Ein Recht auf Anonymität?

Über Identifizierungszwang,
Bürgerrechte und Anonymität

Der Inhalt dieses Heftchens wurde einer Stellungnahme des Arbeitskreises Vorratsdatenspeicherung aus dem November 2009 entnommen.[1]

Darin hat der "AK Vorrat" auf Anfrage der Europäischen Kommission zu der Frage zur möglichen Einführung eines europäischen Identifizierungszwangs für Telekommunikationsnutzer Stellung bezogen.

1 http://www.dataretention2010.net/files/Replies_in_to_the_evaluation_questionnaire_of_September_2009/Fundamental_Rights_Advocacy/reply_arbeitskreis_vorratsdatenspeicherung_de.pdf

Seit 2004 dürfen **in Deutschland** Rufnummern für eingehende Verbindungen nur noch nach Erhebung von Name, Anschrift und Geburtsdatum vom Anschlussinhaber freigeschaltet werden.

Dies ist insbesondere für vorausbezahlte und kostenfreie Dienste von Bedeutung, namentlich für Prepaid-Handykarten. Der Anbieter ist zu einer Überprüfung der Angaben nicht verpflichtet. Die Angaben werden zusammen mit der zugewiesenen Rufnummer über 1.000 öffentlichen Stellen[2] in einem Onlineverfahren zum unmittelbaren Abruf zur Verfügung gestellt einschließlich einer Jokersuche nach beliebigen Kriterien. 2008 wurden auch E-Mail-Anbieter und deren Kundenverzeichnisse in das Verfahren aufgenommen. Seither sind die Kundendaten von 120 Anbietern zugänglich.[3] Die Zahl der Zugriffe steigt von Jahr zu Jahr rasant an. Inzwischen wird jährlich über 4 Mio. mal auf die Kundendaten zugegriffen - ohne Eingriffsschwelle und richterliche Kontrolle.[4]

Dieser Identifizierungszwang führt bei dem Normalbürger dazu, dass ihm eine **anonyme Telekommunikation erschwert** oder unmöglich gemacht wird. Dies hat zum Teil gravierende Folgen. Insbesondere ist darauf hinzuweisen, dass der einzige Umstand, der das Gewicht der Verkehrsdaten-speicherung mindert, die Möglichkeiten anonymer Kommunikation - etwa mithilfe vorausbezahlter Handykarten - sind.

---

2 Bundesnetzagentur, Jahresbericht 2008, http://www.bundesnetzagentur.de/media/archive/15901.pdf, 108.
3 Bundesnetzagentur, Jahresbericht 2008, http://www.bundesnetzagentur.de/media/archive/15901 .pdf, 108.
4 Bundesnetzagentur, Jahresbericht 2008, http://www.bundesnetzagentur.de/media/archive/15901.pdf, 108.

Diese ermöglichen es, trotz Verbindungsdatenspeicherung noch mehr oder weniger anonym zu kommunizieren. Würde auch diese von der Richtlinie zur Vorratsdatenspeicherung voraus gesetzte Möglichkeit beseitigt, würde dies die Auswirkungen der Totalprotokollierung nochmals gravierend verschärfen.

Die fehlende Anonymität der Fernkommunikation wegen der Vorhaltung von Vertragsdaten bei einem Mittelsmann **beeinträchtigt die Bereitschaft zur vertraulichen Kommunikation** auf elektronischem Wege, weil man gegebenenfalls Nachteile infolge der eigenen Verbindungen, Aussagen, Bewegungen oder Interessen befürchten muss. Der Erläuternde Bericht zur Empfehlung des Europarats zum Datenschutz in der Telekommunikation[5] führt in Abs. 5 aus, dass die technische Entwicklung „nicht nur die Privatsphäre von Teilnehmern und Nutzern allgemein gefährden kann, sondern auch deren Kommunikationsfreiheit behindern kann, weil sie das Maß an Anonymität mindert, der sich Teilnehmer und Nutzer unter Umständen bei der Benutzung des Telefons bedienen wollen, indem sie gezwungen werden, ihre Identitäten offenzulegen oder elektronische Spuren zu hinterlassen, die es ermöglichen, die Benutzung ihres Telefons zu überwachen."[6]

Dass das **Recht auf anonyme Meinungsäußerung** grundrechtlich geschützt ist, hat der US-amerikanische Oberste Gerichtshof (Supreme Court) schon früh anerkannt. Er hat in der Entscheidung Talley v. California[7] ausgesprochen, dass die „anonyme Meinungsäußerung" eine wertvolle Rolle für den „Fortschritt der Menschheit" gespielt habe.
Verfolgte Gruppen seien im Lauf der Geschichte nur im Schutz der Anonymität in der Lage gewesen, Unterdrückungspraktiken und -gesetze zu kritisieren.
Auch könne eine „Identifizierung und die Furcht vor

5 Empfehlung R (95) 4 vom 07.02.1995.
6 https://wcd.coe.int/ViewDoc.jsp id=529277&Site=CM&BackColorIntemet=9999CC&BackColorIntranet=FFBB55&-BackColorLogged=FFAC75.

