Rechtsvergleichende Analyse im Hinblick auf die Umsetzung der Richtlinie 2006/24/EG über die Vorratsdatenspeicherung

im Auftrag des Bundesministeriums für Verkehr, Innovation und Technologie

vorgelegt vom
Ludwig Boltzmann Institut für Menschenrechte (BIM)
in Kooperation mit dem
Institut für Rechtsinformatik der Leibniz Universität Hannover (IRI)

10. März 2008

Autorinnen und Autoren

Ludwig Boltzmann Institut für Menschenrechte (BIM):

Lisa Wimmer Andersson (Übersetzung Schweden), Kerstin Buchinger (Zusammenfassung und Auswertung der Ergebnisse; Tschechien), Christian Schmaus (Einleitung; Schweden), Christof Tschohl (Zusammenfassung und Auswertung der Ergebnisse; Dänemark; Niederlande).

Institut für Rechtsinformatik (IRI), Leibniz Universität Hannover:

Marian Arning (Deutschland), Marcelo Corrales (Italien; Portugal; Spanien), Nikolaus Forgó (Einleitung; Belgien; Frankreich), Nils Hoppe (Irland; Vereinigtes Königreich), Dennis Jlussi (Deutschland; Übersetzung Griechenland, Italien), Christian Klügel (Einleitung; Übersetzung Portugal, Spanien), Eleni Kosta (Griechenland) und Tina Krügel (Deutschland).

Inhaltsverzeichnis

I. Einleitung

Kaum ein Thema der europäischen Rechtspolitik der vergangenen Jahre war und ist politisch wie rechtlich so umstritten wie die Richtlinie 2006/24/EG[1] zur Vorratsdatenspeicherung.

Der Regelungsgehalt besagter Richtlinie bricht mit der rechtsstaatlichen Tradition, in die (grund)rechtlich geschützten Positionen des Einzelnen zu Strafverfolgszwecken nur bei Vorliegen entsprechender Verdachtsmomente einzugreifen, normiert doch die Richtlinie, dass im Zuge eines Kommunikationsdienstes erzeugte oder verarbeitete Verkehrs- und Standortdaten aller EU-BürgerInnen ohne Unterschied, verdachtsunabhängig und flächendeckend auf Vorrat gespeichert werden.

Eine solche Maßnahme stellt einen Eingriff in das Grundrecht auf Datenschutz bzw. in die Garantie des Schutzes der Privatsphäre aber auch der Korrespondenz („Briefverkehr") dar, wie sie etwa in Art 8 EMRK zum Ausdruck kommen. Hierzu ist festzuhalten, dass die auf Vorrat zu speichernden Daten im Vergleich zu Inhaltsdaten (also etwa dem aufgezeichneten Inhalt eines Gesprächs) computerunterstützt ungleich effizienter, in größerem Umfang und kürzerer Zeit ausgewertet werden können. Darüber hinaus ermöglichen die erfassten Daten soziale Netzwerke nachzuvollziehen, wie auch – je nach Telefonierverhalten – mehr oder weniger genaue Bewegungsprofile jedes/r Österreichers/in, der/die ein Mobiltelefon sein/ihr Eigen nennt, zu erstellen. Schließlich geben Verkehrsdaten mitunter Aufschluss über den Inhalt der Kommunikation, wird doch ein Anruf etwa bei der „Aidshilfe" oder der „Aktion Leben" in aller Regel eine themenbezogene Beratung oder Hilfestellung zum Inhalt haben. Gleiches gilt für eine telefonische Konsultation eines Anwalts, eines Facharztes oder etwa eines Geistlichen.[2]

Diesem massiven Eingriff in das Grundrecht auf Achtung der Privatsphäre und der Korrespondenz steht ein nur sehr bescheidener Gewinn für Zwecke der Bekämpfung der organisierten Kriminalität und des Terrorismus, derentwegen die Richtlinie erlassen wurde, gegenüber.[3] Jeder technische Laie kann heutzutage bereits mit einfachsten Mitteln der Erfassung

[1] Richtlinie 2006/24/EG des Europäischen Parlaments und des Rates vom 15. März 2006 über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste oder öffentlicher Kommunikationsnetze erzeugt oder verarbeitet werden, und zur Änderung der Richtlinie 2002/58/EG.
[2] Vgl. diesbezüglich auch die Stellungnahme des Ludwig Boltzmann Instituts für Menschenrechte (BIM) im Begutachtungsverfahren über die Regierungsvorlage zum „Bundesgesetz, mit dem das Telekommunikationsgesetz 2003 – TKG 2003 geändert wird" vom 21. Mai 2007.
[3] Das Europäische Parlament hatte in jener legislativen Entschließung, mit welcher der Rahmenbeschluss des Jahres 2004 zur Einführung der Vorratsdatenspeicherung abgelehnt wurde, gefordert *„die Notwendigkeit der geplanten Vorratsspeicherung unzweifelhaft zu belegen"*. Bevor abschließend über neue Maßnahmen entschieden werden könne, wären zwingend die Ergebnisse einer solchen Studie über die Notwendigkeit zu berücksichtigen (Entschließung vom 27. September 2005, A6-0174/2005, unter der Überschrift: *„III. Ergebnis"*, 2. Absatz). Diesen Notwendigkeitsnachweis blieben die Befürworter der Vorratsdatenspeicherung erstaunlicherweise auch

von auf ihn/sie rückführbaren Daten entgehen. Im Bereich der Festnetz- aber auch der Mobiltelefonie genügt etwa die Verwendung von öffentlichen Telefonzellen oder Wertkartenhandys (falls dafür keine Stammdatenspeicherung vorgesehen ist) bzw. von im (nicht EU-)Ausland angemeldeten Handys, um der auf konkrete Personen rückführbaren Datenaufzeichnung mit sehr bescheidenem Mehraufwand zu entgehen. Der Aufzeichnung von E-Mail-Daten im Rahmen der Vorratsspeicherung kann durch Verwendung außereuropäischer E-Mail-Provider entgangen werden. Umso wahrscheinlicher ist, dass terroristische oder andere kriminelle Vereinigungen, deren Bekämpfung die Vorratsspeicherung im Grunde bezweckt, über ungleich bessere technische Möglichkeiten und Kenntnisse verfügen. Für Mitglieder solcher Vereinigungen ist es daher unzweifelhaft ein Leichtes, der auf sie rückführbaren Datenaufzeichnung zu entgehen. Voraussichtlich erfasst werden somit aber die Daten jener Personen oder „Durchschnittsbürger", die entweder keine Kenntnis von der Vorratsspeicherung ihrer Daten haben, oder die kein Interesse an den Tag legen, derselben zu entgehen.

Da einem massiven Eingriff in die durch Art 8 EMRK geschützten Positionen ein nur sehr bescheidener Mehrwert für Zwecke der Strafverfolgung gegenübersteht, stellt sich die Frage, ob die Vorratsspeicherung der Verkehrs- und Standortdaten aller EU-BürgerInnen nicht unverhältnismäßig ist und somit eine Verletzung besagter Rechte darstellt. Es ist zu erwarten, dass Betroffene, gestützt auf Art 8 EMRK, sowie NetzwerkbetreiberInnen aus dem Blickwinkel einer Verletzung des Rechts auf Achtung des Eigentums iSv Art 1 des 1. Zusatzprotokolls zur EMRK rechtliche Schritte ergreifen werden, die zu einer Überprüfung der Grundrechtskonformität der jeweiligen innerstaatlichen Umsetzung und somit in weiterer Folge indirekt zu einer Überprüfung des Regelungsgehaltes der Richtlinie 2006/24/EG führen werden. Jedenfalls verbleibt den Betroffenen wie auch den NetzwerkbetreiberInnen die Möglichkeit, gegen eine abschlägige innerstaatliche Entscheidung des Höchstgerichts – und unbeachtlich einer Entscheidung des EuGH in einem allfälligen Vorabentscheidungsverfahren – vor dem EGMR Beschwerde zu erheben. Dieser könnte im Zuge der Überprüfung des innerstaatlichen Rechtsakts zu dem Ergebnis gelangen, dass die Richtlinie – für deren Erlassung letztendlich sämtliche EU-Mitgliedstaaten die Verantwortung tragen – Art 8 EMRK und Art 1 des 1. ZPEMRK verletzt, woraus die Notwendigkeit der Aufhebung des innerstaatlichen Umsetzungsaktes und in weiterer Folge der dieser innerstaatlichen Umsetzung zu Grunde liegenden Richtlinie folgen könnte.

Aus diesen Gründen wird daher – sollte es in Österreich zu einer Umsetzung der Richtlinie kommen – im Sinne einer eingriffsminimierenden Vorgangsweise und zur Vermeidung frustrierter Aufwendungen empfohlen, die Richtlinie nur im unbedingt erforderlichen Mindestaus-

bis zur Beschlussfassung über die Richtlinie schuldig und beschränkten sich statt dessen auf die Darstellung von Einzelfällen, in denen entsprechende Daten zur Aufklärung beigetragen hätten.

maß umzusetzen. Um den oben dargestellten grundrechtlichen Bedenken zu begegnen, wird hier empfohlen, entsprechende Rechtsschutzvorkehrungen zu treffen. Dazu zählt jedenfalls, einen Zugriff auf die Daten nur mit Richtervorbehalt zu erlauben. Daneben sollte auch eine (zumindest nachträgliche) Informationspflicht gegenüber den Betroffenen normiert werden, soweit dies nicht dem Ermittlungszweck eindeutig entgegensteht. Schließlich können auch effektive Kontrollbefugnisse einer unabhängigen Stelle, beispielsweise der Datenschutzkommission, den Grundrechtseingriff etwas näher in Richtung Verhältnismäßigkeit zu rücken.

Die soeben angesprochenen, durch die Vorgaben der Richtlinie aufgeworfenen Bedenken haben wohl dazu beigetragen, dass die Richtlinie in zahlreichen Mitgliedsstaaten noch nicht wie vorgesehen umgesetzt ist. Dieser Bericht gibt einen Überblick über Umfang, Regulierungsweise und Probleme der Umsetzung in ausgesuchten Mitgliedsstaaten.

Die Analyse zeigt erhebliche Unterschiede in Umsetzungsgeschwindigkeit, –intensität und -form. Darüber hinaus lassen sich auch erhebliche Divergenzen im regulatorischen Grundansatz identifizieren. Während einige Staaten (etwa Deutschland) einen traditionellen ordnungsstaatlichen Ansatz verfolgen, der die Nichtbefolgung der Speicherverpflichtungen mit erheblichen Bußgeldzahlungen bedroht, wird in Großbritannien etwa ein stark marktgetriebener Ansatz verfolgt: (Nur) wer die Speicherverpflichtungen wie vorgesehen erfüllt, kann mit einem Ersatz der anfallenden Kosten rechnen.

Thema der vorgelegten Studie sind jedoch nicht nur die rechtlichen Umsetzungsmaßnahmen, sondern auch Fragen der Reaktion der Zivilgesellschaft auf die normativen Vorgaben. In allen untersuchten Mitgliedsstaaten lassen sich nämlich – freilich in ihrer Intensität sehr stark divergierende – Formen des politischen Widerstands gegen die Umsetzung der Richtlinie identifizieren, wodurch sich möglicherweise die erheblichen Verzögerungen bei der Umsetzung erklären lassen: Ende 2007, nach Ablauf der Umsetzungsfrist, hatten erst neun der 27 Mitgliedsstaaten nach Einschätzung der Kommission die erforderlichen Maßnahmen gesetzt.[4]

Die Widerstände sind, wenngleich in der Regel gegen nationale Umsetzungsmaßnahmen gerichtet, nicht nur auf nationale Bewegungen beschränkt. So geht auf europäischer Ebene etwa die EDRi[5] aktiv gegen die Vorratsdatenspeicherung vor. Die EDRi ist an sich keine

[4] Nämlich Deutschland, Frankreich, Großbritannien, Spanien, Belgien, Lettland, Dänemark, Tschechien und Estland; vgl. MMR 2008, Heft 2, XXIII, online unter http://rsw.beck.de/rsw/shop/default.asp?sessionid=275FE178F9964453A067ED9F17155542&docid=252821&docClass=NEWS&site=MMR&from=mmr.10 (zuletzt abgerufen am 10.03.2008).

[5] European Digital Rights (EDRi) - offizielle Website, abrufbar unter: http://www.edri.org (zuletzt abgerufen am 10.03.2008).

Bürgerrechtsorganisation sondern ein internationaler Dachverband bestehend aus derzeit 28 nationalen Vereinigungen[6], die sich in 17 europäischen Staaten für den Schutz der Privatsphäre in der Informationsgesellschaft einsetzen. Die im Juni 2002 in Berlin gegründete Vereinigung mit Sitz in Brüssel startete im Juli 2005, ähnlich wie die Organisation Privacy International",[7] bereits vor Erlass der Richtlinie zur Vorratsdatenspeicherung eine übergreifende Online-Kampagne unter dem Motto „Data retention is no solution".[8] In dieser Kampagne hat die EDRi zusammen mit dem niederländischen Internetserviceprovider XS4ALL eine internationale Petition aufgesetzt, um gegen die europäischen Pläne einer Vorratsdatenspeicherung zu mobilisieren.

Gegenwärtig lässt sich feststellen, dass die verschiedenen Mitgliedsorganisationen der EDRi sowie wohl auch alle weiteren nationalen Bürgerrechtsorganisationen eher auf nationaler Ebene versuchen, gegen die vollzogenen oder geplanten Umsetzungen der Richtlinie zur Vorratsdatenspeicherung vorzugehen. Dahinter steht das Sekundärziel, die europäische Richtlinie als Grundlage für die nationalen Umsetzungen zu beseitigen. Letzteres könnte – abgesehen von der bereits unter Punkt 1. angesprochenen Möglichkeit zur Erhebung einer Beschwerde an den EGMR – auch dadurch erreicht werden, dass ein nationales Verfassungsgericht eine anhängige Verfassungsbeschwerde dem EuGH zur Entscheidung vorlegt und dieser die Richtlinie direkt für europarechtswidrig erklärt. So könnte ein EU-weites Ergebnis erzielt werden. Da der Bürger nicht unmittelbar vor dem EuGH klagen kann, müssen sich die zivilgesellschaftlichen Organisationen an die nationalen Gerichte wenden. Besonders problematisch ist das in denjenigen Mitgliedstaaten der Europäischen Union, in denen es gar kein nationales Verfassungsgericht gibt, vor dem die Kommunizierenden oder auch die Kommunikationsunternehmen eine Verletzung ihrer Grundrechte rügen könnten.[9]

Bezüglich der internationalen Zusammenarbeit stellte Cristof Remmerts-Fontes, Sprecher, Organisator und Koordinator des Arbeitskreises Vorratsdatenspeicherung, Anfang dieses Jahres in einem Interview mit Jetzt.de fest, dass der Austausch von Informationen und die Vernetzung der Gegenmaßnahmen auf europäischer Ebene bisher leider noch nicht reibungslos verliefe. Es fehle an Dynamik. In einigen Staaten seien zu wenige Personen orga-

[6] Eine Liste aller Mitglieder und Links zu deren Webpräsenz, abrufbar unter: http://wiki.dataretentionisnosolution.com/index.php/Main_Page (zuletzt abgerufen am 10.03.2008).
[7] Siehe: „PI forges coalition to call on European Parliament to reject data retention", http://www.privacyinternational.org/article.shtml?cmd[347]=x-347-478392&als[theme]=PL%20Comms%20Surveillance (zuletzt abgerufen am 10.03.2008).
[8] Online-Kampagne „Data retention is no solution" abrufbar unter: http://www.dataretentionisnosolution.com/index.php?lang=de (zuletzt abgerufen am 10.03.2008).
[9] So beispielsweise in Schweden.

nisiert, obwohl man guten Willen zeige, in anderen sei man offensichtlich insgesamt nicht so gut über die europäische Sicherheitsgesetzgebung informiert.[10]

II. Zusammenfassung und Auswertung der Länderergebnisse

1. Überblick

Bereits umgesetzt wurde die Richtlinie von den Staaten:

- Deutschland
- Frankreich
- Spanien
- Großbritannien
- Dänemark und
- Tschechien

Belgien stellt insofern einen Sonderfall dar, als zwar bisher keine förmliche Umsetzung erfolgt ist, jedoch nach Einschätzung der Kommission die Vorgaben der Richtlinie bereits hinreichend erfüllt sind.

Bislang nicht umgesetzt wurde die Richtlinie von den Staaten:

- Griechenland
- Irland
- Italien
- Portugal
- Niederlande und
- Schweden.

Art 15 Abs 3 der Richtlinie eröffnete den Mitgliedstaaten die Möglichkeit, die Umsetzung bezüglich der Speicherung von Kommunikationsdaten betreffend Internetzugang, Internet-Telefonie (sog. Voice over IP oder kurz VoIP) und Internet-E-Mail bis 15.März 2009 aufzuschieben. Um diese in Anspruch zu nehmen, musste der jeweilige Mitgliedstaat bei Annahme der RL eine entsprechende Erklärung abgeben.

[10] Das vollständige Interview ist abrufbar unter: http://jetzt.sueddeutsche.de/texte/anzeigen/414201 (zuletzt abgerufen am 10.03.2008).

Einen Vorbehalt erklärt und (zumindest teilweise) auch beansprucht haben die Staaten:

- Deutschland
- Belgien
- Griechenland
- die Niederlande und
- Schweden.

Einen Vorbehalt erklärt, jedoch nicht beansprucht, haben die Staaten:

- Großbritannien und
- Tschechien.

Keinen Vorbehalt erklärt haben die Staaten:

- Frankreich
- Irland
- Italien
- Portugal
- Spanien und
- Dänemark.

Zu den Mitgliedstaaten, welche die Richtlinie bereits umgesetzt haben

1.1.1 Art der Umsetzung

Während die Umsetzung in Deutschland, Spanien und Tschechien ausschließlich durch vom jeweiligen Parlament verabschiedete Gesetze erfolgte, wurden in Frankreich, Belgien und Dänemark lediglich die Rahmenbedingungen gesetzlich abgesteckt, die detaillierte Ausführung hingegen fand auf dem Verwaltungsweg (durch Verordnung bzw. Erlass) statt. In Belgien steht eine förmliche und detaillierte Umsetzung durch königlichen Verwaltungsakt bislang allerdings noch aus.

Im Vereinigten Königreich war eine längerfristige Datenspeicherung – wenngleich nicht verpflichtend – bereits in einem Gesetz vom Dezember 2001 (Anti-Terrorism, Crime and Security Act 2001) vorgesehen, welches die Vorgaben der Richtlinie über weite Strecken vorwegnahm. Deren förmliche Umsetzung erfolgte, dem englischen Recht zur Ausführung von Gemeinschaftsrecht entsprechend, durch eine Verordnung, mit der die freiwillige Datenspeicherung zur Pflicht wurde.

1.1.2 Speicherdauer

Mit einer Speicherfrist von 6 Monaten am unteren Limit bleiben nur Deutschland und Tschechien, wobei es in beiden Ländern Ausnahmen gibt. So sind in Deutschland Stammdaten bis zum Ende des auf das Vertragsende folgenden Jahres zu speichern. In Tschechien müssen die sog. „Uniform Resource Identifier“ (URI) – das sind jene Daten, die eine angewählte Resource (Daten, Website, etc.) identifizieren – nur 3 Monate gespeichert werden. Dabei handelt es sich um Daten, die auch Rückschlüsse auf den Inhalt einer Kommunikation zulassen.

In den Ländern Frankreich, Dänemark, dem Vereinigten Königreich und Spanien beträgt die Frist 1 Jahr für alle Kategorien von zu speichernden Daten. Eine Ausnahme besteht in Spanien, weil die Exekutive dort gegenüber einem Provider eine Reduktion auf 6 Monate oder eine Erweiterung auf 2 Jahre erklären kann, wobei keine inhaltlichen Voraussetzungen hierfür normiert sind. Belgien sieht gesetzlich eine Speicherung von mindestens 12 und höchstens 36 Monaten vor, die Konkretisierung bleibt dem noch ausständigen Verwaltungsakt vorbehalten.

Erwähnenswert ist hier auch die derzeit bestehende Regelung in Irland. Dieses Land hat zwar die Richtlinie noch nicht umgesetzt, doch deckt sich die bestehende Rechtslage bereits über weite Teile mit den Vorgaben der Richtlinie. Demzufolge sind alle verfügbaren Daten für einen Zeitraum von 3 Jahren zu speichern, eine Umsetzung würde voraussichtlich eine Verringerung auf höchstens 2 Jahre mit sich ziehen.

1.1.3 Datenkategorien

Die Richtlinie 2006/24/EG schreibt zusammengefasst die Vorratsspeicherung der folgenden Kategorien von Daten vor, wobei diese bei der Erfassung eines Kommunikationsvorgangs immer in Bezug auf Sender und Empfänger zu speichern sind.

- **Daten zur Identifizierung des Nutzers eines Kommunikationsvorgangs**

Darunter sind die sog. Stammdaten zu verstehen, also Name und Anschrift des Teilnehmers oder registrierten Benutzers, evtl. auch die Kundennummer. Diese Daten hat der Dienstanbieter bei der ersten Anmeldung eines Nutzers für einen Dienst bzw. für den Anschluss zu speichern. Eine eindeutige Zuordnung eines Kommunikationsvorgangs zu einem bestimmten Benutzer ist nur durch Verknüpfung mit den entsprechenden Verkehrsdaten möglich.

- **Daten zur Anschlusskennung bzw. zur Identifizierung der Endgeräte**

Dies sind Daten wie Rufnummer, dynamische oder statische IP-Adresse, Benutzerkennung, Mobilteilnehmerkennung (IMSI), Mobilfunkgerätekennung (IMEI), digitaler Teilnehmeranschluss (DSL).

- **Daten zur Bestimmung von Uhrzeit und Dauer der Kommunikation**

Darunter versteht man Beginn und Ende des Kommunikationsvorgangs, Datum und Uhrzeit der An- und Abmeldung beim verwendeten Dienst (Internet-E-Mail oder Internet-Telefonie-Dienst).

- **Daten zur Bestimmung des verwendeten Telefon- bzw. Internetdienstes**

Dies sind etwa „normale" Gesprächsverbindung, Mailbox, SMS, MMS, Anrufweiterleitung, Konferenzschaltung, Internet-E-Mail, FTP, etc.

- **Daten zur Bestimmung des Standorts mobiler Geräte**

Darunter versteht man die Standortkennung (Cell-ID) bzw. die Zuordnung der Cell-ID zu einem geographischen Standort zum Zeitpunkt der Datenspeicherung.

Alle bereits erfolgten nationalen Umsetzungsmaßen erfüllen diese Vorgaben und verpflichten damit die Provider, oben genannte Daten zu speichern. Wenngleich die Definitionen und Einteilungen der Datenkategorien Unterschiede aufweisen, decken sich diese im Ergebnis doch mit jenen der Richtlinie. Nicht von Art 5 Abs 1 RL 2006/24/EG umfasste Datenkategorien sind solche, die „Aufschluss über den Inhalt einer Kommunikation geben (dazu nachfolgend).

Von den untersuchten Mitgliedstaaten kennt nur Belgien eine Regelung, wonach von einer Speicherpflicht für Daten abzusehen ist, die von der Richtlinie eindeutig umfasst sind. Ausdrücklich untersagt ist die Speicherung und Verwendung von Standortdaten bei Mobilfunkdiensten, Ausnahmen existieren bei Notrufen. Hier ist jedoch nochmals darauf hinzuweisen, dass Belgien streng genommen noch gar nicht umgesetzt hat, wenngleich die EU Kommission die bestehende Rechtslage soweit für richtlinienkonform hält.

1.1.4 Daten die „Aufschluss über den Inhalt einer Kommunikation" geben

Solche Daten sind gemäß Art 5 Abs 2 ausdrücklich vom Anwendungsbereich der Richtlinie 2006/24/EG ausgenommen. Wenn ein Mitgliedstaat den Dienstanbietern dennoch die Speicherung solcher Daten vorschreiben, kann er sich nicht auf die Richtlinie berufen. Vorwegzunehmen ist, dass es in keinem der untersuchten Länder eine Ausnahme von der Spei-

cherpflicht solcher *Verkehrs*daten gibt, die einen Rückschluss auf den Kommunikationsinhalt ermöglichen (zB eine E-Mail an soforthilfe@anonymealkoholiker.de). Allerdings ist aus dem Wortlaut der Richtlinie selbst nicht erkennbar, ob solche Verkehrsdaten unter das Verbot des Art 5 Abs 2 fallen sollen.

In den ausgewählten Ländern gibt es Vorschriften, die dem Verbot der Inhaltsdatenerfassung widersprechen, nur ausnahmsweise und in folgendem Umfang:

Frankreich sieht im *Gesetz vom 21. Juni 2004 für das Vertrauen in die Informationswirtschaft* Speicher- und Registrierungspflichten für Access- und Hostprovider vor, um die Verursacher rechtswidriger Inhalte zu identifizieren. Hierzu ist auch die Erfassung von Daten notwendig, die Aufschluss über den Inhalt zulassen. Tschechien schreibt bezüglich der Verwendung von Internetdiensten die Speicherung von sog. „Uniform Resource Identifier" (URI) vor. Das sind jene Daten, die eine angewählte Resource identifizieren. Es handelt sich dabei um eine Zeichenfolge zur Bezeichnung einer Internet-Ressource mit Hilfe des Typs der Ressource (Datei, Textseite, Bild, Programm etc.) und ihrer Adresse, also ihres Speicherorts im Internet. Bekanntestes Beispiel ist die sog. „URL" einer Website (http://www.usw.undsofort.at). Dabei handelt es sich nicht bloß um Daten, die *Rückschlüsse* auf den Inhalt einer Kommunikation zulassen, vielmehr wird der Inhalt eindeutig identifiziert. In welchem Umfang solche URI gespeichert werden müssen, war für die Studienautoren leider nicht eruierbar. Eine konkret geplante Gesetzesnovelle soll hier aber jedenfalls noch Einschränkungen bringen. Dänemark verlangt bei Internetdiensten die Speicherung jedes „Kommunikationspakets", mit dem eine Internetsitzung begonnen oder beendet wird, bzw. jedes 500sten IP-Pakets. Dies ermöglicht Rückschlüsse auf die angewählten Internetseiten.

1.1.5 Daten die vom Netzbetreiber „erzeugt oder verarbeitet werden"

Darunter sind Daten zu verstehen, die beim Betrieb des Kommunikationsdienstes ohnehin „anfallen". Die Speicherpflicht nach der Richtlinie bezieht sich nur auf solche Daten und fordert daher nicht, dass die Anbieter darüber hinausgehende Datensätze erzeugen müssen. Die im vorigen Abschnitt genannten Verkehrs- und Standortdaten (bei Mobilfunk) werden allerdings bei jedem Kommunikationsvorgang „erzeugt", weil diese den Verbindungsaufbau technisch überhaupt ermöglichen. Damit reduziert sich die Einschränkung faktisch auf jene Fälle, in denen aufgrund der Verrechnungsart keine Stammdaten des Nutzers erhoben werden, etwa bei Prepaid-Diensten (z.B. „Wertkartenhandy) oder Flatrate-Tarifen. Dann nämlich werden zwar Daten erzeugt, die eine Identifizierung der Endeinrichtung zulassen, jedoch keinen unmittelbaren Rückschluss auf eine bestimmte Person ermöglichen. Nur insofern – also in Bezug auf die Stammdaten – stimmt die in der Debatte regelmäßig anzutreffende

Aussage, dass sich die Richtlinie auf Daten beschränke, welche die Anbieter ohnehin für Abrechnungszwecke speichern. Die Verkehrsdaten fallen also jedenfalls in den Anwendungsbereich der Richtlinie. Dennoch können diese Informationen für Ermittlungen wertvoll sein, weil die Provider in der Regel zumindest zuordnen können, wann und wo z.B. ein Wertkartenhandy gekauft oder aktiviert wurde (Beispiel: Ermittlung des Täters im „Saliera-Fall", der eine SMS mit seinen Forderungen an die Versicherung mittels Wertkartenhandy schickte. Aufgrund der Erhebung, wann und wo die Prepaid-SIM-Karte erworben wurde, lieferten die Videoaufzeichnungen des Handy-Shops entscheidende Hinweise zum Täter).

Der Wortlaut der Richtlinie 2006/24/EG verbietet nicht, die Erhebung und Speicherung solcher Daten innerstaatlich vorzuschreiben, die nicht bereits beim Betrieb „erzeugt oder verarbeitet werden". Allerdings bleibt es für solche Daten bei den Grundsätzen der Datenschutzrichtlinie 2002/58/EG. Das ist zwar für Telefonie wenig bedeutsam, mangels Verkehrsdaten, die nicht erzeugt oder verarbeitet werden. Nicht so bei Internetanwendungen. Beispielsweise beinhaltet ein E-Mail-Header allerlei Verkehrsdaten, die vom Provider weder erzeugt noch verarbeitet werden, etwa den verwendeten Client; die Speicherung dieser Information dürfte das nationale Recht nicht anordnen, weil insoweit die Datenschutzrichtlinie nicht durch die VorratsRL eingeschränkt wird[11] und die DSRLeK insoweit Vollharmonisierung bezweckt.[12]

Folgende Länder haben dennoch abweichende Regelungen getroffen:

In Deutschland müssen TK-Dienstanbieter die Stammdaten vor der Freischaltung eines Dienstes auch ohne Notwendigkeit für Abrechnungszwecke erheben und speichern. Diese Registrierungspflicht besteht bereits seit der TKG-Novelle 2004 und wurde im Zuge der Richtlinienumsetzung weiter verschärft. Außerdem müssen auch Veränderungen von Verkehrsdaten durch Anonymisierungs- und Weiterleitungsdienste erfasst und gespeichert werden.

In Spanien existieren detaillierte Regelungen zur Speicherpflicht von Kundendaten bei Prepaid-Diensten und Flatrate-Tarifen. Für derartige Dienste, die vor Inkrafttreten des Gesetzes aktiviert wurden, müssen die Daten auch nachträglich innerhalb von 2 Jahren von den Providern erhoben werden. Auch Frankreich, Tschechien und Dänemark sehen Ähnliches vor.

[11] Vgl. den durch Art. 15 VorratsRL eingefügten Art. 15 Abs. 1a DSRLeK.
[12] Vgl. EuGH EuZW 2004, 245 [252: Abs. 96] hinsichtl. DSRL.

1.1.6 Daten von Anrufen „bei denen keine Verbindung zustande kommt“

Eine Speicherung solcher Daten ist gemeinschaftsrechtlich nur geboten, wenn diese Daten schon bisher „erzeugt oder verarbeitet *und* gespeichert (bei Telefoniedaten) oder protokolliert (bei Internetdaten) werden“, sei es zur Fakturierung oder aus technischen Gründen. Auch hiervon bleibt die Zulässigkeit abweichender nationaler Regelungen unberührt.

Eine Speicherpflicht bei „erfolglosen Anrufen“ besteht in den Mitgliedstaaten:

- Deutschland, aber nur, soweit die Daten ohnehin bereits gespeichert werden; also nicht über die Richtlinienvorgaben hinaus. Weil in Deutschland bislang kein TK-Anbieter erfolglose Verbindungsversuche verrechnet, geht diese Pflicht bzgl. Telefonie praktisch ins Leere. Nicht so für Internetdienste, weil hier regelmäßig eine Protokollierung für Zwecke der Störungsbehebung erfolgt.
- Spanien
- Dänemark
- Großbritannien
- Tschechien plant, die Erfassung solcher Daten mit der bevorstehenden Gesetzesnovelle einzuführen.

1.1.7 Verwendung der gespeicherten Daten

Der Zweck und damit auch die Rechtfertigung der vorrätigen Speicherung der oben beschriebenen Daten liegen in der Verhinderung bzw. Verfolgung von schweren Straftaten und der Gefahrenabwehr (siehe auch Art 1 Abs 1 RL 2006/24/EG). Was als „schwere“ Straftat einzustufen ist, ergibt sich prinzipiell aus dem gemeinsamen Nenner der europäischen Rechtskulturen, wobei hier den Staaten wohl ein einigermaßen großer Spielraum zur Verfügung stehen wird. Jedenfalls existiert keine Beschränkung auf terroristische Bedrohungen oder organisierte Kriminalität. In einigen Ländern sind ausdrücklich auch „mittels Telekommunikation begangene Straftaten“ umfasst.

