvr025608.html

52 http://www.daten-speicherung.de/index.php/scharfe-kritik-an-urteil-des-bundesverfassungsgerichts-zur-vorratsdatenspeicherung/

53 http://www.daten-speicherung.de/index.php/ziercke-greift-ak-vorrat-an/

4.6 "Ohne IP-Vorratsdatenspeicherung droht die Rechtsdurchsetzung im Internet und die Verfolgung von Internet-Alltagskriminalität generell leerzulaufen."[55] [56]

Falsch, auch ohne IP-Vorratsdatenspeicherung wird unter allen polizeilich bekannten Internetdelikten eine Aufklärungsquote von 71% erzielt (2010).

Diese Aufklärungsquote übersteigt diejenige für nicht im Internet begangene Straftaten bei Weitem (55%). Solange Straftaten im Internet ohne Vorratsdatenspeicherung weit häufiger aufgeklärt werden als sonstige Straftaten, ist es nicht zu rechtfertigen, ausgerechnet im Internet jedes Lesen eines Zeitungsartikels und jede Meinungsäußerung nachverfolgbar machen zu wollen.

Nach Einführung einer IP-Vorratsdatenspeicherung im Jahr 2009 ist die Aufklärungsquote bei Internetdelikten im Übrigen zurückgegangen, nicht angestiegen. Dies beruht darauf, dass eine Vorratsdatenspeicherung Straftäter zum Einsatz von Umgehungsstrategien veranlasst (z.B. Internetcafés, offene Netzzugänge, Anonymisierungsdienste, unregistrierte Prepaidkarten, nicht-elektronische Kommunikationskanäle), so dass ihre Kommunikation selbst im Verdachtsfall nicht mehr zu überwachen ist.

54 http://www.vorratsdatenspeicherung.de/content/view/481/186/lang,de/

55 http://www.heise.de/ct/artikel/Kommentar-Bei-der-Vorratsdatenspeicherung-gibt-es-nicht-nur-Schwarz-und-Weiss-1337311.html

56 http://www.moenikes.de/ITC/2011/01/18/quick-freeze-%E2%80%93-der-wolf-im-schafspelz/

4.7 "Eine IP-Vorratsdatenspeicherung wird benötigt, um die Verbreitung von Kinderpornografie im Internet verfolgen zu können."

Falsch, auch ohne IP-Vorratsdatenspeicherung wird unter allen polizeilich bekannten Fällen der Verbreitung von Missbrauchsdarstellungen im Internet eine Aufklärungsquote von 76% erzielt (2010).

Die Aufklärungsquote bei Missbrauchsdarstellungen im Internet übersteigt diejenige für nicht im Internet begangene Straftaten (55%) bei Weitem. Solange Straftaten im Internet ohne Vorratsdatenspeicherung weit häufiger aufgeklärt werden als sonstige Straftaten, ist es nicht zu rechtfertigen, ausgerechnet im Internet jedes Lesen eines Zeitungsartikels und jede Meinungsäußerung nachverfolgbar machen zu wollen.

Nach Einführung einer IP-Vorratsdatenspeicherung im Jahr 2009 ist die Aufklärungsquote bei Missbrauchsdarstellungen im Internet im Übrigen zurückgegangen, nicht angestiegen. Dies beruht darauf, dass eine Vorratsdatenspeicherung Straftäter zum Einsatz von Umgehungsstrategien veranlasst (z.B. Postversand von CD-Roms, Internetcafés, offene Netzzugänge, Anonymisierungsdienste, unregistrierte Prepaidkarten, nicht-elektronische Kommunikationskanäle), so dass ihre Kommunikation selbst im Verdachtsfall nicht mehr zu überwachen ist.

4.8 "Bis 2005 war es üblich, dass Internet-Zugangsanbieter IP-Zuordnungen bis zu 90 Tage lang speicherten."[57]

Selbst wenn dies zutrifft, kann eine solche **rechtswidrige Praxis** keine Maßstäbe setzen.

