Vortragsstruktur Vorratsdatenspeicherung

- § 113a TKG lässt bei jeder Verbind. speichern: Rufnummer, Verbindungsanfang und -ende, IMSI (SIM-Nr.) beider Teilnehmer, IMEI (Handynr.) beider Teilnehmer, Funkzelle, deren Adr. und Abstrahlwinkel. Aktivierungszeit und -ort, bei VoIP IP beider Teilnehmer, bei SMS auch Zeit von Versand und Empfang. *E-Mail:* bei jedem Versand E-Mail-Adressen aller Beteiligten, Zeit, Absender-IP. Bei Abruf IP + Zeit. *Internet:* Anschlusskennung, IP.
- Speicherung ohne jeden Verdacht oder Gefahr, 6 Monate. Aber BVerfG v. 04.04.2006 zur Rasterfahndung: *„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.“*
- Bisher: Speicherung nur Abrechnung, IP unzulässig, in der Praxis meist wenige Tage. Danach keine Zuordnung möglich. Telefondaten bei Flatrate od zB Skype gar nicht, i.Ü. Löschung mit Rechnungsversand.
- Es werden Daten über das Kommunikationsverhalten der gesamten Bevölkerung gesammelt. 96% aller deutschen Haushalten haben irgendeinen Telefonanschluss = 132 Mio. Fest- u. Mobilanschlüsse.[1] 71% deutscher Haushalte haben einen Internetanschluss. Jährlich 106 Mrd. Telefonminuten. Durch die VDS werden jederzeit ca. 63 Mrd. Telefon- und SMS-Verbindungen gespeichert.
- Jährlich werden in D 220.000 Verkehrsdaten abgefragt; dabei sind durchschn. 130 Gesprächspartner betroffen, so dass jährl. Das Telekommunikationsverhalten von 28 Mio. Deutschen offen gelegt wird.
- Aufklärungsquote vor VDS bei mittels TK begangenen Straftaten: 55%[2]. Daten fehlten in < 0,01% der Verfahren. Davon lagen in der Mehrzahl der Fälle die Vorgänge so weit zurück, dass auch die VDS nichts nutzt (Überlastung der Justiz). Erforderlich nur 0,0004% der gespeicherten Daten.
- Verwendungen[3] für: Betrug (54%), Beleidigung (6%), Urheberstraftaten (4%). Nur 17% der Anfragen bringen verfahrensrelevante Ergebnisse.[4] Nicht Terrorismus.
- Kriminalitätsrate trotz größerer Maßnahmen konstant, obwohl die Aufklärungsrate steigt. Aufklärungsrate ist seit 1994 von 44% auf 53% gestiegen. In Japan gar keine TK-Überwachung und Kriminalitätsrate vergleichbar. Anonyme Prepaidkarten außerhalb EU erhältlich, bei WTC-Anschlag Schweizer SIM-Karten. In Deutschland werden > 50% der anonymen SIM-Karten binnen 1 Jahr verschenkt od verkauft.

---

[1] Eurostat, http://epp.eurostat.ec.europa.eu/portal/page?_pageid=2973,64549069,2973_64554066&-_dad=portal&_schema=PORTAL.
[2] BKA, Polizeil. Kriminalstatistik 2006, S. 65.
[3] Köbele (Deutsche Telekom), Vortrag am 27.08.2007, https://www.datenschutzzentrum.de/sommerakademie/2007/sak2007-koebele-wirtschaftsunternehmen-verlaengerter-arm-der-sicherheitsbehoerden.pdf, 9.
[4] Albrecht/Arnold/Demko/Braun, Rechtswirklichkeit und Effizienz der Telekommunikationsüberwachung, 455 ff.

