Humanistische Union

Stellungnahme der Humanistischen Union zum Referentenentwurf für das deutsche Umsetzungs-gesetz der Vorratsdatenspeicherung

Die Umsetzung der europäischen Richtlinie zur Vorratsdatenspeicherung in deutsches Recht sollte nach dem Willen des Bundesjustizministeriums im Rahmen einer großen Reform der "verdeckten Ermittlungsmaßnahmen" erfolgen: Ende 2006 legte das Ministerium einen Referentenentwurf für ein "Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG" vor. Eine Arbeitsgruppe der Humanistischen Union gab dazu am 19. Januar 2007 eine umfangreiche Stellungnahme ab. Diese widmet sich neben den geplanten Änderungen der Strafprozessordnung auch der Vorratsdatenspeicherung und behandelte die Rechtmäßigkeit der EU-Richtlinie, die verfassungsrechtliche Bewertung des Umsetzungsgesetzes und die grundsätzliche Frage, ob und wie weitgehend die Vorratsdatenspeicherung in das Fernmeldegeheimnis eingreift.

Stellungnahme der Humanistischen Union zum Referentenentwurf für das deutsche Umsetzungsgesetz der Vorratsda

Die gesamte Stellungnahme (51 Seiten) steht auch als PDF-Dokument zur Verfügung.

Inhalt der Stellungnahme

b) Geeignetheit der Vorratsdatenspeicherung
c) Erforderlichkeit der Vorratsdatenspeicherung
d) Angemessenheit der Vorratsdatenspeicherung

aa) Die von der Vorratsdatenspeicherung erfassten Personen 38
bb) Adressaten der Speicherungspflicht (§ 110a Abs. 1 Satz 1 TKG-E)
cc) Quasi-Verbot der Anonymisierungsdienste
dd) Katalog der zu speichernden Daten (§ 110a Abs. 2 bis 5 TKG-E)
ee) Missbrauchsgefahr durch Private

e) Zwischenergebnis für die erste Stufe

1.3 Stufe 2: Zugriff auf die Vorratsdaten als Eingriff in das Fernmeldegeheimnis aus Art. 10 Abs. 1 GG

a) Straftatenkatalog für den staatlichen Zugriff auf die Vorratsdaten (§ 100g Abs. 1 StPO-E)
b) Unzureichende Differenzierung bezüglich der Kontaktpersonen (Nachrichtenmittler)
c) Die zugriffsberechtigten Behörden
d) Zu niedrige Eingriffsschwelle
e) Zwischenergebnis für die zweite Stufe
2. Verstoß gegen Art. 12 Abs. 1 GG
3. Ergebnis der verfassungsrechtlichen Prüfung

Stellungnahme der Humanistischen Union

zum Referentenentwurf eines "Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG"
Berlin, 19. Januar 2007

I. Die europarechtswidrige Richtlinie

1. Die Entstehung der Richtlinie

Nach den Anschlägen vom 11. März 2004 in Madrid hat sich die Diskussion um die Einführung einer europaweit harmonisierten Vorratsdatenspeicherung von Telekommunikationsverkehrsdaten intensiviert. Auf dem EU-Gipfel am 25. März 2004 wurde eine Erklärung gegen den Terrorismus angenommen und der Rat erhielt den Auftrag, Rechtsvorschriften für die Vorratsdatenspeicherung durch die Telekommunikationsanbieter zu erarbeiten. Der von Irland, Frankreich, Schweden und Großbritannien vorgelegte und auf Art. 31 Abs. 1 Buchstabe c und 34 Abs. 2 Buchstabe b EUV gestützte Entwurf eines entsprechenden Rahmenbeschlusses wurde sehr kontrovers diskutiert, scheiterte letztlich aber an der

fehlenden Einstimmigkeit . Daraufhin legte die Europäische Kommission am 21. September 2005 einen Entwurf für eine entsprechende Richtlinie nach Art. 95 EGV vor. Trotz der mehrfach geäußerten Bedenken gegen die Rechtmäßigkeit der gewählten Rechtsgrundlage sowie gegen den Regelungsinhalt wurde der Entwurf bereits am 14. November 2005 in erster Lesung verabschiedet . Nachdem der zur Annahme der Richtlinie notwendige Mehrheitsbeschluss des Rates der Justiz- und Innenminister am 21. Februar 2006 zu Stande kam, ist die "Richtlinie 2006/24/EG über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste erzeugt oder verarbeitet werden, und zur Änderung der Richtlinie 2002/58/EG" (Vorratsdatenspeicherungsrichtlinie) am 03. Mai 2006 in Kraft getreten.

Der Bundestag hat von der Bundesregierung gefordert, bei der Umsetzung der Richtlinie zur Vorratsdatenspeicherung nicht über die Vorgaben der Richtlinie hinaus zu gehen . Die Bundesregierung erklärte ihrerseits, dieser Forderung folgen zu wollen.

2. Richtlinieninhalt

Nach der Vorratsdatenspeicherungsrichtlinie müssen die Mitgliedsstaaten dafür Sorge tragen, dass die Anbieter öffentlich zugänglicher elektronischer Kommunikationsdienste sowie die Betreiber öffentlicher Kommunikationsnetze verpflichtet werden, die im Zuge der Bereitstellung ihrer Dienste erfassten Verkehrsdaten über den betrieblichen Bedarf hinaus, also ohne einzelfallbezogenen Anlass, auf Vorrat zu speichern. Diese Daten sind unter bestimmten Vorraussetzungen den zuständigen Behörden zum Zwecke der Ermittlung, Feststellung und Verfolgung von schweren Straftaten zur Verfügung zu stellen (Art. 1 Abs. 1, Art. 3 Abs. 1 RL 2006/24/EG). Mit den gespeicherten Daten sollen die eindeutige Rückverfolgung und Identifizierung der Quelle und des Adressaten einer Nachricht nach Datum, Uhrzeit, Dauer und Art der Nachrichtenübermittlung sowie die Bestimmung der Endeinrichtung und des Standorts mobiler Geräte möglich werden (Art. 5 Abs. 1 RL). Gespeichert werden sollen beispielsweise die Rufnummer des anrufenden und des angerufenen Anschlusses, der Beginn und das Ende der Verbindung, bei mobilem Telefonieren auch die Kennung der Mobilfunkkarten und der Endgeräte, bei Diensten der elektronischen Post die E-Mail-Adresse und die Benutzererkennung des Absenders und des Empfängers der übermittelten Nachricht, bei Internetnutzung die zugewiesenen Internetprotokolladressen usw. Die Richtlinie gibt eine Speicherungsdauer von mindestens sechs Monaten und höchstens zwei Jahren für diese Verbindungsdaten vor. Daten, die Aufschluss über die Kommunikationsinhalte geben, dürfen nicht auf Vorrat gespeichert werden (Art. 5 Abs. 2 RL). Die Umsetzung der Richtlinie in das nationale Recht soll bis zum 15. September 2007 erfolgen (Art. 15 Abs. 1 S. 1 RL).

3. Die Europarechtswidrigkeit der Richtlinie

Bereits an der formellen Rechtmäßigkeit der Vorratsdatenspeicherungsrichtlinie bestehen erhebliche Zweifel. Die Richtlinie wird auf Art. 95 EGV gestützt. Diese Norm bietet eine Rechtsgrundlage für Maßnahmen zur Angleichung der Rechts- und Verwaltungsvorschriften der Mitgliedsstaaten, welche die Errichtung und das Funktionieren des Binnenmarktes zum Gegenstand haben. In seiner Rechtsprechung verlangt der EuGH, dass eine auf der Grundlage von Art. 95 EGV erlassene Richtlinie tatsächlich den primären Zweck haben soll, die Voraussetzungen für die Errichtung und das Funktionieren des Binnenmarktes zu verbessern . Dabei hat der EuGH strenge Maßstäbe entwickelt: Eine bloße Feststellung von Unterschieden zwischen den nationalen Vorschriften und eine abstrakte Gefahr der Entstehung von Wettbewerbsverzerrungen rechtfertigen demnach nicht die Berufung auf Art. 95 EGV als Rechtsgrundlage

einer Richtlinie.

