ARTIKEL-29-Datenschutzgruppe

1868/05/DE
WP 113

Stellungnahme 4/2005 zum Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlicher elektronischer Kommunikationsdienste verarbeitet werden, und zur Änderung der Richtlinie 2002/58/EG (KOM(2005) 438 endg. vom 21.9.2005)

Angenommen am 21. Oktober 2005

Die Arbeitsgruppe wurde durch Artikel 29 Richtlinie 95/46/EG eingesetzt. Sie ist ein unabhängiges EU-Beratungsgremium in Datenschutzfragen. Ihre Aufgaben sind in Artikel 30 Richtlinie 95/46/EG sowie in Artikel 15 Richtlinie 2002/58/EG festgelegt.

Die Sekretariatsgeschäfte werden wahrgenommen von: Europäische Kommission, GD Justiz, Freiheit und Sicherheit, Direktion C (Ziviljustiz, Grundrechte und Unionsbürgerschaft), B-1049 Brüssel, Belgien, Büro LX-46 01/43.

Website: http://europa.eu.int/comm/justice_home/fsj/privacy/index_de.htm

ZUSAMMENFASSUNG

Der Vorschlag der Europäischen Kommission für eine Richtlinie über die Vorratsspeicherung von Daten stellt uns vor eine historische Entscheidung.

Die Aufbewahrung von Verkehrsdaten ist ein Eingriff in das unverletzliche Grundrecht auf Achtung des Brief-, Post- und Fernmeldegeheimnisses.

Eingriffe in dieses Grundrecht müssen einem zwingenden Bedarf entspringen, sie sollten nur in Ausnahmefällen gestattet werden und angemessenen Schutzmaßnahmen unterworfen sein.

Die Anbieter öffentlich zugänglicher Kommunikationsdienste wären erstmals gezwungen, Milliarden von Daten über die Kommunikationsvorgänge aller Bürger zu Ermittlungszwecken zu speichern.

Der Terrorismus stellt unsere Gesellschaft vor eine reale und drängende Herausforderung. Die Regierungen müssen auf diese Herausforderung in einer Form reagieren, die dem Bedürfnis der Bürger, in Frieden und Sicherheit zu leben, wirkungsvoll nachkommt, ohne die Menschenrechte des Einzelnen, darunter das Recht auf Privatsphäre und Datenschutz, auszuhöhlen, denn diese Rechte gehören zu den Eckpfeilern unserer demokratischen Gesellschaft.

Die Initiative der Europäischen Kommission könnte im Endergebnis zur Festlegung von maximalen Aufbewahrungsfristen führen, die kürzer sind als diejenigen, die in anderen Vorschlägen der letzten Zeit vorgesehen sind.

Nach Auffassung der Datenschutzgruppe ist es fraglich, ob sich die von den zuständigen Behörden in den Mitgliedstaaten vorgebrachten Rechtfertigungsgründe für eine obligatorische und allgemeine Vorratsdatenspeicherung auf kristallklare Beweise stützen. Die Datenschutzgruppe hegt auch Zweifel, ob die im Richtlinienentwurf vorgeschlagenen Aufbewahrungsfristen überzeugen können.

Wie oben erwähnt muss klar aufgezeigt und nachgewiesen werden, dass eine obligatorische und allgemeine Vorratsdatenspeicherung gerechtfertigt ist. Gleiches gilt für die maximal zulässige Aufbewahrungsdauer. In jedem Fall müssen auch die Bedingungen, unter denen den zuständigen Behörden zur Bekämpfung der terroristischen Bedrohung der Zugriff auf die Daten und deren Nutzung zu gestatten ist, eindeutig benannt werden.

Die Zwecke, zu denen die Daten gespeichert werden, müssen in der Richtlinie klar umrissen werden; dabei sollte auf die Bekämpfung des Terrorismus und der organisierten Kriminalität Bezug genommen werden statt auf nicht näher bestimmte „schwere Straftaten".

Der Existenz von Vorgehensweisen, die weniger in die Privatsphäre eingreifen (z. B. „quick freeze"-Verfahren) ist Rechnung zu tragen.

