RAT DER EUROPÄISCHEN UNION

Brüssel, den 29. Juni 2005 (05.07)
(OR. en)

10609/05

Interinstitutionelles Dossier: 2004/0813 (CNS)

LIMITE

COPEN 102
TELECOM 64

DOKUMENT TEILWEISE ZUGÄNGLICH

VERMERK

des	künftigen Vorsitzes
für	die Gruppe "Zusammenarbeit in Strafsachen"
Nr. Vordokument:	8864/1/05 REV 1 COPEN 91 TELECOM 33
Betr.:	Entwurf eines Rahmenbeschlusses über die Vorratsspeicherung von Daten, die in Verbindung mit der Bereitstellung öffentlicher elektronischer Kommunikationsdienste verarbeitet und aufbewahrt werden, und Daten, die in öffentlichen Kommunikationsnetzen vorhanden sind, für Ermittlung, Aufklärung und Verfolgung bei Straftaten, einschließlich Terrorismus

I. TAGUNG DES RATES (JI) IM JUNI 2005

Der Rat (JI) hat den eingangs genannten Entwurf eines Rahmenbeschlusses auf seiner Tagung am 2. und 3. Juni 2005 auf der Grundlage von Dokument 8864/1/05 REV 1 COPEN 91 TELECOM 33 geprüft. Er war sich einig, dass die Vorratsspeicherung von Kommunikationsdaten einen wichtigen Beitrag zur Bekämpfung von Kriminalität und Terrorismus leistet und dass hierfür ein Rechtsakt der EU erforderlich ist. Bei einigen Fragen konnte jedoch kein Einvernehmen erzielt werden. Nach einer ausführlichen Aussprache zog der Vorsitz die folgenden Schlussfolgerungen:

– Im Interesse rascher Fortschritte sollte bei der Frage, welche Kommunikationsdaten auf Vorrat gespeichert werden sollen, schrittweise vorgegangen werden. Dabei könnte mit der Vorratsspeicherung von Daten der Telefonkommunikation über Festnetz und Mobilfunk begonnen werden. Was das Internet und nicht erfolgreich abgehende Anrufe betrifft, so könnte den Mitgliedstaaten, die nicht in der Lage sind, die betreffenden Kommunikationsdaten sofort zu erheben, eine Übergangszeit eingeräumt werden, deren Dauer noch festzulegen wäre.

– Was die Liste der auf Vorrat zu speichernden Kommunikationsdaten (Artikel 2) anbelangt, so bestand allgemeines Einvernehmen über den Vorschlag des Vorsitzes. Danach gäbe es eine Mindestliste, die vor allem praktisch ausgerichtet wäre, aber auch einige technische Einzelheiten umfassen würde. Die Detailfragen im Zusammenhang mit dieser Liste müssen von den Sachverständigen noch eingehender geprüft werden.
– Es müssen weitere Gespräche zwischen den Anbietern von Kommunikationsdiensten und den Strafverfolgungsbehörden stattfinden, um mehr über die mit der Vorratsspeicherung von Daten verbundenen Kosten in Erfahrung zu bringen.
– Die meisten Delegationen könnten die vom Vorsitz vorgeschlagenen Fristen für die Vorratsspeicherung (Artikel 4) akzeptieren. Danach würden die Daten in der Regel 12 Monate lang gespeichert; die Mitgliedstaaten könnten jedoch in Ausnahmefällen längere Fristen (bis zu 48 Monate) oder kürzere Fristen (mindestens 6 Monate) vorsehen.
– Was die Rechtsgrundlage betrifft, so ist die Mehrheit der Delegationen der Auffassung, dass der vorgeschlagene Rechtsakt unter die dritte Säule fällt.

UK kündigte an, dass das Dossier auf der informellen Tagung der Justiz- und Innenminister im September 2005 weiter erörtert werden soll, damit auf der Tagung des Rates (JI) im Oktober 2005 förmliche Beratungen stattfinden können.

Nach wie vor bestehen auf Seiten mehrerer Delegationen allgemeine Prüfungsvorbehalte bzw. Parlamentsvorbehalte. Der niederländische Minister legte dem Rat die Auffassung des niederländischen Parlaments dar und erklärte, dass er vorerst keine endgültige Stellungnahme zu diesem Thema abgeben könne.

II. WEITERES VORGEHEN

In Anbetracht der Schlussfolgerungen des Rates (JI) vom Juni schlägt der künftige Vorsitz vor, in der Sitzung der Gruppe "Zusammenarbeit in Strafsachen" am 4. und 5. Juli 2005 die folgenden Fragen zu erörtern:

– Liste der auf Vorrat zu speichernden Kommunikationsdaten, einschließlich eines schrittweisen Vorgehens in Bezug auf diese Liste;
– Ausnahmen von den Speicherfristen;
– Kosten und Nutzen der Vorratsspeicherung von Kommunikationsdaten;
– Datensicherheit.

