Humanistische Union

EU setzt Vorratsdatenspeicherung durch

Stellungnahme der Humanistischen Union zur EU-Richtlinie über die Vorratsdatenspeicherung

Mitteilungen Nr. 191, S.7-9

Am 14. Dezember 2005 hat das Europäische Parlament nach heftigen Debatten einer Richtlinie über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlicher elektronischer Kommunikationsdienste verarbeitet werden, zugestimmt. Damit sind nach Übernahme der Richtlinie in nationales Recht die Telekommunikationsanbieter verpflichtet, sämtliche bei der elektronischen Kommunikation anfallenden Verkehrsdaten für einen Zeitraum von sechs bis zu 24 Monaten zu speichern und sie Polizeien und Geheimdiensten zugänglich zu machen. Damit lässt sich feststellen, wer wann mit wem von welchem Ort kommuniziert und auch wer welche Webseite besucht hat.

Die Humanistische Union hat den deutschen Abgeordneten des Europäischen Parlamentes vor der Abstimmung eine ausführliche Stellungnahme zum Richtlinienentwurf zukommen lassen, in der auf grobe Verstöße gegen das Grundgesetz und die Europäische Menschenrechtskonvention hingewiesen wurde. Im Folgenden fassen wir die bürgerrechtliche Bewertung aus der Stellungnahme zusammen.

Konfliktgehalt

Die Nutzung moderner digitaler Kommunikationstechnologie und –dienste wie Handy, E-Mail, Internet, SMS ist in unseren Gesellschaften nicht mehr wegzudenken, sie sind selbstverständlicher Teil des Privatlebens der meisten Bürgerinnen und Bürger geworden. Dadurch, dass diese Kommunikationsdienste digital erbracht werden, ist es auf bislang nie da gewesene Weise technisch möglich, Verhaltensweisen von Einzelpersonen bis hin zu eingehenden Persönlichkeitsprofilen aufzuzeichnen. Die zugrundeliegende digitale Technologie ist derzeit so gestaltet, dass jeder einzelne Nutzungsschritt der genannten Medien zunächst digital aufgezeichnet und in aller Regel einer bestimmten Person zuordenbar ist. Allerdings beschränkt sich die gegenwärtige Praxis der Speicherung bei Telekommunikations- und Internetprovidern grundsätzlich auf diejenigen Verkehrsdaten, welche für die Erbringung des Dienstes und anschließend zu Abrechnungszwecken erforderlich sind. Mit der Einführung einer obligatorischen und verdachtslosen Dauerspeicherung würde der über jeden Bundesbürger anfallende Datenschatten sämtlicher seiner über technische Medien vorgenommenen Verhaltensweisen dauerhaft in einem dem potentiellen Zugriff aller interessierten Stellen angelegten Informationsreservoir zur Verfügung gestellt.

Verstoß gegen Artikel 10 Grundgesetz

Die Einführung einer Vorratsdatenspeicherung bedeutet eine grundlegende Abkehr von tragenden Prinzipien des Fernmeldegeheimnisses und des Grundrechts auf informationelle Selbstbestimmung. Außerdem steht sie im Widerspruch zu den – einfachgesetzlichen – Strukturprinzipien des Telekommunikationsgesetzes (TKG) als auch des Teledienstedatenschutzgesetzes (TDDSG).

Das in Artikel 10 Grundgesetz (GG) geregelte Fernmeldegeheimnis schützt nicht nur Inhalte, sondern auch die Kenntniserlangung von Tatsache und Umständen einer Kommunikation durch den Staat. Der Grundrechtsschutz erstreckt sich damit auch auf die Kommunikationsumstände, insbesondere die Verkehrsdaten. Dazu gehören Informationen darüber, ob wann und wie oft zwischen welchen Personen oder

Fernmeldeanschlüssen Fernmeldeverkehr stattgefunden hat oder versucht worden ist (vgl. BVerfGE 67, 157, 172). Ein Eingriff in das Fernmeldegeheimnis liegt bereits in der generellen Verpflichtung zur Speicherung (über das für die technische Durchführung Erforderliche hinaus) und dem Zugriff (BVerfGE 100, 313, 359, 366 ff.) vor.