Dementsprechend sind in allen Mitgliedstaaten, die bereits umgesetzt haben, die Strafverfolgungsbehörden sowie allenfalls die Geheimdienste als zuständige Behörden iSd Art 4 der Richtlinie berechtigt, die Herausgabe der Daten von den Netzbetreibern und Dienstanbietern zu verlangen. In den meisten Ländern ist vorgesehen, dass die Behörde dafür grundsätzlich jeweils im Einzelfall einen richterlichen Beschluss einzuholen hat (Richtervorbehalt), Ausnahmen bestehen bei Gefahr im Verzug. Die richterliche Kontrolle ergibt sich notwendig aus dem Gebot der Verhältnismäßigkeit im Zusammenhang mit der Europäischen Menschen-

rechtskonvention (EMRK, insb. Art 8, Schutz des Privat- und Familienlebens), worauf sich auch die Richtlinie in Art 4 ausdrücklich bezieht.

Darüber hinaus stellt sich die Frage, ob uU eine Herausgabe von Daten an private zulässig oder gar geboten ist oder die gespeicherten Daten vom Anbieter selbst für eigen Zwecke (über die Abrechnung hinaus, z.B. gezielte Werbemaßnahmen aufgrund erstellter Nutzerprofile) verwendet werden dürfen. Dergleichen ist in keinem der untersuchten Mitgliedstaaten vorgesehen, in Deutschland, England und Dänemark existieren sogar ausdrückliche Verbote.

Hier sollen knapp zusammengefasst die nationalen Verfahrensbestimmungen zur Verwendung der Daten dargestellt werden, soweit sie im Rahmen der Erhebungen zugänglich waren:

Während in Frankreich die entsprechende Regelung des Telekommunikationsgesetzes Polizei und Gendarmerie für Zwecke der Terrorismusbekämpfung den Zugriff auf bestimmte Verkehrsdaten ohne weitere gerichtliche Überprüfung ermöglicht, können die gespeicherten Vorratsdaten in Dänemark und Spanien ausschließlich durch richterlichen Beschluss zugänglich gemacht werden. In Spanien haben neben den Sicherheitsbehörden und dem Geheimdienst auch die leitende Zollbehörde Zugriff auf die gespeicherten Daten. In Deutschland steht die Übermittlung der Daten an die zuständigen Behörden unter Richtervorbehalt, bei Gefahr im Verzug genügt jedoch eine Anordnung des Staatsanwalts. Keine richterliche Anordnung ist für einen Datenzugriff der Nachrichtendienste vorgesehen. Großbritannien kennt für den Datenzugriff keinen Richtervorbehalt. Außerdem dürfen die Daten auch für Zwecke verwendet werden, die über jene der Richtlinie hinausgehen, beispielsweise zur Steuerfahndung. Darüber hinaus ist der Innenminister ermächtigt, weitere Gründe per Verordnung festzulegen.

In Belgien ist gesetzlich bereits vorgesehen, dass die rechtswidrige Verwendung von Inhaltsdaten (auch: „Abhören“) durch Beamte wie auch durch Privatpersonen mit erheblichen Strafen bedroht ist. Genaue Bestimmungen, welche Stellen nach welchem Verfahren die Daten verwenden dürfen, sind durch die noch ausstehende Verordnung zu regeln. In Griechenland, wo die Richtlinie bislang noch nicht formal umgesetzt wurde, steht die anlassfallbezogene Speicherung von Verkehrsdaten zum Zweck der Strafverfolgung ebenfalls unter Richtervorbehalt, in besonders dringenden Fällen genügt eine Anordnung des zuständigen Staatsanwalts mit nachträglicher gerichtlicher Überprüfung. Auch der portugiesische Gesetzesentwurf sieht Ähnliches vor.

1.1.8 Kontrolle und Rechtsschutz

Art 7 der Richtlinie sieht vor, dass die Mitgliedstaaten dafür Sorge zu tragen haben, dass im Hinblick auf die auf Vorrat gespeicherten Daten bestimmte Grundsätze der Datensicherheit eingehalten werden. Insbesondere sind dabei geeignete technische und organisatorische Maßnahmen zu treffen, um die Daten entsprechend zu schützen, um sicherzustellen, dass nur besonders ermächtigte Personen Zugriff auf die Daten erhalten und dass die Daten am Ende der Vorratsspeicherungsfrist grundsätzlich vernichtet werden.

In Belgien etwa sind das rechtswidrige „Abhören" und die Verwendung von Inhaltsdaten mit erheblichen Strafen bedroht. In Deutschland ist hinsichtlich der Datensicherheit im Allgemeinen die „im Bereich der Telekommunikation erforderliche Sorgfalt" zu beachten und ergeben sich die rechtlichen Anforderungen an die technischen Schutzmechanismen aus dem Bundesdatenschutzgesetz. Verletzungen der Speicherpflichten bzw. datenschutzrechtlicher Bestimmungen können mit Bußgeldern bis zu € 250.000,- (im Bereich Datenschutz) bzw. € 500.000,- (im Bereich der Speicherpflichten) belegt werden. Darüber hinaus sind die Ermittlungsbehörden an spezielle Datenkennzeichnungspflichten gebunden. Frankreich schreibt den Telekommunikationsdienstleistern im Rahmen des Telekommunikationsgesetzes jene Datensicherheitsmaßnahmen vor, die für die Verhinderung einer Verwendung von auf Vorrat gespeicherten Daten zu anderen als den gesetzlich definierten Zwecken notwendig sind und sieht für den Fall des Verstoßes gegen Speicher- oder Löschungsverpflichtungen Geldbußen bis zu € 75.000,- vor. In Großbritannien sieht das Datenschutzgesetz zwar vor, dass Daten zu vernichten sind, sobald der Zweck, zu dem sie ursprünglich gespeichert wurden, nicht mehr vorliegt. Allerdings wird u. a. in einer Stellungnahme der Regierung darauf verwiesen, dass eine Abweichung von diesen Vorgaben aus Gründen der nationalen Sicherheit verhältnismäßig und gerechtfertigt sei. In Tschechien wird hinsichtlich geeigneter Datensicherheitsmaßnahmen auf die allgemeinen datenschutzrechtlichen Bestimmungen im Bezug auf die Verwendung personenbezogener Daten verwiesen.

Gemäß Art 9 der Richtlinie benennt jeder Mitgliedstaat eine oder mehrere öffentliche Stellen, die für die Kontrolle der Anwendung der von den Mitgliedstaaten zur Umsetzung von Art 7 erlassenen Vorschriften bezüglich der Sicherheit der Vorratsdaten in seinem jeweiligen Hoheitsgebiet zuständig ist bzw. sind. Diese Stellen, die ihre Kontrolltätigkeit „*in völliger Unabhängigkeit*" wahrnehmen sollen, können, so die Richtlinie in Art 9 Abs 2, dieselben sein, auf die Art 28 der Richtlinie 95/46/EG Bezug genommen wird.

Tatsächlich machen einige der im Rahmen dieser Studie untersuchten Mitgliedstaaten von der in Art 9 Abs 2 genannten Möglichkeit Gebrauch und siedeln die in der Richtlinie vorgese-

henen Kontrollbefugnisse bei jenen Stellen an, die allgemein für die Überwachung der Einhaltung datenschutzrechtlicher Vorgaben im Bereich der Verwendung von personenbezogenen (Verkehrs-)Daten zuständig sind (vgl etwa die Länderberichte zu Belgien, Deutschland, Großbritannien, Portugal, Tschechien). Andere Staaten (wie zB Griechenland) haben eigene Kontrollstellen eingerichtet bzw. die notwendigen Kontrollbefugnisse auf Ministeriumsebene angesiedelt (vgl Frankreich). Inhaltlich sind die faktischen Kontrollmöglichkeiten der betreffenden Behörden unterschiedlich ausgestaltet.

Während in Belgien der König auf Vorschlag des Justizministers und nach Anhörung der Datenschutzkommission und der Telekommunikationsbehörde die Bedingungen festlegt, unter denen Verkehrs- bzw. Stammdaten zu speichern und zu verarbeiten sind, ist in Deutschland etwa die Bundesnetzagentur für die Überwachung der Einhaltung der Speicherpflichten zuständig. In Frankreich wiederum wird über die Legitimität von Auskunftsbegehren im Hinblick auf Verkehrsdaten im Innenministerium entschieden. Griechenland hat eigens eine Behörde für die Sicherstellung von Privatsphäre und Sicherheit von Informationen und Kommunikation eingerichtet, um das Post- und Fernmeldegeheimnis bzw. die Kommunikationsfreiheit zu schützen. Im Gesetzesentwurf Portugals ist vorgesehen, die portugiesische Datenschutzkommission aufgrund der besonderen Vertraulichkeit der Vorratsdaten zu verpflichten, die Datenbank über jene Personen, die Zugriff auf die vorrätig gespeicherten Daten haben sollen, laufend aktuell zu halten. Großbritannien hat als überwachende Behörde den britischen Information Commissioner vorgesehen, der im Falle der Nichteinhaltung der Vorgaben im Hinblick auf Datenschutz und Datensicherheit befugt ist, die Rolle eines Ombudsmannes einzunehmen. In Tschechien werden die Kontrollbefugnisse im Bereich der Vorratsdatenspeicherung vom Büro für den Schutz personenbezogener Daten wahrgenommen.

Um einen effektiven grundrechtskonformen Rechtsschutz zu ermöglichen, wäre eine (zumindest nachträgliche) Information über den Datenzugriff den Betroffenen gegenüber geboten. Wer nicht weiß, dass seine Daten abgefragt wurden, kann dagegen auch keine Rechtsschutzinstrumente in Anspruch nehmen. Was die Rechte der Betroffenen anbelangt, waren die diesbezüglich seitens der Mitgliedstaaten zur Verfügung gestellten Informationen allerdings eher spärlich.

In Deutschland erfolgt eine Information der von einem konkreten Datenzugriff betroffenen Personen je nach Regelung der diversen Spezialgesetze, wobei im Hinblick auf eine Auskunftserteilung über Bestandsdaten die Erteilung von Informationen an den/die Betroffene/n nicht vorgesehen ist, bei Verkehrsdaten grundsätzlich schon.

In Großbritannien etwa ist eine Information der individuellen Nutzer über die Datenspeicherung generell nicht normiert. Lediglich eine (anonymisierte) Aufzeichnung der Zugriffe auf Daten ist von den Anbietern jährlich als Statistik an den Innenminister zu übermitteln. Im Hinblick auf Tschechien ist anzumerken, dass eine generelle Informationspflicht gegenüber betroffenen Personen sich schon aufgrund der geltenden strafrechtlichen Bestimmungen ergibt, wonach Personen über etwaige gegen sie bestehende Verdachtsmomente im Bezug auf ein Delikt und diesbezüglich einzuleitende Aufklärungsschritte informiert werden muss.

1.1.9 Kostenersatz an Netzbetreiber

Generell ist anzumerken, dass in den meisten Mitgliedstaaten, die die Speicherung von Daten auf Vorrat bereits praktizieren, keine expliziten Kostentragungsregelungen vorgesehen wurden. In Dänemark etwa ist der Justizminister zwar dazu ermächtigt, den Kostenersatz per Verordnung zu regeln, er hat bislang von dieser Möglichkeit allerdings keinen Gebrauch gemacht. Den Telekommunikationsdienstleistern in Deutschland werden die mit der Vorratsdatenspeicherung an sich verbundenen Kosten ausdrücklich nicht ersetzt, wobei aber ein Ersatz jener Kosten erfolgt, die im Zusammenhang mit der Beantwortung von Auskunftsersuchen entstehen. Auch in Spanien wurden keine Kostentragungsregeln in das Gesetz aufgenommen, hauptsächlich mit der Begründung, dass im Telekommunikationssektor ohnehin eine ausreichende Gewinnspanne vorläge, um die zusätzlichen Kosten abzudecken. Frankreich, Großbritannien und Tschechien hingegen sehen ausdrücklich vor, dass TK-Dienstleister für ihre Speicherpflichten ökonomisch zu entschädigen sind.

Zu den Mitgliedstaaten, welche die Richtlinie nicht umgesetzt haben

1.2.1 Gründe für die Unterlassung der Umsetzung

Die Gründe, aus denen jene Mitgliedstaaten, die die Richtlinie bislang noch nicht umgesetzt haben, dies bis dato unterlassen haben, fußen überwiegend in politischen Erwägungen.

In Griechenland etwa, wo Pläne einer etwaigen Umsetzung noch nicht bekannt sind, liegen diese Gründe hauptsächlich an der derzeitigen innenpolitischen Situation. Vor allem die Wahlen im vergangenen Jahr haben Verzögerungen im Hinblick auf die Umsetzung politischer Vorhaben mit sich gebracht. Bis heute liegen daher keinerlei Informationen vor, die zeitliche bzw. inhaltliche Umsetzungspläne der Richtlinie 2006/24/EG erkennen lassen würden. Irlands Situation ist jener Griechenlands insoweit ähnlich, als auch hier innenpolitische Gründe für die Nichtumsetzung ausschlaggebend sind. Im Juli 2006 reichte Irland beim Eu-

ropäischen Gerichtshof in Luxemburg eine Klage gegen die Richtlinie 2006/24/EG ein (AZ C-301-06) und beantragte, die Richtlinie aus formellen Gründen für nichtig zu erklären. Die Wahl der Binnenmarktkompetenz (Art 95 EGV) als Rechtsgrundlage sei insoweit fehlerhaft, als die Richtlinie klar und eindeutig auf die Bekämpfung schwerer Verbrechen gerichtet sei und nicht darauf abziele, Mängel des Binnenmarktes zu beheben. Seither zeigt sich im Hinblick auf die Umsetzungsbestrebungen erheblicher Widerwille und wird in parlamentarischen Debatten stets auf das anhängige Verfahren verwiesen. Seit September 2006 ist überdies ein nationales Verfahren vor dem irischen High Court gegen die Umsetzungsbestrebungen anhängig, in dem hauptsächlich die Vereinbarkeit der entsprechenden Normen mit der irischen Verfassung und der EMRK in Frage gestellt wird. Auch im Bezug auf Italien muss die derzeitige politische Lage als eine der möglichen Ursachen für die Nichtumsetzung der Richtlinie in Betracht gezogen werden. Was Portugal anbelangt, so lassen sich die Gründe für das bisherige Ausbleiben einer Umsetzung der Richtlinie nicht mit Gewissheit feststellen. Trotz Vorliegens eines Gesetzesentwurfes und augenscheinlicher Priorität des Umsetzungsvorhabens im Parlament lassen sich keine konkreten Aussagen im Hinblick auf den Umsetzungszeitpunkt treffen.

Die Klage Irlands hat in der griechischen Diskussion über die Umsetzung der Richtlinie praktisch keine Erwähnung gefunden. Auch in Italien, den Niederlanden, Portugal und Schweden konnte ein Einfluss der irischen Klage nicht explizit festgestellt werden.

1.2.2 Umsetzungspläne der säumigen Mitgliedstaaten

Weder in Griechenland, noch in Italien liegen bislang konkrete Umsetzungspläne hinsichtlich der Richtlinie 2006/24/EG vor. Im Bezug auf Irland wird von Bestrebungen berichtet, die Richtlinie trotz anhängigen Verfahrens vor dem EuGH so rasch wie möglich – zB im Wege einer Verordnung – umzusetzen, wobei die geltende Rechtslage sich ohnedies bereits jetzt in vielen Teilen mit den Inhalten der Richtlinie deckt. Die Richtlinienumsetzung wird voraussichtlich zu einer Reduzierung der Speicherfrist auf maximal zwei Jahre führen und inhaltlich die Speicherung anonymer Dienste miteinbeziehen.

In Portugal wurde der Gesetzesentwurf, der darauf abzielt, die Richtlinie in portugiesisches Recht zu transformieren, bereits vom Parlament genehmigt. Die darin vorgesehenen auf Vorrat zu speichernden Datenkategorien gleichen jenen in Art 5 der Richtlinie. Auch Daten, die aus „erfolglosen Anrufsversuchen“ hervorgehen, sind von der Speicherpflicht mitumfasst. Als Speicherfrist, die sich ebenfalls im Rahmen der Richtlinie bewegt, ist ein Zeitraum von einem Jahr vorgesehen. Zugang zu den gespeicherten Daten sollen im Wesentlichen die portugie-

sischen Justiz- und Kriminalpolizeibehörden auf Basis einer richterlichen Anordnung bekommen.

Was Schweden betrifft, so wurde seitens einer eigens dafür eingesetzten Kommission bis November 2007 ein Umsetzungsentwurf ausgearbeitet, der auch bereits die Umsetzung der internetbezogenen Datenkategorien mit einbezieht. Laut Entwurf, der derzeit vom Schwedischen Gesetzesrat geprüft wird und der von der zuständigen Datenschutzbehörde bereits kritisiert wurde, sollen die Vorgaben der Richtlinie teilweise durch eine Novellierung des Gesetzes für elektronische Kommunikation und teilweise per Verordnung umgesetzt werden. Explizite Vorgaben im Hinblick auf Datensicherheitsmaßnahmen sieht der Entwurf derzeit nicht vor, wobei hierzu allerdings eine Ermächtigung der TK-Regulierungsbehörde aufgenommen wurde. Inhaltlich sieht der Entwurf die Speicherung sämtlicher in der Richtlinie vorgesehenen Datenkategorien für eine einheitliche Dauer von zwölf Monaten vor. Der Entwurf geht dabei insoweit über die Richtlinie hinaus, als hinsichtlich der Mobiltelefonie nicht nur die Standortdaten zu Beginn, sondern auch am Ende eines Gespräches bzw. auch Kommunikationsdaten erfolgloser Anrufversuche erfasst werden. Zugang zu den gespeicherten Daten sollen – auf Basis unterschiedlicher Rechtsgrundlagen – sämtliche zur Verbrechensbekämpfung berufenen Behörden und Gerichte haben.

In den Niederlanden existiert zur Umsetzung der Richtlinie ein Gesetzesvorschlag vom 11.Dezember 2006, der die Datenspeicherung für einen Zeitraum von 18 Monaten für alle Datenkategorien einheitlich vorsieht. Die Kategorien entsprechen dem Art 5 Abs 1 der Richtlinie 2006/24/EG, doch ist eine mögliche Erfassung darüber hinausgehender Daten durch Verordnung im Gesetzesentwurf vorgesehen. Die Erfassung von „erfolglosen Verbindungen“ ist aktuell nicht vorgesehen. Eine Verwendung der gespeicherten Daten für Zwecke des Providers selbst (z.B. Marketing) ist nicht zulässig. Aus dem Entwurf geht nicht eindeutig hervor, welche Personen oder Behörden Zugriff auf die Daten haben sollen. Kontrollinstanz ist der Wirtschaftsminister gemeinsam mit der nationalen Datenschutzbehörde (Dutch DPA), welche die Einhaltung der gesetzlichen Bedingungen zur Speicherung und Verwendung der Daten überwachen. Außerdem ist eine finanzielle Abgeltung für die Anbieter im Vorschlag enthalten.

Reaktionen seitens der Zivilgesellschaft

Ganz allgemein kann gesagt werden, dass die Entwicklungen im Hinblick auf die Vorratsspeicherung von Telekommunikationsdaten seitens der Zivilgesellschaft mit regem Interesse verfolgt wird. Während man in Staaten wie Dänemark, Italien, Frankreich, Portugal, Schwe-

den[13], Spanien und Tschechien – zumindest teilweise – ablehnend auf die Richtlinie reagierte und unterschiedlichste Protestaktionen ins Leben rief, sind in Belgien, Griechenland und Großbritannien nennenswerte Reaktionen auf das Thema Vorratsdatenspeicherung bisher ausgeblieben. In Irland hingegen zeigt sich, ausgehend von der Nichtregierungsorganisation (NGO) *Digital Rights Ireland*, überaus deutliche Kritik an der Speicherung von Daten auf Vorrat. Es bleibt abzuwarten, ob es nach Ausgang des derzeit anhängigen nationalen Verfahrens zu einer Prüfung der Verfassungsmäßigkeit der bestehenden (Antiterror-)Gesetzgebung bzw. der die Richtlinie umsetzenden Verordnung kommen wird. Am deutlichsten ausgeprägt ist der zivile Widerstand gegen die Vorratsdatenspeicherung naturgemäß aber in Deutschland. Schon im Jahr 2005 formierte sich dort ein *Arbeitskreis Vorratsdatenspeicherung*, der in einer gemeinsamen Erklärung der einzelnen Unterstützerorganisationen u. a. die verdachtsunabhängige Speicherung von TK-Daten als inakzeptabel bezeichnet. Parallel dazu wurden in Deutschland zahlreiche Demonstrationen sowie Informationsveranstaltungen zum Thema organisiert. Unter der URL www.vorratsdatenspeicherung.de wurde seitens des Arbeitskreises ein Internetportal eingerichtet, das eine Fülle an Hintergrundinformationen bereithält. Im Dezember 2007 wurde schließlich eine Verfassungsbeschwerde gegen das die Richtlinie umsetzende Gesetz eingebracht, die mittlerweile von rund 30.000 BürgerInnen betrieben wird. Neben weiteren Verfassungsbeschwerden wurde das Gesetz auch seitens des *Bündnis 90/Die Grünen* angegriffen, und zwar in Form eines Organstreitverfahrens. Im Gegensatz dazu gibt es natürlich auch BefürworterInnen der Vorratsdatenspeicherung in Deutschland, die etwa erkennen lassen, dass die Sicherheitsbehörden zur Aufklärung bzw. Verhinderung schwerer Straftaten auf derlei Daten angewiesen seien und die Speicherung von TK-Daten auf Vorrat daher von essentieller Bedeutung sei.

[13] In Schweden wurde der Umsetzungsentwurf etwa auch seitens der Datenschutzbehörde kritisiert, die in ihrer Stellungnahme unter anderem festhielt, dass das Vorhaben der Vorratsdatenspeicherung auch aus grundrechtlichen Erwägungen als bedenklich einzustufen sei.

III. Einzelergebnisse der Länderrecherche

Belgien

Zusammenfassung: Belgien hat die Richtlinie bisher nicht förmlich umgesetzt. Derzeit werden mehrere Umsetzungsentwürfe erarbeitet und diskutiert, die vertraulich und also nicht öffentlich zugänglich sind. Zivilgesellschaftlicher Widerstand ist erkennbar, aber nicht deutlich ausgeprägt.

Frage 1:

Welche Regelungen wurden von denjenigen ausgewählten Mitgliedstaaten getroffen, die die Richtlinie bereits umgesetzt haben?

In Belgien wurde die Richtlinie bisher nicht umgesetzt, obwohl der Staat nach Einschätzung der Kommission die europarechtlichen Vorgaben an die Vorratsdatenspeicherung bereits erfüllt.[14] Die einschlägigen Bestimmungen der geltenden Rechtslage vor Richtlinienumsetzung finden sich insbesondere im belgischen Telekommunikationsgesetz,[15] das aus dem Jahr 2005 stammt. In Belgien wird – ähnlich wie in Frankreich – zunächst der Grundsatz einer Löschungs- bzw. Anonymisierungverpflichtung von Verkehrsdaten eingeführt (Art. 122 Abs. 1 belg. TKG).[16] Es gibt jedoch Ausnahmen von diesem Grundsatz, die zu gelten haben für Kooperationszwecke mit Strafverfolgungsbehörden auf gesetzlicher Grundlage sowie für Untersuchungszwecke zur Identifizierung des Missbrauchs von Telekommunikationsanlagen und –dienstleistungen.[17]

Ausdrücklich untersagt wird – von Fällen der Zustimmung des Nutzers abgesehen – die Speicherung und Verwendung von Standortdaten, die bei mobilen Telekommunikationsdienstleistungen anfallen (Art. 123 belg. TKG); seit einer Novelle im April 2007 ist von diesem Grundsatz jedoch in Fällen des Notrufs abzuweichen (Art. 123 Abs. 5 belg. TKG). Ebenfalls ausdrücklich verboten sind die Zurkenntnisnahme von Inhaltsdaten (Art. 124 Abs. 1) sowie von die Kommunikationsteilnehmer identifizierenden Daten (Art. 124 Abs 2) und die Verwendung von Daten, zu deren Erhebung keine Berechtigung bestand, unabhängig da-

[14] Vgl. MMR 2008, Heft 2, XXIII, online unter http://rsw.beck.de/rsw/shop/default.asp?sessionid=275FE178F9964453A067ED9F17155542&docid=252821&docClass=NEWS&site=MMR&from=mmr.10 (zuletzt abgerufen am 10.03.2008).

[15] Loi relative aux communications électroniques vom 13. Juni 2005, online zB unter http://www.ibpt.be/GetDocument.aspx?forObjectID=949&lang=fr (zuletzt abgerufen am 10.03.2008).

[16] « Les opérateurs suppriment les données de trafic concernant les abonnés ou les utilisateurs finals de leurs données de trafic ou rendent ces données anonymes, dès qu'elles ne sont plus nécessaires pour la transmission de la communication. »

[17] Art. 122 Abs. 2: „L'alinéa 1er s'applique sans préjudice du respect des obligations de coopération, prévues par ou en vertu de la loi, avec :
1° les autorités compétentes pour la recherche ou la poursuite d'infractions pénales ;

von, ob deren Zurkenntnisnahme gewollt oder ungewollt vonstatten ging (Art. 124 Abs. 5). Das rechtswidrige „Abhören“ und die Verwendung von Inhaltsdaten durch Beamte (Art. 259 bis Code pénal)[18] wie Nichtbeamte (Art. 314bis Code pénal[19]) ist mit erheblichen Strafen bedroht – allerdings existiert eine weit reichende Ausnahme zugunsten des Geheimdienstes (Art. 259 bis Abs. 5 Code pénal). Die Rechtsschutzgarantien des § 124 belg. TKG wie auch der Art. 259bis und 314bis des Code pénal werden jedoch durch Art. 125 belg. TKG in wichtigen Fällen aufgehoben: Hervorzuheben ist hier insbesondere, dass Art. 125 Nr. 1 eine Generalausnahme für Fälle normiert, in denen die Verarbeitung und Speicherung gesetzlich vorgesehen sind[20]; hier handelt es sich wohl um die „Einbruchsstelle“ zur noch zu erwartenden Normierung der Verbindungsdatenspeicherung anlässlich der Richtlinienumsetzung.[21] Schon jetzt freilich normiert Art. 126 bedeutende Ausnahmen vom Grundsatz des Speicherverbots für Verkehrs- und –stammdaten. Der König kann auf dem Verwaltungsweg auf Vorschlag des Justizministers und nach Anhörung der Datenschutzkommission (Commission pour la protection de la vie privée) und der Telekommunikationsbehörde[22] die Bedingungen fixieren, unter denen Verkehrs- und Nutzerstammdaten zu speichern und zu verarbeiten sind, unter anderem für Zwecke der Verhinderung und der Verfolgung von Straftaten. Derart

---

2° le service de médiation pour les télécommunications pour la recherche de l'identité de toute personne ayant effectué une utilisation malveillante d'un réseau ou d'un service de communications électroniques.

[18] « § 1. Sera puni d'un emprisonnement de six mois à deux ans et d'une amende de cinq cents francs à vingt mille francs ou d'une de ces peines seulement, tout officier ou fonctionnaire public, dépositaire ou agent de la force publique qui, à l'occasion de l'exercice de ses fonctions, hors les cas prévus par la loi ou sans respecter les formalités qu'elle prescrit :

1° soit, intentionnellement, à l'aide d'un appareil quelconque, écoute ou fait écouter, prend connaissance ou fait prendre connaissance, enregistre ou fait enregistrer, pendant leur transmission, des communications ou des télécommunications privées, auxquelles il ne prend pas part, sans le consentement de tous les participants à ces communications ou télécommunications;

2° soit, avec l'intention de commettre une des infractions mentionnées ci-dessus, installe ou fait installer un appareil quelconque;

3° soit, sciemment, détient, révèle ou divulgue à une autre personne le contenu de communications ou de télécommunications privées, illégalement écoutées ou enregistrées, ou dont il a pris connaissance illégalement, ou utilise sciemment d'une manière quelconque une information obtenue de cette facon. »

[19] § 1. Sera puni d'un emprisonnement de six mois à un an et d'une amende de deux cents francs à dix mille francs ou d'une de ces peines seulement, quiconque :

1° soit, intentionnellement, à l'aide d'un appareil quelconque, écoute ou fait écouter, prend connaissance ou fait prendre connaissance, enregistre ou fait enregistrer, pendant leur transmission, des communications ou des télécommunications privées, auxquelles il ne prend pas part, sans le consentement de tous les participants à ces communications ou télécommunications;

2° soit, avec l'intention de commettre une des infractions mentionnées ci-dessus, installe ou fait installer un appareil quelconque.

§ 2. Sera puni d'un emprisonnement de six mois à deux ans et d'une amende de cinq cents francs à vingt mille francs ou d'une de ces peines seulement, quiconque détient, révèle ou divulgue sciemment à une autre personne le contenu de communications ou de télécommunications privées, illégalement écoutees ou enregistrées, ou dont il a pris connaissance illégalement, ou utilise sciemment d'une manière quelconque une information obtenue de cette facon.

Sera puni des mêmes peines quiconque, avec une intention frauduleuse ou à dessein de nuire, utilise un enregistrement, légalement effectué, de communications ou de télécommunications privées.

[20] Art. 125 Abs. 1 Nr. 1: „Les dispositions de l'article 124 de la présente loi et les articles 259bis et 314bis du Code pénal ne sont pas applicables : 1° lorsque la loi permet ou impose l'accomplissement des actes visés ; »

[21] Zumal es dem Gesetzgeber selbstverständlich immer freisteht, im Rahmen der verfassungsrechtlichen Vorgaben Gesetze zu derogieren; vgl. dazu in concreto auch Commission de la protection de la vie privée, Avant projet de loi relatif aux communications électroniques, online unter http://www.privacycommission.be/fr/docs/Commission/2004/avis_08_2004.pdf, 7 (zuletzt abgerufen am 10.03.2008).

[22] Institut belge des services postaux et des télécommunications, http://www.ibpt.be/fr/1/Home/Accueil/Accueil.aspx (zuletzt abgerufen am 10.03.2008).

erhobene Daten sind mindestens zwölf und höchstens 36 Monate aufzubewahren. Genaueres hat wiederum ein königlicher Verwaltungsakt zu fixieren.[23] Belgien untersagt auch die Verwendung technischer Hilfsmittel, die die Erhebung und Verarbeitung der Daten erschweren oder verhindern – mit Ausnahme der Verschlüsselung von Inhaltsdaten (Art. 127 § 2 belg. TKG). Eine Umsetzung der Vorratsdatenspeicherung auf dem Verwaltungsweg ist somit gesetzlich vorbereitet.

Frage 2:

Was sind die Gründe, aus denen die übrigen ausgewählten Mitgliedstaaten noch nicht umgesetzt haben?

Die Gründe liegen, soweit erkennbar, in der angespannten globalpolitischen Situation Belgiens. Bekanntlich wird der Staat nach einer monatelangen Regierungs- und Verfassungskrise nach den Wahlen am 10. Juni 2007 derzeit von einer kommissarischen Regierung geführt.

Frage 3:

Welche Umsetzungspläne verfolgen jene Mitgliedstaaten, die die Richtlinie bislang noch nicht umgesetzt haben, in zeitlicher bzw. inhaltlicher Hinsicht?

Es existieren konkrete, konkurrierende Umsetzungsvorschläge[24], die jedoch inhaltlich nicht bekannt sind und von denen daher auch nicht klar ist, ob einer oder Teile mehrerer umgesetzt werden sollen. Auch über den Zeitplan lassen sich wegen der derzeitigen innenpolitischen Situation keine belastbaren Aussagen treffen.

Frage 4:

Wie wirkt sich die im Juli 2006 von Irland eingebrachte Klage vor dem Europäischen Gerichtshof auf die Umsetzungsbestrebungen dieser Staaten aus?

Soweit erkennbar, spielt die Klage in der innenpolitischen Diskussion keine Rolle.

Frage 5:

Welche Reaktionen seitens der Zivilgesellschaft lassen sich in den ausgewählten Mitgliedstaaten erkennen?

[23] http://www.privacycommission.be/fr (zuletzt abgerufen am 10.03.2008).
[24] Persönliche Mitteilung zweier wissenschaftlicher Mitarbeiter des Interdisciplinary Center for Law and ICT an der KU Leuven an den Autor.