- EDV erlaubt es technisch, diese sensiblen Daten wie Bewegungsprofile der ganzen Bevölkerung auszuwerten, nach best. Kriterien zu ordnen, zu vervielfältigen und mit anderen Datenquellen zu verknüpfen.
- Die Polizeien Bayern, Berlin, Rheinland-Pfalz, Mecklenburg-Vorpommern und Schleswig-Holstein verwenden die Software Rscase,[5] die solche Verknüpfungen mit anderen vorliegenden Daten vornehmen (Antiterrordatei, Vernehmung, bisherige Verfahren etc.).
- Studie des US-Forschungszentrums MIT zur Auswertung aller TK-Verbindungsdaten[6]: Es wurden mit Trefferquote von 90% Kollegen, Bekannte und Freunde aller Personen identifiziert. Mit Trefferquote von 95% konnte sogar vorhergesagt werden, wann sich die Person zu Hause und am Arbeitsplatz aufhalten würde. Zu 90% richtig konnte vorhergesagt werden, ob sich 2 Personen in den nächsten Stunden begegnen werden. Es konnten Schlafgewohnheiten und Zufriedenheit am Arbeitsplatz vorhergesagt werden.
- Nach einer Studie des europ. Parlaments[7] werden auch in westl. Staaten Aktivitäten von Dissidenten, Menschenrechtsaktivisten, Journalisten, Studentenführern, Minderheiten, Gewerkschaftsführern und politischen Gegenspielern mittels Verbindungsdaten überwacht, zB überwacht der brit. Geheimdienst GCHQ Amnesty International.
- Feststellung von Verhaltensmustern wäre selbst mit nur Inhaltsdaten oft nicht möglich (zB belangloses Gespräch mit Nachbar vs. Verbindungsdaten Herrn X zu Anwalt für Steuerstrafrecht oder Telefonat mit Liechtensteiner Bank, regelm. E-Mails von palästinensischen Menschenrechtsorganisation).
- Verbindungsdaten müssen nach Cybercrime-Konvention ins Ausland übermittelt werden, auch wenn dort kein Datenschutz existiert. Zielländer u.a. Albanien, Azerbaijan, Russland. USA und GB könnten Daten zur Wirtschaftsspionage im Ausland verwenden, was dort legal ist. Das TK-Verhalten einer Firma bildet deren geschäftl. Tätigkeit sehr genau ab.[8]
- Bürger können Meinung nicht mehr frei äußern (Meinungsäußerungsfreiheit, auch Art 10 EMRK), wenn alles vorsorglich protokolliert wird. Wer ständig damit rechnen muss, sein TK-Verhalten könnte künftig gegen ihn verwendet werden, wird sich möglichst unauffällig verhalten; eine Demokratie lebt jedoch von der aktiven und unbefangenen Mitwirkung, und furchtlosem Bürgerengagement.[9] In einem Klima der Überwachung kann ein freier und offener demokratischer Prozess nicht stattfinden.
- Art. 5 GG, Art. 10 EMRK
- Journalisten erhalten keinen Kontakt mehr zu Informanten und können nicht mehr recherchieren, insbes. staatskritisch wie Korruption. Ähnlich bei Raen, Geistlichen, Ärzten, Psychologen. Außerdem keine Etschädigung an Telcos. Art. 12.

---

[5] rola Security Solutions GmbH, der Analyst, August 2007, http://www.rola.com/pdf/der_Analyst_August07.pdf, 3.
[6] Massachusetts Institute of Technology, Relationship Inference, http://reality.media.mit.edu/dyads.php.
[7] Omega Foundation, Report (I).
[8] Moechel, Data-Retention, Überwachungsschnittstellen und der Tod, http://www.quintessenz.at/harkank/-Death_at_the_surveillance_interface/Tod_an_der_Ueberwachungsschnittstelle_intro.txt.
[9] Limbach, Jutta: Ist die kollektive Sicherheit Feind der individuellen Freiheit? 10.05.2002, www.zeit.de/reden/Deutsche%20Innenpolitik/200221_limbach_sicherheit. html.

