Am 15.12.2005 hat das Europäische Parlament der von EU-Kommission und -Rat beschlossenen sog. Vorratsdatenspeicherung zugestimmt. In den Medien erscheint das Thema, wenn überhaupt, meist in der Rubrik “Computer” oder “Internet”, und es wird eher wenig darauf eingegangen, was wohl auch daran liegt, dass der Begriff recht abstrakt klingt. Dabei sind die Auswirkungen enorm, denn was auf europäischer Ebene an diesem Tag verabschiedet wurde, ist nicht weniger, als die komplette, sekundengenaue Speicherung aller Daten über die Telekommunikationsverbindungen eines jeden Bürgers. Einer unserer Leser, der sich bei diesem Thema auskennt, hat sich für uns damit befasst.

Hintergrund:

Ziele der Vorratsdatenspeicherung
Durch die Vorratsdatenspeicherung (kurz “VDS”) erhofft sich die EU eine Verbesserung der Bekämpfung von Terrorismus und schwerer Strafdaten, also eine erleichterte Strafverfolgung. Telekommunikationsunternehmen (also auch Mobilfunk- und Internetprovider) werden damit verpflichtet, die sog. “Verkehrsdaten” ihrer Kunden aufzuzeichnen und für eine bestimmte Zeit aufzubewahren. Im Falle einer schweren Straftat haben Polizei und Geheimdienste Zugriff auf diese Daten.
Die Umstände für die Speicherung und Auswertung der Daten ist EU-weit nur teilweise “harmonisiert”. Beispielsweise wurde die Dauer der Speicherung “im Normalfall” auf 6 bis 24 Monate festgelegt, sie darf aber auch explizit jederzeit vom einzelnen Staat überschritten werden (in Polen soll es z.B. eine Speicherungsdauer von 15 Jahren geben). Auch die “schwere Straftat” als Zugriffsvoraussetzung unterliegt der Definition des jeweiligen EU-Mitglieds, wodurch Unterschiede in der Rechtssprechung innerhalb der Union unausweichlich sind.

Gespeicherte Daten
Zu den gespeicherten Daten gehören u.a. die Telefonnummern eines jeden Anrufers und Angerufenen im Festnetz und beim Mobilfunk, Standortdaten bei Mobiltelefonen (Funkzelle), SMS-Daten, aber auch die IP-Adressen von Computern, die bereits für sich alleine ein großes Problem darstellen.
(Eine IP-Adresse ist, sehr grob gesagt, eine eindeutige Nummer, die einem Computer z.B. bei der Einwahl ins Internet vom Provider zugewiesen wird, und anhand derer der Rechner dann weltweit für Datensendung und -empfang angesprochen werden kann. Sie lässt sich damit in etwa mit einer Art Haus- oder Telefonnummer vergleichen.
Spätestens über den Provider ist anhand der IP-Adresse auch die Identifikation des Nutzers bzw. Besitzers möglich (auch hier besteht übrigens, bezüglich der Unterscheidung von Besitzer und etwaigem Nutzer – z.B. ein Gast -, juristisches Konfliktpotenzial, etwa in der

Frage der Haftung).)

Die IP-Adresse ist an allen Aktionen im Internet unmittelbar beteiligt, seien es Aufrufe von Webseiten, Dateitransfer über FTP, Chatten mittels Instant Messenger, und anderem. (Genauere Informationen z.B. bei wikipedia).

Inhalte, etwa von E-Mails oder Telefongesprächen werden nicht aufgezeichnet.
Gerade anhand gespeicherter URLs (Webadressen) lassen sich jedoch ohne Probleme die Inhalte der aufgerufenen Webseiten herausfinden, bzw. Die Identität der Aufrufer einer Webseite über deren IP.

Die Haltung des Deutschen Bundestags zur Vorratsdatenspeicherung:
Am 17. Februar 2005 hat der Deutsche Bundestag eine Vorratsdatenspeicherung explizit abgelehnt. Es erging ferner die Aufforderung an die Bundesregierung, diesen ablehnenden Beschluss auch auf EU-Ebene zu vertreten und demzufolge einen EU-Beschluss “pro VDS” nicht mit zu tragen.