Die Reaktionen der Zivilgesellschaft sind schwach ausgeprägt. Politischer Lobbyismus gegen die Vorratsdatenspeicherung wird von der Liga voor de Mensenrechten (www.mensenrechten.be) und auch dem Verband der Internetserviceanbieter (www.ispa.be) betrieben, die politische Durchschlagskraft scheint jedoch, soweit erkennbar, gering zu sein.

Dänemark

Zusammenfassung: Dänemark hat die Richtlinie seit 15. September 2007 vollständig in nationales Recht umgesetzt. Die Umsetzung geht in manchen Bereichen über die Vorgaben der Richtlinie hinaus. Widerstand in der Zivilgesellschaft ist vorhanden, jedoch nach einer mehr als vierjährigen Umsetzungsphase mit etlichen Kompromissen zuletzt nur mehr schwach ausgeprägt.

Frage 1:

Welche Regelungen wurden von denjenigen ausgewählten Mitgliedstaaten getroffen, die die Richtlinie bereits umgesetzt haben?

Die endgültige Umsetzung der Richtlinie erfolgte durch den von Justizministerium und Ministerium für Wissenschaft und Technologie gemeinsam entworfenen Verwaltungserlass (Verordnung) Nr. 988 vom 28. September 2006 „über die Registrierung und Speicherung von Informationen über den Datenverkehr von Nutzern elektronischer Kommunikationsnetzwerke und –dienste“[25], welcher am 15. September 2007 in Kraft getreten ist. Die gesetzliche Grundlage findet sich im Absatz 786 des dänischen Justizverwaltungsgesetzes und wird durch den Erlass implementiert bzw. näher ausgeführt. Die entsprechende Erweiterung dieser Bestimmung zur Einführung der Vorratsdatenspeicherung wurde bereits im Juni 2002 als Teil des dänischen „Antiterror-Pakets“ vom dänischen Parlament angenommen[26], also beträchtliche Zeit vor Verabschiedung der EG-Richtlinie. Damit korrespondiert auch, dass die dänische Ratspräsidentschaft im zweiten Halbjahr 2002 bedeutende Impulse zur Vorratsdatenspeicherung auf gemeinschaftsrechtlicher Ebene gesetzt hat.

Der Verwaltungserlass schreibt eine Speicherdauer von einem Jahr vor (Art 9 Erlass Nr. 988/2006), einheitlich für alle Kategorien der zu speichernden Daten. Entsprechend der Richtlinie betrifft dies bei Festnetz- und Mobiltelefonie folgende Daten: Telefonnummer; Kundennummer, Name und Adresse des Nutzers; IMSI/IMEI Nummer; Uhrzeit und Dauer; Daten zur Bestimmung des Dienstes (Mailbox, Rufweiterleitung, Konferenz, SMS, MMS); Daten zur Standortbestimmung bei Mobiltelefonen.

Folgende Daten sind bei Internetsitzungen (einschließlich E-Mail und Voice over IP) zu speichern: IP-Adresse; Benutzerkennung; E-Mail Adresse; Kundennummer, Name und Adresse des Nutzers; Telefonnummer des Einwahlknotens; Daten zur Bestimmung des Dienstes (Port-Nummer und Transportprotokoll); Uhrzeit und Dauer einer Sitzung; bei Drahtlosen Zu-

[25] Auf Dänisch: ”Bekendtgørelse nr. 988 af 28/09/2006 om udbydere af elektroniske kommunikationsnets og elektroniske kommunikationstjenesters registrering og opbevaring af oplysninger om teletrafik (logningsbekendtgørelsen)”.

gangspunkten (sog. Hot Spots) Ort und Identität derselben. Diese Daten sind stets hinsichtlich Sender und Empfänger einer Kommunikation zu speichern, bei VoIP und E-Mail aber nur bezüglich der vom Provider selbst angebotenen Dienste (also nicht bzgl. hotmail, yahoo! und ähnlichen).

Gespeichert werden muss zudem jedes „Kommunikationspaket", mit der eine Internetsitzung begonnen oder beendet wird – oder, wenn dies technisch nicht durchführbar ist, jedes 500ste „Kommunikationspaket". Diese Regelung ist deshalb problematisch, weil damit (auch) Inhaltsdaten erfasst werden, die eine Identifizierung der angewählten Internetseiten ermöglicht,[27] obwohl die Richtlinie dies in Art 5 Abs 2 ausdrücklich untersagt. Außerdem geht die dänische Regelung insofern über die Vorgaben der Richtlinie hinaus, als sie auch Daten umfasst, die in den gegenwärtigen Systemen der Service-Provider erzeugt und verarbeitet, jedoch nicht für Abrechnungszwecke benötigt werden. Soweit also Daten bei Prepaidkarten oder Flatrate- Tarifen bereits erzeugt und verarbeitet werden, unterliegen auch diese der Speicherpflicht. Ebenfalls gespeichert werden Daten von Anrufen „bei denen keine Verbindung zustande kommt" (Art 3 Abs 2 RL 2006/24/EG). Der dänische Verwaltungserlass kennt auch keine ausdrückliche Ausnahme von der Speicherpflicht für solche Daten, die „Aufschluss über den Inhalt einer Kommunikation" iSd Art 5 Abs 2 RL 2006/24/EG geben.

Die gespeicherten Daten dürfen ausschließlich zum Zweck der Untersuchung und Verhütung von Straftaten verwendet werden (Art 1 Erlass Nr. 988/2006). Es ist sicherzustellen, dass die Daten zu keinem anderen Zweck missbraucht werden. Die Verwendung der vorrätig gespeicherten Daten ist nur durch die dänische Polizei zulässig, die dafür einen gerichtlichen Beschluss einzuholen hat (Art 783 f Justizverwaltungsgesetz).

Die Anbieter sind nicht verpflichtet, in neue Systeme zu investieren, sie müssen aber rund um die Uhr gegenüber behördlichen Anfragen zur Verfügung stehen. Die Vorschriften richten sich an alle kommerziellen Provider, während gemeinnützige Anbieter, Wohnungsverbände mit weniger als 100 Einheiten, Bibliotheken, Universitäten und andere gemeinnützige öffentliche Institutionen ausgenommen sind. Der Justizminister ist ermächtigt, den Kostenersatz gegenüber den Providern per Verordnung zu regeln, was bislang aber noch nicht geschehen ist.

Wie oben dargestellt beinhaltet die dänische Umsetzung bereits die Speicherung von Kommunikationsdaten betreffend Internetzugang, Internet-Telefonie und Internet-E-Mail, zumal

[26] Act No. 378 vom 6.Juni 2002.
[27] Aus der Korrespondenz des Autors mit Mr. Martin Futtrup, Mitarbeiter des Danish Institute for Human Rights.

Dänemark auch keinen Aufschub gem. Art 15 Abs 3 der Richtlinie in Anspruch genommen hat.

Frage 2:
Was sind die Gründe, aus denen die übrigen ausgewählten Mitgliedstaaten noch nicht umgesetzt haben?

Nicht einschlägig für Dänemark.

Frage 3:
Welche Umsetzungspläne verfolgen jene Mitgliedstaaten, die die Richtlinie bislang noch nicht umgesetzt haben, in zeitlicher bzw. inhaltlicher Hinsicht?

Nicht einschlägig für Dänemark.

Frage 4:
Wie wirkt sich die im Juli 2006 von Irland eingebrachte Klage vor dem Europäischen Gerichtshof auf die Umsetzungsbestrebungen dieser Staaten aus?

Die irische Klage hatte keinen Einfluss auf die Umsetzung der Richtlinie in Dänemark.

Frage 5:
Welche Reaktionen seitens der Zivilgesellschaft lassen sich in den ausgewählten Mitgliedstaaten erkennen?

Die im Juni 2002 vom dänischen Parlament verabschiedeten Maßnahmen zur Verhütung von Terrorismus und zur Bekämpfung der Internetkriminalität (z.B. Verbreitung von Kinderpornografie), welche auch die grundsätzliche Einführung der Vorratsdatenspeicherung umfaßten, wurden zu diesem Zeitpunkt von der Mehrheit der Dänischen Bevölkerung unterstützt, nicht zuletzt vor dem Hintergrund der Ereignisse des 11. September 2001. Gleichwohl geriet das vorgeschlagene System während der vierjährigen Entwurfsphase wiederholt ins Kreuzfeuer der Kritik, insbesondere von Seiten der Telekom- und IT-Industrie, der Datenschutzbehörden, des Danish Institute for Human Rights und diverser NGOs. Im Zentrum stand dabei, dass es sich um einen massiven und unangemessenen Eingriff in die Privatsphäre handelt, der sehr viele Menschen betrifft, obwohl gleichzeitig dem Großteil der gespeicherten Daten keine Relevanz bei der Verbrechensbekämpfung zukommt. Dabei wurde auch die Effektivität der Regelung in Frage gestellt, zumal eine Umgehung aufgrund der vie-

len Ausnahmen, etwa bei öffentlichen Computern (z.B. Universitäten, Bibliotheken) oder internationaler Freemail-Dienste (z.B. Yahoo!, Hotmail, GMail) keine Schwierigkeit darstelle.[28] Während der Umsetzungsphase hat die dänische Regierung einige Vorschläge (insbesondere der vorhergehende vom Frühjahr 2004) in die Diskussion eingebracht, die wesentlich intensivere Eingriffe vorsahen. Gleichzeitig waren Vertreter der Zivilgesellschaft (Provider, betriebliche Interessenvertreter, NGOs) in den Prozess eingebunden, so wurde diesen auch der letzte Verordnungsentwurf im Juli 2006 zur Begutachtung und Stellungnahme bis 10. August 2006 vorgelegt. Weil die nunmehrige Umsetzung viele der früheren Kritikpunkte berücksichtigt, vor allem solche aus der Telekom- und IT-Branche, wurde diese letztlich ohne großen Aufschrei akzeptiert.[29]

[28] Siehe dazu den zweiwöchentlich erscheinenden Newsletter von European Digital Rights(EDRi), auf deutsch unter http://www.unwatched.org/node/844 (zuletzt abgerufen am 10.03.2008).
[29] http://www.unwatched.org/node/191 (zuletzt abgerufen am 10.03.2008).

Deutschland

Zusammenfassung: Deutschland hat die Richtlinie bereits in nationales Recht umgesetzt; die volle Wirksamkeit der Umsetzung wird im Jahr 2009 erreicht. Die deutsche Umsetzung erfasst auch Anonymisierungsdienste. Die Weitergabe der auf Vorrat gespeicherten Verkehrsdaten ist bisher nur für die Zwecke der Verfolgung schwererer oder mittels Telekommunikation begangener Straftaten zulässig; die Verarbeitung der Daten durch den TK-Diensteanbieter ist auch zulässig, soweit dies für eine vorgeschriebene Auskunft über Stammdaten erforderlich ist. Die Richtlinie und ihre Umsetzung sind gesellschaftlicher Kritik ausgesetzt; es hat mehrere Kundgebungen und Aktionen gegeben. Mehrere zehntausend Bürger haben gegen das Umsetzungsgesetz Verfassungsbeschwerde erhoben.

Frage 1:

Welche Regelungen wurden von denjenigen ausgewählten Mitgliedstaaten getroffen, die die Richtlinie bereits umgesetzt haben?

Umsetzung und Wirksamkeit

Deutschland hat die Richtlinie 2006/24/EG durch das *Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG* umgesetzt. Neben der Umsetzung der Richtlinie sind vor allem Regelungen zur Überwachung der Telekommunikation von Berufsgeheimnisträgern Gegenstand des Gesetzes. Deutschland setzt die Bestimmungen der Richtlinie selbst durch Änderungen im Telekommunikationsgesetz (TKG) um. Die gem. Art. 4 der Richtlinie ausdrücklich dem nationalen Recht überlassene Verwendung der gespeicherten Daten wird durch geänderte Bestimmungen in der StPO geregelt. Der Gesetzentwurf wurde von der Bundesregierung am 27. April 2007 in den Bundesrat[30] und am 27. Juni 2007 in den Bundestag[31] eingebracht. Dort wurde er am 21. Dezember 2007 beschlossen und schließlich am 31. Dezember 2007 verkündet[32] und ist im wesentlichen[33] entsprechend seines Art. 16 mit Beginn des Jahres 2008 in Kraft getreten. Obwohl das Gesetz bereits in Kraft getreten ist, ist es noch nicht voll wirksam. Es gelten noch Übergangsfristen gem. § 150 Abs. 12b TKG: Internetanbieter (Access-, Email- und VoIP-Provider) müssen die Speicherpflichten aus dem Gesetz erst spätestens am 1. Januar 2009 erfüllen. Deutschland schöpft damit die durch seine Erklärung[34] bis zum 15. März 2009 verlängerte Umsetzungsfrist für den Bereich der Internet-Verbindungsdaten nicht voll aus. Hinsichtlich der „klassischen" TK-Diensteanbieter sind zwar die Speicherpflichten mit dem Jahr 2008 in Kraft getreten, allerdings können Sanktionen nach § 149 TKG für Verstöße gegen die Speicherpflicht auch insoweit erst ab 1. Januar 2009

[30] BR-Drs. 275/07.
[31] BT-Drs. 16/5846.
[32] BGBl. I Nr. 70/2007, 31.12.2007, S. 3198.
[33] Die wenigen Ausnahmen betreffen nicht die Richtlinienumsetzung.

verhängt werden. Die Bundesregierung will vorerst nichts unternehmen, um die wirksame Anwendung des Gesetzes in der Praxis zu fördern oder zu untersuchen; sie setzt darauf, dass das Gesetz ohne weiteres bis zum Ablauf der Übergangsfristen von den TK-Diensteanbietern zur Anwendung gebracht wird.[35]

Umfang der Speicherpflichten

Deutschland hat die Speicherpflichten scharf nach Bestands- und Verkehrsdaten getrennt. § 111 TKG wurde dahingehend geändert, dass TK-Diensteanbieter die Bestandsdaten[36] vor Freischaltung vollständig erheben und speichern müssen, und zwar auch soweit die Daten für betriebliche Zwecke nicht erforderlich sind (z. B. bei Guthabenkarten). Die Speicherungspflichten für Verkehrsdaten ergeben sich hingegen aus § 113a TKG. Soweit die Richtlinie also die Speicherung von Name und Anschrift von Telekommunikationsteilnehmern verlangt (z. B. Art. 5 Abs. 1 lit. a Nr. 1 Ziff. ii), ist diese Information nur mittelbar gespeichert, nämlich durch Zusammenführung der Datensätze mittels der Anschlusskennung, die sowohl Bestandteil der Bestands- als auch der Verkehrsdatensätze ist.

Die von der Richtlinie auf einen Umsetzungskorridor von sechs Monaten bis zwei Jahren festgelegte Speicherungsfrist setzt Deutschland hinsichtlich der Verkehrsdaten mit sechs Monaten um; die Daten sind dann binnen eines weiteren Monats zu löschen, § 113a Abs. 1, 11 TKG. Die Umsetzung am unteren Rand hat die Bundesregierung nach Aufforderung durch den Bundestag vorgeschlagen.[37] Bestandsdaten sind hingegen gem. § 111 Abs. 4 TKG bis zum Ende des auf das Vertragsende folgenden Jahres zu speichern, also mindestens ein und höchstens knapp zwei Jahre über das Vertragsende hinaus. Eine Beauskunftung ist allerdings wegen der nach sechs bis sieben Monaten fehlenden Verkehrsdatensätze nicht mehr möglich, wenn das Auskunftsbegehren auf Bestandsdaten, die nur mittels Verkehrsdaten ermittelbar sind, gerichtet ist. Von der Speicherpflicht in Deutschland sind auch Anonymisierungs- und Weiterleitungsdienste erfasst, § 113a Abs. 6 TKG. Demnach hat, wer Telekommunikationsdienste erbringt und dabei die Verkehrsdaten „verändert", die geänderten Daten und den Zeitpunkt zu speichern. Die Bundesregierung geht davon aus, dass auch Anonymisierungsdienste im Internet ohne weiteres TK-Diensteanbieter im Sinne des Gesetzes sind.[38]

Hinsichtlich der Verkehrsdaten erfolgloser Verbindungen gilt gem. § 113a Abs. 5 TKG, dass die Verkehrsdaten dann auf Vorrat zu speichern sind, wenn sie vom TK-Diensteanbieter ohnehin zulässigerweise gespeichert werden; gem. § 96 Abs. 2 TKG gehören zu den zulässi-

[34] Erklärung Deutschlands, ABl. L 105 vom 13.04.2006, S. 63. i.V.m. Art. 15 Abs. 3 Data Retention Richtlinie.
[35] Antwort auf die Anfrage der Bundestagsabgeordneten Leutheusser-Schnarrenberger, BT-Drs. 16/7892, S. 20.
[36] So die deutsche Terminologie für Stammdaten.
[37] BT-Drs. 16/545, S. 4.

gen Zwecken Abrechnung, Einzelverbindungsnachweis und Störungsbeseitigung. Hinsichtlich erfolgloser Telefonanrufe (Nichtmelden, besetzt) dürfte diese Regelung die Speicherung praktisch ausschließen, da in Deutschland kein TK-Diensteanbieter erfolglose Verbindungsversuche berechnet. Relevant hingegen dürfte diese Regelung für Fehlerprotokolle im Bereich der Internet-TK-Dienstleistungen sein. Sofern etwa ein Email-Provider zur (insoweit auch präventiv zulässigen[39]) Störungsbeseitigung Übertragungsfehler protokolliert, unterliegen die protokollierten Verkehrsdaten der Vorratsspeicherung. Die Vorratsspeicherung von Kommunikationsinhalten bleibt ausgeschlossen. Eine Ausnahme von der Speicherungsfrist für etwaige Verkehrsdaten, die als solche bereits Aufschluss über den Inhalt der Kommunikation geben (z.B. eine E-Mail an soforthilfe@anonymealkoholiker.de), ist nicht vorgesehen. Die Speicherung aufgerufener Internetadressen ist ausdrücklich ausgeschlossen, § 113a Abs. 8.

Für die mit der Speicherung der Daten verbundenen Kosten werden TK-Diensteanbieter ausdrücklich nicht entschädigt, § 111 Abs. 5 TKG. Die Beantwortung von Auskunftsersuchen wird hingegen gemäß den Vorschriften der Verordnung nach § 110 Abs. 9 TKG entschädigt.

Verwendung der Verkehrsdaten

Bei der möglichen Verwendung der Daten ist zwischen Bestands- und Verkehrsdaten zu unterscheiden. Die Verwendung der auf Vorrat gespeicherten Verkehrsdaten ist gem. § 113b TKG für die Strafverfolgung, für die Gefahrenabwehr und für geheim- und nachrichtendienstliche Zwecke möglich. § 113b ist insoweit jedoch nur die Erlaubnisnorm für den Diensteanbieter; die Befugnis der zuständigen Behörde muss sich aus dem jeweiligen Gesetz ergeben, und zwar unter ausdrücklicher Bezugnahme auf § 113a TKG. Eine solche Bezugnahme findet sich jedoch bisher allein in § 100g StPO; diese Vorschrift erlaubt – grundsätzlich unter Richtervorbehalt[40] - die Verwendung der Vorratsdaten für die Verfolgung schwerer Straftaten, wobei die Katalogtaten des § 100a StPO für § 100g StPO als Regelbeispiele gelten und die Tat auch im Einzelfall bedeutsam sein muss, sowie für alle mittels Telekommunikation begangener Straftaten, wenn anderweitige Ermittlungsmöglichkeiten aussichtslos erscheinen und die Datenverwendung verhältnismäßig ist. Eine Anordnung nach § 100g StPO kann sich nur gegen den Beschuldigten selbst oder einen mutmaßlichen Nachrichtenmittler richten. Der Katalog des § 100a StPO enthält Straftaten, die unter Berücksichtigung nationalen Ermessens in der europäischen Rechtskultur als schwerere Straftaten gelten dürften, ist jedoch nicht auf terroristische Taten oder organisierte Kriminalität beschränkt. Für die Bedeutsamkeit im Einzelfall will die Bundesregierung „mittlere Kriminalität“ genügen lassen.[41] Nach alter

[38] BT-Drs. 16/5846, S. 71f.
[39] BeckTKG-*Wittern*, § 100 TKG Rn. 6 unter Verweis auf § 109 Abs. 2 TKG.
[40] Bei Gefahr im Verzug genügt staatsanwaltliche Anordnung.
[41] BT-Drs. 16/5846, S. 40.

Rechtslage kam es nur auf den Straftatbestand an, also die abstrakte Schwere der Tat; das Erfordernis der Bedeutsamkeit im Einzelfall folgt der dahingehenden Rechtsprechung des Bundesverfassungsgerichts.[42]

Hinsichtlich der „mittels Telekommunikation" begangenen Straftaten hat sich zwar die auskunftsfähige Datenbasis durch die Vorratsdatenspeicherung vergrößert, gegenüber der bislang möglichen Verwendung (ohnehin gespeicherter) Verkehrsdaten ist hingegen die Anwendung nunmehr auf vollendete Delikte beschränkt und unterliegt der Subsidiaritätsklausel und einer besonderen Verhältnismäßigkeitsprüfung. Als Beispiel für Unverhältnismäßigkeit nennt die Bundesregierung „geringfügige Beleidigungstaten".[43] Fraglich ist die Verhältnismäßigkeit bei urheberrechtlichen Delikten (insb. § 106 UrhG), soweit kein besonderes öffentliches Interesse vorliegt (§ 109 UrhG).

In anderen Gesetzen – insbesondere bezüglich des Bundesnachrichtendienstes, des Verfassungsschutzes und anderer Sicherheitsbehörden – wurde eine Bezugnahme auf § 113a TKG bisher nicht eingefügt. Auch eine Verwendung der Daten im Rahmen privatrechtlicher Auskunftspflichten ist unzulässig; durch die Umsetzung der Durchsetzungsrichtlinie 2004/48/EG in § 101 Abs. 2 UrhG-Entwurf[44] ändert sich nach dem derzeitigen Stand des Gesetzgebungsverfahrens daran nichts. Für die vorgenannten Zwecke kommt daher nur die Verwendung von Verkehrsdaten in Frage, die ohnehin zulässigerweise entsprechend § 96 Abs. 2 TKG (in Umsetzung der Datenschutzrichtlinie für elektronische Kommunikation, 2002/58/EG) gespeichert werden, nicht aber Verkehrsdaten, die nur auf Vorrat gespeichert werden. Das gilt gleichermaßen für die Verwendung für eigene Zwecke des TK-Diensteanbieters.

Verwendung der Bestandsdaten

Die Bestandsdaten unterliegen den Auskunftspflichten nach §§ 112, 113 TKG für die Verfolgung von Straftaten und Ordnungswidrigkeiten, die Gefahrenabwehr und die Tätigkeit von Nachrichtendiensten und Verfassungsschutz. In Literatur und Rechtsprechung ist umstritten, ob Auskünfte über Bestandsdaten, für deren Ermittlung durch den TK-Diensteanbieter Verkehrsdaten verarbeitet werden müssen, den Anforderungen für Bestands- oder für Verkehrsdaten unterliegen.[45] Hinsichtlich der gem. § 113a TKG gespeicherten Daten hat der Gesetz-

[42] BVerfGE 107, 299 [322].
[43] BT-Drs. 16/5846, S. 52.
[44] BT-Drs. 16/5048.
[45] Für die Behandlung als Verkehrsdaten: *LG Ulm*, MMR 2004, 187 [187]; *LG Bonn*, DuD 2004, 628 [628f.]; *Bär*, MMR 2002, 358 [359f.] und 2004, 187 [187] und 2005, 626 [627]; *Dietrich*, GRUR-RR 2006, 145 [147]; Löwe/Rosenberg-*Schäfer*, § 100g Rn. 22 und § 100a Rn. 21; *Splittgerber/Klytta*, K&R 2007, 78 [82]; *Wiebe*, MMR 2005, 828 [829]. Für die Behandlung als Bestandsdaten: *LG Stuttgart*, MMR 2005, 624 [625] und 628 [628f.]; *LG Würzburg*, NStZ-RR 2006, 46 [46]; *LG Hechingen*, NJW-RR 2006, 1196 [1197]; *LG Hamburg*, MMR 2005, 711; *Burhoff*, ZAP 2002, Fach 22, 359 [360]; *Malek*, Strafsachen im Internet, Rn. 397; KKStPO-*Nack*, § 100g Rn. 11;

geber dies entschieden: Die auf Vorrat gespeicherten Verkehrsdaten dürfen für die manuelle Auskunft über Bestandsdaten (§ 113 TKG) verwendet werden, § 113b Satz 1 a.E. TKG. Soweit an Private Auskunft über Bestandsdaten gegeben werden muss,[46] ist die Verwendung der auf Vorrat gespeicherten Verkehrsdaten zu deren Ermittlung unzulässig, da die entsprechenden Normen nicht auf § 113a TKG verweisen.

Sicherheit, Transparenz und Aufsicht

Für die Sicherheit der Vorratsdaten ist gem. § 113a Abs. 10 TKG die „im Bereich der Telekommunikation erforderliche Sorgfalt" zu beachten. Die rechtlichen Anforderungen an den technischen Datenschutz ergeben sich aus § 9 BDSG nebst Anlage (Umsetzung von Art. 17 Abs. 1 Datenschutzrichtlinie 95/46/EG). Zuständige Datenschutzbehörde ist für TK-Diensteanbieter gem. § 115 Abs. 4 TKG der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) in Zusammenarbeit mit dem Referat für TK-Datenschutz der Bundesnetzagentur. Die Bundesnetzagentur ist auch zuständige Behörde für die Überwachung der Einhaltung der Speicherpflichten. Verletzungen der Speicherpflichten einerseits und der Datenschutzbestimmungen andererseits können als Ordnungswidrigkeiten mit Bußgeldern bis zu 250.000 Euro (Datenschutz) bzw. 500.000 Euro (Speicherpflichten) geahndet werden. Für die Ermittlungsbehörden gelten für über § 100g StPO erlangte Verkehrsdaten zusätzlich besondere Datenkennzeichnungspflichten nach § 101 Abs. 3 StPO. Die Information des Betroffenen wird durch das jeweilige Spezialgesetz geregelt. Für die Beauskunftung von Bestandsdaten ist sie nicht vorgesehen. Für die Auskunft über Verkehrsdaten gem. § 100g StPO ist – vorbehaltlich ermittlungstaktischer Hindernisse – die Benachrichtigung der betroffenen Teilnehmer vorgesehen, § 101 Abs. 4 Nr. 6 StPO; die Möglichkeit nachträglichen Rechtsschutzes besteht, § 101 Abs. 7 StPO.

Frage 2:

Was sind die Gründe, aus denen die übrigen ausgewählten Mitgliedstaaten noch nicht umgesetzt haben?

Für Deutschland nicht einschlägig.

Frage 3:

Welche Umsetzungspläne verfolgen jene Mitgliedstaaten, die die Richtlinie bislang noch nicht umgesetzt haben, in zeitlicher bzw. inhaltlicher Hinsicht?

Für Deutschland nicht einschlägig.

Sankol, MMR 2006, 361 [365]. Für die vergleichbare Diskussion in Österreich vgl. *OGH*, MMR 2005, 827 [828] entgegen *OLG Linz*, MMR 2005, 592 [592].

Frage 4:

Wie wirkt sich die im Juli 2006 von Irland eingebrachte Klage vor dem Europäischen Gerichtshof auf die Umsetzungsbestrebungen dieser Staaten aus?

Die Bundesregierung vertritt ausdrücklich die Auffassung, dass die Umsetzungsfristen der Richtlinie ungeachtet der Nichtigkeitsklage Irlands einzuhalten seien. Dies ergebe sich schon aus Art. 242 Satz 1 EG: Da der Nichtigkeitsklage der Suspensiveffekt fehle, sei die Richtlinie fristgerecht umzusetzen.[47] Von den Oppositionsparteien im Deutschen Bundestag wird diese Auffassung jedoch nicht geteilt: Am 26. Mai 2006 beantragte eine große Anzahl von Abgeordneten der Fraktionen von Bündnis 90/Die Grünen, der Linken und der FDP, dass die deutsche Bundesregierung gegen die Richtlinie 2006/24/EG des Europäischen Parlaments und des Rates vom 15. März 2006 (Richtlinie zur Vorratsdatenspeicherung) Nichtigkeitsklage vor dem Europäischen Gerichtshof gemäß Artikel 230 des Vertrags zur Gründung der Europäischen Gemeinschaft (EGV) erheben und somit der Klage Irlands beitreten solle.[48] Begründet wurde dieser Antrag damit, dass die Richtlinie primär dem Zweck der Strafverfolgung diene und sich eine derartige Richtlinie deshalb nicht auf Art. 95 EGV stützen könne, der lediglich der Sicherstellung des Funktionierens des Binnenmarktes diene. Gestützt wird diese Auffassung insbesondere auch auf das Urteil des EuGH zum Umweltstrafrecht vom 13. September 2005 (Kommission gegen Rat C-176/03). Der EuGH bestätigt darin, dass es bei der Wahl der richtigen Rechtsgrundlage auf den Hauptzweck der zu treffenden Regelung ankomme und dass Straf- und Strafprozessrecht grundsätzlich nicht in die Zuständigkeit der Gemeinschaft falle. Insbesondere könne die Zuständigkeit der EG auch nicht durch Art. 47 EUV begründet werden. So habe die Richtlinie 2002/58/EG über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation) keinen gemeinschaftlichen Besitzstand geschaffen, in den nach Art. 47 EUV nicht eingegriffen werden dürfe. Art. 1 Abs. der Richtlinie schließe die Anwendbarkeit dieser Richtlinie im strafrechtlichen Bereich ausdrücklich aus, so dass ein gemeinschaftlicher Besitzstand im Hinblick auf die Vorratsdatenspeicherung zum Zwecke der Strafverfolgung nicht existiere. Mangels Zuständigkeit der EG müsse die Bundesregierung im Namen der Bundesrepublik Deutschland als einzig privilegierte Klageberechtigte Nichtigkeitsklage nach Art. 230 EGV vor dem EuGH erheben.

Für den Deutschen Bundestag sei es zudem unzumutbar, Richtlinien umsetzen zu müssen, die auf unrichtigen Rechtsgrundlagen beruhen würden, so dass zudem beantragt wurde, die Umsetzung der Richtlinie in Deutschland bis zur Entscheidung des EuGH auszusetzen. Der

[46] Im Einzelnen strittig; spätestens aber mit Umsetzung der Durchsetzungsrichtlinie2004/48/EG.
[47] BT-Drs. 16/5846, S. 29.

Schaden, der dadurch entstünde, dass eine nichtige Richtlinie zunächst in nationales Recht umgesetzt würde und das Umsetzungsgesetz dann wieder zurückzunehmen wäre, sei erheblich.

Diese Anträge wurden am 20. Juni 2006 im Deutschen Bundestag mit den Stimmen der CDU/CSU-Fraktion sowie der SPD-Fraktion abgelehnt.[49] Im Rahmen der zweiten Beratung über die Umsetzung der Richtlinie in deutsches Recht brachten sechs Abgeordnete der Fraktion Bündnis 90/Die Grünen zusammen mit ihrer Bundestagsfraktion am 01. November 2007 einen Änderungsantrag ein, um das Gesetz durch einen zusätzlichen Absatz zu ergänzen.[50] In diesem Absatz sollte festgelegt werden, dass, wenn der EuGH in dem Verfahren Irland/Rat der Europäischen Union, Europäisches Parlament die Nichtigkeit der Richtlinie feststellt, die Regelungen zur Umsetzung der Richtlinie in Deutschland mit Ablauf des Tages außer Kraft treten, an dem die Entscheidung des EuGH im Amtsblatt der EU verkündet wird. Dieser Änderungsantrag wurde jedoch am 09. November 2007 mit den Stimmen aller übrigen Fraktionen im Bundestag abgelehnt.[51]

Im Rahmen der dritten Beratung zur Umsetzung der Richtlinie wurde am 07. November 2007 von der großen Mehrheit der Abgeordneten der FDP-Bundestagsfraktion erneut beantragt, die Richtlinie nicht umzusetzen, bzw. ihre Umsetzung zu verschieben und grundrechtsschonender umzusetzen.[52] Es wurde wiederum die fehlende Zuständigkeit der EG bemängelt und auf das laufende Verfahren zur Feststellung der Nichtigkeit der Richtlinie vor dem EuGH hingewiesen, verbunden mit der Forderung, dass der deutsche Gesetzgeber vor der Umsetzung ins nationale Recht die Entscheidung des EuGH abwarten solle.

