

**Zur Verfassungsmäßigkeit  
der Vorratsdatenspeicherung**

**Meta-Rhein-Main-Chaos-Days**  
**TU Darmstadt, 06.09.2008**

**Jonas Breyer**

FB Rechtswissenschaft  
Johann Wolfgang Goethe-Universität Frankfurt am Main

# Zu speichernde Daten (1)

## Bei jeder Sprach- und SMS-Verbindung:

- Rufnummer
- Start- und Endzeit
- IMSI (SIM-Nummer) beider Teilnehmer
- IMEI (Endgerätenummer) beider Teilnehmer
- Funkzelle und deren Ort und Abstrahlwinkel
- Bei Voice-over-IP auch IP und Zeit beider Teilnehmer
- Bei SMS auch Zeit von Versand und Empfang

# Zu speichernde Daten (2)

## Bei jeder Datenverbindung:

- Internetverbindung
  - Darüber hinaus Anschlusskennung
  - IP
- E-Mail
  - E-Mail-Adressen aller Beteiligten
  - Zeit
  - Absender-IP
  - Bei E-Mail-Abruf Abrufer-IP und Zeit

# Voraussetzungen

Die Daten werden immer und bei jedem Bürger für 6 Monate ohne Verdacht oder Gefahr gespeichert.

Dagegen hat das Bundesverfassungsgericht u.a. am 04.04.2006 (Rasterfahndung) entschieden:

*„Der Grundsatz der Verhältnismäßigkeit führt dazu, dass der Gesetzgeber intensive Grundrechtseingriffe erst von bestimmten Verdachts- oder Gefahrenstufen an vorsehen darf [...] Verzichtet der Gesetzgeber auf begrenzende Anforderungen an die Wahrscheinlichkeit des Gefahreneintritts sowie an die Nähe der Betroffenen zur abzuwehrenden Bedrohung und sieht er gleichwohl eine Befugnis zu Eingriffen von erheblichem Gewicht vor, genügt dies dem Verfassungsrecht nicht.“*

# Ausmaß in Deutschland (1)

- 96% der deutschen Haushalte haben einen oder mehrere Telefonanschlüsse (132 Mio. Fest- und Mobilanschlüsse; jährlich 106 Mrd. Telefonminuten)
- 71% der deutschen Haushalte haben einen Internetanschluss
- Durch die Vorratsdatenspeicherung werden jederzeit über 63 Mrd. Verbindungen gespeichert

---

Q: Eurostat,

[http://epp.eurostat.ec.europa.eu/portal/page?\\_pageid=2973,64549069,2973\\_64554066&-\\_dad=portal&\\_schema=PORTAL](http://epp.eurostat.ec.europa.eu/portal/page?_pageid=2973,64549069,2973_64554066&-_dad=portal&_schema=PORTAL).

## Ausmaß in Deutschland (2)

- Jährlich werden in Deutschland 220.000 Verbindungsdaten abgefragt
- Dabei sind durchschnittlich 130 andere Gesprächspartner mitbetroffen
- Dadurch wird jährlich das Telekommunikationsverhalten von 28 Mio. Bürgern offengelegt.

---

Q: Eurostat,

[http://epp.eurostat.ec.europa.eu/portal/page?\\_pageid=2973,64549069,2973\\_64554066&-\\_dad=portal&\\_schema=PORTAL](http://epp.eurostat.ec.europa.eu/portal/page?_pageid=2973,64549069,2973_64554066&-_dad=portal&_schema=PORTAL).

# Bedarf an Verbindungsdaten

- Abgefragt werden 0,0004% der gespeicherten Daten
- Vor der Vorratsdatenspeicherung fehlten den Behörden Daten in unter 0,01% der Fälle, dabei waren die Daten häufig auch so alt, dass auch die Vorratsdatenspeicherung nichts nützt
- Aufklärungsquote mittels Telekommunikation begangener Straftaten vor Vorratsdatenspeicherung 54%

---

Q: BKA, Polizeiliche Kriminalstatistik 2006, S. 65.