- Art. 8 EMRK schützt Privatsphäre, denn die Speicherung personenbezogener Daten greift ins Privatleben ein[10]. Ggf. EGMR.
- Beeinrächtigte Grundrechte: Art. 1 I, 2 I informationelles Selbstbestimmungsrecht (=Jeder hat das Recht, selbst über die Preisgabe und Verwendung seiner Daten zu bestimmen. Datenschutz ist aber nicht Schutz von Daten, sondern Schutz des Persönlichkeitsrechts. Der Mensch kann seine Persönlichkeit nur entfalten, wenn er frei entscheiden kann, wer was über ihn weiß.)
- Art. 3 Gleichbehandlung (Telcos vs. Post, kleinere Telcos in Existenz bedroht), Art. 4 Religionsfreiheit (E-Mails an Pfarrer), Art. 5 Meinungsfreiheit (Informationsfreiheit), Art. 5 Kunstfreiheit (Kunstveröffentlichungen),
- Art. 5 Forschungsfreiheit (Recherchen für wissenschaftl. Veröffentlich.), Art. 8 Versammlungsfreiheit (Onlinedemo), Art. 9 Koalitionsfreiheit (polit. Online-Ortsvereine), Art. 10 Fernmeldegeheimnis (E-Mails, Chat), Art. 12 Berufsfreiheit (Onlineshopping Beratungsdienste wie Aids, Drogenberatung, Seelsorge, Stelle für Opfer sexuellen Missbrauchs werden weniger in Anspruch genommen),
- Art. 13 Unverletzlichk. d. Wohng. (wenn Telefonat aus privater Wohnung), Art. 14 Eigentumsfreiheit (Telcos können teils ihre Anlagen nicht mehr benutzen), Art. 17 Petitionsrecht (E-Mail-Beschwerden bei Behörden), Art. 20 III Verhältnismäßigkeitsprinzip: geeignet (funktionieren), erforderlich (keine gleich wirksame mildere Maßnahme), zumutbar (weniger Freiheitsverlust als Gewinn).
- Fernmeldegeheimnis (aufführen) wurde eingeführt, weil bei Verbindungen über Distanz die Teilnehmer den leicht zu bewerkstelligenden heimlichen staatlichen Eingriffen ausgeliefert sind.
- Immer mehr Verhalten verlagern sich in den Bereich der TK: Telearbeit, Telemedizin, Telebanking, Telelernen, Teleshopping, so dass ein immer größer werdender Teil des Privatlebens von der VDS erfasst wird.
- Staat irrt sich: Von 947.000 angeklagten Personen werden nur 771.000 verurteilt, also 82%. Gefahr der Stigmatisierung auch ohne falsche Verurteilung. Auch jedem erfolgreichen Rechtsmittel liegt ein Fehlurteil zu Grunde. Gefahr unrechtmäßiger Verfolgung. Immer öfter geht die Polizei nach dem Ausschlussprinzip vor; ein TK-Datensatz kann ein Indiz sein, so dass der Angekl. u.U. seine Unschuld beweisen muss (§ 261 StPO). Doch auch ohne falsche Verurteilung bei Ermittlungsverfahren Durchsuchung, U-Haft, Reiseverbot. In Nürnberg wurde ein Mann wegen seiner IP wegen des Abrufs illegaler Erotikseiten festgenommen, keiner glaubte seinem Leugnen; jemand hatte sein WLAN benutzt. Falscher Verdacht: Bei vermeintl. Filesharern oft IP-Adressen falsch eingegeben/aufgeschrieb. Teilweise Kinderpornoverdacht, Durchsuch: Job, Familie.
- Nach einer repräs. Forsa-Umfrage vom Mai 08:[11] 52% würden nicht mehr per Tel, Handy, E-Mail Kontakt aufnehmen zu Eheberatung, Psychotherapeuten (kann lebensgefährlich sein), Drogenberatung.
- Terror: Nach einer Studie der WHO ist die Gefahr, Opfer irgendeiner Gewaltstraftat zu werden, überhaupt gering. Der Verlust gesunder Lebenszeit beruht danach zu: 92%

---

[10] EGMR, Malone-GB (1984); EuGRZ 1985, 17 (23).
[11] http://www.daten-speicherung.de/data/forsa_2008-06-03.pdf.

Krankheit, 2% Verkehrsunfälle, 2% Suizid, 1% Stürze, 0,2% Gewalt. Damit ist Gewalt statistisch genauso gefährlich wie versehntliche Vergiftungen, Karies, Rückenschmerzen oder Durchfall.

