Alvar C.H. Freude, Jan Mönikes, Henning Tillmann

Vorratsdatenspeicherung

Materialien zum Hintergrundgespräch mit Innenminister Ralf Jäger

Version 0.6.1 vom 30. August 2011

Die Autoren

Henning Tillmann
Mitglied im Gesprächskreis *Netzpolitik und digitale Gesellschaft* SPD-Parteivorstand

Finowstraße 24
10247 Berlin
(030) 49 20 83 22
(01 62) 681 680 4
henning.tillmann@gmail.com
http://www.henning-tillmann.de/

Alvar C.H. Freude
Mitglied der *Enquête-Kommission Internet und digitale Gesellschaft* des Deutschen Bundestages

Fideliostraße 16
70597 Stuttgart
(01 79) 13 46 47 1
(07 11) 75 88 47 79
af@alvar-freude.de
http://alvar.a-blast.org/

Jan Mönikes
Rechtsanwalt
SCHALAST & PARTNER Rechtsanwälte

Dorotheenstraße 54
10117 Berlin
(0 30) 32 53 80 68
(01 72) 296 75 66
jan.moenikes@schalast.com
http://www.moenikes.de

Vorbemerkung und Zusammenfassung

Die Diskussion über die sog. „Vorratsdatenspeicherung“ (VDS) wird oft nur schwarz/weiß und stark emotionalisiert geführt. Bei einer genaueren Betrachtung ist aber eine tiefergehende Differenzierung nötig: Tatsächlich kann eine Vorratsdatenspeicherung die Dimensionen eines Überwachungsstastes annehmen, bei der jeder Bürger auf Schritt und Tritt überwacht und sein gesamtes Kommunikationsverhalten kontrolliert wird. Wer hat wann mit wem von welchem Ort telefoniert? Wer hat wann wem eine E-Mail geschrieben? All das und noch viel mehr musste mit dem vom Bundesverfassungsgericht für verfassungswidrig erklärten Gesetz zur Vorratsdatenspeicherung monatelang gespeichert werden.

Auf der anderen Seite gibt es ein legitimes Interesse der Ermittlungsbehörden, Straftaten aufzuklären. Bei Internet-Delikten ist es besonders wichtig, eine Zuordnung von der so genannten IP-Adresse (Internet-Protokoll-Adresse) zu einem Internet-Anschluss herzustellen. Diese IP-Speicherung war jahrelang üblich und ein wichtiges Instrument bei der Ermittlung von Straftätern.

Der Gesprächskreis „Netzpolitik und digitale Gesellschaft“ beim SPD-Parteivorstand hat über mehre Monate einen Antrag entwickelt, der eben genau den Ausgleich zwischen Freiheitsrechten und moderner Strafverfolgung schaffen soll: durch eine Anwendung einer Datenspeicherung mit Augenmaß können alle Interessen bewahrt werden. Die Speicherung von IP-Adressen halten wir für vertretbar, wenn die Herausgabe an die vom Bundesverfassungsgericht gestellten Bedingungen geknüpft ist. Der Eingriff in die Privatsphäre der Bürger ist relativ gering, da nur nach einer konkreten Tat ein Rückschluss auf den Täter möglich ist, aber eine gefürchtete Totalüberwachung ausgeschlossen bleibt.

Die Speicherung weiterer Daten sehen wir kritisch; für Details sei hier auf den angehängten Musterantrag verwiesen.

Diskussionsstand

Stand der politischen Diskussion in Europa

Rechtliche Grundlage der Vorratsdatenspeicherung ist die EU Richtlinie vom 14. Dezember 2005. Diese befindet sich in der Evaluierung durch die EU-Kommission. Das Ergebnis wurde am 18. April 2011 offiziell veröffentlicht. Kernaussagen:

- RiL zur VDS hat keine Harmonisierung und keine gleichen Wettbewerbsbedingungen erzielt.
- Kommission will daher u.a. Wege zur „übereinstimmenden Kostenerstattung für alle Betreiber“ suchen.
- Jedes künftige Konzept zur verdachtslosen Protokollierung von Nutzerspuren muss Verhältnismäßigkeitsprinzip respektieren und „geeignet“ sein für die Bekämpfung schwerer Verbrechen und von Terrorismus.
- Zudem soll RiL u.a. auch noch hinsichtlich Effizienz der Strafverfolgung überprüft werden. Ein „Schürfen in den Daten“ soll verhindert werden
- Das Alternativkonzept des BMJ („Quick Freeze“) wird auf EU-Ebene bislang nicht ernsthaft diskutiert.

Stand der politischen Diskussion in Deutschland

Forderung des BMI

Eine zeitnahe Verabschiedung eines neuen Gesetzes zur Vorratsdatenspeicherung, mit wenigen Änderungen gegenüber der vom Bundesverfassungsgericht für verfassungswidrig erklärten Regelung und mindestens 6 Monaten Speicherfrist.

Vorschlag des BMJ

Aus dem Eckpunktepapier zur Sicherung von Verkehrsdaten und Gewährleistung von Bestandsdatenauskünften im Internet

- Für „ohnehin“ vorhandene TK-Daten soll eine anlassbezogene Speicherung nach „einfacher“ behördlicher Anordnung gelten.
- Beauskunftung nur nach § 100g StPO – Strengere Anforderungen für Erhebungsanordnung als für Sicherungsanordnung.

- Anlasslose Speicherung von IP-Verkehrsdaten um Bestandsdatenauskünfte im Internet zu ermöglichen – nur für 7 Tage
- Der Gesetzentwurf auf Basis des Eckpunktepapiers ist seit Juni 2011 in der Ressortabstimmung

Der Vorschlag des BMJ würde die derzeitige Richtlinie der EU nicht umsetzen.

Vorschlag des Arbeitskreises gegen Vorratsdatenspeicherung

Der AK Vorrat schlägt einen grundsätzlichen Verzicht für jede Art von Speicherung (auch für IP-Adressen) vor. Die Speicherung soll nur bei konkretem Verdacht erfolgen.