Außerdem wurde gerügt, dass die Speicherung von Telekommunikationsdaten für sechs Monate in das Fernmeldegeheimnis gem. Art. 10 GG eingreife, da durch die Strafverfolgungsbehörden genaue Bewegungsprofile der Bürger erstellt werden könnten. Außerdem würde in das Recht der Bürger auf informationelle Selbstbestimmung nach Art. 2 Abs. 1 iVm. Art. 1 Abs. 1 GG eingegriffen. Mit der anlass- und verdachtslosen Speicherung sämtlicher Verbindungsdaten würden alle Bürger unter einen Generalverdacht gestellt, so dass diese Eingriffe auch mangels Verhältnismäßigkeit und Bestimmbarkeit nicht gerechtfertigt werden könnten. Bedenken bestünden zudem in Hinblick auf die Pressefreiheit gem. Art. 5 Abs. 1 GG, da durch die Aufzeichnung der Verbindungsdaten das Vertrauensverhältnis zwischen Informanten und Journalisten erheblich beeinträchtigt werden könne.

---

[48] BT-Drs. 16/1622 v. 26.05.2006
[49] BT-Plenarprotokoll 16/38, S. 3508D - 3527D (3527 C)
[50] BT-Drs. 16/7016 v. 07.11.2007
[51] BT-Plenarprotokoll 16/124, S. 12993C ff. (13005D)

Außerdem rügten die Abgeordneten, dass die deutsche Umsetzung über die Anforderungen der Richtlinie hinausgehe, da sie den Zugriff der Daten bei jedem Verdacht einer „erheblichen“ oder einer „mittels Telekommunikation begangenen Straftat“ ermögliche. Zudem würde ein Zugriff der Nachrichtendienste auf diese Daten ermöglicht und zwar ohne das Erfordernis einer richterlichen Prüfung und Anordnung. Somit sei das Gebot zur grundrechtsschonenden Umsetzung von Richtlinien verletzt. Außerdem würde die Umsetzung der Richtlinie unzumutbare Kosten für die Telekommunikationsanbieter ohne angemessene Entschädigung verursachen, zumal auch die Umsetzungsfristen für die Anbieter viel zu kurz bemessen seien. Auch dieser Antrag wurde am 09.11.2007 mit den Stimmen der CDU/CSU-Fraktion, der SPD-Fraktion und von der Fraktion Bündnis 90/Die Grünen abgelehnt.[53]

Frage 5:

Welche Reaktionen seitens der Zivilgesellschaft lassen sich in den ausgewählten Mitgliedstaaten erkennen?

In Deutschland ist der Widerstand gegen die Vorratsdatenspeicherung seitens der Zivilbevölkerung gut organisiert. Bereits im Dezember 2005 ist anlässlich eines Treffens beim Chaos Communication Congress (der „Jahrestagung“ das Chaos Computer Clubs in Berlin) der „Arbeitskreis Vorratsdatenspeicherung[54]“ entstanden. Die Grundsätze des Arbeitskreises sind in einer gemeinsamen Erklärung[55] der einzelnen Unterstützerverbände festgelegt, in der die verdachtsunabhängige Speicherung von Telekommunikationsdaten als inakzeptabel zurückgewiesen wird. Die Liste der teilnehmenden Verbände und Institutionen ist ebenso lang wie prominent.

Um nur einige zu nennen:
Deutsche Vereinigung für Datenschutz e.V. (DVD)
(http://www.datenschutzverein.de/)
Bundesverband Deutscher Zeitungsverleger e.V. (BDZV)
(http://www.bdzv.de/)
Deutschen Journalisten-Verband (DJV)
(http://www.djv.de/)
Neue Richtervereinigung e.V. (NRV)
(http://www.nrv-net.de/)
Verband der deutschen Internetwirtschaft e.V. (eco)
(http://www.eco.de/)

---

[52] BT-Drs. 16/7017 v. 07.11.2007
[53] BT-Plenarprotokoll 16/124, S. 12993C ff. (13012A)
[54] http://www.vorratsdatenspeicherung.de/component/option,com_frontpage/Itemid,1/lang,de/ .
[55] http://www.vorratsdatenspeicherung.de/content/view/80/100/lang,de/ .

Deutscher Anwaltverein e.V. (DAV)
(http://anwaltverein.de/)
Deutsche Gesellschaft für Soziologie e.V. (DGS)
(http://www.soziologie.de/)
Reporter ohne Grenzen e.V
(http://www.reporter-ohne-grenzen.de/)
Bundesverband deutscher Pressesprecher e.V. (BdP)
(http://www.pressesprecherverband.de/)
Bundesverband Digitale Wirtschaft e.V. (BVDW)
(http://www.bvdw.org/).[56]

Zahlreiche Demonstrationen, Informations- und Podiumsveranstaltungen wurden organisiert. Der Widerstand gegen das am 31. Dezember 2007 verkündete Gesetz erreichte mit der am selben Tag von acht Erstbeschwerdeführern eingereichten 150-seitigen Verfassungsbeschwerde[57], verbunden mit dem Antrag, das Gesetz bis zur Entscheidung außer Kraft zu setzen, seinen vorläufigen Höhepunkt. Nach Angabe des Arbeitskreises Vorratsdatenspeicherung wird die Verfassungsbeschwerde von rund 30.000 Bürgern betrieben. Aufgrund organisatorischer Probleme mit der Erfassung und Auswertung der erforderlichen Vollmachten treten diese zurzeit jedoch noch nicht als Beschwerdeführer auf. [58] Das BVerfG wird noch im März 2008 über den Eilantrag entscheiden. Wann eine Entscheidung im Hauptsacheverfahren verkündet wird, ist derzeit noch völlig offen.[59]

Die eingereichte Verfassungsbeschwerde richtet sich gegen die in den §§ 113a und 113b TKG geregelte Vorratsdatenspeicherung. Es werden die folgenden Grundrechtsverstöße gerügt:

Eine generelle Verkehrsdatenspeicherung verletze das Fernmeldegeheimnis (Art. 10 Abs. 1 3. Alt. GG) und das Recht auf informationelle Selbstbestimmung gem. Art. 2 Abs. 1, 1 Abs. 1 GG der an den Kommunikationsvorgängen Beteiligten, denn sie sei unverhältnismäßig. Dies ergebe sich insbesondere daraus, dass nicht nur vermutete Straftäter oder Störer oder deren vermutete Kontaktpersonen betroffen seien, sondern jeder Telekommunikationsnutzer, ohne dass er einen Grund für die Überwachung geliefert habe, die Bürger gleichzeitig jedoch die Nutzung von Telekommunikationsnetzen nicht oder nur unter unzumutbaren Nachteilen mei-

[56] Eine vollständige Auflistung ist abrufbar unter:
http://www.vorratsdatenspeicherung.de/content/view/80/100/lang,de/.
[57] http://wiki.vorratsdatenspeicherung.de/images/Verfassungsbeschwerde_Vorratsdatenspeicherung.pdf.
[58] http://www.vorratsdatenspeicherung.de/content/view/78/86/lang,de/.
[59] Auch eine Gruppe von FDP-Politikern hat eine Verfassungsbeschwerde inklusive Eilantrag eingereicht, die weiter unten ausführlicher dargestellt wird. Auch über diesen Eilantrag wird noch im März 2008 entschieden werden: http://www.heise.de/newsticker/meldung/103544.

den können. Zudem würden hiervon nicht nur öffentlich zugängliche Daten oder Adressdaten, sondern unmittelbar die Privatsphäre betreffende Daten über das Verhalten des Einzelnen erfasst. Die Aussagekraft dieser Daten sei extrem hoch und eine missbräuchliche Verwendung könne großen Schaden anrichten. Gleichzeitig könne nach derzeitigem Erkenntnisstand nicht davon ausgegangen werden, dass eine generelle Vorratsdatenspeicherung einen die vielfältigen Eingriffe rechtfertigenden Erfolg bei der Vereitelung von Straftaten gegen die Allgemeinheit hervorbringen werde. Vielmehr würde der Schwerpunkt der durch die Vorratsdatenspeicherung aufgeklärten Straftaten solche betreffen, die sich gegen Rechtsgüter von Einzelnen richten, insb. im Bereich des Urheberrechts. Nach allem müsse daher die durch die Vorratsdatenspeicherung möglicherweise verbesserte Strafverfolgung hinter dem höherwertigen Zweck zurückstehen, sensible Daten der unzähligen rechtmäßig handelnden Nutzer vor unberechtigten und missbräuchlichen Zugriffen zu schützen. Nur so sei den Bürgern ein unbefangenes Gebrauchen ihrer grundrechtlich geschützten Freiheiten zu ermöglichen.[60]

Eine generelle Vorratsdatenspeicherung verstoße zudem gegen die Berufsfreiheit (Art. 12 Abs. 1 GG) der zur Durchführung der Speicherung verpflichteten Unternehmen und Organisationen, denn es sei nach wie vor unklar, mit welchen Kosten eine generelle Vorratsspeicherung von Telekommunikationsdaten tatsächlich verbunden sei und in welchem Maß die betroffenen Unternehmen diese Kosten auffangen könnten. Die Bundesregierung sei jedoch verpflichtet gewesen, eine solche Untersuchung vorzunehmen, bevor sie die Unternehmen zur Kostentragung verpflichte. In Ermangelung einer solchen Untersuchung der Refinanzierungsmöglichkeiten und der Aufnahme ergänzender Kostenerstattungsregelungen auch für Investitionskosten sei den betroffenen Unternehmen eine Kommunikationsdatenspeicherungspflicht daher nicht zumutbar. Zudem verstoße die Regelung gegen die Berufsfreiheit, weil sie keine Ausnahme für Berufsgeheimnisträger und Vertrauensberufe bereithalte. Auch dieser Eingriff sei angesichts einer nur möglicherweise verbesserten Strafverfolgung unverhältnismäßig in Anbetracht des wichtigen Interesses, persönliche Geheimnisse der rechtmäßig handelnden Betroffenen vor missbräuchlichen Zugriffen zu schützen und den unbefangenen Kontakt mit Angehörigen von Vertrauensberufen zu ermöglichen. Im Fall von Presseinformanten diene dieser Schutz zudem in besonderer Weise auch dem demokratischen Gemeinwesen insgesamt, das auf eine effektive Kontrolle der öffentlichen Gewalt angewiesen sei.[61]

Weiters würden im Bereich des Internets durch eine generelle Vorratsdatenspeicherung auch die Meinungsfreiheit aus Art. 5 Abs. 1 S. 1 Hs. 1 GG, die Informationsfreiheit aus Art. 5

[60] http://www.starostik.de/downloads/anwalt-berlin-verfassungsbeschwerde-vorratsdatenspeicherung.pdf , Seite 37 ff.

Abs. 1 S. 1 Hs. 2 GG und die Rundfunkfreiheit nach Art. 5 Abs. 1 S. 2 2. Alt. GG verletzt. Die fehlende Kostentragungsregelung werde zu erheblich höheren Preisen der betroffenen Unternehmen führen. Dies wiederum habe zur Folge, dass weniger finanzkräftige Unternehmen und Organisationen zu einer Einschränkung des Abrufs und der Verbreitung von Tatsachenbehauptungen und Meinungen über Telekommunikationsnetze gezwungen seien. Der verminderte Austausch von Meinungen und Informationen sei typische und vorhersehbare Folge der Einführung einer Vorratsspeicherungspflicht ohne finanzielle Kompensation. Zudem liege ein Verstoß gegen die vorgenannten Grundrechte auch deshalb vor, weil Telekommunikationsvorgänge zurückverfolgbar gemacht würden und dies Anbieter wie Nutzer von Informationen abschrecken könne.

Letztlich verletze eine generelle Verkehrsdatenspeicherung die Rechte der Kommunizierenden und die Rechte der zur Durchführung der Speicherung verpflichteten Unternehmen und Organisationen aus Art. 3 Abs. 1 GG (Gleichbehandlungsgebot). Zunächst liege eine Ungleichbehandlung des Informationsaustausches über Telekommunikationsnetze gegenüber dem räumlich-unmittelbaren Informationsaustausch vor. Dies könne nur gerechtfertigt sein, wenn der durchschnittliche Telekommunikationsvorgang Rechtsgüter in erheblich höherem Maß gefährde als der typische räumlich-unmittelbare Kommunikationsvorgang. Ob dies der Fall sei, sei jedoch angesichts versäumter vorheriger Untersuchung durch die Bundesregierung ungeklärt, weshalb eine Rechtfertigung der Ungleichbehandlung nicht in Betracht komme.[62] Zudem werde durch das Gesetz der Informationsaustausch von Bürgern via Telekommunikation gegenüber dem Postwesen ungleich behandelt. Auch hier lasse sich mangels empirischer Untersuchung nicht mit hinreichender Sicherheit auf ein höheres Gefährdungspotential der Telekommunikation schließen, weshalb es auch für diese Ungleichbehandlung keine Rechtfertigung gebe. Gleiches gelte für die Ungleichbehandlung von Telekommunikationsunternehmen gegenüber Postunternehmen. Auch sei eine Ungleichbehandlung darin zu sehen, dass der Gesetzgeber von der Wahl eines milderen Mittels als einer generellen Vorratsspeicherung abgesehen habe. Dies sei nur dann zu rechtfertigen, wenn alle Mittel, die weniger eingreifend sind, insgesamt einen geringeren Nutzen versprechen, dies sei aber gerade nicht geklärt.[63] Kleinere Telekommunikationsunternehmen würden zudem mit anderen Telekommunikationsunternehmen gleichbehandelt, obwohl dieses ungerechtfertigt sei. So würden sich Kosten steigernde Belastungen auf die Wettbewerbssituation von Kleinunternehmen von vornherein stärker auswirken als auf größere Unternehmen, die über eine gewisse Kapitaldecke verfügen. Aus diesem Grund seien seitens der Kleinunternehmen Insolvenzen und ähnliche schwerste Belastungen ernsthaft zu befürchten. Eine obligatorische Vorratsspeicherung von Telekommunikationsdaten sei mit den Art. 3 Abs. 1, 12 Abs. 1 GG

[61] Ebenda, Seite 112 ff.
[62] Ebenda, Seite 129.

daher nur vereinbar, wenn für Kleinunternehmen eine weitgehende Kostenerstattung vorgesehen werde.[64] Letztlich würden durch eine generelle Vorratsdatenspeicherung Telekommunikationsunternehmen und ihre Kunden gegenüber der Allgemeinheit der Steuerzahler ungerechtfertigt ungleich behandelt. Die generelle Vorratsdatenspeicherung sei zur Abwehr von Gefahren und als Mittel der Strafverfolgung eine staatliche Aufgabe, weshalb die dabei anfallenden Kosten zulasten der Allgemeinheit gehen müssten. Tatsächlich sei aber vorgesehen, dass nur der Gruppe der Telekommunikationsunternehmen und ihren Kunden die Lasten staatlicher Aufgabenwahrnehmung aufgebürdet werden, hierfür sei keine Rechtfertigung ersichtlich.[65]

Zudem wird auch hier vorgetragen, dass die dem Gesetz zugrunde liegende Richtlinie 2006/24/EG in formeller Hinsicht rechtswidrig sei, da es der Europäischen Gemeinschaft an der Kompetenz zum Erlass der in der Richtlinie enthaltenen Regelungen fehle. Auf Art. 95 EGV könne die Richtlinie jedenfalls nicht gestützt werden.

Darf man den Angaben über die Anzahl der sich der Verfassungsbeschwerde noch anschließenden Beschwerdeführer glauben, ist die Flut von Verfassungsbeschwerden bisher einzigartig in der Geschichte des Bundesverfassungsgerichtes. Der Arbeitskreis Vorratsdatenspeicherung hat unter www.vorratsdatenspeicherung.de ein Internetportal eingerichtet, das auf aktuelle Veranstaltungen hinweist und eine Fülle von Hintergrundinformationen, Materialien und Stellungnahmen zum Thema bereithält.

Es gibt weitere Verfassungsbeschwerden gegen das Gesetz. Zwei davon, eine von Abgeordneten der FDP, eine von Abgeordneten der Grünen, richten sich, wie die zuvor genannte, im Kern gegen die Vorratsdatenspeicherung gem. §§ 113a und 113b TKG. Eine weitere greift zudem zahlreiche strafprozessuale Vorschriften, die durch das *Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG* eingefügt, beziehungsweise geändert worden sind, als verfassungswidrig an.

Die ebenfalls mit Eilantrag verknüpfte Verfassungsbeschwerde aus dem Lager der FDP ist von einer Gruppe um den früheren Bundestagsvizepräsident Burkhard Hirsch (FDP) eingereicht worden.[66] Hirsch legte die Verfassungsbeschwerde im eigenen Namen ein sowie für weitere FDP-Politiker, darunter Bundestags-Vizepräsident Hermann Otto Solms, die frühere Bundesjustizministerin Sabine-Leutheusser-Schnarrenberger, der frühere Bundesinnenmi-

[63] Ebenda, Seite 141.
[64] Ebenda, Seite 144.
[65] Ebenda, Seite 150.
[66] http://www.spiegel.de/netzwelt/web/0,1518,524610,00.html , die Verfassungsbeschwerde lag leider nicht vor.

nister Gerhart Baum und Gisela Piltz, die innenpolitische Sprecherin der FDP-Bundestagsfraktion. Auch diese Verfassungsbeschwerde soll damit begründet worden sein, dass das angefochtene Gesetz grundlegende Verfassungsrechte in grober Weise missachten würde und die dem Gesetz zugrunde liegende Richtlinie rechtswidrig sei.[67]

Die Verfassungsbeschwerde von zahlreichen Abgeordneten von Bündnis 90/Die Grünen ist erst Anfang Februar 2008 eingereicht worden.[68] Mit ihr soll ebenfalls ein unverhältnismäßiger Eingriff in die Bürgerrechte, insbesondere in das Fernmeldegeheimnis gerügt werden. Es bestehe die Gefahr, dass durch die anlasslose Protokollierung der Nutzerspuren viele Bürger zu einer Veränderung ihres Kommunikationsverhaltens veranlasst würden.

Gleichzeitig wird das Gesetz von Bündnis 90/Die Grünen mit einem Organstreitverfahren angegriffen, denn es greife auch unverhältnismäßig in den Status der Abgeordneten ein. Da auch die Kommunikation von Abgeordneten mit den Bürgern erfasst sei, werde durch die Speicherung der Telekommunikationsdaten die Vertrauensbeziehung der Bürger zu ihren Abgeordneten gefährdet. Im Organstreitverfahren machen Bündnis 90/Die Grünen daher die Verletzung ihrer Abgeordnetenrechte geltend.[69]

Die beiden erstgenannten Verfassungsbeschwerden sind am 29. Januar 2008[70] dem ersten Senat des Bundesverfassungsgerichts zugewiesen worden, wohingegen sich der zweite Senat mit der zuvor erwähnten weiteren Verfassungsbeschwerde[71] befassen wird, die sich im Schwerpunkt gegen die strafprozessualen Vorschriften richtet. Allerdings beruhen die mit dieser Verfassungsbeschwerde angegriffenen Teile des deutschen Umsetzungsgesetzes nicht auf Vorgaben der Richtlinie 2006/24/EG; mit ihr sollen vielmehr über die Verfassungswidrigkeit der Vorratsdatenspeicherung hinaus die folgenden Grundrechtsverstöße gerügt werden:[72]

Die § 100a Abs. 4 S. 1 StPO und § 100f Abs. 1 und 2 StPO zur Telefonüberwachung und Observierung würden keinen ausreichenden Schutz des Kernbereichs privater Lebensgestaltung gewährleisten und daher das Fernmeldegeheimnis (Art. 10 Abs. 1 3. Alt. GG) und das Recht auf informationelle Selbstbestimmung gem. Art. 2 Abs. 1, 1 Abs. 1 GG verletzen. Sei für Telefonüberwachungen zumindest ein unzureichender Schutz des Kernbereichs geregelt, fehle ein solcher für Observationen gänzlich. Um diese Vorschriften verfassungskonform

[67] http://www.focus.de/politik/deutschland/vorratsdatenspeicherung_aid_138954.html.
[68] http://www.gruene-bundestag.de/cms/presse/dok/219/219756.weg_in_den_ueberwachungsstaat_stoppen.html, auch diese Verfassungsbeschwerde lag leider nicht vor.
[69] Ebenda.
[70] http://www.bundesverfassungsgericht.de/pressemitteilungen/bvg08-011.html.
[71] Es konnte leider nicht geklärt werden, von wem diese Verfassungsbeschwerde eingereicht worden ist.
[72] http://www.daten-speicherung.de/index.php/zweite-verfassungsbeschwerde-gegen-vorratsdatenspeicherung/ .

auszugestalten, wäre eine Regelung erforderlich, die für den Fall einer Verletzung des Kernbereichs vorsehe, dass eine Vorlage an das zuständige Gericht erfolgt, weil die Ermittlungsbeamte die Erkenntnisse andernfalls dennoch zu weiteren Ermittlungen verwenden würden. Zudem rügt die Verfassungsbeschwerde fehlende, beziehungsweise stark eingeschränkte Benachrichtigungspflichten gegenüber den Betroffenen im Falle einer Überwachung (§ 101 StPO). In § 101 Abs. 5 und 6 StPO seien weit reichende Ausnahmen vorgesehen, hierdurch werde gegen das Recht auf informationelle Selbstbestimmung (Art. 2, Abs. 1, 1 Abs. 1), das Recht auf effektiven Rechtsschutz (Art. 19 Abs. 4 GG) und den Anspruch auf rechtliches Gehör (Art. 103 GG) verstoßen.

Zudem wird ein unzureichender Schutz des Berufsgeheimnisses geltend gemacht. Mit § 160a Abs. 1 und 2 StPO werde gegen das Recht auf informationelle Selbstbestimmung (Art. 2, Abs. 1, 1 Abs. 1), das Fernmeldegeheimnis (Art. 10 Abs. 1 3. Alt. GG) und die Berufsfreiheit (Art. 12 Abs. 1 GG) der Rechtsanwälte verstoßen, denn die Ausnahme für Rechtsanwälte nach § 160 Abs. 2 StPO sei zu unbestimmt. Mandanten müssten sich darauf verlassen können, dass der Kontakt mit ihrem Rechtsanwalt vertraulich sei, dass heißt, nicht abgehört oder sonst geheim ausgeforscht werde. Letztlich erlaube § 160a Abs. 4 StPO die Überwachung von Berufsgeheimnisträgern schon dann, wenn sie einer beliebigen Straftat verdächtig seien; eine solche Überwachung sei jedoch auch dem Bundesgerichtshof zufolge nur im Falle einer schweren, in § 100a StPO genannten Straftat verhältnismäßig.

Freilich regt sich gegen die Vorratsdatenspeicherung in Deutschland nicht nur Widerstand: Befürwortet wird die Vorratsdatenspeicherung in Deutschland von der Gewerkschaft der Polizei (GdP), der mitgliederstärksten Berufsvertretung der Polizei in Deutschland. So heißt es in einer Pressemitteilung der GdP vom 06. November 2007,[73] dass die Sicherheitsbehörden für die Aufklärung schwerer Straftaten und zur Verhinderung zukünftiger Straftaten auf diese Daten angewiesen seien. Da die Ermittlungen immer langwieriger und schwerer würden, sei die bisherige Speicherzeit nicht mehr ausreichend gewesen. Durch strenge Auflagen, wie z.B. einem Richtervorbehalt, und durch den verantwortungsvollen Umgang der Polizei mit diesen Daten bestünde auch keine Gefahr, dass der Bürger „gläsern“ würde.

Sehr starke Befürworter der Vorratsdatenspeicherung im Bereich des Internets sind zudem die deutsche Musikindustrie, der deutsche Buchhandel, die deutsche Filmindustrie, Verlage und diverse weitere Verwertungsgesellschaften, die für ihre Mitglieder Urheber- und verwandte Schutzrechte wahrnehmen. Diese Akteure haben sich zum „Forum der Rechteinhaber“ zusammengeschlossen. Am 21. August 2007 veröffentlichte dieses Forum eine Stel-

[73] Pressemitteilung der GdP vom 06.11.2007, abrufbar unter: http://www.gdp.de/gdp/gdpcms.nsf/id/p71102/$file/p71102Vorratsdaten.pdf .

lungnahme zur geplanten Umsetzung der Richtlinie in Deutschland, in der die Vorratsdatenspeicherung als wichtiger Schritt zur Bekämpfung von Urheberrechtsverletzungen im Internet bezeichnet wird.[74] Insbesondere die massenhafte Nutzung von P2P-Filesharing-Netzwerken, in denen urheberrechtlich geschützte Werke ohne Zustimmung des Rechteinhabers angeboten und heruntergeladen werden, habe zu massiven Umsatz- und Arbeitsplatzeinbußen in der Industrie geführt. Um etwaige Rechtsverstöße straf- und zivilrechtlich geltend machen zu können, müsse gewährleistet sein, dass IP-Adressen, die für bestimmte Aktionen im Internet benutzt wurden, einem bestimmten Nutzer zugeordnet werden können. Bisher seien die Internetserviceprovider jedoch gar nicht (bei Flatrates) oder nur für einen sehr kurzen Zeitraum verpflichtet, die Zuordnungsdaten zu speichern, so dass eine Rechtsverfolgung in vielen Fällen bisher nicht möglich sei. Deshalb begrüßt das Forum der Rechteinhaber die Regelungen zur Vorratsdatenspeicherung grundsätzlich, kritisiert aber, dass die Regelungen nicht weitreichend genug seien. So fordert das Forum, die Speicher- und Herausgabepflicht der Internetserviceprovider nicht auf Zwecke der Strafverfolgung zu beschränken. Der Gesetzgeber solle sicherstellen, dass ein Internetserviceprovider auch Auskunft über den Inhaber einer dynamischen IP-Adresse zur zivilrechtlichen Durchsetzung der Rechte am geistigen Eigentum erteilen könne und dabei die gespeicherten Daten zur Erfüllung des Auskunftsersuchens intern verarbeiten dürfe. Andernfalls wären die Rechteinhaber auch zukünftig gezwungen, über den Umweg einer Strafanzeige an die entsprechenden Daten zu gelangen, um dann zivilrechtliche Schadensersatzansprüche geltend machen zu können.

[74] Stellungnahme des Forums der Rechteinhaber vom 21.08.2007, abrufbar unter: http://www.musikindustrie.de/uploads/media/pp_gesetz_nat_stellungn_20070821_forum_vorrat.pdf .

Frankreich

Zusammenfassung: Frankreich hat die Vorgaben der Richtlinie bereits vor deren Verabschiedung umgesetzt. Zivilgesellschaftlicher Widerstand ist erkennbar, aber vergleichsweise schwach ausgeprägt.

Frage 1:

Welche Regelungen wurden von denjenigen ausgewählten Mitgliedstaaten getroffen, die die Richtlinie bereits umgesetzt haben?

In Frankreich ist die Vorratsdatenspeicherung in Art. 34-1 des Telekommunikationsgesetzes geregelt; die Bestimmung stammt vom Januar 2000, wurde jedoch mehrfach, zuletzt am 23. Januar 2006, novelliert. Die Norm sieht als Regelfall eine Löschungs- bzw. Anonymisierungsverpflichtung von Verbindungsdaten für Telekommunikationsdienstleister vor[75] und gilt auch für Gratisangebote.[76] Damit sind Diensteanbieter wie Internetcafebetreiber, Hotels, die W-Lan anbieten, öffentliche Bibliotheken etc. vom Normbereich erfasst.[77] Im Zuge der legistischen Maßnahmen nach dem 11. September 2001 wurde der Grundsatz des Speicherverbots jedoch in einen Grundsatz des Speichergebots verkehrt. Dies geschah in Grundzügen bereits 2002 durch das Gesetz zur alltäglichen Sicherheit (LOI no 2001-1062 du 15 novembre 2001 relative à la sécurité quotidienne (1))[78], dessen Art. 29 das Telekommunikationsgesetz entsprechend modifizierte.

Vom Grundsatz der Löschungs- bzw. Anonymisierungsverpflichtung macht daher Art. 34-2 Telekommunikationsgesetz nun eine erhebliche Ausnahme: Zur Untersuchung, Feststellung und Verfolgung bestimmter Straftaten darf, ausschließlich für Zwecke der Verwendung der zuständigen Behörden, eine Speicherung bestimmter technischer Daten für bis zu ein Jahr vorgesehen werden.[79] Näheres ist durch ein Dekret des Conseil d'Etat nach Anhörung der Datenschutzkommission (Commission nationale de l'informatique et des libertés[80]) zu bestimmen.[81] Insbesondere ist dort festzulegen, welche Daten wie lange zu speichern sind

[75] « Les opérateurs de communications électroniques, et notamment les personnes dont l'activité est d'offrir un accès à des services de communication au public en ligne, effacent ou rendent anonyme toute donnée relative au trafic, sous réserve des dispositions des II, III, IV et V. »
[76] Art. 34-I Satz 2.
[77] Vgl. Actualités du droit de l'information, Nr. 68, April 2006, online unter http://www.adbs.fr/site/publications/droit_info/adi/68/adi_adbs_no68.html .
[78] Online zB unter http://www.legifrance.gouv.fr/affichTexte.do;jsessionid=813497396715CE118A7DC9A28AC5EDF4.tpdjo06v_1?cidTexte=LEGITEXT000005631673&dateTexte= .
[79] Art. 34-II Satz 1: „Pour les besoins de la recherche, de la constatation et de la poursuite des infractions pénales, et dans le seul but de permettre, en tant que de besoin, la mise à disposition de l'autorité judiciaire d'informations, il peut être différé pour une durée maximale d'un an aux opérations tendant à effacer ou à rendre anonymes certaines catégories de données techniques."
[80] http://www.cnil.fr/ .
[81] Art. 34-II Satz 2: „Un décret en Conseil d'Etat, pris après avis de la Commission nationale de l'informatique et des libertés, détermine, dans les limites fixées par le V, ces catégories de données et la durée de leur conservation, selon l'activité des opérateurs et la nature des communications ainsi que les modalités de compensation, le

und wie Telekommunikationsdienstleister für die Speicherungspflichten ökonomisch zu entschädigen sind.

Art. 34-1-1 des Telekommunikationsgesetzes, der derzeit befristet bis zum 31. Dezember 2008 in Kraft ist, schafft für Polizei und Gendarmerie für Zwecke der Terrorismusbekämpfung Zugriff auf diese Verkehrsdaten[82] ohne weitere gerichtliche Überprüfung.[83] Über die Legitimität entsprechender Auskunftsbegehren hat eine im Innenministerium angesiedelte Person zu befinden.[84]

Ausdrücklich gesetzlich verboten sind die Erhebung und Speicherung von Inhaltsdaten.[85] Gesetzlich wird den Telekommunikationsdienstleistern auch die Ergreifung jener Datensicherheitsmaßnahmen aufgetragen, die erforderlich sind, um eine Verwendung der erhobenen Daten zu anderen als den gesetzlich bestimmten Zwecken zu verhindern.[86] Verstöße gegen eine Speicher- oder Löschungsverpflichtung sind mit Geldbuße bis zu 75.000,- € belegt.[87]

Am 24. März 2006 wurde in Umsetzung des Art. 34-2 ein Dekret verabschiedet, in dem die zu speichernden Datenkategorien näher umschrieben wurden.[88] Zu speichern sind demnach

a) Informationen, die eine Identifizierung des Nutzers erlauben
b) Daten zu den für die Kommunikation verwendeten Endgeräten

---

cas échéant, des surcoûts identifiables et spécifiques des prestations assurées à ce titre, à la demande de l'Etat, par les opérateurs. »

[82] Afin de prévenir [Dispositions déclarées non conformes à la Constitution par la décision du Conseil constitutionnel n° 2005-532 DC du 19 janvier 2006] les actes de terrorisme, les agents individuellement désignés et dûment habilités des services de police et de gendarmerie nationales spécialement chargés de ces missions peuvent exiger des opérateurs et personnes mentionnés au I de l'article L. 34-1 la communication des données conservées et traitées par ces derniers en application dudit article.
Les données pouvant faire l'objet de cette demande sont limitées aux données techniques relatives à l'identification des numéros d'abonnement ou de connexion à des services de communications électroniques, au recensement de l'ensemble des numéros d'abonnement ou de connexion d'une personne désignée, aux données relatives à la localisation des équipements terminaux utilisés ainsi qu'aux données techniques relatives aux communications d'un abonné portant sur la liste des numéros appelés et appelants, la durée et la date des communications.

