



POSITIONSPAPIER

VON ALEXANDER ALVARO, MDEP

Berichterstatter des Europäischen Parlaments zu dem Entwurf eines Rahmenbeschlusses über die Vorratsspeicherung von Daten, die in Verbindung 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 8958/04)

I. Hintergrund

Im Rahmen der Ratstagung für Justiz und Inneres am 29./30. April 2004 haben Frankreich, Großbritannien, Irland und Schweden einen gemeinsamen Vorschlag¹ für einen Rahmenbeschluss zur Vorratsspeicherung von Kommunikationsdaten vorgelegt. Hintergrund der Initiative ist eine am 25. März 2004 vom Europäischen Rat verabschiedete Erklärung zum Kampf gegen den Terrorismus², in der der Rat beauftragt wurde, Maßnahmen für die Erarbeitung von Rechtsvorschriften über die Aufbewahrung von Verkehrsdaten durch Diensteanbieter zu prüfen.

Ziel des Vorschlages ist die Erleichterung der justiziellen Zusammenarbeit in Strafsachen, indem die Rechtsvorschriften der Mitgliedstaaten über die Vorratsspeicherung von Daten, die durch Diensteanbieter eines öffentlich zugänglichen elektronischen Kommunikationsdienstes verarbeitet und gespeichert werden, für die Zwecke der Vorbeugung, Untersuchung, Feststellung und Verfolgung von Straftaten, einschließlich Terrorismus, angeglichen werden.

Erfasst werden sollen Verkehrs- und Standortdaten einschließlich Teilnehmer- und Nutzerdaten, die im Rahmen der folgenden Kommunikationsvorgänge erzeugt werden³:

- Telefonie, ausgenommen SMS-Kurzmitteilungen, elektronische Mediendienste und Multimedia Datentransferdienste;
- SMS-Kurzmitteilungen, elektronische Mediendienste und Multimedia-Datentransferdienste, die als Teil eines Telefondienstes angeboten werden;
- Internet-Protokolle, einschließlich E-Mail, Protokolle für Sprachübermittlung über das Internet, World Wide Web, Dateiübertragungsprotokolle, Netzübertragungsprotokolle, Hypertextübertragungsprotokolle, Sprachübermittlung über Breitband und Subsets von Internet-Protokoll-Nummern, Daten zur Umsetzung der Netzadresse.

Im Sinne des Rahmenbeschlusses bezeichnet der Ausdruck Daten folgende Arten von Daten: Telefonnummern, Internetadressen, Rechnungsadressen des Kunden und die Telefonnummern/Kommunikationsvorgänge, die unter Nutzung eines bestimmten Telefons/ Computers angerufen werden bzw. stattgefunden haben.

Darüber hinaus werden vom Rahmenbeschluss auch Daten abgedeckt, die eine Ermittlung folgender Angaben ermöglichen: wohin ein Anruf vorgenommen oder eine Kommunikation hergestellt wurde, die Dauer eines Anrufs/ einer Verbindung und der Ort, an dem sich das Telefon befand, von dem der Anruf ausging bzw. das den Anruf empfangen hat.⁴

Die Inhalte der Kommunikation werden nicht erfasst.

Grundsätzlich ist im Rahmen des Vorschlages eine Speicherdauer von mindestens 12 und maximal 36 Monaten vorgesehen. Für die zweite und dritte Gruppe können die Mitgliedstaaten Abweichungen von der vorgesehenen Speicherfrist beschließen.

Die Mitgliedstaaten sollen im Rahmen von Rechtshilfeersuchen auf die in den anderen EU-Staaten vorhandenen Vorratsdaten zugreifen können.

Entschädigungsregeln für entstehende Kosten enthält der Vorschlag nicht.

II. Bewertung des Vorschlages

Ich bin der festen Überzeugung, dass die gemeinsame Bekämpfung der organisierten Kriminalität und des Terrorismus eine der wesentlichen Aufgaben und Herausforderungen der Europäischen Union ist. Ferner stelle ich fest, dass diesen Verbrechen, die unter Einsatz moderner elektronischer Kommunikationssysteme verabredet, vorbereitet und begangen werden, effiziente Möglichkeiten gegenüberstehen müssen, die die Durchführung oder Koordinierung von Ermittlungen zur Vorbeugung und Aufklärung erleichtern.