Ziel und der Inhalt der Vorratsdatenspeicherungsrichtlinie betreffen aber in erster Linie die Vorsorge zur Strafverfolgung . Die Angleichung nationaler Rechtsvorschriften zwecks Verbesserung des Binnenmarktes kann bei der Vorratsdatenspeicherung, wenn überhaupt, lediglich als sekundärer Zweck bezeichnet werden . Auch die politische Diskussion um die Vorratsspeicherung von Verkehrsdaten erfolgte auf europäischer Ebene stets im Kontext der polizeilichen und justiziellen Zusammenarbeit in Strafsachen. Der Wechsel zur Handlungsform der Richtlinie wurde erst vollzogen, nachdem die für den ursprünglich vorgelegten Entwurf eines Rahmenbeschlusses nach Art. 31 und 34 EUV erforderliche Einstimmigkeit nicht erreicht werden konnte.

Die Vorratsdatenspeicherungsrichtlinie ist wegen ihrer fehlenden Rechtsgrundlage deshalb als formell nichtig anzusehen. Es ist zu erwarten, dass die von Irland erhobene Nichtigkeitsklage gegen die Richtlinie Erfolg haben wird . Diese Prognose wird durch die neuere Rechtsprechung des EuGH bekräftigt. Im Urteil vom 30. Mai 2006 zur Übermittlung von Flugpassagierdaten in die USA erklärte der EuGH in ähnlicher Konstellation die ebenfalls auf Art. 95 EGV gestützte Richtlinie mangels Rechtsgrundlage für nichtig.

Hinzu kommen erhebliche Zweifel, ob der Inhalt der Richtlinie dem Maßstab von Art. 8 EMRK standhält. Bei der Prüfung der Eingriffe in das durch Art. 8 EMRK gewährleistete Grundrecht auf Privatsphäre und private Telekommunikation orientiert sich der EuGH an der Rechtsprechung des EMGR. Eingriffe in dieses Grundrecht sind zulässig, insoweit sie gesetzlich vorgesehen sind und Maßnahmen darstellen, die in einer demokratischen Gesellschaft zum Schutz der nationalen Sicherheit, der öffentlichen Ordnung sowie zur Verhütung von Straftaten und zum Schutz der Rechte und Freiheiten anderer notwendig sind (Art. 8 Abs. 2 EMRK). Durch die Verpflichtung zur vorrätigen Speicherung der Kommunikationsdaten sämtlicher Nutzer greift die Richtlinie in das Gemeinschaftsgrundrecht auf Achtung des Privatlebens und der Korrespondenz aus Art. 8 EMRK unverhältnismäßig ein. Eine Erfassung sämtlicher Telekommunikation aller EU-Bürger ohne konkreten Anlass und ohne jeglichen Tatverdacht kann in einer demokratischen Rechtsordnung nicht als notwendig angesehen werden.

Sollte die Vorratsdatenspeicherungsrichtlinie vom EuGH für nichtig erklärt werden, bestünde für die Mitgliedsstaaten keine Umsetzungspflicht mehr. Aus rechtspolitischer Sicht erscheint es deswegen sachgerecht, bis zur Entscheidung des EuGH über die Nichtigkeitsklage von Irland von der Umsetzung der Richtlinie 2006/24/EG in nationales Recht abzusehen. Die Opposition im Deutschen Bundestag hat dies schon mit Nachdruck gefordert: "Der Schaden, der dadurch entstünde, dass eine nichtige Richtlinie zunächst in nationales Recht umgesetzt würde und das Umsetzungsgesetz dann wieder zurückzunehmen wäre, ist erheblich. Eine u.U. verzögerte Umsetzung ist deshalb unter dem Gesichtspunkt der Verhältnismäßigkeit hinzunehmen". Die Bundesregierung wird außerdem aufgefordert, während der EU-Ratspräsidentschaft auf die Rücknahme der Richtlinie zur Vorratsdatenspeicherung hinzuwirken bzw. im Falle eines neuen EU-Rahmenbeschlusses wegen der verfassungsrechtlichen Bedenken gegen die Vorratsdatenspeicherung nicht zuzustimmen.

II. Zur Verfassungsmäßigkeit des deutschen Umsetzungsgesetzes

Wegen der erheblichen Einschränkungen des Rechts auf vertrauliche Telekommunikation sowie des Rechts auf Achtung des Privatlebens, die mit einer Umsetzung der Richtlinie 2006/24/EG verbunden wären, erscheint es mehr als zweifelhaft, ob eine verfassungskonforme Umsetzung in das deutsche Recht überhaupt möglich ist.
Mit dem vorliegenden Umsetzungsentwurf würden die schon jetzt bestehenden exzessiven Speicherungs-, Zugriffs- und Verwendungsmöglichkeiten telekommunikationsrelevanter Daten erheblich erweitert . Die bisherige Berechtigung der Telekommunikationsunternehmen, bestimmte Daten für die Zwecke einer

korrekten Abrechnung zu speichern, werden in eine Pflicht umgewandelt, fast alle anfallenden Verbindungsdaten sowie die Nutzungs- und Standortdaten zu erfassen, zu speichern und ggf. den Strafverfolgungsbehörden auf Anordnung unverzüglich zur Verfügung zu stellen. Damit soll es zu Zwecken einer wirksamen Strafverfolgung schnell nachvollziehbar sein, wer, wann, mit wem, wie lange, von wo aus und über welches Telekommunikationsmedium kommuniziert hat. Da den zugreifenden Strafverfolgungsbehörden keine Schranken bei der Auswertung dieser Daten auferlegt sind, wird die Erstellung von Kommunikations- und Bewegungsprofilen aller Telekommunikationsteilnehmer möglich. Eine Entschädigung für die Inanspruchnahme der Telekommunikationsunternehmen bei der Erhebung der Verkehrsdaten ist nicht vorgesehen.

Der vorgelegte Gesetzentwurf widerspricht mit diesen Regelungen tragenden Prinzipien des Datenschutzrechts (Datensparsamkeit, Zweckbindungsgebot, hohe Anforderungen bei der Anwendung des Verhältnismäßigkeitsgrundsatzes) und schränkt das Grundrecht auf Fernmeldegeheimnis und auf informationelle Selbstbestimmung unverhältnismäßig ein. Insbesondere mit der vorgesehenen Verwendung der gespeicherten Daten für die Verfolgung mittelschwerer und mittels Telekommunikationseinrichtungen begangener Straftaten (vgl. § 100g Abs. 1 StPO-E) wird das Gesetz unverhältnismäßig. Der Gesetzentwurf öffnet Tür und Tor für spätere Erweiterungen des staatlichen Zugriffs auf die Vorratsdaten. Angesichts der großen Bandbreite und der zeitlichen Tiefe der vorrätigen Verbindungsdaten erscheint die Zugriffsregelung mit ihrem generellen Verweis auf die in § 100a Abs. 2 StPO-E aufgezählten Straftaten ebenfalls nicht angemessen.
Vor diesem Hintergrund stellt sich die Frage nach der Verfassungsmäßigkeit der einzelnen Regelungen im Gesetzentwurf.

1. Der Verstoß gegen Art. 10 GG (Fernmeldegeheimnis)

Der Schutzbereich des Telekommunikationsgeheimnisses umfasst sowohl den Inhalt der Telekommunikation als auch die näheren Umstände des Fernmeldeverhältnisses . "Dazu gehört insbesondere, ob, wann und wie oft zwischen Personen oder Endeinrichtungen Telekommunikationsverkehr stattgefunden hat oder versucht wurde. Anderenfalls wäre der grundrechtliche Schutz unvollständig, denn die Verbindungsdaten haben einen eigenen Aussagegehalt. Sie können im Einzelfall erhebliche Rückschlüsse auf das Kommunikations- und Bewegungsverhalten zulassen. Häufigkeit, Dauer und Zeitpunkt von Kommunikationsverbindungen geben Hinweise auf Art und Intensität von Beziehungen und ermöglichen auf den Inhalt bezogene Schlussfolgerungen".