Der Zeitraum, über den die Daten gespeichert werden müssen, sollte so kurz wie möglich sein und die für alle Mitgliedstaaten geltende Höchstgrenze darstellen; dabei sollte es den Mitgliedstaaten freistehen, kürzere Aufbewahrungsfristen festzulegen. Die möglicherweise eingeführten Maßnahmen müssen umfassend bekannt gemacht werden.

Die Beweise, auf die sich diese Maßnahmen stützen, müssen regelmäßig bewertet werden. Die beabsichtigten Maßnahmen zur Vorratsdatenspeicherung sollten einer zeitlichen Befristung auf Grundlage einer periodischen Bewertung unterliegen, die mindestens alle 2-3 Jahre durchzuführen und zu veröffentlichen wäre (Konzept der „sunset legislation"). Die Datenschutzgruppe hält eine Dreijahresfrist für angemessen.

In jedem Fall ist es im bestehenden europäischen Rechtsrahmen inakzeptabel, den Kommunikationsdiensteanbietern die betreffenden Aufbewahrungspflichten aufzuerlegen, ohne vorab angemessene und spezifische Schutzvorkehrungen zu treffen.

Zum Abschluss schlägt die Datenschutzgruppe zwanzig spezifische Schutzvorkehrungen vor, unter besonderer Berücksichtigung der Anforderungen an Empfänger und Weiterverarbeitung, der Notwendigkeit von Autorisierungen und Kontrollen, der von Diensteanbietern zu ergreifenden Maßnahmen im Hinblick auf die Sicherheit und die logische Trennung der Daten, der Festlegung der betroffenen Datenkategorien und ihrer Aktualisierung und der Notwendigkeit, Inhaltsdaten von der Speicherung auszunehmen.

eingesetzt durch die Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995,

gestützt auf Artikel 29 sowie Artikel 30 Absatz 1 Buchstabe a und Absatz 3 dieser Richtlinie sowie auf Artikel 15 Absatz 3 der Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002,

gestützt auf ihre Geschäftsordnung, insbesondere auf Artikel 12 und 14,

hat folgende Stellungnahme angenommen:

I. Hintergrund

Im Rahmen der europäischen Initiativen zur Bekämpfung des Terrorismus und der organisierten Kriminalität unterbreitete die Europäische Kommission am 21. September dieses Jahres einen *„Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlicher elektronischer Kommunikationsdienste verarbeitet werden, und zur Änderung der Richtlinie 2002/58/EG“*[1].

Der Gegenstand dieses Vorschlags ist für alle Bürger von erheblicher Bedeutung.

Die Freiheit und die Vertraulichkeit des Briefverkehrs und sonstiger Kommunikationsformen gehören zu den Säulen einer modernen demokratischen Gesellschaft. Ihre Unverletzlichkeit ist in verschiedenen Rechtsinstrumenten, z. T. mit Verfassungsrang, verankert und steht unter dem besonderen Schutz der Europäischen Menschenrechtskonvention, die eine der Grundlagen des Gemeinschaftsrechts bildet.

Der Richtlinienentwurf stellt uns vor eine historische Entscheidung. Mit der vorgeschlagenen Richtlinie soll erstmals europaweit die Pflicht eingeführt werden, Milliarden von Daten über die Kommunikationsvorgänge aller Bürger zu Ermittlungszwecken zu speichern. Nach geltendem Gemeinschaftsrecht werden derartige Daten von den Anbietern elektronischer Kommunikationsdienste entweder gar nicht gespeichert oder nur für einen begrenzten Zeitraum und ausschließlich zu Vertragszwecken.

