

Die Vorratsdatenspeicherung - Berufsgeheimnis nicht mehr geheim!

von Noëmi Löllgen

(12.2007) Die Kommunikation von Ärzten, Anwälten, Psychotherapeuten und Journalisten über das Telefon, Handy und Internet wird künftig legal staatlich überwacht. Dies ist Teil der sehr kontroversen Debatte, die das „Gesetz zur Neuregelung der Telekommunikationsüberwachung“ nicht erst seit seiner Verabschiedung am 9.November 2007 ausgelöst hat.

Gesetzes-Novelle zur Telekommunikationsüberwachung

Das Gesetz ermöglicht zum 1. Januar 2008 die sechsmonatige Speicherung aller Kundendaten durch die Telekommunikationsgesellschaften, die bei Nutzern von Telekommunikation entstehen. Diese Daten können dann von der Polizei, der Staatsanwaltschaft und von Gerichten zur Ermittlung von Straftaten von staatlichen Stellen angefordert, eingesehen und analysiert werden. Bisher speichern Telefondienstleister diese Daten bereits, jedoch nur um die Abrechnungen mit den Nutzern abwickeln zu können. Danach waren die Daten unverzüglich zu löschen. Ein Einsichtsrecht stand staatlichen Stellen nicht zu.

Bei den zu speichernden Daten handelt es sich nicht um die Inhalte der jeweiligen Kommunikationsvorgänge. Jedoch unterfallen der Speicherung alle sonstigen Daten aller Kunden während der Nutzung von Telefon, Handy und Internet. Bei Telefonaten sind Rufnummer, Datum, Uhrzeit und Dauer der Verbindung mit Beginn und Ende des Gesprächs zu speichern, sowohl vom Anrufer als auch vom Angerufenen. Erfolgt das Gespräch über ein Mobiltelefon, speichert das Telekommunikationsunternehmen die Kennung des Anrufers und des Angerufenen, den Zeitpunkt und Adressatennummer eines SMS/MMS-Versands, Standort des Handys, Geräte- und Kartenummer und bei Kommunikation via Internet Kennung, Absender, Empfänger, Betreff und Postzugriff von Emails, sowie die IP-Adresse.

Zweck der Überwachung

Die Datenüberwachung dient in erster Linie der effektiven Verfolgung von Straftaten. Die gespeicherten Daten sollen ohne Wissen der Betroffenen bei dem Verdacht der schweren Straftat von den Telekommunikationsanbietern an die staatlichen Ermittlungsstellen übermittelt werden, wenn die Ermittlungen ansonsten wesentlich erschwert oder aussichtslos sind.

Die Telekommunikationsüberwachung ist ein wichtiges, erfolgreiches und unverzichtbares Mittel zur Aufklärung schwer ermittelbarer Kriminalität. Erschwerend kommt hinzu, dass die Entwicklung der Abrechnungsmodalitäten keine Speicherungen in dem bisherigen Umfang mehr erfordern, z.B. bei Pauschaltarifen ("Flatrate-Telefonieren") oder Prepaidkarten, die ohne Vertrag und damit ohne die

Angabe der personenbezogenen Daten nutzbar sind. Das hat die Folge, dass die Datenerhebung und –verwendung und somit die Strafverfolgung immer schwerer und aussichtsloser wird.

Kommunikationsmittel sind als Strafverfolgungswerkzeuge aber notwendig und wirksam, insbesondere dort, wo organisierte Kriminalität passiert. Insbesondere der internationale Terrorismus nutzt vor allem das Internet und die Anonymität, die der Datenschutz bietet, um kriminelle Akte auf dem elektronischen Weg vorzubereiten, oder, wie bei den Anschlägen in Madrid über Mobiltelefone, sogar auszuüben.

