1. Die Vorratsdatenspeicherung

Under Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR), everyone has the right to respect for his private life and his correspondence. Public authorities may interfere with the exercise of that right only in accordance with the law... – *EU-Richtline 2006/24/EC, 15.3.2006*

- Urgeschichte
- Die EU-Richtline
- It's becoming law
- Telefonie

- Internet
- Zugriffsrechte
- Szenarien
- Was tun?

2. Urgeschichte

Bevor jemand eine kriminelle Handlung begehen kann, muss der Computer einen Alarm geben, so dass die Sicherheitskräfte diese kriminelle Handlung verhindern können. Das ist nur möglich durch lückenlose Aufklärung der persönlichen Lebensverhältnisse. [...] Ich habe mich zu keiner Zeit gegenüber den Mitgliedern des Bonner Krisenstabes mit den zitierten Sätzen und mit dem behaupteten Inhalt geäußert. Auch habe ich weder jemals eine „komplette Überwachung des Telefonverkehrs" geplant oder gefordert noch wurde eine „Telefonverbindungsdatenbank" aufgebaut
– *Horst Herold in einer Gegendarstellung zu einer DLF-Sendung vom 12.5.2007*

- 1977 – der „Deutsche Herbst" bringt den großen Auftritt für die EDV bei Polizei und Diensten.
- 1980er – vor allem die Bewegung gegen die Volkszählung führt zur Etablierung eines Datenschutzrechts und verzögert den effizienten Einsatz der EDV bei der Polizei.
- Ende 1980er – die Post digitalisiert das Telefonnetz („ISDN") und schafft so die Grundlage für eine breite Erfassung von Verbindungsdaten.
- Anfang 2000er – im Zeichen des „Terrors" wird der Druck der „Sicherheitslobby" für eine umfassende Speicherung von Verbindungsdaten immer stärker, doch bleiben die Widerstände groß.

3. Die EU-Richtline

Dieser Mechanismus - über die EU durchsetzen, was national nicht durchsetzbar ist - funktioniert noch heute. Und folgendes kommt noch hinzu: Was einmal auf „europäischer" Ebene – also von nationalen Regierungen über den Umweg Europa – durchgesetzt wurde, wirkt als vermeintlicher Sachzwang zurück auf die nationale Ebene.
– Dirk Eckert, Philtrat Nr. 28, 1999

Gegen 2002 Beratungen auf EU-Ebene – bemerkenswerterweise auf Initiative der rechtsradikalen dänischen Regierung; zunächst absurde Bestimmungen (alle „Verbindungen" auch im Netz, auch vergebliche Verbindungsversuche). Heftige Lobbytätigkeit der Telekoms.

Intensivierung ab 2004 im Kielwasser der Anschläge von Madrid. Entwurf wird von fr, ie, se und uk getragen. Nun auch präventive Verwendung zugelassen. Schließlich Kommissionsentwurf in erster Säule. Eigentlich gehört Repression in die dritte Säule der EU, am Schluss wurde die Richtline in die erste gesteckt, weil sie auf diese Weise einfacher durchzusetzen ist (weniger Vetomöglichkeiten für bürgerrechtsbegeisterte MinisterInnen): Europäische Regelung ist nötig, damit Telekoms in Staaten ohne Vorratsdatenspeicherung keinen Vorteil gegenüber anderen haben.

Kommissionsentwurf 14.12.2005 EU-Parlament, 21.12.2006 EU-Rat gegen Stimmen von Irland und Slowakei. ie klagt derzeit gegen den Entwurf, weil er in die dritte Säule soll – ie hofft wohl, auf diese Weise Verschärfungen durchsetzen zu können. Das EU-Parlament hat sich disqualifiziert, nachdem sein Berichterstatter, Alexander Alvaro, zwischendurch aus den Verhandlungen der Kommission ausgebootet worden war.

Regelungen: Geforderte Daten weitgehend identisch mit deutscher Umsetzung; Speicherfrist nach Wahl 6 bis 24 Monate, Möglichkeit, Umsetzung im IP-Bereich bis März 2009 zu verzögern (was fast alle Staaten tun).

