Humanistische Union

Telekommunikationsdaten – ein begehrtes Gut

Studie des Max-Planck-Instituts Freiburg stellt Notwendigkeit der Vorratsdatenspeicherung in Frage und warnt vor dem Überwachungspotential der Verkehrsdaten.

Mitteilungen Nr. 200, Seite 10 - 12

Am 9. November 2007 verabschiedete der Bundestag das Gesetz zur Einführung der Vorratsdatenspeicherung in Deutschland. Keiner der Abgeordneten konnte zum damaligen Zeitpunkt die bisherige Praxis der Abfrage sogenannter Telekommunikations-Verkehrsdaten seriös einschätzen. Es lagen weder wissenschaftlich gesicherte Informationen noch Statistiken dazu vor, welche Rolle die Daten für eine effektive Strafverfolgung spielen, wie die Auskunftsersuchen in der Praxis umgesetzt würden oder ob eine sechsmonatige Speicherfrist der Daten wirklich unerlässlich sei. Einen Bericht zur bisherigen Praxis der Verkehrsdatenabfrage, der genau auf diese Fragen eingehen sollte, hatte der Bundestag bereits drei Jahre zuvor angefordert. Als eine Woche vor der Abstimmung bekannt wurde, dass eine Studie des Max-Planck-Instituts für ausländisches und internationales Strafrecht bereits erstellt war, verweigerte das Bundesjustizministerium (BMJ) ihre Veröffentlichung jedoch mit dem Hinweis, es gebe noch redaktionellen Änderungsbedarf. So musste das Gesetz zur Vorratsdatenspeicherung im Blindflug verabschiedet werden. Im März diesen Jahres veröffentlichte das BMJ die Studie - die Gelegenheit für eine erste Lektüre.

Die Verkehrsdatenabfrage – das neue Standardinstrument verdeckter Ermittlungen

Die Studie zur „*Rechtswirklichkeit der Auskunftserteilung über Telekommunikationsverbindungsdaten nach § § 100g, 100h StPO...*" (Albrecht et al. 2008) bezieht ihre empirische Basis aus drei Quellen: Einerseits führten die Forscher Experteninterviews mit Vertretern der Polizei, der Staatsanwaltschaften und Richtern, aber auch mit Strafverteidigern, Datenschutzbeauftragten und Mitarbeitern der Telekommunikationsfirmen. Darüber hinaus werteten die Autoren insgesamt 467 Verfahrensakten (der Jahre 2003 und 2004) sowie Daten von verschiedenen Telekommunikations-Providern aus. In den 467 Akten fanden sich 1.257 Beschlüsse zur Verkehrsdatenabfrage, die insgesamt 1.909 Telekommunikationsanschlüsse (mit großer Mehrheit Mobilfunkanschlüsse) betrafen. Insbesondere die Analyse dieser Ermittlungs- und Verfahrensakten zeichnet ein interessantes Bild von der Realität der Verkehrsdatenabfrage, das die an einigen Stellen verzerrten Einschätzungen der Beteiligten zu korrigieren vermag. Aus der umfangreichen Untersuchung seien hier nur einige bürgerrechtlich bedeutsame Highlights angeführt:

• **Die Abfrage von Verkehrsdaten trifft meistens Unschuldige**: Wie viele Personen jeweils von einer Abfrage der Verkehrsdaten betroffen waren, ließ sich den Akten nicht entnehmen. Aufhorchen lässt aber die Tatsache, dass nur in 30% der Fälle die Beschuldigten auch die Inhaber der abgefragten Anschlüsse waren – in 60% der Fälle gehörte der überwachte Anschluss Dritten, die selbst nicht beschuldigt wurden. (S. 276ff)

• **Die richterliche Prüfung der Anträge zur Verkehrsdatenabfrage bleibt weitgehend wirkungslos**: In einem Vergleich zwischen den polizeilichen Anregungen, den Anträgen der Staatsanwaltschaften und den richterlichen Beschlüssen zeigen die Autoren, dass nur 25% der richterlichen Beschlüsse auf eine substantielle Prüfung der Anträge schließen lassen (S. 196). Mehrheitlich finden sich in den richterlichen Beschlüssen pauschale Verweise auf die gesetzlichen Voraussetzungen, formelhafte Entscheidungen, Verweise auf die Begründung der staatsanwaltschaftlichen Anträge oder gar fertige Formulare, die den Richtern zur Beschlussfassung vorgelegt wurden und die sie nur noch unterzeichnen mussten. Dazu passend

erklärte lediglich einer der zehn befragten (Ermittlungs-)Richter (S. 215), dass er die Begründung für die richterlichen Beschlüsse zur Verkehrsdatenabfrage selbst formuliere. Die mangelnden richterlichen Kontrollmöglichkeiten spiegeln sich auch im Zeitaufwand wider, den die Richter für die Genehmigung eines Antrags angeben: „*Teilweise wurde ausgeführt, dass die Bearbeitung nur ein paar Minuten dauere, da meist kaum Erkenntnisse vorliegen.*" (S. 216)