# Verwendung und Nutzen abgefragter Verbindungsdaten

- Betrug: 54%
- Beleidigung: 6%
- Urheberrechtsstraftaten: 4%
- 83% aller erfolgreichen Abfragen bringen kein verfahrensrelevantes Ergebnis

---

Q: BKA, Polizeiliche Kriminalstatistik 2006, S. 65;  
Köbele (Dt. Telekom), Vortrag am 27.08.2007,  
<https://www.datenschutzzentrum.de/sommerakademie/2007/sak2007-koebele-wirtschaftsunternehmen-verlaengerter-arm-der-sicherheitsbehoerden.pdf>, 9.

# Kriminalitätsentwicklung

- Trotz immer größerer Eingriffsbefugnisse ist die Kriminalität in den letzten 15 Jahren konstant
- In Japan, wo es keinerlei Telekommunikationsüberwachung gibt, ist die Kriminalitätsrate vergleichbar
- Aufklärungsrate der mittels Telekommunikations begangener Straftaten ist von 44% auf 54% angestiegen

---

Q: BKA, Polizeiliche Kriminalstatistik 2006, S. 65;

# Gefahren (1)

- Erstellung von Persönlichkeits- und Bewegungsprofilen der gesamten Bevölkerung
- EDV ermöglicht eine Auswertung, Verknüpfung und Übermittlung der Verbindungsdaten.
- Dies machen die Polizeien Bayern, Berlin, Rheinland-Pfalz, Mecklenburg-Vorpommern und Schleswig-Holstein mit der Software „RsCase“ schon heute (Abgleich mit Antiterrordatei, Vernehmungen, bisherigen Verfahren etc.)

---

Q: Der Analyst, 08/2007,  
[http://www.rola.com/pdf/der\\_Analyst\\_August07.pdf](http://www.rola.com/pdf/der_Analyst_August07.pdf), 3.

## Gefahren (2)

### Studie des US-Forschungsinstituts MIT zur Auswertung von Telekommunikations-Verbindungsdaten

- Mit einer Trefferquote von 90% konnten Kollegen, Bekannte und Freunde aller Personen identifiziert werden
- Mit einer Trefferquote von 90% konnte vorhergesagt werden, ob sich 2 Personen in den nächsten Stunden treffen werden
- Die Daten gaben zuverlässig Auskunft über Schlafgewohnheiten und Zufriedenheit am Arbeitsplatz

---

Q: Massachusetts Institute of Technology, Relationship Inference, <http://reality.media.mit.edu/dyads.php>.

## Gefahren (3)

- Nach einer Studie des Europäischen Parlaments wird Telekommunikationsüberwachung auch in der EU zur Überwachung von Dissidenten, Menschenrechtsaktivisten, Journalisten, Studentenführern, Minderheiten, Gewerkschaftsführern und politischen Gegnern
- Amnesty International steht etwa unter der Überwachung des britischen Geheimdiensts GCHQ.

---

Q: Omega Foundation, Report (I).

## Gefahren (4)

- Zwar werden Kommunikations*inhalte* nicht aufgezeichnet, *Verbindungsdaten* können aber genauso oder noch verdächtiger sein:
- etwa belangloses Gespräch mit dem Nachbarn vs. Verbindung zu Liechtensteiner Bank oder Rechtsanwalt für Steuerstrafrecht

## Gefahren (5)

- Verbindungsdaten müssten nach der Cybercrime-Convention auch in andere Länder mit fragwürdigem Datenschutzniveau übermittelt werden.
- Darunter sind u.a. Albanien, Azerbaijan und Russland
- In den USA und GB ist es legal, Daten zur Wirtschaftsspionage im Ausland zu verwenden. Die Telekommunikationsdaten von Unternehmen bilden ihre geschäftliche Tätigkeiten sehr genau ab

---

Q: Moechel, Data-Retention, Überwachungsschnittstellen und der Tod, [http://www.quintessenz.at/harkank/Death\\_at\\_the\\_surveillance\\_interface/Tod\\_an\\_der\\_Ueberwachungsschnittstelle\\_intro.txt](http://www.quintessenz.at/harkank/Death_at_the_surveillance_interface/Tod_an_der_Ueberwachungsschnittstelle_intro.txt).