Vergeltung von vollkommen friedlichen Diskussionen wichtiger öffentlicher Angelegenheiten abschrecken". Eine Pflicht zur Nennung der Verantwortlichen auf Flugzetteln hat der Gerichtshof daher als Verstoß gegen die Meinungsfreiheit verworfen.

In einer späteren Entscheidung[8] hat der Oberste Gerichtshof ausgeführt, Anonymität stelle oft ein „Schutzschild vor der Tyrannei der Mehrheit" dar. Nur im Schutz der Anonymität könne man seine Meinung äußern, ohne dass sie allein wegen der Person des Äußernden abgelehnt werde. Auf diese Weise helfe die Anonymität der Verbreitung von Ideen. Anonyme Meinungsäußerungen „exemplifizieren den Zweck des Grundrechtskatalogs und insbesondere der Meinungsfreiheit: unbeliebte Personen vor Vergeltung in einer intoleranten Gesellschaft zu schützen - und ihre Ideen vor Unterdrückung". Der Oberste Gerichtshof hat auch anerkannt, dass Vereine die Liste ihrer Mitglieder nicht offen legen müssen.[9] Es müsse möglich bleiben, anonym Mitglied eines unbeliebten Vereins zu sein, um die Freiheit auch unpopulärer Meinungen zu gewährleisten. Zuletzt haben die US-amerikanischen Instanzgerichte das Recht auf Anonymität auch auf das Internet angewandt.

Der Washington District Court entschied 2001[10] das Recht auf anonyme Meinungsäußerung sei von grundlegender Bedeutung für die Verabschiedung der US-amerikanischen Verfassung selbst gewesen, weil sowohl Befürworter („Federalist Papers") wie auch Widersacher ohne Namensnennung über die Ratifizierung der Verfassung stritten.

7 362 U.S. 60 (1960).
8 Mclntyre v. Ohio Elections Commission, 514 U.S. 334 (1995).
9 NAACP v. Alabama ex. rel. Patterson, 357 U.S. 449 (1958).
10 Doe v. 2TheMart.com, 140 F.Supp.2d 1088.

Das Gericht entschied wörtlich: „Das Internet begünstigt den reichhaltigen, vielfältigen und weitreichenden Austausch von Ideen. Die Möglichkeit, seine Meinung im Internet äußern zu können, ohne dass die andere Seite alle Tatsachen über die eigene Identität kennt, kann offene Kommunikation und robuste Debatte fördern."[11]

Auch **in Deutschland** haben sich die politische Opposition und der Widerstand gegen die Obrigkeit immer wieder der Anonymität bedienen müssen. Berühmte Schriftsteller wie Erich Kästner oder Kurt Tucholsky schrieben nicht unter ihrem eigenen Namen. 1849 veröffentlichte der Rechtswissenschaftler Theodor Mommsen einen Kommentar über die in der neuen Verfassung von 1848 garantierten „Grundrechte des deutschen Volkes" - anonym. Im gleichen Jahr veröffentlichte Adolph Streckfuß sein Werk „Das freie Preußen. Geschichte des Berliner Freiheitskampfes vom 18. März 1848 und seine Folgen", ohne seinen Namen zu nennen.

11 Doe v. 2TheMart.com, 140 F.Supp.2d 1088.

Die Möglichkeit, sich anonym informieren und kommunizieren zu können, ist für viele Menschen unverzichtbar:

- Menschen in besonderen Situationen (z.B. **Notlagen**, Krankheiten) sind nur in vollständiger Anonymität bereit, Informationen und Hilfe zu suchen, sich untereinander auszutauschen und sich beraten zu lassen (z.B. Chatrooms für Opfer sexuellen Missbrauchs).