• **Die Verkehrsdatenabfrage funktionierte auch ohne Vorratsdatenspeicherung besser, als ihr nachgesagt wurde**: In den Interviews berichteten die Staatsanwälte von zahlreichen Problemen in der Kooperation mit den TK-Anbietern. Nach ihren Angaben (S. 250) würden die Dienstleister häufig oder gelegentlich Anfragen zu spät beantworten (50%), würden Abfragebeschlüsse nicht akzeptieren (33%) oder hätten die notwendigen Daten zu kurz (49%) oder überhaupt nicht (31%) gespeichert. Die Auswertung der Akten ergab jedoch ein gänzlich anderes Bild: Lediglich bei 27 von 1.257 Beschlüssen weigerten sich die Anbieter, die geforderten Verkehrsdaten herauszugeben. Darunter waren 11 Fälle, in denen die Provider nach einer Eilanordnung zunächst einen richterlichen Beschluss einforderten, um die Daten zu übermitteln sowie 8 Fälle, in denen die Provider aufgrund offensichtlicher Fehler in den Beschlüssen die Datenübermittlung verweigerten (z.B. falsche oder unvollständige Rufnummern, Anbieter nicht als Verpflichteter aufgeführt, keine oder nicht die aktuelle Rechtslage benannt). „*Zu sonstigen Verzögerungen ohne explizite, den Akten zu entnehmende Weigerung der Anbieter, kam es in 32 Fällen. In acht Fällen beruhte dies darauf, dass der Beschluss fehlerhaft war, wobei vor allem eine falsche Ruf- oder IMEI-Nummer die Fehlerhaftigkeit begründete (fünf). Daneben gab es einen Fall, in dem kein Abfragezeitraum genannt wurde und zwei Fälle, in denen der Beschluss nicht eindeutig war.*" (S. 252)
Auch in Bezug auf die Ergebnisse der Datenabfrage bestand nach der Aktenlage wenig Grund zur Klage. Bei 1909 abgefragten TK-Anschlüssen gab es nur 42 Fälle, bei denen die angefragten Daten bereits gelöscht waren bzw. 12 Fälle (z.B. bei Prepaid-Mobiltarifen), bei denen überhaupt nicht gespeichert wurde.

• **Die Benachrichtigung der Betroffenen über die Datenerhebung ist die seltene Ausnahme**: Bei insgesamt 1.257 Beschlüssen zur Verbindungsdatenabfrage fanden sich in der Mehrzahl der Fälle (1.105) keinerlei Hinweise darauf, ob die Betroffenen nachträglich informiert wurden oder nicht. Lediglich in 40 Fällen wurden Betroffene ausdrücklich benachrichtigt, bei weiteren 53 Fällen erhielten die Betroffenen durch andere Umstände (etwa während einer Befragung im Ermittlungsverfahren) Kenntnis von der Verkehrsdatenabfrage. Für ganze 33 dokumentierte Fälle einer ausrücklichen Nicht-Benachrichtigung wurde mehrheitlich die Gefährdung des Untersuchungszweckes, fünf Mal die nicht einschlägige Geheimhaltungspflicht für nicht-öffentliche Nachrichten (§ 89 Telekommunikationsgesetz) sowie einmal der Schutz einer V-Person als Begründung genannt. (s.S. 280)

In Bezug auf die quantitative Ausbreitung der Verkehrsdatenabfrage kann die Untersuchung wenig Neues vermelden. Da es bisher keine Statistiken über Verkehrsdatenabfragen gab, können die empirischen Grundlagen der Studie nur einen Ausschnitt beschreiben. Vor dem Hintergrund ihrer eigenen Untersuchung und der Forschungsliteratur schätzen die Autoren, dass es im Jahre 2005 in Deutschland ca. 41.000 Verkehrsdatenabfragen gab (S. 90). Wie rasant sich diese Nutzung von Kommunikationsdaten in den letzten Jahren entwickelt hat, zeigt ein Vergleich mit neueren Daten der Deutschen Telekom. Der Konzern rechnete 2007 allein für seinen Bereich mit 25.500 Abfragen im Telefonbereich und 210.000 Abfragen im Internetbereich.

Telekommunikationsdaten inhaltsreicher als bisher angenommen?