Antrag der SPD-Bundestagsfraktion in der Internet-Enquete

Differenzierte Betrachtung je nach Datentyp: Speicherung der ermittlungstechnisch wichtigeren IP-Adressen für ca. 80 Tage unter Einhaltung der Vorgaben des Bundesverfassungsgerichtes (revisionssichere Protokollierung, Informationspflichten usw). Weitere Daten nur für wenige Tage und Zugriff nur bei schweren Straftaten.

Neuformulierung der EU-Richtlinie.

Vorschlag des Gesprächskreises Netzpolitik beim SPD-Parteivorstand

Vergleichbar mit dem Vorschlag der SPD-Fraktion, mit nochmals genauerer Differenzierung bzgl. unterschiedlicher Daten-Typen.

Grundsätzliche Leitfragen

- Welche Maßnahmen können durch die VDS getroffen werden?
- Was bedeutet Vorratsdatenspeicherung? Welche Maßnahmen sind enthalten?
- Was ist verhältnismäßig und zu welchem Preis?

Der Bedarf in Theorie und Praxis

Die EU-Richtlinie zur Vorratsdatenspeicherung sieht eine sehr umfangreiche Liste der zu protokollierenden Daten vor:

Folgende Datenkategorien müssen auf Vorrat gespeichert werden:

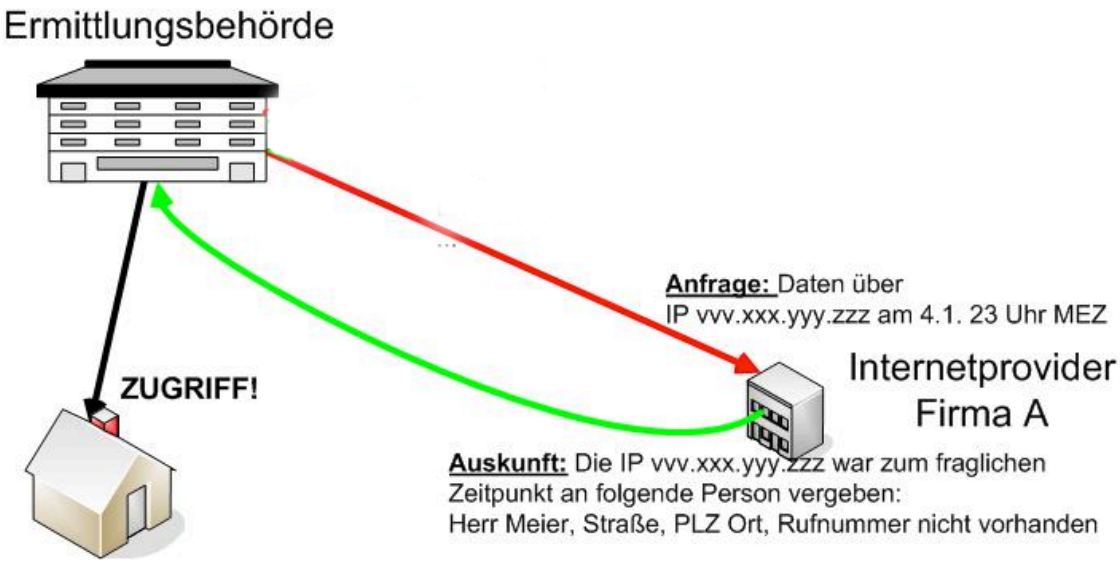
1. zur Rückverfolgung und Identifizierung der Quelle einer Nachricht benötigte Daten:
    1. betreffend Telefonfestnetz und Mobilfunk:
        1. die Rufnummer des anrufenden Anschlusses,
        2. der Name und die Anschrift des Teilnehmers bzw. registrierten Benutzers
    2. betreffend Internetzugang, Internet-E-Mail und Internet-Telefonie:
        1. die zugewiesene Benutzerkennung,
        2. die Benutzerkennung und die Rufnummer, die jeder Nachricht im öffentlichen Telefonnetz zugewiesen werden,
        3. der Name und die Anschrift des Teilnehmers bzw. registrierten Benutzers, dem eine IP-Adresse, Benutzerkennung oder Rufnummer zum Zeitpunkt der Nachricht zugewiesen war;
2. zur Identifizierung des Adressaten einer Nachricht benötigte Daten:
    1. betreffend Telefonfestnetz und Mobilfunk:
        1. die angewählte(n) Nummer(n) (die Rufnummer(n) des angerufenen Anschlusses) und bei Zusatzdiensten wie Rufweiterleitung oder Rufumleitung die Nummer(n), an die der Anruf geleitet wird,
        2. die Namen und Anschriften der Teilnehmer oder registrierten Benutzer;
    2. betreffend Internet-E-Mail und Internet-Telefonie:
        1. die Benutzerkennung oder Rufnummer des vorgesehenen Empfängers eines Anrufes mittels Internet-Telefonie,
        2. die Namen und Anschriften der Teilnehmer oder registrierten Benutzer und die Benutzerkennung des vorgesehenen Empfängers einer Nachricht;
    3. zur Bestimmung von Datum, Uhrzeit und Dauer einer Nachrichtenübermittlung benötigte Daten:
        1. betreffend Telefonfestnetz und Mobilfunk: Datum und Uhrzeit des Beginns und Endes eines Kommunikationsvorgangs;
        2. betreffend Internetzugang, Internet-E-Mail und Internet-Telefonie:
            1. Datum und Uhrzeit der An- und Abmeldung beim Internetzugangsdienst auf der Grundlage einer bestimmten Zeitzone, zusammen mit der vom Internetzugangsanbieter einer Verbindung zugewiesenen dynamischen oder statischen IP-Adresse und die Benutzerkennung des Teilnehmers oder des registrierten Benutzers;
            2. Datum und Uhrzeit der An- und Abmeldung für einen Internet-E-Mail-Dienst oder einen Internet-Telefonie-Dienst auf der Grundlage einer bestimmten Zeitzone;
4. zur Bestimmung der Art einer Nachrichtenübermittlung benötigte Daten:
    1. betreffend Telefonfestnetz und Mobilfunk: der in Anspruch genommene Telefondienst;
    2. betreffend Internet-E-Mail und Internet-Telefonie: der in Anspruch genommene Internetdienst;
5. zur Bestimmung der Endeinrichtung oder der vorgeblichen Endeinrichtung von Benutzern benötigte Daten:
    1. betreffend Telefonfestnetz: die Rufnummern des anrufenden und des angerufenen Anschlusses;
    2. betreffend Mobilfunk:
        1. die Rufnummern des anrufenden und des angerufenen Anschlusses,
        2. die internationale Mobilteilnehmerkennung (IMSI) des anrufenden Anschlusses,
        3. die internationale Mobilfunkgerätekennung (IMEI) des anrufenden Anschlusses,
        4. die IMSI des angerufenen Anschlusses,
        5. die IMEI des angerufenen Anschlusses,
        6. im Falle vorbezahlter anonymer Dienste Datum und Uhrzeit der ersten Aktivierung des Dienstes und die Kennung des Standorts (Cell-ID), an dem der Dienst aktiviert wurde;
    3. betreffend Internetzugang, Internet-E-Mail und Internet-Telefonie:
        1. die Rufnummer des anrufenden Anschlusses für den Zugang über Wählanschluss,
        2. der digitale Teilnehmeranschluss (DSL) oder ein anderer Endpunkt des Urhebers des Kommunikationsvorgangs;
6. zur Bestimmung des Standorts mobiler Geräte benötigte Daten:
    1. die Standortkennung (Cell-ID) bei Beginn der Verbindung,
    2. Daten zur geographischen Ortung von Funkzellen durch Bezugnahme auf ihre Standortkennung (Cell ID) während des Zeitraums, in dem die Vorratsspeicherung der Kommunikationsdaten erfolgt.

