



**Sebastian Blumenthal**

Mitglied des Deutschen Bundestages  
Vorsitzender des Unterausschusses Neue Medien

**Marco Buschmann**

Mitglied des Deutschen Bundestages  
Vorsitzender der Arbeitsgruppe Recht der FDP-Fraktion

**Manuel Höferlin**

Mitglied des Deutschen Bundestages  
Vorsitzender der Arbeitsgruppe IT und  
Netzpolitik der FDP-Fraktion  
Vorsitzender des FDP LV Net

**Jimmy Schulz**

Mitglied des Deutschen Bundestages  
Obmann der FDP in der Enquete-Kommission  
Internet und digitale Gesellschaft

13. Dezember 2010

**Argumentationshilfe „Vorratsdatenspeicherung“**

Liebe Kolleginnen und Kollegen,

in den letzten Wochen berichteten die Medien intensiv über das Thema Vorratsdatenspeicherung.

Wie Ihnen bekannt ist, hat die FDP geschlossen gegen das Umsetzungsgesetz der Vorratsdatenspeicherungs-Richtlinie in der letzten Wahlperiode gestimmt. Die große Koalition sorgte trotzdem dafür, dass das Gesetz in Kraft trat. Am 2. März 2010 wurde die Vorratsdatenspeicherung aufgrund einer Entscheidung des Bundesverfassungsgerichts außer Kraft gesetzt.

Momentan ist in der Koalition strittig, ob und auf welche Weise die Vorratsdatenspeicherung wieder eingeführt werden soll. Sie werden möglicherweise mit dieser Frage konfrontiert. Wir möchten Ihnen deswegen, zur Unterstützung Ihrer Arbeit, den angefügten Argumentationskatalog überreichen. Er zeigt, dass die Vorratsdatenspeicherung keine sinnvolle, sondern sogar eine schädliche Maßnahme ist.

Für weitere Rückfragen und Erläuterungen im Detail stehen wir Ihnen gerne zur Verfügung.

Mit kollegialen Grüßen

Sebastian Blumenthal

Marco Buschmann

Manuel Höferlin

Jimmy Schulz

## 1. Was ist die Vorratsdatenspeicherung?

Anbieter von Telekommunikationsdiensten sollen zur Registrierung sämtlicher elektronischer Kommunikationsvorgänge für die **Dauer von sechs Monaten** verpflichtet werden. Jedes Telefonat oder jede Verbindung mit dem Internet soll registriert und einer Person zugeordnet werden.

Bei **Telefonaten** werden alle Verbindungsdaten durch den Anbieter gespeichert, also:

- Wer hat mit wem telefoniert?
- An welchem Tag und zu welcher Uhrzeit wurde telefoniert?
- Bei einem Telefonat über ein Mobiltelefon wird zusätzlich der Aufenthaltsort gespeichert.

Wer wem wann und wo eine **SMS** schickt, wird ebenfalls gespeichert.

Zusätzlich werden **Bewegungen im Internet** registriert, also:

- Wer hat wem wann eine E-Mail geschickt, bzw. wer hat von wem wann eine E-Mail empfangen?
- Wer hat zu welchem Zeitpunkt welche Internetseite besucht?

Die Vorratsdatenspeicherung soll soziale Beziehungen identifizieren. Sie soll dadurch helfen, schwere Straftaten, insbesondere terroristische Angriffe, zu verhüten und zu verfolgen. Allerdings werden die Daten völlig unabhängig davon erfasst, ob ein Anfangsverdacht oder konkrete Hinweise auf derartige Gefahren vorliegen.

## 2. Welche Vorgeschichte hat die aktuelle Debatte um VDS?

- Am 3. Mai 2006 trat die EU-Richtlinie (2006/24/EG) in Kraft, die alle EU-Mitgliedsstaaten verpflichtet, die Vorratsdatenspeicherung umzusetzen.
- 2007 beschlossen CDU, CSU und SPD das deutsche Umsetzungsgesetz, gegen die Stimmen der FDP. Dies trat am 01.01.2008 für Telefoniedaten und am 01.01.2009 für Internetdaten in Kraft.
- Am 02.03.2010 erklärte das Bundesverfassungsgericht das deutsche Umsetzungsgesetz rückwirkend für nichtig. Sämtliche Daten, die auf dessen Grundlage gespeichert worden waren, wurden gelöscht.