## Gefahren (6)

- Bürger, die befürchten, dass ihr Verhalten ständig vorsorglich protokolliert wird und dies gegen sie verwendet wird, werden sich möglichst unauffällig verhalten (vgl. Art. 5 GG, Art. 10 EMRK)
- Eine Demokratie lebt jedoch von einer aktiven und unbefangenen Mitwirkung und Debatte und furchtlosem Bürgerengagement.

---

Q: Limbach, Jutta: Ist die kollektive Sicherheit Feind der individuellen Freiheit? 10.05.2002,  
[www.zeit.de/reden/Deutsche%20Innenpolitik/200221\\_limbach\\_sicherheit.html](http://www.zeit.de/reden/Deutsche%20Innenpolitik/200221_limbach_sicherheit.html).

# Gefahren (7)

## Artikel 5 Grundgesetz (GG):

*„Jeder hat das Recht, seine Meinung in Wort, Schrift und Bild frei zu äußern und zu verbreiten und sich aus allgemein zugänglichen Quellen ungehindert zu unterrichten. Die Pressefreiheit und die Freiheit der Berichterstattung durch Rundfunk und Film werden gewährleistet. Eine Zensur findet nicht statt.“*

## Artikel 10 Europ. Menschenrechtskonvention (EMRK):

*„Jede Person hat das Recht auf freie Meinungsäußerung. Dieses Recht schließt die Meinungsfreiheit und die Freiheit ein, Informationen und Ideen ohne behördliche Eingriffe und ohne Rücksicht auf Staatsgrenzen zu empfangen und weiterzugeben.“*

## Gefahren (8)

- Informanten nehmen sicherheitshalber keinen Kontakt mehr zu (besonders regierungskritischen) Journalisten mehr auf, so dass sie nicht mehr recherchieren können und die Pressefreiheit eingeschränkt wird
- Ähnliche Hemmungen bestehen beim Kontaktieren von Rechtsanwälten, Beratungsstellen, Geistlichen, Ärzten oder Psychologen
- Telcos werden für staatliche Tätigkeit nicht entschädigt

Artikel 12 Grundgesetz (GG):

*„Alle Deutschen haben das Recht, Beruf, Arbeitsplatz und Ausbildungsstätte frei zu wählen.“*

## Gefahren (9)

Die Vorratsdatenspeicherung greift ständig und tief in die Privatsphäre aller Bürger ohne Gefahr oder Verdacht ein.

Artikel 8 Europ. Menschenrechtskonvention:

*„Jede Person hat das Recht auf Achtung ihres Privat- und Familienlebens, ihrer Wohnung und ihrer Korrespondenz. Eine Behörde darf in die Ausübung dieses Rechts nur eingreifen, soweit der Eingriff gesetzlich vorgesehen und in einer demokratischen Gesellschaft notwendig ist für die nationale oder öffentliche Sicherheit, für das wirtschaftliche Wohl des Landes, zur Aufrechterhaltung der Ordnung, zur Verhütung von Straftaten, zum Schutz der Gesundheit oder der Moral oder zum Schutz der Rechte und Freiheiten anderer.“*

# Gefahren (10)

## Weitere beeinträchtigte Grundrechte (Teil 1):

- Art. 1 I, 2 I GG: Informationelles Selbstbestimmungsrecht, der Bürger kann nicht mehr selbst über Speicherung entscheiden
- Art. 3 GG: Gleichbehandlung, etwa werden Telcos anders als Post behandelt
- Art. 4 GG: Religionsfreiheit, etwa bei vertraulichen E-Mails an den Pfarrer oder, sofern akzeptiert, Onlinebeichte
- Art. 5 GG: Meinungs- und Informationsfreiheit, etwa bei Internetrecherchen
- Art. 5 GG: Kunstfreiheit, etwa bei Onlineveröffentlichung von Bildern