In der Sitzung sollen die noch offenen Detailfragen im Zusammenhang mit den Artikeln 1-5 geklärt und es sollen Vorarbeiten für eine Aussprache über Kosten und Nutzen der Vorratsspeicherung von Daten auf der informellen Tagung der Justiz- und Innenminister im September 2005 geleistet werden. Bei den noch offenen Fragen betreffend die Rechtsgrundlage und die Vorschriften über die justizielle Zusammenarbeit (Artikel 7) erfolgt eine Verweisung an den Ausschuss "Artikel 36"/ AStV/Rat (JI).

a) Liste der auf Vorrat zu speichernden Daten

Der künftige Vorsitz beabsichtigt, die Liste in der Sitzung eingehend zu prüfen. Er hat daher eine überarbeitete Fassung der Artikel 2, 3 und 8 (siehe Anlage) erstellt. Die neue Fassung von Artikel 3 enthält die Liste der auf Vorrat zu speichernden Kommunikationsdaten, einschließlich Festnetz- und Mobilfunkdaten, Internetdaten sowie Daten über nicht erfolgreich abgehende Anrufe. Artikel 8 sieht eine Übergangsfrist für Internetdaten und Daten über nicht erfolgreich abgehende Anrufe vor.

b) Fristen für die Vorratsspeicherung

Auf der Tagung des Rates (JI) im Juni war das Konzept für die Speicherfristen in Artikel 4 auf Zustimmung gestoßen. Einige Delegationen bekundeten allerdings Interesse für den Vorschlag, für bestimmte Daten eine Ausnahme von der sechsmonatigen Speicherfrist vorzusehen (siehe Vermerk 8864/1/05 REV 1 COPEN 91 TELECOM 33). In Anbetracht der Ergebnisse dieser Aussprache schlägt der künftige Vorsitz Änderungen zu Artikel 4 (siehe Anlage) vor, um die Beratungen voranzubringen.

c) Kosten und Nutzen

Der Rat (JI) war auf seiner Tagung im Dezember 2004 übereingekommen, dass bei dem Rahmenbeschlussentwurf besonders auf Verhältnismäßigkeit geachtet werden muss. Daher bedarf es genauerer Informationen über die mit der Vorratsspeicherung von Kommunikationsdaten verbundenen Kosten und den voraussichtlichen Nutzen der Speicherung dieser Daten für Zwecke der Strafverfolgung.

Bei den Beratungen auf der Tagung des Rates (JI) hat sich ergeben, dass zunächst eindeutig ermittelt werden muss, welche Kosten die Vorratsspeicherung der unter Artikel 2 fallenden Kommunikationsdaten verursachen würde. Der künftige Vorsitz schlägt vor, die Kostenfrage mit dem Ziel zu prüfen,

– eine Bilanz der vorliegenden Informationen zu ziehen,

– zu erörtern, wie diese Informationen ergänzt werden können, da es genauer, verlässlicher und ausführlicher Informationen bedarf, um Kosten und Nutzen der Maßnahme gegeneinander abwägen zu können.

Zu diesem Zweck schlägt der künftige Vorsitz zudem die überarbeitete Fassung des Erwägungsgrunds 16 (siehe Anlage) vor.

Was die voraussichtlichen Kosten und den zu erwartenden Nutzen der Maßnahme betrifft, so wird UK vor der Sitzung am 4./5. Juli 2005 ein gesondertes Papier verteilen, in dem ausführlich dargelegt werden wird, welche Erfahrungen im Vereinigten Königreich bislang mit der Verwendung von Kommunikationsdaten für Ermittlungen in Strafsachen gemacht wurden. Dieses Papier wird Statistiken über die von den Strafverfolgungsbehörden angeforderten auf Vorrat gespeicherten Daten enthalten, wobei auch das Alter der Daten und die jeweilige Straftat genannt werden; zudem wird dem Papier zu entnehmen sein, welche Kosten die Vorratspeicherung dieser Daten verursacht hat. Der künftige Vorsitz ersucht die anderen Delegationen, in der kommenden Sitzung ausführlich über die Erfahrungen ihres Landes mit der Nutzung von Kommunikationsdaten zu berichten und diese Informationen möglichst vor der Sitzung dem Generalsekretariat (E-Mail bent.mejborn@consilium.eu.int) zu übermitteln.

d) Datensicherheit

Der künftige Vorsitz möchte die Fußnoten zu Artikel 5 mit dem Ziel prüfen, die Beratungen über diese Bestimmung abzuschließen.

ANLAGE

Entwurf
Rahmenbeschluss
über die Vorratsspeicherung von Daten, die in Verbindung mit der Bereitstellung öffentlicher elektronischer Kommunikationsdienste verarbeitet und aufbewahrt werden, und Daten, die in öffentlichen Kommunikationsnetzen vorhanden sind, für (…), Ermittlung, Aufklärung und Verfolgung bei Straftaten, einschließlich Terrorismus [1]

DER RAT DER EUROPÄISCHEN UNION –

gestützt auf den Vertrag über die Europäische Union, insbesondere auf Artikel 31 Absatz 1 Buchstabe c und Artikel 34 Absatz 2 Buchstabe b,

auf Initiative der Französischen Republik, Irlands, des Königreichs Schweden und des Vereinigten Königreichs,

nach Stellungnahme des Europäischen Parlaments,

in Erwägung nachstehender Gründe:

(1) Für ein hohes Maß an Schutz in einem Raum der Freiheit, der Sicherheit und des Rechts bedarf es bei Straftaten einer effizienten und wirkungsvollen (…), Ermittlung, Aufklärung und Verfolgung unter Achtung der grundlegenden Menschenrechte des Einzelnen.

(2) Maßnahmen gegen Hightech-Kriminalität wurden gefordert im Aktionsplan des Rates und der Kommission zur bestmöglichen Umsetzung der Bestimmungen des Amsterdamer Vertrags über den Aufbau eines Raums der Freiheit, der Sicherheit und des Rechts, in den Schlussfolgerungen des Europäischen Rates von Tampere (15./16. Oktober 1999) und Santa Maria da Feira (19./20. Juni 2000), von der Kommission in ihrem "Fortschrittsanzeiger" sowie vom Europäischen Parlament in seiner Entschließung vom 19. Mai 2000.