In der Praxis wird bei Straftaten im Internet vor allem eine Zuordnung benötigt: die IP-Adresse.

Ein Praxis-Beispiel

Ein Straftäter verbreitet über eine Online-Plattform illegale Inhalte, beispielsweise lädt er kinderpornografische Bilder in einem sozialen Netzwerk hoch. Die typische Ermittlungsarbeit sieht folgendermaßen aus:

- Die Ermittler stellen ein Auskunftsersuchen an den Plattformbetreiber.
  - Sie erhalten eine IP-Adresse und einen Zeitstempel, Beispielsweise 79.197.236.6 und 2011-08-29 20:53:47
  - Oft stellen die Plattformbetreiber nach Kenntnis entsprechender Vorgänge auch selbst Strafanzeige.
- Über die IP-Adresse finden sie mittels des Internet-Whois-Dienstes den Zugangsanbieter des Verdächtigen Heraus, in dem Falle die Deutsche Telekom AG.
  - Dort stellen Sie eine Anfrage nach dem Anschlussinhaber.
  - Der Zugangsanbieter liefert Name und Anschrift des Anschlussinhabers.
- Die Ermittler wissen nun, über welchen Anschluss die Straftat begangen wurde.



Port-Speicherung

So genannte IP-Ports werden verwendet, um unter einer IP-Adresse mehrere Dienste kontaktieren oder anbieten zu können. Sie sind ein festes Element des Internet-Proto-

kolls. Ein- und ausgehende Datenpakete werden neben der IP-Adresse über die Portnummer adressiert; damit können diese Pakete dem entsprechenden Programm zugeordnet werden.

Mobilfunkanbieter bringen unter einer öffentlichen IP-Adresse mehrere Internet-Nutzer ins Netz. Für jede einzelne Internet-Verbindung wird dann anhand der Ports entschieden, welcher Nutzer adressiert werden muss. Dies ist ein internes Verfahren des Protokolls. Damit reicht aber zur Identifizierung die IP-Adresse nicht mehr aus.

IP-Adressen in laufenden Ermittlungen stammen i.d.R. aus Protokolldateien von Diensteanbietern (Server-Logs), die zu technischen Zwecken gespeichert wurden. Portnummern werden in diesen Protokolldateien nicht gespeichert, nur die IP-Adresse. Port-Nummern werden auch in anderen Kontexten so gut wie nie gespeichert sondern nur intern verarbeitet. Auch wenn die Mobilfunkanbieter also anhand von IP-Adresse, Port-Nummer und Zeitstempel einen Anschlussinhaber identifizieren könnten, würde dies nichts helfen, da diese Daten den Ermittlern nahezu nie vorliegen.

Zusätzlich muss man sich im Klaren sein, dass eine Speicherung aufgrund der hohen Datenmengen praktisch unmöglich ist: So entstehen pro einzelnem Webseitenaufruf bei dem Zugangsanbieter dutzende von Datensätze – Beispiel spiegel.de: rund 150. Für jede einzelne Seite, für jeden „Klick“. Das zu speichernde Datenvolumen wäre außerordentlich groß und ein Vielfaches von allen anderen anfallenden Daten.

Ein Grund für die mehrfache Zuordnung von einer IPv4-Adresse an mehrere Endanwender im Mobilfunkbereich ist die Knappheit der verfügbaren IP-Adressen. Dieses Problem erledigt sich bald von selbst: durch die künftige Etablierung von IPv6 sind genügend Adressen vorhanden, um allen heutigen und zukünftigen Anwendungen und Geräten mehrere eigene IP-Adressen zu geben.

Was ist verhältnismäßig?

Über die IP-Adresse lässt sich also ermitteln, von welchem Internet-Anschluss aus die Straftat begangen wurde. Dies ist verhältnismäßig und betrifft weitgehend nur den Täter.

Es lässt sich damit kein Bewegungsprofil erstellen, sprich: es lässt sich nicht ermitteln, welche Interessen eine Person hat, welche Webseiten sie besucht oder mit wem sie kommuniziert.

Die Zuordnung IP-Adresse zum Anschlussinhaber wurde auch bereits vor der Einführung der Vorratsdatenspeicherung bei den Zugangsanbietern gespeichert. In der Regel waren ca. 80 Tage üblich.