[83] Siehe Christiane Feral-Schuhl, Données de communication : quel traitement ?, http://www.journaldunet.com/solutions/expert/7676/donnees-de-communication-quel-traitement.shtml .

[84] Art. 34-1-1 Abs. 4 : « Les demandes des agents sont motivées et soumises à la décision d'une personnalité qualifiée, placée auprès du ministre de l'intérieur. Cette personnalité est désignée pour une durée de trois ans renouvelable par la Commission nationale de contrôle des interceptions de sécurité sur proposition du ministre de l'intérieur qui lui présente une liste d'au moins trois noms. Des adjoints pouvant la suppléer sont désignés dans les mêmes conditions. La personnalité qualifiée établit un rapport d'activité annuel adressé à la Commission nationale de contrôle des interceptions de sécurité. Les demandes, accompagnées de leur motif, font l'objet d'un enregistrement et sont communiquées à la Commission nationale de contrôle des interceptions de sécurité."

[85] Art. 34-V Satz 2: „Elles ne peuvent en aucun cas porter sur le contenu des correspondances échangées ou des informations consultées, sous quelque forme que ce soit, dans le cadre de ces communications. »

[86] Art. 34-V Satz 4: „Les opérateurs prennent toutes mesures pour empêcher une utilisation de ces données à des fins autres que celles prévues au présent article. »

[87] Art. 39-3.

[88] Für einen ausführlichen Überblick über die Datenkategorien vgl. etwa Anne-Catherine Lorrain/Garance Mathias, Données de connexion : la publication du premier décret ou la première pierre d'un édifice encore inachevé, in : Revue Lamy droit de l'immateriel, Juin 2006, 35-38, online unter http://www.aclorrain.fr/docs/donnees-de-connexion_06.pdf .

c) die technischen Eigenschaften der verwendeten Geräte sowie das Datum, die Uhrzeit und die Dauer der Kommunikation
d) Daten zu zusätzlichen nachgefragten oder verwendeten Dienstleistungen und deren Anbieter
e) Daten zur Identifizierung des Empfängers oder der Empfänger der Kommunikation[89]

Das Dekret enthielt im Übrigen Regeln zur finanziellen Entschädigung der Telekommunikationsdiensteanbieter. Die Speicherdauer beträgt im Regelfall ein Jahr. Ungeregelt bleibt das Format, in dem die Daten zu speichern sind.[90]

Das Dekret wurde in zwei Verfahren, die von der französischen Vereinigung der (alternativen) Telekommunikationsanbieter[91] angestrebt wurden, vor dem Conseil d'Etat angegriffen. Die Beschwerde gegen die Regeln zur Datenspeicherung wurde vollumfänglich abgewiesen.[92] Klargestellt wurde insbesondere, dass die Erhebung und Speicherung auch des Empfängers eines Kommunikationsvorgangs zulässig sei[93] und dass der Umfang der erhobenen Daten verhältnismäßig wäre und in keinem Widerspruch zu Art. 8 EMRK stünde.[94]
Hingegen war die zweite Beschwerde gegen einige Aspekte des Kostenersatzes für den Telekommunikationsanbieter erfolgreich.[95]

Neben die telekommunikationsrechtlichen Vorschriften treten auch Maßnahmen zur Identifizierung der Verursacher rechtswidriger Inhalte, die über Webseiten wie etwa Blogs verbreitet werden. Hervorzuheben ist hier insbesondere das Gesetz vom 21. Juni 2004 *für das Vertrauen in die Informationswirtschaft* („Loi n° 2004-575 du 21 juin 2004 pour la confiance dans

[89] Article R 1013 du décret du 24 mars 2006 : « Aux termes de ce I, doivent être conservées : « a) Les informations permettant d'identifier l'utilisateur ; b) Les données relatives aux équipements terminaux de communication utilisés ; c) Les caractéristiques techniques ainsi que la date, l'horaire et la durée de chaque communication ; d) Les données relatives aux services complémentaires demandés ou utilisés et leurs fournisseurs ; e) Les données permettant d'identifier le ou les destinataires de la communication »
[90] Siehe Christiane Feral-Schuhl, Données de communication : quel traitement ?, http://www.journaldunet.com/solutions/expert/7676/donnees-de-communication-quel-traitement.shtml .
[91] Association française des opérateurs de réseaux et de services de télécommunications (Afors Telecom), vgl. http://www.aforstelecom.fr/.
[92] Conseil d'État Section du contentieux 7 août 2007, online zB unter http://www.legalis.net/jurisprudence-decision.php3?id_article=2000.
[93] Ebd : « Considérant que les dispositions précitées de la seconde phrase du deuxième alinéa du V de l'article L. 341 n'interdisent que la conservation des données relatives au contenu des communications ; qu'au premier alinéa du V de cet article, il est précisé que parmi les catégories de données à conserver, figurent celles portant sur l'identification des personnes utilisatrices du service ; qu'en conséquence, en insérant dans le code cette disposition, le législateur a entendu autoriser la conservation, non seulement des données relatives aux personnes qui émettent une communication électronique, mais encore celles relatives aux personnes qui en sont destinataires ; que, par suite, le e) de l'article R. 1013, qui mentionne ces dernières parmi les données à conserver, n'est pas contraire aux prescriptions législatives susmentionnées ; »
[94] Ebd. : « Considérant, d'une part, que pour le motif exposé ci-dessus, le décret attaqué ne porte pas au droit au respect de la vie privée une atteinte qui serait disproportionnée par rapport aux buts de sécurité publique poursuivis et ne méconnaît pas, par suite, les stipulations de l'article 8 de la convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales ; »
[95] Conseil d'État Section du contentieux 7 août 2007. Association française des opérateurs de réseaux et de services de télécommunications (Afors Telecom) et autres requérants, online zB unter http://www.legalis.net/jurisprudence-decision.php3?id_article=2001 .

l'économie numérique[96]), das entsprechende Speicher- und Registrierungspflichten für Internetaccess- und –hostprovider vorsieht (insb. in seinem Art. 6-II)[97] – wiederum auch bei Gratisangeboten[98]. Auch hier sind Präzisierungen durch ein Dekret vorgesehen. Dieses existiert bisher nur in einem Entwurf, mit einem Erlass in der näheren Zukunft ist jedoch zu rechnen.[99] Der Entwurf sieht eine Verpflichtung zur Speicherung von Daten für ein Jahr vor, die erforderlich sind, um den Ersteller eines Inhalts zu identifizieren („'identification de quiconque a contribué à la création du contenu ou de l'un des contenus."). Damit geht Frankreich erheblich über die Vorgaben der Richtlinie hinaus.[100]

Frage 2:

Was sind die Gründe, aus denen die übrigen ausgewählten Mitgliedstaaten noch nicht umgesetzt haben?

Für Frankreich nicht einschlägig.

Frage 3:

Welche Umsetzungspläne verfolgen jene Mitgliedstaaten, die die Richtlinie bislang noch nicht umgesetzt haben, in zeitlicher bzw. inhaltlicher Hinsicht?

Für Frankreich nicht einschlägig.

Frage 4:

Wie wirkt sich die im Juli 2006 von Irland eingebrachte Klage vor dem Europäischen Gerichtshof auf die Umsetzungsbestrebungen dieser Staaten aus?

Für Frankreich nicht einschlägig.

Frage 5:

---

[96] Online zB über http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000801164&dateTexte= .

[97] I. - Les personnes mentionnées aux 1 et 2 du I détiennent et conservent les données de nature à permettre l'identification de quiconque a contribué à la création du contenu ou de l'un des contenus des services dont elles sont prestataires.
Elles fournissent aux personnes qui éditent un service de communication au public en ligne des moyens techniques permettant à celles-ci de satisfaire aux conditions d'identification prévues au III.
L'autorité judiciaire peut requérir communication auprès des prestataires mentionnés aux 1 et 2 du I des données mentionnées au premier alinéa.
Les dispositions des articles 226-17, 226-21 et 226-22 du code pénal sont applicables au traitement de ces données.
Un décret en Conseil d'Etat, pris après avis de la Commission nationale de l'informatique et des libertés, définit les données mentionnées au premier alinéa et détermine la durée et les modalités de leur conservation."

[98] Art. 6-I 2 leg. cit.

[99] Vgl. CNIL, Rétention des données de connexion : quelles obligations ? (19. 02. 2008), http://www.cnil.fr/index.php?id=2398&news[uid]=522&cHash=fa9b3406f6 .

[100] So auch Philippe Ballet, Conservation des données d'identification : un projet de décret d'ici fin 2007…, http://www.alain-bensoussan.com/pages/1135/ .

Welche Reaktionen seitens der Zivilgesellschaft lassen sich in den ausgewählten Mitgliedstaaten erkennen?

Wie in zahlreichen anderen Mitgliedsstaaten auch, lassen sich auch in Frankreich Stimmen gegen die Richtlinie und/oder ihre Umsetzung vernehmen. Diese sind jedoch – gemessen an der Schnelligkeit und Rigidität der Umsetzung – relativ schwach ausgeprägt. Eine publizistische Plattform bietet immerhin http://www.vie-privee.org, eine Organisation, die etwa 20 Bürgerrechts- und Netzaktivistenvereinigungen umfasst. Daneben finden sich zahlreiche kritische Webberichte und Zeitungsartikel, die jedoch eine organisierte Verfasstheit nicht erreicht haben.[101]

[101] Vgl. zB http://www.pcinpact.com/actu/news/41881-donnees-connexions-retention-decret-contenu.htm; http://www.lemonde.fr/technologies/article/2008/02/20/le-projet-de-conservation-des-donnees-largement-conteste_1013774_651865.html; http://www.couchet.org/blog/index.php?2005/09/27/62-conservation-des-donnees:; http://www.mac4ever.com/news/34910/conservation_des_donnees_sur_les_internautes_le_retour/; http://www.zdnet.fr/actualites/internet/0,39020774,39378763,00.htm?xtor=RSS-1; http://www.ecrans.fr/Internet-le-retour-de-Big-Brother.html.

Griechenland

Zusammenfassung: Griechenland hat die Richtlinie noch nicht umgesetzt und auch noch kein Gesetzgebungsverfahren begonnen. Nach geltendem griechischem Recht ist die Speicherung von Verkehrsdaten nur im Einzelfall anlassbezogen und grundsätzlich nur auf richterliche Anordnung zulässig. Die Richtlinie und ihre etwaige Umsetzung finden in der griechischen Öffentlichkeit kaum Beachtung.

Frage 1:

Welche Regelungen wurden von denjenigen ausgewählten Mitgliedstaaten getroffen, die die Richtlinie bereits umgesetzt haben?

Griechenland hat mit dem Gesetzgebungsverfahren zur Umsetzung der Richtlinie zur Vorratsdatenspeicherung noch nicht begonnen. Der Wortlaut oder Einzelheiten der Umsetzung sind daher noch nicht bekannt.

Frage 2:

Was sind die Gründe, aus denen die übrigen ausgewählten Mitgliedstaaten noch nicht umgesetzt haben?

Die Gründe für die ausbleibende Umsetzung der Richtlinie liegen vor allem in der politischen Situation Griechenlands. Die Wahlen im September 2007 haben Verzögerungen vieler politischer Prozesse bewirkt, darunter die Umsetzung der Richtlinie zur Vorratsdatenspeicherung; die Umsetzung scheint keine politische Priorität zu genießen.

Frage 3:

Welche Umsetzungspläne verfolgen jene Mitgliedstaaten, die die Richtlinie bislang noch nicht umgesetzt haben, in zeitlicher bzw. inhaltlicher Hinsicht?

Umsetzungspläne

Das griechische Justizministerium (Υπουργείο Δικαιοσύνης) ist in Ermangelung einer anderen politischen Festlegung verantwortlich für die Umsetzung. Das Justizministerium war auch verantwortlich für die Umsetzung der Datenschutzrichtlinie für elektronische Kommunikation (2002/58/EG), die durch das Gesetz 3471/2006 „Schutz personenbezogener Daten und der Privatsphäre im Bereich elektronischer Kommunikation und zur Änderung des Gesetzes 2472/1997“ (Amtsblatt der Regierung (ΦΕΚ) A΄133/28.6.2006)[102] umgesetzt wurde. Ein Berichtsausschuss für die Umsetzung der Richtlinie ist noch nicht eingerichtet worden, so dass

[102] Griechisch: Νόμος 3471/2006 «Προστασία δεδομένων προσωπικού χαρακτήρα και της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών και τροποποίηση του ν.2472/1997».

keine Informationen über den geplanten Inhalt der Umsetzung der Richtlinie zur Vorratsdatenspeicherung in nationales griechisches Recht vorliegen und keine bestimmten Erwartungen an die Umsetzung genannt werden können. Es ist bis heute kein Gesetzentwurf und kein Zeitplan für die Umsetzung veröffentlicht worden. Griechenland hat die Erklärung gem. Art. 15 Abs. 3 der Richtlinie abgegeben, die eine Verlängerung der Umsetzungsfrist hinsichtlich der Vorratsspeicherung von Internet-Access-, VoIP- und Email-Daten um achtzehn Monate nach der in Art. 15 Abs. 2 genannten Frist zur Folge hat.[103]

Die gegenwärtige Praxis in Griechenland im Hinblick auf Telekommunikationsdaten und ihre Übermittlung an Sicherheitsbehörden

Im griechischen Recht gibt es keine Pflicht für die Anbieter öffentlich verfügbarer elektronischer Kommunikationsdienste (TK-Diensteanbieter) zur anlassunabhängigen Speicherung von Verkehrs- und Standortdaten. Griechenland hat den Weg der anlassabhängigen Speicherung eingeschlagen, indem die jeweilige Anordnung zur Einschränkung des Fernmeldegeheimnisses zu Ermittlungszwecken genau bestimmt, welche Daten offen zulegen sind. Der Gedanke des größtmöglichen Erhalts des Datenschutzes durch die fallweise anlassbezogene Festlegung weicht grundlegend von dem Grundmodell der Richtlinie zur Vorratsdatenspeicherung ab, die eine anlassunabhängige Speicherung bestimmter Verkehrs- und Standortdaten erfordert.

Die Richtlinie 2002/58/EG wurde in Griechenland umgesetzt durch das Gesetz 3471/2006 „Schutz personenbezogener Daten und der Privatsphäre im Bereich elektronischer Kommunikation und zur Änderung des Gesetzes 2472/1997“[104]. Artikel 1 dieses Gesetzes beschreibt den Zweck des Gesetzes, nämlich den Schutz von Grundrechten und insbesondere der Privatsphäre einerseits und die Festlegung der Anforderungen an die Verarbeitung personenbezogener Daten unter Berücksichtigung des Fernmeldegeheimnisses im Bereich der elektronischen Kommunikation.

Die TK-Diensteanbieter dürfen Verkehrsdaten nicht speichern oder verarbeiten, nachdem sie nicht mehr für den Telekommunikationsvorgang gebraucht werden.[105] Daten dürfen gespeichert werden, soweit sie für Abrechnungszwecke – sowohl in Bezug auf eigene Kunden als auch in Bezug auf andere TK-Diensteanbieter – benötigt werden, und zwar solange die Abrechnung angefochten oder die Forderung verfolgt werden kann,[106] also sechs Monate.[107]

[103] Erklärung der Hellenischen Republik zu Art. 15 Abs. 3 der Richtlinie 2006/24/EG, veröffentlicht am Ende der Richtlinie im ABl. EU.
[104] Amtsblatt der Regierung (ΦΕΚ) A΄133/28.6.2006. Griechisch: Νόμος 3471/2006 «Προστασία δεδομένων προσωπικού χαρακτήρα και της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών και τροποποίηση του ν.2472/1997».
[105] Art. 6 Abs. 1 des Gesetzes 3471/2006.
[106] Art. 6 Abs. 2 des Gesetzes 3471/2006.

Die Verarbeitung von Standortdaten ist nur zulässig, wenn diese anonymisiert wurden oder mit der ausdrücklichen Einwilligung des Benutzers oder Teilnehmers, soweit und solange dies für die Bereitstellung eines Mehrwertdienstes erforderlich ist.[108] Durch Ausnahmeregelungen ist es TK-Diensteanbietern erlaubt, Standortdaten zu verarbeiten, um – ausschließlich – erforderliche Standortinformationen an Sicherheitsbehörden für öffentliche Zwecke, z.B. Strafverfolgung oder Notfallrettung, weiterzugeben, ohne dass eine vorherige Einwilligung des Benutzers oder Teilnehmers vorliegen muss.[109] Griechenland hat keinen Gebrauch von dem in Art. 15 der Datenschutzrichtlinie für elektronische Kommunikation (2002/58/EG) vorgesehenen Vorbehalt gemacht und die Vorratsspeicherung von Verkehrsdaten für eine bestimmte Zeit für Zwecke der nationalen Sicherheit und Verteidigung oder für die Ermittlung und Aufklärung von Straftaten oder die unbefugte Benutzung eines elektronischen Kommunikationssystems nicht erlaubt.

Griechenland hat eine Behörde für die Sicherstellung von Privatsphäre und Sicherheit von Informationen und Kommunikation (ADAE) eingerichtet,[110] um das Post- und Fernmeldegeheimnis und die Kommunikationsfreiheit in jeder Hinsicht zu schützen. Auf Grundlage von Art. 9 des Gesetzes, durch das diese Behörde eingerichtet wurde,[111] ist das präsidiale Dekret 47/2005[112] erlassen worden, das den TK-Diensteanbietern auferlegt, unverzüglich auf eine Anordnung für die Durchbrechung des Kommunikationsgeheimnisses der zuständigen Behörde zu reagieren. Das Dekret regelt nicht, wann die Reaktion als unverzüglich zu gelten hat. Gleichwohl ist eine Speicherung der Verkehrsdaten, die nicht sofort an die zuständige Behörde übermittelt werden können, durch den TK-Diensteanbieter bis zum nächstmöglichen Zeitpunkt der Übermittlung zulässig, jedoch längstens sieben Tage.[113]

Neben dem präsidialen Dekret 47/2005 wird das Verfahren der Einschränkung des Fernmeldegeheimnisses durch die Art. 4, 5 des Gesetzes 2225/1994[114] in der Fassung des Gesetzes 3115/2003 sowie durch Art. 253 der Strafprozessordnung geregelt. Gemäß Art. 4 des Gesetzes 2225/1994 ist die Einschränkung des Fernmeldegeheimnisses zulässig bei verschiedenen schweren Verbrechen, etwa Hochverrat, Sprengstoffdelikte, Tötungsdelikte, Raub,

---

[107] *Sotiropoulos V./Talidou Z*, „Speicherung von Telekommunikationsdaten für Strafverfolgungszwecke", Medien- und Kommunikationsrecht (Δίκαιο Μέσων Ενημέρωσης & Επικοινωνίας), 2/2006, S. 181-195 [184].
[108] Art. 6 Abs. 3 des Gesetzes 3471/2006.
[109] Art. 6 Abs. 3 des Gesetzes 3471/2006.
[110] Durch das Gesetz 3115/2003 "Behörde für die Sicherstellung von Privatsphäre und Sicherheit von Informationen und Kommunikation" (Amtsblatt der Regierung (ΦΕΚ) Α΄47/27.02.2003). Griechisch: Νόμος 3115/2004 «Αρχή διασφάλισης του απορρήτου των επικοινωνιών».
[111] Ebendort.
[112] Präsidiales Dekret Nr. 47/2005 „Verfahren sowie technische und organisatorische Schutzmaßnahmen für die Einschränkung des Fernmeldegeheimnisses und dessen Gewährleistung", Amtsblatt der Regierung (ΦΕΚ) Α΄64/10.03.2005. Griechisch: Προεδρικό διάταγμα 47/2005 «Διαδικασίες καθώς και τεχνικές και οργανωτικές εγγυήσεις για την άρση του απορρήτου των επικοινωνιών και για τη διασφάλισή του».
[113] Art. 7 Abs. 2 lit. γ des präsidialen Dekrets Nr. 47/2005.

schwere Militärstraftaten u.a. Die Einschränkung darf nur für bestimmte Personen oder Personen, die in Zusammenhang mit den Ermittlungen stehen oder für Personen, die als Nachrichtenmittler für den Beschuldigten oder Teilnehmer an der Straftat in Frage kommen, angeordnet werden.

Die besonderen Verfahrensbestimmungen[115] für die Einschränkung des Fernmeldegeheimnisses sind unbedingt verbindlich. Die Strafkammer des Apellationsgerichts (Συμβούλιο Εφετών) oder das erstinstanzliche Strafgericht (Συμβούλιο Πλημμελειοδικών) erlassen auf Antrag des zuständigen Bezirksstaatsanwalts binnen 24 Stunden eine Anordnung[116] über die Einschränkung des Fernmeldegeheimnisses. In besonders dringenden Fällen kann die Anordnung vom ermittlungsleitenden Staatsanwalt oder von einem ordentlichen Ermittlungsrichter getroffen werden. In diesem Fall muss die Anordnung binnen drei Tagen von der Kammer bestätigt werden; nach Ablauf dieser Frist endet die Anordnung sonst automatisch. Die Anordnung kann für nicht länger als zwei Monate getroffen werden; Verlängerungen sind nur bis zur Gesamtdauer von zehn Monaten zulässig.[117]

Erwähnenswert ist, dass mehrere griechische Mobilfunkanbieter aufgefordert wurden, Sicherheitsbehörden (und anderen) Auskünfte über Verkehrsdaten ihrer Kunden zu geben, ohne dass das Verfahren gemäß des Gesetzes 2225/1994 eingeleitet wurde. Die griechische Datenschutzbehörde ADAE hat in Bezug darauf eine Stellungnahme veröffentlicht,[118] nachdem sie von dem Mobilfunkanbieter „TIM Hellas“ angerufen worden war. Die ADAE hat festgestellt, dass die äußeren Umstände der Telekommunikation (also insb. Verkehrsdaten) dem Fernmeldegeheimnis unterfallen, das durch Art. 19 der griechischen Verfassung geschützt ist. Die Behörde hat außerdem festgestellt, dass das Verfahren gem. Gesetz 2225/1994 unbedingt einzuhalten ist, und zwar auch dann, wenn der Tatverdächtige auf frischer Tat betroffen wurde.

Zusammenfassend lässt sich feststellen, dass, obwohl es in Griechenland keine Pflicht zur Speicherung von Daten speziell für Zwecke der Strafverfolgung gibt, die TK-Diensteanbieter rechtlich verpflichtet sind, im Einzelfall anlassbezogen Verkehrsdaten zu speichern. Die Speicherung erfolgt zum Zweck der Verfolgung schwerer Straftaten und steht grundsätzlich unter Richtervorbehalt.

---

[114] Gesetz 2225/1994 „Über die freie Berichterstattung und Kommunikation sowie weitere Regelungen“, Amtsblatt der Regierung (ΦΕΚ) Α΄ 121/20.07.1994, Griechisch: Νόμος 2225/1994 «Για την προστασία της ελευθερίας της ανταπόκρισης και επικοινωνίας και άλλες διατάξεις».
[115] Art. 4 des Gesetzes 2225/1994.
[116] Die für die erforderliche Bestimmtheit der Anordnung notwendigen Angaben ergeben sich aus Art. 5 Abs. 1 bis 3 des Gesetzes 2225/1994.
[117] Art. 5 Abs. 6 des Gesetzes 2225/1994.
[118] Stellungnahme 1/2005, http://www.adae.gr/adae/docs/nomothetiko_plaisio/893-2005.pdf (auf Griechisch)

Frage 4:

Wie wirkt sich die im Juli 2006 von Irland eingebrachte Klage vor dem Europäischen Gerichtshof auf die Umsetzungsbestrebungen dieser Staaten aus?

Die Klage, die Irland gegen den Rat und das Europäische Parlament vor dem Europäischen Gerichtshof mit dem Ziel eingebracht hat, die Richtlinie mangels tragender Primärrechtsgrundlage für nichtig zu erklären, hat in der politischen Diskussion in Griechenland praktisch keine Erwähnung gefunden.

Frage 5:

Welche Reaktionen seitens der Zivilgesellschaft lassen sich in den ausgewählten Mitgliedstaaten erkennen?

Einige Bürgerrechtsorganisationen haben ihre Ablehnung der Vorratsdatenspeicherung zum Ausdruck gebracht (insb. http://www.digitalrights.gr/tiki/tiki-index.php?page=DataRetention) und in einigen Presseerzeugnissen sind kritische Artikel erschienen. Die Vorratsdatenspeicherung ist jedoch kein in der Gesellschaft weithin bekanntes Thema, so dass nennenswerte Reaktionen bisher ausgeblieben sind.

Großbritannien

Zusammenfassung: Großbritannien hat die Richtlinie 2006/24/EG vollständig in nationales Recht transponiert. Sie deckte sich bereits inhaltlich mit seit 2001 bestehender Anti-Terror-Gesetzgebung, die eine freiwillige Datensicherung durch die Kommunikationsbranche vorsah. Durch die Richtlinie änderten sich lediglich die Rahmenbedingungen für die Entschädigung der betroffenen Kommunikationsanbieter sowie die Tatsache, dass eine entsprechende Datenspeicherung nun verpflichtend geboten ist.

Frage 1:

Welche Regelungen wurden von denjenigen ausgewählten Mitgliedstaaten getroffen, die die Richtlinie bereits umgesetzt haben?

Die für Festnetz- und Mobiltelefonie einschlägigen Regelungen der Richtlinie 2006/24/EG (die Richtlinie) wurden im Vereinigten Königreich von Großbritannien und Nordirland am 26. Juli 2007 im Rahmen des Statutory Instrument 2007 No. 2199 (die Verordnung) umgesetzt. Der European Communities Act 1972 sieht vor, dass Richtlinien durch entsprechende Verordnungen in nationales Recht umzusetzen sind, hier handelt es sich also um die normale Vorgehensweise der Umsetzung einer Richtlinie mit der Einschränkung, dass in einer solchen Verordnung keine Sanktionen zu verankern sind. Großbritannien wählte aus diesem Grund den Weg eines ‚incentive' statt einer Sanktion, um die Einhaltung der Regelungen zu gewährleisten.

Bereits vor der Umsetzung der Richtlinie hatte UK als direkte Folge der Anschläge vom 11. September eine längerfristige Datenspeicherung zu Strafverfolgungszwecken und zur Terrorismusbekämpfung vorgesehen, die in einem Gesetzesentwurf mündete und im Dezember 2001 als Anti-Terrorism, Crime and Security Act 2001 (ATCSA) verabschiedet wurde. Eine Consultation zu dem Gesetz fand 2003 statt und resultierte in einer Vereinbarung mit der Telekommunikationsbranche.[119] In Part 11 enthält das Gesetz Regelungen zur längerfristigen Speicherung von Kommunikationsdaten. Das Gesetz führte eine freiwillige Vereinbarung mit den britischen Telekommunikationsanbietern ein,[120] in deren Rahmen eine Datenspeicherung vereinbart wurde, die sich im Wesentlichen mit jenen in der Richtlinie deckt.[121]

Durch die Umsetzung der Richtlinie ergibt sich nunmehr eine Verpflichtung der Telekommunikationsanbieter zu einer solchen Datenspeicherung. Schon in der *Consultation* zum ATC-

[119] „Anti-Terrorism, Crime and Security Act 2001 - Voluntary retention of communications data", Public Consultation Paper, http://www.homeoffice.gov.uk/documents/data-retention-2003/ [26.2.08].
[120] Code of Practice on Voluntary Retention of Communication Data: http://www.opsi.gov.uk/si/si2003/draft/5b.pdf [26.2.08].
[121] 1.6, Consultation Paper for the Initial Transposition of Directive 2006/24/EC, March 2007, S.3 (*Consultation Paper*).

SA sprachen sich einige Kommunikationsanbieter für eine verpflichtende Regelung statt der freiwilligen Vereinbarung aus. Dieser Gedanke wurde in der *Consultation* zu der Richtlinienumsetzung von März 2007 aufgegriffen und weiterentwickelt. Part 11, Section 107 des ATC-SA sieht vor, dass den Anbietern eine angemessene Entschädigung für die zusätzlich entstehenden Kosten der Datenspeicherung zukommen soll („appropriate contributions towards the costs incurred"). Aus der Formulierung lässt sich allerdings keine Gesamtkostenübernahme ableiten. Mit der Überführung der Regelung von einem freiwilligen zu einem verpflichtenden System ist eine Gesamtkostenübernahme für alle zusätzlich (nur durch die Umsetzung der Richtlinie) entstehenden Kosten fest vorgesehen. Diskutiert wurden Modelle, in denen die betroffenen Anbieter die durch die neue Verordnung entstehenden Kosten vollständig selber zu tragen haben, bis hin zu einer vollständigen Kostenübernahme. Die oben angesprochene Einschränkung der Verwendung eines *Statutory Instrument*, sprich einer Verordnung statt eines Gesetzes, besteht darin, dass in einer solchen Verordnung keine Sanktionen verankert werden dürfen. Sträuben sich also Anbieter gegen die in der Verordnung verankerten Vorschriften, so gibt es keine Handhabe gegen diese Anbieter. Stattdessen wählte Großbritannien den Weg eines *incentive*: Durch die vollständige Kostenübernahme soll es den Anbietern leicht gemacht werden, die Vorschriften zu akzeptieren. Aus der Evaluation der Annahme der freiwilligen Vorschriften von 2001 ergab sich, dass es generelle Zustimmung in der Branche gab, so es denn zu einer angemessenen Kompensation kommt. Gleichzeitig geht das deutliche Signal aus, dass es bei einer Nichtbeachtung der neuen Regelungen zu einer gesetzlichen Festlegung der Norm in einem *Act of Parliament* und somit zu strafrechtlicher Sanktionierbarkeit kommen würde [122]

Inhaltlich bewegt sich die Umsetzung deutlich im Rahmen des bereits bestehenden nationalen Rechts zur Datenspeicherung.[123] Gleichwohl geht sie leicht über das in der Richtlinie genannte hinaus. Die Verordnung geht nicht spezifisch auf die in Art. 1(2) und 5(2) der Richtlinie enthaltene Einschränkung ein, dass keine Inhalte der Kommunikation zu speichern sind. Es wurde im Rahmen der *Consultation* aber deutlich darauf hingewiesen, dass keine solchen Inhalte zu speichern sind.[124] Das *Consultation Paper* geht spezifisch auf die Fragestellung der Verhältnismäßigkeit einer Speicherung der Daten für 12 Monate ein und verweist auf die *Consultation* im Rahmen des vorgenannten Voluntary Code of Practice. Hier wurde die Frage der Verhältnismäßigkeit des Eingriffes in die Privatsphäre der Telekommunikationsnutzer ausgiebig diskutiert.[125] Geltendes nationales[126] und supranationales Recht[127] sehen vor, dass Verhältnismäßigkeitsprinzipien bei der Speicherung von Daten zu wahren sind – der Data

[122] Vgl. 7.2., Regulatory Impact Assessment, Annex C, *Consultation Paper*, März 2003.
[123] Part 11, Anti-terrorism, Crime and Security Act 2001.
[124] 2.2, Consultation Paper.
[125] http://www.homeoffice.gov.uk/documents/consult.pdf [26.2.08].
[126] Data Protection Act 1998.
[127] Europäische Konvention zum Schutze der Menschenrechte und Grundfreiheiten.

Protection Act schreibt sogar vor,[128] dass Daten zu vernichten sind, sobald sie für ihren bestimmungsmäßigen Zweck nicht mehr gebraucht werden. Obschon die Stellungnahme der Regierung deutlich macht, dass die Vorratsdatenspeicherung über den Zeitpunkt, zu dem die erhobenen Daten zu geschäftlichen oder operativen Zwecken nicht mehr notwendig sind, hinaus eine Verletzung dieser Bestimmungen darstellt, wird doch deutlich, dass hier schwerer wiegende Belange der nationalen Sicherheit überwiegen.[129] In der Stellungnahme der Regierung[130] und im *Regulatory Impact Assessment*[131] wird allerdings darauf verwiesen, dass eine Abweichung von den Vorgaben des Data Protection Act und der Konventionsrechte auf Grund des offenkundigen Bedürfnisses aus Gründen der nationalen Sicherheit gerechtfertigt und verhältnismäßig sei.