¹ Ratsdokument 8958/04 v. 28. April 2004

² Ratsdokument 7764/04 v. 28. März 2004

³ vgl. 8958/04 Art. 2 Abs. 3

⁴ 8958/04 ADD 1 vom 20. Dezember 2004

1. Rechtsgrundlage

Am Anfang der Überlegungen muss festgestellt werden, ob der Rahmenbeschluss tatsächlich aufgrund der angegebenen Rechtsgrundlage erlassen werden kann. Der Rat beruft sich vorliegend auf Artikel 31 Absatz 1 Buchstabe c und Artikel 34 Absatz 2 Buchstabe b des Vertrages über die Europäische Union. Somit handelt es sich nach Ansicht des Rates bei dem vorliegenden Rahmenbeschluss um eine Maßnahme, die der dritten Säule der Union zuzuordnen ist.

Ich teile diese Rechtsauffassung nicht und bin der Ansicht, dass der Vorschlag vielmehr aus Maßnahmen, die der ersten Säule der Union zuzuordnen sind (z.B. Fristen und zu speichernde Daten) und Maßnahmen, die der dritten Säule zuzuordnen sind (z.B. verstärkte justizielle Zusammenarbeit).

Zur Klärung dieser wesentlichen Frage hat der Ausschuss für bürgerliche Freiheiten, Justiz und Inneres gemäß Art. 35 Absatz 2 der Geschäftsordnung des Europäischen Parlaments den Rechtsausschuss um seine Stellungnahme gebeten.

Gegebenfalls sollte dem Rat der Vorschlag nahe gelegt werden, den vorliegenden Rahmenbeschluss den jeweiligen Säulen entsprechend aufzuteilen, so dass zwei Dokumente beraten werden können, deren Rechtsgrundlage unzweifelhaft ist.

2. Verhältnismäßigkeit der Maßnahme

Unabhängig von der Frage der Rechtsgrundlage muss die Suche nach geeigneten Lösungsmöglichkeiten unter Beachtung des Grundsatzes der Verhältnismäßigkeit stattfinden, der auch fundamentales Prinzip der Europäischen Union ist. Ich bezweifle nicht, dass ein legitimer Zweck (Vorbeugung und Verfolgung von Straftaten) sowie ein legitimes Mittel (Speicherung von Daten) dem Entwurf zugrunde liegen.

Darüber hinaus müssen die vorgesehenen Maßnahmen aber auch in einer angemessenen Zweck-Mittel-Relation stehen, die nur dann gegeben ist, wenn die Regelungen geeignet und erforderlich sind und keine unzumutbare Härte der Betroffenen darstellen.

Bei dem zu speichernden Datenvolumen, insbesondere im Bereich des Internets, ist fraglich, ob eine zielführende Auswertung der Daten überhaupt möglich ist.

Die Geeignetheit einer Vorratsdatenspeicherung muss im Vorfeld durch aussagekräftige Untersuchungen und Statistiken, die konkrete Informationen darüber enthalten, geprüft werden. In welchem Umfang Ermittlungen durch das Fehlen solcher Daten behindert werden, ist bisher nicht veröffentlicht worden. Insbesondere fehlen Angaben darüber, ob und in welchem Umfang die Zusammenarbeit der Mitgliedstaaten im Rahmen der Kriminalitätsbekämpfung tatsächlich beeinträchtigt wurde.

Teilnehmer aus dem Umfeld der organisierten Kriminalität und des Terrorismus werden aufgrund neuerer technischer Mittel, aber auch durch einfache praktische Möglichkeiten, die Verfolgbarkeit ihrer Daten leicht zu verhindern wissen. Möglichkeiten hierzu wären der Erwerb von Telefonkarten durch Strohmänner oder wechselnd eingesetzte Mobiltelefone von ausländischen Anbietern, die Nutzung öffentlicher Telefonzellen, die Veränderung der bei der Nutzung eines E-Mail-Service verwendeten IP-Adresse oder E-Mail-Adresse oder gleich die Nutzung von Internet Service Providern, die außerhalb Europas liegen und einer Verpflichtung bezüglich der Vorratsdatenspeicherung nicht unterliegen.