Die Vorratsspeicherung von Verkehrsdaten ist ein Eingriff in das Grundrecht auf Achtung des Brief-, Post- und Fernmeldegeheimnisses, das dem Einzelnen durch Artikel 8 der Europäischen Menschenrechtskonvention garantiert wird. In einer demokratischen Gesellschaft können Eingriffe in dieses Grundrecht gerechtfertigt sein, wenn sie für die nationale Sicherheit notwendig sind. Sie können letzten Endes dazu führen, dass sämtliche Kontakte und Beziehungen von Personen verfolgt und aufgezeichnet werden, einschließlich der Orte, an denen sie stattfinden, und der verwendeten Kommunikationsmittel. Der Europäische Gerichtshof für Menschenrechte hat betont, dass bei heimlicher Überwachung die Gefahr

[1] KOM (2005) 438 endg. vom 21.9.2005 (noch nicht im Amtsblatt veröffentlicht).

besteht, dass die Demokratie mit der Begründung, sie verteidigen zu wollen, unterminiert oder zerstört wird. Er hat darüber hinaus bekräftigt, dass die Vertragsstaaten zur Bekämpfung der Spionage oder des Terrorismus nicht jede Maßnahme beschließen dürfen, die sie für angemessen halten. [2]

Aus diesem Grund müssen Eingriffe in dieses Grundrecht einem zwingenden Bedarf entspringen und sollten nur in Ausnahmefällen gestattet werden und angemessenen Schutzmaßnahmen unterworfen sein. Die Vorratsspeicherung von Verkehrsdaten (einschließlich Standortdaten) zu Strafverfolgungszwecken muss strengen Auflagen genügen[3]; sie darf insbesondere nur während eines begrenzten Zeitraums erfolgen und nur dann, wenn dies in einer demokratischen Gesellschaft notwendig, angemessen und verhältnismäßig ist.

Die Befugnisse der Strafverfolgungsbehörden müssen zwar eine wirksame Bekämpfung des Terrorismus ermöglich, aber sie dürfen weder unbegrenzt sein noch missbraucht werden. Es ist auf Verhältnismäßigkeit und Ausgewogenheit zu achten, um sicherzustellen, dass wir die Gesellschaft, die wir schützen wollen, nicht untergraben. Dies gilt insbesondere dann, wenn Kommunikationsdiensteanbieter zur Speicherung von Daten gezwungen werden, die sie selbst nicht benötigen, denn damit wäre letzten Endes eine beispiellose, fortgesetzte und alles durchdringende Überwachung jeder Art von Kommunikation und Bewegung sämtlicher Bürger im Alltag möglich. Es würde eine riesige Menge an Informationen gespeichert, die tatsächlich nur in einer begrenzten Zahl von Fällen für Ermittlungszwecke von Nutzen sind.

Zu berücksichtigen ist ferner, dass von einer derart umfassenden Speicherpflicht auch Kommunikationsvorgänge betroffen sind, die heikle Fragen in Bezug auf das Berufs- und/oder Untersuchungsgeheimnis oder bestimmte Tätigkeiten unter besonderem rechtlichem Schutz stehender Institutionen aufwerfen.

Aus diesem Grund vertreten sowohl die Datenschutzgruppe als auch die Konferenz der Europäischen Datenschutzbeauftragten seit Jahren einen festen und klaren Standpunkt. Die Datenschutzgruppe[4] und die Europäische Konferenz[5] haben seit 1997 wiederholt die Notwendigkeit einer allgemeinen Vorratsspeicherung von Daten in Frage gestellt.

---

[2] Klass und andere gegen Deutschland, Absatz 49.

[3] Siehe insbesondere Artikel 15 Absatz 1 der Richtlinie 2002/58/EG.

[4] Siehe
- **Stellungnahme 9/2004** zum Entwurf eines Rahmenbeschlusses […] (Ratsdokument 8958/04 vom 28.4.2004). Der Anhang dieser Stellungnahme enthält eine Zusammenfassung der folgenden Dokumente:
- **Stellungnahme 1/2003** zur Speicherung von Verkehrsdaten zu Zwecken der Gebührenabrechnung;
- **Stellungnahme 5/2002** zur Erklärung der europäischen Datenschutzbeauftragten auf der Internationalen Konferenz in Cardiff (9.-11. September 2002) zur obligatorischen systematischen Aufbewahrung von Verkehrsdaten im Bereich der Telekommunikation;
- **Stellungnahme 10/2001** zur Notwendigkeit eines ausgewogenen Vorgehens im Kampf gegen den Terrorismus;
- **Stellungnahme 4/2001** zum Entwurf einer Konvention des Europarates über Cyberkriminalität;
- **Stellungnahme 7/2000** zum Vorschlag der Europäischen Kommission für eine Richtlinie des Europäischen Parlaments und des Rates über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation vom 12. Juli 2000, KOM(2000) 385;
- **Empfehlung 3/99** zur Aufbewahrung von Verkehrsdaten durch Internet-Dienstanbieter für Strafverfolgungszwecke;
- **Empfehlung 2/99** zur Achtung der Privatsphäre bei der Überwachung des Fernmeldeverkehrs;
- **Empfehlung 3/97** über Anonymität im Internet.
(Sämtliche genannten Dokumente sind abrufbar unter *http://europa.eu.int/comm/internal_market/privacy*.)