Der Schutz des Art. 10 Abs. 1 GG erstreckt sich auch auf den Informations- und Datenverarbeitungsprozess, der sich an zulässige Kenntnisnahmen anschließt und den Gebrauch, der von den erlangten Kenntnissen gemacht wird.

1.1. Zweistufiger Eingriff in das Grundrecht aus Art. 10 Abs. 1 GG

Ein Eingriff in das Fernmeldegeheimnis liegt vor, wenn staatliche Stellen sich ohne Zustimmung der Betroffenen Kenntnis von dem Inhalt oder den Umständen eines fernmeldetechnisch vermittelten Kommunikationsvorgangs verschaffen . Die im Gesetzentwurf vorgesehenen Regelungen zur Umsetzung der Richtlinie 2006/24/EG greifen zweistufig in das Fernmeldegeheimnis ein. Auf der ersten Stufe erfolgt der Eingriff in das Kommunikationsgeheimnis mit der gesetzlich angeordneten Verpflichtung der Anbieter öffentlicher Telekommunikationsdienste, fast alle anfallenden Verbindungsdaten für 6 Monate zu speichern (vgl. § 110a Abs. 2 TKG-E). Die Tatsache, dass die Erhebung und Speicherung der Daten durch die

Telekommunikationsunternehmen erfolgt, ändert an ihrer Qualität als staatlichem Eingriff in das Fernmeldegeheimnis nichts. Die vorgesehene Erfassung und Speicherung ist hoheitlich angeordnet, die Unternehmen verfügen dabei über keinen Handlungsspielraum . Auf der zweiten Stufe erfolgt der Eingriff in das Grundrecht aus Art. 10 Abs. 1 GG durch die Regelungen, die einen staatlichen Zugriff auf die auf Vorrat gespeicherten Verkehrsdaten und ihre Verwendung ermöglichen. Die Telekommunikationsunternehmen werden ausdrücklich verpflichtet, die erfassten und gespeicherten Daten den zuständigen staatlichen Stellen auf Ersuchen unverzüglich zur Verfügung zu stellen (§ 110b Abs. 1 TKG-E). Aufgrund der in den § § 100g, 100a StPO-E vorgesehenen Normen können sich dann staatliche Stellen ohne Wissen und Zustimmung der Beteiligten von den Umständen aller gespeicherten Telekommunikationsvorgänge ein genaues Bild machen.

Der Zugriff auf die umfangreichen Verbindungsdaten erlaubt einen umfassenden Einblick in das Kommunikationsverhalten der Betroffenen, deren Identität feststellbar ist. Auf beiden Stufen greift der Gesetzesvorschlag intensiv in Art. 10 GG ein. Dabei ermöglicht die Vielzahl der erfassten Daten Rückschlüsse auf Kommunikationsstrukturen, z. T. auch auf den Inhalt der Telekommunikation . Die Bewertung der zahlreichen Standortdaten erlaubt außerdem die Erstellung genauer Bewegungsprofile der Betroffenen.

Wegen der Unterschiedlichkeit der Eingriffe auf der ersten und zweiten Stufe wird ihre Verfassungsmäßigkeit nacheinander geprüft.

1.2. Stufe 1: Die anlasslose Erhebung und Speicherung sämtlicher Verbindungsdaten als genereller Verstoß gegen das Fernmeldegeheimnis

a) Legitimität des Zwecks der Speicherungspflicht

Zweifel bestehen zunächst einmal an der Legitimität des Zwecks der Vorratsdatenspeicherung. Nach der Begründung des BMJ soll die pauschale Speicherung sämtlicher elektronischer Kommunikationsvorgänge die Verfügbarkeit der Verkehrs- und Standortdaten für die Zwecke späterer Strafverfolgung sicherstellen.

In einer freiheitlichen Demokratie darf die Spurensicherung nur im Verdachtsfall erfolgen. Der Staat darf nicht jeden Bürger vorsorglich als potenziellen Verbrecher behandeln. Nach etablierter Rechtsprechung und Rechtspraxis ist eine vorsorgliche Überwachung für künftige Strafverfolgungsmaßnahmen bisher in der Bundesrepublik Deutschland an das Vorhandensein einer konkreten Gefahrenlage oder einer negativen Kriminalprognose der betroffenen Personen gebunden. Mit einer anlass- und verdachtslosen Speicherung sämtlicher Verbindungsdaten würde praktisch allen Benutzerinnen und Benutzern elektronischer Telekommunikationsmittel unterstellt, sie könnten in der Zukunft zum Objekt staatlicher Strafverfolgung werden. Dieser generelle Verdacht schränkt nicht nur das Recht auf vertrauliche Kommunikation ein, sondern stellt auch grundlegende Prinzipien des Datenschutzes, die Sparsamkeit und Zweckgebundenheit von staatlich angeordneter Datenspeicherung, auf den Kopf.

Vor diesem Hintergrund erscheint es aus verfassungsrechtlicher Sicht bedenklich, dass Daten, die ansonsten nicht vorliegen würden, zu allgemeinen Sicherheitszwecken gespeichert werden sollen. Man darf zu Zwecken einer eventuellen späteren Strafverfolgung die Entstehung einer umfangreichen Sammlung personenbezogener Daten auch deswegen nicht zulassen, weil auf diese Weise die Unschuldsvermutung partiell wegfallen würde. Maßnahmen wie die Vorratsdatenspeicherung, die eine verdachtlose "vorbeugende Verbrechensbekämpfung" bzw. eine "Strafverfolgungsvorsorge" gewährleisten sollen, dienen daher keinem legitimen Zweck. Vielmehr verstößt diese gesetzgeberische Zwecksetzung gegen die Unschuldsvermutung

bei der Strafverfolgung, von der auch das Grundgesetz ausgeht.

Nach einem vom Bundesverfassungsgericht entwickelten Grundsatz "muss der Zweck, zu dem Eingriffe in das Fernmeldegeheimnis vorgenommen werden dürfen, bereichsspezifisch und präzise bestimmt werden. Eine Sammlung nicht anonymisierter Daten auf Vorrat zu unbestimmten oder nicht bestimmbaren Zwecken wäre damit unvereinbar" . Das Bundesverfassungsgericht hat ausdrücklich festgestellt, dass das Grundgesetz eine "globale und pauschale Überwachung" zu Zwecken der Auslandsaufklärung nicht zulässt . Es leuchtet wenig ein, warum dies bei der Strafverfolgungsvorsorge anders sein soll. Die allgemeine Zweckbestimmung des Gesetzentwurfs, die Speicherung der Verbindungsdaten diene der Strafverfolgung, genügt vor diesem Hintergrund nicht den verfassungsrechtlichen Anforderungen.

b) Geeignetheit der Vorratsdatenspeicherung

Zweifel an der Geeignetheit ergeben sich daraus, da Kriminelle oder Terroristen mit relativ einfachen Mitteln die Überwachungsmaßnahmen unterlaufen können. Dazu bräuchten die Betroffenen lediglich ihre Kommunikationsgeräte über Dritte erwerben oder auf öffentliche Kommunikationsmittel - wie Internetcafés, Straßentelefonzellen, Mailkonten außerhalb der EU und den USA oder vorausbezahlte international einsetzbare SIM-Karten - zurückgreifen . Darüber hinaus muss auch die Möglichkeit berücksichtigt werden, Anonymisierungsdienste einzusetzen. Beide Methoden einer anonymen Nutzung der Telekommunikation werden eher besonders gefährliche Straftäter als Kleinkriminelle oder gar Unbeteiligte gebrauchen. Für die Verfolgung besonders schwerer Straftaten erscheint die Speicherung von Vorratsdaten daher wenig geeignet, die eigentliche "Zielgruppe" der Maßnahme wird sich ihr entziehen. Wenn die vorhandenen Verbindungsdaten keiner Person eindeutig zugeordnet werden können, dann ist ihre Verwertbarkeit bei einer strafrechtlichen Ermittlung sehr gering. Auch eine erhebliche gesetzliche Beschränkung oder ein Verbot von Anonymisierungsdiensten, worauf das Umsetzungsgesetz praktisch abzielt, könnte daran nichts ändern, da sich die anonyme Nutzung von Telekommunikationsnetzen technisch kaum verhindern lässt .
Die vorhandenen empirischen Angaben lassen ebenfalls Zweifel daran entstehen, ob die Vorratsdatenspeicherung in einem großen Maße zur Verbesserung der Strafverfolgung beitragen kann. In der Praxis scheitern demnach nur wenige Ermittlungsverfahren an Telekommunikationsverkehrsdaten, zumal die Strafverfolgungsbehörden oft nur an den Bestandsdaten interessiert sind.