Das Telekommunikationsgesetz bestimmt seit jeher, dass Diensteanbieter nur die zur Bereitstellung und Abrechnung ihrer Dienste erforderlichen Verbindungsdaten speichern dürfen. Die IP-Adresse darf nicht protokolliert werden, weil das geschuldete Entgelt von ihr nicht abhängt. Der Internet-Zugangsanbieter T-Online speicherte früher dennoch 80 Tage lang, welchem Kunden wann welche IP-Adresse zugewiesen war. Holger Voss klagte erfolgreich gegen die Datenspeicherung, und das Unternehmen wurde verurteilt, die zugewiesenen IP-Adresse mit Verbindungsende umgehend löschen. Der Bundesdatenschutzbeauftragte setzte 2007 allgemein durch[58], dass Internet-Zugangsanbieter IP-Adressen nicht oder nicht länger als sieben Tage speicherten. So ist es auch heute wieder.

57 http://henning-tillmann.de/blog/wp-content/uploads/2011/08/spd-musterantrag-vds.pdf

4.9 "IP-Adressen müssen wie auch Telefonnummern ihrem Inhaber zuzuordnen sein."

Nein, Telefonnummern sind mit IP-Adressen nicht vergleichbar. Das Internet ist kein Telefon.

Laut Bundesverfassungsgericht kann die Zuordnung einer IP-Adresse nicht mit der Identifizierung einer Telefonnummer gleichgesetzt werden. Da der Inhalt von Internetseiten anders als das beim Telefongespräch gesprochene Wort elektronisch fixiert und länger wieder aufrufbar sei, lasse sich mit ihr vielfach verlässlich rekonstruieren, mit welchem Gegenstand sich der Kommunizierende auseinander gesetzt hat. Werde der Besucher einer bestimmten Internetseite mittels der Auskunft über eine IP-Adresse individualisiert, wisse man nicht nur, mit wem er Kontakt hatte, sondern kenne in der Regel auch den Inhalt des Kontakts.

Im Telefonnetz ist die Möglichkeit anonymer Telekommunikation trotz personenbezogener Rufnummern dadurch gewährleistet, dass die Rufnummer dem Gesprächspartner nur auf Wunsch angezeigt wird und man einen Pauschaltarif oder Prepaidtarif mit sofortiger Datenlöschung wählen kann. Im Internet dagegen lässt sich die Übermittlung der IP-Adresse an den Kommunikationspartner und deren Protokollierung dort nicht einfach abstellen. Deswegen ist technisch nicht versierten Normalnutzern eine anonyme Information und Kommunikation im Internet nur mithilfe einer anonymen Kennung möglich.

58 http://www.heise.de/newsticker/meldung/Datenschuetzer-haelt-siebentaegige-Speicherung-von-Verbindungsdaten-fuer-angemessen-150197.html

4.10 "IP-Adressen müssen wie auch Kfz-Kennzeichen ihrem Inhaber zuzuordnen sein."

Nein, Kfz-Kennzeichen sind mit IP-Adressen nicht vergleichbar. Das Internet ist kein Auto.

Niemand schreibt mit, wo man wann mit dem Auto gewesen ist. Im Internet wird dagegen verbreitet jeder Klick und jede Eingabe mitsamt der IP-Adresse protokolliert, so dass die Anonymität von IP-Adressen von zentraler Bedeutung ist. Im Straßenverkehr ist die Möglichkeit anonymer Fortbewegung trotz personenbezogener Kfz-Kennzeichen dadurch gewährleistet, dass man sich zu Fuß, mit dem Fahrrad, mit einer Mitfahrgelegenheit oder mit dem Bus auch ohne eigenes Kfz-Kennzeichen fortbewegen kann. Das Internet kann man demgegenüber nicht ohne eine IP-Adresse nutzen. Deswegen ist technisch nicht versierten Normalnutzern eine anonyme Information und Kommunikation im Internet nur mithilfe einer anonymen Kennung möglich.

