FIfF e.V. & DVD e.V. c/o
Werner Hülsmann - Am Leutenberg 1 - D-87745 Mörgen

Forum InformatikerInnen für Frieden und gesellschaftlich e Verantwortung e.V.
Telefon +49 (0) 421 / 33 65 92 55
Telefax: +49 (0) 421 / 33 65 92 56
E-Mail: fiff@fiff.de
http://www.fiff.de
Büro: Goetheplatz 4
D-28203 Bremen
Vereinsregister Bonn Nr. VR 5102

Deutsche Vereinigung für Datenschutz e.V.
Telefon: +49 (0) 228/22 24 98
Telefax: +49(0) 228/24 38 470
E-Mail: dvd@datenschutzverein.de
http://www.datenschutzverein.de
Büro: Bonner Talweg 33-35
D-53113 Bonn
Vereinsregister Bonn Nr. VR 4257

Hintergrundinformationen zur Pressemitteilung vom 30.09.2004

„EU will bis zu drei Jahre im nachhinein wissen, wer wann mit wem und womit telefoniert, gesimst oder gemailt hat und wer wann wie lange welche Internetseiten aufgerufen hat“

Mörgen, 22.09.2004

Für Rückfragen und weitere Informationen steht Ihnen zur Verfügung: Werner Hülsmann
Tel.: +49 (0) 8266 / 869 36 - 80; FAX: - 79
Mobil: +49 (0) 179 / 46 86 484;
E-Mail: werner@fiff.de

Inhaltsverzeichnis

Hintergrund des EU-Entwurfs

Im Rahmen der Ratstagung für Justiz und Inneres am 29./30. April 2004 haben Frankreich, Großbritannien, Irland und Schweden einen gemeinsamen Vorschlag für einen Rahmenbeschluss zur Vorratsspeicherung von Kommunikationsdaten vorgelegt: Entwurf eines Rahmenbeschlusses über die Vorratsspeicherung von Daten, die in Verbindung mit der Bereitstellung öffentlicher elektronischer Kommunikationsdienste verarbeitet und aufbewahrt werden, oder von Daten, die in öffentlichen Kommunikationsnetzen vorhanden sind, für die Zwecke der Vorbeugung, Untersuchung, Feststellung und Verfolgung von Straftaten, einschließlich Terrorismus (Ratsdokument 8958/04) (zu finden unter: http://fiff.almeprom.de/telekommunikation.htm)

Gemäß dieses Rahmenbeschlussen sollen Verkehrs- und Standortdaten einschließlich Teilnehmer- und Nutzerdaten, die im Rahmen der folgenden Kommunikationsinfrastrukturen, -architekturen und -protokolle erzeugt werden erfasst und gespeichert werden:

- Telefonie (Festnetz und Mobilfunk),
- SMS-Kurzmitteilungen und elektronische Medien- und Multimedia-Datentransferdienste,
- Internet-Protokolle (einschließlich E-Mail und Protokolle für Sprachübermittlung über das Internet).

Nicht betroffen von diesem Entwurf sind die Inhalte der Kommunikation. Für die zweite und dritte Gruppe können die Mitgliedstaaten Abweichungen von der vorgesehenen Speicherfrist beschließen. Diese müssen allerdings dem Rat und der Kommission mitgeteilt und jährlich überprüft werden.

Die vorgeschlagene Speicherdauer beträgt mindestens 12 bis maximal 36 Monate. Die Mitgliedstaaten sollen im Rahmen von Rechtshilfeersuchen auf die in den anderen EU-Staaten vorhandenen Vorratsdaten zugreifen können.

Derzeitige Praxis der TK-Verkehrsdatenspeicherung in Deutschland

Zum 01. Juli ist in Deutschland das neue Telekommunikationsgesetz (TKG2004) in Kraft getreten. Dabei hat der deutsche Gesetzgeber die Einführung einer Mindestspeicherungsfrist für Verkehrsdaten abgelehnt. Diese Ablehnung erfolgte, obwohl die Sicherheitsbehörden eine Einführung einer Vorratsdatenspeicherung gefordert haben. Regelungen zur Verarbeitung personenbezogener Daten zu Zwecken der Strafverfolgung müssen einen sachgerechten Ausgleich zwischen den Interessen der Strafverfolgung, den wirtschaftlichen Belangen der Telekommunikationsunternehmen und dem Datenschutz der Nutzer öffentlicher Kommunikationsnetze sicherstellen. Die Abwägung dieser zum Teil gegensätzlichen Interessen führte zu der deutlichen Ablehnung der Mindestspeicherfristen durch den Deutschen Gesetzgeber. Die Sicherheitsbehörden konnten – trotzt regelmäßiger Aufforderung u.a. durch Datenschutzbeauftragte - nicht konkret angeben, welche TK-Verkehrsdaten sie noch benötigen und inwieweit die fehlenden Verkehrsdaten ihre Ermittlungen behindern.