Es sind aber nicht nur solche Zahlen, sondern auch die systematischen in der Praxis zutage tretenden Mängel, die nach einer strikten Begrenzung dieser massenhaften Kommunikationsüberwachung verlangen. In Ihrer Studie gehen die Freiburger Forscher der Frage nach, welche Aussagekraft den Kommunikationsdaten zukommt. Wenn Telefonate abgehört oder E-Mails mitgelesen werden ist unbestritten, dass dies einen Eingriff in die Privatsphäre der überwachten Personen bedeutet. Umstritten ist

jedoch, wie jener Eingriff in die grundrechtlich geschützte Vertraulichkeit der Kommunikation zu bewerten ist, der sich aus der Einsichtnahme in Verkehrsdaten ergibt. Oder anders gefragt: Was können Ermittlungsbehörden und Geheimdienste schon erkennen, wenn sie meine Kommunikationsdaten auswerten? Welche Informationen sind in den „äußeren Umständen der Kommunikation" enthalten, welche Aufschlüsse geben diese möglicherweise über die Inhalte meines Austauschs, über mein Verhalten und meine Beziehungen zu anderen?

Gemeinhin wird in der Erhebung von Verkehrsdaten im Verhältnis zu den Inhalten der Kommunikation, wie sie eine Überwachung nach § 100a Strafprozessordnung offenlegt, ein geringfügigerer Eingriff in die Privatsphäre der Betroffenen gesehen. Auf den ersten Blick ist dies auch verständlich: Allein aus der Erkenntnis, wann, wie und wo zwei Menschen miteinander kommunizierten, kann man nicht schlussfolgern, dass sie sich dabei zu einer Straftat verabredet haben. Aus der Sicht der Ermittlungsbehörden bieten die Verkehrsdaten gegenüber dem gesprochenen oder geschriebenen Wort allerdings einen Vorteil: Sie lassen sich automatisiert auswerten und verarbeiten, mit ihnen können ganze Kommunikationsnetze ermittelt werden.

Die Freiburger Studie zitiert zwei neuere Forschungsansätze, die sich dieses Themas annehmen und die einige Hinweise darauf geben, dass die Abstufung der Grundrechtssensitivität zwischen Kommunikationsinhalten und Kommunikationsumständen neu zu überdenken ist. Beim ersten handelt es sich um ein Forschungsprojekt am Massachusetts Institute of Technology (MIT). Dort wertete die *Human Dynamics Group* unter Leitung von *Nathan Eagle* die Kommunikationsdaten von 95 Testpersonen über mehrere Monate aus. Als Datenbasis nutzten die Forscher vor allem Verkehrsdaten der Mobiltelefone, zur Erfassung der direkten Kontakte und Nahkommunikationen kamen auch Bluetooth-Empfänger zum Einsatz. Aus den Daten versuchten die Forscher, persönliche Beziehungen zwischen den TeilnehmerInnen sowie deren Berufszufriedenheit vorauszusagen. Die Ergebnisse der Datenanalyse wurden mit einer Befragung der Probanden verglichen. Das überraschende Ergebnis dieses Vergleichs: Die Beziehungen zwischen den Mitgliedern der Testgruppe und die Zufriedenheit der Teilnehmenden ließen sich mit den Verkehrsdaten besser (mit einer Wahrscheinlichkeit von 95%) vorhersagen als mit den Ergebnissen der direkten Befragung.

Die zweite Untersuchung von *George Danezis* und *Bettina Wittneben* von der Erasmus-Universität Rotterdam widmet sich vor allem der effektiven Überwachung eines Kommunikationsnetzwerkes. Ihre Untersuchung geht von der Überlegung aus, dass die Vertraulichkeit elektronischer Kommunikation nicht nur auf der Absicherung des Übertragungsweges beruht. Die meisten technischen Systeme zur Absicherung elektronischer Kommunikation, die etwa die Integrität von Absender und Empfänger (durch Authentifizierung), den Weg der Nachrichtenübertragung (durch Anonymisierung) und deren Inhalte (durch Verschlüsselung) schützen wollen, übersehen dabei, dass sich solche Kommunikationen innerhalb sozialer Netzwerke abspielen, in dem sich Spuren einer Kommunikation an verschiedensten Stellen wiederfinden. „*In most cases Alice and Bob would be embedded in a social network, and their identities and conversations would not only leak information about themselves but also about other actors in the network.*" Eine Überwachung von Alice und Bob (den klassischen Personenbeispielen von Kommunikationstechnikern) könne deshalb auch außerhalb von deren Kommunikationswegen stattfinden.