Zur Frage der inhaltlichen Detailumsetzung kann festgestellt werden, dass die Richtlinie fast wortidentische Umsetzung findet. Die einzigen Abweichungen bestehen darin, dass die logische Verknüpfung 'oder' in Regulation 5. (1) (a) und Regulation 5. (1) (b) durch 'und' ersetzt wurden. Daraus ergibt sich möglicherweise die Notwendigkeit einer Speicherung von Daten, die über die in der Richtlinie festgelegten hinaus geht (nämlich dann, wenn 'subscriber' und 'registered user' zwei unterschiedliche Entitäten sind). Die in Artikel 5 (2) der Richtlinie enthaltene Maßgabe, dass keine Inhalte der Kommunikation im Rahmen der Richtlinie zu speichern sind, findet sich in der transponierten Fassung nicht wieder, ist aber in der *Consultation* ausdrücklich erwähnt. Die Dauer der Speicherung der Daten wird auf 12 Monate ab Erhebung festgelegt.[132] In Großbritannien generierte Daten zu ‚erfolglosen Anrufversuchen' sind zu speichern.[133] Grundsätzlich sind nur Daten zu speichern, die im normalen Geschäftsverkehr der Telekommunikationsanbieter erhoben werden und keine zusätzlichen Daten.[134]

Diskutiert wurden im Vorfeld auch andere Speicherfristen als die nun geltenden 12 Monate. Aufgrund von statistischen Daten, die sich aus der Evaluation der Effektivität der Vorgaben des ATCSA ergeben hatte, wurde die Dauer von 12 Monaten als sinnvollste Balance zwischen den Bedürfnissen der Strafverfolgungsbehörden und den Rechten der betroffenen Individuen erachtet.[135] Sollte der Telekommunikationsanbieter die Speicherung der Daten über diesen Zeitpunkt hinaus für geschäftliche Zwecke benötigen, so greifen die herkömmlichen Datenschutzregelungen des Data Protection Act 1989. In Fällen, in denen die Daten nur auf Grund der Verordnung gespeichert waren, ist eine weitere Nutzung über die in der

[128] Schedule 1, Part 1, Data Protection Act 1998.
[129] 2.2, Regulatory Impact Assessment, Annex C, Consultation Paper, März 2003.
[130] Vgl. 3.1 und 5.4, *Consultation Paper*, März 2003.
[131] Vgl. 2.2, 4.12.2, Annex C, Consultation Paper.
[132] Regulation 4(2).
[133] S.I. 2007 No. 2199, Regulation 4(3) i.V.m. Regulation 2(h).
[134] S.I. 2007 No. 2199, Regulation 4(1).
[135] Vgl. 4.16., Regulatory Impact Assessment, Annex C, *Consultation Paper*, März 2003.

Verordnung genannte Speicherfrist hinaus ausgeschlossen.[136] Um eine Rückerstattung der zusätzlich entstehenden Kosten zu erhalten, muss der Telekommunikationsanbieter diese Kosten im Vorfeld vom Innenministerium genehmigen lassen und die tatsächlich entstandenen Kosten später anzeigen und im Detail nachweisen. Die Möglichkeit eines Audit ist in der Verordnung vorgesehen.[137]

Die Verordnung enthält keine spezifischen Regelungen für den rechtmäßigen Zugriff auf die Daten. Die Daten unterliegen den normalen Bedingungen für den Zugriff auf gespeicherte Daten zu Strafverfolgungszwecken. [138] Zugreifen auf die Daten dürfen somit Security Service, der Secret Intelligence Service und das Government Communications Headquarters und vom Innenministerium spezifisch legitimierte Einzelpersonen.[139] Ein Zugriff darf nur erfolgen, wenn er ein spezifisches vom Gesetz vorgesehenes Ziel verfolgt.[140] Regulation 6 (b) untersagt darüber hinaus die anderweitige Verwendung der gespeicherten Daten ohne explizite Genehmigung – darunter würde die Verwendung zu Marketingzwecken fallen, falls der Nutzer dem nicht bereits zugestimmt hat. Die Verordnung sieht nicht vor, dass der individuelle Nutzer über die Datenspeicherung zu informieren ist. Allerdings entspricht auch das entsprechende Datenschutzrecht nicht den von der EU vorgegebenen Maßstäben.[141]

Zugriffe auf die Daten werden von den Telekommunikationsanbietern in einer Statistik gespeichert und jährlich an den Innenminister übermittelt.[142] Die Statistik soll Auskunft über die Anzahl erfolgreicher Datenzugriffe[143] und die Anzahl erfolgloser Zugriffe[144] auf die Daten geben. Die Aufzeichnung von Daten respektive der Identität zugreifender Einrichtungen oder der konkret abgerufenen Daten ist nicht vorgesehen. Als überwachende Behörde ist der Information Commissioner[145] von Großbritannien vorgesehen.[146] Für die vom Commissioner zu überwachende Datensicherheit wird festgelegt: die Daten sollen (a) die selbe Qualität haben und denselben Schutz genießen wie jene, die über das Kommunikationsnetzwerk regelmäßig übermittelt werden, (b) sie sollen mit entsprechenden technischen und organisatorischen

[136] S.I. 2007 No. 2199, Regulation 6(d).
[137] S.I. 2007 No. 2199, Regulation 10.
[138] Regulation of Investigatory Powers Act (RIPA) 2000.
[139] Section 5, RIPA.
[140] Section 22(2) a-h: Aufrechterhaltung der nationalen Sicherheit, Prävention oder Aufklärung von Straftaten, Verhinderung von Störungen der öffentlichen Ordnung, wenn der Eingriff im wirtschaftlichen Interesses Großbritanniens ist, zum Schutze der Öffentlichkeit, zum Schutze der öffentlichen Gesundheit, zur Steuerfahndung, zur Verhinderung oder Begrenzung körperlichen oder seelischen Schadens eines Einzelnen oder aus allen vom Innenminister per Verordnung festgelegten Gründen.
[141] Chalton, S. (1997) „The Transposition into UK Law of EU Directive 95/46/EC (the Data Protection Directive)" International Review of Law, Computers & Technology (11)1: 25-32, S. 28, http://www.informaworld.com/smpp/title~content=g713427069~db=all [27.2.08].
[142] S.I. 2007 No. 2199, Regulation 9.
[143] S.I. 2007 No. 2199, Regulation 9(2) a.
[144] S.I. 2007 No. 2199, Regulation 9(2) b.
[145] Ein von der Krone ernannter Beamter, der die Einhaltung des Data Protection Act 1998 und des Freedom of Information Act 2000 überwacht.
[146] S.I. 2007 No. 2199, Regulation 8.

Schutzmechanismen vor versehentlicher Löschung oder Beschädigung und fremdem Zugriff geschützt werden, (c) nur autorisierten Personen zugänglich sein und (d) am Ende der Speicherfrist gelöscht werden.[147]

Bei einer Nichteinhaltung der Vorgaben zum Datenschutz und der Datensicherheit ist der Information Commissioner lediglich befugt, die Rolle eines Ombudsmannes einzunehmen.[148] Falls es zu keiner einvernehmlichen Lösung kommt, steht der normale Weg des Judicial Review (gerichtliche Überprüfung) offen.[149]

Frage 2:
Was sind die Gründe, aus denen die übrigen ausgewählten Mitgliedstaaten noch nicht umgesetzt haben?

Für Großbritannien nicht einschlägig.

Frage 3:
Welche Umsetzungspläne verfolgen jene Mitgliedstaaten, die die Richtlinie bislang noch nicht umgesetzt haben, in zeitlicher bzw. inhaltlicher Hinsicht?

Für Großbritannien nicht einschlägig.

Frage 4:
Wie wirkt sich die im Juli 2006 von Irland eingebrachte Klage vor dem Europäischen Gerichtshof auf die Umsetzungsbestrebungen dieser Staaten aus?

Die Stellungnahme der Regierung zu der Umsetzung der Richtlinie geht mehrfach auf das irische Verfahren ein und unterstreicht, dass selbst ein Scheitern der Richtlinie vor dem EuGH keinen Einfluss auf die Wirkung der Verordnung in Großbritannien habe.[150] Es erscheint durchaus deckungsgleich mit den Bestrebungen der britischen Regierung, das bisher freiwillige System der Datenspeicherung zur Terrorismusbekämpfung in ein verbindliches System zu überführen und auch ohne die EU Norm würde eine solche Gesetzgebung in Großbritannien zweifelsfrei erfolgen.

[147] S.I. 2007 No. 2199, Regulation 6 (a)-(d).
[148] http://www.ico.gov.uk/complaints/privacy_and_electronic_communications.aspx [27.2.08].
[149] Für England und Wales: Part 54, Civil Procedure Rules.

Frage 5:

Welche Reaktionen seitens der Zivilgesellschaft lassen sich in den ausgewählten Mitgliedstaaten erkennen?

Zur Frage der gesellschaftlichen Reaktion ist offenkundig, dass die ursprüngliche Richtlinie zwar in der einschlägigen Fachpresse kontrovers diskutiert wurde, die umsetzende Verordnung allerdings deutlich weniger Aufmerksamkeit erregte als in vergleichbaren Jurisdiktionen wie z.B. die der Republik Irland (wo Interessengruppen ein zivilrechtliches Verfahren in der Sache anstrengen). Interessenverbände und –gruppen, wie z.B. *The National Council on Civil Liberties* kommentieren weder die Richtlinie noch die Verordnung in einschlägigen Publikationen.[151] Über die in Printmedien diskutierten Auswirkungen der Richtlinie für Strafverfolgungen in Urheberrechtsfällen im Internet hinausgehende Reaktionen sind augenscheinlich nicht zu verzeichnen. Eine merkliche Reaktion kann somit nicht festgestellt werden, wäre aber in Anbetracht der bereits seit Jahren existierenden identischen Normen auch verspätet.

[150] 2.6, Regulatory Impact Assessment, Annex C, Consultation Paper, März 2003; 6.5, Consultation Paper, März 2003.

[151] Vgl. „Liberty's response to the Home Affairs Committee Inquiry into 'A Surveillance Society'", April 2007, http://www.liberty-human-rights.org.uk/pdfs/policy07/home-affairs-ctte-surveillance-society.pdf [26.2.08].

Artikel 5 Transposition Matrix

Art. 5, Directive		*Regulation 5, SI*	
1.(a) (1) (i.)	*The calling telephone number.*	*(1) (a)*	
1.(a) (1) (ii.)	*Name and address of the subscriber or registered user*	*(1) (a)*	*The name and address of the subscriber <u>and</u> registered user of that telephone.*
1.(b) (1) (i.)	*The numbers dialled, the number or numbers to which the call is routed*	*(1) (b)*	
1.(b) (1) (ii.)	*Name and addresses of the subscribers or registered users*	*(1) (b)*	*Name and address of the subscriber <u>and</u> registered user*
1.(c) (1)	*Date and time of the start and the end of the communication*	*(1) (c)*	
1.(d) (1)	*The telephone service used*	*(1) (c)*	
1.(e) (1)	*For fixed network telephony: The calling and called telephone numbers*	*(1) (a) – above*	
1.(e) (2) (i.)	*For mobile telephony: the calling and called telephone numbers*	*(1) (a) – above*	
1.(e) (2) (ii.)	*For mobile telephony: the IMSI of the calling party*	*(2) (a)*	
1.(e) (2) (iii.)	*For mobile telephony: the IMEI of the calling party.*	*(2) (a)*	
1.(e) (2) (iv.)	*For mobile telephony: the IMSI of the called party.*	*(2) (b)*	

1.(e) (2) (v.)	***For mobile telephony: the IMEI of the called party.***	***(2) (b)***
1.(e) (2) (vi.)	***For prepaid or anonymous mobile telephony: the date and time of the initial activation of the service and the Cell ID from which the service was activated.***	***(2) (c)***
1.(f) (1)	***For mobile telephony: the location label (Cell ID) at the start of the communication***	***(2) (d)***
1.(f) (2)	***For mobile telephony: data identifying the the geographic location of cells by reference to their location labels (Cell ID).***	***(2) (e)***
2.	***No Data in relation to the content of the communication.***	***N/A***

Irland

Zusammenfassung: Die Republik Irland hat die Richtlinie bisher noch nicht umgesetzt. Die Gründe hierfür liegen an der unklaren Rechtslage, insbesondere auf nationaler Ebene (wo ein Verfahren anhängig ist) und an dem Wunsch, den Ausgang des EuGH Verfahrens abzuwarten. Bestehende Normen sehen bereits eine Datenspeicherung für drei Jahre vor, so dass sich erhebliche Proteste von Interessengruppen gegen diese Normen und auch gegen die geplanten neuen Normen richten. Die Umsetzung der Richtlinie würde die Speicherfrist auf zwei Jahre reduzieren allerdings auch bisher noch nicht erfasste Daten in die Vorratsdatenspeicherung mit einbeziehen. Mit einer Umsetzung wird frühestens Ende März gerechnet.

Frage 1:

Welche Regelungen wurden von denjenigen ausgewählten Mitgliedstaaten getroffen, die die Richtlinie bereits umgesetzt haben?

Die Frage ist noch nicht einschlägig für die Republik Irland. Eine Umsetzung wird inzwischen im Rahmen eines *Statutory Instrument*[152] bis Ende Februar angekündigt.[153] Der Wortlaut ggf. existierender Entwürfe für eine Rechtsverordnung liegt noch nicht vor. Bereits bestehende Normen in der irischen Antiterrorgesetzgebung[154] gehen in Teilen über die in der Richtlinie verlangten hinaus, in anderen Teilen erreichen sie nicht das in der Richtlinie vorgegebene Maß. Hierauf wird im weiteren Verlauf (3.) noch eingegangen.

Frage 2:

Was sind die Gründe, aus denen die übrigen ausgewählten Mitgliedstaaten noch nicht umgesetzt haben?

Die Republik Irland hat wegen der Rechtsgrundlage (Art. 95 EG Vertrag) die Richtlinie vor dem EuGH angefochten.[155] Obschon die Umsetzung der Richtlinie nicht von der Entscheidung des EuGH abhängig ist, zeigt sich – auch auf Grund eines komplexen nationalen Verfahrens zur Verhinderung der Vorratsdatenspeicherung – erheblicher Widerwillen bei der Umsetzung.[156] Außerdem ist in Irland noch eine Klage gegen die Umsetzungsbestrebungen

[152] Secondary Legislation (Rechtsverordnung) die ohne maßgebliche Beteiligung des Parlaments und somit sehr schnell in Kraft treten kann.
[153] The Irish Times, 19. Januar 2008.
http://www.ireland.com/newspaper/frontpage/2008/0119/1200605160420.html [27.2.08].
[154] Criminal Justice (Terrorist Offences) Act 2005.
[155] Case C-301/06.
[156] In parlamentarischen Debatten wird stets auf das anhängige Verfahren verwiesen um die Verzögerung der Umsetzung zu begründen: Oireachtas Debate, 14. Nov. 2006, Seiten 825 und 826.
http://debates.oireachtas.ie/Xml/29/DAL20061114A.PDF [27.2.08].

vor dem High Court anhängig.[157] Das seit September 2006 laufende nationale Verfahren, in dessen Rahmen eine Nichtregierungsorganisation (Digital Rights Ireland) die Verfassungskonformität der entsprechenden Normen anficht, erstreckt sich sowohl auf die Vorratsdatenspeicherung, die im Antiterrorgesetz vorgesehen ist, als auch auf die Umsetzung der Richtlinie.[158] Bemängelt wird die Vereinbarkeit der neuen Normen mit der irischen Verfassung und der Europäischen Konvention zum Schutze der Menschenrechte und Grundfreiheiten.

Frage 3:

Welche Umsetzungspläne verfolgen jene Mitgliedstaaten, die die Richtlinie bislang noch nicht umgesetzt haben, in zeitlicher bzw. inhaltlicher Hinsicht?

Die irische Presse berichtet, dass die derzeitigen Bestrebungen darauf abzielen, eine Umsetzung vor Ende Februar zu erreichen. Diese Umsetzung soll, im Interesse einer schnellstmöglichen Umsetzung, im Rahmen einer Verordnung stattfinden. Gerade diese Vorgehensweise wird wegen des damit einhergehenden Mangels an einer parlamentarischen Beteiligung kritisiert.[159] Auch wird der Zeitplan von Experten schon allein deshalb als unrealistisch eingeschätzt, weil noch keine Konsultation mit der ISPAI (Internet Service Providers of Ireland) zu der Verordnung stattgefunden hat.[160, 161] Eine Umsetzung wird dementsprechend frühestens Ende März erwartet.[162]

Der Status quo in Irland deckt sich jedoch bereits jetzt in vielen Teilen mit den von der Richtlinie umfassten Bestimmungen.[163] Die bestehenden Antiterrorgesetze sehen vor, dass auf Anordnung eines Polizeipräsidenten[164] ein spezifischer Telekommunikationsanbieter[165] alle verfügbaren Daten für drei Jahre aufzubewahren hat.[166] Das Gesetz ist deutlich abstrakter

---

[157] *Digital Rights Ireland Ltd. v The Minister for Communications, Marine and Natural Resources et al.* (2006) No. 3785P (High Court). Statement of Claim (Klageschrift): http://www.mcgarrsolicitors.ie/wp-content/Files/Statement%20of%20claim.pdf [27.2.08].

[158] *Digital Rights Ireland Ltd. v The Minister for Communications, Marine and Natural Resources et al.*, Klageschrift, Nr. 17 u. 18.

[159] The Irish Times, 19. Januar 2008. http://www.ireland.com/newspaper/frontpage/2008/0119/1200605160420.html [27.2.08].

[160] Irland hat die Ausnahmeregelung nach Artikel 15(3) der Richtlinie nicht in Anspruch genommen und plant sowohl Festnetz- und Mobilfunkdaten als auch internetbasierte Daten zu erfassen.

[161] Korrespondenz mit TJ McIntyre, Lecturer für Informatikrecht in der Law School der University College Dublin und Vorsitzender von Digital Rights Ireland.

[162] TJ McIntyre, [26.2.08].

[163] Die Genese des irischen Telekommunikationsrechts und der Normen zur Vorratsdatenspeicherung lässt sich einem umfassenden Artikel entnehmen: McIntyre, TJ (2007) „Data Retention: History and Developments" Data Protection Law and Policy 2:14. Der Autor ist Vorsitzender der Organisation, die sich vehement gegen die Umsetzung der Richtlinie ausspricht.

[164] Garda Commissioner (etwa: Polizeipräsident).

[165] Es liegen keine Zahlen vor, wie vielen Telekommunikationsanbietern eine entsprechende Anordnung erhalten haben. Der Justizminister gibt an anderer Stelle (und im Kontext der mit dem selben rechtlichen Mechanismus anzuordnenden Abhörverfahren) zu bedenken, dass die Veröffentlichung der Daten den Interessen der nationalen Sicherheit widerspräche. Irish Independent, 14.3.07. http://www.independent.ie/national-news/mcdowell-wont-reveal-number-of-phone-taps-hes-authorised-49609.html [27.2.08].

[166] Section 63, Criminal Justice (Terrorist Offences) Act 2005: "*traffic data* and *location data*" (Kommunikationsdaten und geographische Daten).

als die Richtlinie und erstreckt sich auf einige wenige Absätze. Die in der Richtlinie genannten Daten, so sie denn geschäftsmäßig von dem Telekommunikationsanbieter erhoben werden, sind in den Formulierungen jedoch allesamt erfasst. Die Ausnahme stellen Daten von anonymen Diensten dar (im Gesetz sind dies jene Dienste, die nicht einer konkreten Person zugeordnet werden können) – hier besteht keine Verpflichtung, die Daten zu speichern.[167] Dies erfasst nicht die in der Richtlinie genannten Prepaid und anonymen Dienste. Die Umsetzung der Richtlinie in Irland würde demnach voraussichtlich zu einer Verringerung der Speicherfrist auf maximal 2 Jahre führen sowie die Speicherung anonymer Dienste mit einbeziehen.

Frage 4:

Wie wirkt sich die im Juli 2006 von Irland eingebrachte Klage vor dem Europäischen Gerichtshof auf die Umsetzungsbestrebungen dieser Staaten aus?

Die Klage verzögert im Wesentlichen die Umsetzung, wird sie aber nicht verhindern. Innerhalb der Regierung scheint es Unstimmigkeiten zu der Umsetzung zu geben: Das Department of Justice spricht sich für die Vorratsdatenspeicherung aus, das Department of Communications eher dagegen.[168] Nach einer Rüge der EU Kommission im Januar 2008 scheint nun Bewegung in die Umsetzungsbestrebungen gekommen zu sein.[169]

Frage 5:

Welche Reaktionen seitens der Zivilgesellschaft lassen sich in den ausgewählten Mitgliedstaaten erkennen?

Bereits seit Inkrafttreten der Antiterrorgesetzgebung zeigt sich deutliche und laute Kritik an der Vorratsdatenspeicherung, die sich nun auch auf die Umsetzung der Richtlinie erstreckt. Vorreiter bei der Kritik an der Umsetzung der Richtlinie ist die Nichtregierungsorganisation *Digital Rights Ireland*, die sowohl in den Medien dagegen opponiert[170] als auch durch den *High Court* die Vorratsdatenspeicherung gerichtlich überprüfen lässt.[171] Der *Irish Council for Civil Liberties* hat sich bereits gegen die Antiterrorgesetze ausgesprochen, die eine weitaus größere Vorratsdatenspeicherung vorsieht.[172] Darüber hinaus wurde berichtet,[173] dass sich auch die irische staatliche Regulierungsbehörde für Menschenrechte (*An Coiumisiún um*

[167] Section 63(6), Criminal Justice (Terrorist Offences) Act 2005.
[168] TJ McIntyre, [26.2.08]
[169] Irish Times, 19.1.08. http://www.ireland.com/newspaper/frontpage/2008/0119/1200605160420.html [27.2.08].
[170] Irish Times, 19.1.08; http://www.digitalrights.ie/category/data-retention/ .
[171] *Digital Rights Ireland Ltd. v The Minister for Communications, Marine and Natural Resources et al.* (2006) No. 3785P (High Court).
[172] http://www.iccl.ie/DB_Data/press/Govt_Prop_Comm_monitor_02_161.htm [27.2.08].
[173] Irish Times, 7.12.07, http://www.ireland.com/newspaper/finance/2007/1207/1196839051643.html [27.2.08]; auch Verfügbar hier: http://www.techno-culture.com/?p=131 [27.2.08].

Chearta Duine, Irish Human Rights Commission[174]) als *amicus curiae* in das nationale Verfahren einschalten wird. Falls es in dem Verfahren zu einer Entscheidung im Sinne der Klägerin kommt, ist damit zu rechnen, dass es zu einer Prüfung der Verfassungsmäßigkeit der bestehenden Gesetzgebung und der die Richtlinie umsetzenden Verordnung kommen muss.

[174] http://www.ihrc.ie/home/default.asp [27.2.08].

Italien

Zusammenfassung: Italien hat die Richtlinie noch nicht umgesetzt. Bis zum Ende des Jahres 2007 bestanden in Italien rechtliche Regelungen, die über die Richtlinie noch hinausgingen. Für die Umsetzung gibt es zwar Gesetzentwürfe, deren Mehrheitsfähigkeit aber nicht feststeht. Mehrere Nichtregierungsorganisationen haben Kritik an der Richtlinie geäußert. Eine weitere Organisation hat zudem einen zurückhaltenden Umsetzungsentwurf verfasst.

Frage 1:

Welche Regelungen wurden von denjenigen ausgewählten Mitgliedstaaten getroffen, die die Richtlinie bereits umgesetzt haben?

Italien hat die Richtlinie bisher nicht umgesetzt.

Frage 2:

Was sind die Gründe, aus denen die übrigen ausgewählten Mitgliedstaaten noch nicht umgesetzt haben?

Italien hat von der Möglichkeit, die Umsetzungsfrist im Hinblick auf Access-, VoIP- und Email-Provider durch eine entsprechende Erklärung bis zum 15. März 2009 zu verlängern, [175] keinen Gebrauch gemacht. Die Umsetzungsfrist endete daher auch in Bezug auf diese Daten am 15.09.2007. Eine mögliche Ursache für die Verzögerung der Umsetzung ist die gegenwärtige politische Lage Italiens. Unter diesen Umständen lässt sich kaum feststellen, ob die Umsetzung im Parlament hohe Priorität genießt.

Italien verfügte, unabhängig von der Richtlinie 2006/24/EG, mit dem Dekret 259/2003[176] und vor allem mit dem Dekret-Gesetz Nr. 144 über nationale Bestimmungen zur Vorratsdatenspeicherung. Allerdings waren die Teile der Dekrete, die die Vorratsspeicherung regelten, bis zum 31. Dezember 2007 befristet. Da ihre Gültigkeit nicht verlängert wurde, verfügt Italien seit dem 01. Januar 2008 über keine Vorschriften mehr, die eine Vorratsdatenspeicherung erlauben. Es erscheint wahrscheinlich, dass die Umsetzung der Richtlinie 2006/24/EG zunächst wegen der bis zum 31. Dezember 2007 bestehenden Regelungen nicht als prioritär angesehen und letztlich durch die politische Krise Ende 2007 nicht angegangen wurde.

[175] Art. 15 Abs. 3 der Richtlinie. Vgl. auch die Erklärungen anderer Mitgliedstaaten im Anhang der Richtlinie.
[176] http://www.agcom.it/L_naz/cod_comunicaz_dl259_03.htm .

Frage 3:

Welche Umsetzungspläne verfolgen jene Mitgliedstaaten, die die Richtlinie bislang noch nicht umgesetzt haben, in zeitlicher bzw. inhaltlicher Hinsicht?

Italien hat die Richtlinie 2006/24/EG noch nicht in italienisches Recht umgesetzt. Derzeit sind keine Hinweise auf einen konkreten Umsetzungsprozess auffindbar, sodass gegenwärtig auch keine Aussage über den Inhalt der zukünftigen Regelungen getroffen werden kann, mit denen die Richtlinie umgesetzt werden soll. Allerdings hatte Italien bereits nach der EG-Datenschutzrichtlinie für elektronische Kommunikation (2002/58/EG) gesetzliche Regelungen zur Vorratsdatenspeicherung erlassen. Diese waren jedoch bis zum 31.12.2007 befristet, so dass sie keine Gültigkeit mehr besitzen. Trotzdem werden sie im Folgenden kurz beschrieben, da sich die Regelungen zur Umsetzung der Richtlinie 2006/24/EG eventuell an diesen Vorschriften orientieren könnten. Im August 2003 trat das Dekret 259/2003[177] in Kraft, das die Pflicht zur Vorratsspeicherung von Telefonie-Verkehrsdaten – jedoch nicht von Standortdaten[178] – für die Dauer von 48 Monaten vorgeschrieben hat.

Im Juli 2005 hat die italienische Regierung außerdem das Dekret-Gesetz Nr. 144 über Maßnahmen zur Terrorismusbekämpfung erlassen, das die Vorratsdatenspeicherung unter Verdrängung aller einschlägigen Datenschutzbestimmungen bis zum 31.12.2007 eingeführt hat.[179]

Das Dekret-Gesetz Nr. 144 hat darüber hinaus auch eine Verpflichtung zur Identifikation von Mobilfunk-Teilnehmern eingeführt, und zwar bevor der Dienst aktiviert wird, also bei Bestellung oder spätestens Übergabe der SIM-Karte.[180] Hinsichtlich Prepaid-Karten müssen die Mobilfunkanbieter bestmöglich sicherstellen, dass die Identität des Karteininhabers feststeht und zu diesem Zweck u.a. eine Fotokopie des Lichtbildausweises aufbewahren. Art. 6 des Dekrets schreibt vor, dass die TK-Diensteanbieter alle Daten betreffend „die Rückverfolgbarkeit des Zugangs und – soweit möglich – des in Anspruch genommenen Dienstes“ speichern müssen, jedoch ausdrücklich ohne Kommunikationsinhalte.[181]

Es ist zu erwarten, dass in den Anwendungsbereich der italienischen Umsetzung nicht nur Mobilfunkanbieter und Access-Provider fallen, sondern auch Internetcafés sowie Gaststät-

[177] Dekret 259 vom 1.08.2003: „Codice delle comunicazioni elettroniche“ (Gesetz über elektronische Kommunikation), http://www.agcom.it/L_naz/cod_comunicaz_dl259_03.htm (auf italienisch).
[178] Siehe auch Gesetz 196/2003, „Codice in materia di protezione dei dati personali“ (Gesetz über den Schutz personenbezogener Daten).
[179] Dekret-Gesetz Nr. 144 vom 27.07.2005, „Misure urgenti per il contrasto del terrorismo internationale” (Eilmaßnahmen zur Bekämpfung des internationalen Terrorismus), http://gazzette.comune.jesi.an.it/2005/173/1.htm (auf italienisch).
[180] Art. 6 Abs. 2 des Dekret-Gesetzes Nr. 144, der ausdrücklich Art. 55 Abs. 7 des Dekrets Nr. 259 vom 1.08.2003 derogiert.

ten, Hotels, Flughäfen usw.[182] Tatsächlich müssen bereits gem. Art. 7 des Dekret-Gesetzes Nr. 144 Intenetcafés und Telefonshops mit drei oder mehr Endgeräten eine Lizenz bei einem Quaestor (örtliche Vertretung des Innenministeriums) beantragen. Außerdem müssen die Stammdaten der Kunden erhoben werden. WLAN-Hotspots und ähnliche Einrichtungen, die keine Verkehrsdaten speichern, müssen amtliche Lichtbildausweise von den Benutzern einsehen.[183]

Dem italienischen Abgeordnetenhaus liegt ein Gesetzentwurf der Partei „La Rosa nel Pugno“[184] vor, die allerdings angesichts eines Stimmanteils von 2,6% bei den Parlamentswahlen 2006 und 18 Sitzen in der Abgeordnetenkammer, über keinen nennenswerten politischen Einfluss verfügt. Der Titel der Vorlage ist „Regelungen zur automatischen Erhebung, Verwendung, Speicherung und Löschung von standort- und zeitbezogenen Daten, die eindeutige Benutzerkennungen enthalten“. [185]

Der Gesetzentwurf wurde von der Bürgerrechtsorganisation „Winston Smith Project“ [186] initiiert und hadert nicht mit den Speicherpflichten der Richtlinie, sondern versucht, im Rahmen der Umsetzung die Quantität der zu speichernden Daten zu minimieren und eine Löschungspflicht zu etablieren, wonach automatisch erhobene Daten nicht länger aufbewahrt werden sollen, als zur Erreichung des Speicherungszwecks unbedingt notwendig. Der Gesetzentwurf zielt insgesamt darauf ab, die Löschung der Daten zur Regel – und nicht zur Ausnahme – zu machen. [187]

Frage 4:

Wie wirkt sich die im Juli 2006 von Irland eingebrachte Klage vor dem Europäischen Gerichtshof auf die Umsetzungsbestrebungen dieser Staaten aus?

Da derzeit ein mit realen Umsetzungschancen versehenes Gesetzesvorhaben nicht vorliegt, kann nicht festgestellt werden, welchen Einfluss die Klage Irlands auf den noch zu erwartenden Gesetzgebungsprozess haben wird.

---

[181] Ebendort.
[182] *Cameron Craig / Alisa Bergman* (DLA Piper Rudnick Gray Cary), „Data retention“, 26. April 2006, http://www.totaltele.com/View.aspx?ID=81829&t=4.
[183] *EDRI*, „Italy Decrees Data Retention Until 31 December 2007“, http://www.edri.org/edrigram/number3.16/Italy.
[184] Laizistische sozialistische liberale radikale Partei „La Rosa nel Pugno“, http://www.rosanelpugno.it.
[185] “New Proposal on Data Retention”, 23.11.2006, http://www.legislationline.org/?jid=27.
[186] In Anlehnung an George Orwells Romanfigur Winston Smith, http://pws.winstonsmith.info/index-e.html.
[187] “New Proposal on Data Retention”, 23.11.2006, http://www.legislationline.org/?jid=27.

Frage 5:

Welche Reaktionen seitens der Zivilgesellschaft lassen sich in den ausgewählten Mitgliedstaaten erkennen?

