Gier und schlechtes Gewissen

Die Vorratsdatenspeicherung ist auf der Zielgeraden

> Wer regelmäßig den ARD-Tatort verfolgt, wird es gemerkt haben: Die Polizei will dringend auch im Nachhinein nachvollziehen können, wer alles wie kommuniziert hat. In fast jeder Folge kommen zentrale Ergebnisse (und natürlich spannende Rätsel) aus den letzten Nummern in Mobiltelefonen, kryptischen Nachrichten auf Anrufbeantwortern oder auch mal einer Mail. Noch bewegen sich Professor Boerne und Co damit in einer rechtlichen Grauzone (was das Internet angeht) oder haben auch mal Pech (wenn Telefon-Abrechnungsdaten schon gelöscht sind). Doch spätestens zum 15.9.2007 hat es damit ein Ende.

So sehr allerdings die ZuschauerInnen der ARD mit dem sympathischen Assistenten fiebern, wenn dieser versucht, geschickt an die erwünschten Daten zu kommen, so wenig begeistert sind sie trotz aller Politik der Angst, wenn plötzlich ihr eigenes Kommunikations- und Bewegungsverhalten bis in Details unter Umständen jahrelang nachvollziehbar bleibt. Das wussten auch die diversen Regierungen von Kohl bis Merkel (ein paar polternde Extremisten wie Schily oder Schäuble vielleicht ausgenommen), und so näherten sie sich dem Objekt der Begierde mit dem Umweg über Brüssel.

Während nämlich der Bundestag in braver Sorge um die Bürgerrechte -- und natürlich auf eifrige Lobbyarbeit der Telekoms hin -- die Pflichtspeicherung der „Verkehrsdaten“ (dazu unten mehr) 2005 zwei Mal praktisch einstimmig ablehnte („fordert [...], einen etwaigen Beschluss in den Gremien der Europäischen Union, der eine solche Verpflichtung für Unternehmen in Deutschland vorsähe, nicht mitzutragen.“), haben die Berliner Exekutiven in Brüssel und Straßburg eine Richtline vorangetrieben, die genau dieses große Überwachungsprojekt mandatiert.

Der erste Entwurf dieser Richtlinie zeugte vor allem von atemberaubender Inkompetenz bezüglich der Funktionsweise des Internets, sah er doch vor, Verkehrsdaten seien für *alle* Verbindungen zu erheben. Das ist schon deshalb Quatsch, weil der Begriff der Verbindung in einem paketvermittelten Netz wie dem Internet jedenfalls schwierig ist; aber auch mit ausreichender Klärung der Begrifflichkeit wäre das bei den Telekoms anfallende (und dann auf deren Kosten zu speichernde) Datenvolumen gigantisch gewesen. Diese waren daher, leider noch vor MenschenrechtlerInnen und Antirepressionsgruppen, die schärfsten Kritiker der Vorlage und haben das Ding schließlich auf etwas zusammengestutzt, womit sie werden leben können. Sie, aber nun wirklich nicht die Menschenrechte.

Die am Schluss allseits abgenickte Richtlinie verlangt von den Mitgliedstaaten, bis zum 15.9.2007 ihre Telekoms zu verpflichten, für sechs bis 24 Monate zu speichern:

- für jedes Festnetzgespräch die beteiligten Telefonnummern, die Anfangszeit und die Dauer des Gesprächs.
- für Mobiltelefongespräche und SMS zusätzlich IMSI (die Nummer, die die SIM-Karte identifiziert) und IMEI (eine Nummer, die das Gerät identifiziert) sowie die Funkzellen, in denen die beteiligten Geräte am Anfang der Verbindung waren.
- für Verbindungen zu Internet Service Providern (ISPs), also den Unternehmen, die Zugang zum Internet vermitteln, wann wer unter welcher Kennung (der IP-Adresse oder kurz IP) im Netz war.
- für E-Mail und Internet-Telefonie die Benutzerkennungen und IP-Adressen der Beteiligten.

Dabei müssen alle Kennungen jeweils auf „richtige“ Personen zurückführbar sein -- das bedeutet unter anderem das faktische Ende quasi-anonymer Accounts bei Webmailern und dergleichen innerhalb der EU.

Für die Vorratsdatenspeicherung im Netz erlaubt die Richtline den Mitgliedsstaaten, ihre Umsetzung nach Meldung (die fast alle Staaten gemacht haben) erst zum 15.9.2009 umzusetzen, vielleicht in der Ahnung, dass dafür teilweise komplett neue Infrastruktur geschaffen werden muss, vielleicht auch, weil die Telekoms, die das vermutlich reingelobbyt haben, hoffen, dass der Käse bis dahin aus Bürgerrechtserwägungen heraus abgeschossen wird.