c) Erforderlichkeit der Vorratsdatenspeicherung

Bedenken bestehen auch hinsichtlich der Erforderlichkeit der vorgesehenen Vorratsdatenspeicherung zur Terrorismus- und Verbrechensbekämpfung. Mit dem sogenannten "Quick-freeze-Verfahren" oder "Data Preservation", das u.a. in den USA praktiziert wird, steht ein milderes Mittel zur Verfügung, durch das die Ziele des Gesetzgebers weitgehend zu erreichen wären . Dabei werden die Daten einer verdächtigen Person nach der Aufforderung durch die Strafverfolgungsorgane ab sofort gespeichert, der Zugriff auf diese Daten ist dann nach Erlass einer richterlichen Anordnung möglich. Dieses Verfahren erfüllt allerdings nur dann in gleichem Maße den angestrebten Zwecken, wenn es um eine Beobachtung / Ermittlung andauernden strafwürdigen Verhaltens geht, die fraglichen Verbindungsdaten also in der Gegenwart und Zukunft anfallen. Für einen Zugriff auf in der Vergangenheit angefallene Daten ist das "Data Preservation"-Verfahren nutzlos und nicht im gleichen Maße förderlich wie die generelle Vorratsdatenspeicherung .
Trotzdem ist zu bemerken, dass erhebliche Zweifel an der Notwendigkeit der Speicherungsdauer von sechs Monaten bestehen. Erfahrungsgemäß betreffen die Zugriffe der berechtigten Behörden in ähnlichen Konstellationen fast ausschließlich die ersten drei Monate der Speicherung . Unter dem Gesichtspunkt der Erforderlichkeit wäre daher eine dreimonatige Speicherfrist hinreichend - allerdings würde die Umsetzung sich damit gegen die minimale Speicherungsfrist aus Art. 6 der Richtlinie 2006/24/EG wenden.

d) Angemessenheit der Vorratsdatenspeicherung

aa) Die von der Vorratsdatenspeicherung erfassten Personen

Eine Unterscheidung der betroffenen Personen, deren Daten auf Vorrat gespeichert werden sollen, nimmt

der Gesetzesentwurf nicht vor. Es fehlt jegliche Differenzierung nach fahndungsrelevanten Personengruppen, vielmehr sollen die Daten aller Telekommunikationsteilnehmer gleichermaßen gespeichert werden. Da der Speicherungsvorgang - zumindest die personenbezogenen Daten betreffend - einen Grundrechtseingriff darstellt und dabei jegliche Unterscheidung zwischen Tatverdächtigen, Kontaktpersonen und völlig unbeteiligten Bürgern unterbleibt, erscheint diese gesetzgeberische Lösung völlig unangemessen. "Im Ergebnis wird damit pauschal die gesamte Ebene der bei der Frage der rechtlichen Zulässigkeit maßgeblichen Verarbeitungsebene Speicherung/Nichtspeicherung der zukünftigen rechtsstaatlichen Gestaltung entzogen. Damit zeichnet sich ein überwachungsstaatliches Szenario ab, bei dem zukünftig über einzelne Zugriffe seitens bestimmter Institutionen verhandelt wird, wohingegen die Frage der staatlichen Verfügbarkeit der Daten selbst dem Streit entzogen sind. Eine derartige Regelung ist mit den verfassungsfesten Schutzkonzeptionen von Artikel 10 GG als auch Artikel 2 Absatz 2 GG unvereinbar".

Die Regelungen des Gesetzentwurfes stehen damit im Gegensatz zu wichtigen verfassungsrechtlichen Grundsätzen des Datenschutzes . Durch die Vorratsdatenspeicherung werden Strukturprinzipien wie Datensparsamkeit, Datenvermeidung und Zweckbindungsgebot als Ausfluss des Verhältnismäßigkeitsprinzips ausgehöhlt. Die Datenerhebung erfolgt unabhängig von einem im Einzelfall bestehenden Tatverdacht. Es werden alle Kommunikationsvorgänge sämtlicher Kommunikationsteilnehmer auf Vorrat gespeichert. Wenn es einerseits "kein belangloses Datum" mehr gibt und die Vorratsdatenspeicherung andererseits ermöglicht, dass praktisch alle Verkehrs- und Standortdaten von allen Telekommunikationsteilnehmern gespeichert werden, dann liegt die Verfassungswidrigkeit der jeweiligen Vorschriften auf der Hand.
Im "IMSI-Catcher"-Beschluss hat das Bundesverfassungsgericht in Zusammenhang mit der bevorstehenden Gesamtregelung der strafprozessualen heimlichen Ermittlungsmaßnahmen darauf hingewiesen, dass zu prüfen ist, "ob und in welchem Umfang von einer neuerlichen Ausdehnung heimlicher Ermittlungsmethoden im Hinblick auf Grundrechtspositionen unbeteiligter Dritter Abstand zu nehmen ist" . Dass dies durch den vorgestellten Gesetzentwurf geschieht, ist nicht ersichtlich.

bb) Adressaten der Speicherungspflicht (§ 110a Abs. 1 Satz 1 TKG-E)

In § 110a Abs. 1 Satz 1 TKG-E wird der Kreis der zur Speicherung Verpflichteten festgelegt. Danach sind zur Speicherung diejenigen verpflichtet, die Telekommunikationsdienste für die Öffentlichkeit erbringen oder an der Erbringung solcher Dienste mitwirken. Gespeichert werden müssen nur Verkehrsdaten, die vom jeweiligen Dienstanbieter bei der Nutzung seines Dienstes erzeugt oder verarbeitet werden. Die Pflicht besteht auch dann, wenn ein Anbieter Telekommunikationsdienste erbringt, ohne eine eigene Telekommunikationsanlage zu betreiben (§ 110a Abs. 1 S. 2 TKG-E). Bei der Festlegung der Adressaten der Speicherungspflicht werden zahlreiche unbestimmte Begriffe verwendet. Es stellt sich daher die Frage, ob das Bestimmtheitsgebot ausreichend berücksichtigt wurde.
Bei der Rechtsanwendung können durchaus Zweifel entstehen, ab wann von einem "Mitwirken" bei der Erbringung eines Telekommunikationsdienstes ausgegangen werden kann oder ab welcher Stufe von einer "Erzeugung" und "Verarbeitung" von Daten ausgegangen wird. Vergleichbare Anwendungsschwierigkeiten gab es beispielsweise beim Streit darum, ob der Mautsystembetreiber Toll Collect GmbH im Sinne des TKG Telekommunikationsdienste erbringt oder daran mitwirkt und dementsprechend Normadressat des §100g StPO wäre . Vergleichbare Streitfälle werden mit dem Gesetzentwurf nicht beseitigt, sondern eher noch verstärkt.
Ähnlich problematisch ist der maßgebliche Bezug der Adressaten auf die "Öffentlichkeit" im Sinne des § 110a Abs. 1 S. 1 TKG-E. Leider trägt auch die Begründung nicht zur Klärung des Adressatenkreises bei: Demnach bestünde für "den nicht öffentlichen Bereich (z.B. unternehmensinterne Netze, Nebenstellenanlagen oder E-Mail-Server von Universitäten ausschließlich für dort immatrikulierte Studierende oder Bedienstete sowie die Telematikinfrastruktur im Gesundheitswesen)" keine Speicherungspflicht. Auch die Begriffsbestimmungen des § 3 TKG helfen nicht bei der Auslegung des Tatbestands "Öffentlichkeit", weil dort keine Definitionen von "Öffentlichkeit" oder "öffentlichen Telekommunikationsnetzen" enthalten sind. Eine gesetzliche Klärung des Begriffs der "Öffentlichkeit"

erscheint aus Gründen der Rechtssicherheit dringend geboten.