Datenschutz durch Datenvermeidung

Bereits 1997 zog der deutsche Gesetzgeber – gerade aus der besonderen Situation des Internet – den Schluss, es müsse das Grundprinzip der Datenvermeidung gelten: Nur wenn unmittelbar nach Ende der jeweiligen Nutzung die Nutzungsdaten gelöscht werden – mit Ausnahme der Abrechnungsdaten – könne der Datenschutz der Nutzer wirksam gewährleistet werden. Auch die Novellierung des Bundesdatenschutzgesetzes im Jahre 2001 führte das zentrale Prinzip des Systemdatenschutzes ein: Bereits bei der Gestaltung der Systeme sollten datenvermeidende bzw. datensparsame Techniken eingesetzt werden. Dieser bewusst vorgenommene Paradigmenwechsel in den Datenschutzkonzepten des deutschen – einfachgesetzlichen – Gesetzgebers droht nun, aus Brüssel gezielt entwertet zu werden. Das unumstritten wirksamste Instrument des Datenschutzes, die Datenvermeidung, wird den Bürgerinnen und Bürgern damit bereits auf technischer Infrastrukturebene aus der Hand geschlagen.

Besondere Sensitivität der Daten

Soweit in der öffentlichen Debatte betont wird, es handele sich bei den zu speichernden Verkehrsdaten um keine Inhaltsdaten, kann dem nicht ohne weiteres zugestimmt werden. Nutzerprofile von Internetsurfern geben z.B. aufgrund der Aussagen über die genutzten Webseiten weitgehenden Aufschluss über mögliche politische Interessen, über mögliche Hobbies, persönliche Vorlieben etc. Hier ist es ohne große Probleme möglich, Inhalte zumindest zu rekonstruieren. Die insoweit betonte Abgrenzung zwischen den einen geringeren Eingriff nach sich ziehenden Verkehrsdaten und den Inhaltsdaten ist daher weitestgehend obsolet. Die undifferenzierte Dauerspeicherung sowohl von Internetnutzungs- als auch Telekommunikationsdaten wird auch nicht durch die von der Regelung vorgenommene zeitliche Abstufung der Speicherdauer aufgewogen. Vielmehr ist aus grundrechtlicher Sicht davon auszugehen, dass im Wesentlichen die Schutzmaßstäbe für Inhaltsdaten anzuwenden sind.

Unbestimmte Zweckänderung

Für zahlreiche der von der geplanten Regelung umfassten Verkehrsdaten fehlt es derzeit an jeglichem berechtigenden Interesse der Provider zur weiteren Speicherung. So handelt es sich bei der Speicherung von IP-Adressen, welche zur Nutzung des Internet den Rechnern von Kunden zugeordnet werden, um Daten, die allenfalls für die Dauer der technischen Erbringung vonnöten sind. Soweit diese Daten zukünftig gespeichert werden sollen, handelt es sich um eine gesetzlich erzwungene Zweckänderung der Nutzung für allgemeine Sicherheitsinteressen. Eine solche Zweckänderung ist als eigener Eingriff in das Fernmeldegeheimnis zu werten, der entsprechend gerechtfertigt werden muss.

Der von der EU bislang vorgegebene Katalog von Straftaten, bei denen Sicherheitsbehörden der Zugriff auf die anfallenden Daten eingeräumt werden soll, ist bereits so weit gefasst, dass er als nicht hinreichend bestimmt im Sinne der grundgesetzlichen Anforderungen zu bezeichnen ist. Darüber hinaus liegt in der fehlenden beschränkenden Festlegung der nationalen Gesetzgeber auf einzelne schwere Straftaten etwa in Verbindung mit Terrorstraftaten eine die Anforderung der Bestimmtheit der Zwecke verletzende Regelung.