Besonders putzig an der Richtlinie ist, dass sie sich nicht etwa auf die „dritte Säule“ der EU stützt (polizeiliche und justizielle Zusammenarbeit), sondern auf die „erste Säule“, also die wirtschaftliche Zusammenarbeit. Grund dafür ist offenbar, dass die Datenschutzrichtlinie für elektronische Kommunikation die Löschung oder wenigstens Anonymisierung der fraglichen Daten vorsieht und so in klarem Gegensatz zu den Plänen steht. Da aber die Regierungen dennoch Vorratsdatenspeicherung haben wollen, muss diese auch trotz Verbot EU-weit geregelt werden, da sonst der Wettbewerb der Telekoms untereinander behindert wäre. So oder ähnlich dürfte die verquere Argumentation gehen, aber so genau weiß das niemand, denn die Kommission hat die Herausgabe einschlägiger Dokumente unter Hinweis auf ein von Irland und der Slowakei vor dem Europäischen Gerichtshof angestrengtes Verfahren verweigert (nebenbei: die beiden klagenden Regierungen haben nicht etwa Menschenrechtsbedenken, nein, sie wollen lieber schärfere Regelungen haben, die sie in der ersten Säule nicht für durchsetzbar halten).

ReferentInnen entwerfen

Angesichts doch spürbarer Widerstände, beschränkter technischer Kenntnisse und wohl auch einer guten Portion schlechten Gewissens hat sich das Zypries-Ministerium schwer getan, ein Gesetz zur Umsetzung der Richtlinie zu basteln, und bis zur Abfassung dieses Artikels (April 2007) liegt nur ein Referentenentwurf vor, der noch nicht im Parlament angekommen ist. Er soll und muss aber noch vor der Sommerpause durchgewunken werden, wenn es mit dem Inkrafttreten Mitte September etwas werden soll, und mithin dürfte er schon in den Ausschüssen zirkulieren, wenn dieses Heft gedruckt ist.

Zum Ausgleich für den knappen Zeitplan hat das Ministerium aber auch gleich den großen Wurf vorgelegt. Auf 211 Seiten wird der Versuch unternommen, eine komplette Neuregelung verdeckter Überwachungsmaßnahmen mit Patches zu 13 Gesetzen vorzunehmen und, immerhin *eine* gute Nachricht, erste Schritte zu einer geschlechtsneutralen Formulierung der Strafprozessordnung zu tun. Buy 1, get 13 free, das hilft, blöden Nachfragen auch blöde Antworten entgegensetzen zu können („Was wollen Sie eigentlich, es gibt jetzt doch viel mehr Rechtssicherheit...“).

Auch wenn die Begründung dies nicht explizit formuliert, enthält der Gesetzestext das Eingeständnis, dass in dem Bereich in den letzten Jahren Wildwuchs herrschte -- so wurde die „konventionelle“ Telefonüberwachung bisher für drei Monate angeordnet und konnte beliebig um jeweils drei Monate verlängert werden, während das neue Gesetz eine Anordnung für zwei Monate bei Verlängerung um jeweils einen Monat vorsieht und nach sechs Monaten das nächsthöhere Gericht prüfen muss. Nicht nennenswert nachgebessert wurden hingegen die Regelungen zur Benachrichtigung der Opfer der Überwachungsmaßnahmen. Auch künftig können die Behörden auf allerlei Gründe verweisen, warum eine solche Benachrichtigung gerade im vorliegenden Fall unterbleiben darf und muss, und so wird weiterhin nur in Ausnahmefällen mal rauskommen, wo gelauscht wurde.

In Richtung Legislative sieht der Entwurf hingegen umfangreiche Berichtspflichten vor, wo bisher in Eigeninitiative einzelner Abgeordneter nur quasi prekär eine gewisse Transparenz in die polizeiliche Überwachungspraxis kam. Außerdem werden die Anlasstatbestände in §100a StPO-- also das, was Verdächtigen angehängt werden muss, um vom Gericht die Anordnung zu bekommen -- neu organisiert und dabei de facto ausgeweitet. Natürlich bleibt der Gummiparagraph 129a im Katalog, in politischen Verfahren wird also auch weiter munter abgehört werden.