5 Irrtümer und Populismen zum Nutzen von Überwachung

Einige Menschen aus Politik und Gesellschaft kultivieren in den letzten Jahren eine Einstellung, die man als Sicherheitsideologie bezeichnen kann.

Sie beschwören unsere „Bedrohung“ durch Kriminelle und Terroristen, vor der wir uns schützen müssten. Sie verweisen auf „schreckliche Verbrechen“, die in der Tagespresse groß aufgemacht werden, oder auf Schlagworte wie „Kinderpornografie“ und „internationaler Terrorismus“. Dann fordern sie, dass die Täter endlich gefasst werden müssten und die Sicherheitsbehörden dazu alle nötigen Mittel bräuchten. Wer ihnen diese verweigere, mache sich mitschuldig an den begangenen Verbrechen.

5.1 „Wir brauchen mehr Überwachung, um uns vor Kriminalität/Terroristen/Sexualstraftätern zu schützen und um in Sicherheit leben zu können."

Falsch. Mehr Überwachung bringt nicht mehr Sicherheit.

Wie sicher wir leben, lässt sich an der Kriminalitätsrate ablesen. Dass mehr Überwachung zu einer niedrigeren Kriminalitätsrate führt, ist **weder erwiesen**, noch wird dies von den Innenpolitikern auch nur behauptet. Tatsächlich lässt sich ein messbarer Einfluss von Überwachungs-maßnahmen auf die Kriminalitätsrate weder im zeitlichen, noch im internationalen Vergleich feststellen. Umgekehrt zeigt eine amerikanische Vergleichsstudie, dass kein Zusammenhang zwischen dem Ausmaß der Ermittlungsbefugnisse der Strafverfolgungsbehörden einerseits und der Kriminalitätsrate andererseits besteht.

Dass Überwachungsmaßnahmen den Behörden in einzelnen Fällen nützlich sein können, mag durchaus sein. Insgesamt gesehen ist der Nutzen aber vernachlässigbar gering. Es gibt eine Statistik der Weltgesundheitsorganisation, die den Verlust gesunder Lebenszeit durch vorzeitigen Tod, Krankheit oder Behinderung misst. Dieser Statistik zufolge beruht der Verlust gesunder Lebenszeit für Westeuropäer zu 92% auf Krankheiten, zu 2% auf Verkehrsunfällen, zu 1% auf Stürzen, zu 1,7% auf Suizid und gerade einmal zu 0,2% auf Gewalt. Straftaten sind der Statistik zufolge für die Gesundheit der Bevölkerung in etwa so schädlich wie versehentliche Vergiftungen, Karies, Rückenschmerzen oder Durchfall. Eurostat zufolge sterben weniger als 0,002% der Europäer jährlich als Opfer einer Straftat, terroristische Anschläge eingeschlossen. Ausweislich der Statistik ist es um ein Vielfaches wahrscheinlicher, wegen eines ungesunden Lebensstils (z.B. falsche Ernäherung, Bewegungsmangel, Alkohol, Nikotin), durch einen Sturz oder im Straßenverkehr zu sterben als infolge einer Straftat. Die großen Risiken für unsere Gesundheit sind

andere als Kriminalität: Bluthochdruck, Tabak, Alkohol, Cholesterin, Übergewicht, Fehlernäherung und Bewegungsmangel sind die Hauptrisikofaktoren. Würde man z.B. den Tabakkonsum nur um 2% zurückfahren, dann würde man der Gesundheit der Bevölkerung einen größeren Dienst erweisen als durch die Verhinderung sämtlicher Gewalttaten. Auch dass uns Zivilisationsrisiken wie Krankheit, Armut, Arbeitslosigkeit oder Naturkatastrophen treffen, ist weitaus wahrscheinlicher als das Risiko, Opfer einer Straftat zu werden.

