

Bundesvorstand:
Prof. Dr. Rosemarie Will, Vorsitzende
Dr. Christoph Bruch
Gerd Eggers
Jochen Goerdeler
Nils Leopold, LL.M.
Dr. Fredrik Roggan, stellv. Vors.
Hartmuth H. Wrocklage

Geschäftsführung:
Martina Kant
Sven Lüders

Beiratsmitglieder:
Prof. Edgar Baeger
Prof. Dr. Thea Bauriedl
Prof. Dr. Volker Bialas
Prof. Dr. Lorenz Böllinger
Daniela Dahn
Dr. Dieter Deiseroth
Prof. Dr. Erhard Denninger
Prof. Dr. Helga Einsele †
Prof. Carl-Heinz Evers
Prof. Dr. Monika Frommel
Prof. Dr. Hansjürgen Garstka

Prof. Dr. Wilfried Gottschalch
Prof. Dr. Gerald Grünwald
Dr. Klaus Hahnzog
Dr. Heinrich Hannover
Prof. Dr. Hartmut von Hentig
Heide Hering
Dr. Burkhard Hirsch
Prof. Dr. Herbert Jäger
Prof. Dr. Walter Jens
Prof. Dr. Helmut Kentler
Elisabeth Kilali
Ulrich Krüger-Limberger

Prof. Dr. Erich Küchenhoff
Renate Künast, MdB
Prof. Dr. Martin Kutscha
Prof. Dr. Rüdiger Lautmann
Sabine Leutheusser-Schnarrenberger, MdB
Dr. Till Müller-Heidelberg
Prof. Dr. Heide Pfarr
Claudia Roth, MdB
Jürgen Roth
Georg Schlaga
Helga Schuchardt
Prof. Dr. Jürgen Seifert †

Prof. Klaus Staeck
Prof. Dr. Ilse Staff
Prof. Dr. Wilhelm Steinmüller
Werner Vitt
Prof. Ulrich Vultejus
Dr. Klaus Waterstradt
Heidemarie Wieczorek-Zeul, MdB
Rosi Wolf-Almanasreh
Prof. Dr. Karl-Georg Zinn

Stand: September 2005

BÜRGERRECHTSORGANISATION seit 1961

HUMANISTISCHE UNION e.V.
Haus der Demokratie und Menschenrechte,
Greifswalder Str. 4, 10405 Berlin

Tel.: 030 / 20 45 02 -56
Fax: 030 / 20 45 02 -57
info@humanistische-union.de
www.humanistische-union.de

**Humanistische
Union**

Berlin, 12.12.2005

Stellungnahme der Humanistischen Union e.V.

zum Entwurf der Richtlinie des Europäischen Parlaments und des Rates über die Vorratsdatenspeicherung von Daten, die bei der Bereitstellung öffentlicher elektronischer Kommunikationsdienste verarbeitet werden und zur Änderung der Richtlinie 2002/58/EG, KOM(2002) 438 endg.; Ratsdok. 12671/05

Inhalt:

- I. Gegenstand
- II. Vorgeschichte
- III. Rezeption der Entwürfe der EU-Institutionen in der Öffentlichkeit
- IV. Vorgeschichte der Vorratsdatenspeicherung auf EU-Ebene
- V. Bürgerrechtliche Bewertung
 1. Konfliktgehalt
 2. Verstoß gegen Artikel 10 Grundgesetz (Fernmeldegeheimnis) und des Rechts auf Achtung des Privatlebens in Artikel 8 der Europäischen Menschenrechtskonvention
 3. Generelle Anforderungen
 4. Dauer der Speicherung
 5. Besondere Sensitivität der Daten
 6. Unbestimmte Zweckänderung
 7. Verstoß gegen das Übermaßverbot
 8. Flächendeckende Infrastrukturmaßnahme unverhältnismäßig
 9. Beeinträchtigung des demokratischen Gemeinwohls
 10. Verstoß gegen Artikel 8 EMRK

I. Gegenstand

Der derzeitige Richtlinienentwurf **verpflichtet die Mitgliedstaaten zur Schaffung gesetzlich zwingender Bestimmungen, welche die Telekommunikationsanbieter aller europäischen Mitgliedstaaten verpflichten, für Zwecke der Vorbeugung, Untersuchung, Feststellung und Verfolgung von Straftaten verschiedene Verkehrsdaten aus den Bereichen Telefonie, SMS und Internet (wer kommuniziert wann und wo mit wem, aber auch: wer ruft welche Webseite im Internet auf) zu speichern.** Der Entwurf sieht nach bisherigen Verhandlungen zwischen dem Euro-

päischen Parlament und dem Europäischen Rat vor, dass die Mitgliedstaaten die Dauer der Speicherung zwischen einer verpflichtenden Mindestspeichergrenze von **sechs Monaten und nach oben bis zu zwei Jahren** festlegen können.