Verbrechensbekämpfung nicht um jeden Preis

Es bestehen keine Zweifel daran, dass die Spuren der gespeicherten Daten zur Auflösung schwerer Verbrechen geeignet sind. Bei der Verfolgung dieses Zwecks bleibt aber die Frage, ob diese pauschale Überwachung der Telekommunikationsdaten aller Staatsbürger angemessen ist. Diese Zweifel werden deutlicher, indem nicht einmal die Personen von der Überwachung ausgenommen werden, die als Vertrauenspersonen auf die Geheimhaltung der Daten angewiesen sind, wie bspw. Ärzte, Rechtsanwälte, Psychotherapeuten und Journalisten. Das Gesetz regelt zwar, dass die Datenerhebung und -verwendung gerade bei diesen Personen im Einzelfall für unzulässig erklärt und deren Löschung veranlasst werden kann. Dem geht jedoch zum einen die Abwägung des öffentlichen Strafverfolgungsinteresses mit dem Geheimhaltungsinteresse des Einzelnen voraus, statt von vornherein ausgeschlossen zu sein.

Der Versuch, die Grundrechte zu wahren

Die Gefährdung folgender Grundrechte durch dieses Gesetz ist denkbar:

Das Recht auf die informationelle Selbstbestimmung, indem nicht mehr frei bestimmt werden kann, wann und innerhalb welcher Grenzen persönliche Daten erhoben und verwendet werden.

Das Patienten-/ Mandantengeheimnis im Rahmen der Schweigepflicht, indem auch aus den nicht-inhaltlichen Daten Rückschlüsse auf die private Lebensführung gezogen werden können.

Das Fernmeldegeheimnis, denn auch hier besteht die Möglichkeit, aus den gespeicherten Daten Rückschlüsse auf den Inhalt der erfolgten Kommunikation.

Die Pressefreiheit, indem die Informationsquellen nicht mehr anonym sind und das besondere Vertrauensverhältnis zwischen Presse und Informanten nicht mehr gewährleistet ist.

Der Gesetzgeber hat Maßnahmen zur Wahrung der Verfassungsgrundsätze in das Gesetz eingearbeitet: die umfassende Wahrheitsermittlung durch Analyse der Datenspeicherungen ist notwendigerweise an hohe Anforderungen geknüpft. Bevor staatliche Stellen Einsicht in die gespeicherten Daten erhalten, z.B. das Bundeskriminalamt oder der Verfassungsschutz, ist eine gerichtliche Anordnung der Herausgabe der Daten gegenüber dem Telekommunikationsanbieter erforderlich. Ein solcher Gerichtsbeschluss ergeht nur bei Bejahung eines erhöhten Anfangsverdachts hinsichtlich bestimmter schwerer Straftaten wie Mord oder terroristische Anschläge.

Die Inanspruchnahme der Daten darf zudem nur erfolgen, wenn andere Ermittlungsansätze aussichtslos wären. Die Anordnung begrenzt das Einsichtsrecht auf bestimmte Personen und Telekommunikationsanlagen sowie den Zeitraum der Dateneinsicht. Zudem können mangels Inhaltsspeicherung der jeweiligen Kommunikation keine Bewegungsprofile erstellt werden. Absolut unzulässig ist die Überwachung von Seelsorgern, Bundestagsabgeordneten und Strafverteidigern, sowie im Rahmen von Maßnahmen, die allein den Kern der privaten Lebensgestaltung betreffen.

Die Realität zeigt sich anders

Diese Ansätze der verfassungsgemäßen Regelung erfassen aber nicht das Kernproblem. Tatsächlich handelt es sich bei der neuen Handhabung der Datenspeicherung um eine präventive Überwachungsmaßnahme. Ohne einen vorherigen Verdacht und ohne einen unmittelbaren Verwendungszweck werden alle anfallenden Daten erst einmal aufgezeichnet und gespeichert. Die Folgen können fatal sein: auch wenn keine Inhalte der Gespräche und Schriftwechsel gespeichert werden, ergeben die Verkehrsdaten im Rückschluss ebenso ein Persönlichkeitsprofil des Nutzers. Es ist aus den Daten ersichtlich, wer Patient bei welchem Arzt ist, welche Personen Mandanten eines Rechtsanwalts sind oder welche Nutzer eine Psychotherapie durchführen.