Bereits mit dem 1996 in Kraft getretenem Telekommunikationsgesetz (TKG1996) und der dazugehörigen Telekommunikationsdatenschutzverordnung (TDSV2000) war es den Telekommunikations-Dienstleistern (kurz TK-Dienstleistern) erlaubt, die für die Abrechnung erforderlichen Abrechnungsdaten bis zu sechs Monate nach Versand der Rechnung aufzubewahren. Hieran hat sich durch die Verabschiedung des TKG2004 nichts geändert. Verkehrsdaten, die nicht für die Abrechnung benötigt werden, waren und sind sofort zu löschen. Vergleichbare Regelungen finden sich für Internetprovider im Teledienstedatenschutzgesetz (TDDSG, vgl. dort § 6 Abs. 7).

Eine Umfrage des Bundesbeauftragten für den Datenschutz bei den TK-Dienstleistern nach den aktuellen Speicherfristen für die Abrechnungsdaten hat ergeben, dass die 80-Tage-Frist, die vor Inkrafttreten des TKG1996 galt, bislang nur unwesentlich verlängert wurden. So werden bei den meisten TK-Dienstleistern die Abrechnungsdaten für maximal drei Monate nach Rechnungserstellung gespeichert. Begründet wurde die Nichtausnutzung der Sechsmonatsfrist mit erheblichen Kostenaufwendungen für die zusätzlichen erlaubten aber nicht erforderlichen Speicherzeiträume.

Die Sicherheitsbehörden haben die Möglichkeit in gesetzlich vorgesehenen Fällen unbemerkt auf die Bestandsdaten von Kunden der TK-Dienstleister zuzugreifen und bei konkreten Verdachtsmomenten Telekommunikationsüberwachungen durchzuführen. Die hierfür erforderlichen technischen Einrichtungen und Maßnahmen sind von den TK-Dienstleistern auf eigene Kosten vorrätig zu halten.

Mit Einführung des TKG2004 sind Mobilfunkbetreiber gesetzlich verpflichtet auch beim Kauf von Pre-Paid-Mobilfunkkarten Name, Anschrift, Geburtsdatum des Käufers zu erfassen und sich durch Ausweisvorlage bestätigen zu lassen, obwohl diese Angaben zur Erbringung der TK-Dienstleistungen nicht erforderlich sind.

Anforderungen aus dem Grundgesetz der Bundesrepublik Deutschland

Verfassungsmäßige Grundsätze

Nach dem Grundgesetz, der Verfassung der Bundesrepublik Deutschland, muss sich staatliches Handeln an den Grundsätzen von Verhältnismäßigkeit, Erforderlichkeit und Zweckmäßigkeit halten.

Erforderlichkeit

In Verbindung mit der Speicherung von personenbezogenen Daten – und solche sind die TK-Verkehrsdaten heitß das: Es dürfen nur die personenbezogenen Daten erhoben werden, die notwendig sind um den gesetzlich vorgegebenen Zweck zu erfüllen. Gibt es eine Möglichkeit, den gleichen Zweck mit weniger (sensiblen) personenbezogenen Daten zu erfüllen, ist diese Möglichkeit vorzuziehen

Zweckmäßigkeit

Verfahren und personenbezogene Daten die zur Erfüllung des Zwecks nicht geeignet sind, dürfen nicht verwendet werden.

Verhältnismäßigkeit

Der Umfang der Datenerhebung, Erfassung, Verarbeitung und Speicherung muss in einem angemessenem Umfang zum angestrebten rechtlich zulässigen Zweck der Datenverarbeitung stehen

Recht auf informationelle Selbstbestimmung

Bereits im Dezember 1983 hat das Bundesverfassungsgericht in seinem „Volkszählungsurteil“ begründet auf Artikel 1 Abs. 1 in Verbindung mit Artikel 2 Abs. 1 des Grundgesetzes das „Recht auf informationelle Selbstbestimmung“ und damit das Grundrecht auf Datenschutz zu Verfassungsrang erhoben. „Das Grundrecht gewährleistet insoweit die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen.“ (BVerfGE 65,1)