# Gefahren (11)

## Weitere beeinträchtigte Grundrechte (Teil 2):

- Art. 5 GG: Forschungsfreiheit, etwa Recherchen für wissenschaftliche Publikation
- Art. 8 GG: Versammlungsfreiheit, etwa bei Online-Demonstrationen
- Art. 9 GG: Koalitionsfreiheit, etwa bei der Bildung politischer Onlinevereine
- Art. 10 GG: Fernmeldegeheimnis, Vertraulichkeit etwa durch Missbrauch gefährdet
- Art. 12 GG: Berufsfreiheit, etwa bei Teilnahme am E-Commerce, Onlineshopping

# Gefahren (12)

## Weitere beeinträchtigte Grundrechte (Teil 3):

- Art. 13 GG: Unverletzlichkeit der Wohnung, Internetsurfen findet meist in der eigenen Wohnung statt
- Art. 14 GG: Eigentumsfreiheit, etwa können Provider ihre alte Anlage nun nicht mehr verwenden
- Art. 17 GG: Petitionsfreiheit, etwa E-Mail-Beschwerden an Behörden
- Art. 20 III GG: Verhältnismäßigkeitsprinzip (=Geeignetheit, Erforderlichkeit und Zumutbarkeit)

## Gefahren (13)

Das Fernmeldegeheimnis (Art. 10 GG) wurde speziell deshalb geschaffen, weil durch die Distanz staatliche Eingriffe leicht möglich werden, ohne, dass sich der Bürger dagegen wehren kann. Die Vorratsdatenspeicherung widerspricht dem.

Immer größere (private) Lebensbereiche verlagern sich aber in den telekommunikativen Bereich und werden von der Vorratsdatenspeicherung erfasst: Telearbeit, Telemedizin, Telebanking, Telelernen, Teleshopping etc.

# Gefahren (14)

## „Der Staat wird es schon richten“

- Von allen Strafverfahren werden 72% ohne Anklage eingestellt
- Von den verbleibenden kommt es in 82% zur Verurteilung
- Demnach sind 77% aller Beschuldigten unschuldig
- Dennoch große Stigmatisierung, Verlust von Ehe oder Arbeitsplatz durch Ermittlungsverfahren (vgl. Ausschlussprinzip)
- Rechtlich Gefahr von Durchsuchungen, Beschlagnahme, U-Haft, Reiseverbot etc.
- Verbindungsdaten könnten Indiz sein, auf Grund dessen der Beschuldigte seine Unschuld beweisen muss (§ 261 StPO)

## Gefahren (15)

Nach einer repräsentativen Forsa-Umfrage 05/2008 würden wegen der Vorratsdatenspeicherung 52% der Bürger nicht mehr per Telefon, Mobiltelefon oder E-Mail Kontakt zu Eheberatung, Psychotherapeut [dadurch kann die Vorratsdatenspeicherung Leben gefährden, siehe folgend] oder einer Drogenberatungsstelle aufnehmen.

---

Q: [http://www.daten-speicherung.de/data/forsa\\_2008-06-03.pdf](http://www.daten-speicherung.de/data/forsa_2008-06-03.pdf).

# Gefahren (16)

## Studie der Weltgesundheitsorganisation über die Ursachen für den Verlust gesunder Lebenszeit (1):

- 92% Krankheiten
- 2% Verkehrsunfälle
- 2% Suizide
- 1% Stürze
- 0,2% Gewalt

Damit ist Gewalt (einschl. Terrorismus) statistisch genauso gefährlich wie Karies, Rückenschmerzen oder Durchfall.

# Gefahren (17)

## **Studie der Weltgesundheitsorganisation über die Ursachen für den Verlust gesunder Lebenszeit (2):**

Würde etwa nur der Tabakkonsum um 2% gesenkt, würde dies mehr Leben retten als die Verhinderung sämtlicher Gewaltstraftaten.