[1] Angesichts der Ausführungen des Juristischen Dienstes auf der Tagung des AStV vom 19. Mai 2005 hat der Vorsitz, vorbehaltlich einer weiteren Prüfung, den Ausdruck "Vorbeugung" aus dem Titel des Entwurfs und aus bestimmten Erwägungsgründen gestrichen.

(3) Der Rat hat sich in seinen Schlussfolgerungen vom 20. September 2001 dafür ausgesprochen, die Strafverfolgungsbehörden in die Lage zu versetzen, Ermittlungen zu kriminellen Handlungen durchzuführen, die unter Nutzung elektronischer Kommunikationssysteme begangen wurden, und Maßnahmen gegen die Urheber zu ergreifen, und dabei darauf zu achten, dass ein Gleichgewicht zwischen dem Schutz personenbezogener Daten und der Notwendigkeit des Zugangs der Strafverfolgungsbehörden zu Daten für strafrechtliche Ermittlungszwecke gewährleistet ist. In seinen Schlussfolgerungen vom 19. Dezember 2002 hat der Rat festgestellt, dass die beträchtliche Ausweitung der Möglichkeiten bei der elektronischen Kommunikation dazu geführt hat, dass Daten über die Nutzung elektronischer Kommunikationsmittel heutzutage ein besonders wichtiges und hilfreiches Mittel für die (…), Ermittlung, Aufklärung und Verfolgung bei Straftaten, insbesondere von organisierter Kriminalität und Terrorismus, darstellen.

(4) In der vom Europäischen Rat am 25. März 2004 angenommenen Erklärung zum Kampf gegen den Terrorismus wurde der Rat beauftragt, Maßnahmen für die Erarbeitung von Rechtsvorschriften über die Aufbewahrung von Verkehrsdaten durch die Diensteanbieter zu prüfen und diese bis Juni 2005 anzunehmen.

(5) Es ist von wesentlicher Bedeutung, dass in öffentlichen Kommunikationsnetzen vorhandene Daten, die aufgrund eines Kommunikationsvorgangs erzeugt worden sind, nachstehend "Daten" genannt, für die (…) Ermittlung, Aufklärung und Verfolgung bei Straftaten, insbesondere unter Nutzung elektronischer Kommunikationssysteme begangene Straftaten, auf Vorrat gespeichert werden. Dieser (…) Rahmenbeschluss bezieht sich nur auf Daten, die aufgrund eines Kommunikationsvorgangs oder eines Kommunikationsdienstes erzeugt worden sind, und nicht auf Daten, die den Kommunikationsinhalt darstellen. Es ist insbesondere erforderlich, Daten auf Vorrat zu speichern, um die Quelle eines illegalen Inhalts, z.B. Kinderpornografie und rassistisches und fremdenfeindliches Material, sowie die Urheber von Angriffen auf die Informationssysteme ermitteln und diejenigen identifizieren zu können, die sich an der Nutzung der elektronischen Kommunikationsnetze für die Zwecke der organisierten Kriminalität und des Terrorismus beteiligen.

(6) Die Sicherungsspeicherung spezifischer Daten zu bestimmten Personen in besonderen Fällen allein reicht nicht aus, um diesen Anforderungen zu entsprechen. Bei Ermittlungen kann es vorkommen, dass die benötigten spezifischen Daten oder die betreffende Person erst Monate oder Jahre nach dem ursprünglichen Kommunikationsvorgang identifiziert werden können. Daher ist es geboten, bestimmte Datentypen, die bereits zu Fakturierungszwecken, zu kommerziellen Zwecken oder zu anderen rechtmäßigen Zwecken verarbeitet und aufbewahrt werden, während (...) zusätzlicher Zeiträume aus der Überlegung heraus auf Vorrat zu speichern, dass sie für künftige Ermittlungen oder Gerichtsverfahren erforderlich sein könnten. Dieser Rahmenbeschluss betrifft daher die Vorratsspeicherung von Daten und nicht die Sicherungsspeicherung von Daten.

(7) In Anerkennung der Notwendigkeit, dass Daten auf Vorrat gespeichert werden, wurde in Artikel 15 der Richtlinie 2002/58/EG die Möglichkeit vorgesehen, Rechtsvorschriften zu erlassen, die unter bestimmten Voraussetzungen die Vorratsspeicherung von Daten für die Zwecke der Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten ermöglichen. Der vorliegende Rahmenbeschluss betrifft nicht die anderen Zielsetzungen nach Artikel 15 der genannten Richtlinie und enthält daher keine Vorschriften über die Vorratsspeicherung von Daten für den Schutz der nationalen Sicherheit (d.h. der Sicherheit des Staates), die Landesverteidigung und die öffentliche Sicherheit. Er betrifft auch nicht die unrechtmäßige Nutzung des elektronischen Kommunikationssystems, wenn diese Nutzung keine strafbare Handlung darstellt.

(8) Viele Mitgliedstaaten haben Rechtsvorschriften über eine Vorratsspeicherung von Daten zum Zwecke der Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten erlassen. In anderen Mitgliedstaaten sind entsprechende Arbeiten im Gang. Der Inhalt dieser Rechtsvorschriften ist in den einzelnen Mitgliedstaaten sehr unterschiedlich.