Nett auch: No later than 15 September 2010, the Commission shall submit to the European Parliament and the Council an evaluation of the application of this Directive and its impact on economic operators and consumers [...] with a view to determining whether it is necessary to amend the provisions of this Directive, in particular with regard to the list of data in Article 5 and the periods of retention provided for in Article 6.

4. Der Gesetzentwurf

Der Deutsche Bundestag bekräftigt seine [...] Ablehnung einer Mindestspeicherungsfrist für Verkehrsdaten und fordert [...] die Bundesregierung auf, einen etwaigen Beschluss in den Gremien der Europäischen Union, der eine solche Verpflichtung für Unternehmen in Deutschland vorsähe, nicht mitzutragen. – Bundestagsdrucksache 15/4597, 2004

Der Bundestag hat zwar mehrfach Vorratsdatenspeicherung abgelehnt, hat dann aber 2/2006 doch die Umsetzung der EU-Richtlinie gefordert.

Ergebnis: Änderungen an StPO, TKG und 12 anderen Gesetzen, die komplette verdeckte Ermittlung wird neu geregelt und dabei in der Regel verschärft. Als Reaktion auf das Urteil zum großen Lauschangriff stehen aber immerhin auch ein paar nette Sachen drin, etwa erweiterte Berichtspflichten (FWIW).

Zentraler Begriff: Verkehrsdaten – „technische Informationen, die bei der Nutzung eines Telekommunikationsdienstes (Telefonie, Internetnutzung) beim jeweiligen Telekommunikationsunternehmen (Provider) anfallen und von diesem erhoben, gespeichert, verarbeitet, übermittelt oder genutzt werden." Das ist offensichtlich erheblich mehr als nur die Daten, wer mit wem gesprochen hat. Die Definition wurde vor allem erweitert, um auch Standortdaten zu erfassen.

Der Gesetzentwurf wurde am 9.11.2007 abgenickt.

5. Telefonie

Erfasst werden für Gespräche, SMS etc. (§ 113a TKG)

- Kennung der verbundenen Anschlüsse und ggf. weiterer beteiligter Anschlüsse
- Anfang und Ende der Verbindung
- Genutzter Dienst (z.B. Fax bei ISDN)
- IMEI und IMSI der beteiligten Geräte
- Funkzellen bei Beginn der Verbindung
- Bei Prepaid weiter die Zeit und Ort der ersten Aktivierung
- Bei IP-Telefonie die beteiligten IP-Adressen

∩ Für die meisten TK-Unternehmen ist da nicht viel Neues dabei, weil sie die meisten dieser Daten für die meisten KundInnen ohnehin schon 6 Monate zu Abrechnungszwecken aufgehoben haben. Mühsam dürfte die IMEI werden, die in den meisten Netzen bisher nicht abgefragt wurde, sowie wohl die Funkzelle, zumal das Gesetz die Provider verpflichtet, die Funkzellen so zu dokumentieren, dass eine möglichst präzise Lokalisation möglich ist. Das dürfte wohl nochmal umfangreiche Nachmessungen erfordern.

Insbesondere die Speicherung der Funkzelle ist natürlich wüst – hier wird die rückwirkende Er-
∪ fassung von Bewegungsprofilen möglich.

6. Internet

Erfasst werden:

- Beim Versenden von Mail die sendende Adresse, die einlieferende IP und die Adressen der EmpfängerInnen.
- Beim Empfangen von Mail die empfangende Adresse, die einliefernde IP und die Adresse des/der AbsenderIn.
- Beim Lesen von Mail die Adresse des Postfachs und die IP, von der aus gelesen wird.
- Am Anfang und Ende einer Bereitstellung eines Zugangs: IP und eindeutige Benutzerkennung.
- Zu allem die Zeiten der Vorgänge.

∩ Hier stellen sich viele Fragen, so etwa, was Mail wohl sei (ähnlich übrigens bei IP-Telefonie).

Die für Mails zu speichernden Daten wurden bisher auch schon geloggt, mussten aber eigentlich
∪ schnell gelöscht werden. Gleiches gilt für die Erfassung der Zugangsdaten.