Die Lebenserwartung der Europäer steigt seit Jahrzehnten. Vor diesem Hintergrund stellt die Kriminalität zwar ein ernst zu nehmendes Problem dar, das der Staat mit angemessenen Maßnahmen einzudämmen versuchen sollte. Die Kriminalität ist aber nur ein Risiko unter vielen, mit denen das Leben notwendig verbunden ist, und ein vergleichsweise geringes Risiko. Außerdem hat die Kriminalität Ursachen in unserer Gesellschaft, welche die Polizei nicht beseitigen kann. Diese Kriminalitätsursachen müssen anders angegangen werden.

5.2 „Wir müssen alles tun/alle verfügbaren Mittel einsetzen, um künftig solche schrecklichen Verbrechen/Terroranschläge/Kindesmissbrauch/… zu verhindern."

Falsch. Es dient unserer Sicherheit, dass der Staat nicht alle verfügbaren Mittel einsetzen darf.

Der Staat verfolgt nicht nur Straftäter, sondern er ermittelt gegen Verdächtige. Darunter befinden sich viele Menschen, deren Unschuld sich erst später herausstellt oder deren Schuld im weiteren Verlauf nicht festgestellt werden kann. Die Instrumente der Strafverfolgungsbehörden (z.B. Telefonüberwachung, Observation, Nachbarbefragung, Untersuchungshaft) treffen in vielen Fällen Unschuldige. Weil jeder Opfer eines Irrtums oder einer Falschverdächtigung werden kann, müssen wir zu unserer eigenen Sicherheit dafür sorgen, dass die staatliche Macht begrenzt bleibt.

Bestimmte Methoden (z.B. Folter) widersprechen außerdem der Würde jedes Menschen, auch der des Straftäters. In unserer Geschichte haben wir gelernt, dass die uneingeschränkte Förderung von „Gemeinwohl" und „Volksgemeinschaft" letztendlich nicht in unserem Interesse liegt. Andere Instrumente (z.B. verdachtslose Überwachung beliebiger Personen) sind unverhältnismäßig. Ihr Nutzen steht außer Verhältnis zu ihren negativen Auswirkungen auf eine demokratische Gesellschaft, die auf das unbefangene Mitwirken gerade kritischer Bürgerinnen und Bürger angewiesen ist.

Langfristig dienen rechtsstaatliche Beschränkungen und die Achtung der Menschenrechte der Sicherheit, denn **exzessive Kontrolle und Repression erzeugt Unzufriedenheit und Widerstand**. Die Achtung der Grundrechte macht uns sicherer,

nicht verletzlicher. Der Oberste Gerichtshof des Staates Israel führte im Jahr 1999 zutreffend aus: „Dies ist das Schicksal der Demokratie, weil nicht alle Mittel mit ihr vereinbar und nicht alle Methoden ihrer Feinde für sie verfügbar sind. Obwohl eine Demokratie oft mit einer Hand auf ihren Rücken gebunden kämpfen muss, behält sie trotzdem die Oberhand. Die Erhaltung der Rechtsstaatlichkeit und die Anerkennung der Freiheit des Einzelnen bilden einen wichtigen Bestandteil ihres Verständnisses von Sicherheit. Letztlich erhöht dies ihre Stärke."

5.3 „Wenn auch nur ein Mensch/Kind gerettet werden kann, rechtfertigt das schon das gesamte Überwachungssystem.“

Falsch. Zum Schutz Unbeteiligter müssen Grundrechte und **Verhältnismäßigkeit** stets gewahrt bleiben.

Würde schon ein gerettetes Menschenleben jegliche Maßnahme rechtfertigen, dann müsste die Politik z.B. den Straßenverkehr verbieten, denn es gibt unzählige Unfalltote jedes Jahr. Dieses Beispiel zeigt: So schrecklich jeder Unfalltod und jede Straftat ist, so unangemessen ist eine radikale Reaktion, die Unbeteiligte unzumutbar belastet. Das Leben ist untrennbar mit dem Risiko verbunden, Opfer einer Straftat zu werden oder in einen Verkehrsunfall verwickelt zu werden. Der Staat sollte diesen Risiken entgegenwirken. Er darf aber nur effektive Mittel einsetzen, die Unbeteiligte nicht übermäßig belasten.