Die Zivilgesellschaft reagierte auch in Italien zum Teil ablehnend auf die Richtlinie. Dies gilt insbesondere für die unabhängige Organisation ALCEI, [188] die auch mit der irischen Bewegung Digital Rights Ireland (DRI)[189] zusammenarbeitet. ALCEI hat ihren statutorischen Sitz in Mailand, operiert jedoch in ganz Italien und darüber hinaus. ALCEI bespricht und unterstützt auf seiner Website die Nichtigkeitsklage Irlands gegen die Richtlinie.[190]

[188] ALCEI steht für "Associazione per la libertà nella comunicazione elettronica interattiva" (Vereinigung für die Freiheit der elektronischen interaktiven Kommunikation), http://www.alcei.org/.
[189] Digital Rights Ireland, http://www.digitalrights.ie.
[190] http://www.alcei.org/?p=23.

Niederlande

Zusammenfassung: In den Niederlanden wurde die Richtlinie bislang nicht umgesetzt, ein Gesetzesentwurf liegt seit Dezember 2006 vor. Der Vorschlag zeichnet sich vor allem durch mangelnde Rechtsschutzregelungen aus. Widerstand in der Zivilbevölkerung ist äußerst schwach ausgeprägt, öffentlich kritisch zeigt sich hingegen wiederholt die niederländische Datenschutzbehörde.

Frage 1:

Welche Regelungen wurden von denjenigen ausgewählten Mitgliedstaaten getroffen, die die Richtlinie bereits umgesetzt haben?

Da die Niederlande die Richtlinie innerstaatlich noch nicht umgesetzt haben, ist diese Frage nicht einschlägig.

Frage 2:

Was sind die Gründe, aus denen die übrigen ausgewählten Mitgliedstaaten noch nicht umgesetzt haben?

Nach Aussagen des niederländischen Staatssekretärs für europäische Angelegenheiten ist die nationale Umsetzung der Vorratsdatenspeicherung nicht nur technisch höchst kompliziert sondern auch politisch umstritten. Vor allem aber habe die notwendige Beratung mit den Interessenvertretern (insbesondere der Provider und der Ermittlungsbehörden) sehr viel Zeit in Anspruch genommen, worauf die Verzögerung maßgeblich zurückzuführen sei.[191]

Frage 3:

Welche Umsetzungspläne verfolgen jene Mitgliedstaaten, die die Richtlinie bislang noch nicht umgesetzt haben, in zeitlicher bzw. inhaltlicher Hinsicht?

Seit 11. Dezember 2006 liegt ein Entwurf vor, mit dem das Telekommunikationsgesetz sowie das Gesetz zur Wirtschaftskriminalität geändert und damit die Richtlinie 2006/24/EG in niederländisches Recht umgesetzt werden soll.[192] Der Gesetzesentwurf eröffnet der Verwaltung einen großen Spielraum. So ist zwar keine explizite Abweichung von den zu speichernden Datenkategorien nach Art 5 Abs 1 der Richtlinie vorgesehen, doch können diese Kategorien durch Verordnung bestimmt werden. Eine Speicherung von Daten über „erfolglose Gesprächsverbindungen“ iSd Art 3 Abs 2 der RL ist nicht vorgeschrieben.

[191] http://www.minbuza.nl/nl/actueel/brievenparlement,2008/01/Kamerbrief-inzake-stand-van-zaken-implementatie-Eu.html.

Obwohl Anfang 2006 eine Mehrheit des Parlaments anscheinend zugestimmt hatte, die Vorratsdatenspeicherungsfristen in den Niederlanden zu kürzen, entschied sich die Regierung in der Gesetzesvorlage nun für die beinahe maximale Frist von 18 Monaten sowohl für Telefon- als auch für Internetaufzeichnungen.

Das Parlament verabschiedet außerdem ein Gesetz, wonach die niederländischen Geheimdienste und die nationale Sicherheitsbehörde (AIVD) befugt sind, vollständige Datenaufzeichnungen aus dem öffentlichen und privaten Bereich einzufordern. Die neuen Befugnisse richten sich gezielt auf den Transit, die elektronischen Kommunikationen und den Finanzsektor. Diese Gesetzgebung wird es den Behörden ermöglichen, den maximalen Nutzen aus den ausgeweiteten Speicherungen von persönlichen Daten in diesen Sektoren zu schlagen.[193]

Die Aufsichtsfunktion in Sachen Vorratsdatenspeicherung kommt dem Wirtschaftsminister zu. Der Minister hat seine diesbezüglichen Tätigkeiten mit der nationalen Datenschutzbehörde (Dutch Data Protection Authority) zu koordinieren. Diese selbst hat dann Kontrollbefugnisse, wenn es um Daten geht, die als „persönliche Daten" zu qualifizieren sind. Die Kontrollaufgaben des Wirtschaftsministers beziehen sich auf 4 Bereiche: Er überwacht die Einhaltung der Speicherverpflichtung durch die Provider; die – gesetzlich noch zu regelnden – Bedingungen, unter denen die Daten gespeichert werden (insbesondere im Hinblick auf Sicherheitsstandards); die Sicherheitsmaßnahmen gegen Missbrauch der vorrätig gespeicherten Daten; schließlich überwacht er die rechtzeitige Löschung der Daten nach Ablauf der Speicherfrist.

Darüber hinaus kennt der Entwurf jedoch keine subjektiven Rechtsschutzgarantien für Personen, die von einer Datenabfrage betroffen sind. Dass diese über einen erfolgten Datenzugriff informiert werden müssen, ergibt sich aber aus Art 35 des niederländischen Datenschutzgesetzes, welches die *Richtlinie 95/46/EG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr* umsetzt.

Die Kosten, welche den Nezt- und Dienstanbietern durch die Vorratsspeicherung erwachsen, werden nach dem Entwurf ersetzt. Die Provider sind aber nicht berechtigt, die Daten für eigene Zwecke (z.B. Marketing) zu verwenden.

[192] In holländischer Sprache abrufbar unter http://www.minez.nl/dsresource?objectid=149506&type=PDF.

Frage 4:

Wie wirkt sich die im Juli 2006 von Irland eingebrachte Klage vor dem Europäischen Gerichtshof auf die Umsetzungsbestrebungen dieser Staaten aus?

Die eingebrachte Klage hat keinen Einfluss auf die Umsetzung der Richtlinie in den Niederlanden.

Frage 5:

Welche Reaktionen seitens der Zivilgesellschaft lassen sich in den ausgewählten Mitgliedstaaten erkennen?

Ablehnende Reaktionen aus der Zivilbevölkerung sind in den Niederlanden nur sehr schwach ausgeprägt. Hervorzuheben ist die niederländische Bürgerrechtsorganisation Bits of Freedom. Im Jahr 2004 förderten deren Nachforschungen samt einem entsprechenden formellen Antrag eine vom niederländischen Justizministerium 2002 in Auftrag gegebene Studie zutage, die von der Regierung bis dahin unter Verschluss gehalten wurde, auch gegenüber dem Parlament. Es handelte sich dabei um Statistiken über die Wirksamkeit der Vorratsdatenspeicherung bzw. eine Dokumentation über Probleme bei fehlender Datenspeicherung, also eine Untersuchung der Polizeiarbeit auf ihre Abhängigkeit von Speicherdaten. Dabei stellten Polizei und das Beratungsunternehmen Stratix fest, dass in 90 Prozent aller Ermittlungen auf Verkehrsdaten zugegriffen wurde, die der Provider für die Abrechnung gespeichert hatte. Allerdings hätten selbst beim kompletten Verzicht auf diese Daten noch zwei Drittel der Fälle erfolgreich abgeschlossen werden können. Dieses Dokument spielte in der nachfolgenden parlamentarischen Debatte zur Richtlinienumsetzung eine nicht geringe Rolle.[194]

Doch ist die Organisation Bits of Freedom mittlerweile nur mehr sehr eingeschränkt aktiv, einzig die Verleihung der niederländischen *Big Brother Awards*[195] steht noch auf ihren Agenden. 2007 wurde diese „Auszeichnung" wegen dem offenbaren Desinteresse der Öffentlichkeit und der Unbekümmertheit, mit der die Mehrheit der niederländischen Bürger ihre Privatsphäre für das Versprechen von mehr Sicherheit aufgibt, an die Bevölkerung selbst verliehen.

---

[193] Aus dem zweiwöchentlich erscheinenden Newsletter von European Digital Rights(EDRi), auf deutsch unter http://www.unwatched.org/node/849.

[194] Onlineauszug aus dem Computermagazin c't 22/2004, S. 66 unter http://www.heise.de/ct/04/22/066.

[195] Die Big Brother Awards sind Negativpreise, die jährlich in mehreren Ländern an Behörden, Firmen, Organisationen und Personen vergeben werden. Die Preise werden an jene verliehen, die in besonderer Weise und nachhaltig die Privatsphäre von Personen beeinträchtigen oder Dritten persönliche Daten zugänglich gemacht haben oder machen. Ins Leben gerufen wurden die Big Brother Awards 1998 von Privacy International, einer 1990 gegründeten, international tätigen Menschenrechtsorganisation mit Sitz in London; siehe http://www.privacyinternational.org.

Deutliche und auch inhaltlich scharf ausgeprägte Kritik kommt demgegenüber von der nationalen Datenschutzbehörde, der Dutch Data Protection Authority (Dutch DPA)[196]. Gerügt wird vor allem, dass die im Vorschlag enthaltene Speicherfrist von 18 Monaten einen unverhältnismäßigen Eingriff in das Recht auf Privatsphäre (Art 8 EMRK) darstelle, zumal nicht gezeigt werden konnte, warum es zu Zwecken der Verhütung oder Verfolgung schwerer Straftaten notwendig sei, die Daten derart lange zu speichern. Außerdem bemängelt die Behörde, dass im Entwurf keine ausreichende Beschränkung der Personen/Behörden enthalten sei, die Zugang zu den Informationen haben. Gleichzeitig seien kaum effektive Kontrollmechanismen vorgesehen. Dass zudem die Entscheidung über die Kategorien der zu speichernden Daten an die Verwaltung delegiert sei, negiere die demokratische Schutzfunktion einer formellen Gesetzgebung. Überhaupt würden die mit der Speicherverpflichtung für die Provider und letztlich für deren Kunden einhergehenden Kosten den Nutzen eindeutig übersteigen. Die Dutch DPA fordert schließlich, dass die nationale Umsetzung unter größtmöglichster Transparenz erfolgen müsse, jedenfalls sei die Veröffentlichung von Statistiken, ob und in welcher Weise Betroffene über eine Abfrage ihrer Daten benachrichtigt wurden, unbedingt notwendig.

[196] College bescherming persoonsgegevens (CBP), siehe http://www.dutchdpa.nl; eine offizielle Stellungnahme findet sich in englischer Übersetzung unter http://www.dutchdpa.nl/documenten/en_med_20070124_european_directive.shtml?refer=true.

Portugal

Zusammenfassung: Portugal hat die Richtlinie noch nicht umgesetzt, jedoch liegt ein entsprechender Gesetzentwurf dem Parlament vor. Entwurfsgemäß sollen viele Polizei- und Sicherheitsbehörden Zugriff auf die zu speichernden Daten erhalten. Der Straftatenkatalog für die Verwendung der Verkehrsdaten stimmt mit dem für die Aufzeichnung von Kommunikationsinhalten überein. Es gibt mehrere zivilgesellschaftliche Aktionen gegen die Richtlinie und ihre Umsetzung, insbesondere von Journalistenverbänden.

Frage 1:

Welche Regelungen wurden von denjenigen ausgewählten Mitgliedstaaten getroffen, die die Richtlinie bereits umgesetzt haben?

Portugal hat die Richtlinie bisher nicht umgesetzt. Es existiert jedoch ein Umsetzungsentwurf.

Frage 2:

Was sind die Gründe, aus denen die übrigen ausgewählten Mitgliedstaaten noch nicht umgesetzt haben?

Laut dem Summary Report der Europäischen Union über die Umsetzung der Richtlinie[197] in den Mitgliedstaaten liegt dem portugiesischen Parlament zwar ein Gesetzentwurf zur Vorratsdatenspeicherung vor, dessen Umsetzung in der portugiesischen Politik mit Priorität verfolgt werde. Aussagen, wann die Umsetzung tatsächlich erfolgen wird, seien allerdings nicht möglich.[198] Portugal hat zudem keine Erklärung gem. Art. 15 Abs. 3 der Richtlinie abgegeben, die eine Verlängerung der Umsetzungsfrist hinsichtlich der Vorratsspeicherung von Internet-Access-, VoIP- und Email-Daten um achtzehn Monate nach der in Art. 15 Abs. 2 genannten Frist zur Folge gehabt hätte. Dementsprechend ist die Umsetzungsfrist für Portugal auch hinsichtlich dieser Datenkategorien am 15. September 2007 abgelaufen.

Frage 3:

Welche Umsetzungspläne verfolgen jene Mitgliedstaaten, die die Richtlinie bislang noch nicht umgesetzt haben, in zeitlicher bzw. inhaltlicher Hinsicht?

Zurzeit arbeitet Portugal noch an der Umsetzung der europäischen Richtlinie zur Vorratsdatenspeicherung. Am 4. Januar 2008 wurde der Gesetzesentwurf Nr. 161/X, der darauf ab-

[197] Summary Report der Europäischen Union über die Umsetzung der Richtlinie 2006/24/EG vom 30. November 2006 Seite 10. Brüssel, DG JLS D1/NK/em D (2007) 18102. Abrufbar unter: http://ec.europa.eu/justice_home/news/events/data_retention/meeting_report_30_11_07.pdf

[198] Vergleiche Fußnote: 1.

zielt, die Richtlinie in portugiesisches Recht umzusetzen, vom Parlament genehmigt.[199] Die in Art. 4 des portugiesischen Gesetzentwurfs genannten Maßnahmen sind identisch mit denjenigen Maßnahmen, die die Richtlinie in Art. 5 bezüglich der auf Vorrat zu speichernden Daten anordnet. Der portugiesische Gesetzentwurf nennt keine weiteren, neuen Datenkategorien. Er geht also insofern nicht über den von der Richtlinie gesetzten Rahmen hinaus. Die Speicherfrist der auf Vorrat gespeicherten Daten beträgt ein Jahr, beginnend ab dem Zeitpunkt des konkreten Kommunikationsvorgangs.[200] Diese Frist hält sich in den von Art. 6 der Richtlinie bestimmten Grenzen.

Die Pflicht zur Vorratsdatenspeicherung schließt die in Art. 4 des portugiesischen Gesetzentwurfs genannten Daten im Zusammenhang mit „erfolglosen Anrufversuchen" ein, welche von den Anbietern öffentlich zugänglicher elektronischer Kommunikationsdienste oder den Betreibern eines öffentlichen Kommunikationsnetzes erzeugt oder verarbeitet und gespeichert werden.[201]

Die Behörden, die Zugriff auf die Vorratsdaten erhalten können, sind die Justizbehörden („autoridades judiciárias") und die Kriminalpolizeibehörden („autoridades de polícia criminal") der:

- „Polícia Judiciá" (wohl eine Art Ermittlungsdienst der Staatsanwaltschaft),
- „Guarda Nacional Republicana" (Nationale Republikanische Garde),
- "Polícia de Suguranca Pública" (etwa die Bundespolizei)
- „Polícia Judiciária Militar" (etwa die Militärpolizei)
- „ Servico de Estrangeiros e Fronteiras" (Dienst für Ausländer und Staatsgrenzen),
- „Polícia Marítima" (wohl vergleichbar mit der Küstenwache),
- „Inspecção-Geral do Ambiente e do Ordenamento do Território (IGAOT)" (etwa das Bundesumweltamt und die Bauplanungsämter) und diejenigen staatlichen Stellen, die in den autonomen Gebieten für Umweltstraftaten zuständig sind, soweit diese Straftaten als schwere Straftaten im Sinne dieses Gesetzes einzustufen sind,
- "Os órgãos da administração tributária" (etwa die Finanzämter/ die Finanzverwaltungen),
- "Agencies of the Social Security Administration" (etwa die Sozialämter).[202]

Vorraussetzung für den Zugang zu diesen sensiblen Daten ist immer eine richterliche Anordnung und er kann ausschließlich dem Staatsanwalt sowie bestimmten Abteilungen der Kri-

[199] Nachrichten Artikel vom 6. Januar 2008, abrufbar unter: http://www.jornalistas.online.pt/noticia.asp?id=6269&idselect=87&idCanal=87&p=0
[200] Art. 6 des portugiesischen Gesetzesentwurfs.
[201] Art. 5 des portugiesischen Gesetzesentwurfs.
[202] Art. 1 f) des portugiesischen Gesetzesentwurfs.

minalpolizei gestattet werden. Die Übermittlung von Daten an die berechtigten Behörden wird nur gestattet, wenn dies für die Ermittlung, Feststellung oder Verfolgung schwerer Straftaten notwendig ist.[203] Die "schweren Straftaten", die dazu ermächtigen, Konversations- oder Kommunikationsdaten (keine Inhaltsdaten!) abzufangen, aufzunehmen und zu überwachen, werden von der portugiesischen Strafprozessordnung bestimmt.[204] Laut Art. 187 der portugiesischen Strafprozessordnung – welcher einen vollständigen Katalog dieser Delikte enthält – fallen hierunter z.B. Straftaten mit einen Mindeststrafe von drei Jahren Haft, Drogenhandel, Delikte gegen das Waffenrecht, Terrorismus, organisierte Kriminalität, Schmuggel, Körperverletzung, Bedrohung, Geiselnahme und Nötigung. Aufgrund der besonderen Vertraulichkeit der Vorratsdaten ist die "Comissão Nacional de Protecção de Dados (CNDP)" (portugiesische Datenschutzkommission) verpflichtet, die elektronische Datenbank, die die Personen ausweist, die Zugang zu den auf Vorrat gespeicherten Daten haben sollen, permanent zu aktualisieren.[205]

Frage 4:

Wie wirkt sich die im Juli 2006 von Irland eingebrachte Klage vor dem Europäischen Gerichtshof auf die Umsetzungsbestrebungen dieser Staaten aus?

Nach den uns vorliegenden Materialien kann ein Einfluss der Klage Irlands gegen die Europäische Kommission und das Europäische Parlament vor dem EuGH die Umsetzungsbestrebungen bezüglich der Richtlinie 2006/24/EG auf den Gesetzgebungsprozess in Portugal weder bejaht noch verneint werden.

Frage 5:

Welche Reaktionen seitens der Zivilgesellschaft lassen sich in den ausgewählten Mitgliedstaaten erkennen?

In Portugal gibt es einige politische und soziale Reaktionen auf den portugiesischen Gesetzentwurf. Diese Reaktionen spiegeln sich einerseits in einem Brief wider, den die Portugiesische Kommunistische Partei an das Parlament geschickt hat. In diesem Brief führt die Partei als Gegenargumente zu dem Gesetzentwurf insbesondere an, dass die Speicherung der Daten nicht sicher sei und dass zu viele staatliche Institutionen Zugang zu den auf Vorrat gespeicherten Daten erlangen können.[206] Auch die Vereinigung portugiesischer Journalisten hat in einem Brief an das portugiesische Parlament ihre starke Ablehnung gegenüber dem Gesetzentwurf bekundet. Der Brief der portugiesischen Journalistenvereinigung wurde am

[203] Art. 9 Abs. 1 & 2 des portugiesischen Gesetzesentwurfs.
[204] Art. 1 g) des portugiesischen Gesetzesentwurfs.
[205] Art. 8 des portugiesischen Gesetzesentwurfs.

22. November 2007 verschickt und enthält eine Reihe von Argumenten gegen den Gesetzentwurf. Insbesondere stützt sich die Argumentation der Journalisten auf eine Verletzung der Pressefreiheit, da die meisten der Kommunikationsmittel, die Journalisten für ihre täglichen Nachforschungen benötigen, durch den Gesetzentwurf tangiert werden.[207]

[206] Vollständige Version des Briefs, abrufbar unter: http://www.pcp.pt/index.php?option=com_content&task=view&id=31137&Itemid=120.
[207] Lesenswert bezüglich der Reaktion der Vereinigung Portugiesischer Journalisten: http://www.jornalistas.online.pt/noticia.asp?id=6269&idselect=87&idCanal=87&p=0.

Spanien

Zusammenfassung: Spanien hat die Richtlinie bereits umgesetzt. Es dürfen keine Daten gespeichert werden, die den Inhalt der Kommunikation offenbaren. Zugriff auf die Vorratsdaten haben Polizei- und Sicherheitsbehörden. In Spanien gibt es einen lebhaften Protest gegen die Richtlinie und ihre Umsetzung.

Frage 1:

Welche Regelungen wurden von denjenigen ausgewählten Mitgliedstaaten getroffen, die die Richtlinie bereits umgesetzt haben?

In Spanien wurde die Richtlinie zur Vorratsdatenspeicherung kürzlich in nationales Recht umgesetzt. Im Mai 2007 hat die "Comisión de Justicia" (Justiz-Kommission) des spanischen Parlaments ein entsprechendes Gesetz verabschiedet. Es handelt sich dabei um das *Gesetz zur Vorratsspeicherung von Daten im Rahmen elektronischer Kommunikation und öffentlich zugänglicher elektronischer Kommunikationsnetzwerke*,[208] welches am 21. Juni 2007 von der „Cámara de Diputados del Congreso Espanol" (Abgeordnetenkammer des spanischen Parlaments) genehmigt und anschließend dem Senat zur Bewilligung übermittelt wurde. Von dort aus wurde das Gesetz zurück an die „Cámara de Diputados" gesendet.[209] Am 9. November 2007 trat das Gesetz[210] in Kraft.

Das erste Kapitel des Gesetzes legt die Art der Daten fest, die notwendigerweise auf Vorrat gespeichert werden müssen, um einerseits den Ursprungs- und Bestimmungsort einer Nachricht ermitteln und andererseits sowohl den Teilnehmer als auch den registrierten Benutzer identifizieren zu können. Ferner werden das Datum, die Uhrzeit und die Dauer einer Nachrichtenübermittlung, die Art des Kommunikationsdienstes und die Daten, die zur Bestimmung der Endeinrichtung der Nutzer benötigt werden, als unentbehrliche Speicherdaten angeführt. Keinesfalls dürfen jedoch Daten auf Vorrat gespeichert werden, die es ermöglichen, den Inhalt einer Kommunikation zu offenbaren.[211]

Das Gesetz führt eine detaillierte Liste derjenigen Daten an, die bezüglich der Telekommunikation mittels Telefonfestnetz, Mobilfunk oder Internet verpflichtend auf Vorrat gespeichert werden müssen.[212] Die in Art. 3 des spanischen Gesetzes angeführten, auf Vorrat zu spei-

---

[208] Spanischer Gesetzesentwurf zur Vorratsdatenspeicherung vom 11. Juli 2007, ausschließlich abrufbar unter: http://www.congreso.es/public_oficiales/L8/CONG/BOCG/A/A_128-09.PDF .

[209] http://www.edri.org/edrigram/number5.14/data-retention-spain .

[210] *Das spanische Gesetz*, "LEY 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones", abrufbar unter: http://www.derecho.com/legislacion/boe/3676766 .

[211] Bericht der Kommission des spanischen Parlaments zum Gesetzesentwurf zur Vorratsdatenspeicherung, Seite 62. http://www.congreso.es/public_oficiales/L8/CONG/BOCG/A/A_128-09.PDF .

[212] Art. 3 des spanischen Gesetzes.

chernden Daten sind im Grundsatz identisch mit denjenigen Daten, die in Art. 5 der Richtlinie genannt sind. Allerdings wird in Art. 3 des Gesetzes vereinzelt stärker differenziert und ins Detail gegangen, so wird in der Datenkategorie zur Bestimmung von Datum, Uhrzeit und Dauer einer Nachrichtenübermittlung betreffend Telefonfestnetz und Mobilfunk (vgl. Art. 5 Abs. 1 c) Nr. 1 VRS-RL) nicht abstrakt auf einen „Kommunikationsvorgang" abgestellt, sondern konkret auf „Anrufe, Kurznachrichtendienste (SMS) oder Multimediadienste (MMS)".

Ferner werden in der Datenkategorie zur Bestimmung der Art einer Nachrichtenübermittlung im Bereich des Telefonfestnetzes und des Mobilfunks (vgl. Art. 5 Abs. 1 d) Nr. 1 VRS-RL) die in Anspruch genommenen Telefondienste aufgeführt und gegeneinander abgegrenzt. Unterschieden werden demnach „Anrufe" (einschließlich Sprachtelefonie, Sprachspeicherdienst, Konferenzschaltungen, Datenabrufungen), „Zusatzdienste" (einschließlich Rufweiterleitung und Rufumleitung) oder Mitteilungsdienste und Multimediadienste (einschließlich Kurznachrichtendienste (SMS), erweiterte Nachrichtendienste (EMS) und Multimediadienste (MMS)).[213] Diese Spezifizierung findet sich in der Richtlinie jedoch nahezu wortgleich in den Begriffsbestimmungen (vgl. Art. 2 Abs. 2 c)).

Gemäß Art. 5 Abs. 1 des Gesetzes beträgt die Speicherfrist in Spanien grundsätzlich zwölf Monate ab dem Zeitpunkt des Kommunikationsvorgangs. Abhängig von der Kategorie der auf Vorrat zu speichernden Daten und nach Konsultierung des Kommunikationsnetzbetreibers bzw. des Kommunikationsdienstanbieters kann die generelle Speicherpflicht von zwölf Monaten auf minimal sechs Monate verkürzt oder auf maximal 24 Monate verlängert werden.[214] Es lassen sich der Vorschrift allerdings keine konkreteren Hinweise bezüglich der Umstände bzw. Vorraussetzungen entnehmen, aufgrund derer eine Verkürzung oder Verlängerung der Speicherungsfrist erfolgen kann. Die etwaige Verlängerung der Speicherungsfrist ist sehr umstritten gewesen und seitens einiger Organisationen wurde bemängelt, dass die Entscheidung über eine Verlängerung der Frist nicht im Ermessen der Exekutiven liegen dürfe.[215]

Gemäß Art. 4 Abs. 2 des spanischen Gesetzes umfasst die Verpflichtung zur Vorratsdatenspeicherung auch Daten in Zusammenhang mit erfolglosen Anrufversuchen. Kapitel 2 des Gesetzes bestimmt, welche Behörden unter welchen Umständen Zugriff auf die Daten haben können.[216] Die berechtigten Behörden sind demzufolge:

---

[213] Art. 3 d) Nr. 1 des spanischen Gesetzes.
[214] Art. 5 Abs. 1 des spanischen Gesetzes.
[215] Weitere Informationen im Bericht von Alexander Benalal bei Bird & Bird Law Firm, abrufbar unter: http://www.twobirds.com/english/publications/articles/Spain_proposed_implementation_Data_Retention_Directive.cfm .
[216] Art. 6 Abs. 2 a), b) and c) des spanischen Gesetzes.

- Die Mitglieder der „Fuerza y Cuerpo de Seguridad" (spanische Sicherheitsbehörden), soweit sie die in Art. 547 des spanischen Gesetzes 6/1985 vom 1. Juli 1985 bestimmten Funktionen erfüllen.
- Die offiziellen Angestellten der "Dirección Adjunta de Vigilancia Aduanera" (spanische leitende Zollbehörden), soweit sie die in Art. 283 Abs. 1 der spanischen Strafprozessordnung bestimmten Funktionen erfüllen, und
- Mitarbeiter des "Centro Nacional de Inteligencia" (spanischer Geheimdienst) in Zusammenhang mit ihren Untersuchungen natürlicher oder juristischer Personen, soweit diese im Einklang mit den Bestimmungen des spanischen Gesetzes 11/2002 vom 6. Mai 2002[217] und des spanischen Gesetzes 2/2002 vom 6. Mai 2002 stehen.

Gemäß Art. 7 des Gesetzes, können die Daten ausschließlich durch richterlichen Beschluss zugänglich gemacht werden. Dieser Beschluss muss ferner die konkrete Art der Daten angeben, die den ermächtigten, zuständigen Behörden übermittelt werden dürfen. Die Frist zur Umsetzung der richterlichen Anordnung wird von den Gerichten jeweils abhängig vom gegenständlichen Einzelfall bestimmt. Soweit keine genaue Frist bestimmt worden ist, gilt eine 72-Stunden-Frist, die um 8:00 Uhr des auf den Empfang der Anordnung folgenden Werktages zu laufen beginnt.

Im letzten Kapitel des Gesetzes finden sich einige Bestimmungen bezüglich Prepaid-Telefonkarten. Der Umgang mit Prepaid-Telefonkarten soll zukünftig nicht mehr anonymisiert ablaufen. Vielmehr sind die Kommunikationsnetzbetreiber bzw. die Kommunikationsdienstanbieter verpflichtet, die Daten der Prepaid-Kunden zu erfassen.[218] Im Rahmen dieses Identifizierungsverfahrens muss der Kunde beim Kauf einer Prepaid-Telefonkarte nunmehr einen gültigen Ausweis vorlegen, zudem müssen der Vor- und Nachnamen sowie die Staatangehörigkeit angeben werden. Diese Daten werden anschließend in einer Datenbank registriert. Im Falle juristischer Personen, erfolgt die Identifizierung über eine Art Steuerausweis „tarjeta de identificación fiscal", der zusammen mit dem Namen der juristischen Person „denominación social" und deren Steuernummer „código de identificación fiscal" registriert wird.[219] In Fällen, in denen die Prepaid-Karte vor Inkrafttreten des Gesetzes gekauft worden ist, besteht für die Kommunikationsnetzbetreiber bzw. die Kommunikationsdienstanbieter die Verpflichtung, die Daten der Karteneigentümer innerhalb eines Zeitraums von zwei Jahren nachträglich zu erfassen. Falls dies nicht möglich sein sollte, müssen die Karten vom Netz getrennt und unbrauchbar gemacht werden. Die Nutzer haben jedoch einen Anspruch auf Geldentschädi-

[217] Das Gesetz 11/2002 dient der Regulierung des spanischen Geheimdienstes.
[218] Anhang des spanischen Gesetzes, Nr. 1.
[219] Anhang des spanischen Gesetzes, Nr. 1.

gung für das auf den Karten zum Zeitpunkt der Außerbetriebnahme verbliebene Guthaben.[220]

Wie in vielen anderen Ländern wurde auch in Spanien keine Kostentragungsregeln in das Gesetz aufgenommen.[221] Dies wurde damit begründet, dass die Gewinnmarge in diesem Sektor ausreichend hoch sei, um die zusätzlich entstehenden Kosten aufzufangen.[222]

Frage 2:
Was sind die Gründe, aus denen die übrigen ausgewählten Mitgliedstaaten noch nicht umgesetzt haben?

Nicht einschlägig für Spanien.

Frage 3:
Welche Umsetzungspläne verfolgen jene Mitgliedstaaten, die die Richtlinie bislang noch nicht umgesetzt haben, in zeitlicher bzw. inhaltlicher Hinsicht?

Nicht einschlägig für Spanien.

Frage 4:
Wie wirkt sich die im Juli 2006 von Irland eingebrachte Klage vor dem Europäischen Gerichtshof auf die Umsetzungsbestrebungen dieser Staaten aus?

Es konnten keine Hinweise gefunden werden, ob die Klage Irlands gegen die Europäische Kommission und das Europäische Parlament vor dem EuGH die Umsetzung der Richtlinie 2006/24/EG in spanisches Recht beeinflusst hat oder während des Gesetzgebungsverfahrens von Bedeutung war.

Frage 5:
Welche Reaktionen seitens der Zivilgesellschaft lassen sich in den ausgewählten Mitgliedstaaten erkennen?

[220] Anhang des spanischen Gesetzes, Nr. 8.
[221] Summary Report der Europäischen Union über die Umsetzung der Richtlinie 2006/24/EG vom 30. November 2006 Seite 8. Brüssel, DG JLS D1/NK/em D (2007) 18102. “Replying to a question from Mme Cecilia VERKLEIJ (DG JLS) as to which Member States did not have or plan to have any reimbursement scheme in place now or in the future, the following confirmed they do not envisage reimbursement systems: Cyprus, Czech Republic, Greece, Hungary, Ireland, Latvia, Lithuania, Poland, Slovakia, Slovenia and **Spain**”.
[222] Summary Report der Europäischen Union über die Umsetzung der Richtlinie 2006/24/EG vom 30. November 2006 Seite 7.