Einschränkungen dieses Grundrechts sind zwar vom Verfassungsgericht vorgesehen, an diese Einschränkungen werden aber hohe Anforderungen gestellt:

> „Einschränkungen dieses Rechts auf ‚informationelle Selbstbestimmung’ sind nur im überwiegenden Allgemeininteresse zulässig. Sie bedürfen einer verfassungsgemäßen gesetzlichen Grundlage, die dem rechtsstaatlichen Gebot der Normenklarheit entsprechen muß. Bei seinen Regelungen hat der Gesetzgeber ferner den Grundsatz der Verhältnismäßigkeit zu beachten. Auch hat er organisatorische und verfahrensrechtliche Vorkehrungen zu treffen, welche der Gefahr einer Verletzung des Persönlichkeitsrechts entgegenwirken“ (BVerfGE 65,1)

Weiter führt das Bundesverfassungsgericht aus:

> „Mit dem Recht auf informationelle Selbstbestimmung wären eine Gesellschaftsordnung und eine diese ermöglichende Rechtsordnung nicht vereinbar, in der Bürger nicht mehr wissen können, wer was wann und bei welcher Gelegenheit über sie weiß. Wer unsicher ist, ob abweichende Verhaltensweisen jederzeit notiert und als Information dauerhaft gespeichert, verwendet oder weitergegeben werden, wird versuchen, nicht durch solche Verhaltensweisen aufzufallen. Wer

> damit rechnet, daß etwa die Teilnahme an einer Versammlung oder einer Bürgerinitiative behördlich registriert wird und daß ihm dadurch Risiken entstehen können, wird möglicherweise auf eine Ausübung seiner entsprechenden Grundrechte (Art. 8, 9 GG) verzichten. Dies würde nicht nur die individuellen Entfaltungschancen des Einzelnen beeinträchtigen, sondern auch das Gemeinwohl, weil Selbstbestimmung eine elementare Funktionsbedingung eines auf Handlungsfähigkeit und Mitwirkungsfähigkeit seiner Bürger begründeten freiheitlichen demokratischen Gemeinwesens ist.“ (BVerfGE 65,1)

Und:

> „Bei seinen Regelungen hat der Gesetzgeber ferner den Grundsatz der Verhältnismäßigkeit zu beachten. Dieser mit Verfassungsrang ausgestattete Grundsatz folgt bereits aus dem Wesen der Grundrechte selbst, die als Ausdruck des allgemeinen Freiheitsanspruchs des Bürgers gegenüber dem Staat von der öffentlichen Gewalt jeweils nur soweit beschränkt werden dürfen, als es zum Schutz öffentlicher Interessen unerläßlich ist“ (BVerfGE 65,1)

Und weiter:

> „Ein Zwang zur Angabe personenbezogener Daten setzt voraus, daß der Gesetzgeber den Verwendungszweck bereichsspezifisch und präzise bestimmt und daß die Angaben für diesen Zweck geeignet und erforderlich sind. Damit wäre die Sammlung nicht anonymisierter Daten auf Vorrat zu unbestimmten oder noch nicht bestimmbaren Zwecken nicht zu vereinbaren. Auch werden sich alle Stellen, die zur Erfüllung ihrer Aufgaben personenbezogene Daten sammeln, auf das zum Erreichen des angegebenen Zieles erforderliche Minimum beschränken müssen.“ (BVerfGE 65,1)

Aus diesem Grundrecht auf informationelle Selbstbestimmung wird der Grundsatz der Datenvermeidung und Datensparsamkeit abgeleitet, der sich in mehreren deutschen Gesetzen wieder findet:

> „Gestaltung und Auswahl von Datenverarbeitungssystemen haben sich an dem Ziel auszurichten, keine oder so wenig personenbezogene Daten wie möglich zu erheben, zu verarbeiten oder zu nutzen. Insbesondere ist von den Möglichkeiten der Anonymisierung und Pseudonymisierung Gebrauch zu machen, soweit dies möglich ist und der Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.“ (§ 3a Bundesdatenschutzgesetz, BDSG, vgl. aber auch TDDSG und TKG2004)