Eine derart geplante Sammlung nicht anonymisierter Daten auf Vorrat zu unbestimmten oder noch nicht hinreichend bestimmbaren Zwecken ist mit der Verfassung unvereinbar. Speicherung und Verwendung erlangter Daten sind grundsätzlich an den (hinreichend konkret) zu bestimmenden Zweck gebunden, den das zur Kenntnisnahme ermächtigende Gesetz festgelegt hat (BVerfG 1 BvR 2226/94 v. 14.7.1999, sog. Staubsauger-Urteil; ebenso im Volkszählungsurteil: BVerfGE 65, 1, 47).

Verstoß gegen das Übermaßverbot

Die geplante verbindliche Speicherung aller Verkehrsdaten aus Telekommunikation und Internet stellt einen schweren Eingriff in das Fernmeldegeheimnis dar. Sie verstößt klar gegen den Verhältnismäßigkeitsgrundsatz und ist deshalb verfassungswidrig.

Das grundlegend neue Element im Vorgehen des europäischen Gesetzgebers bei der Vorratsdatenspeicherung besteht in der verpflichtenden Speicherung sämtlicher Daten sämtlicher Nutzer. Damit wird – zumindest mit Blick auf den bei personenbezogenen Daten unstreitig als Grundrechtseingriff zu qualifizierenden Speicherungsvorgang – jegliche Unterscheidung zwischen mutmaßlichen Tatverdächtigen, bloßen Kontaktpersonen und bislang völlig unbescholtenen Bürgern aufgegeben. Im Gegenteil müssen sämtliche Bürgerinnen und Bürger einen massiven Eingriff hinnehmen, um die nach Aussagen von Experten sich bei dieser Vorgehensweise allenfalls im Promillebereich bewegende potentielle Erkennung eines Straftäters zu ermöglichen.

Im Ergebnis wird damit pauschal die gesamte Ebene der bei der Frage der rechtlichen Zulässigkeit maßgeblichen Verarbeitungsebene Speicherung/Nicht-Speicherung der zukünftigen rechtsstaatlichen Gestaltung entzogen. Damit zeichnet sich ein überwachungsstaatliches Szenario ab, bei dem zukünftig allenfalls noch über einzelne Zugriffe seitens bestimmter Institutionen verhandelt würde, wohingegen die Frage der staatlichen Verfügbarkeit der Daten selbst dem Streit entzogen würde. Eine derartige Regelung ist mit den verfassungsfesten Schutzkonzeptionen von Artikel 10 GG als auch Artikel 2 Absatz 1 GG (Recht auf informationelle Selbstbestimmung) unvereinbar.

Flächendeckende Infrastrukturmaßnahme unverhältnismäßig

Im Gegensatz zu rechtsstaatlich fragwürdigen, weil undifferenziert alle Bürgerinnen und Bürger beeinträchtigenden polizeilichen Maßnahmen wie etwa der Raster- und der Schleierfahndung wird hier auf einer viel grundlegenderen Ebene in die Rechte der Betroffenen eingegriffen. Bereits die genannten Maßnahmen können nur dann zulässig sein, wenn sie über einen eng begrenzten Zeitraum unter strikt formulierten rechtsstaatlichen Anforderungen in einem begrenzten Rahmen (z.B. Schleierfahndung an einer bestimmten Örtlichkeit) ein herausragend wichtiges und anerkanntes Ziel verfolgen. Die vorliegende Regelung hingegen zielt auf eine verbindliche technische Infrastrukturvorgabe, die damit dauerhaft den gesamten Rahmen der Kommunikationsinfrastrukturen von Telekommunikation und Internet verändert. Die Regelung der Vorratsdatenspeicherung schafft die Grundlage für eine völlig unverhältnismäßige Überwachungsdichte und zielt auf eine flächendeckende europaweite Praxis der undifferenzierten Speicherung von personenbezogenen Daten über deren eigentliche Zwecke hinaus. Damit droht konkret u.a. die Einrichtung einer mit Hilfe moderner Data-Mining-Tools leicht zu realisierenden multifunktionalen Dauer-Rasterung der persönlichen Daten ganzer Bevölkerungsteile. Ebenfalls droht die Anmeldung weiterer Interessenten für den Zugriff, so z.B. der Telekommunikationsprovider selbst. Diese dürften in hohem Maße ein Eigeninteresse an der Auswertung z.B. im Rahmen der Effektivierung ihrer Kundenbindungssysteme

haben.