Sowohl der bislang vorliegende Rahmenbeschlusentwurf als auch der Richtlinienentwurf sehen eine verpflichtende Speicherung auch von erfolglosen Anrufen und für den Mobilfunkbereich die Speicherung von Standortdaten vor. Bei den am 2.12.2005 stattgefundenen Gesprächen zwischen Vertretern des EP und des Europäischen Rates soll eine Einigung erfolgt sein, wonach es den Mitgliedstaaten in der Richtlinie freigestellt wird, ob diese Daten ebenfalls gespeichert werden müssen.

II. Vorgeschichte

Die Aktivitäten der Europäischen Union sind inhaltlich eher im Kontext der Aktivitäten der dritten Säule – der Schaffung eines einheitlichen Raumes der „Freiheit, der Sicherheit und des Rechts“ einzuordnen. Einschlägiges rechtliches Instrument zur Umsetzung der Pläne wäre demnach an sich der Weg über einen Rahmenbeschluss. Nach den Terror-Anschlägen in Madrid und in London wurden Forderungen insbesondere der betroffenen Staaten laut, wonach zur Ermittlung der Täter der Anschläge eine allgemeine Vorratsdatenspeicherung der bei der Telekommunikation und bei der Nutzung des Internet anfallenden Verkehrsdaten erfolgen müsse.

Die Europäische Kommission hat am 21.9.2005, als Reaktion auf den

„Entwurf eines Rahmenbeschlusses des Europäischen Rates vom 28.04.2004 über die Vorratspeicherung von Daten, die in öffentlichen Kommunikationsnetzen vorhanden sind, für die Zwecke der Vorbeugung, Untersuchung, Feststellung und Verfolgung von Straftaten, einschließlich Terrorismus/Ratsdok. 8958/04“

einen eigenen Gesetzentwurf in der Form einer EG-Richtlinie vorgelegt. Hintergrund dieses Vorstoßes der Kommission war deren Auffassung, die Materie müsse in der ersten Säule geregelt werden.

Der Richtlinienentwurf steht am 12. bzw. 13./14. Dezember 2005 im Europäischen Parlament zur Abstimmung.

III. Rezeption der Entwürfe der EU-Institutionen in der Öffentlichkeit

Sowohl der Rahmenbeschlusentwurf des Rates als auch der Richtlinienentwurf der Kommission sind in der europäischen Öffentlichkeit von Beginn an auf massive Kritik gestoßen. Allein in drei Mitgliedstaaten (England, Niederlande und Deutschland) bestehen zumindest für Teilbereiche der geplanten Regelungen Beschlüsse der jeweiligen nationalen Parlamente, welche die Einführung einer Vorratsdatenspeicherung ausdrücklich zurückweisen. So wurde in Deutschland im Rahmen der Novellierung des – im Wesentlichen am 26. Juni 2004 in Kraft getretenen – Telekommunikationsgesetzes (TKG) die Einführung einer Mindestspeicherfrist für Verkehrsdaten im Bundestag diskutiert und ausdrücklich u.a. mit Verweis auf verfassungsrechtliche Bedenken verworfen. Zahlreiche Aufrufe nationaler und internationaler Organisationen, zuletzt etwa der auch von der HUMANISTISCHEN UNION unterstützte Aufruf der Datenschutzorganisation Privacy International vom 5.12.2005, fordern die Europäischen Institutionen auf, ihr Vorhaben der Vorratsdatenspeicherung unverzüglich und in Gänze aufzugeben. Sie verweisen insbesondere auf die Europäische Menschenrechtskonvention (EMRK) und sprechen von einer evidenten Verletzung des insoweit einschlägigen Artikel 8 EMRK – des Rechts auf Achtung der Privatsphäre.

IV. Vorgeschichte der Vorratsdatenspeicherung auf EU-Ebene

Mit der 1995 verabschiedeten Datenschutzrichtlinie 95/46/EG unterstrich die Europäische Union ihren Willen, neben den Markt-Grundfreiheiten auch das Grundrecht der Bürgerinnen und Bürger auf Schutz ihrer Privatsphäre schützen zu wollen. Zentraler Erwägungsgrund war es, neben der Harmonisierung unterschiedlicher Datenschutzbestimmungen in den Mitgliedstaaten, dass Datenverarbeitungssysteme im Dienste des Menschen stehen: Diese Systeme haben, „ungeachtet der Staatsangehörigkeit oder des Wohnortes der natürlichen Personen, deren Grundrechte und -freiheiten und insbesondere deren Privatsphäre zu achten (...)“ (Erwägungsgrund 2 der EG-Datenschutzrichtlinie). Die Richtlinie lehnt sich inhaltlich stark an das deutsche Datenschutzmodell an.