In Spanien kam es früh zur Entstehung erster Protestbewegungen gegen die Richtlinie zur Vorratsdatenspeicherung. Organisationen wie beispielsweise EDRI[223] und XS4ALL[224] protestieren stark gegen die Richtlinie und haben eine internationale Kampagne unter dem Motto „Vorratsdatenspeicherung ist keine Lösung“[225] ins Leben gerufen, in welcher die spanische Abteilung der „Computerexperten für soziale Verantwortung“ (CPRS-ES)[226] mitwirkte.

[223] European Digital Rights (EDRI) http://www.edri.org/ .
[224] http://www.xs4all.nl/en/ .
[225] http://www.dataretentionisnosolution.com/ .
[226] Die CPRS-ES hat eine Informationsbroschüre entworfen, um die Zivilbevölkerung über die Bedeutsamkeit des Kampfes gegen die Richtlinie zu informieren und zu sensibilisieren. Spanische Version abrufbar unter: http://wiki.dataretentionisnosolution.com/index.php/Texto_cpsr_es .

Schweden

Zusammenfassung: Schweden gehört zu jenen Staaten der Europäischen Union, welche sich schon länger für die europaweite Vorratsdatenspeicherung einsetzen. So wurde etwa der Entwurf des Rahmenbeschlusses des Jahres 2004[227] neben Frankreich, Irland und dem vereinigte Königreich auch von Schweden ausgearbeitet.

Dennoch ist Schweden mit der innerstaatlichen Umsetzung der Richtlinie säumig. Einer der Hauptgründe liegt im Bemühen die Vorratsdatenspeicherung nicht etappenweise umzusetzen, sondern auch die Vorgaben der Richtlinie hinsichtlich der internetbezogenen Daten mit umzusetzen. Der derzeit in Schweden vorliegende Umsetzungsentwurf soll grundsätzlich mit 1. Jänner 2009 in Kraft treten, wobei derzeit – soweit den Quellen entnehmbar – noch nicht absehbar ist, wann es zu einer parlamentarischen Behandlung und möglichen Beschlussfassung kommen wird.

Auch in Schweden wird Kritik an der geplanten Umsetzung geübt. So gibt es Stimmen, welche die Diskussion in Schweden mit jener in Deutschland vergleichen, wobei ein koordiniertes Vorgehen wie es etwa im Beschreiten des Rechtswegs in Form der Beschwerdeerhebung vor dem deutschen Bundesverfassungsgericht durch mehr als 30.000 Bundesbürger zum Ausdruck kommt, in Schweden zumindest noch nicht erkennbar ist. Ein rechtliches Vorgehen gegen die (noch nicht vorliegende) innerstaatliche Umsetzung wäre – im Vergleich etwa zu Deutschland oder Österreich – aber auch insofern erschwert, als es in Schweden kein nationales Verfassungsgericht gibt, vor dem Betroffene eine Verletzung ihrer Grundrechte rügen können.

Schließlich ist festzuhalten, dass auch von offizieller Seite, wie von der für Datenschutz zuständigen Behörde aber auch von Standesvertretungen (etwa jene der Rechtsanwälte) Kritik an dem vorliegenden Umsetzungsentwurf wie auch an dem Regelungsgehalt der Richtlinie an sich geübt wird.

Frage 1:
Welche Regelungen wurden von denjenigen ausgewählten Mitgliedstaaten getroffen, die die Richtlinie bereits umgesetzt haben?

Da Schweden die Richtlinie noch nicht umgesetzt hat, ist diese Frage nicht einschlägig.

[227] *„Entwurf eines Rahmenbeschlusses über die Vorratsspeicherung von Daten, die in Verbindungen mit der Bereitstellung öffentlicher elektronischer Kommunikationsdienste verarbeitet und aufbewahrt werden, oder von Daten, die in öffentlichen Kommunikationsnetzen vorhanden sind, für die Zwecke der Vorbeugung, Untersuchung, Feststellung und Verfolgung von Straftaten, einschließlich Terrorismus.“,* Ratsdokument, Nr. 8958/04.

Frage 2:

Was sind die Gründe, aus denen die übrigen ausgewählten Mitgliedstaaten noch nicht umgesetzt haben?

Ein wesentlicher Grund für die nicht fristgerechte Umsetzung liegt im Wunsch der schwedischen Regierung nach einer „Gesamtlösung", also einer Umsetzung unter Einbeziehung der internetbezogenen Daten. Ein weiterer Grund dürfte auch in der aus Sicht der Betreiber/Anbieter von Telekommunikations- und Internetdiensten ungeklärten Kostenfrage liegen. So äußerten Telekommunikations- und Internetbetreiber bereits im Jahr 2006 die Sorge, dass die Vorratsdatenspeicherung mit enormen Kosten verbunden sein würde, welche die Betreiber nicht übernehmen könnten[228]. Auch wurde befürchtet, dass eine unterschiedliche Lösung der Kostenfrage in verschiedenen EU-Staaten zu einer Wettbewerbsverzehrung führen könnte[229].

Frage 3:

Welche Umsetzungspläne verfolgen jene Mitgliedstaaten, die die Richtlinie bislang noch nicht umgesetzt haben, in zeitlicher bzw. inhaltlicher Hinsicht?

Im Bemühen, den Regelungsgehalt der Richtlinie innerstaatlich umzusetzen, beauftragte die schwedische Regierung am 18.05.2006 das Justizministerium, eine Kommission bestehend aus Juristen[230] und weiteren Experten aus verschiedene Bereichen[231], einen Umsetzungsentwurf *„unter Berücksichtigung der Integrität der Staatsbürger, welche in ein angemessenes Verhältnis zu den Notwendigkeiten der Bekämpfung der schweren Kriminalität zu setzen ist"*[232], auszuarbeiten. Mit der Leitung dieser Kommission wurde *Gudrun Antemar* betraut, die Generaldirektorin der für die Bekämpfung der Wirtschaftkriminalität zuständigen Behörde (*Ekobrottsmyndigheten*). Der Umsetzungsentwurf hätte auftragsgemäß bis zum 1. April 2007 ausgearbeitet werden sollen, sodass die Einhaltung der Umsetzungsfrist möglich gewesen

---

[228] In diesem Sine äußerte sich etwa der für Behördenkontakte zuständige Leiter bei Telia Sonera, Gunnar Forsgren: *„Självklart kan vi inte svälja de här kostnaderna själva, telekom- och bredbandspriserna är så pressade att det inte finns några marginaler. Om vi inte kan få ersättning från statsbudgeten så måste vi föra över kostnaderna på slutkunderna, säger Gunnar Forsgren, chef för myndighetskontakter på Telia Sonera.";* http://www.nyteknik.se/nyheter/it_telekom/allmant/article38966.ece.

[229] So etwa Ylva Hambreus Björling, Direktorin des IT-företagen, in dem unter der Adresse http://www.nyteknik.se/nyheter/it_telekom/allmant/article38966.ece *erschienen Artikel: „Det kan bli förödande för konkurrensen om vissa av länderna exempelvis lastar över alla kostnader på bolagen, säger också Ylva Hambreus Björling."*

[230] Jeweils ein Vertreter der Regulierungsbehörde für den Telekommunikationsbereich, des Justizministeriums, der für Fragen des Datenschutzes zuständigen Behörde (*Datainspektion*) und des Oberverwaltungsgerichtes; siehe den unter dem Titel *Lagring av trafikuppgifter för brottsbekämpning* erschienen Bericht, S 3 unter der Überschrift *Till statsrådet och chefen för Justitiedepartementet;* http://www.regeringen.se/sb/d/8586/a/91521.

[231] So insbesondere aus den Bereichen der Polizeibehörden, des Justizministeriums, der Staatsanwaltschaft, des Verteidigungsministeriums, des Wirtschaftsministeriums, der IT - Unternehmen, des Dachverbandes der schwedischen Rechtsanwälte; Quelle: siehe Fn. 4.

[232] Siehe den unter der Überschrift *Lagring av trafikuppgifter för brottsbekämpning* erschienen Bericht, S 44, Pkt. 1.2. *„(...)som tillgodoser både behovet av bekämpning av allvarlig brottslighet och skyddet för medbor-garnas integritet.";* http://www.regeringen.se/sb/d/8586/a/91521.

wäre. Bereits am Beginn ihrer Arbeit regte die Kommission an, auch die Umsetzung hinsichtlich der internetbezogenen Datenkategorien mit einzubeziehen, da eine getrennte Behandlung und Umsetzung nach Ansicht der Kommission nicht sinnvoll wäre[233]. Die schwedische Regierung verlängerte daraufhin die Frist zur Erstattung des Umsetzungsentwurfes bis zum 1. November 2007.

Die Kommission erarbeitete einen entsprechenden Entwurf unter Einbindung von Arbeitsgruppen, welche aus Vertretern der verschiedener Telekommunikations- und Internetbetreiber sowie der politischen Parteien zusammengesetzt waren und veröffentlichte diesen im November des Jahres 2007[234]. Derzeit wird der ausgearbeitete Entwurf vom *Schwedischen Gesetzesrat* (*Lagrådet)* geprüft. Aufgabe dieses Gremiums ist die Prüfung von Legislativvorschlägen auf deren Verfassungskonformität sowie deren Einklang mit der schwedischen Rechtsordnung[235].

Dem Entwurf zu Folge sollen die Vorgaben der Richtlinie durch Änderungen des Gesetzes für elektronische Kommunikation[236] und des Geheimhaltungs- bzw. Verschwiegenheitsgesetzes[237], sowie teils in Verordnungsform umgesetzt werden. Im Gesetzesrang sollen insbesondere die Speicherdauer, die Verschwiegenheitspflicht, die Betroffenenrechte sowie die Ermächtigung zum Datenzugriff beschlossen werden. Vorgenannte Verordnung soll die zu speichernden Datenkategorien sowie Ausnahmen von der Vorratsspeicherungspflicht festlegen. Weder der Gesetzes- noch der Verordnungsentwurf enthalten Vorgaben zur Datensicherheit. Diesbezüglich findet sich im Verordnungsentwurf eine Ermächtigung der für den Telekommunikationsbereich zuständigen Regulierungsbehörde, welche unter Einbindung der Polizei- und der Datenschutzbehörde entsprechende Vorgaben zu erlassen hat[238].

Der Entwurf sieht die Speicherung aller in Art. 5 der Richtlinie vorgegebenen Datenkategorien (also auch der internetbezogenen) für eine einheitliche Dauer von einem Jahr vor[239]. Über die Vorgaben der Richtlinie hinausgehend sollen dem Entwurf zu Folge

---

[233] Siehe den in Fn. 6 genannten Bericht, S 44, Pkt. 1.1.: *„Vi drog emellertid tidigt den slutsatsen att det inte var meningsfullt att först föreslå regler om lagring av trafikuppgifter som enbart rörde fast och mobil telefoni för att senare återkomma med förslag rörande övriga delar. I stället behövde förslagen presenteras i ett sammanhang.“*

[234] Siehe den in Fn 6 genannten Bericht.

[235] Siehe: http://www.regeringen.se/sb/d/8586/a/91521.

[236] *Lagen (2003:389) om elektronisk kommunikation.*

[237] *Sekretesslagen (1980:100).*

[238] Siehe hierzu § 1 des Verordnungsentwurfes auf S 41 in den in Fn 6 genannten Berichts:
11 § Post- och telestyrelsen får efter samråd med Rikspolisstyrel-sen och Datainspektionen meddela verkställighetsföreskrifter om säkerhet enligt 6 kap. 3 § andra stycket lagen (2003:389) om elek-tronisk kommunikation.

[239] Siehe § 6b des entsprechenden Gesetzentwurfes, welcher auf S 37 des in Fn 6 genannten Bericht aufgenommen wurde:*„6 b § Lagring enligt 6 a § ska pågå under ett år från det datum kommunikationen ägde rum. Vid lagringstidens slut ska uppgifterna utplånas, om de inte har begärts utlämnade men ännu inte läm-nats ut eller den lagringsskyldige annars har rätt att fortsätta be-handla dem.“*

- hinsichtlich der Mobiltelefonie nicht nur die Standortdaten zu Beginn des Gespräches, sondern auch jene am Gesprächsende[240] sowie

- auch die Kommunikationsdaten erfolgloser Anrufversuche[241] (Art. 3 Abs. 2 der Richtlinie)

erfasst werden.

Zugang zu den gespeicherten Daten sollen alle zur Verbrechensbekämpfung berufenen Behörden und Gerichte haben, wobei die Zugriffrechte von der jeweils herangezogenen Rechtsgrundlage abhängen:

- Die auf Vorrat gespeicherten Daten können, wenn und soweit bereits eine bestimmte Person einer konkreten Straftat verdächtig wird (einschließlich der Vorbereitung und des Versuchs derselben), welche mit nicht weniger als sechsmonatiger Freiheitsstrafe bedroht ist, hinsichtlich dieser Person sowie weiterer Personen, die mit der verdächtigen Person in Verbindung stehen, abgefragt werden. Hierzu ist ein entsprechender gerichtlicher Beschluss erforderlich. Die Daten müssen für den konkreten Zweck der Ermittlung wesentlich sein[242]. Dieses Zugriffsrecht soll im Gerichtsgesetz (*Rättegånsbalken)* geregelt werden.
- Ohne Beschluss eines Gerichtes können auf Vorrat gespeicherte Daten abgefragt werden wegen[243]

---

[240] Siehe § 5 des Verordnungsentwurfes auf S 40 des in Fn 6 genannten Berichts:
„5 § Vid mobil telefoni ska utöver det som anges i 4 § uppgifter om följande lagras: (...)
– lokaliseringsinformation för kommunikationens början och slut, samt (...).“

[241] Siehe § 10 des Verordnungsentwurfes auf S 41 des in Fn 6 genannten Berichts:
„10 § Lagringsskyldigheten för uppgifter enligt 4-6 §§ gäller även vid misslyckad uppringning.“

[242] Siehe S 27 siehe des in Fn 6 genannten Berichtes:
„Förutsättningarna för att få ut trafikuppgifter enligt bestämmel-serna *om hemlig teleövervakning i rättegångsbalken är följande.*
1. Det ska finnas en skäligen misstänkt person.
2. Misstanken ska röra
a) brott för vilket inte är föreskrivet lindrigare straff än fängelse i sex månader (även anstiftan och medhjälp),
b) dataintrång, barnpornografibrott som inte är ringa, narkoti-kabrott eller narkotikasmuggling, eller
c) försök, förberedelse eller stämpling till brott under a) och b).
3. Åtgärden ska vara av synnerlig vikt för utredningen.
4. Åtgärden får avse uppgifter om telemeddelanden som befordras eller har befordrats till eller från teleadresser med viss anknytning till den misstänkte.
5. Åtgärden ska beslutas av domstol.“

[243] siehe S 28 siehe des in Fn 6 genannten Berichtes:
„Förutsättningarna för att få ut trafikuppgifter enligt lagen om elektronisk kommunikation är följande (i jämförelse med rätte-gångsbalken).
1. Det behöver inte finnas en skäligen misstänkt person.
2. Det ska vara fråga om brott för vilket inte är föreskrivet lindriga-re

- mit zumindest zweijähriger Freiheitsstrafe bedrohten Delikten,

- beschränkt auf einen konkreten Kommunikationsvorgang

Dieses Zugriffsrecht soll im Gesetz über die elektronische Kommunikation (*Lagen om elektronisk kommunikation*) geregelt werden.

- An erleichterte Voraussetzungen ist die Abfrage von (insbesondere Stamm-)Daten geknüpft, wenn diese ohne Bezug auf einen konkreten Telekommunikationsvorgang erfolgen soll. Diese Abfragemöglichkeit setzt grundsätzlich Ermittlungen im Bezug auf ein mit Freiheitsstrafe bedrohtes Delikt voraus, in Ausnahmefällen genügt es aber, dass das Delikt mit Geldstrafe bedroht ist[244]. Dieses Zugriffsrecht soll im Gesetz über die elektronische Kommunikation (*Lagen om elektronisk kommunikation*) geregelt werden.

Die vorgenannten Zugriffrechte entsprechen der bereits geltenden Rechtslage in Schweden. Seitens der Kommission wird kein Bedarf gesehen, diese Bestimmungen aus Anlass der Richtlinienumsetzung zu ändern.

Wie oben bereits angesprochen wird im Verordnungsentwurf auch von Ausnahmen von der Vorratsdatenspeicherungspflicht gesprochen. In Anlehnung an Dänemark, wo dem Bericht der Kommission zu Folge, Vereine, welchen lediglich unter 100 „Einheiten" („*enheter")* angehören, von der Speicherungspflicht ausgenommen seinen, enthält der schwedische Entwurf eine Ermächtigung der Aufsichtsbehörde, bestimmte Betreiber bzw. Anbieter von der generellen Speicherungspflicht auszunehmen[245]. Bei der Entscheidung hierüber sollen die den Betreibern bzw. Anbietern entstehenden Kosten gegen den Nutzen für Strafverfolgungszwecke abgewogen werden[246].

---

straff än två års fängelse (även anstiftan och medhjälp).

3. Åtgärden behöver inte vara av synnerlig vikt för utredningen.
4. Åtgärden är inte begränsad till vissa teleadresser men uppgiften ska angå ett särskilt elektroniskt meddelande.
5. Åtgärden beslutas av den brottsbekämpande myndigheten."

[244] siehe S 169 siehe des in Fn 6 genannten Berichtes:
„När de brottsbekämpande myndigheterna behöver uppgifter om abonnemang, t.ex. namn, adress, telefonnummer och IP-nummer, krävs inte samma svårhetsgrad rörande brottet. I sådana fall är det enligt lagen om elektronisk kommunikation tillräckligt att det för brottet är föreskrivet fängelse och att det i det enskilda fallet kann bli fråga om annan påföljd än böter."

[245] Siehe S 169 des in Fn 6 genannten Berichtes: „I t.ex. det danska förslaget har en generell gräns för skyldigheten att lagra satts till 100 "enheter", dock enbart för vissa typer av före-ningar (andelsforeninger, ejerforeninger, antenneforeninger og lig-nende foreninger eller sammenslutninger heraf). Enligt vår bedöm-ning är det inte lämpligt att koppla skyldigheten att lagra trafik-uppgifter till antalet enheter/kunder eller till en viss minsta om-sättning. (...) Det får i första hand vara en fråga för tillsynsmyndigheten att närmare avgöra vilka leverantörer som ska undantas från skyldighe-ten att lagra trafikuppgifter."

Der Bericht der Kommission beziffert die durch die Umsetzung der Richtlinie entstehenden Kosten mit Rund 200 Mio. Kronen (entspricht etwa 21,5 Mio Euro). Diese den Betreibern/ Anbietern durch die Anschaffung und den Betrieb der entsprechenden Anlagen erwachsenden Kosten sollen nicht ersetzt werden. Geplant ist lediglich im Falle einer erfolgten Abfrage die diesbezüglich konkret entstandenen Kosten zu ersetzen[247]. Dass die übrigen Kosten von den Betreibern/ Anbieter zu tragen sein sollen, stieß auf heftige Kritik seitens der Unternehmen. So sagte etwa Marcus Nylen, Direktor eines der größten schwedischen Internetbetreiber, Bredbansbolaget, dass die entstehenden Kosten enorm seien und die Kunden wohl nicht bereit wären, für die Speicherung der eigenen Daten zu zahlen[248].

Soweit dem Bericht entnehmbar, dürfen die auf Vorrat gespeicherten Daten nicht für unternehmenseigene Zwecke (Marketing, etc.) verwendet werden.

Anzumerken ist schließlich, dass die für Fragen des Datenschutzes zuständige Behörde, die *Datainspektion,* welche auch in der Kommission vertreten war, die den in Rede stehenden Bericht ausgearbeitet hatte, sich in einer gesonderten Stellungnahme[249] dem Ergebnis gegenüber kritisch eingestellt zeigt:

Seitens der *Datainspektion* wird kritisiert, dass

- Daten auch ohne Gerichtsbeschluss ausgefolgt werden könne sowie dass

- ein Teil der Umsetzung nicht in Gesetzes- , sondern in Verordnungsform erfolgen soll.

Darüber hinaus hält die *Datainspektion* in ihrer Stellungnahme fest, dass das Vorhaben „Vorratsdatenspeicherung“ an sich auch aus grundrechtlichen Erwägungen, insbesondere wegen des Eingriffs in die Privatsphäre der Betroffenen als bedenklich einzustufen ist.

Frage 4:

Wie wirkt sich die im Juli 2006 von Irland eingebrachte Klage vor dem Europäischen Gerichtshof auf die Umsetzungsbestrebungen dieser Staaten aus?

---

[246] Siehe S 169 des in Fn 6 genannten Berichtes.
[247] Siehe S 30 des in Fn 6 genannten Berichtes.
[248] Marcus Nylen, Direktor eines der größten schwedischen Internetbetreiber, *Bredbansbolaget*, in einem in der Computerzeitung *Computer Sweden* erschienen Artikel, in welchem er ausführt: *„Självklart kommer vi inte att snåla, men det är en enorm kostnad och jag tror inte att man som kund är beredd att betala mer för att ens uppgifter ska lagras, säger Marcus Nylén.“; http://www.idg.se/2.1085/1.129928.*
[249] http://datainspektionen.webhotel.qd.se/presstjanst/nyheter/rattslig-provning-bor-kravas-for-att-lamna-ut-trafikdatauppgifter (zuletzt abgerufen am 10.03.2008).

Die eingebrachte Klage hat – soweit erkennbar – keinen nennenswerten Einfluss auf die Umsetzung der Richtlinie in Schweden.

Frage 5:

Welche Reaktionen seitens der Zivilgesellschaft lassen sich in den ausgewählten Mitgliedstaaten erkennen?

In zahlreichen Internetforen findet sich – teils massive – Kritik gegenüber der geplanten Umsetzung der Vorratsdatenspeicherung wie auch der diesem Umsetzungsvorhaben zu Grunde liegenden Richtlinie als solcher. Auch gibt es Stimmen, welche die Diskussion in Schweden mit jener in Deutschland vergleichen, wobei – wie oben ausgeführt - ein koordiniertes Vorgehen, wie etwa das Beschreiten des Rechtsweg in Form der Beschwerdeerhebung vor dem deutschen Bundesverfassungsgericht durch mehr als 30.000 Bundesbürger, in Schweden zumindest noch nicht erkennbar ist.[250] Ein solches Vorgehen gegen die (noch nicht vorliegende) innerstaatliche Umsetzung wäre im Vergleich etwa zu Deutschland oder Österreich aber – wie eingangs bereits festgehalten – auch insofern erschwert, als es in Schweden kein nationales Verfassungsgericht gibt, vor dem Betroffene eine Verletzung ihrer Grundrechte rügen könnten.

Ausgesprochen kritisch äußerte sich auch der Dachverband der schwedischen Rechtsanwälte, wobei die Vorratsdatenspeicherung als *gefährliche Bedrohung* gesehen und darauf hingewiesen wurde, dass die BürgerInnen das *„Vertrauen in die Behörden und Gerichtswesen“* verlieren könnten. Darüber hinaus bedrohe die Vorratsdatenspeicherung ganz grundsätzlich die Vertraulichkeit der anwaltlichen Kommunikation[251].

Wie schon oben in Beantwortung der Frage 3 ausgeführt, wurde schließlich auch Kritik seitens der *Datainspektion* geübt. Da diese aber als Behörde nicht der Zivilgesellschaft als solcher zuzurechnen ist, wird hier von einer ausführlicheren Darstellung der Kritik Abstand genommen.

---

[250] So ist etwa unter der Adresse http://www.der-elch.se/2007/03/22/der-aufwiegler zu lesen: *„Der Arbeitskreis Vorratsdatenspeicherung bewacht diese Fragen — zumindest für Deutschland und nach meinem Ermessen — mit Bravour. Hier in Schweden verlaufen die Diskussionen in ähnlichen Bahnen wie in Deutschland.“.*

[251] Siehe den in der Zeitschrift *Computer Sweden* unter der Überschrift *EU-lag mångmiljonsmäll för operatörerna* erschienen Artikel sowie das dort veröffentlichte, mit Anne Ramberg, Generalssekretärin des schwedischen Anwaltsdachverbandens, geführte Interview; http://www.idg.se/2.1085/1.125298

Tschechien

Zusammenfassung: Tschechien ist einer von derzeit neun EU-Mitgliedstaaten, die die Richtlinie (jedenfalls zum Teil) bereits umgesetzt haben. Derzeit wird über eine Novelle zum Gesetz über die elektronische Kommunikation beraten, die eine vollständige Umsetzung der Richtlinie bewirken soll.

Frage 1:

Welche Regelungen wurden von denjenigen ausgewählten Mitgliedstaaten getroffen, die die Richtlinie bereits umgesetzt haben?

Tschechien ist einer von derzeit neun EU-Mitgliedstaaten, die die Richtlinie bereits umgesetzt haben.[252] Die Umsetzung erfolgte bisher allerdings lediglich zum Teil, d. h. abgesehen von Art 3 Abs 2, Art 7 und Art 10. Eine vollständige Umsetzung der Richtlinie in nationales Recht ist mit einer entsprechenden Novelle zum Gesetz über die elektronische Kommunikation[253] geplant. Derzeit geht die Anzahl der zu speichernden Datenkategorien über die Vorgaben der Richtlinie hinaus, wobei die besagte Novelle diesbezüglich Einschränkungen vorsieht. Beispielsweise verlangt das Gesetz auch die Speicherung von Informationen im Bezug auf die Verwendung von prepaid-Karten. Auch Daten die IMEI und MSISDN verbinden müssen gespeichert werden. Was die Dauer der Speicherung anbelangt, so beläuft diese sich derzeit im Allgemeinen auf sechs Monate, wobei im Hinblick auf besondere Kategorien von Daten (etwa sog. „Uniform Resource Identifier“ - URI) lediglich eine Speicherdauer von drei Monaten vorgesehen ist. Bei letzteren handelt es sich um Daten, die auch Rückschlüsse auf den Inhalt einer Kommunikation zulassen. Mit der angesprochenen Novelle soll die Dauer auf sechs bzw. zwölf Monate ausgedehnt werden. Momentan werden Daten von Anrufen, *„bei denen keine Verbindung zustande kommt“* nicht gespeichert, nach Inkrafttreten der Novelle wird sich dies allerdings ändern bzw. werden auch solche Daten zu speichern sein.

Zugriff auf bzw. Zugang zu den jeweils auf Vorrat gespeicherten Daten haben die Polizeibehörden der Tschechischen Republik, und zwar im Hinblick auf die Ausforschung und Aufklärung sämtlicher Deliktsarten. Die konkrete Vorgehensweise der Polizei bzw. deren im Hinblick auf die Datenverwendung bestehenden Befugnisse sind per Verordnung festgelegt.[254]

---

[252] Vgl. Vorratsdatenspeicherung: Umsetzung erst in 9 von 27 EU-Staaten, in: MMR 2008, Heft 2, XXIII, online unter http://rsw.beck.de/rsw/shop/default.asp?sessionid=275FE178F9964453A067ED9F17155542&docid=252821&docClass=NEWS&site=MMR&from=mmr.10 (zuletzt abgerufen am 10.03.2008).

[253] Gesetz Nr. 127/2006 vom 22. Februar 2005.

[254] Vlg. Verordnung Nr. 485/2005 Coll., Vylhláška ze dne 7. prosince 2005 o rozsahu provozních a lokalizačních údajů, době jejich uchovávání a formě a způsobu jejich předávání orgánům oprávněným k jejich využívání, online unter http://www.mvcr.cz/sbirka/2005/sb169-05.pdf (zuletzt abgerufen am 10.03.2008).

Die durch die Speicherung entstehenden Kosten werden den Betreibern seitens des Innenministeriums ersetzt, wobei hierbei lediglich auf die tatsächlich angefallenen Kosten abgestellt wird.

Wie oben bereits kurz erwähnt, sind nach derzeitiger Rechtslage auch jene Daten zu erfassen, die nicht *„im Zuge der Bereitstellung der betreffenden Kommunikationsdienste (...) erzeugt oder verarbeitet werden“ (*Art 3 Abs 1 der Richtlinie), etwa im Hinblick auf die Verwendung von prepaid-Karten. Daten, *„die Aufschluss über den Inhalt einer Kommunikation geben“* (vgl Art 5 Abs 2 der Richtlinie) werden nicht gespeichert. Ausnahmen bestehen diesbezüglich lediglich für jene Fälle, in denen das Gericht eine Aufzeichnung von Inhaltsdaten anordnet.

Den Betreibern steht es frei, die erfassten Daten für unternehmenseigene Zwecke, konkret zu Verrechnungszwecken, zu nutzen. Zu Marketingzwecken können Daten nach wie vor nur auf Basis datenschutzrechtlicher Bestimmungen verwendet werden, zB dann, wenn die betreffende Person dem zustimmt.

Im Hinblick auf Betroffenenrechte ist anzumerken, dass betroffene Personen prinzipiell schon aufgrund von strafrechtlichen Regelungen über etwaige gegen sie bestehende Verdachtsmomente und diesbezügliche Aufklärungsschritte informiert werden müssen. Über eine allfällige Weitergabe von Daten an Dritte erfolgt allerdings keine entsprechende Information. Die Kontrollbefugnisse im Zusammenhang mit der Verwendung von personenbezogenen Daten liegen ganz allgemein in der Kompetenz des tschechischen Büros für den Schutz Personenbezogener Daten (www.uoou.cz), das seine Aufgaben hauptsächlich auf Basis des Gesetzes Nr. 101/2000 vom 4. April 2000 über den Schutz Personenbezogener Daten wahrnimmt. Es wurden an sich keine speziellen Datensicherheitsmaßnahmen vorgesehen. Zwar wurde das Format definiert, in dem die Protokolldateien zur Verfügung gestellt werden müssen (plain text Format), generell kommen aber die allgemeinen datenschutzrechtlichen Bestimmungen im Bezug auf die Verwendung personenbezogener Daten zur Anwendung.

Frage 2:
Was sind die Gründe, aus denen die übrigen ausgewählten Mitgliedstaaten noch nicht umgesetzt haben?

Für Tschechien nicht einschlägig.

Frage 3:

Welche Umsetzungspläne verfolgen jene Mitgliedstaaten, die die Richtlinie bislang noch nicht umgesetzt haben, in zeitlicher bzw. inhaltlicher Hinsicht?

Für Tschechien nicht einschlägig.

Frage 4:

Wie wirkt sich die im Juli 2006 von Irland eingebrachte Klage vor dem Europäischen Gerichtshof auf die Umsetzungsbestrebungen dieser Staaten aus?

Die Klage, die Irland gegen den Rat und das Europäische Parlament vor dem Europäischen Gerichtshof mit dem Ziel eingebracht hat, die Richtlinie mangels adäquater Primärrechtsgrundlage für nichtig zu erklären, hat in der politischen Diskussion in Tschechien praktisch keine Erwähnung gefunden.

Frage 5:

Welche Reaktionen seitens der Zivilgesellschaft lassen sich in den ausgewählten Mitgliedstaaten erkennen?

Im Jahr 2005 wurde die internationale Kampagne „*Data retention is no solution*" ins Leben gerufen, an der Iuridicum Remedium (IuRe, www.iure.org) und deren UnterstützerInnen von tschechischer Seite aktiv partizipieren. IuRe ist nach wie vor aktiver Gegner der Vorratsdatenspeicherung und hofft diesbezüglich dem Irischen Beispiel folgen zu können. Überdies hat IuRe erst kürzlich eine Stellungnahme zur geplanten Novelle des tschechischen Gesetzes über elektronische Kommunikation abgegeben, in der empfohlen wurde, 1. die zu speichernden Datenkategorien auf jene zu limitieren, die in der Richtlinie angeführt sind, 2. den Zugang zu den gespeicherten Daten auf Polizeibehörden zu beschränken und 3. die Umsetzung der geplanten Maßnahmen auch im Hinblick auf die finanzielle Machbarkeit zu revidieren.

Abgesehen von IuRe konnten in den Medien hinsichtlich der Richtlinienumsetzung gelegentlich kritische Stimmen von Seiten technischer bzw. open source Gemeinschaften vernommen werden.[255]

[255] Vgl. etwa : Operátoři zřejmě dají policii novou zbraň − údaje o neuskutečněných hovorech, 27.02.2008, abrufbar unter: http://mobil.idnes.cz/operatori-zrejme-daji-policii-novou-zbran-udaje-o-neuskutecnenych-hovorech-17n-/mob_operatori.asp?c=A080227_124316_mob_operatori_hro (zuletzt aufgerufen am 10.03.2008).