In der Begründung des Gesetzentwurfs wird zum Begriff des "Verarbeitens" erklärt, dass er weit zu verstehen sei und etwa auch die Fälle erfasse, in denen ein Mobilfunknetzbetreiber die von einem Teilnehmer eines anderen Netzbetreibers initiierte Verbindung "übernimmt" und die Verbindung zu seinem eigenen Endnutzer herstellt . Welche anderen Leistungen noch unter dem Begriff des "Verarbeitens" in Zusammenhang mit der Vorratsdatenspeicherung zu subsumieren wären, ist offen. Ähnliches gilt für das Merkmal des "Mitwirkens": Die im Schrifttum verbreitete Ansicht, dass als "Mitwirkende" alle zu behandeln sind, die an einer Nachrichtenübermittlung in irgendeiner Form beteiligt sind, trägt zu einer effektiven Rechtsanwendung kaum bei.

Zu bemerken ist außerdem, dass die geplante Regelung keine Begrenzung der Speicherungspflicht auf solche Betreiber vorsieht, die Telekommunikationsdienste geschäftsmäßig erbringen oder daran mitwirken. Dabei bleibt unklar, ob auch Privatpersonen zur Speicherung verpflichtet sind, wenn sie kostenlos einen öffentlichen WLAN-Zugang, einen E-Mail-Dienst oder Ähnliches anbieten.
Vor diesem Hintergrund ist anzunehmen, dass es in der Praxis zu zahlreichen Anwendungsproblemen kommen wird, da die Adressaten der Speicherungspflicht nicht hinreichend bestimmt sind. Im Rahmen des Art. 10 GG kommt aber dem Bestimmtheitsgebot eine besondere Bedeutung zu: Umfang und Voraussetzungen der Einschränkungen müssen sich klar aus dem Gesetz ergeben.

cc) Quasi-Verbot der Anonymisierungsdienste

Das Gesetz regelt auch den Status derjenigen, die so genannte Anonymisierungsdienste betreiben und anbieten. Darunter werden Programme verstanden, die Internetverbindungen durch ein verteiltes Netz von Servern leiten. Durch die Nutzung von mehreren Servern kann die Quelle einer Nachricht derart verschleiert werden, dass die Identität des Nutzers nicht mehr feststellbar ist . Bezüglich dieser Anonymisierungsdienste wird in der Begründung zum Gesetzesentwurf ausgeführt: "Einen Telekommunikationsdienst für die Öffentlichkeit im Sinne des § 110a Abs. 1 TKG-E erbringt auch, wer einen Anonymisierungsdienst betreibt und hierbei die Ausgangskennung des Telekommunikationsnutzers durch eine andere ersetzt". Wenn aber die Anbieter von Internetanonymisierungsdiensten die entsprechenden in § 110a TKG-E aufgelisteten Daten, also auch alle in der Kette der Anonymisierung vergebenen IP-Adressen, speichern sollen, bedeutet dies praktisch, dass eine "Re-Anonymisierung" möglich wird. Der Gesetzentwurf läuft praktisch auf ein Verbot der Anonymisierungsdienste hinaus.

Eine Speicherungspflicht für Betreiber von Anonymisierungsdiensten ergibt sich nicht unmittelbar aus der Richtlinie 2006/24/EG. Die Richtlinie bezieht sich lediglich auf elektronische Telekommunikationsdienste, nicht aber auf Teledienste, wozu Anonymisierungsdienste bisher gezählt werden. Insoweit geht die Verpflichtung zur Vorratsdatenspeicherung für die Anbieter solcher Dienste über die Anforderungen der Richtlinie hinaus. Zudem widerspricht der Entwurf der geltenden Rechtslage, wonach die Anbieter von Telediensten verpflichtet sind, den Nutzern die Inanspruchnahme sowie die Bezahlung von Telediensten anonym zu ermöglichen, soweit dies technisch möglich und zumutbar ist (vgl. § 4 Abs. 6 TDDSG).

dd) Katalog der zu speichernden Daten (§ 110a Abs. 2 bis 5 TKG-E)

Eng mit den Vorschriften, die den Adressatenkreis der Speicherungspflicht regeln, sind die Normen verbunden, die die zu speichernden Daten festlegen. Der Katalog der zu speichernden Daten (§ 110a Abs. 2 bis 5 TKG-E) entspricht größtenteils der Forderung des Deutschen Bundestages sowie der Ankündigung der Bundesregierung, bei der Umsetzung der Richtlinie keine über die Mindestanforderungen der Richtlinie hinausgehenden Pflichten zu regeln . Allerdings erscheint es bezüglich einzelner Daten zweifelhaft, ob ihre Speicherung über die Richtlinie hinaus geht und ob ihr Nutzen im Vergleich zu den negativen Folgen der Vorratsdatenspeicherung verhältnismäßig ist. Dies betrifft beispielsweise die Pflicht zur Speicherung der ersten Aktivierung des jeweiligen Dienstes (bei vorausbezahlten Diensten wie beispielsweise Prepaid-SIM-Karten oder Flatrate-Tarifen für den Internetzugang) (§ 110a Abs. 2 Nr. 4 d) TKG-E); die Pflicht zur Speicherung erfolgloser Anrufsversuche (Art. 3 Abs. 2 RL, § 110a Abs. 5 TKG-E) ; die Erhebung von Daten

in Echtzeit (§ 100g Abs. 1 S. 3 StPO-E); die Angaben über die Hauptstrahlrichtung der Funkantennen beim Mobilfunk (§ 110a Abs. 6 TKG-E); das praktische Verbot von anonymen E-Mail-Konten (111 TKG-E) . Bei all diesen Daten ist sehr zweifelhaft, ob ihr praktischer Nutzwert den Grundrechtseingriff durch ihre Speicherung rechtfertigen kann. Außerdem lässt der Katalog der zu speichernden Daten trotz seiner detaillierten Aufzählungen zahlreiche Fragen offen, ob bestimmte Dienste bzw. Daten wie etwa Hot-Spots, Skype usw. davon erfasst werden.

Mit der im Gesetzentwurf vorgesehenen Speicherung der Kennung eines ankommenden Anrufs (§ 110a Abs. 2 Nr. 1 TKG-E) wird die bisherige, umstrittene "Zielwahlsuche" (§ 100g Abs. 2 StPO) entbehrlich. Für jedes Benutzerkonto werden künftig nicht nur alle ausgehenden, sondern auch alle ankommenden Verbindungen gespeichert. Die doppelte Speicherung aller Verbindungsdaten bei Sender und Empfänger zeigt einmal mehr, wie umfassend die künftige Vorratsdatenspeicherung von Verkehrsdaten ist und mit welcher Intensität sie in die Grundrechte eingreift.

Nach § 110a Abs. 2 Nr. 4 Buchst. c TKG-E sind die Standortdaten des anrufenden und des angerufenen Anschlusses bei Beginn der Verbindung zu speichern. Da ein betriebsbereites Mobiltelefon in geringen zeitlichen Abständen Signale an die nächststehende Funkzelle sendet, kann der Standort des Apparats bzw. seines Nutzers relativ genau bestimmt werden . Durch die Möglichkeit der Ortung eines eingeschalteten Mobiltelefons können genaue Bewegungsprofile erstellt werden. Die Tatsache, dass die Speicherung der Standortdaten durch die Telekommunikationsunternehmen nur beim Beginn der Verbindung erfolgt, ändert daran nichts, denn § 100g Abs. 1 S. 3 StPO-E soll künftig die Erhebung von Standortdaten durch die Strafverfolgungsbehörden in Echtzeit ermöglichen, auch wenn das Mobiltelefon gerade nicht genutzt wird . Damit würde das eingeschaltete Mobiltelefon "zu einer Art ungewolltem Peilsender" , der die Bewegung seines Nutzers meldet. Somit wird auch die aus verfassungsrechtlicher Sicht äußerst bedenkliche Ermittlungsmethode des sogenannten "stillen SMS" de facto legalisiert.