5.4 „Datenschutz ist Täterschutz. Er steht dem Schutz unschuldiger Menschen im Weg."

Falsch. Datenschutz ist Grundrechtsschutz. Er dient dem Schutz unschuldiger Menschen.

Dass der Staat nicht unbegrenzt Wissen über uns sammeln und unsere Daten nicht beliebig rastern darf, dient unserem eigenen Schutz. Je mehr der Staat über uns weiß, desto mehr Ansatzpunkte für Ermittlungen stehen ihm zur Verfügung und desto größer wird die Gefahr von Falschverdächtigungen. Außerdem laden umfangreiche Datenbestände zu Missbrauch ein. In der Vergangenheit hat es immer wieder Fälle gegeben, in denen Polizeibeamte gegen Bezahlung oder aus privaten Gründen auf Polizeidaten zugegriffen haben. Schon die Befürchtung von Missverständnissen oder Missbräuchen kann unsere Entscheidungsfreiheit beeinträchtigen. Wenn wir anonym handeln können oder wissen, dass unsere Daten unverzüglich gelöscht oder wenigstens nicht zu anderen Zwecken genutzt werden, dann scheuen wir auch vor sensiblen Aktivitäten nicht zurück (z.B. Teilnahme an Demonstrationen, Mitarbeit in Oppositionsgruppe, Inanspruchnahme psychologischer Beratung, sexuelle Aktivitäten). Datenschutz ist daher Freiheitsschutz.

5.5 „Wir müssen etwas gegen die Kriminalität unternehmen. Wir können nicht die Hände in den Schoß legen und kapitulieren."

Falsch. Aktionismus von Politikern ist nutzlos.

Keiner will gegen Kriminalität „die Hände in den Schoß legen". Tätig werden müssen aber die Sicherheitsbeamte und nicht die Abgeordneten. Wenn spektakuläre Verbrechen in das Rampenlicht der Öffentlichkeit rücken, ist das in allererster Linie ein Weckruf an die zuständigen Behörden, künftig noch intensiver an der Verhinderung solcher Vorfälle zu arbeiten. Politiker reagieren oft mit der Forderung nach „verbesserten" Gesetzen. Neue Gesetze sind für Politiker zwar ein einfaches und billiges Mittel, um öffentlichkeitswirksam Tatkraft und Entschlossenheit zu demonstrieren. Derartiger **Aktionismus** führt aber oft zu Gesetzen, die dem Bürger keinen messbaren Nutzen bringen. Wer Sicherheit durch immer neue Gesetze verspricht und – zwangsläufig – Straftaten gleichwohl nicht verhindern kann, der verliert mittelfristig das Vertrauen der Bürgerinnen und Bürger und fördert die Politikverdrossenheit. Er gefährdet damit letztlich die Funktionsfähigkeit unserer Demokratie.

5.6 „Der Staat ist verpflichtet, seine Bürger zu schützen. Die Bürger haben einen Anspruch auf Sicherheit.“

Falsch. Mehr als angemessene Maßnahmen gegen Kriminalität können die Bürger vom Staat nicht verlangen.

Einen „Anspruch auf Sicherheit“ kann es schon deshalb nicht geben, weil kein Staat eine vollständige Sicherheit vor Straftaten gewährleisten kann. Selbst Polizeistaaten mit unbegrenzter Macht (z.B. die DDR) haben die Kriminalität nie beseitigen können. Umgekehrt gab es in solchen Staaten viel Korruption, Willkür und Staatskriminalität. Ein demokratischer Rechtsstaat geht entschlossen gegen Straftäter vor. Er erlegt sich zum Schutz Unschuldiger und zur Gewährleistung einer freiheitlichen Gesellschaft aber bewusst Grenzen und Fesseln auf. Gerade dies macht seinen Charakter und seine Stärke als Rechtsstaat aus.