Mit der Vorratsdatenspeicherung kamen aber viele neue Daten hinzu, beispielsweise Mobilfunk-Standortdaten.

Mit Telefon- und E-Mail-Verbindungsdaten lassen sich umfangreiche Nutzungs- sowie Kommunikationsprofile und mit Mobilfunkdaten zusätzliche Bewegungsprofile erstellen. Die mit dem Grimme Online Award ausgezeichnete[1] Visualisierung von *Zeit Online* der aufgrund der ehemaligen gesetzlichen Vorgaben gespeicherten Vorratsdaten von Malte Spitz zeigt eindrucksvoll, was eine allgegenwärtige Beobachtung bedeutet.[2]

[1] zur Begründung der Jury siehe http://www.grimme-institut.de/html/index.php?id=1345

[2] vgl. http://www.zeit.de/datenschutz/malte-spitz-vorratsdaten und http://blog.zeit.de/open-data/2011/02/24/vorratsdaten-unter-der-lupe/

Musterantrag des Gesprächskreises *Netzpolitik und digitale Gesellschaft* beim SPD-Parteivorstand

Grundrechte wahren, Freiheit und Sicherheit stärken: Vorratsdatenspeicherung verfassungskonform überarbeiten und differenziert betrachten!

Der Bundesparteitag möge beschliessen:

Die SPD setzt sich auf europäischer Ebene für eine grundlegende Überarbeitung der europäischen Richtlinie über die Vorratsdatenspeicherung ein. Ziel muss sein, eine differenzierte und verfassungskonforme Richtlinie zu erstellen und in deutsches Recht umzusetzen. Jegliche Art von Vorratsdatenspeicherung ist für die Sozialdemokratie ein erheblicher Eingriff in die Grundrechte der Bürgerinnen und Bürger und darf daher, wenn überhaupt, nur in engen Grenzen erfolgen. Als einzige Partei betrachtet die deutsche Sozialdemokratie die Vorratsdatenspeicherung differenziert, um die die unveräußerlichen Freiheitsrechte der Bürgerinnen und Bürger zu sichern, andererseits die Kriminalitätsbekämpfung für das 21. Jahrhundert zu rüsten.

Die sozialdemokratische Europa- und Bundestagsfraktion sowie die über den Bundesrat beteiligten sozialdemokratischen Funktionsträger in den Ländern, werden daher aufgefordert:

1. Auf europäischer Ebene darauf hinzuwirken, dass die Richtlinie 2006/24/EG über die Vorratsspeicherung grundlegend überarbeitet wird: Es soll den Mitgliedsstaaten überlassen sein, ob sie Telekommunikationsanbieter zur Speicherung verpflichten (Kann-Regelung). Bei Beibehaltung einer europaweiten Verpflichtung ist die Maximalspeicherfrist von verdachtslos gespeicherten Daten auf sechs Monate, statt bisher auf zwei Jahre, festzulegen. Für sensible Daten wie beispielsweise Telefon-Verbindungsdaten sollte eine maximal auf wenige Tage beschränkte Speicherverpflichtung und hohe Zugriffshürden gelten. Bewegungsprofile durch Funkzellenauswertung dürfen generell nicht ermöglicht werden.

2. Keine gesetzliche Regelung für eine Vorratsdatenspeicherung kann die Arbeit von Ermittlungsbehörden ersetzen. Die SPD setzt sich daher dafür ein, dass Polizei und Staatsanwaltschaften ausreichend personell sowie technisch ausgestattet sind, damit Straftaten – egal wo sie stattfinden – rasch aufgeklärt werden können. Dem technischen Fortschritt sollte mit umfangreichen Weiterbildungsinitiativen für Ermittlungsbehörden Rechnung getragen werden.

3. Sich sowohl auf Bundes- als auch europäischer Ebene nur für solche Regelungen einzusetzen, die mit den Maßgaben des Urteils des Bundesverfassungsgerichts vereinbar sind. Darüber hinausgehend ist für die SPD eine Zustimmung zu einer Vorratsdatenspeicherung wenn überhaupt nur möglich, wenn folgende Anforderungen berücksichtigt werden:

   a) Der Abruf und die Nutzung der Verbindungsdaten darf nur bei Verdacht auf schwerste Straftaten erfolgen. Das sind insbesondere Straftaten gegen das Leben, die körperliche Unversehrtheit und die sexuelle Selbstbestimmung (Katalogstraftaten nach §100a StPO). Auskünfte für Ordnungswidrigkeiten sind auszuschließen.

   b) Keinesfalls darf eine verdachtslose Speicherung von Funkzellen (Cell-IDs) bei Mobiltelefonen (Telefonverbindungen und mobiles Internet) stattfinden. Gleiches gilt für die Speicherung von E-Mail-Verbindungsdaten.

   c) Die Beauskunftung von Anschlussinhabern anhand einer IP-Adresse kann als milderes und weniger eingriffsintensives Mittel zur Aufklärung von Straftaten genutzt werden. Dabei sollte ein Abruf jedoch nur innerhalb einer angemessenen Frist erfolgen können.

   d) Eine Nutzung der Daten darf ausschließlich für strafrechtliche, nicht für zivilrechtliche Auskünfte erfolgen.

   e) Jeder Abruf von Vorratsdaten muss unter Richtervorbehalt stehen.

   f) Es ist eine generelle Unterrichtungspflicht für die von einem Datenabruf Betroffenen aufzunehmen.

   g) Für Berufsgeheimnisträger und andere Geheimnisträger (wie Journalisten, Abgeordnete, Rechtsanwälte, Priester, etc.) muss ein absolutes Verwertungsverbot gelten.

   h) Die Bestimmungen zum technischen Datenschutz sind entsprechend den verfassungsgerichtlichen Vorgaben deutlich auszubauen. Dazu gehören namentlich eine getrennte Speicherung, die sichere Verschlüsselung von Daten, das Vier-Augen-Prinzip verbunden mit fortschrittlichen Verfahren zur Authentifizierung für den Zugang zu den Schlüsseln und eine revisionssichere Protokollierung von Zugriff und Löschung.

   i) Der Bundesdatenschutzbeauftragte muss die Umsetzung sowie den laufenden Betrieb jederzeit kontrollieren können. Verstöße gegen den Datenschutz oder das Verbot der Datenabfrage müssen wirksam sanktioniert werden. Neben entsprechenden Bußgeldtatbeständen ist ein gesetzliches

Beweisverwertungsverbot für zu Unrechte erlangte Auskünfte einzuführen.

j) Eine Erstattung der Kosten der Telekommunikationsanbieter zur Umsetzung der Vorratsdatenspeicherung sind vorzusehen.