## 3. Was spricht gegen VDS?

Die FDP setzt sich dafür ein, dass den Sicherheitsbehörden rechtliche Instrumente zur Verfügung stehen, um die Sicherheit messbar zu steigern und nicht unverhältnismäßig in die Grundrechte einzugreifen. Diese Anforderungen sind bei VDS, wie sie in Deutschland umgesetzt worden ist, nicht erfüllt:

VDS führt **nicht** zu einer effektiven Verbesserung der Sicherheitslage:

- Laut dem Verband der deutschen Internetwirtschaft e.V. (eco) reichen in 99,95 % der Ermittlungsverfahren die klassischen Methoden aus.

- In der Zeit, in der auf Vorrat gespeichert wurde, ist die Aufklärungsquote bei Straftaten im Internet sogar gesunken – und zwar kontinuierlich: Von 82,9 % im Jahr 2007 über 79,8 % 2008 auf 75,7 % 2009 (Quelle: Polizeiliche Kriminalstatistik).
- Terroristen oder Schwerkriminelle können VDS sehr leicht umgehen – z.B. durch die Nutzung von Mobiltelefonen mit Prepaid-Karten. Vor der Nutzung vieler Prepaid-Karten ist lediglich eine Internet-Registrierung ohne weitere Kontrollmechanismen erforderlich. In manchen Ländern, beispielsweise in Schweden, ist beim Kauf einer Prepaid-Karte generell keine namentliche Registrierung notwendig. Auch die Internet-Anonymisierung, gefördert vom Staat, ermöglicht unidentifizierbares Surfen.
- Schwere terroristische Anschläge in der Vergangenheit hätten durch VDS erwiesenermaßen nicht verhindert werden können. Auch zur Aufklärung der Bombenanschläge in London und Madrid hat die VDS nicht beigetragen.

VDS führt zu erheblichen **Einschränkungen in grundrechtlich geschützten Lebensbereichen:**

- Das Bundesverfassungsgericht stellte fest, dass VDS, jedenfalls wie sie in Deutschland umgesetzt worden ist, das Fernmeldegeheimnis verletzt und nicht mit Art. 10 des Grundgesetzes vereinbar ist.
- Sie ermöglicht eine weitgehende Überwachung praktisch sämtlicher Formen der Telekommunikation der Bürger. Jedem ist jederzeit bewusst, dass seine Verbindungsdaten prinzipiell dem Zugriff des Staates zur Verfügung stehen. Nicht umsonst hat das Bundesverfassungsgericht in seiner Entscheidung vom 2. März 2010 zur Vorratsdatenspeicherung betont: „Dass die Freiheitswahrnehmung der Bürger nicht total erfasst und registriert werden darf, gehört zur verfassungsrechtlichen Identität der Bundesrepublik Deutschland.“
- Durch ihren „flächendeckenden“ Einsatz erhöht VDS massiv die Gefahr, dass unbeteiligte Bürger zu Unrecht in das Visier der Behörden geraten.
- VDS ist unverhältnismäßig, da für die Datenverwendung keinerlei Schutz von auf besondere Vertraulichkeit angewiesenen Telekommunikationsverbindungen vorgesehen ist.
- Sie wirkt in sensiblen Situationen abschreckend, z. B. beim Anruf bei Selbsthilfegruppen oder Suchtberatungen, sowie auch bei politischer Meinungsäußerung im Internet.  
Die anlass- bzw. verdachtslose Speicherung von personenbezogenen Daten bildet einen Fremdkörper im System des deutschen Polizei- und Strafprozessrechts. Denn Eingriffsbefugnisse in Grundrechte sind hier erst ab einer bestimmten Verdachts- oder Gefahrenschwelle zugelassen.

VDS führt zu erheblichen **Kosten:**

- Obwohl der Mehrwert von VDS für die Sicherheit zweifelhaft ist, wären die Kosten immens: Laut Branchenverband Eco drohen den Telekommunikationsunternehmen finanzielle Mehrbelastungen von bis zu 336 Millionen Euro. Zum Vergleich: Diese Summe entspricht fast dem gesamten Etat des BKA im Jahr 2010 (380 Mio. Euro).