5.7 „Ich habe nichts zu verbergen.“

Falsch. Jeder hat eine Intim- und Privatsphäre, die den Staat nichts angeht.

Wer von sich behauptet, nichts zu verbergen zu haben, muss sich fragen lassen, warum er seine Wohnung bekleidet verlässt oder die Toilettentür hinter sich schließt. Jeder hat einmal Erlebnisse gehabt, die niemanden etwas angehen und die er nicht der Gefahr eines Bekanntwerdens aussetzen möchte. Auch dass er sich noch nie etwas zuschulden kommen lassen hätte, kann wohl kaum jemand von sich behaupten. Noch nie schwarz gefahren? Noch nie beim Autoverkauf geflunkert (Betrug)? Immer alle Einnahmen in der Steuererklärung angegeben? Noch nie zu schnell gefahren? Wenn der Staat jemanden nur lange genug überwacht, wird er früher oder später immer ein Vergehen feststellen. Hinzu kommt: Selbst wer vollkommen unschuldig ist, hat handfeste Nachteile durch Überwachung und Datensammlung zu befürchten (siehe nächste Frage).

Sollte sich trotzdem jemand finden, der sein Leben in einem Big Brother-Container verbringen möchte, der kann dies gerne tun. Er soll anderen aber nicht vorwerfen, dass sie ihre Geheimnisse für sich behalten wollen.

Übrigens hat auch der Staat selbst etwas zu verbergen. Das nennt man „Staatsgeheimnisse“. Abgeordnete wehren sich gegen „zuviel“ Transparenz, wollen ihre Einkünfte nicht offen legen. Auch staatliche Überwachungsmaßnahmen selbst werden verborgen. Sie sollen vor den Überwachten geheim bleiben.

5.8 „Wer nichts zu verbergen hat, hat nichts zu befürchten."

Falsch. Unschuldige geraten immer wieder zu Unrecht in das Visier von Behörden.

Auch unschuldige Menschen müssen sich fragen lassen: „Wenn du nichts zu verbergen hast, kannst du davon auch den Polizisten oder den Einreisebeamten überzeugen?" Auch wer unschuldig ist, muss zunehmend mit polizeilichen Maßnahmen rechnen. Oft ziehen schon ein falscher Verdacht, vermeintliche Risikofaktoren (z.B. „falsche" Religion, „falsche" Nationalität, „falscher" Geburtsort, „falscher" Name, „falsche" Bücher gelesen, „falsche" Meinung geäußert) oder unglückliche Umstände einschneidende Maßnahmen nach sich. In der Folge kann es zur Befragung von Nachbarn und Arbeitskollegen kommen, zur Observation, zu Wohnungsdurchsuchungen oder zur Festnahme. Derartige Maßnahmen können Vorverurteilungen im sozialen Umfeld und sogar Existenzvernichtungen zur Folge haben. Auch unberechtigte Aus- und Einreiseverweigerungen, Vermögensbeschlagnahmen, Grenzzurückweisungen wegen Namensverwechselungen bis hin zu Verschleppungen durch Geheimdienste und irrtümlichen Tötungen durch Polizei oder „Sky-Marshalls" werden immer wieder bekannt. Dafür gibt es viele Beispiele[59].

Überwachung und Datensammlung liefern eine Flut von Informationen, aus denen sich Unregelmäßigkeiten ablesen lassen oder ein Verdacht konstruieren lässt. Dann hilft es nicht, wenn man „nichts zu verbergen" hat.

Außerdem: Wer „nichts zu verbergen" hat, braucht auch nicht überwacht zu werden.