[5] Siehe die in Stockholm (April 2000) und Cardiff (April 2002) angenommenen Erklärungen.

II. VORLÄUFIGE BEWERTUNG UND ALLGEMEINE VORAUSSETZUNGEN

1. Gespeicherte Daten können für Ermittler von Nutzen sein, aber die oben genannten Voraussetzungen müssen deutlich aufgezeigt und belegt sein.

Erstens muss das Ziel einer derartigen Maßnahme unmissverständlich zum Ausdruck gebracht werden. Zweitens muss klar aufgezeigt und nachgewiesen werden, dass eine obligatorische und allgemeine Vorratsdatenspeicherung gerechtfertigt ist. Gleiches gilt für die maximal zulässige Aufbewahrungsdauer. Drittens müssen die Bedingungen, unter denen den zuständigen Behörden zur Bekämpfung der terroristischen Bedrohung der Zugriff auf die Daten und deren Nutzung zu gestatten ist, eindeutig benannt werden.

Die Beweise müssen zumindest regelmäßig bewertet und die Bewertungsergebnisse veröffentlicht werden; dabei ist zu berücksichtigen, dass der Terrorismus und das organisierte Verbrechen auf die Einführung von Maßnahmen zur generellen Überwachung der Bürger mit Strategien zur Vermeidung bestimmter Kommunikationsmittel reagieren könnten. Dies hätte zur Folge, dass neue Methoden einer noch strengeren Überwachung entwickelt werden müssten und somit eine Spirale möglicher Eingriffe in die Grundrechte der Bürger in Gang gesetzt würde, die nur schwer aufzuhalten wäre. Darüber hinaus würde eine solche Entwicklung das Wesen der Gesellschaft verändern, die wir zu bewahren trachten.

Die Datenschutzgruppe erkennt an, dass sich einige Bedingungen in unseren Gesellschaften hinsichtlich der mit der terroristischen Bedrohung verbundenen Risiken verändert haben, und nimmt zur Kenntnis, dass manche Daten gelegentlich für bestimmte Ermittlungen nützlich sind und zu Recht verwendet werden. Des Weiteren stellt die Datenschutzgruppe fest, dass die Initiative der Europäischen Kommission im Endergebnis zur Festlegung von maximalen Aufbewahrungsfristen führen könnte, die kürzer sind als diejenigen, die in der Vergangenheit vorgesehen waren und zu denen sich die Datenschutzgruppe ablehnend geäußert hat – zuletzt in ihrer am 9. November 2004 angenommenen Stellungnahme 9/2004 (WP 99).

Gleichwohl hat es nicht den Anschein, dass sich die Begründungen für die Datenspeicherung, obwohl sie sich angeblich an den Anforderungen seitens der zuständigen Behörden in den Mitgliedstaaten orientieren, auf kristallklare Beweise stützen können. Demzufolge erscheinen die vorgeschlagenen Fristen bislang nicht überzeugend.

Es gibt andere nützliche Maßnahmen, die für Ermittlungszwecke in Betracht gezogen werden können und die in geringerem Maße in die Grundrechte der Bürger eingreifen, beispielsweise das „quick freeze"-Verfahren, das weder die Kommunikationsanbieter noch die Internet-Diensteanbieter zur generellen Speicherung von Verkehrsdaten verpflichten würde. Bei diesem Verfahren wenden sich die Strafverfolgungsbehörden in begründeten Fällen an die Unternehmen und verlangen die Speicherung bestimmter Daten. Anschließend haben die Behörden mehrere Wochen Zeit zum Sammeln von Beweismitteln, um eine richterliche Anordnung zu erwirken. Gestützt auf diese Anordnung erhalten sie dann Zugriff auf die Daten.