- **Unternehmen** kommunizieren anonym, um Wirtschaftsspionage im Zusammenhang mit Vertragsverhandlungen zu verhindern, aber auch um sich selbst bei Wettbewerbern zu informieren, ohne ihre Identität preisgeben zu müssen.

- **Regierungsbehörden** (z.B. Nachrichtendienste) kommunizieren anonym, um im Internet recherchieren zu können, ohne als Regierungsbehörde identifizierbar zu sein. Zugleich sind sie darauf angewiesen, dass Menschen Straftaten anonym anzeigen können, die andernfalls nicht gemeldet würden und unaufgeklärt blieben. Dies gilt für die anonyme Offenlegung verschiedenster Missstände wie Steuerhinterziehung oder Korruption (sogenanntes „Whistleblowing").

- Nur anonyme Telekommunikation erlaubt es der **Bevölkerung autoritärer Staaten**, sich über politische Nachrichten zu informieren, die in ihrem eigenen Land durch Zensurmaßnahmen gesperrt sind.

- Deutsche **Journalisten**, die in autoritären Staaten arbeiten, sind auf anonyme Fernkommunikation angewiesen, um Informationen sicher empfangen und nach Deutschland übermitteln zu können, ohne dass der Aufenthaltsstaat dies zum Anlass für Maßnahmen gegen sie nehmen kann. Auch im Inland sind Informanten zunehmend nur noch im Schutz der Anonymität bereit, Auskunft zu geben. Im Wege anonymer Kommunikation gelingt es dann nicht selten, gravierende Missstände an das Licht der Öffentlichkeit zu bringen.

- Deutsche **Menschenrechtsgruppen** brauchen anonyme Kommunikationstechnik für ihre Arbeit mit autoritären ausländischen Staaten, sei es, um von diesen Staaten aus unerkannt mit ihrem Heimatbüro zu kommunizieren, sei es, um unerkannt mit oppositionellen Gruppen in den entsprechenden Staaten in Verbindung zu treten. Eine offene Kommunikation ist hier regelmäßig mit einem nicht zu verantwortenden Sicherheitsrisiko für die Beteiligten verbunden.

- **Regierangskritiker**, Blogger, Journalisten und Oppositionelle in autoritären ausländischen Staaten (z.B. Iran, Burma, Tibet), die sich für demokratische Reformen in ihrem Land einsetzen, können nur mithilfe anonymer Netze untereinander kommunizieren und die Öffentlichkeit auf die Situation in ihrem Land aufmerksam machen. Ohne den Schutz der Anonymität sind sie Verhaftungen, Gefängnisstrafen und Folter ausgesetzt; anonyme Fernkornmunikation schützt also Leben und Freiheit dieser Personen. Beispielsweise in Burma ist die demokratische Opposition auf die anonyme Kommunikation per Internet angewiesen.

Gary Marx nennt insgesamt **15 Funktionen von Anonymität in unserer Gesellschaft:**[12]

1. Erleichterung des Informations- und Kommunikationsflusses über **öffentliche Angelegenheiten** durch Schutz des Informationsgebers (z.B. Hotlines zur anonymen Anzeige von Problemen oder Verstößen durch Whistle Blower, anonyme Informanten der Presse).
2. Ermöglichung der **wissenschaftlichen Erforschung** von Sachverhalten, über die nur im Schutz der Anonymität Auskunft gegeben wird (z.B. Telefonstudien über Sexualverhalten, strafbares Verhalten, Gesundheit).
3. Zu verhindern, dass die Offenlegung des Urhebers einer Nachricht die **Wahrnehmung ihres Inhalts** verhindert oder beeinflusst (z.B. wegen Vorurteilen gegen den Autor).
4. Förderung des Meldens, Informierens, Kommunizierens, Austauschs und der Selbsthilfe im Hinblick auf Zustände oder Handlungen, die **stigmatisieren**, nachteilig sind oder intim (z.B. Hilfe für und Austausch der Betroffenen von Dro-genmissbrauch, Gewalt in der Familie, abweichender sexueller Identität, psychischer oder physischer Krankheiten, AIDS oder anderer Sexualkrankheiten, Schwangerschaft; Kauf von Verhütungsmitteln, Medikamenten oder bestimmten Magazinen).
5. Ermöglichung von **Hilfe** trotz Strafbarkeit oder gesellschaftlicher Verachtung (z.B. anonyme Beratung von Drogenabhängigen, anwaltliche Beratung von Beschuldigten).
6. Schutz der Unterstützer **unbeliebter Handlungen** vor Verpflichtungen, Forderungen, Vorverurteilung, Verwicklungen oder Rache (z.B. Schutz der Identität verdeckter Ermittler oder von Polizist/innen oder von Menschenrechtsorganisationen).