Der Entwurf legalisiert gleich noch IMSI-Catcher (mit denen SIM-Karten in laufenden Telefonen geortet werden können) und die Erweiterung auf IMEI-Catcher (die die Geräte selbst orten), enthält neue Regelungen für über Fotos hinausgehende verdeckte Überwachung (darunter hat man sich z.B. Ortung durch

GPS vorzustellen), die Durchsuchung von Speicherplatz, der nicht im Anwesen der Beschuldigten liegt (etwa Webmail-Sachen, Webspace oder virtuelle Platten im Netz) und einige Teufeleien dieser Art mehr.

Der eigentliche Knaller ist aber die Neufassung des §100g StPO, der für „Straftat[en] von auch im Einzelfall erheblicher Bedeutung“ (hier wird also der Katalog aus §100a wieder ausgehebelt) oder die „mittels Telekommunikation begangen“ wurden vorsieht (und das auch bisher schon tat), *Verkehrsdaten* (gegenüber bisher: Verbindungsdaten) zur „Erforschung des Sachverhalts oder [...] Ermittlung des Aufenthaltsorts des Beschuldigten“ einzusetzen. „Verkehrsdaten“ sind dabei „Daten, die bei der Erbringung eines Telekommunikationsdienstes erhoben, verarbeitet oder genutzt werden“. Gegenüber den alten Verbindungsdaten kann dabei also noch eine Ecke mehr zusammenkommen, vor allem, wenn es um Mobiltelefone geht -- die Gerätekennung IMEI beispielsweise wurde bisher gar nicht erfasst, weil sie für Verbindungen überhaupt keine Rolle spielt, und auch Standortdaten aus Funkzellen sind definitiv keine Verbindungsdaten. In Echtzeit immerhin dürfen Standortdaten nur für Katalogstraftaten nach §100a abgezogen werden -- alle anderen aber unter den Bedingungen für im Nachhinein bestellte Verkehrsdaten, also im Groben immer.

Deutlich gelockert wurden ebenfalls die Bedingungen, die an die Definition der Zielpersonen geknüpft werden. So müssen nicht mehr wie bisher Name und Telefonnummer des Opfers der Maßnahme genannt werden. Stattdessen reicht jetzt nur noch die Telefonnummer oder die Nummer des Endgeräts, im Zweifelsfall auch nur eine „räumlich und zeitlich hinreichend bestimmte Bezeichnung der Telekommunikation“.

Letzteres muss man sich auf der Zunge zergehen lassen. Die Polizei kann beim nächsten Castortransport *legal* (ggf. unter Hinweis auf §129a) Standortdaten der Masten rund um die Strecke abgreifen -- nach den Erfahrungen mit den Einschränkungen des Demonstrationsrechts ist von den zuständigen RichterInnen kein Widerspruch zu erwarten. Da weiter die gerätespezifischen IMEIs mit abgefragt werden, hilft jetzt auch die Verwendung einer alternativen SIM-Karte nichts mehr: Solange euer Mobiltelefon an ist, weiß die Polizei, wer ihr seid und wo ihr seid. Da auch hier Berichtspflichten vorgesehen sind, werden wir hoffentlich erfahren, ob sowas schon im ersten Jahr läuft oder ob die Polizei noch etwas braucht, bis sie mit dieser Sorte Daten umgehen kann.

Wo Unrecht zu Recht wird...

Der Katalog der zu speichernden Daten wird nach dem Entwurf in §110a des Telekommunikationsgesetzes stehen. Was die Telefonie angeht, gibt es keine Überraschungen. Die in der EU-Richtline empfohlene Speicherung *aller* Funkzellen, die während eines Telefonats berührt wurden, hat die Regierung nicht ins Gesetz geschrieben, damit die Telefonieanbieter nicht viel mehr speichern müssen als bisher. Da diese bereits jetzt für die meisten KundInnen zu Abrechnungszwecken einen Großteil der verlangten Daten speichern, und zwar, so die KundInnen nichts explizit Löschung nach Rechnungsversand bestellt haben, auch für ein halbes Jahr, müssen sie lediglich zusätzlich die IMEIs abfragen und in ihren Datenbanken halten. Sonst ändert sich, abgesehen von der wegen der gesenkten Anordnungsschwelle wohl größeren Frequenz der Anfragen, erstmal wenig. Nur Flatrate-Anbieter, die bisher diese Daten schnell hätten löschen müssen, müssen eventuell umdenken.