In jedem Fall muss eine allgemeine Aufbewahrungsfrist klar geregelt werden. Sie sollte möglichst kurz sein und weitest gehend mit der Aufbewahrungsfrist übereinstimmen, die für die ursprünglichen Zwecke gilt, zu denen die Daten von den Kommunikationsdiensteanbietern aufgezeichnet werden.

2. Die von der Kommission derzeit vorgeschlagene Harmonisierung der Rechtsvorschriften in den Mitgliedstaaten muss klarstellen, dass die Festlegung einer verbindlichen Speicherfrist auf europäischer Ebene auf Grundlage einer auf europäischer Ebene durchgeführten Bewertung der Verhältnismäßigkeit erfolgt, die auch dem grenzüberschreitenden Charakter des organisierten Verbrechens sowie den Erfordernissen eines Höchstmaßes an Sicherheit in allen Mitgliedstaaten Rechnung trägt.

Des Weiteren muss klargestellt werden, dass die in der Richtlinie genannte Aufbewahrungsfrist als für alle Mitgliedstaaten geltende einheitliche Höchstgrenze zu betrachten ist.

Das heißt, es muss deutlich zum Ausdruck kommen, dass die Mitgliedstaaten keine längeren Speicherfristen als in der Richtlinie vorgesehen festlegen dürfen, während es ihnen freisteht, kürzere Zeiträume vorzuschreiben. Außerdem ist darauf hinzuweisen, dass die Daten nach Ablauf der genannten Fristen gelöscht werden müssen. Vor diesem Hintergrund ist der derzeitige Wortlaut des Artikels 11 des Richtlinienentwurfs als nicht zufriedenstellend anzusehen.

Die Datenschutzgruppe begrüßt, dass der Vorschlag in Artikel 12 eine mindestens alle zwei Jahre durchzuführende regelmäßige Bewertung vorsieht.

Diese Bewertung sollte sich auch auf die Notwendigkeit der von den Strafverfolgungsbehörden in spezifischen und genau umrissenen Fällen verwendeten Verkehrsdaten beziehen und unter Mitwirkung der Datenschutzbehörden erfolgen. Das Ergebnis der Bewertungen ist zu veröffentlichen.

Dabei ist jedoch darauf hinzuweisen, dass sich die Bewertung nicht auf einen unbegrenzten Zeitraum beziehen sollte, da der Vorschlag auf der konkreten Beurteilung der in ihm genannten Annahmen und Voraussetzungen basiert. Daher müssen die beabsichtigten Maßnahmen zur Vorratsdatenspeicherung gemäß dem Konzept der Befristung von Rechtsvorschriften („sunset legislation“) zeitlich befristet werden. Die Datenschutzgruppe hält eine Dreijahresfrist für angemessen. Nach Ablauf dieses Zeitraums müssen die innerstaatlichen Maßnahmen, mit denen die Speicherung von Daten in Umsetzung der Richtlinie vorgeschrieben wird, ihre Rechtskraft verlieren, unbeschadet der Möglichkeit, die Analyse, die im Vorfeld einer neuerlichen Entscheidung des Rates und des Europäischen Parlaments zur Billigung einer neuen Richtlinie erforderlich ist, auch vor Ablauf der drei Jahre einzuleiten.

Im Hinblick auf den Grundsatz der Verhältnismäßigkeit begrüßt die Datenschutzgruppe, dass die Datenmenge, die zur Internetnutzung vorgehalten werden soll, beschränkt wird. Darüber hinaus ist die Festlegung einer Höchstmenge zu speichernder Daten einer Minimalliste vorzuziehen. Generell sind die zu speichernden Daten auf diejenigen zu beschränken, die von den Anbietern zu technischen Zwecken und zur Gebührenabrechnung gesammelt werden.

Wesentlich sind Festlegungen bezüglich des Zugangs zu den Daten und der Verwendungszwecke; es ist sicherzustellen, dass Maßnahmen zur generellen Vorratsdatenspeicherung von strengsten Schutzmaßnahmen begleitet sind und einer Prüfung unterzogen werden.