Terroristische Straftaten fordern weltweit etwa 20 Menschenleben (ohne Kriegsgebiete, aber einschl. WTC). Damit sterben jährlich an terroristischen Straftaten so viele Menschen, wie in Badewannen ertrinken oder von Meteoriten erschlagen werden.

# Gefahren (18)

## Kosten der Vorratsdatenspeicherung

- Provider werden zu Staatsdiensten gezwungen und nicht dafür entschädigt
- Alle Deutschen Telcos werden durch die Einführung der Vorratsdatenspeicherung mit ca. € 205 Mio. belastet, danach jährlich € 50 Mio. für Betrieb und Wartung. Dies gibt die Bundesregierung auch zu. AOL GB zahlt jährlich € 14 Mio. und speichert 292 TB, was 360.000 CD-ROMs entspricht
- Die Kosten für die Vorratsdatenspeicherung werden zwangsläufig auf den Kunden umgelegt

---

Q: Uhe/Herrmann, Überwachung im Internet (I), 124.

# Gefahren (19)

## Missbrauch der Vorratsdaten (1)

- Der VATM gibt zu, dass es wiederholt Fälle gab, in denen Telco-Mitarbeiter oder Hacker unbefugt Telekommunikationsdaten kriminell genutzt oder sogar verkauft haben (vgl. AOL)
- Der Bundesdatenschutzbeauftragte schätzt den Wert eines 6-monatigen Persönlichkeitsprofils durch Vorratsdaten auf € 100. Die Vorratsdaten haben folglich Milliardenwert
- Provider geben selbst zu, dass sie Missbrauch nie völlig ausschließen können.
- Insofern verhindert die Vorratsdatenspeicherung keine Straftaten, sondern schafft neue Anreize hierzu

---

Q: VATM: 15 Punkte zur TKG-Novelle, 17.12.2002,  
[www.vatm.de/images/dokumente/15\\_punkte\\_tkg.pdf](http://www.vatm.de/images/dokumente/15_punkte_tkg.pdf)

# Gefahren (20)

## Missbrauch der Vorratsdaten (2)

- Bei AOL USA verkaufte ein Mitarbeiter illegal 92 Mio. Kundendatensätze für \$ 150.000, und diese waren noch ohne Vorratsdaten
- Sind die Daten erst einmal da, kann ihre Nutzung beliebig erweitert werden. Nutzungszwecke können ausgeweitet werden
- Es haben schon Interesse angemeldet: Presse, Wirtschaftsauskunfteien, Banken, Versicherungen, Arbeitgeber, Inhaber gewerblicher Schutzrechte (Filmstudios etc.)

# Verfassungsbeschwerde AK Vorrat

## Stationen bisher:

- 31.12.2007: Einreichung der Verfassungsbeschwerde gegen die Vorratsdatenspeicherung mit Antrag auf einstweilige Aussetzung beim Bundesverfassungsgericht
- 11.03.2008: Bundesverfassungsgericht entspricht Antrag auf einstweilige Aussetzung teilweise, so dass Daten einstweilen weiter gespeichert werden, aber nur beim Verdacht schwerer Straftaten auf sie zugegriffen werden darf
- 01.09.2008: Verlängerung der einstweiligen Anordnung
- 13.08.2008: Weiterer Aussetzungsantrag
- Vgl. EuGH

# Gegenmaßnahmen

## Technisch:

- Datenvermeidung, Wahl datensparsamer Dienste
- Kostenloser SIM-Kartentausch ([www.daten-speicherung.de](http://www.daten-speicherung.de))
- Jondonym ([www.jondos.de](http://www.jondos.de))
- TOR

## Politisch:

- Mitarbeit in Parteien oder Bürgerrechtsgruppen, z.B. AK Vorrat ([www.vorratsdatenspeicherung.de](http://www.vorratsdatenspeicherung.de)). Demo in Berlin am 11.10.
- Berücksichtigung bei Wahl 