12 Marx, What's in a Name? Some Reflections on the Sociology of Anonymity (1999), http://web.mit.edu/gtmarx/www/anon.html.

7. Wahrnehmung **wirtschaftlicher Interessen** durch Einschaltung von Mittelsmännern/-frauen, um zu vermeiden, dass der Hintergrund einer geschäftlichen Transaktion bekannt wird (z.B. anonyme Testkäufe, anonyme Versteigerungen).

8. Schutz der eigenen Zeit, des eigenen Raums und der eigenen Person **vor unerwünschtem Eindringen** (z.B. durch Stalker, Fans oder Werbetreibende).

9. Dafür zu sorgen, dass **Entscheidungen** ohne Ansehung der Person getroffen werden (z.B. anonyme Bewerbung).

10. Schutz der eigenen Reputation und Ressourcen vor **Identitätsdiebstahl** (Handeln anderer unter dem eigenen Namen).

11. **Verfolgten Personen** die sichere Teilnahme am öffentlichen Leben ermöglichen (z.B. sich illegal aufhaltende Flüchtlinge).

12. Durchführung von **Ritualen**, Spielen und Feiern, welche das Verbergen der eigenen Identität oder das Annehmen einer fremden Identität zum Gegenstand haben und denen eine förderliche Wirkung auf die Persönlichkeitsentwicklung und psychische Gesundheit zugeschrieben wird (z.B. Rollenspiele).

13. Förderung des **Experimentierens** und Eingehens von Risiken ohne Furcht vor Konsequenzen, Scheitern oder Gesichtsverlust (z.B. Auftreten unter dem anderen Geschlecht in einem Chatroom).

14. Schutz der eigenen **Persönlichkeit**, weil die eigene Identität andere schlichtweg nichts angeht.

15. Erfüllung **traditioneller Erwartungen** (z.B. die traditionelle Möglichkeit, anonym Briefe schreiben zu können).

Ersetzt der Staat den **Grundsatz der Anonymität und Datensparsamkeit** durch einen Zwang zur Identifizierung und Datensammlung, hat dies dementsprechend gravierende Auswirkungen.

So verkaufte im Jahr 2006 ein Mitarbeiter des deutschen Mobilfunkunternehmens **T-Mobile** die Daten sämtlicher 17 Mio. Prepaid- und Postpaid-Kunden des Mobilfunkunternehmens. Die Daten umfassen den Namen, die Mobilfunknummer, die Anschrift, teils das Geburtsdatum und in einigen Fällen auch die E-Mail-Adresse. Die Daten werden in kriminellen Kreisen gehandelt. In den Daten finden sich nicht nur viele Prominente aus Kultur und Gesellschaft wie Hape Kerkeling, Günther Jauch und Til Schweiger, sondern auch eine erstaunliche Anzahl geheimer Nummern und Privatadressen von bekannten Politikern, Ministern, Ex-Bundespräsidenten, Wirtschaftsführern, Milliardären und Glaubensvertretern, für die eine Verbreitung ihrer Kontaktdaten in kriminellen Kreisen eine Bedrohung ihrer Sicherheit darstellt (etwa Charlotte Knobloch, Präsidentin des Zentralrats der Juden). Das Bundeskriminalamt musste nach dem Bekanntwerden eine Gefährdungsanalyse erstellen, um Betroffene schützen zu können.[13] Hätte T-Mobile nicht die Identität aller Kunden erhoben, wären weit weniger Personen gefährdet worden.

13 Spiegel, Diebe klauten 17 Millionen T-Mobile-Kundendatensätze (04.10.2008), http://www.spiegel.de/wirtschaft/0,1518,581938,00.html.

Der massiven Abschreckungswirkung sowie dem Risiko von Pannen und Missbrauch steht **kein nachweisbarer Nutzen** auf Seiten der staatlichen Ermittlungsbehörden gegenüber. Vielmehr berichten deren Vertreter, dass bei Ermittlungen im Bereich ernsthafter Kriminalität praktisch nie eine Handykarte auf den Nutzer registriert sei. Handykarten werden trotz Identifizierungspflicht mit Fantasiedaten angemeldet, von anderen Personen übernommen oder identifizierungsfrei außerhalb Deutschlands gekauft.