Sofern sämtliche von dem Beschluss umfassten Verkehrsdaten tatsächlich gespeichert werden müssten - einschließlich Internetdaten - würde im Netz eines großen Internet-Service-Providers bereits bei heutigem Verkehrsaufkommen eine Datenmenge von 20 - 40.000 Terabyte anfallen. Dies ist ein Datenvolumen, das ungefähr 4 Mio. km gefüllter Aktenordner entspricht - dies entspricht zehn Aktenbergen, die jeweils von der Erde bis zum Mond reichen würden.

Bei dieser gewaltigen Datenmenge würde ein einmaliger Suchlauf bei einem Einsatz der vorhandenen Technik ohne zusätzliche Investitionen 50-100 Jahre dauern.

Auch vor diesem Hintergrund sind daher Untersuchungen durchzuführen, in welchem Umfang Umgehungsmöglichkeiten für potentielle Straftäter bestehen, die Verfolgbarkeit von Daten leicht zu verhindern.

Gegenüber dem bestehenden Vorschlag der umfassenden Vorratsdatenspeicherung könnte das Mittel der anlassbezogenen Speicherung sowohl gleich geeignet als auch milder sein. Ein Vorteil der anlassbezogenen Datenspeicherung wäre, dass nicht gewaltige Datenmengen gespeichert und ausgewertet werden müssten, sondern die Daten bestimmter verdächtiger Personen mit deutlich geringerem Aufwand gespeichert und den Ermittlungsbehörden zur Verfügung gestellt werden können. Soweit zurzeit im Bereich der anlassbezogenen Datenspeicherung Defizite bestehen, könnte eine Optimierung dieses Ansatzes das Ziel einer effektiven Vorbeugung und Verfolgung von Straftaten sicherstellen. Dies ist im Übrigen auch das Modell, das von der Cybercrime-Convention des Europarats vorgegeben ist⁵.

Im Rahmen der Diskussion und damit auch in der Begründung eines Textvorschlages müssen Gründe dargelegt werden, warum die alternativen Lösungsansätze, wie z.B. die anlassbezogene Speicherung von Daten bestimmter Personen als nicht geeignet angesehen werden. So wird in dem erläuternden Dokument zum Rahmenbeschluss über die Vorratsdatenspeicherung lediglich festgestellt, dass die anlassbezogene Speicherung von Daten "keinen Beitrag zur Überprüfung von Personen leisten kann, die noch nicht verdächtigt werden, einer kriminellen oder terroristischen Organisation anzugehören [...] Sie kann daher nicht den Bedarf der Sicherheits-, Geheimdienst- und Strafverfolgungsstellen im Hinblick auf die Bekämpfung heutiger Straftäter, zu denen auch Terroristen gehören, decken"⁶. Mit Blick auf diese Formulierung des Rates drängt sich zudem die Frage auf, inwiefern diese Zielsetzung der vorgesehenen Vorratsdatenspeicherung mit dem - auch in der Europäischen Union grundlegenden - Prinzip der Unschuldsvermutung vereinbar ist. Der vorgeschlagene Beschluss wäre nicht nur auf einzelne Personen anwendbar, die auf Grund besonderer Gesetze überwacht würden, sondern auf alle Personen, die die elektronische Kommunikation nutzen.

In der Praxis hat sich herausgestellt, dass weniger der fehlende Umfang von Daten ein Problem bei der Vorbeugung und Verfolgung von Straftaten zu sein scheint, sondern der grenzüberschreitende Austausch der Daten sich als Hindernis erweist. In diesem Zusammenhang schlägt der Ich alternativ vor, die Harmonisierung des Speicherformats der vorgesehenen Daten anzustreben und Rechtsvorschriften für einen deutlich verbesserten grenzüberschreitenden Austausch der Daten zu erarbeiten.