Drastischer kommt es für Anbieter von E-Maildiensten. Zwar stehen die meisten der Daten, die sich die Regierung gönnt, bereits in irgendwelchen Logs, aber mit denen wurde bisher typischerweise eher hemdsärmelig umgegangen -- irgendein Programm sorgte dafür, dass sie nach einer Weile gelöscht wurden, ansonsten war die Hoffnung, dass keineE DatenschützerIn so genau hinsehen würde, denn natürlich lebten diese Logs in einer rechtlich sehr grauen Zone. Aus dieser heraus wandeln sie sich nun in zu hätschelndes Staatseigentum. Immerhin: Um diesen Quatsch ist leicht herumzukommen, denn das Gesetz schreibt vor, dass „Anbieter von Diensten der elektronischen Post“ die Speicherung zu übernehmen hätten (im Gegensatz zu den ISPs, die durch Mithören des Datenverkehrs in der Regel auch solche Daten produzieren könnten). Sitzt euer Anbieter im (Nicht-EU-) Ausland, gibt es keine Speicherung (nach diesem Gesetz -- was die entsprechenden Läden sonst noch mit den Daten anfangen, steht natürlich auf einem anderen Blatt).

Die ISPs schließlich müssen jetzt speichern, wer wann welche IP-Adresse hat. Dies war für die in dem Bereich typischen Flatrates erst 2005 gerichtlich klar verboten worden, da ja keine Abrechungszwecke verfolgt

werden können. Dieser harte Schlag für die Musikindustrie und auch für dauerbeleidigte Firmen, die sich in Internetforen verleumdet sehen, wird jetzt ins Gegenteil verkehrt: Unrecht wird wieder mal zu Recht, und was dann zur Pflicht wird, muss LeserInnen dieser Zeitschrift nicht erklärt werden.

Trotz 211 Seiten Referentenentwurf ist bei all dem jedenfalls im Internetbereich doch keine Normenklarheit vorhanden -- *was* ist eigentlich E-Mail oder Internet-Telefonie? Fallen Instant Messaging-Programme nach Art von jabber (oder, im Reich des Bösen, ICQ und Co) unter Mail und so unter die Vorratsdatenspeicherung? Sind die Sprachfetzen, die sich SpielerInnen bei üblichen Ballerspielen durchs Netz zurufen („Camper!“) Internet-Telefonie? Ist das Abrufen von E-Mail durch POP oder IMAP (über diese Protokolle kommen die Mails von gmx, web.de, gmail und Co auf euren Rechner, wenn ihr nicht Webmail macht) speicherpflichtig? Wer immer das Gesetz geschrieben hat, ahnte wohl wenig von solchen Fragen.

Die Träume

Um zu verstehen, was aus Sicht der GesetzesmacherInnen so toll an dieser Geschichte ist, einmal ein paar (fiktionale) Szenarien, wie moderne Repression so aussehen wird.

(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.

(1a) 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.

(2) 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...

(3) 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.

(4) In Hamburg fällt eine Erwerbslose auf, weil sie eine Demo anmeldet und die Anmeldegebühr von 200 Eu-

ro 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...

(5) bis (2000) bleiben eurer Fantasie überlassen. Schöne Geschichten nehmen wir gerne unter der Mailadresse unten entgegen und veröffentlichen sie auf unserem Wiki. Entscheidend ist: nach der Verabschiedung von irgendwas, das die EU-Richtlinie umsetzt, sind all diese Geschichten jederzeit möglich (tatsächlich ginge ein guter Teil schon jetzt -- nach der Abwehr dieses Entwurfs bleibt also durchaus noch Arbeit zu tun). Und in nicht weiter Ferne werden, da gehen wir jede Wette ein, die Daten insgesamt zur „Auswertung“ herangezogen werden. Das Ergebnis davon: Ein Sozioskop, mit dem mal richtig nett zu arbeiten sein wird. Passende Interessen vorausgesetzt.

Weitere Informationen und Vorschläge für den Widerstand gegen die Vorratsdatenspeicherung finden sich auf der Webseite des AK Vorratsdatenspeicherung, http://www.vorratsdatenspeicherung.de.

Erratum: In der RHZ 1/2007 hatten wir bereits im Teaser behauptet, am 1.12.2006 sei das Terrorismusbekämpfungsergänzungsgesetz „verlängert“ worden. Dabei ist leider der Reiz des Bürokratendeutschen mit uns durchgegangen, denn wir hätten uns entweder für „Terrorismusbekämpfungsergänzungsgesetz verabschiedet“ oder für „Terrorismungsbekämpfungsgesetz verlängert“ (und dann besser auch noch gleich „verschärft“) entscheiden sollen.

Datenschutzgruppe der Roten Hilfe Heidelberg

datenschutzgruppe@rotehilfe.de

PGP Fingerprint: a3d8 4454 2e04 6860 0a38 a35e d1ea ecce f2bd 132a

http://www.datenschmutz.de