59 http://daten-speicherung.de/wiki/index.php/F%C3%A4lle_von_Datenmissbrauch_und_-irrt%C3%BCmern

5.9 „Die Überwachung erfolgt ausschließlich zur Bekämpfung schwerer Straftaten."

Falsch. Ein Missbrauch zu anderen Zwecken kommt immer wieder vor.

Fälle wie die Journalistenbespitzelung durch den BND zeigen immer wieder, dass Sicherheitsgesetze **missbraucht** werden. Neben Journalisten haben auch staatskritische Aktivisten wie Globalisierungskritiker mit Missbrauch zu rechnen. Weil staatskritische Journalisten und Aktivisten zu unser aller Nutzen handeln, sollte uns ihre Freiheit nicht gleichgültig sein.

Das Bundesverfassungsgericht warnt: „Die Befürchtung einer Überwachung mit der Gefahr einer Aufzeichnung, späteren Auswertung, etwaigen Übermittlung und weiteren Verwendung durch andere Behörden **kann schon im Vorfeld zu einer Befangenheit in der Kommunikation, zu Kommunikationsstörungen und zu Verhaltensanpassungen […] führen.**" Die ehemalige Präsidentin des Bundesverfassungsgerichts, Frau Prof. Dr. Limbach, wird noch deutlicher: „**Eine demokratische politische Kultur lebt von der Meinungsfreude und dem Engagement der Bürger**. Das setzt Furchtlosigkeit voraus. Diese dürfte allmählich verloren gehen, wenn der Staat seine Bürger biometrisch vermisst, datenmäßig durchrastert und seine Lebensregungen elektronisch verfolgt."

Außerdem zeigt die Erfahrung, dass Zugriffsbeschränkungen mit der Zeit immer weiter aufgeweicht werden. Es finden sich immer mehr Behörden und immer mehr Fälle, in denen die Überwachungsmaßnahmen oder die gesammelten Daten nützlich sind. Schlussendlich wird die Überwachung oder Datenabfrage in allen Fällen erlaubt, in denen sie irgendwie einmal nützlich sein könnte.

5.10 „Überwachung ist nur ein geringfügiger, kaum merklicher Eingriff."

Falsch. Überwachung kann einschneidende Folgen für Betroffene haben, bis hin zur Existenzvernichtung.

Auch wenn die Überwachung selbst nicht weh tut – ihre Folgen können es durchaus. Wenn Überwachungsergebnisse den Verdacht der Behörden erregen, kann dies zur Befragung von Nachbarn und Arbeitskollegen führen, zu einer Observation, zu Wohnungsdurchsuchungen oder zur Festnahme. Auch unberechtigte Aus- und Einreiseverweigerungen, Vermögensbeschlagnahmen, Grenzzurückweisungen wegen Namensverwechselungen bis hin zu Verschleppungen durch Geheimdienste und irrtümlichen Tötungen durch Polizei oder „Sky-Mashalls" sind Realität.

5.11 „Überwachung stärkt das Sicherheitsgefühl der Bevölkerung."

Falsch. Symbolische Maßnahmen bilden kein Vertrauen.

Selbst wenn Überwachungsmaßnahmen kurzfristig populär sind, stärken sie das Sicherheitsgefühl letztlich nicht. Die Bürgerinnen und Bürger werden weiterhin spektakuläre Straftaten von den Medien präsentiert bekommen. Politischer Aktionismus ist auch kontraproduktiv, denn zur Durchsetzung neuer Gesetzesvorhaben werden Kriminalitätsängste meist geschürt. Um das Sicherheitsgefühl wirksam zu steigern, bieten sich andere Mittel an: Da das tatsächliche Ausmaß an Kriminalität verbreitet überschätzt wird, ist eine Aufklärung über das wahre Risiko sinnvoll. Auch bauliche Maßnahmen (z.B. bessere Beleuchtung) und ein besserer Kontakt zu Nachbarn und Polizei können hilfreich sein, um Kriminalitätsangst entgegenzuwirken.