Der vorliegende Vorschlag geht nicht auf die möglichen Belastungen der Betroffenen ein. Neben den tiefen Eingriffen in den Schutz der persönlichen Daten des Einzelnen, sind enorme Belastungen für die europäische Telekommunikationsindustrie sowie kleinere und mittlere Telekommunikationsunternehmen zu befürchten. Alleine bei größeren Festnetz- und Mobilfunkunternehmen im Bereich der klassischen leitungsvermittelnden Telefonie ist zu erwarten, dass pro Jahr um die fünfhundert Milliarden (500.000.000.000) zusätzlich zu speichernde Datensätze mit einem Datenvolumen von ca. 8 Terabyte (1 Terabyte = 1 Mio. Megabytes) entstehen.

Kosten erwachsen in diesem Zusammenhang vor allen Dingen aus:

- der Anpassung der Systemtechnik zur Generierung und Speicherung der Daten,
- der Anpassung der betrieblichen Abläufe zur sicheren Archivierung der Daten sowie
- der Bearbeitung und Auswertung von Anfragen der Sicherheitsbehörden.

Der hierfür erforderliche Investitionsaufwand im Bereich der klassischen leitungsvermittelten Telefonie liegt nach Schätzungen verschiedenster größerer Unternehmen innerhalb der Mitgliedstaaten bei 180 Mio. Euro im Jahr pro Unternehmen. Die jährlichen Betriebskosten könnten damit bis zu 50 Mio. Euro betragen. Für kleinere und mittlere Unternehmen wäre hierdurch der Geschäftsbetrieb sicher gefährdet.

Die bei Implementierung der für die geplante Vorratsdatenspeicherung erforderlichen Software entstehenden Kosten

- für den erforderlichen Speicherplatz
- für die Anpassung der Systemtechnik zur Generierung und Speicherung der im Internetbereich anfallenden Daten
- für eine Optimierung der Datenbanken sowie die Kosten zur Anpassung der betrieblichen Abläufe und
- zur sicheren Archivierung

⁵ ETS Nr. 185, 8. November 2001

⁶ Ratsdokument 8958/04 ADD 1

würden den Investitionsaufwand bei der klassischen leitungsvermittelten Telefonie nach Schätzungen um ein Vielfaches übersteigen.

Grundsätzlich kann davon ausgegangen werden, dass sich der Internetverkehr in Europa jährlich verdoppelt, was das zu speichernde Datenvolumen exponentiell ansteigen lassen würde.

So muss auch berücksichtigt werden, dass der Artikel 36 Ausschuss dieses Problem erkannt hat und hinsichtlich des zu speichernden Datenumfanges vorschlägt, weiterhin lediglich die ohnehin anfallenden Daten zu erfassen⁷. Dies würde den Anforderungen an die Bekämpfung der organisierten Kriminalität und des Terrorismus genügen, wie praktische Erfahrungen belegen.

Der Vorschlag des Rates mangelt an einer, bei vorgesehener europaweiter Harmonisierung der Vorratsdatenspeicherung, europaweit harmonisierten Regelung zur Verteilung der hierdurch entstehenden Kostenlast. Denn uneinheitliche und unzureichende Entschädigungsregime führen zu Wettbewerbsverzerrungen, gefährden langfristig tragfähige Wettbewerbsstrukturen und verhindern damit die Vollendung eines einheitlichen europäischen Binnenmarktes.

Bei der erforderlichen Abwägung, ob die grenzüberschreitende Kriminalitätsbekämpfung tatsächlich im Wege einer verbindlich vorgeschriebenen Vorratsdatenspeicherung verbessert werden kann und soll, muss vorrangig der Schutz der Grundrechte der EU-Bürger (Recht auf informationelle Selbstbestimmung und Vertraulichkeit der eigenen Daten; Grundsatz der Datensparsamkeit) gewährleistet sein.

III. Vereinbarkeit des Rahmenbeschlusses mit Artikel 8 der Europäischen Menschenrechtskonvention und Artikel 15 der Richtlinie 2002/58/EG

Der Entwurfstext geht zwar im Rahmen der Erwägungsgründe auf den Eingriff in die Privatsphäre des Einzelnen durch eine Vorratsdatenspeicherung ein. Es fehlt allerdings eine Auseinandersetzung mit Artikel 8 der Europäischen Menschenrechtskonvention (Recht auf Achtung des Privatlebens und der Korrespondenz), der den garantierten Schutz personenbezogener Daten festschreibt.