Kritik:

Verhältnismäßigkeit
Eine anlasslose, präventive Überwachung der Kommunikation sämtlicher Bürger der Europäischen Union entspricht nicht dem rechtsstaatlichen Grundsatz der Verhältnismäßigkeit. Sie ist, selbst bei erhöhter Gefahreinschätzung, in ihren Ausmaßen nicht angemessen und verstößt damit, schon angesichts der enormen Diskrepanz zwischen der Anzahl Betroffener und der (befürchteten) Verbrechen, gegen das Übermaßverbot.

Fehlen eines Anfangsverdachts
In einem demokratischen Rechtsstaat herrscht eine allgemeine Unschuldsvermutung. Diese ist im Grundgesetz implizit (Art.20), in der Europäischen Menschenrechtskonvention explizit (Art.6) enthalten. Eine Aufnahme von Ermittlungen und damit z.B. eine Überwachungsmaßnahme wie die VDS erfordert einen Anfangsverdacht, der voraussetzt, dass “zureichende tatsächliche Anhaltspunkte vorliegen.” (§152 Abs. 2 Strafprozessordnung).
Dieser Anfangsverdacht ist im Fall der VDS aber nicht gegeben – angesichts von bald nahezu einer halben Milliarde Menschen in der EU kaum verwunderlich.
Da eine Aufnahme von Ermittlungen, wie gesagt, einen Anfangsverdacht voraussetzt, wird im Rückschluss durch die Vorratsdatenspeicherung jeder EU-Bürger gleichermaßen einem Generalverdacht ausgesetzt: Er könnte ja ein potentieller Terrorist (oder “schwerer Verbrecher”)sein, der überwacht werden muss.

Verletzung des Rechts auf informationelle Selbstbestimmung
Das Datenschutz-Grundrecht auf informationelle Selbstbestimmung garantiert dem Bürger das Recht, über die Offenbarung und Verwendung personenbezogener Datenselbst selbst zu verfügen.
Die gespeicherten “Verkehrsdaten” fallen per Definition in diese Kategorie, da sie sich einer bestimmten Person zuordnen lassen (siehe auch Bundesdatenschutzgesetz).

Dieses Grundrecht wird mit der zwangsweisen automatischen Speicherung der individuellen Telekommunikationsdaten eklatant verletzt. Der Bürger hat als Betroffener der VDS weder die Verfügungsmacht, noch die Kontrolle darüber, was er von seinem Telekommunikationsverhalten preisgeben möchte.
Um das “Volkszählungsurteil” des Bundesverfassungsgerichts zu zitieren, es besteht die Gefahr, dass:

> […personenbezogene Daten…] zu einem teilweise oder weitgehend vollständigen Persönlichkeitsbild zusammengefügt werden, ohne dass der Betroffene dessen Richtigkeit und Verwendung zureichend kontrollieren kann.

Weiterhin dürfte die Speicherung auch dem Post- und Fernmeldegeheimnis zuwiderlaufen.

Grundgesetzwidrigkeit
Angesichts der Verstöße gegen zentrale Aspekte des Grundgesetzes sowie der Rechtsordnung der Bundesrepublik Deutschland, wie oben ausgeführt, kann die VDS nur als grundgesetzwidrig eingestuft werden.

Urteile des Bundesverfassungsgerichtes
Im bereits erwähnten “Volkszählungsurteil” vom 15. Dezember 1983 hat das Bundesverfassungsgericht eine Vorratsdatenspeicherung nicht anonymisierter Daten abgelehnt und dabei zusätzlich das Gebot der Verhältnismäßigkeit als einem “mit Verfassungsrang ausgestatteten Grundsatz” betont.

Mögliche Alternative: “Quick Freeze”
Die USA verwendet eine VDS, wie jetzt von der EU vorgesehen, nicht, sondern dort kommt eine “Quick Freeze” genannte Praxis zum Tragen. Diese wird in begründeten Verdachtsfällen eingesetzt: Auf richterlichen Beschluss erfolgt dann eine Überwachung der Telekommunikationsdaten des jeweiligen Verdächtigen. Es kommt also zu einer individuellen, anlassbezogenen Speicherung, im Gegensatz zur VDS in der EU, die eben

kollektiv und anlasslos geschieht.