Vereinbarkeit mit dem Grundgesetz der Bundesrepublik Deutschland

Bereits aus den dargestellten Aussagen des Bundesverfassungsgerichts im Volkszählungsurteil lässt sich ableiten, dass eine Vorratsdatenspeicherung der TK-Verkehrsdaten aller Nutzer und Nutzerinnen selbst für die berechtigten Zwecke der Strafverfolgung schon wegen der gravierenden Verletzung des Rechts auf informationelle Selbstbestimmung nicht mit dem Grundgesetz der Bundesrepublik Deutschland zu vereinbaren wäre. Auch die Zwecke eine möglichen Strafverfolgung oder Terrorismusbekämpfung rechtfertigen die mit der TK-Vorratsdatenspeicherung verbundenen Eingriffe in dieses Grundrecht nicht. Weitere Entscheidungen des Bundesverfassungsgerichts – wie die jüngste Entscheidung zur Verfassungswidrigkeit des so genannten Großen Lauschangriffs (vgl. BVerfG, 1 BvR 2378/98 vom 3.3.2004) – unterstützen diese Aussage.

Die Speicherung der TK-Verkehrsdaten von vielen Millionen Nutzern und Nutzerinnen auf Vorrat ist zudem nicht erforderlich und verstößt gegen den Verhältnismäßigkeitsgrundsatz des Grundgesetzes. Bereits für die aktuellen rechtlich zulässigen Möglichkeiten der Telekommunikationsüberwachung und der Abfrage von Bestands- und Verbindungsdaten durch die Sicherheitsbehörden fehlt der Nachweis, dass die in den letzten Jahren erfolgten Ausweitungen der Befugnisse der Sicherheitsbehörden zu tatsächlichen Fahndungserfolgen oder zur Verhinderung von Straftaten geführt hätten. So ist die TK-Überwachungsdichte in Deutschland deutlich höher als in den USA. Die Aufklärungsquote bei den entsprechenden

Straftaten ist dagegen nicht signifikant höher. Selbst wenn in wenigen Einzelfällen, die Ermittlungen durch die Hinzuziehung von 12 bis 36 Monaten alten TK-Verkehrsdaten vereinfachen würden, so rechtfertig dies nicht die unbegründete Vorratsdatenspeicherung der Verbindungsdaten von Millionen unbescholtener Bürger und Bürgerinnen. Der Nachweis, dass Ermittlungen durch das Nichtvorhandensein von älteren TK-Verkehrsdaten verhindert würden, ist auch im letzten Gesetzgebungsverfahren zur Änderung des TKG den Sicherheitsbehörden nicht gelungen. Selbst die Festschreibung der seit 1996 erlaubten maximalen Speicherungsfrist für Abrechnungsdaten von sechs Monaten als Mindestspeicherungsfrist ließ sich nicht ausreichend begründen. Eine Speicherung aller TK-Verkehrsdaten – also nicht nur der Abrechungsdaten – für einen Zeitraum von mindestens 12 bis 36 Monaten lässt sich noch viel weniger begründen. Diese Aussage wird auch vom Unabhängigen Zentrum für Datenschutz unterstützt:

> „Die Vorratsspeicherung würde einen schwerwiegenden Eingriff in Kommunikationsgrundrechte einhalten, weil die einzelnen Kommunikationsvorgänge für staatliche Zwecke aufgehoben würden und zugleich auch das Missbrauchsrisiko bei den privaten Daten speichernden Stellen stiege. Im Übrigen ist zu erwarten, dass die Bürger von ihren Grundrechten auf Zugang zu Informationen und zur freien Meinungsäußerung dann zurückhaltender Gebrauch machen, wenn sie damit rechnen müssen, bei entsprechenden Aktivitäten in eine vorsorgliche Protokollierung zu geraten.“ (http://www.datenschutzzentrum.de/material/themen/rotekarte/hintergr.htm#3)

Fazit:

Die vorgesehene Vorratsdatenspeicherung ist mit dem Grundgesetz der Bundesrepublik Deutschland nicht zu vereinbaren!

Kosten der TK-Vorratsdatenspeicherung

> „Der Branchenverband BITKOM bezifferte den Aufwand je Unternehmen mit einem "hohen zweistelligen Millionenbetrag". Die Deutsche Telekom nannte bereits für eine Vorratsspeicherung von 6 Monaten Investitionskosten in Höhe von 180 Mio. € sowie jährliche Mehrkosten von 40 Mio. €.“
> (http://www.datenschutzzentrum.de/material/themen/rotekarte/anhoerung090204.htm)

Daher haben sich die Vertreter der TK-Diensteanbieter auf einer Anhörung des Deutschen Bundestages zum Telekommunikationsgesetz (TKG) am 9. Februar 2004 einmütig gegen eine Vorratsspeicherung von Verbindungsdaten ausgesprochen. In dieser Anhörung ging es „nur“ um eine Mindestspeicherungsfrist von sechs Monaten. Die oben genannten Kosten wären bereits bei einer Mindestspeicherungsfrist von 12 Monaten mehr als zu verdoppeln, da die jetzigen Speicherungsfristen bei den TK-Dienstleistern bei 80 Tagen bis drei Monaten liegen. Alleine in der Bundesrepublik kämen auf die TK-Dienstleister und Internetprovider jährliche Mehrkosten in Höhe mehreren Milliarden Euro zu.