Die Datenschutzgruppe Art. 29 hat den Rahmenbeschluss auf seine Vereinbarkeit mit Artikel 8 der Europäischen Menschenrechtskonvention hin umfassend geprüft⁸. So weist sie unter anderem darauf hin, dass berücksichtigt werden muss, dass die Bürger für alltägliche Tätigkeiten zunehmend elektronische Kommunikationsnetze und -dienste nutzen. Die bei dieser Form der Kommunikation generierten Daten, die so genannten „Verkehrsdaten“, können Informationen über Ort, Zeitpunkt und Gesprächspartner von Mobil- oder Festnetztelefonatesprächen, Telefaxkommunikation, E-Mails, SMS und anderen Formen der Internetkommunikation enthalten und daher in zunehmendem Maße die Lebensführung der Nutzer widerspiegeln.

Auch Artikel 15 der Richtlinie 2002/58/EG sieht nicht vor, dass unter den aufgeführten Möglichkeiten eine europaweit verbindlich vorgeschriebene Vorratsdatenspeicherung in Erwägung gezogen werden kann. Die besagte Richtlinie sieht gerade vor, dass "die Mitgliedstaaten Rechtsvorschriften erlassen können", die die Aufbewahrung von Daten für einen begrenzten Zeitraum regeln⁹.

Der Europäische Gerichtshof für Menschenrechte hat zwar die Befugnis der Vertragsstaaten anerkannt, in Ausnahmefällen und unter besonderen Umständen die Korrespondenz und Telekommunikation von Personen auch heimlich zu überwachen. Er hat aber hinzugefügt:

„... dies bedeutet nicht, dass die Vertragsstaaten ein unbeschränktes Ermessen haben, Personen in ihrem Hoheitsgebiet einer heimlichen Überwachung zu unterwerfen. Angesichts der Tatsache, dass entsprechende Befugnisse mit der Begründung, die Demokratie verteidigen zu wollen, diese gerade zu unterminieren oder zu zerstören drohen, betont der Gerichtshof, dass die Vertragsstaaten zur Bekämpfung der Spionage oder des Terrorismus nicht jede Maßnahme beschließen dürfen, die sie für angemessen halten“.

In ihrer Empfehlung 2/99 vom 3. Mai 1999 zur Achtung der Privatsphäre bei der Überwachung des Fernmeldeverkehrs definierte die Datenschutzgruppe die Überwachung des Fernmeldeverkehrs als die Kenntnisnahme von Inhalt von und/ oder Daten im Zusammenhang mit privaten

⁷ 15098/04 vom 23. November 2004

⁸ Artikel 29 Datenschutzgruppe, 11885/04 vom 9. November 2004

⁹ vgl. Richtlinie 2002/58/EG, Art. 15 Abs. 1

Telekommunikationsverbindungen zwischen zwei oder mehreren Teilnehmern durch einen Dritten, insbesondere der mit der Telekommunikationsnutzung verbundenen Verkehrsdaten. In diesem Zusammenhang stellte die Datenschutzgruppe seinerzeit auch fest, dass jede Überwachung des Fernmeldeverkehrs (einschließlich der Überwachung und des Data Mining von Verkehrsdaten) eine Verletzung des Rechts von Einzelpersonen auf Privatsphäre und eine Verletzung des Brief- und Fernmeldegeheimnisses darstelle. Daraus folgt, dass Überwachungen abzulehnen sind, sofern sie nicht drei grundlegende Kriterien erfüllen, die sich aus der Auslegung von Artikel 8 Absatz 2 der Europäischen Menschenrechtskonvention durch den Europäischen Gerichtshof für Menschenrechte ergeben: Sie müssen gesetzlich vorgesehen und in einer demokratischen Gesellschaft notwendig sein und einem der in der Konvention aufgeführten legitimen Ziele dienen. Nach Auffassung der Datenschutzgruppe gelten dieselben grundlegenden Erfordernisse für die Speicherung von Verkehrsdaten, soweit sie über das für die Erbringung der Kommunikationsdienstleistungen und andere legitime Geschäftszwecke Notwendige hinausgehen, sowie für jeden anschließenden Zugriff auf diese Daten für Strafverfolgungszwecke. Wie vorliegend geprüft erscheint die Erfüllung aller notwendigen Kriterien im Rahmen des vorliegenden Ratsdokumentes zumindest fraglich.