Gefahren durch die Datenspeicherung:
Allgemein gesagt, besteht die größte Gefahr der Vorratsdatenspeicherung darin, dass sich genaue Persönlichkeitsprofile eines Menschen herstellen lassen:
Wer war wann, wie oft und wie lange im Internet?
Was hat er da gemacht, welche Seiten aufgerufen?
Was hat er herunter geladen?
Wer telefonierte mit wem?
Wo hat sich jemand bei einem Anruf XY aufgehalten?

Ein paar Beispiele:

Bewegungsprofile
Über die Aufzeichnung der Funkzellen bei Mobiltelefonen lässt sich in einer Zeit, in der das Handy immer alltäglicher geworden ist, besonders bei häufigem Telefonieren ein ziemlich genaues Bewegungsprofil erstellen.

Der “gläserne Bürger”
Das komplette Kommunikationsverhalten aller EU-Bürger wird durch die VDS rekonstruierbar. Wer auf die Daten Zugriff hat, sieht, wer wann mit wem telefoniert, „gesimst“ und gemailt hat und welche Seiten ein „User“ im Internet besucht.
Er erkennt dadurch soziale Beziehungen, wirtschaftliche Aspekte (Netshops, aber auch Schuldnerberatungsstellen, zum Beispiel), sexuelle Präferenzen, religiöse Überzeugungen, medizinische Daten (von Informationsseiten über psychische Probleme bis hin zur Schwangerschaftsberatung), und, selbstverständlich, politische Interessen.
Es geht also beim Protest gegen die VDS gar nicht so sehr um mögliche Ordnungswidrigkeiten und Straftaten, sondern darum, dass jeder ungewollt und je nach Internetnutzung, ein fast komplettes persönliches Profil abliefert, in einer Genauigkeit und mit einer Sensibilität der Daten, der wohl kein Mensch freiwillig zustimmen würde.
Dass alle diese Daten auch noch fehlinterpretiert werden können, und man somit beispielsweise durch einen islamischen Bekannten unter Umständen in den Verdacht von Kontakten zu terroristischen Umtrieben geraten könnte, oder, wie vor einiger Zeit eine alte Dame in Amerika, des illegalen Filesharings angeklagt wird, obwohl man nicht einmal die entsprechende Software installiert hat, ist nur noch eine zusätzliche Gefahr dieser Speicherung.

Die Einschränkung oder zumindest die Kontrollmöglichkeit der Meinungsfreiheit ein Nebeneffekt

Mittels der nach Umsetzung der Richtlinie langfristigen Möglichkeit der Zuordnung von IP-Adressen zu Personen lässt sich jede Form der Meinungsäußerung im Netz zu ihrem Urheber zurückführen, sei es ein Beitrag im Usenet, oder in Webforen. Auch die Arbeit an einer Website wird durch die Speicherung der IP desjenigen, der sie hochlädt transparent. Zudem ist bereits das Wissen um die Existenz der Kommunikationsüberwachung geeignet, Nutzer in ihrem Verhalten und insbesondere ihrer freien Meinungsäußerung zu beeinflussen.

Gerade dieser Punkt wird auch von Bürgerrechtlern immer wieder betont. Nicht umsonst ist die freie Meinungsäußerung einer der elementaren Grundsätze einer modernen Demokratie. Wer weiß, dass er überwacht wird, und eventuell gar Sanktionen zu fürchten hat, verhält sich im Zweifelsfall “vorsichtiger”, selbst wenn seine Kritik, an wem auch immer, noch so berechtigt ist.