Tragendes Strukturprinzip der Richtlinie zur Realisierung des Schutzes der Daten der Bürger ist das sog. Zweckbindungsprinzip sowie das eng damit zusammenhängende Übermaßverbot.

Nach Artikel 6 der Richtlinie sind personenbezogene bzw. personenbeziehbare Daten

- nach Treu und Glauben auf rechtmäßige Weise nur für festgelegte eindeutige und rechtmäßige Zwecke zu erheben und nicht in einer mit diesen Zweckbestimmungen nicht zu vereinbarenden Weise weiterzuverarbeiten.
- Sie haben den Zwecken zu entsprechen, für die sie erhoben und/oder weiterverarbeitet werden, für die sie erheblich sind und sie dürfen nicht darüber hinausgehen und
- sie sind nicht länger, als es für die Realisierung der Zwecke, für die sie erhoben oder weiterverarbeitet werden, erforderlich ist, in einer Form aufzubewahren, die eine Identifizierung der betroffenen Personen ermöglicht.

Bereits in der EG-Telekommunikationsdatenschutz-Richtlinie 97/66/EG vom 15.12.1997 sowie zuletzt in der Datenschutzrichtlinie für Elektronische Kommunikation 2002/58/EG vom 12.7.2002 (dort: Artikel 15) wurde das Prinzip der strengen Zweckbindung insofern aufgeweicht, als den Mitgliedstaaten die Möglichkeit eingeräumt wurde, freiwillig Vorratsspeicherungen der anfallenden Verbindungsdaten für bestimmte Zwecke der öffentlichen Sicherheit und der Strafverfolgung vorzunehmen. Der entscheidend darüber hinausgehende Schritt, der mit dem nun vorgelegten Richtlinienentwurf realisiert wird, besteht in der **Verpflichtung aller Mitgliedstaaten** zu einer **Mindestspeicherung** der Verbindungsdaten über die bestehenden, zumeist an Abrechnungszwecken orientierten Fristen hinaus.

V. Bürgerrechtliche Bewertung

Die Pläne stehen im Spannungsfeld des auch die Aufgaben der Europäischen Union betreffenden Zielkonfliktes der Gewährleistung sowohl von Sicherheit als auch Freiheit gleichermaßen.

1. Konfliktgehalt

Der Weg aller modernen Industriestaaten in die Informationsgesellschaft hat das Alltagsleben der Menschen grundlegend verändert. Bis Anfang der 90er Jahre war das Internet noch völlig unbekannt. Telekommunikation wurde auf analoger Technologie beruhend ohne die Erfassung und Speicherung der Verkehrsdaten der Nutzer erbracht. Mobilfunk war für die breite Masse der Bürgerinnen und Bürger unerschwinglich und bestimmte Kommunikationsdienste, insbesondere E-Mail und SMS waren noch völlig unbekannt.

Heute sind die Nutzung der genannten Medien selbstverständlicher Teil des Privatlebens nahezu aller Bürgerinnen und Bürger, insbesondere in den westlichen Industriestaaten. Ebenso basiert die Privatwirtschaft auf der intensiven Nutzung dieser Kommunikationsmöglichkeiten. Auf diese Weise können Verhaltensweisen von Einzelpersonen auf bislang nie da gewesene Weise bis hin zu **eingehenden Persönlichkeitsprofilen** technisch gewährleistet werden. 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 Inter-

net Providern grundsätzlich auf diejenigen Verkehrsdaten, welche für die Erbringung des Dienstes und anschließend zu Abrechnungszwecken erforderlich sind. Der Zeitraum der Speicherung übersteigt grundsätzlich nicht drei Monate. Diese Praxis entspricht zumindest überwiegend der Gesetzeslage.

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.

2. Verstoß gegen Artikel 10 Grundgesetz (Fernmeldegeheimnis) und des Rechts auf Achtung des Privatlebens in Artikel 8 der Europäischen Menschenrechtskonvention

Die geplante Einführung einer Vorratsdatenspeicherung bedeutet eine grundlegende Abkehr von tragenden Prinzipien des Fernmeldegeheimnisses und des Grundrechts auf informationelle Selbstbestimmung. Ihre Realisierung würde eine massive Schwächung des Grundrechtsschutzes aller europäischen Bürgerinnen und Bürger nach sich ziehen.