Darüber hinaus liefert der vorliegende Rahmenbeschluss keine Antworten auf essentielle rechtsstaatliche Fragen, wie die Beweislast im Falle einer nicht zutreffenden Analyse der Daten durch staatliche Behörden, die Informationspflicht gegenüber dem Betroffenen Bürger im Falle einer unbegründeten Datenabfrage oder den Auskunftsanspruch des Bürgers bezüglich seiner gespeicherten Daten. Diese offenen Fragen bedürfen klarer Antworten.

Ferner ist es unter rechtsstaatlichen Gesichtspunkten als fraglich zu bewerten, ob im speziellen Fall des Artikel 2 Absatz 4 des Rahmenbeschlusses dem Grundsatz der Bestimmtheit der Norm Rechnung getragen worden ist.

IV. Tatsächlicher Bedarf der Vorratsdatenspeicherung

Die Vereinigten Staaten von Amerika, die infolge der Anschläge vom 11. September 2001 die Sicherheitsregeln in vielen Bereichen erheblich verschärft haben, scheinen eine anlassbezogene Datenspeicherung für ausreichend und angemessen zu halten. Mir ist zumindest nicht bekannt, dass es weiterreichende Forderungen z.B. an Internetserviceprovider (ISP) gibt, auf Vorrat Verbindungs- und Nutzungsdaten ihrer Kunden zu speichern.

Untersuchungen europäischer Telefongesellschaften haben gezeigt, dass das Gros der von Strafverfolgungsbehörden abgerufenen Daten nicht älter als sechs Monate war. Das belegt, dass längere Aufbewahrungsfristen eindeutig unverhältnismäßig sind¹⁰.

Vor der Diskussion eines konkreten Textvorschlages für einen Rahmenbeschluss muss daher eine von Wissenschaft, Wirtschaft und Justiz begleitete und auf konkrete Untersuchungen basierende Analyse durchgeführt werden.

V. Zusammenfassung

Hinsichtlich des vorliegenden Rahmenbeschlusses 8958/04 bezweifle ich, dass

- die gewählte Rechtsgrundlage den Umfang des Rahmenbeschlusses deckt,
- die Maßnahmen geeignet sind,
- die Maßnahmen erforderlich sind,
- das Prinzip der Unschuldsvermutung beachtet wurde,
- Richtlinie 2002/58/EG und Richtlinie 95/46/EC sowie die Europäische Menschenrechtskonvention hinreichend beachtet worden sind,
- Artikel 2 Absatz 4 dem Bestimmtheitsgebot entspricht sowie
- die finanziellen Auswirkungen des Rahmenbeschlusses in Erwägung gezogen worden sind.

Ich schlage in diesem Zusammenhang vor, dass

- der Rahmenbeschluss seinen Maßnahmen entsprechend in zwei Dokumente geteilt wird, die dann jeweils der entsprechenden Säule der Union zugeordnet werden können,
- anstelle der Einführung der Vorratsdatenspeicherung die Mängel im Rahmen der anlassbezogenen Datenspeicherung beseitigt werden und die grenzüberschreitende Zusammenarbeit verbessert wird,

¹⁰ vgl. 11885/04 vom 9. November 2004

- die Fristen der Datenspeicherung europaweit auf sechs Monate begrenzt werden,
- der Umfang der zu speichernden Daten nicht über das für Geschäftszwecke notwendige Maß hinausgeht,
- europaweit harmonisierte Entschädigungsregeln erarbeitet werden sowie
- eine Datenschutzrichtlinie für die dritte Säule der Union entwickelt wird.

Brüssel, 21. Januar 2005