- Würde etwa nur der Tabakkonsum um 2% gesenkt, würde das der Bevölkerung mehr dienen als die Verhinderung sämtlicher Gewaltstraftaten. Etwa könnte man Kinder davon abhalten zu rauchen. Todesopfer jährlich speziell durch Terrorismus: Jährl. ~20 weltweit ohne Kriegsgebiete, Deutschland 0 (7 Anschlägspläne, aber alle nicht ausgeführt oder opferlos). Damit sterben durch Terror genauso viele Menschen wie in Badewannen ertrinken oder von einem Meteoriten erschlagen werden.
- Art: 12: keine Entschädigung der Telcos; Einführung kostet die deutschen Telcos insges. € 205 und danach jährl. € 50 Betrieb + Wartung.[12] AOL GB zahlt für VDS jähr. € 14 Mio. bei 292 TB = 360.000 CD-Roms, die auf den Kunden umgelegt werden müssen.[13] BReg selbst gibt zu, dass pro ISP Kosten von mehreren € 100.000.[14]
- Es gab immer Fälle, in denen sich Telco-Mitarbeiter unbefugt Zugriff auf TK-Daten verschafft und diese für 6-stellige Beträge verkauft oder sonst zu kriminellen Zwecken missbraucht haben (VATM).[15] Dies künftig auch für VDS-Daten. Wenn selbst MS ständig Sicherheitslücken stopfen muss, dürfte es auch bei Telcos Hackeransätze geben. Je mehr Daten gespeichert sind, desto größer deren Wert und desto größer die Gefahr. Der BfDI schätzt den Wert eines TK-Persönlichkeitsprofils der letzten 6 Monate pro Kunde auf € 100, die VDS-Daten haben folglich Milliardenwert. Provider sagen selbst, dass sie Missbrauch nicht sicher ausschließen können.[16]
- In den USA verkaufte ein AOL-Mitarbeiter illegal 92 Mio. Kundendatensätze (ohne VDS-Daten) für $ 150.000. Wegen der Schaffung dieses Anreizes dient die VDS nicht der Bekämpfung von Straftaten, sondern schafft Anreiz dazu. Nutzungszweck kann jederzeit erweitert werden. Interesse haben viele angemeldet: Presse, Wirtschaftsauskunfteien, Banken, Versicherungen, Arbeitgeber.[17]
- Richtlinie 2006/24/EG und Verfahrensablauf: 31.12.07 Einreichung Beschwerde und Antrag auf einstweil. Anordnung der Aussetzung. 11.03.2008 BVerfG entspricht einstweil. Anordn. teilweise (Speicherung, aber Zugang begrenzt). 01.09.2008 Verlängerung. Derzeit Antrag Aussetzung Internet. Gesetz überschießend auch Nutzung zur Gefahrenabwehr und Nachrichtendienste (Bundesnachrichtendienst, Bundesamt für Verfassungsschutz, Militärischer Abschrimdienst, Verfassungsschutzbehörden der Länder), Anonymisierungsdienste (sinnlos, da Ausland zB Tor), Bestandsdatenerhebung bei Prepaidkarten. RiL nur Speicherung zur Verfolgung schwerer Straftaten. Überschießend auch IP bei E-Mail-Verkehr.
- Klage Irlands: Unzuständigkeit, da Rahmenbeschluss (Rat einstimm.) statt Richtlinie (Parlament), Entscheidung wohl nächstes Jahr.

---

[12] Eco, Verband der dt. Internetwirtschaft auf http://www.heise.de/newsticker/meldung/96162.
[13] Uhe/Herrmann, Überwachung im Internet (I), 124.
[14] BReg in: BT-Drs. 16/5846, 34.
[15] VATM: 15 Punkte zur TKG-Novelle, 17.12.2002, www.vatm.de/images/dokumente/15_punkte_tkg.pdf
[16] EuroISPA, Internet Service Providers' Association (Europe): Position on the Impact of Data Retention Laws on the Fight against Cybercrime, 30.09.2002, www.euroispa.org/docs/020930eurousispa_dretent.pdf, 2.
[17] Gridl, Datenschutz in globalen Telekommunikationssystemen, 39 und 61.