#### 4. Welche Haltung hat die FDP bislang zu VDS?

- 2007 hat die FDP-Bundestagsfraktion geschlossen gegen das „Gesetz zur Neuregelung der Telekommunikationsüberwachung“, also das deutsche Umsetzungsgesetz zur VDS, gestimmt.
- Viele FDP-Abgeordnete, darunter auch die heutige Bundesjustizministerin, haben als Antragsteller zusammen mit fast 35.000 Bürgern an dem umfangreichsten Verfassungsbeschwerde-Verfahren in der deutschen Geschichte teilgenommen.
- Mehrere FDP-Abgeordnete haben an den verschiedenen „Freiheit Statt Angst“-Demonstrationen teilgenommen und gegen VDS öffentlich demonstriert.
- Verschiedenste FDP-Gremien haben durch Beschluss VDS abgelehnt: So der Bundesparteitag erneut im April 2010, so die Bundestagsfraktion jüngst wieder im November 2010 in ihrem Positionspapier „Eckpunkte zur Verbesserung der Kriminalitätsbekämpfung im Internet: Freiheit und Sicherheit im Internet bewahren“. Auch die JuLis haben VDS konsequent abgelehnt.

#### 5. Muss Deutschland nicht die VDS-Richtlinie umsetzen?

Natürlich gibt es eine europarechtliche Verpflichtung, die VDS-Richtlinie in deutsches Recht umzusetzen. Es gibt jedoch eine Vielzahl sachlicher Gründe, die eine sorgfältige Prüfung notwendig erscheinen lassen:

- Das Bundesverfassungsgericht hat das deutsche Umsetzungsgesetz für nichtig erklärt. Die lange und komplexe Urteilsbegründung muss sorgfältig ausgewertet werden, damit die Maßstäbe, die das Gericht auch künftig anlegen wird, eingehalten werden.
- Die VDS-Richtlinie wird derzeit durch die EU-Kommission evaluiert. Die Ergebnisse sollen bis Ende des ersten Quartals 2011 vorliegen. Es scheint nicht sinnvoll, ein deutsches Umsetzungsgesetz auf den Weg zu bringen, wenn noch gar nicht klar ist, welchen Rahmen die Richtlinie künftig in ggf. geänderter Form setzen wird.
- Die VDS-Richtlinie ist in Europa besonders umstritten:
  - Österreich hat die VDS-Richtlinie nicht umgesetzt.
  - Schweden weigert sich, die VDS-Richtlinie umzusetzen.
  - Der Rumänische Verfassungsgerichtshof hat das nationale Umsetzungsgesetz für verfassungswidrig erklärt.
  - Der Irische High Court hat die VDS-Richtlinie dem Europäischen Gerichtshof (EuGH) zur Prüfung am Maßstab der EU-Grundrechtecharta vorgelegt.
- Im Rahmen der Vorlage durch den irischen High Court kann es dazu kommen, dass die VDS-Richtlinie wegen Verletzungen der EU-Grundrechtecharta durch den EuGH gekippt wird. Die Ergebnisse sollten abgewartet werden, damit nicht ein höchst umstrittenes Umsetzungsgesetz in Kraft treten muss, dessen europarechtliche Grundlage nicht rechtssicher ist.

#### 6. Welche Daten werden aktuell gespeichert?

Heute gilt in Deutschland der Rechtszustand, wie er vor Inkrafttreten des deutschen Umsetzungsgesetzes zur Vorratsdatenspeicherung bestanden hat. Das bedeutet, dass

Telekommunikationsanbieter Verbindungsdaten speichern können, die zu Abrechnungszwecken und bei Störungen und Missbrauch erforderlich sind.

Technische Probleme gibt es aktuell noch bei der Erfassung bzw. Identifizierung des Surfens über mobile Plattformen (Handys, Tablet-Pcs) via UMTS. Klar ist, dass diese Probleme bei einer Vorratsdatenspeicherung genauso auftreten würden.

## **7. Gibt es Sicherheitslücken?**

Den Sicherheitsbehörden stehen bereits viele Mittel für ihre erfolgreiche Ermittlungsarbeit zur Verfügung, bei denen der Grundsatz der Verhältnismäßigkeit gewahrt wird.