(9) Die Unterschiede zwischen den Rechtsvorschriften der Mitgliedstaaten beeinträchtigen die Zusammenarbeit der Behörden, die für (…) Ermittlung, Aufklärung und Verfolgung bei Straftaten zuständig sind. Für eine wirksame polizeiliche und justizielle Zusammenarbeit in Strafsachen muss daher sichergestellt werden, dass alle Mitgliedstaaten die erforderlichen Schritte unternehmen, um bestimmte Arten von Daten eine gewisse Zeit lang gemäß festgelegten Vorgaben für die Zwecke der (…) Ermittlung, Aufklärung und Verfolgung bei Straftaten, einschließlich Terrorismus, auf Vorrat zu speichern. Diese Daten hätten den anderen Mitgliedstaaten gemäß den nach Titel VI des Vertrags über die Europäische Union angenommenen Rechtsakten über die justizielle Zusammenarbeit in Strafsachen zur Verfügung stehen. Dies sollte auch für Regelungen gelten, die nicht gemäß diesem Titel angenommen wurden, denen die Mitgliedstaaten aber beigetreten sind und auf die in den gemäß Titel VI des Vertrags über die Europäische Union angenommenen Rechtsakten über die justizielle Zusammenarbeit in Strafsachen Bezug genommen wird.

(9a) In einem Raum der Freiheit, der Sicherheit und des Rechts sind gesetzliche Verpflichtungen für die Wirtschaft zur Vorratsspeicherung von Daten nur dann zu rechtfertigen, wenn diese notwendig sind, um Interessen zu wahren, die in einer demokratischen Gesellschaft von Belang sind. Diese Notwendigkeit ergibt sich daraus, dass die Ermittlung, Aufklärung und Verfolgung von terroristischen Straftaten oder anderen schweren Straftaten die Analyse bestimmter historischer Daten erfordert. Stellen diese Daten den einzigen erfolgversprechenden Ansatz für die tatsächliche Aufklärung solcher Straftaten dar, so lässt sich ihre Verfügbarkeit für einen bestimmten Zeitraum nur mit Hilfe einer gesetzlichen Verpflichtung auf zuverlässige Weise gewährleisten[1].

[1] Vorschlag des künftigen Vorsitzes auf der Grundlage des Textvorschlags von **GESTRICHEN** in Fußnote 4 zu Artikel 1 in Dok. 8864/1/05 REV 1 COPEN 91 TELECOM 33.

(10) Diese Vorratsspeicherung von Daten und der Zugriff auf diese Daten können einen Eingriff in das Privatleben des Einzelnen darstellen. Diese Eingriffe stellen jedoch keine Verletzung der internationalen Vorschriften über den Schutz der Privatsphäre und die Verarbeitung personenbezogener Daten dar, die insbesondere in der Europäischen Konvention zum Schutze der Menschenrechte und Grundfreiheiten vom 4. November 1950, im Übereinkommen Nr. 108 des Europarates zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten sowie in den Richtlinien 95/46/EG, 97/66/EG und 2002/58/EG enthalten sind, in denen solche Eingriffe gesetzlich erlaubt sind, sofern sie zweckdienlich sind, in einem strikt angemessenen Verhältnis zum beabsichtigten Zweck stehen und innerhalb einer demokratischen Gesellschaft notwendig sind und sofern sie mit angemessenen Garantien im Hinblick auf (…) Ermittlung, Aufklärung und Verfolgung bei Straftaten, einschließlich Terrorismus, verbunden sind.

(11) In Anbetracht sowohl der Notwendigkeit einer wirksamen und harmonisierten Vorratsspeicherung der Daten wie auch des Erfordernisses, den Mitgliedstaaten wegen der Unterschiede zwischen den einzelstaatlichen strafrechtlichen Systemen genügend Handlungsspielraum für ihre eigene individuelle Einschätzung einzuräumen, sollten Parameter für die Vorratsspeicherung von Daten festgelegt werden.

(12) Daten dürfen je nach Datentyp für unterschiedliche Fristen auf Vorrat gespeichert werden. Die Fristen für die Vorratsspeicherung der einzelnen Datentypen richten sich nach dem Nutzen der Daten für (…) Ermittlung, Aufklärung und Verfolgung bei Straftaten und nach den Kosten der Vorratsspeicherung der Daten. Die Fristen der Vorratsspeicherung müssen in einem angemessenen Verhältnis zur Notwendigkeit solcher Daten für (…) Ermittlung, Aufklärung und Verfolgung bei Straftaten sowie zum Eingriff in die Privatsphäre stehen, zu der eine solche Vorratsspeicherung bei Freigabe solcher Daten führt.

(13) Bei der Erstellung von Listen der auf Vorrat zu speichernden Datentypen ist auf eine ausgewogene Berücksichtigung des Nutzens der Aufbewahrung der einzelnen Datentypen für die (…) Ermittlung, Aufklärung und Verfolgung bei Straftaten und des damit verbundenen Umfangs des Eingriffs in die Privatsphäre zu achten.

(14) Dieser Rahmenbeschluss gilt nicht für den Zugriff auf Daten während der Übertragung, d.h. für das Abhören, die Überwachung oder die Aufzeichnung von Telekommunikationsvorgängen.

(15) Die Mitgliedstaaten müssen sicherstellen, dass der Zugriff auf die auf Vorrat gespeicherten Daten unter Beachtung der Datenschutzbestimmungen erfolgt, die in den völkerrechtlichen Vorschriften über den Schutz personenbezogener Daten festgelegt sind.