7. Zugriffsrechte

In aller Regel verwenden die Gerichte nur formelhafte Begründungen und kopieren häufig die fehlerhaften Anträge der Staatsanwaltschaft in ihre Anträge.
– Ulla Jelpke bei der ersten Lesung, 11.7.07

Der Zugriff auf die Verkehrsdaten ist in § 100g StPO geregelt – möglich bei einer Straftat „von auch im Einzelfall erheblicher Bedeutung“ oder einer „mittels Telekommunikation“ begangenen Straftat, in Echtzeit nur im ersten Fall.

Zugriff erfolgt auf auf Antrag der Staatsanwaltschaft auf gerichtliche Anordnung, aber wie immer „Gefahr im Verzug“ (aber dann rückwirkende Bestätigung durch Gericht).

Es reicht die Angabe einer Kennung oder im Zweifel auch nur eine „räumlich und zeitlich hinreichend bestimmte Bezeichnung“ zur Abfrage.

In Wirklichkeit sind diese Regelungen weitgehend für die Füße, jedenfalls, solange die Gerichte zumal in politischen Geschichten Überwachungsbefugnisse mit dem Gummistempel ausstellen und selbst in Fällen, in denen die Polizei unter Berufung auf „Gefahr im Verzug“ illegal Daten abfragt, die Zuständigen keinerlei Schwierigkeiten bekommen. Nichts deutet darauf hin, dass mit dem neuen Gesetz die Obrigkeit auch ein neues Bürgerrechtsbewusstsein eingeblasen bekommen wird.

Entscheidend ist allerdings vorläufig, dass die Polizei vorläufig nur Zugriff auf einen verschwindenden Bruchteil der vorhandenen Daten hat. Die große Katastrophe wird kommen, wenn nach dem übernächsten Großanschlag im Westen die komplette Datensammlung an die Polizei bzw. die Dienste geht – dem Herold'schen Sozioskop steht dann nichts mehr im Weg.

8. Szenarien

Verabredungen zu Verbrechen und Terror setzen Kommunikation voraus. Ganz klar: Man muss miteinander reden. *– Jürgen Gehb (CDU/CSU) bei der ersten Lesung, 11.7.07*

1. Ein Antifa aus Ostwestfalen ruft auf seiner (gewitzt anonym im Ausland eingerichteten) Webseite dazu auf, „die Nazis in Bielefeld zu stoppen“. Das ist sicher Aufruf zu Straftaten, und auch wenn es im Einzelfall vielleicht nicht schwer wiegt, die Straftat ist eindeutig mittels Telekommunikation erfolgt. Die Verkehrsdaten zu einer auf der Webseite angegebenen Mailadresse (unvorsichtigerweise bei gmx.de und somit unter deutscher Jurisdiktion stehend) gehören also schon der Polizei (da ein Altfall vorliegt, gibt es noch keine „richtige“ Adresse zum Mail-Account). Dabei ergeben sich 20 IP-Adressen, von denen aus Mails angefordert wurden. Diese lässt man von den Providern zurückverfolgen. Vier waren Internet-Cafes, die anderen laufen bei einem Rechner zusammen. Auf zur fröhlichen Beschlagnahme.“
2. Der besagte Antifa ist ja gewitzt (das mit gmx.de war der einzige Fehler) und hat deshalb ziemlich viel Krempel verschlüsselt, so dass kein zusätzliches Beweismaterial auf der inzwischen beschlagnahmten Maschine zu finden ist. Vor allem die Herkunft der toll martialischen Grafik auf der Webseite bleibt im Dunkeln, und das ist auch gut so, denn damit lässt sich nochmal ein Verfahren wegen Verwendung verfassungsfeindlicher Symbole machen, und wieder wurde die Straftat mittels Telekommunikation begangen. Dieses Mal bestellt die Polizei die Mailkontakte des Antifas der letzten Zeit, insbesondere rund um den Zeitpunkt, zu dem Grafik ins Netz kam. Die anfallenden Mailadressen werden durch schnelle Anfragen zu Identitäten aufgelöst und diese dann gegen die in der BKA-Verbunddatei Innere Sicherheit vermerkten Antifas abgeglichen. Übrig bleiben drei Leute, deren Elektronik nun auch beschlagnahmt werden kann.
3. Eine Atomkraftgegnerin aus dem bayrischen Schwaben wird bei einem Abendspaziergang in der Nähe das AKW Gundremmingen mit einem feststellbaren Messer aufgegriffen. Sie gibt an, sie habe nur Bärlauch sammeln wollen, aber da das angesichts der von ihr vermuteten