Begründung:

Wir möchten erreichen, dass die europäische Zusammenarbeit in der Verfolgung schwerer Straftaten erleichtert wird, Freiheitsrechte ohne Wenn und Aber gesichert und sogar gestärkt werden. Durch ihre zu weit gefassten Regelungen hat die bestehende Richtlinie zur Vorratsdatenspeicherung das Ziel einer europäischen Harmonisierung bestehender nationaler Regelungen verfehlt. Das Bundesverfassungsgericht hat das deutsche Gesetz zur Umsetzung daher auch in weiten Teilen beanstandet, wie auch andere Verfassungsgerichte in Europa.

Wir sind überzeugt, dass die Konzentration auf sehr viel weniger, dafür aber einheitlich festgelegte Datenarten, die Entscheidung für ein kürzere Mindestspeicherfristen und die scharfe Eingrenzung des Katalogs der Straftaten, zu deren Verfolgung auf die Daten zugegriffen werden darf, die Freiheitsrechte sichert und zugleich die Effizienz der Kriminalitätsbekämpfung über die europäischen Grenzen hinweg erhöht. Eine verhältnismäßige Begrenzung der Vorratsdatenspeicherung auf europäischer Ebene wird auch den Interessen aller Bürgerinnen und Bürger in Europa eher gerecht, die anlasslos einen Eingriff in ihr Telekommunikationsgeheimnis hinnehmen sollen.

Insbesondere folgende Punkte sind mit sozialdemokratischen Positionen in Übereinstimmung zu bringen:

- Sowohl aus kriminalistischer als auch aus bürgerrechtlicher Sicht ist eine stärkere Differenzierung zwischen den verschiedenen anfallenden Daten geboten: Durch die Speicherung der Zuordnung von IP-Adressen zu Anschlussinhabern bei Internet-zugangsanbietern ist keine Totalüberwachung der Bevölkerung möglich, ebenso keine rückwirkende Erstellung von exakten Nutzungsprofilen. Aber nach einer konkreten Straftat haben Ermittler zumindest eine Chance, den Anschlussinhaber des Anschlusses, von dem aus die Tat begangen wurde, zu ermitteln um von dort aus vielleicht mit anderen, konventionellen polizeilichen Mitteln zu arbeiten. Bis vor wenigen Jahren war es zudem bereits üblich, dass die Internet-Zugangsanbieter diese Zuordnung bis zu 90 Tage lang speicherten.
- Die erst durch die Vorratsdatenspeicherung eingeführte Pflicht zur Speicherung von Funkzellen (Cell-IDs) bei der Nutzung von Mobiltelefonen dagegen ermög-

lichen ein umfassendes Bewegungsprofil. Da Mobilfunkgespräche und die mobile Internetnutzung durch Flatrates immer mehr an Bedeutung gewinnen, lässt sich durch die Aufzeichnung der Ortungsdaten ein umfassendes Bewegungsprofil erstellen. Die SPD lehnt die verdachtsunabhängige und flächendeckende Speicherung von Ortungsdaten deshalb entschieden als einen zu weit gehenden Eingriff in die Privatsphäre unverdächtiger Bürgerinnen und Bürger ab.

- Die Erfassung von E-Mail-Kommunikationsdaten ist auch für technisch nicht versierte Kriminelle sehr leicht umgehbar. Gleichzeitig stellt sie aber einen massiven Eingriff in das Kommunikationsgeheimnis unbescholtener Bürgerinnen und Bürger dar: Die Aufzeichnung von E-Mail-Kommunikationsdaten ohne konkreten Verdacht entspräche der Anordnung an die Post, Kopien sämtlichen Briefumschlägen anzufertigen. Ein solcher Eingriff wäre nur verhältnismäßig, wenn er im Rahmen einer konkreten Strafverfolgung angeordnet wird. Wir Sozialdemokraten sind überzeugt, dass eine effiziente Strafverfolgung dieses Instrument ansonsten nicht braucht, vor allem da dieses ohnehin einfach zu umgehen ist.
- Die Beauskunftung von Daten ohne richterlichen Beschluss und die undifferenzierte Verpflichtung von Internet- und Telekommunikationsunternehmen, selbst wenn bei diesen aufgrund kriminalistischer Erfahrung keine relevanten Daten zu erwarten sind, ist ebenso abzulehnen, wie der Verzicht auf eine Erstattung der tatsächlichen Kosten der Verpflichteten. Nur wenn Speicherung und Beauskunftung auch einen realen Preis haben, kann vermieden werden, dass die Vorratsdatenspeicherung zu einem „billigen“ Ersatz für andere Ermittlungsmaßnahmen wird und nicht die Ausnahme bleibt.
- Eine (nachgelagerte) Unterrichtungspflicht für die von einem Datenabruf Betroffenen gebietet unser Rechtsstaatsverständnis und entspricht im Übrigen den verfassungsrechtlichen Vorgaben.
- Nur ein Verwertungsverbot für besonders geschützte Personengruppen und in den Fällen rechtswidriger Auskunftserteilung kann, gemeinsam mit technischen Maßnahmen und Kontrollen der unabhängigen Datenschutzbehörden, Ausuferungen und Missbräuchen wirksam verhindern.