(16) Die Mitgliedstaaten stellen sicher, dass die Durchführung (…) dieses Rahmenbeschlusses nach entsprechender Konsultation der Wirtschaft, insbesondere hinsichtlich der Durchführbarkeit und der Kosten der Vorratsspeicherung erfolgt. In Anerkennung der Tatsache, dass die Vorratsspeicherung von nicht länger zu Geschäftszwecken benötigten Daten einen praktischen und finanziellen Aufwand für die Wirtschaft darstellen kann, sollten die Mitgliedstaaten eine angemessene Beteiligung an den Kosten erwägen, die der Wirtschaft aufgrund der mit der Umsetzung dieses Rahmenbeschlusses verbundenen Verpflichtungen oder Selbstverpflichtungen entstehen –

HAT FOLGENDEN RAHMENBESCHLUSS ANGENOMMEN:

Artikel 1[1]

Geltungsbereich und Ziel

(1) Mit diesem Rahmenbeschluss soll die justizielle Zusammenarbeit in Strafsachen erleichtert werden, indem die Rechtsvorschriften der Mitgliedstaaten über die Vorratsspeicherung von Kommunikationsdaten[2], die von Anbietern eines öffentlich zugänglichen elektronischen Kommunikationsdienstes oder von Betreibern eines öffentlichen Kommunikationsnetzes erzeugt oder verarbeitet[3] werden, für die Zwecke der Ermittlung, Aufklärung und Verfolgung bei Straftaten angeglichen werden.

(2) Dieser Rahmenbeschluss gilt für alle Kommunikationsdaten, die von Anbietern eines öffentlich zugänglichen elektronischen Kommunikationsdienstes erzeugt oder verarbeitet werden (...).

(3) Dieser Rahmenbeschluss gilt nicht für den Inhalt des Kommunikationsaustauschs, auch nicht für den Abruf von Informationen unter Nutzung eines elektronischen Kommunikationsnetzes.

---

1 **GESTRICHEN** haben einen Prüfungsvorbehalt zu Artikel 1.

2 **GESTRICHEN** legte einen Prüfungsvorbehalt zur Verwendung des Begriffs "*communication*" ein, der in der Richtlinie 2002/58/EG definiert ist. Der Vorsitzende bemerkte dazu, dass im vorliegendem Entwurf der Begriff "*communication data*" ("Kommunikationsdaten") und nicht nur "*communication*" benutzt werde und der Text somit nicht in Konflikt mit der Definition von "*communication*" ("Nachricht") in der genannten Richtlinie stehe.

3 **GESTRICHEN** schlug den folgenden Erwägungsgrund vor: "Der Begriff 'verarbeitet' sollte sich nur auf solche Daten beziehen, die erforderlich sind, um Verbindungen für diesen Dienst herzustellen, aufrechtzuerhalten und zu verwalten (Verkehrsdaten zu Teilnehmern und Nutzern, die vom Betreiber eines öffentlichen Kommunikationsnetzes oder vom Anbieter eines öffentlich zugänglichen elektronischen Kommunikationsdienstes verarbeitet werden); Daten, die hierzu nicht erforderlich sind, sollten nicht eingeschlossen sein (z.B. die Betreffzeile in einer E-Mail)."
Einige Delegationen haben einen Prüfungsvorbehalt zu diesem Vorschlag.

(4) Unberührt von diesem Rahmenbeschluss bleiben

– nationale Rechtsvorschriften über die Vorratsspeicherung von Kommunikationsdaten, die von Anbietern eines öffentlich zugänglichen elektronischen Kommunikationsdienstes oder von Betreibern eines öffentlichen Kommunikationsnetzes für die Zwecke der Verhütung von Straftaten verarbeitet oder erzeugt werden;
– die für die justizielle Zusammenarbeit in Strafsachen geltenden Vorschriften über die Überwachung und Aufzeichnung von Telekommunikationsvorgängen;
– die im Rahmen der polizeilichen Zusammenarbeit geltenden Vorschriften über den Informationsaustausch; [1]
– Maßnahmen im Bereich der öffentlichen Sicherheit, der Landesverteidigung und der nationalen Sicherheit (d.h. der Sicherheit des Staates);

[1] Prüfungsvorbehalt von **GESTRICHEN**.

Artikel 2

Begriffsbestimmungen

(1) Im Sinne dieses Rahmenbeschlusses bezeichnet der Ausdruck "Kommunikationsdaten"

a) Verkehrsdaten und Standortdaten nach Artikel 2 der Richtlinie 2002/58/EG;

b) Nutzerdaten, d.h. Daten zu (...) einer natürlichen oder juristischen Person, die einen öffentlich zugänglichen elektronischen Kommunikationsdienst für private oder geschäftliche Zwecke nutzt, ohne diesen Dienst notwendigerweise abonniert zu haben;

c) Teilnehmerdaten, d.h. Daten zu einer (...) natürlichen oder juristischen Person, die einen öffentlich zugänglichen elektronischen Kommunikationsdienst für private oder geschäftliche Zwecke abonniert hat, ohne diesen Dienst notwendigerweise genutzt zu haben.

(2) (...)

Artikel 3

Vorratsspeicherung von Kommunikationsdaten

(1) Jeder Mitgliedstaat trifft die erforderlichen Maßnahmen, um sicherzustellen, dass für die Zwecke der justiziellen Zusammenarbeit in Strafsachen Kommunikationsdaten (...), die von Anbietern eines öffentlich zugänglichen elektronischen Kommunikationsdienstes oder von Betreibern eines öffentlichen Kommunikationsnetzes erzeugt oder verarbeitet werden, gemäß den Bestimmungen dieses Rahmenbeschlusses auf Vorrat gespeichert werden.

(2) Die für die in Artikel 1 genannten Zwecke auf Vorrat zu speichernden Kommunikationsdaten umfassen mindestens folgende Daten:

a) Daten, die zur Rückverfolgung und Identifizierung der Quelle einer Nachricht notwendig sind:

   1. im Telefonfestnetz
      a) die Rufnummer des anrufenden (...) Anschlusses,
      b) die Namen und Anschriften der Nutzer oder Teilnehmer, auf die die Telefonnummern zum Zeitpunkt der Verbindung angemeldet waren,
      c) (...)