Das eigentliche Problem besteht also in der Einschränkung der informationellen Selbstbestimmung bereits vor dem Akt der Telekommunikation selbst während des Speichervorgangs: Patienten, die wissen, dass jeder Anruf bei ihrem Psychotherapeuten gespeichert und staatlichen Stellen zugänglich ist, werden sich genau überlegen, ob sie einen Anruf tätigen, wie lange dieser andauern soll und wer der Angerufene sein wird. Rechtsanwälte werden E-mail-Verkehr mit Mandanten meiden, weil Rückschlüsse daraus gezogen und diese als Verstöße gegen ihre Schweigepflicht gewertet werden könnten. Oder Informanten der Presse meiden die Weitergabe von Materialien, weil der Schutz der

Anonymität durch den Datenschutz aufgehoben wäre. Eine freie und ungezwungene Kommunikation ist in dem Bewusstsein dieser Datenspeicherung nicht mehr möglich. Dabei ist gerade das Vertrauen in den Datenschutz schlechthin konstituierend für den Beruf des Arztes oder eines Rechtsanwalts oder auch für die Presse.

Eine freie Meinungsäußerung und Meinungsbildung ist durch das Gefühl des Überwachtwerdens und das Risiko des Missbrauchs nicht verletzt, aber erheblich gefährdet.

Gefahr des Missbrauchs und falscher Verdächtigung

Die Speicherung von Daten dient der Strafverfolgung zudem nur begrenzt. Für Kenner ist es nicht schwer, den Speichervorgang zu umgehen. Unproblematisch sind die Ermittlungen von Straftaten von Kriminellen vereitelt, während im Gegenzug durch zufällig passende Daten Unschuldige in falsche Verdächtigungen schwerer Straftaten geraten. Zudem können die erhobenen und gespeicherten Daten dem Missbrauch zum Opfer fallen, sodass sie planwidrig nicht ausschließlich für die Ermittlung von Straftaten gebraucht werden.

Die unbefugte Verwendung von Daten ist bereits jetzt eine übliche Form des Datenmissbrauchs zur Erkundung von Persönlichkeitsprofilen. Dem Missbrauch von personenbezogenen Daten wird durch die Erweiterung des Datenumfangs ein weiterer Anreiz geboten.

Überarbeitung des Gesetzes erforderlich

Der grundsätzliche Ansatz der Kriminalitätsbekämpfung durch Analyse von Daten ist begrüßenswert. Der Nutzen einer pauschalen Telekommunikationsüberwachung in dem nun gegebenen Ausmaß ist jedoch im Verhältnis zu der Schwere der Eingriffe in die Persönlichkeitsrechte insbesondere der Berufsgeheimnisträger aber auch der auf das Vertrauen angewiesenen Bürger gering.

Der ungezwungene Umgang mit den Möglichkeiten der Telekommunikation ist nicht mehr möglich. Eine Nachbesserung des Gesetzes ist notwendig.

Beispielsweise könnte der Beginn der Datenspeicherung erst einsetzen, wenn ein Verdacht einer schweren Straftat vorliegt und der Personenkreis, der Datenumfang und der Zeitraum der Speicherung von vornherein in einer gerichtlichen Anordnung feststehen.

Ausblick

Das Gesetz soll am 1. Januar 2008 in Kraft treten. Dazu muss aber der Bundespräsident seine Zustimmung geben und den Gesetzesbeschluss unterzeichnen.

Zudem hat eine Vielzahl von Bürgern eine Massenverfassungsbeschwerde gegen die geplante Telekommunikationsüberwachung initiiert, mit der die Verfassungsmäßigkeit des neuen

Überwachungsgesetzes überprüft werden soll.

Die Entwicklungen dürfen also gespannt verfolgt werden.

Artikel erschienen auf www.akademiker-im-www.de im Dezember 2007