Nach dem Telekommunikationsgesetz können Verkehrs- und Standortdaten von Telekommunikationsverbindungen bis zu 6 Monate gespeichert werden. Ein Rückgriff auf diese Daten ist heute auch möglich. Stoßen Ermittler auf strafbare Handlungen im Internet, wie zum Beispiel die Verbreitung von Kinderpornographie, so kann die Identität des Täters durch sofortige Abfrage vom Provider ermittelt werden.

Im Übrigen: Das Bundesverfassungsgericht hat bei der Abwägung von Grundrechten eventuelle Schutzlücken explizit in Kauf genommen. Gespeicherte Daten dürfen nur zum Schutz von überragend wichtigen Rechtsgütern verwendet werden. Darunter fallen Leib, Leben oder Freiheit einer Person - aber nicht das Vermögen. Einen „Rundum“-Schutz, z. B. gegen Online-Betrug, toleriert es also nicht.

## **8. Warum wird gerade jetzt so vehement die Wiedereinführung der Vorratsdatenspeicherung gefordert?**

Häufig wird angesichts einer erhöhten Gefährdungslage reflexartig nach mehr Sicherheitsgesetzen gerufen. Die Zahlen und Argumente zur Erforderlichkeit der Vorratsdatenspeicherung sind jedoch weitgehend falsch, nicht nachvollziehbar oder nicht überprüfbar. Insbesondere wird auch nicht hinreichend berücksichtigt, dass Strafverfolgung von Taten, die mittels Internet begangen wurden, nicht von einem einzigen Instrument abhängt. Ein effektiv eingesetzter Maßnahmenmix ist immer der beste Weg. Rechtsstaatliche Schranken der Überwachung erhöhen den Druck, Überwachungsmaßnahmen zielgerichtet und effektiv auszugestalten.

## **9. Was ist eine liberale Alternative zur Vorratsdatenspeicherung?**

Die FDP setzt sich für eine verfassungskonforme Alternative zu VDS ein, die wir „Quick Freeze“ nennen.

Wir wollen für das Quick-Freeze-Verfahren eine gesetzliche Grundlage schaffen. Danach soll es möglich sein, die Telekommunikationsprovider zu verpflichten, für einen bestimmten Zeitraum bestimmte Telekommunikationsverbindungsdaten mit Personenbezug kurzfristig zu puffern (schnelles Einfrieren der Daten, „quick freeze“), falls Verdacht auf eine Straftat besteht oder Hinweise auf eine konkrete Gefahr vorliegen. Der Zugriff auf die so gepufferten Daten (das „Auftauen“) und deren Nutzung stehen dann unter Richtervorbehalt.

Schon heute werden insbesondere bei Ermittlungen in Foren, Tauschbörsen oder bei bekannten Angeboten im World Wide Web wegen schwerer und schwerster Kriminalität erfolgreich für einen bestimmten Beobachtungs- und Ermittlungszeitraum solche Daten in strafprozessual zulässiger und verfassungsrechtlich unbedenklicher Weise erhoben (§§ 100 a und g StPO). Die ohnehin bei Telekommunikationsanbietern befindlichen Daten können durch „Quick Freeze“ bis zur Auswertung durch richterliche Anordnung gepuffert, ihr routinemäßiges Löschen verhindert werden. Um die gepufferten Daten Personen zuordnen zu können, ist es darüber hinaus notwendig, für den Ermittlungszeitraum auch solche Telekommunikationsverbindungsdaten kurzfristig zu sichern, die mangels Veranlassung von Telekommunikationsanbietern bislang oft nicht gesichert werden.

Auf diese Weise können wichtige Ermittlungsansätze erlangt und genutzt werden. Behörden haben so Gelegenheit zu weiteren Ermittlungen, die die notwendige Klarheit darüber erbringen sollen, ob die Voraussetzungen für eine, dann unter Richtervorbehalt stehende, Datenerhebung und damit ein „Auftauen“ der Daten vorliegen. Ist die Sicherungsfrist abgelaufen und hat sich der Verdacht nicht bestätigt, sind die Daten unverzüglich zu löschen. Das gibt den Behörden soviel Ermittlungsansätze wie für eine effektive Strafverfolgung nötig und Bürgern soviel kommunikative Freiheit wie möglich.

Quick Freeze ist somit die verfassungskonforme Alternative zur Vorratsdatenspeicherung.