2. beim Mobilfunk

a) die Rufnummer des (…) anrufenden Anschlusses,

b) (…)

b) die Namen und Anschriften der Nutzer oder Teilnehmer, auf die die Telefonnummern zum Zeitpunkt der Verbindung angemeldet waren;

3. beim Internetzugang und den Internetdiensten

a) die vom Internetzugangsanbieter einer Verbindung zugewiesene dynamische oder statische Internet-Protokoll-Adresse (IP-Adresse),

b) die Anschluss- oder Benutzerkennung, über die die Verbindung zum Internetzugangsanbieter hergestellt wurde,

c) (…)

d) die Benutzerkennung, z.B. E-Mail Adresse, der Quelle einer Nachricht,

e) die Anschlusskennung oder Rufnummer, die jeder Nachricht im öffentlichen Telefonfestnetz zugewiesen wird,

f) der Name und die Anschrift des Nutzers oder Teilnehmers, dem die IP-Adresse, die Anschlusskennung oder die Benutzerkennung zum Zeitpunkt der Verbindung zugewiesen war;

b) Daten, die zur Ermittlung des (…) Bestimmungsziels einer Nachricht notwendig sind:

1. im Telefonfestnetz

a) die Rufnummer(n) des angerufenen Anschlusses,

b) die Namen und Anschriften der Nutzer oder Teilnehmer, auf die die Telefonnummern zum Zeitpunkt der Verbindung angemeldet waren;

2. beim Mobilfunk

a) die Rufnummer(n) des angerufenen Anschlusses,

b) die Namen und Anschriften der Nutzer oder Teilnehmer, auf die die Telefonnummern zum Zeitpunkt der Verbindung angemeldet waren;

3. beim Internetzugang und den Internetdiensten

a) die Anschluss- oder Benutzerkennung, z.B. E-Mail-Adresse, des Nachrichtenempfängers,

b) der Name und die Anschrift des Nutzers oder Teilnehmers, dem die IP-Adresse, die Anschluss- oder die Benutzerkennung zum Zeitpunkt der Verbindung zugewiesen war;

c) Daten, die zur Ermittlung von Datum, Uhrzeit und Dauer eines Kommunikationsvorgangs notwendig sind (…):

1. im Telefonfestnetz und beim Mobilfunk (…):
a) Datum und Uhrzeit von Beginn und Ende eines Kommunikationsvorgangs;

2. beim Internetzugang und den Internetdiensten:
a) Datum und Uhrzeit der An- und Abmeldung für Internet-Sitzungen auf der Grundlage einer bestimmten Zeitzone;

d) Daten, die zur Identifizierung der Art des Kommunikationsvorgangs notwendig sind:

1. im Telefonfestnetz
a) der in Anspruch genommene Telefondienst, z.B. Sprachübertragung, Konferenzschaltung, Kurznachrichtendienst (SMS), Enhanced Media Service oder Multimedia Service;

2. beim Mobilfunk
a) der in Anspruch genommene Telefondienst, z.B. Sprachübertragung, Konferenzschaltung, Kurznachrichtendienst (SMS), Enhanced Media Service oder Multimedia Service,
b) eine erklärbare oder nicht erklärbare Beendigung des Kommunikationsvorgangs;

3. beim Internetzugang und den Internetdiensten:
a) der in Anspruch genommene Internetdienst, z.B. E-Mail, Chat oder Surfen;

e) Daten, die zur Ermittlung der Endeinrichtung oder der vorgeblichen Endeinrichtung notwendig sind:

1. im Telefonfestnetz
a) die Rufnummern des anrufenden und des angerufenen Anschlusses;

2. beim Mobilfunk
a) die Rufnummern des anrufenden und des angerufenen Anschlusses,
b) die internationale Teilnehmerkennung (IMSI) des anrufenden Anschlusses,
c) die internationale Mobilfunkgerätekennung (IMEI) des anrufenden Anschlusses,
d) die internationale Teilnehmerkennung (IMSI) des angerufenen Anschlusses,
e) die internationale Mobilfunkgerätekennung (IMEI) des angerufenen Anschlusses;

3. beim Internetzugang und den Internetdiensten:

a) die Rufnummer des anrufenden Anschlusses für den Zugang über Wählanschluss,

b) ein asymmetrischer digitaler Teilnehmeranschluss (ADSL) oder ein anderer Endpunkt des Urhebers des Kommunikationsvorgangs,

c) die MAC-Adresse (Media Access Control) oder eine andere Hardware-Kennung des vom Urheber des Kommunikationsvorgangs benutzten Geräts;

f) Daten, die zur Ermittlung des Standorts mobiler Geräte bei Beginn und Ende des Kommunikationsvorgangs notwendig sind:

a) die Standortkennung (Cell-ID) bei Beginn und Ende der Verbindung,

b) das Data-Mapping zwischen den Standortkennungen und ihrem geografischen Standort zum Zeitpunkt der Verbindung.

(3) Die Mitgliedstaaten ergreifen die geeigneten Maßnahmen für die technische Umsetzung von Absatz 1.

Artikel 4 [1]

Fristen für die Vorratsspeicherung von Kommunikationsdaten

(1) Jeder Mitgliedstaat trifft die erforderlichen Maßnahmen, um sicherzustellen, dass die in Artikel 3 genannten Kommunikationsdaten nach ihrer Erzeugung 12 Monate lang auf Vorrat gespeichert werden. Für Teilnehmerdaten läuft diese Frist ab dem Ende des Abonnements.