3. Die Schutzvorkehrungen, die der geltende Rechtsrahmen für den Datenschutz innerhalb der ersten Säule (Richtlinien 95/46/EG und 2002/58/EG) bietet, müssen für die mit der Vorratsdatenspeicherung verknüpften Strafverfolgungszwecke näher spezifiziert werden. Solche spezifischen Schutzvorkehrungen sind von entscheidender Bedeutung, um sicherzustellen, dass der Schutz, den Richtlinie 2002/58/EG insbesondere für das Recht auf Vertraulichkeit bei der Verwendung öffentlich zugänglicher elektronischer Kommunikationsdienste bietet, nicht in wesentlichen Punkten ausgehöhlt wird.

Darüber hinaus bedarf es nach Ansicht der Datenschutzgruppe eines angemessenen Schutzes in Bezug auf die Datenverarbeitung in Bereichen, die gegenwärtig nicht in den Geltungsbereich dieser Richtlinien fallen.

Aus diesem Grund vertritt die Datenschutzgruppe u. a. die Auffassung, dass der Richtlinienentwurf selbst entsprechende Schutzmaßnahmen vorsehen sollte oder aber zusammen mit anderen geeigneten Rechtsinstrumenten bewertet und verabschiedet werden sollte. Die Datenschutzgruppe ist insbesondere der Meinung, dass in diesem Zusammenhang auch der „Rahmenbeschluss des Rates über den Schutz personenbezogener Daten, die im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen verarbeitet werden“ einer sorgfältigen Bewertung zu unterziehen ist.

Abschließend ist die Datenschutzgruppe angesichts der Auswirkungen auf die Grundrechte und -freiheiten der betroffenen Bürger der Überzeugung, dass die möglicherweise einzuführenden Maßnahmen umfassend bekannt gemacht werden müssen.

III. SONSTIGE SPEZIFISCHE SCHUTZVORKEHRUNGEN

Im Übrigen müssen nach Auffassung der Datenschutzgruppe die folgenden Aspekte zumindest in Angriff genommen werden:

1. ZWECKE

Die Daten dürfen nur zu spezifischen Zwecken der Bekämpfung des Terrorismus und der organisierten Kriminalität gespeichert werden, statt auf andere, nicht näher bestimmte „schwere Straftaten“ Bezug zu nehmen. Diese beschränkte Zweckbestimmung sollte auch im Titel der vorgeschlagenen Richtlinie zum Ausdruck kommen.

2. EMPFÄNGER

Die Richtlinie sollte vorsehen, dass die Daten nur eigens benannten Strafverfolgungsbehörden verfügbar gemacht werden und nur insoweit, als dies zur Ermittlung, Feststellung, Verfolgung und/oder Verhütung von Terrorakten notwendig ist. Ein Verzeichnis der eigens benannten Strafverfolgungsbehörden sollte öffentlich zugänglich sein.

3. DATA MINING

Die Terrorismusprävention darf nicht mit flächendeckendem Data Mining auf Grundlage der in der Richtlinie genannten Informationen über das Reise- und Kommunikationsverhalten von Personen einhergehen, die von den Strafverfolgungsbehörden nicht zum Kreis der Verdächtigen gezählt werden. Der Zugang muss auf diejenigen Daten beschränkt werden, die im Rahmen spezifischer Ermittlungen benötigt werden.

4. WEITERVERARBEITUNG

Jedwede Weiterverarbeitung vorgehaltener Daten durch die Strafverfolgungsbehörden für andere verwandte Verfahren muss verboten oder gestützt auf spezifische Schutzvorkehrungen streng begrenzt werden; jeder Zugriff anderer staatlicher Behörden auf die Daten muss unterbunden werden. Die in früheren europäischen Rechtsinstrumenten festgelegten Vorschriften für den Bereich der elektronischen Kommunikation dürfen nicht in einer Art und Weise angewandt werden, die mit diesem Grundsatz unvereinbar ist.