Antrag der SPD-Bundestagsfraktion in der Internet-Enquête des Bundestages

Der grundrechtliche Schutz informationeller Selbstbestimmung wurde durch die Rechtsprechung des Bundesverfassungsgerichts in jüngerer Zeit schärfer konturiert, nicht zuletzt durch die Entscheidung zur Vorratsdatenspeicherung. Das Bundesverfassungsgericht hat am 02. März 2010[3] entschieden, dass die Vorratsdatenspeicherung in Deutschland in ihrer bisherigen Umsetzung verfassungswidrig sei, da das Gesetz zur anlasslosen Speicherung umfangreicher Daten sämtlicher Nutzer elektronischer Kommunikationsdienste keine konkreten Maßnahmen zur Datensicherheit vorsehe und hat zudem die Hürden für den Abruf dieser Daten als zu niedrig bewertet. Das Urteil verpflichtete deutsche Telekommunikationsanbieter zur sofortigen Löschung der bis dahin gesammelten Daten. Das Bundesverfassungsgericht hat jedoch auch festgestellt, dass die Vorratsdatenspeicherung unter schärferen Sicherheits- und Transparenzvorkehrungen sowie begrenzten Abrufmöglichkeiten für die Sicherheitsbehörden grundsätzlich zulässig sei.

Die Enquete-Kommission empfiehlt dem Deutschen Bundestag,

- eine grundsätzliche und offene Debatte über die Notwendigkeit und auch die Grenzen der Vorratsdatenspeicherung zu führen. Dabei ist auch zu klären, ob und wie eine Speicherung auf Vorrat grundrechtsschonend und verfassungskonform ausgestaltet werden könnte. Die Enquete-Kommission geht dabei davon aus, dass es eine Zustimmung des Deutschen Bundestages für die Vorratsdatenspeicherung nur geben kann, wenn es zu einer grundsätzlichen Überarbeitung der damaligen Vorgaben zur Umsetzung der der Vorratsdatenspeicherung und auch eine Überarbeitung der europäischen Rechtsgrundlage kommt.
- auch mögliche Alternativen zu einer anlasslosen Vorratsdatenspeicherung zu überprüfen.
- zu klären, ob bezüglich der Dauer einer Speicherung und des Datenumfangs eine Rückkehr zu der bis ca. 2006 geltenden Situation möglich ist: Internet-Access-Provider haben damals IP-Adressen ca. 80 Tage gespeichert, E-Mail- Verbindungsdaten hingegen nur wenige Tage zu technischen Analysezwecken,
- dass, sofern eine Datenspeicherung auf Vorrat erfolgen soll, die Art der zu speichernden Daten als auch die Speicherdauer nicht einzelnen Unternehmen überlassen werden darf, sondern gesetzlicher Regelungen bedürfen.

[3] 1 BVerfG, Urteil vom 2. März 2010 – 1 BvR 256/08 zur Vorratsdatenspeicherung

•

Die Enquete-Kommission fordert deshalb den Deutschen Bundestag auf:

1. die Bundesregierung aufzufordern, auf europäischer Ebene darauf hinzuwirken, dass die Richtlinie 2006/24/EG über die Vorratsspeicherung grundlegend überarbeitet und eine Verkürzung der Speicherfrist von deutlich unter 6 Monaten aufgenommen wird. Dabei sollten insbesondere für sensible Daten wie beispielsweise Telefon-Verbindungsdaten, Mobilfunk- Ortsdaten und E-Mail-Verbindungsdaten maximal eine auf wenige Tage beschränkte Speicherdauer und hohe Zugriffshürden gelten. Bei den weniger sensiblen aber in der Praxis wichtigeren IP-Adressen sind längere Speicherfristen denkbar.

2. dass, sollte an der Vorratsdatenspeicherung festgehalten werden, verfassungskonforme gesetzliche Regelungen notwendig sind, die eine Speicherung von Daten und den Zugriff auf diese durch den Staat regelt und mit dem Urteil des Bundesverfassungsgerichts vereinbar ist.

3. Bei der konkreten Fassung der Regelungen sollten folgende Anforderungen mit aufgenommen werden:

   a) Der Abruf und die Nutzung der Verbindungsdaten darf nur bei Verdacht auf schwerste Straftaten erfolgen. Das sind insbesondere Straftaten gegen das Leben, die körperliche Unversehrtheit und die sexuelle Selbstbestimmung.

   b) Als milderes und weniger eingriffsintensives Mittel kann eine Beauskunftung von IP-Adressen geregelt werden. Dabei sollte ein Abruf innerhalb einer kurzen Frist von wenigen Tagen ab Speicherung zudem zum Zwecke der Verfolgung von Straftaten erfolgen können. Nach Ablauf dieser Frist darf der Datenabruf bis zur Löschung der Daten nur noch zur Verfolgung schwerster Straftaten erfolgen.

   c) Für Berufsgeheimnisträger soll ein absolutes Verwertungsverbot gelten.

   d) Der Abruf aller Verbindungsdaten soll unter Richtervorbehalt stehen.

   e) Es ist eine Unterrichtungspflicht für die von einem Datenabruf Betroffenen aufzunehmen. Dies gebietet das Rechtsstaatsverständnis und entspricht im Übrigen den verfassungsrechtlichen Vorgaben.

   f) Die Bestimmungen zum technischen Datenschutz müssen entsprechend den verfassungsgerichtlichen Vorgaben deutlich ausgebaut

werden. Dazu gehören namentlich eine getrennte Speicherung, die sichere Verschlüsselung von Daten, das Vier-Augen-Prinzip verbunden mit fortschrittlichen Verfahren zur Authentifizierung für den Zugang zu den Schlüsseln und eine revisionssichere Protokollierung von Zugriff und Löschung.

g) Eine effektive Kontrolle muss gewährleistet werden, Verstöße müssen wirksam sanktioniert werden.

h) Eine Nutzung der Daten darf ausschließlich für strafrechtliche, nicht für zivilrechtliche Auskünfte erfolgen.