Gefahr des Datenmissbrauchs

Im Augenblick sind diese Daten “nur” für Strafverfolgungsbehörden und Nachrichtendienste zugänglich. Dass dies immer so bleibt, kann jedoch kaum garantiert werden.
Erst kürzlich ist schließlich mit der LKW-Maut bereits der Fall eingetreten, dass explizit und ausschließlich für einen bestimmten Zweck (Mautabrechnung) bestimmte Daten für andere Ziele zugänglich gemacht werden sollten.
Nimmt man nun noch hinzu, dass Innenminister Schäuble sogar ein Gesetz (welches überhaupt erst vor relativ kurzer Zeit beschlossen worden ist) ändern will, um das zu ermöglichen, sollte das Vertrauen in die gesetzliche Absicherung Zweckbindung der per VDS gesammelten Daten weiter schwinden.
Und dies wäre dann endgültig die Öffnung der Büchse der Pandora, z.B.:
Zugänglichmachen der Daten für Krankenkassen (Beitragserhöhungen für Risikopatienten wären wohl noch das Mindeste, was in diesem Fall droht)
Zugriff für Arbeitgeber (gerade sensible Daten, wie beispielsweise der Besuch von Selbsthilfeseiten im Internet können der Todesstoß für eine Anstellung oder auch ein existierendes Arbeitsverhältnis sein).
Zugriff für Versicherungen (auch hier dasselbe wie bei den Krankenkassen).
Es kann im Licht des Mautdatenkonflikts und trotz aller Beteuerungen daher wohl kaum hundertprozentig garantiert werden, dass jetzt und in Zukunft einzig staatliche Stellen Zugriff auf die gespeicherten Daten haben (auch das alleine stellt ohnehin bereits ein Unding dar, da die grundlegende Problematik bestehen bleibt). Angesichts des momentanen, mehr als bedenklichen Umgangs der staatlicher Stellen mit Menschenrechts- und Grundgesetzfragen, mag man erahnen, was bei einer Zunahme der terroristischen

Bedrohung, nicht alles an staatlichen Abwehrmaßnahmen als gerechtfertigt betrachtet wird. Ganz unabhängig davon besteht außerdem immer noch die Möglichkeit des illegalen Zugriffs auf die Daten durch Hacks, sowie deren anschließende Weiterverbreitung.

Zum Schluss: “Ich habe doch nichts zu verbergen” … Wirklich?

Es hat sicherlich seine Gründe, dass Kontoauszüge in undurchsichtigen Umschlägen verschickt werden, und wer hat noch nie eine kleine Notlüge benutzt, um z.B. Ärger mit dem Chef auszuweichen? Es sind für den normalen Bürger nicht die spektakulären, sondern die “Alltagsgeheimnisse”, die auf dem Spiel stehen, oder, einfacher gesagt, die Privatsphäre.
Die wenigsten Menschen dürften Spaß daran haben, wildfremden Menschen freiwillig ein genaues Persönlichkeitsprofil ihrer selbst vorzulegen, einschließlich gesundheitlicher und psychischer Probleme, dem wirtschaftlichen und sozialen Stand, der politischen Überzeugungen und der persönlichen Meinung zu aktuellen oder nicht mehr so aktuellen Themen.
Wieso sollte all dies, und das Recht auf diese Selbstbestimmung, in der elektronischen Telekommunikation auf einmal keinen Bestand mehr haben?
Persönliche Daten sind erst einmal neutral, aber damit sind sie auch ein zweischneidiges Schwert: Sie können positiv genutzt, und sie können gefährlich werden.
Als 1933 vom Staat eine Volkszählung durchgeführt wurde, dürfte kaum einer, der dort, wie gefordert, seinen (jüdischen) Glauben angab, etwas von den Gräueln geahnt haben, die die Zukunft bringen würde.

Auch wenn es nicht wieder so weit kommt, ist im Sinne einer freiheitlichen Demokratie lieber mehr Datenschutz zu wagen, als zu wenig. Eine Nagelprobe für den Leitsatz „Mehr Freiheit wagen.“

Einige Links zur Thematik:

http://www.heise.de/ct/aktuell/meldung/66857
[Heise Online: ausführliche Berichterstattung über die Vorratsdatenspeicherung]

http://www.datenschutzzentrum.de/material/themen/rotekarte/
[Informationen des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein]

http://stop1984.com/
[VDS-Rubrik der NGO (Nicht-Regierungs-Organisation) zur Förderung von Bürgerrechten]

http://www.sueddeutsche.de/computer/artikel/212/66146/
[Berichterstattung der Süddeutschen Zeitung]

http://de.wikipedia.org/wiki/Vorratsdatenspeicherung
[Wikipedia-Seite über VDS]