Die Regelung verstößt konkret gegen Artikel 10 Grundgesetz (GG) und gegen Artikel 8 EMRK. Sie steht **in massivem Widerspruch** zur Rechtsprechung des Bundesverfassungsgerichts zum Recht auf informationelle Selbstbestimmung und im Übrigen zu den tragenden – einfachgesetzlichen – **Strukturprinzipien** des Telekommunikationsgesetzes (TKG) als auch des Teledienstedatenschutzgesetzes (TDDSG).

Das in Artikel 10 GG geregelte Fernmeldegeheimnis schützt nicht nur Inhalte, sondern auch die Kenntniserlangung von Tatsache und Umständen einer Kommunikation durch den Staat. Wenn dieser sich vom jeweiligen privaten Kommunikationsmittler Kenntnis geben lässt und wenn er die so erlangten Daten speichert, verwertet oder weitergibt, ist dies ebenfalls vom Schutz umfasst. 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.

3. Generelle Anforderungen

Ein solcher Eingriff mag zwar gemäß Artikel 10 Absatz 2 GG grundsätzlich anordenbar sein. Es bedarf dafür aber nicht nur einer gesetzlichen Regelung, die einen legitimen Gemeinwohlzweck verfolgt und im Übrigen den Grundsatz der Verhältnismäßigkeit wahrt. Vielmehr ergeben sich aus Artikel 10 GG auch besondere Anforderungen an den Gesetzgeber, die gerade die Verarbeitung personenbezogener Daten betreffen, welche mittels Eingriffen in das Fernmeldegeheimnis erlangt worden sind. Insoweit sind die Maßgaben, die das Bundesverfassungsgericht im Volkszählungsurteil aus Artikel 2 Absatz 1 in Verbindung mit Artikel 1 Absatz 1 GG entwickelt hat, weitgehend auf die speziellere Garantie in Artikel 10 GG zu übertragen. Zu diesen Anforderungen gehört, dass sich Voraussetzungen und Umfang der Beschränkungen klar und für den Einzelnen erkennbar aus dem Gesetz ergeben. Insbesondere muss der Zweck, zu dem Eingriffe in das Fernmeldegeheimnis vorgenommen werden dürfen, bereichsspezifisch und präzise bestimmt werden, und das erhobene Datenmaterial muss für diesen Zweck geeignet und erforderlich sein.

4. Dauer der Speicherung

Der auf der technischen Ebene ansetzende Vorgang der verpflichtenden Speicherung von Daten, also das Erfassen, Aufnehmen oder Aufbewahren personenbezogener Daten auf Datenträgern zum

Zweck der weiteren Verarbeitung oder Nutzung, hat insbesondere eine zeitliche Komponente. In zeitlicher Hinsicht ermöglicht die Speicherung in Abhängigkeit von der Speicherdauer den Abruf und die Nutzung der Daten zu späteren Zeitpunkten und in veränderten Situationen. Die Speicherung entscheidet somit darüber, zu welchen Zeitpunkten und in welchen Zusammenhängen welche Daten welchen Stellen zur Verfügung stehen. Bereits 1997 zog der deutsche Gesetzgeber deshalb – 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.

5. 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 beispielsweise 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 geplanten Regelung vorgenommene zeitliche Abstufung der Speicherdauer aufgewogen. Vielmehr ist aus grundrechtlicher Sicht davon auszugehen, dass im Wesentlichen die Schutzmaßstäbe für Inhaltsdaten anzuwenden sind.

6. 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 Terrorstrafaten eine die Anforderung der Bestimmtheit der Zwecke verletzende Regelung.

Eine derart geplante Sammlung **nicht anonymisierter Daten auf Vorrat zu unbestimmten oder noch nicht hinreichend bestimmbar**en 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. Senat 2226/94 vom 14. Juli 1999, sog. Staubsauger-Urteil; ebenso im Volkszählungsurteil: BVerfGE 65, 1, 47).

7. 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 unstrittig als Grundrechtseingriff zu qualifizierenden Speichervorgang – 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 bewegend 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.

8. 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 Überwachungsichte 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 Interessen 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. Derartige Umwidmungen von zunächst kritisierten staatlichen Vorgaben im unternehmerischen Eigeninteresse sind aus der Privatwirtschaft bereits bekannt (Beispiel Research-Systeme für Geldwäsche in der Kreditwirtschaft).

9. 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 Informati-

ongesellschaft. 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.

10. 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.

Nils Leopold
*für den Bundesvorstand
der Humanistischen Union e.V.*