Zu der bei der letzen Änderung des TKG diskutierten Forderung der Sicherheitsbehörden nach einer Vorratsdatenspeicherung erklärt der Bundesverband Informationswirtschaft, Telekommunikation und neue Medien (BITKOM) e.V.

> „Die vorgesehene Vorratsdatenspeicherung bedeutet zudem eine starke Belastung der betroffenen Unternehmen, da diese erst einmal die erforderlichen Speicherkapazitäten und die Systeme aufbauen müssten, um derartige Datenmengen zu verwalten. ‚Wenn wirklich künftig ein halbes oder sogar ein ganzes Jahr jede Telefonverbindung und jeder Click im Internet gespeichert werden sollen, dann braucht das Lagerhallen voller Datenspeicher’, stellt Rohleder fest. Für jeden größeren Anbieter summieren sich die Kosten schnell auf mehrere Millionen Euro. Aber gerade auch die vielen kleinen Unternehmen könnten die damit verbundenen Investitionen kaum schultern. Der Aufwand steht dabei in einem völlig inakzeptablen Verhältnis zu dem letztlich erzielbaren Erfolg. Schon die bisherigen Ermittlungsbefugnisse, etwa zur Überwachung der Telekommunikation,

können, wenn sie konsequent eingesetzt werden, eine hinreichende Sicherheit gewähren. Ein wesentlicher Zusatznutzen ist durch die Vorratsdatenspeicherung nicht zu erwarten.“ (http://www.bitkom.org/de/presse/archiv/18510_2203.aspx)

Die entstehenden Mehrkosten würden die TK-Dienstleister und Internetprovider wiederum auf ihre Kunden und Kundinnen abwälzen was zu signifikanten Kostensteigerungen im TK- und Internetdienstleistungsbereich führen würde. Nicht abwälzbare Kosten würden zu niedrigeren Gewinnen auf Seiten der TK-Dienstleister und Internetprovider führen. Die Verteuerungen der TK- und Internetdienstleistungen würden wiederum zur Verteuerung von Dienstleistungen führen, die auf TK- und Internetdienstleistungen basieren. Im Endeffekt würde sich negative Auswirkungen auf die Inflationsrate, auf die verfügbare Kaufkraft der Verbraucher und Verbraucherinnen aber auch auf die Einnahmen des Staates zeigen. Diese negativen Auswirkungen würden den Euro-Stabilitätspakt gefährden und die wirtschaftliche Entwicklung in Europa zumindest verlangsamen.

Fazit:

Aus auch wirtschaftlichen Gründen ist eine Vorratsdatenspeicherung der TK-Verkehrsdaten abzulehnen.

Europäische Betrachtung

Im Rahmen einer Konsultation der EU-Kommission (DIRECTORATE-GENERAL INFORMATION SOCIETY, Directorate B: Communication services: policy and regulation framework und DIRECTORATE-GENERAL JUSTICE AND HOME AFFAIRS Directorate D : Internal Security and Criminal Justice) haben über 90 Organisationen ein ausführliches Papier verabschiedet in dem die TK-Vorratsdatenspeicherung entschieden abgelehnt wird:
http://www.privacyinternational.org/issues/terrorism/rpt/responsetoretention.html

Anläßlich des auf EU-Ebene von den oben genannten Direktorien durchgeführten Workshops wurde deutlich, dass nicht nur Bürgerrechtsorganisationen und Datenschutzinstitutionen sondern auch TK-Dienstleister und Wirtschaftsverbände diese Vorratsdatenspeicherung ablehnen. Ein Bericht des Workshops findet sich in englischer Sprache unter http://www.epic.org/privacy/intl/data_retention.html

Der Vorsitzende der Europäischen Datenschutzbeauftragten (Art. 29 Gruppe) und Bundesbeauftragte für den Datenschutz Peter Schaar legte dar, dass die geplanten Regelungen auch gegen Art. 8 der Europäischen Menschenrechtskonvention verstoßen!

Fazit: Auch mit Europarecht ist der Entwurf nicht vereinbar