Entsprechend den Vorgaben der Richtlinie (Art. 5 Abs. 2 RL) sieht der Gesetzesentwurf generell vor, dass keine Daten gespeichert werden dürfen, die Aufschluss über den Inhalt der Kommunikation geben . Zum einen kann eine Trennung zwischen Inhaltsdaten und "reinen" Verbindungsdaten in vielen Fällen technisch kaum erfolgreich vorgenommen werden. Insbesondere bei E-Mail und SMS wird diese Trennung sehr schwierig sein, weil beide Dienste diese Daten auf Protokollebene vermischen . Zum anderen können auf Grund einer umfangreichen Sammlung von Verkehrs-, Standort- und Bestandsdaten Kommunikationsinhalte durchaus nachgebildet werden. Nach § 110a Abs. 4 Nr. 1 TKG-E sollen die den Nutzern für jede Internetsitzung zugewiesenen dynamischen und statischen IP-Adressen künftig gespeichert werden. Bei entsprechenden Auswertungen auf Grund beschlagnahmter Webserver könnten die darauf erfassten URLs mit den IP-Adressen abgeglichen werden und Kenntnisse über die Kommunikationsinhalte einzelner Nutzer gewonnen werden. Mit Hilfe ausgefeilter technischer Methoden zur Analyse der Verkehrsdaten lassen sich daraus detaillierte Informationen über soziale Netzwerke, Freundeskreise, persönliche Präferenzen etc. gewinnen sowie speziell im Internetbereich Profile über einzelne Nutzer erstellen. Experten weisen darauf hin, dass aus der Dauer eines http-Aufrufs eines Webservers darauf geschlossen werden kann, welche Teile einer Internetseite bzw. eines Online-Angebotes die Nutzerin / der Nutzer in Anspruch genommen hat - die Verbindungsdaten damit Rückschlüsse auf die Inhalte der Verbindung zulassen.

Ebenfalls ist zu berücksichtigen, dass die weitgehenden technischen Möglichkeiten einer automatischen Verarbeitung von Verkehrsdaten deren längerfristige Speicherung und Auswertung zu einem ähnlich intensiven Grundrechtseingriff werden lassen, wie die Speicherung von Kommunikationsinhalten. Das Bundesverfassungsgericht hat schon im Volkszählungsurteil betont, dass es bei der Bemessung der Intensität eines Grundrechtseingriffs nicht allein auf die Art der Angaben, sondern auf ihre Nutzbarkeit und Verwendungsmöglichkeit ankommt . Indem Verkehrsdaten in digitalisierter, standardisierter Form erfasst werden, bestehen für sie ungleich mehr Möglichkeiten ihrer (automatisierten) Auswertung und Verarbeitung als bei Inhaltsdaten . Der Nutzen von Inhaltsdaten ist zudem sehr eingeschränkt, wenn sie keiner konkreten Person zugeordnet werden können, was aber auf Grund der Verkehrsdaten möglich wird. Daher ist die Behauptung, der durch die Vorratsdatenspeicherung erfolgende Grundrechtseingriff sei geringer einzustufen,

weil es sich dabei "nur" um Verkehrsdaten handele, in ihrer Pauschalität irreführend.

Nach alledem ist festzuhalten, dass die Pflicht zur Speicherung und Aufbewahrung der in § 110a Abs. 2 bis 5 TKG-E aufgelisteten Daten zu einer sehr umfangreichen Sammlung von sensiblen personenbezogenen Daten führt. Auf deren Grundlage können umfassende Kommunikations- und Bewegungsprofile jedes Nutzers von Telekommunikationsdiensten erstellt werden. Der erwartete Nutzen für die Verbesserung der Strafverfolgung ist im Vergleich zur Intensität der Beeinträchtigung der Kommunikationsfreiheit und der Privatsphäre sämtlicher Kommunikationsnutzer verhältnismäßig gering. Die entsprechenden Regelungen im Gesetzesentwurf verstoßen daher gegen den Verhältnismäßigkeitsgrundsatz.

ee) Missbrauchsgefahr durch Private

Die massenhafte Speicherung von Verkehrs- und Standortdaten erhöht das Risiko eines Datenmissbrauchs. Sobald die Datensammlungen einmal vorhanden sind, werden staatlicherseits als auch von Privaten zunehmende Versuchungen bestehen, diese Daten für andere Zwecke zu nutzen oder die Daten an andere Interessenten zu übermitteln. Dies ist den Verfassern des Gesetzesentwurfes nicht entgangen, denn § 110b Abs. 3 S. 2 TKG-E verpflichtet die Telekommunikationsanbieter, durch technische und organisatorische Maßnahmen sicherzustellen, dass der Zugang zu den gespeicherten Daten ausschließlich hierzu besonders ermächtigten Personen möglich sein soll. Wie diese Maßnahmen konkret aussehen sollen und welche diese "besonders ermächtigten" Personen sein sollen, wird aber nicht geregelt und bleibt offensichtlich im freien Ermessen der verpflichteten Telekommunikationsdienstanbieter. Für die Benutzerinnen und Benutzer der Dienste bleibt das Risiko eines unberechtigten Zugriffs durch die Mitarbeiter der Telekommunikationsunternehmen bestehen. Die Tatsache, dass die Speicherung automatisch, also ohne jede Kenntnisnahme durch Personen erfolgen soll, kann dieses Risiko nicht mindern. Technische Fehler führten bereits mehrfach zur Offenlegung von zahlreichen Kundendaten, die plötzlich im Internet zugänglich waren. Wenn aber sensible personenbezogene Daten auch nur für kurze Zeit zugänglich sind, können sich die Betroffenen gegen einen potenziellen Missbrauch ihrer Verbindungsdaten kaum mehr entziehen. Dafür, dass ein solcher Missbrauch keinesfalls nur theoretisch denkbar ist, existieren leider schon zahlreiche Beispiele, etwa für den unberechtigten Zugriff einzelner Unternehmensmitarbeiter auf Telekommunikationsdaten oder für den Verkauf solcher Daten an andere Unternehmen. Die sogenannte "Telefonüberwachungsaffäre", die im letzten Jahr in Italien für Schlagzeilen sorgte, ist ein weiteres markantes Beispiel solcher Missbrauchsgefahren. Wegen des hohen kommerziellen Werts der Verkehrsdaten ist auch nicht auszuschließen, dass die zur Speicherung Verpflichteten selbst gern die gesammelten Daten anderweitig als im Gesetz vorgesehen nutzen würden . Auf diese Weise könnte die Vorratsdatenspeicherung zu kontraproduktiven Effekten bei der Verbrechensbekämpfung führen, weil sie das Begehen bestimmter Straftaten erleichtern würde. Ein wirksames präventives Datenschutzmanagement erscheint daher im behandelten Zusammenhang zwingend geboten. Der Gesetzesentwurf enthält allerdings keine Vorkehrungen, die dieses gewährleisten können.

e) Zwischenergebnis für die erste Stufe

Die durch das Umsetzungsgesetz vorgesehene Vorratsdatenspeicherung von Telekommunikationsverkehrsdaten stellt wegen der Erfassung umfangreicher Telekommunikationsdaten einer Vielzahl von Personen ohne jeglichen Verdacht generell einen unverhältnismäßigen Eingriff in das Grundrecht auf Fernmeldegeheimnis aus Art. 10 Abs. 1 GG dar. Mit der umfangreichen anlasslosen Speicherung sensibler Verkehrs- und Standortdaten und den damit verbundenen Gefahren würde es in einem gewissen Sinne keine unbeobachtete Telekommunikation mehr geben. Es bliebe kaum ein Telekommunikationsvorgang, der dem staatlichen Zugriff entzogen ist. Eine freie und unbefangene Telekommunikation wäre unter diesen Umständen nicht mehr möglich. In der Phase der Datenspeicherung

wird die Aufzeichnung des Fernmeldeverkehrs weder rechtlich noch tatsächlich begrenzt.