Beeinträchtigung des demokratischen Gemeinwohls

Schließlich droht die geplante Vorratsdatenspeicherung das Vertrauen der Bevölkerung in die Nutzung dieser Kommunikationsmittel insgesamt und nachhaltig zu beschädigen. Damit beschädigt die Europäische Union massiv auch den von ihr so vielfach geforderten Weg Europas in die Informationsgesellschaft. Denn Grundlage dieser mit sensitivsten Daten der Bürger arbeitenden Infrastrukturen ist das – stets auch von der Europäischen Union betonte – Vertrauen in deren datenschutzrechtlich abgesicherte Nutzbarkeit.

Dies trifft den vom Bundesverfassungsgericht in ständiger Rechtsprechung hervorgehobenen Punkt, wonach die Befürchtung einer staatlichen Überwachung schon im Vorfeld zu Befangenheit in der Kommunikation und damit zu Kommunikationsstörungen und Anpassungen führen könne. Damit betreffen die drohenden Einschränkungen der Grundrechte die Kommunikation einer freien Gesellschaft insgesamt. Aufgrund dieses stets betonten Gemeinwohlbezuges des Grundrechtsschutzes insbesondere bei Artikel 10 GG ist eine flächendeckende Überwachungsinfrastrukturmaßnahme wie die Vorratsdatenspeicherung bereits deshalb klar verfassungswidrig.

Verstoß gegen Artikel 8 EMRK

Nach Artikel 8 Absatz 1 EMRK hat jedermann das Recht auf Achtung seines Privat- und Familienlebens, seiner Wohnung und seines Briefverkehrs. Eingriffe sind nur zulässig, soweit sie gesetzlich vorgesehen sind und eine Maßnahme darstellen, die in einer demokratischen Gesellschaft zum Schutz der öffentlichen Sicherheit, der Ruhe und Ordnung notwendig ist.

In zahlreichen Entscheidungen hat der Europäische Gerichtshof für Menschenrechte zu staatlichen Überwachungsmaßnahmen Stellung genommen. Ohne explizit Datenschutzrechte zu benennen, hat er dabei Vorgaben formuliert, die auch im vorliegenden Fall der Vorratsdatenspeicherung zum Tragen kommen. Danach sind staatliche Überwachungen grundsätzlich auf Fälle zu beschränken, bei denen tatsächliche Anhaltspunkte für den Verdacht einer Straftat vorliegen. Erfasst werden dürfen grundsätzlich ausschließlich verdächtige Personen. Die Überwachungsmaßnahme ist zeitlich zu beschränken. Bei Anwendung dieser Grundsätze und unter Beachtung des auch bei der Auslegung der EMRK zentral zu beachtenden allgemeinen Verhältnismäßigkeitsprinzips bei Grundrechtseingriffen liegt eine klare Verletzung von Artikel 8 EMRK vor. Hierauf haben auch die nach der EG-Datenschutzrichtlinie 95/46 eingerichtete Artikel 29-Gruppe der Datenschutzbeauftragten der Mitgliedstaaten als auch der europäische Datenschutzbeauftragte richtig hingewiesen. Die geplante Richtlinie sollte daher umgehend dem Europäischen Gerichtshof zur Bewertung vorgelegt werden, dessen Entscheidungen ganz wesentlich auf der Rechtsprechung zur EMRK sowie auf der Verfassungstradition der Mitgliedstaaten beruhen.

Die vollständige Stellungnahme kann über die Bundesgeschäftsstelle angefordert oder im Internet heruntergeladen werden:

www.humanistische-union.de/article.php

Abgerufen am: 01.10.2022