(2) Abweichend von Absatz 1 kann ein Mitgliedstaat für die Vorratsspeicherung der in Artikel 3 genannten Kommunikationsdaten gemäß den nationalen Kriterien längere Fristen von bis zu 48 Monaten vorsehen, wenn dies eine notwendige, angemessene und verhältnismäßige Maßnahme innerhalb einer demokratischen Gesellschaft darstellt.

(3) Abweichend von Absatz 1 und vorbehaltlich des Absatzes 4 kann ein Mitgliedstaat für die Vorratsspeicherung der in Artikel 3 genannten Kommunikationsdaten (...) kürzere Fristen – von mindestens 6 Monaten [2] – vorsehen, wenn er die Fristen für die Vorratsspeicherung nach Absatz 1 gemäß den nationalen Verfahrens- oder Konsultationsprozessen nicht für annehmbar hält.

[(4) Abweichend von den Absätzen 1 und 3 kann ein Mitgliedstaat für die Vorratsspeicherung von Kommunikationsdaten über Nachrichtendienste und MMS-Dienste unter Nutzung des Telefonfestnetzes oder des Mobilfunks kürzere Fristen – von mindestens 6 Monaten – vorsehen, wenn er die Fristen für die Vorratsspeicherung nach Absatz 1 gemäß den nationalen Verfahrens- oder Konsultationsprozessen nicht für annehmbar hält.]

(5) Abweichend von Absatz 1 kann ein Mitgliedstaat für die Vorratsspeicherung von Kommunikationsdaten ausnahmsweise kürzere Fristen als 6 Monate vorsehen, sofern diese Daten für geschäftliche Zwecke normalerweise weniger als 7 Tage lang aufbewahrt werden, wenn er die Fristen für die Vorratsspeicherung nach Absatz 1 gemäß den nationalen Verfahrens- oder

---

[1] **GESTRICHEN** haben einen Prüfungsvorbehalt zu Artikel 4.

[2] Vorbehalt von **GESTRICHEN**, die keine Mindestfrist wünscht und der Auffassung ist, dass drei Monate in jedem Fall ausreichend sind. Prüfungsvorbehalt von **GESTRICHEN**.

Konsultationsprozessen nicht für annehmbar hält.

(6) Ein Mitgliedstaat, der beschließt, Absatz 2, 3 [4] oder 5 anzuwenden, setzt den Rat und die Kommission von den für die Vorratsspeicherung vorgesehenen Fristen unter Angabe der betreffenden Kommunikationsdaten in Kenntnis. Diese Ausnahmen werden mindestens alle fünf Jahre überprüft.

Artikel 5 [1]

Datensicherheit

Jeder Mitgliedstaat trägt dafür Sorge, dass in Bezug auf die nach diesem Rahmenbeschluss auf Vorrat gespeicherten Kommunikationsdaten mindestens die gemäß der Richtlinie 95/46/EG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr angenommenen Vorschriften, Artikel 4 der Richtlinie 2002/58/EG sowie die nachstehenden Datensicherheitsgrundsätze eingehalten werden:

a) Die auf Vorrat gespeicherten Daten sind von derselben Qualität wie die im Netz vorhandenen Daten;
b) in Bezug auf die Daten werden geeignete technische und organisatorische Maßnahmen getroffen, um die Daten gegen zufällige oder unrechtmäßige Zerstörung, zufälligen Verlust, unberechtigte Änderung, unberechtigte Weitergabe oder unberechtigten Zugang und gegen jede andere Form der unrechtmäßigen Verarbeitung zu schützen;
c) alle Daten werden am Ende der Vorratsspeicherungsfrist vernichtet, mit Ausnahme jener Daten, die abgerufen und gesichert worden sind.

---

[1] **GESTRICHEN** verwies auf ihren Vorschlag in Dok. 6909/05 COPEN 45 TELECOM 14. **GESTRICHEN** schlug mit Unterstützung mehrerer Delegationen (**GESTRICHEN**) folgenden Wortlaut vor:

"Jeder Mitgliedstaat trägt dafür Sorge, dass die nach diesem Rahmenbeschluss auf Vorrat gespeicherten Daten mindestens den folgenden Datensicherheitsgrundsätzen unterliegen und dass die Bestimmungen von Artikel 4 der Richtlinie 2002/58/EG eingehalten werden:

a) (unverändert)
b) (unverändert)
c) die Daten werden nicht an Personen weitergegeben, die nicht rechtmäßig für die Ermittlungen oder die Kontrolle der Rechtmäßigkeit der Ermittlungen zuständig sind;
d) jeder Mitgliedstaat garantiert auf wirksame Weise durch technische und organisatorische Maßnahmen, dass der Zugang zu den auf Vorrat gespeicherten Daten nur berechtigten Personen und nur für einen im Einzelfall vorher festgelegten und begrenzten Zeitraum gewährt wird, nachdem die zuständige Justizbehörde die Rechtmäßigkeit des Zugangs geprüft hat;
e) (ehemaliger Buchstabe c unverändert).

GESTRICHEN schlug vor, Artikel 5 zu streichen und folgenden Erwägungsgrund aufzunehmen:

"(9a) Anbieter eines öffentlich zugänglichen elektronischen Telekommunikationsdienstes oder Betreiber eines öffentlichen Kommunikationsnetzes sind bei der Verarbeitung personenbezogener Daten an nationale, ein hohes Datenschutzniveau bietende Datenschutzbestimmungen gebunden, insbesondere an diejenigen Vorschriften, die nach der Richtlinie 95/46/EG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr und der Richtlinie 2002/58/EG über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation erlassen worden sind. Diese Vorschriften sind einzuhalten, wenn personenbezogene Daten nach Maßgabe dieses Rahmenbeschlusses verarbeitet werden."