1.3 Stufe 2: Zugriff auf die Vorratsdaten als Eingriff in das Fernmeldegeheimnis aus Art. 10 Abs. 1 GG

Auch wenn anzunehmen wäre, dass die anlasslose Erhebung und Speicherung sämtlicher Verbindungsdaten aller Kommunikationsteilnehmer generell nicht gegen das durch Art. 10 Abs. 1 GG gewährleistete Fernmeldegeheimnis verstößt, sind die im Entwurf geregelten Zugriffs- und Verwendungsmöglichkeiten der auf Vorrat gespeicherten Daten selbständige unverhältnismäßige Eingriffe in das Fernmeldegeheimnis aus Art. 10 Abs. 1 GG.
Das Bundesverfassungsgericht hat in ständiger Rechtsprechung besondere Anforderungen an den staatlichen Informationszugriff auf personenbezogene Telekommunikationsdaten gestellt. Bei der Bemessung der Intensität des Grundrechtseingriffs sind danach die Gestaltung der Eingriffsschwellen, die Bestimmung der zugriffsberechtigten Behörden, die Zahl der Betroffenen und ihre Identifizierbarkeit, die Intensität der Beeinträchtigungen, die Missbrauchsgefahren sowie die aus dem Bestimmtheitsgebot folgende Notwendigkeit einer hinreichenden und normenklaren Bestimmung des Zwecks der Datenerhebung und -verwendung zu berücksichtigen.

a) Straftatenkatalog für den staatlichen Zugriff auf die Vorratsdaten (§ 100g Abs. 1 StPO-E)

Gemäß Art. 1 Abs. 1 Richtlinie 2006/24/EG bezweckt sie die verbindliche Speicherung und die Sicherung der Verfügbarkeit der Verkehrsdaten zum Zwecke der Ermittlung, Feststellung und Verfolgung von schweren Straftaten. Es wird nicht festgelegt, was unter "schwere Straftaten" zu verstehen ist . Auch zur Frage, ob die Daten für weitere Zwecke verwendet werden dürfen, verhält sich die Richtlinie nicht. Den EU-Mitgliedsstaaten stehen daher erhebliche Ermessensspielräume zu.

Nach § 100g Abs. 1 StPO-E darf Auskunft über die gespeicherten Verkehrsdaten zur Verfolgung von Straftaten von auch im Einzelfall erheblicher Bedeutung, insbesondere eine in § 100a Abs. 2 StPO-E bezeichnete Straftat, sowie zur Verfolgung von mittels Telekommunikation begangenen Straftaten verlangt werden. Der Verweis auf § 100a Abs. 2 StPO-E ist also nur beispielhaft, d.h. es kann auch andere Straftaten von "erheblicher Bedeutung" geben, zu deren Verfolgung ein Zugriff auf die gespeicherten Daten möglich sein soll. Zu bemerken ist außerdem, dass in der entsprechenden Norm des § 110b Abs. 1 TKG-E lediglich von "Verfolgung von Straftaten" die Rede ist.

Dabei ist zunächst fraglich, was unter "Straftat von erheblicher Bedeutung" zu verstehen ist, was im Zusammenhang mit dem Bestimmtheitserfordernis im Rahmen des Art. 10 Abs. 1 GG von besonderer Bedeutung ist. Entsprechend dem aus dem Rechtsstaatsprinzip ableitbaren Bestimmtheitsgebot müssen sich die Voraussetzungen und der Umfang der Beschränkungen klar und für den Einzelnen erkennbar aus dem Gesetz ergeben. Bezüglich der Tatbestandsvoraussetzung der "Straftat von erheblicher Bedeutung" in § 100g Abs. 1 Nr. 1 StPO-E erscheint es zweifelhaft, ob diese hinreichend bestimmt ist . Die Begründung zum Gesetzesentwurf geht davon aus, dass eine solche Straftat mindestens dem Bereich der mittleren Kriminalität zuzurechnen sein, den Rechtsfrieden empfindlich stören und dazu geeignet sein müsse, das Gefühl der Rechtssicherheit der Bevölkerung zu beeinträchtigen . Sowohl der Normtext als auch die Begründung enthalten unbestimmte Begriffe, die eine sehr weite Auslegung erlauben und damit für die Rechtsanwendung keine feste Grundlage bieten. Dem Gebot der Normklarheit, das bei Eingriffen in das Fernmeldegeheimnis besonders zu berücksichtigen ist, wird somit nicht Genüge getan. Vielmehr erscheint es geboten, die betreffenden Straftaten in einem enger verfassten abschließenden Katalog aufzulisten . Der Gesetzesentwurf geht auch in diesem Punkt über die europarechtlichen Vorgaben hinaus (Art. 1 Abs. 1 Richtlinie 2006/24/EG).

Es ist außerdem fragwürdig, ob der generelle Verweis auf den Straftatenkatalog des § 100a Abs. 2 StPO-E angesichts der "Streubreite" der Vorratsdatenspeicherung angemessen ist. Der Gesetzgeber müsste prüfen und begründen, ob die Verwendung der durch die Vorratsdatenspeicherung gewonnenen Daten bei der Verfolgung aller im § 100a Abs. 2 StPO-E aufgezählten Straftaten dem Verhältnismäßigkeitsgrundsatz entspricht. Zu kritisieren ist, dass die Subsidiaritätsklausel des § 100g Abs. 1 S. 2 StPO-E nur die Kategorie der mittels Telekommunikation begangenen Straftaten betrifft. Der Zugriff auf die gespeicherten Verkehrsdaten ist also im Fall einer der im § 100a Abs. 2 StPO-E genannten Straftaten nicht an die Voraussetzung gebunden, dass die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes des Beschuldigten auf andere Weise aussichtslos wäre und die Erhebung der Daten in einem angemessenen Verhältnis zur Bedeutung der Sache steht.

Bezüglich der mittels Telekommunikationsmittel begangenen Straftaten sieht der Gesetzesentwurf nicht vor, dass sie auch schwere Straftaten bzw. Straftaten von erheblicher Bedeutung sein müssen und geht über die Vorgaben der Richtlinie hinaus (vgl. Art. 1 Abs. 1 RL). Dies widerspricht dem vom Bundesverfassungsgericht entwickelten Grundsatz der möglichst grundrechtsschonenden Umsetzung von EG-Richtlinien.

Zusammenfassend ist festzustellen, dass mit der Verwendung der gesammelten Daten zur Aufklärung mittelschwerer und mittels Telekommunikationseinrichtungen begangener Straftaten eine unverhältnismäßige Lösung vorgeschlagen wurde, die über die Vorgaben der Vorratsdatenspeicherungsrichtlinie hinaus geht.

b) Unzureichende Differenzierung bezüglich der Kontaktpersonen (Nachrichtenmittler)

Nach § 100a Abs. 3 StPO-E darf sich die Anordnung auch gegen eine Person richten, von der auf Grund bestimmter Tatsachen anzunehmen ist, dass sie für den Beschuldigten bestimmte oder von ihm herrührende Mitteilungen entgegennimmt oder weitergibt oder dass der Beschuldigte ihren Anschluss benutzt. Diese Vorschrift bezieht sich auf die Telekommunikationsüberwachung, soll aber auf die Erhebung von Verkehrsdaten entsprechend angewandt werden.
Auch diese Regelung erscheint angesichts der Intensität des Grundrechtseingriffs, den sie herbeiführt, nicht ausreichend bestimmt. Es fehlt ein handhabbarer Maßstab für die Prüfung, beim Vorliegen welcher konkreter Tatsachen eine Unterstützung des Beschuldigten durch eine Drittperson mittels Kommunikationsmittel anzunehmen ist. Eine restriktive Auslegung könnte das Bestimmtheitsdefizit nicht beseitigen.

c) Die zugriffsberechtigten Behörden

Die Vorratsdatenspeicherungsrichtlinie eröffnet den Mitgliedsstaaten breite Ermessensspielräume, was die Bestimmung der zugriffsberechtigten Behörden und der Zugriffsvoraussetzungen und -verfahren betrifft (vgl. Art. 11 RL 2006/24/EG i.V.m. Art. 15 Abs. 1 der Datenschutzrichtlinie für elektronische Kommunikation 2002/58/EG).