Eine unterschiedliche Behandlung von IP-Adressen und anderen sensiblen Daten ist bereits im genannten Urteil des Bundesverfassungsgerichts zur Vorratsdatenspeicherung angelegt, ergibt sich aber auch aus der Eingriffstiefe und Sensibilität der Daten. Mit Telefon- und E-Mail-Verbindungsdaten lassen sich umfangreiche Nutzungs- sowie Kommunikationsprofile und mit Mobilfunkdaten zusätzliche Bewegungsprofile erstellen. Die mit dem Grimme Online Award ausgezeichnete[4] Visualisierung von Zeit Online der aufgrund der ehemaligen gesetzlichen Vorgaben gespeicherten Vorratsdaten von Malte Spitz zeigt eindrucksvoll, was eine allgegenwärtige Beobachtung bedeutet.[5]

Eine viel geringere Eingriffstiefe hat jedoch die Speicherung der Zuordnung von IP-Adressen zu Anschlussinhabern bei Internetverbindungen. Anders als vielfach behauptet ist damit keine komplette Überwachung des Surfverhaltens der Nutzer möglich. Im Gegensatz zur Durchführung einer gezielten Telekommunikationsüberwachung kann damit nicht festgestellt werden, welche Webseiten ein Internetnutzer aufgerufen hat. Es ist ausschließlich möglich, im Nachhinein nach einer konkreten Straftat bei Kenntnis der IP-Adresse den Anschlussinhaber herauszufinden. Die Sorge einer Totalüberwachung der Bevölkerung ist daher im Gegensatz zur Speicherung von Handy- und E-Mail-Daten unbegründet.

Bei mit Hilfe des Internets begangenen Straftaten ist die IP-Adresse oftmals die einzige verwertbare Spur. Daher ist der Wunsch der Ermittlungsbehörden nachvollziehbar, dieses Ermittlungsinstrument nutzen zu können. Dennoch sollten die Transparenz-

[4] zur Begründung der Jury siehe http://www.grimme-institut.de/html/index.php?id=1345 (abgerufen am 30. Juni 2011)

[5] vgl. http://www.zeit.de/datenschutz/malte-spitz-vorratsdaten und http://blog.zeit.de/open-data/2011/02/24/vorratsdaten-unter-der-lupe/ (abgerufen am 30. Juni 2011)

pflichten erhöht und die Speicherfristen auf ein Maß verkürzt werden, das auch vor der Vorratsdatenspeicherung jahrelang üblich war.

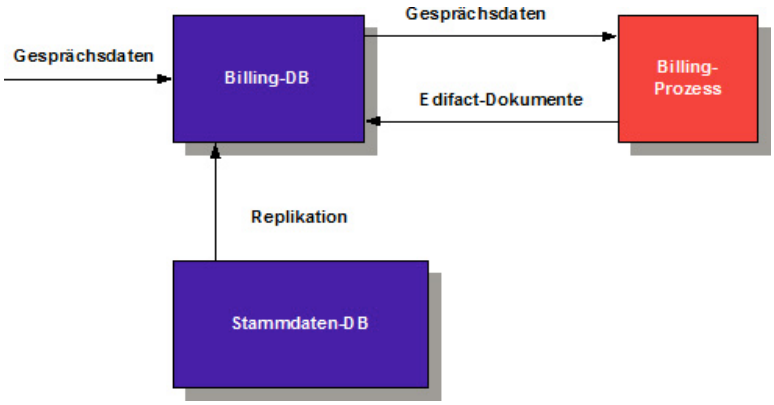
Eine große Angst in der Bevölkerung ist, dass die Speicherung von IP-Adressen weiter zu Massenabmahnungen bei der Nutzung von P2P-Tauschbörsen führt. Allerdings sind diese Abmahnungen auch ohne Speicherung der IP-Adressen durch Echtzeitabfragen oder entsprechende Speicheranforderungen („Quick Freeze“) möglich.

Da mit der skizzierten Regelung sowohl den berechtigten Interessen der Strafverfolgung als auch der Privatsphäre der Bürger Rechnung getragen wird als auch eine grundrechtsschonende Lösung vorliegt, empfiehlt die Enquête-Kommission dem Deutschen Bundestag auf europäischer Ebene eine entsprechende Initiative zu empfehlen und in Deutschland auf den Weg zu bringen.

Weitere Beispiele und grafische Darstellungen

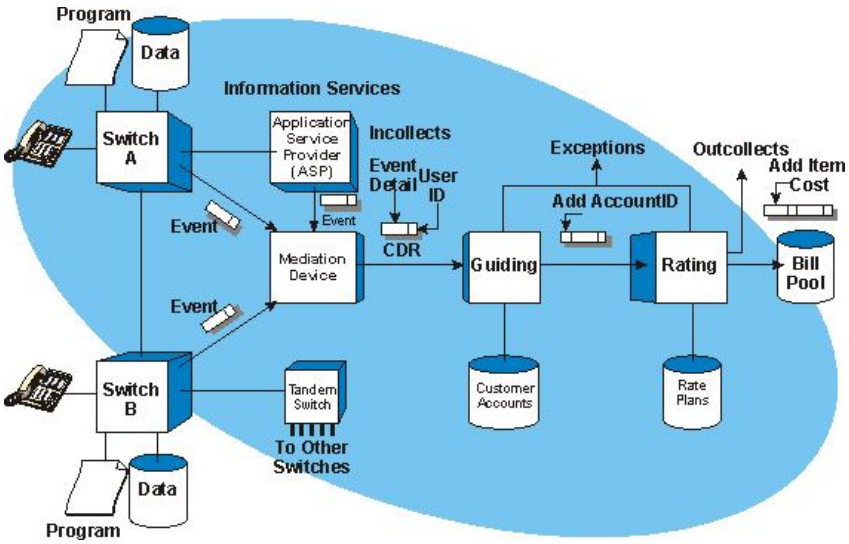
Vorratsdatenspeicherung/Quick Freeze
Beispiel: Datenerfassung Billing

- Grundschema:

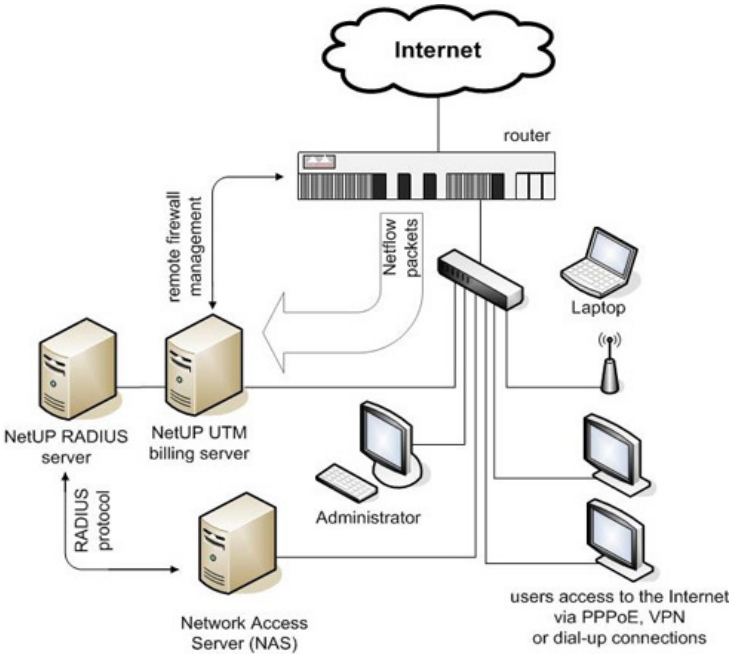


Vorratsdatenspeicherung/Quick Freeze
Beispiel: Datenerfassung Billing Sprache

- Detail:

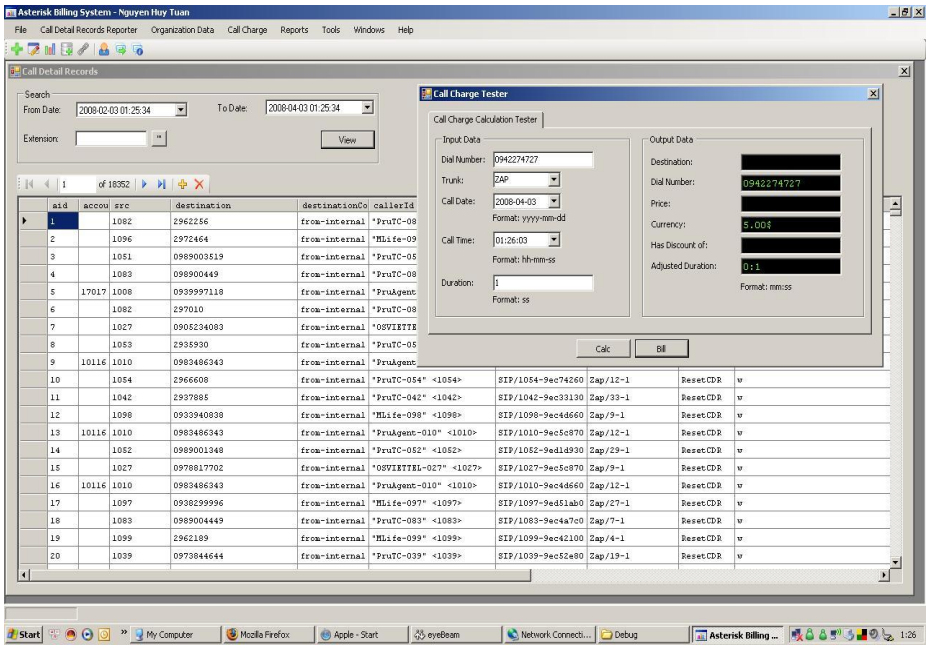


Billing bei Internet-Verbindungen

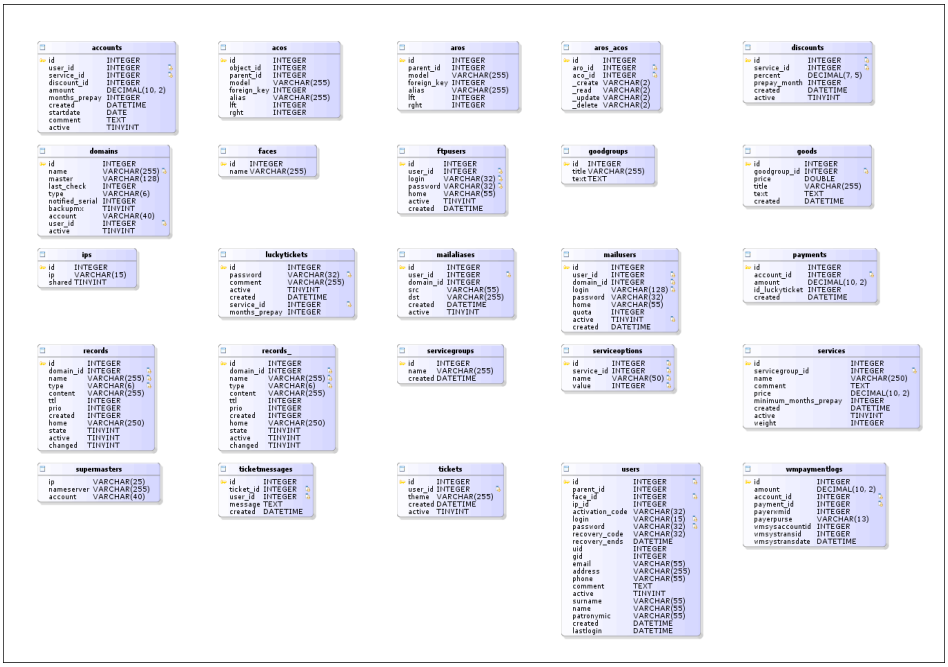


Vorratsdatenspeicherung/Quick Freeze

Beispiel: Datensatz ausgeleitete (Roh-) Daten



Vorratsdatenspeicherung/Quick Freeze
Beispiele der im Geschäftsverkehr relevanten Datensätze



Vorratsdatenspeicherung/Quick Freeze
Beispiel: Datensatz Kunde