5.12 „Datenschützer sind paranoid, ihre Schreckensszenarien sind übertrieben.“

Falsch. Fehler und Missbrauch sind tägliche Realität[60], wobei die bekannt gewordenen Fälle nur die Spitze des Eisbergs sein dürften.

60 http://daten-speicherung.de/wiki/index.php/F%C3%A4lle_von_Datenmissbrauch_und_-irrt%C3%BCmern

5.13 „Wir werden sowieso schon bei allem überwacht, was wir tun."

Falsch. Wenn die totale Überwachung schon Realität wäre, dann würde die Politik nicht immer wieder neue Gesetze auf den Weg bringen, um sie auszuweiten.

Der internationalen Datenschutzorganisation Privacy International zufolge[61] ist in Deutschland die Privatsphäre weltweit noch mit am besten geschützt. Diesen Schutz müssen wir verteidigen und die in den letzten Jahren verloren gegangene Freiheit zurückerobern.

61 http://www.privacyinternational.org/article.shtml?cmd%5B347%5D=x-347-559597

5.14 „Man kann ja doch nichts daran ändern."

Falsch. Es gibt viele Möglichkeiten, sich gegen die Sicherheitsideologie einzusetzen.

Wenn eine Person aktiv wird, ändert das vielleicht noch nicht viel. Wenn sich aber viele Menschen engagieren, kann die Politik das auf Dauer nicht ignorieren. Politiker sind sehr sensibel für die Stimmung in ihrer Wählerschaft.

Weitere Informationen:

- Beispiele[62] von Möglichkeiten, wie man sich einsetzen kann.
- Liste von Bürgerrechtsorganisationen[63], in denen man sich engagieren kann.

62 http://wiki.vorratsdatenspeicherung.de/Was_kann_ich_tun%3F

6 Über uns

Der Arbeitskreis Vorratsdatenspeicherung (AK Vorrat) versteht sich als ein bundesweiter, politisch unabhängiger und überparteilicher Zusammenschluss von Menschen, Gruppen und Initiativen, der sich gegen die ausufernde Überwachung im Allgemeinen und gegen die Vollprotokollierung der Telekommunikation und anderer Verhaltensdaten im Besonderen einsetzt.

Wir freuen uns über jede Form von Mitarbeit und Unterstützung, jede Anregung und jede konstruktive Kritik und sind unter folgender E-Mail erreichbar:

kontakt@vorratsdatenspeicherung.de

Weitere zahlreiche Informationen über die für jeden und jede offene Gruppe des "AK Vorrat" sowie über seine vor Ort aktiven "Ortsgruppen" gibt es auf der Homepage

http://www.vorratsdatenspeicherng.de

sowie in dem sehr umfangreichen und zum Mitmachen einladenden Wiki des AK Vorrat unter

http://wiki.vorratsdatenspeicherung.de

63 http://www.vorratsdatenspeicherung.de/content/view/92/79/#Unterst.C3.BCtzer

Herausgegeben vom:
Arbeitskreis Vorratsdatenspeicherung

Stand:
November 2011

Quellen:
www.vorratsdatenspeicherung.de
www.daten-speicherung.de

Titelbild:
"The secret" von Tryndelka, Creative Commony by-sa 3.0
https://commons.wikimedia.org/wiki/File:The_Secret.jpg

Dank:
An alle im AK Vorrat engagierten Menschen, insbesondere an Patrick Breyer

Im Internet ist dieses Heft als pdf-Datei verfügbar unter:
http://wiki.vorratsdatenspeicherung.de/images/Populismen-zu-vds-und-ueberwachung.pdf

Das gedruckte Heft kann man im Unterstützungsshop des FoeBuD e.V. bestellen:
https://shop.foebud.org/thema/ak-vorrat

64 http://creativecommons.org/licenses/by/2.0/de/

Arbeitskreis Vorratsdatenspeicherung
www.vorratsdatenspeicherung.de