Der Gesetzentwurf sieht dementsprechend grundlegende Änderungen bezüglich des staatlichen Zugriffs auf Verkehrsdaten vor. Durch die Neufassung des § 100g Abs. 1 StPO-E soll der bisherige Auskunftsanspruch der Strafverfolgungsbehörden gegenüber den Telekommunikationsunternehmen in eine umfassende

Erhebungsbefugnis für Verkehrsdaten umgewandelt werden . So würde es Ihnen künftig ermöglicht, selbst und in Echtzeit Verkehrsdaten sowie Standortdaten zu erheben und zu verwerten. Die Auskunftsverpflichtung der Dienstanbieter bleibt davon unberührt . Dies ist ein tiefgehender Eingriff in das Grundrecht auf vertrauliche Telekommunikation, für dessen Rechtfertigung keine Gründe ersichtlich sind.

Bei der Bewertung der geplanten Regelungen über den staatlichen Zugriff auf die vorrätig gespeicherten Daten ist weiterhin von Bedeutung, ob den Nachrichtendiensten dieser Zugriff erlaubt wird. Nach der geltenden Rechtslage dürfen nicht nur die Strafverfolgungsbehörden, sondern auch die Nachrichtendienste sowie die Verfassungsschutzämter auf bestimmte Verkehrsdaten zugreifen. Nach der Begründung zum Gesetzesentwurf soll eine Übermittlung der aufgrund des § 110a TKG-E gespeicherten Vorratsdaten für andere Zwecke als zur Verfolgung von Straftaten gemäß § 110b Abs. 1 S. 1 TKG-E nicht zulässig sein. Damit sei - so die Begründung - "insbesondere eine Übermittlung der allein auf der Grundlage des § 110a TKG-E gespeicherten Daten für Zwecke der Gefahrenabwehr, der Aufgabenerfüllung der Dienste oder auch zur Erfüllung zivilrechtlicher Ansprüche" ausgeschlossen . Dies wird auch durch die Vorschrift des § 110b Abs. 1 S. 3 TKG-E betont. Das darin enthaltene umfassende Übermittlungsverbot ist positiv zu bewerten. Wäre es beispielsweise auch den Nachrichtendiensten erlaubt, auf alle vorrätig gespeicherten Daten zuzugreifen, wäre dies wegen der diesbezüglichen geringen Rechtsschutzmöglichkeiten der Betroffenen mit dem Grundgesetz nicht vereinbar.

Bedenken bestehen aber hinsichtlich des staatlichen Zugriffs auf die dynamischen IP-Adressen im Internetbereich. De lege lata ist diesbezüglich die Norm des § 113 Abs. 1 TKG relevant. Danach sind die Anbieter von Telekommunikationsdiensten verpflichtet, den zuständigen Stellen Auskunft über die nach den § § 95 und 111 TKG erhobenen Bestandsdaten zu erteilen, soweit dies für die Verfolgung von Straftaten oder Ordnungswidrigkeiten, zur Abwehr von Gefahren für die öffentliche Sicherheit oder für die Erfüllung der Aufgaben der Verfassungsschutzbehörden, des Bundesnachrichtendienstes oder des Militärischen Abschirmdienstes erforderlich ist. Nach allgemeiner Auffassung ist die Norm bei Auskunftsersuchen bezüglich statischer IP-Adressen einschlägig, weil diese Adressen als Bestandsdaten im Sinne von § 3 Nr. 3 TKG anzusehen sind . Dementsprechend dürfen derzeit Auskunftsersuchen bezüglich dynamischen IP-Adressen nach Maßgabe der § § 100g und 100h StPO angeordnet werden. Die relevante Rechtsprechung ist allerdings uneinheitlich. Eine gesetzliche Klarstellung erscheint daher notwendig. Richtigerweise stellen die dynamischen IP-Adressen aber Verkehrsdaten dar, u.a. weil sie in keinem unmittelbaren Zusammenhang mit dem jeweiligen Vertragsverhältnis stehen.

d) Zu niedrige Eingriffsschwelle

Für den Zugriff auf die von den Telekommunikationsanbietern gespeicherten Daten ist lediglich ein Anfangsverdacht vorgesehen (§ 100g Abs. 1 S. 1 StPO-E). Die Praxis hat gezeigt, dass es nicht selten vorkommt, dass ein Anfangsverdacht allein auf Grund der Tatsache, dass jemand auf einer E-Mail-Userliste steht, angenommen wird. Diese niedrige Eingriffsschwelle ist angesichts des breiten Betroffenenkreises und der Vielzahl der gespeicherten Daten unangemessen. Zweifelhaft ist außerdem, ob das damit einhergehende Ausmaß der vorgesehenen Zugriffsbefugnisse in einem angemessenen Verhältnis zu ihrem tatsächlichen Nutzen steht .

e) Zwischenergebnis für die zweite Stufe

2. Verstoß gegen Art. 12 Abs. 1 GG

Mit der Verpflichtung der Telekommunikationsunternehmen zur Speicherung der in § 110a Abs. 2 bis 5 TKG-E bezeichneten Daten wird in ihre Unternehmensfreiheit als Unterfall der Berufsfreiheit (Art. 12 Abs. 1 GG) eingegriffen. Um die Speicherungspflichten zu erfüllen, müssten die Dienstanbieter erhebliche Investitionen vornehmen und ggf. neues Personal anstellen . Außerdem werden zusätzliche Betriebskosten entstehen. Davon würden insbesondere die kleineren Telekommunikationsunternehmen besonders hart betroffen, so dass Insolvenzen als Folge der neuen Gesetzeslage durchaus möglich erscheinen.

Weitere Eingriffe in die Unternehmensfreiheit stellen die in § 110a Abs. 6 TKG-E enthaltene Verpflichtung der Telekommunikationsunternehmen, Angaben zu ihrer Netzplanung zu machen, das praktische Verbot von Anonymisierungsdiensten sowie die Pflicht zur Erhebung von Kundendaten und Kundenidentifizierung bei Eröffnung eines E-Mail-Kontos (§ 111 TKG-E) dar. Auch dies beeinträchtigt die Unternehmensfreiheit der Telekommunikationsunternehmen, die zu befürchten haben, dass viele Kunden deswegen verloren gehen.

Der Eingriff in die Unternehmensfreiheit der zur Speicherung verpflichteten Telekommunikationsanbieter wird besonders dadurch intensiviert, dass der Gesetzesentwurf keine Entschädigung vorsieht . Dabei ist zu berücksichtigen, dass der Deutsche Bundestag die Bundesregierung ausdrücklich aufgefordert hat, zeitnah einen Gesetzesentwurf für eine angemessene Entschädigung der Telekommunikationsunternehmen für die Inanspruchnahme im Rahmen der Erfüllung hoheitlicher Ermittlungsmaßnahmen im Bereich der Telekommunikation vorzulegen . Ob dies mit der geplanten Änderung des JVEG in ausreichendem Maße geschehen wird, bleibt abzuwarten. Jedenfalls stellt die Verpflichtung der Telekommunikationsunternehmer zur Speicherung und Weitergabe von Verkehrsdaten ohne eine Entschädigung für die daraus entstehenden Zusatzkosten und für die sonstigen wirtschaftlichen Nachteile eine unverhältnismäßige Einschränkung der Unternehmensfreiheit dar und ist somit verfassungswidrig. Ein Blick ins Ausland zeigt, dass die Verfassungsgerichte von Österreich und Frankreich schon in diesem Sinne entschieden haben.

3. Ergebnis der verfassungsrechtlichen Prüfung

Die Umsetzung zur Vorratsdatenspeicherung verstößt mehrfach gegen grundrechtliche Schutzgarantien. Die Vorratsdatenspeicherung ist bereits mit ihrem Ansatz, sämtliche Verbindungsdaten aller Kommunikationsteilnehmer anlasslos zu speichern, verfassungswidrig. Eine verfassungskonforme Umsetzung kann insoweit nicht gelingen.

---

https://www.humanistische-union.de/thema/stellungnahme-der-humanistischen-union-zum-referentenentwurf-fuer-das-deutsche-umsetzungsgesetz-der/
Abgerufen am: 19.03.2025