radioaktiven Belastung der Pflanzen unglaubwürdig ist, muss eine terroristische Organisation dahinterstecken (soweit ist das noch keine reine Fiktion). Um diese auszuforschen, sieht man nach, wann die Betreffende laut Verkehrdaten so in der Nähe das AKW telefoniert hat. Es liegen für die letzten sechs Monate fünf solche Daten vor. Nun fragt man, wer in den betreffenden Zeiten *noch* aus dieser Funkzelle telefoniert hat („räumlich und zeitlich hinreichend bestimmt"). Dies sind 1500 Menschen. Nach einem Abgleich mit Mail-Verbindungsdaten der Verdächtigen bleiben nur noch drei übrig, mit denen die Verdächtige offenbar im Hinblick auf das AKW enger zu tun hat (gerade so genug für eine glaubhafte Terrorzelle). Eine schnelle Abfrage in NADIS ergibt, dass einer davon im AKW selbst arbeitet. Jetzt muss alles schnell gehen. Schön, dass das Sondereinsatzkommando auch mal den Pressesprecher des AKW Gundremmingen verhaftet...

4. Ein Asylbewerber aus Kurdistan, von den Behörden nach Northeim gesteckt, sympathisiert laut Auskunft türkischer Geheimdienste mit der PKK. Mithin haben wir einen Fall nach § 129b und gucken mal zur Sicherheit in Echtzeit, wo der Junge so rumläuft. Ah, er geht nach Osten. Noch ein Stück, und noch eins, und da ist doch die Kreisgrenze? Tatsache. Er verletzt die Residenzpflicht. Einfangen, abschieben, fertig. Hätte ja sein Cellphone auch abschalten können.

5. In Hamburg fällt eine Erwerbslose auf, weil sie eine Demo anmeldet und die Anmeldegebühr von 200 Euro ohne sichtbare Regung auf den Tisch legt. Wenn da mal kein Missbrauch staatlicher Leistungen vorliegt. Der Richter zögert zwar ein wenig, unterschreibt dann aber doch die Anforderung für Verbindungsdaten, denn die Erschleichung der großzügigen Sozialleistungen unseres Staates wiegt in jedem Einzelfall schwer. Als erstes kommt heraus, dass die Dame bis zu fünf Stunden am Tag telefoniert, nie jedoch werktags von 17.30 Uhr bis 20 Uhr. Leider hat sie kein Mobiltelefon, so dass nicht ganz klar ist, wo sie in dieser Zeit so ist. Aber immerhin: am 30.4. hat sie doch mal in der fraglichen Zeit telefoniert. Davor hatte sie an dem Tag 11 Telefongespräche. 10 davon sind nicht vielversprechend (weil, so ergibt ein schneller Abgleich, mit anderen armen Leuten oder Internet-Einwahlpunkten geführt), aber eines mit der kleinen Bürogemeinschaft stadtbekannt linker Anwälte könnte doch ein Hinweis sein. Schicken wir doch mal morgen um 17.30 jemanden da vor die Tür. Wollen doch mal sehen, ob die Erwerbslose da einer nicht angemeldeten Tätigkeit nachgeht...

9. Was tun?

Die Debatte um die informationelle Selbstbestimmung stammt aus der Zeit der Volkszählung vor zwanzig Jahren. Heute würde doch jeder zugeben, dass die Befürchtungen von damals hysterische Übertreibungen waren. – *Wolfgang Schäuble im Stern 17/2007*

Entscheidend: Politisch Widerstand leisten.

Im Telefoniebereich: Sehen, wie weit Cellphones verzichtbar sind (Lokalisation!). Evtl. ausländische Calling Cards.

Im IP-Bereich: Mailaccounts auf Nicht-EU-Rechnern oder Rechnern, die nicht der Vorratsdatenspeicherung unterliegen (z.B. eigene Mailserver unterhalten). Evtl. über Tor nachdenken.

http://www.vorratsdatenspeicherung.de