Eine Umfrage unter über 100.000 Internetnutzern im Jahr 2009[14] hat ergeben, dass jeder vierte Internet-Nutzer zum Schutz seiner Daten immer oder vorwiegend unter **Fantasienamen** im Netz unterwegs ist. Jeder fünfte Internetnutzer macht Fantasieangaben bei Online-Registrierungen. Fantasieangaben werden aus den folgenden Gründen gemacht:

- 66% wollen auf diese Weise die Zusendung **unerwünschter Werbung** verhindern.
- 62% wollen auf diese Weise einen **Verkauf ihrer Daten** verhindern.
- 58% wollen auf diese Weise ein Internetangebot **anonym nutzen.**
- 53% wollen sich dagegen wehren, dass **unangemessen viele Daten abgefragt** werden.
- 41% wollen im Internet **überall anonym** bleiben.

Wenngleich sich die Umfrage nicht auf **Telekommunikationsangebote** bezieht, ist zu vermuten, dass ebenso viele Menschen bei der Registrierung von Handy-SIM-Karten oder von E-Mail-Diensten Fantasieangaben machen wie bei der Registrierung von Internetdiensten.

14 http://www.w3b.org/nutzerverhalten/furcht-vor-datenmissbrauch-beeinflusst-nutzerverhalten.html.

Speziell zu Handy-SIM-Karten heißt es in einem Papier des **Bundeswirtschaftsministeriums** aus dem Jahr 2002:

> *„Derzeit werden Prepaid-Karten von Strqftätem **häufig unter Angabe falscher bzw. fiktiver Personalien** oder unter dem Namen der Vertriebspartner (Händler) erworben und registriert, oder es werden nicht existente Anschriften angegeben, l,..] Außerdem kommt es wegen der zum Teil falschen Angabe von Personalien unbeteiligter Dritter immer wieder zu [...] Ermittlungsmaßnahmen gegen Unschuldige. [...] Regelmäßig kommt es auch zu Schwierigkeiten bei der Telekommunikationsüberwachung (z.B. nach§ lOOa StPO), denn dort sind Anschlussinhaberfeststellungen von entscheidender Bedeutung. [...} Gegenwärtig sind lediglich in Frankreich die Anbieter von Prepaid-Karten verpflichtet, Kundendaten zu erheben. Es kommt vor, dass trotz Vorgaben von Regierungsseite völlig unzutreffende Angaben gemacht werden. In den anderen EU-Staaten, aus denen Informationen vorliegen, gibt es keine gesetzlichen Regelungen, die bei dem Verkauf von Prepaid-Karten zu beachten sind. [...] Etwa 50 % der Karten werde innerhalb eines Jahres verschenkt, größtenteils innerhalb der Familie."*[15]

15 BMWi-Ressortarbeitsgruppe, Eckpunkte zur Anpassung der Regelungen des § 90 TKG vom 28.03.2002, www.almeprom.de/fiff/material/Eckpunkte_90_TKG_Prepaid.pdf, 7.

Die in diesem Papier beschriebene Situation hat sich jedenfalls in den Kreisen, die für den Bereich ernsthafter Kriminalität von Interesse sind, durch die deutsche Identifizierungspflicht **nicht geändert.** Selbst die Bundesregierung schätzt, dass 10% der Bestandsdaten von Prepaidkunden gegenwärtig nicht korrekt sind.[16] Es ist nicht ersichtlich, dass die Identifizierungspflicht die Datenlage verbessert hätte. Erst recht nicht hat sie eine Erhöhung der Aufklärungsquote oder gar Senkung der Kriminalitätsrate bewirkt.

Ein Identifizierungszwang bewirkt im Ergebnis somit keine empirisch feststellbare, statistisch relevante Verbesserung der Strafverfolgung oder gar der Sicherheit. Berücksichtigt man demgegenüber die schweren Nachteile eines Identifizierungszwangs, so ergibt sich, **dass die Kommission keinesfalls die Einführung eines Identifizierungszwangs befürworten** oder gar vorschlagen darf. Dementsprechend sieht weder die Cybercrime-Konvention des Europarats noch die Richtlinie zur Vorratsdatenspeicherung einen Identifizierungszwang vor.

16 Bevollmächtigter der Bundesregierung, Schriftsatz vom 31.01.2007 an das Bundesverfassungsgericht, http://daten-speicherung.de/data/TKG-StN.pdf, 61.

Arbeitskreis Vorratsdatenspeicherung
www.vorratsdatenspeicherung.de