5. ZUGRIFFSPROTOKOLLE

Jeder Abruf der Daten ist zu protokollieren. Die Aufzeichnungen dürfen nur auf Anforderung und nur der Behörde und/oder dem unter Punkt 6 genannten Organ sowie den Datenschutzbehörden zu Kontrollzwecken zur Verfügung gestellt werden und müssen ein Jahr nach Erstellung gelöscht werden.

6. RICHTERLICHE/UNABHÄNGIGE PRÜFUNG

Der Zugang zu den Daten muss grundsätzlich im Einzelfall von einer Justizbehörde ordnungsgemäß genehmigt werden, unbeschadet der Tatsache, dass der Zugriff in manchen Ländern für bestimmte Fälle unter unabhängiger Aufsicht rechtlich zulässig ist. Wo dies angebracht ist, sollten die Genehmigungen die in den betreffenden Fällen benötigten Daten aufführen.

7. ADRESSATEN

Die Richtlinie muss eindeutig festlegen, für welche Anbieter öffentlich zugänglicher Kommunikationsdienste die Pflichten gelten. In Bezug auf das Internet ist eine Beschränkung auf Zugangsanbieter und auf Individualkommunikation (E-Mail-Dienste, Internettelefonie) erforderlich.

8. IDENTIFIZIERUNG

Ferner muss in dieser Richtlinie auch klargestellt werden, dass keine Identifikationspflicht in den Fällen besteht, in denen eine Identifizierung weder zur Gebührenabrechnung noch zu anderen Vertragszwecken erforderlich ist.

9. ZWECKE DER ÖFFENTLICHEN ORDNUNG

Den Anbietern öffentlich zugänglicher elektronischer Kommunikationsdienste oder Betreibern öffentlich zugänglicher elektronischer Kommunikationsnetze darf nicht gestattet werden, allein zu Zwecken der öffentlichen Ordnung gespeicherte Daten zu ihren eigenen Zwecken zu verarbeiten.

10. GETRENNTE SYSTEME

Insbesondere müssen die für die Datenspeicherung zu Zwecken der öffentlichen Ordnung verwendeten Systeme von den Systemen, die für die geschäftlichen Zwecke der Anbieter verwendet werden, logisch getrennt und durch strengere Sicherheitsvorkehrungen geschützt werden (z. B. durch Verschlüsselung), um einen unautorisierten Zugang und eine Nutzung durch Unbefugte zu verhindern.

11. SICHERHEITSMAßNAHMEN

Die Gemeinschaftsmaßnahmen müssen Mindeststandards für die von den Anbietern zu treffenden technischen und organisatorischen Sicherheitsvorkehrungen vorschreiben; dabei ist auf die in Richtlinie 2002/58/EG aufgestellten allgemeinen Anforderungen an Sicherheitsmaßnahmen Bezug zu nehmen.

12. DRITTE

Die Gemeinschaftsmaßnahmen müssen festlegen, dass der Zugang Dritter zu den gespeicherten Daten rechtswidrig ist.

13. DEFINITIONEN

Die Datenkategorien müssen klar definiert werden; außerdem muss eine Beschränkung auf Verkehrsdaten erfolgen.

14. AUFLISTUNG DER DATEN UND REVISIONSMECHANISMEN

Die zu speichernden personenbezogenen Daten müssen in der Richtlinie selbst konkret aufgelistet werden. Dies ist für eine genaue Beurteilung der Auswirkungen auf die Grundrechte und -freiheiten der betroffenen Bürger wichtig; dabei sind die Gefahren für ihre Privatsphäre ebenso zu berücksichtigen wie Fragen, die mit der Gewährleistung der Genauigkeit und Korrektheit der vorgehaltenen Daten verbunden sind. Vorschläge zur Änderung des Verzeichnisses der zu speichernden Daten müssen stets einer strengen Prüfung der Notwendigkeit unterzogen werden. Angesichts der Auswirkungen dieser Maßnahmen auf die Grundrechte und -freiheiten sollte die Überarbeitung des besagten Verzeichnisses nur mit Billigung des Europäischen Parlaments und unter Einbeziehung der Datenschutzbehörden erfolgen. Auch die Beteiligung von Vertretern der Verbraucher- und Nutzerverbände, anderer relevanter Nichtregierungsorganisationen und der europäischen Verbände der Kommunikationsindustrie sollte in Betracht gezogen werden. In dieser Hinsicht erscheint es nicht als angemessen, die Überarbeitung des Verzeichnisses wie in der Richtlinie vorgesehen lediglich im Ausschussverfahren durchzuführen.