Mehrere Delegationen legten einen Prüfungsvorbehalt zu Artikel 5 ein. Einige Delegationen

waren der Meinung, dass diese Bestimmung gestrichen werden sollte.

Artikel 6

Zugang zu auf Vorrat gespeicherten Kommunikationsdaten

Jeder Mitgliedstaat stellt sicher, dass der Zugang zu den nach diesem Rahmenbeschluss auf Vorrat gespeicherten Kommunikationsdaten zu den in Artikel 1 genannten Zwecken mindestens den nachstehenden Vorschriften unterliegt, und bietet Rechtsbehelfe gemäß den Bestimmungen des Kapitels III der Richtlinie 95/46/EG (Rechtsbehelfe, Haftung und Sanktionen):

a) Die Daten werden von den zuständigen Behörden fallbezogen gemäß den nationalen Rechtsvorschriften für festgelegte, eindeutige und rechtmäßige Zwecke abgerufen und nur in einer Weise weiter verarbeitet, die mit diesen Zwecken vereinbar ist;

b) jeder Mitgliedstaat legt im innerstaatlichen Recht das Verfahren und die Bedingungen fest, die für den Abruf von auf Vorrat gespeicherten Daten und für die Sicherung abgerufener Daten einzuhalten sind;

c) die Daten entsprechen den Zwecken, für die sie abgerufen werden, sind für sie von Belang und stehen in angemessenem Verhältnis zu ihnen; die Daten werden nach Recht und Billigkeit verarbeitet;

d) von den zuständigen Behörden abgerufene Daten dürfen in einer Form, die die Identifizierung der betroffenen Personen ermöglicht, nicht länger gespeichert werden, als es für die Zwecke, für die sie erhoben und/oder weiter verarbeitet werden, erforderlich ist;

e) die Vertraulichkeit und Integrität der Daten ist zu gewährleisten;

f) die Daten müssen korrekt sein und es sind alle erforderlichen Maßnahmen zu treffen, damit personenbezogene Daten, die im Hinblick auf die Zwecke, für die sie erhoben und/oder weiter verarbeitet werden, unzutreffend sind, gelöscht oder berichtigt werden.

Artikel 7

Ersuchen um Übermittlung von auf Vorrat gespeicherten Kommunikationsdaten im Rahmen der justiziellen Zusammenarbeit in Strafsachen

Jeder Mitgliedstaat kommt einem Ersuchen eines anderen Mitgliedstaats um Übermittlung von Kommunikationsdaten, die gemäß den Artikeln 3 und 4 auf Vorrat gespeichert wurden, gemäß den für die justizielle Zusammenarbeit in Strafsachen geltenden Rechtsakten nach. [Der ersuchte Mitgliedstaat kann seine Zustimmung zu einem solchen Ersuchen um Kommunikationsdaten mit den Auflagen versehen, die in einem vergleichbaren innerstaatlichen Fall gelten würden.] [1]

[1] Mehrere Delegationen und die Kommission fordern die Streichung dieses Satzes, der ihrer Ansicht nach dazu führen könnte, dass Rechtshilfeersuchen in einem größeren Umfang abgelehnt werden, als es im Rahmen der derzeitigen Rechtsinstrumente möglich ist. Andere Delegationen (**GESTRICHEN**) sind hingegen der Meinung, dass dieser Satz nicht gestrichen werden sollte.

Artikel 8

Umsetzung

(1) Die Mitgliedstaaten treffen die erforderlichen Maßnahmen, um diesem Rahmenbeschluss innerhalb von zwei Jahren nach seinem Inkrafttreten nachzukommen.

(2) Innerhalb derselben Frist teilen die Mitgliedstaaten dem Generalsekretariat des Rates und der Kommission den Wortlaut der Bestimmungen mit, mit denen sie die sich aus diesem Rahmenbeschluss ergebenden Verpflichtungen in ihr innerstaatliches Recht umgesetzt haben. Das Generalsekretariat des Rates übermittelt den Mitgliedstaaten die gemäß diesem Artikel erhaltenen Informationen.

(3) Jeder Mitgliedstaat kann für einen Zeitraum von bis zu vier Jahren ab dem Inkrafttreten dieses Rahmenbeschlusses dessen Anwendung auf die Vorratsspeicherung folgender Kommunikationsdaten verschieben:

a) Daten über ineffektive Kommunikationsverbindungen, d.h. nicht erfolgreich abgehende oder unbeantwortete Anrufe über Telefonfestnetz oder Mobilfunk, und/oder

b) Daten über Internetzugang und Internetdienste.

Jeder Mitgliedstaat, der diesen Absatz anzuwenden beabsichtigt, setzt das Generalsekretariat des Rates hiervon im Wege einer Erklärung bei der Annahme dieses Rahmenbeschlusses in Kenntnis. Diese Erklärung wird im Amtsblatt der Europäischen Union veröffentlicht.

(4) Die Kommission legt dem Rat bis [1. Januar 2008] einen Bericht vor, in dem untersucht wird, inwieweit die Mitgliedstaaten Maßnahmen getroffen haben, um diesem Rahmenbeschluss nachzukommen.

Artikel 9

Inkrafttreten

Dieser Rahmenbeschluss tritt am zwanzigsten Tag nach seiner Veröffentlichung im Amtsblatt der Europäischen Union in Kraft.