Danezis und Wittneben untersuchten deshalb, wie viele Beteiligte eines größeren Kommunikationsnetzes überwacht werden müssten, um alle bzw. die meisten Kommunikationen innerhalb des Netzwerkes kontrollieren zu können, wie eine effiziente Auswahl der überwachten Personen erfolgen sollte und wie stark eine Anonymisierung des Netzwerkes dessen Überwachung behindere. Als Datenbasis nutzten sie das Archiv einer politisch ausgerichteten Mailingliste mit 2.338 Teilnehmern verteilt auf 373 Orte. Ihr erstes Ergebnis: Sämtliche Kommunikation auf der Mailingliste ließ sich mit einer Überwachung von 8% ihrer Teilnehmer kontrollieren.

Nun stellt eine solche Mailingliste natürlich ein besonderes Kommunikationsnetzwerk dar. Die Forscher untersuchten nur Kommunikationen, die über diese Liste vermittelt wurden – der möglicherweise privat nebenher laufende Austausch wurde nicht erfasst. Allerdings präsentiert die Untersuchung einen Ansatz, wie aus einer probeweisen Überwachung einzelner Teilnehmer der Mailingliste sukzessive Informationen über

das Netzwerk und die Auswahl besser geeigneter Personen zur Überwachung gewonnen werden könne, bis das gesamte Netzwerk offen liege. Die Kommunikation aller Beteiligten ließe sich deshalb nur schützen, wenn das gesamte Netzwerk anonymisiert arbeite, da andernfalls immer Ansatzpunkte für eine Ausforschung bestünden. Genau hierin besteht nach Danezis und Wittneben auch die Gefahr der europaweiten Vorratsdatenspeicherung: „*Similarly, the debate about traffic data retention can be illuminated by our findings. The availability of such data makes the job of target selection trivial allowing the selection of a handful of targets that are exactly within the 8% of the people that would provide most information, allowing the optimal invasion of everyone elses privacy*."

Fazit

Mit Bezug auf derartige Untersuchungen kommen Albrecht et al. (S.88) zu der Frage, ob die Auswertung von Verkehrsdaten konventionelle Ermittlungsmethoden wie die Befragung von Zeugen und Verdächtigen verdrängen könnte. Eine solche Entwicklung dürfte vor allem dadurch befördert werden, dass die Abfrage und Auswertung der Kommunikationsdaten unter ökonomischen Gesichtspunkten wesentlich effizienter, weil mit geringem Personaleinsatz verbunden ist. Vor dieser Form der Effizienz muss jedoch gewarnt werden: Selbst die beste prognostische Methode liefert am Ende nur Indizien, aber keinen kausalen Beweis für eine Straftat. Jenseits der reinen, mittels Kommunikationseinrichtungen begangenen Vergehen sind Verkehrsdaten meist nur Spuren der Täter, und nicht Spuren der Tat.

Mit Blick auf das deutsche Umsetzungsgesetz zur Vorratsdatenspeicherung wird ein weiteres Manko im Umgang mit den Verkehrsdaten deutlich: Es ist eben nicht nur die Frage der Erhebung und Speicherung solcher Daten, die einen Eingriff in die Privatsphäre der Betroffenen ausmacht. Darüber entscheidet am Ende auch, welche Methoden des Data-Mining, der Gewinnung neuer Informationen aus den kumulierten Kommunikationsdaten, eingesetzt werden. In dieser Hinsicht gibt der Gesetzgeber bisher keine Grenzen vor: Sofern Sicherheitsbehörden die Daten erst einmal abgefragt haben, dürfen sie in jeder nur erdenklichen Form ausgewertet werden.

Sven Lüders
ist Geschäftsführer der Humanistischen Union e.V.

Hintergrund:

Hans-Jörg Albrecht, Adina Grafe und Michael Kilchling: Rechtswirklichkeit der Auskunftserteilung über Telekommunikationsverbindungsdaten nach § § 100g, 100h StPO. Forschungsbericht im Auftrag des Bundesministeriums der Justiz. Forschungsgruppe Kriminologie des Max-Planck-Institut für ausländisches und internationales Strafrecht. Freiburg,
Februar 2008. 499 Seiten. Online: http://www.bmj.de/files/ 3dfc9ae120ef598aa31e13850a22f470/3045/MPI-GA-2008-02-13%20Endfassung.pdf

Nathan Eagle, Alex Pentland & David Lazer (2007): Inferring Social Network Structure using Mobile Phone Data. Science Report. Online:
http://www.socialsciences.cornell.edu/0508/sciencereport_formatted_10.12.pdf
Ausführliche Informationen zur Arbeit der Human Dynamics Group am MIT unter:
http://reality.media.mit.edu/

George Danezis und Bettina Wittneben (2006): The Economics of Mass Surveillance and the Questionable Value of Anonymous Communications. K.U. Leuven, ESAT/COSIC, RSM Erasmus University, Rotterdam. Online: http://weis2006.econinfosec.org/docs/36.pdf

---

ein-begehrtes-gut/
Abgerufen am: 05.02.2023