15. KEINE SPEICHERUNG VON INHALTSDATEN

Da der Kommunikationsinhalt vom Geltungsbereich des Vorschlags ausgenommen sein soll, müssen spezifische Schutzvorkehrungen eingeführt werden, um eine scharfe und wirksame Trennung zwischen Inhalts- und Verkehrsdaten sicherzustellen, sowohl für den Bereich des Internets (d. h. Beschränkung auf Anmelde- und Abmeldedaten oder sonstige Informationen wie Mailserver- und Web-Cache-Protokolle und Aufzeichnungen des IP-Verkehrs) als auch für den Bereich der Telefonie (Konferenzschaltungen, Fax, SMS, Sprachtelefonie).

16. NICHT ZUSTANDE GEKOMMENE KOMMUNIKATION

Die verschiedenen Kategorien von Verkehrsdaten zu nicht zustande gekommenen Kommunikationen sollten ohne gründliche Bewertung der Angemessenheit im Lichte der oben genannten Grundsätze nicht einbezogen werden.

17. STANDORTDATEN

Die Speicherung von Standortdaten sollte nicht über die Funkzellen-Identifikationsnummer (Cell-ID) zu Beginn eines Kommunikationsvorgangs hinausgehen.

18. WIRKSAME AUFSICHT

Die ursprüngliche Nutzung und jede weitere mit ihr zu vereinbarende Verwendung (einschließlich Vervielfältigung) müssen wirksamen Kontrollen unterliegen, und zwar im Rahmen und zu Zwecken eines Strafverfahrens durch die Justizbehörden sowie in Bezug auf Datenschutzaspekte unabhängig von der Existenz eines Gerichtsverfahrens durch die Datenschutzbehörden.

19. VERÖFFENTLICHUNG

Die Richtlinie sollte die Pflicht zur angemessenen Information aller Bürger über jedwede Verarbeitungsoperationen enthalten, die möglicherweise nach Umsetzung der in ihr vorgesehenen Maßnahmen durchgeführt werden.

20. KOSTEN

Die Datenschutzgruppe stellt fest, dass die Anbieter öffentlich zugänglicher elektronischer Kommunikationsdienste oder Betreiber öffentlich zugänglicher elektronischer Kommunikationsnetze für zusätzliche Kosten von den Mitgliedstaaten entschädigt werden müssen. Die Datenschutzgruppe möchte die Bedeutung dieses Aspekts ausschließlich in Bezug auf direkt mit dem Datenschutz in Verbindung stehende Merkmale betonen. Maßnahmen zur Vorratsdatenspeicherung sollten verbunden sein mit der Erstattung von Investitionen in die Anpassung der Kommunikationssysteme, von Auslagen für die Übermittlung der Daten an die Strafverfolgungsbehörden und für Sicherheitsvorkehrungen. Hier ist eine umfassende Betrachtung erforderlich, um negative Folgen zu vermeiden, sowohl in Bezug auf den Datenschutz als auch in wirtschaftlicher Hinsicht für die Bürger, denen unter Umständen einige der den Anbietern/Betreibern entstehenden Kosten in Rechnung gestellt werden. In diesem Zusammenhang könnte auch in Erwägung gezogen werden, den Anspruch der Anbieter/Betreiber auf Kostenerstattung von der Einhaltung der Mindeststandards abhängig zu machen und im Einzelfall zu prüfen.

Die Datenschutzgruppe ist zuversichtlich, dass die in dieser Stellungnahme enthaltenen Überlegungen angemessene Berücksichtigung finden werden, und weist darauf hin, dass alle oben genannten Schutzmaßnahmen getroffen werden sollten, ehe die Vorratsspeicherpflicht in die Praxis umgesetzt wird.

Brüssel, den 21. Oktober 2005

Für die Datenschutzgruppe

Der Vorsitzende

Peter Schaar