RAT DER EUROPÄISCHEN UNION

Brüssel, den 20. Dezember 2004 (07.01)
(OR. en)

8958/04
ADD 1

CIMORG 36
TELECOM 82

ADDENDUM ZUM ÜBERMITTLUNGSVERMERK

Absender:	die Französische Republik, Irland, das Königreich Schweden und das Vereinigte Königreich
Eingangsdatum:	28. April 2004
Empfänger:	der Generalsekretär/Hohe Vertreter, Herr Javier SOLANA
Betr.:	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

Die Delegationen erhalten anbei einen erläuternden Vermerk zu der im Betreff genannten Initiative.

ERLÄUTERNDER VERMERK

RAHMENBESCHLUSS ÜBER DIE VORRATSSPEICHERUNG VON KOMMUNIKATIONSDATEN

(DOK. 8958/04)

1. EINLEITUNG

Vorratsspeicherung

Als Vorratsspeicherung wird die Speicherung von Kommunikationsdaten bezeichnet, die von den Erbringern von Kommunikationsdienstleistungen bei der Ausübung ihrer Tätigkeit generiert werden. Wie lange die einzelnen Erbringer von Kommunikationsdiensten diese Daten speichern, hängt von zahlreichen Faktoren wie den betrieblichen Erfordernissen, den Möglichkeiten und Kapazitäten der Plattform sowie den einzelstaatlichen Rechtsvorschriften ab. Derzeit gibt es in der Europäischen Union große Unterschiede in Bezug auf die Dauer, für die die Erbringer von Kommunikationsdiensten Kommunikationsdaten speichern, und zwar sowohl zwischen den Mitgliedstaaten als auch innerhalb der Mitgliedstaaten.

Hintergrund

Die Europäische Union, die aus städtisch geprägten Gesellschaften mit verwundbaren Infrastrukturen und durchlässigen Grenzen besteht, wird zunehmend durch grenzüberschreitende kriminelle Tätigkeiten gefährdet. Die Notwendigkeit einer europaweiten Politik im Bereich der Vorratsspeicherung von Daten wurde zunächst als Antwort auf diese Zunahme des internationalen Kriminalität erkannt.

Die Ausarbeitung dieses Rahmenbeschlusses fiel jedoch in eine Zeit, in der die terroristische Bedrohung im Mittelpunkt der Aufmerksamkeit stand. Die am 11. März 2004 in Madrid verübten Bombenattentate machten Europa die schwerwiegende Bedrohung der Mitgliedstaaten durch radikale terroristische Gruppen sehr deutlich. Die zunehmende Bedrohung durch terroristische Attentate verstärkt, nährt und erzeugt das Gefühl, dass eine europaweite Politik betreffend die Vorratsspeicherung von Daten dringend erforderlich ist, und bildet nicht nur die prinzipielle Grundlage dieser Politik. Dieser Rahmenbeschluss stellt daher sowohl auf kriminelle Machenschaften im Allgemeinen als auch auf terroristische Anschläge ab.

Es ist offenkundig, dass sich äußerst versierte internationale kriminelle und terroristische Vereinigungen, die sich der Unterschiede in den gesetzlichen Anforderungen zwischen den Mitgliedstaaten in Bezug auf die Vorschriften über die Vorratsspecherung von Daten bewusst sind, auf die Mitgliedstaaten konzentrieren werden, die den Erbringern von Kommunikationsleistungen einen Netzbetrieb mit geringeren Anforderungen an die Dauer der Vorratsspeicherung von Daten gestatten. Ziel dieses Vorgehens wäre es, in den Genuss der dadurch gebotenen Anonymität zu kommen und die Bemühungen von Fahndern zu erschweren, die versuchen, die bei der Kommunikation hinterlassenen Spuren zu verfolgen, um sie entweder dem Tatort einer Straftat zuordnen oder alle Beteiligten und Mitverschwörer ermitteln zu können. Eine Angleichung der Bestimmungen über die Vorratsspeicherung wird sowohl die Gefahr einer Entstehung solcher "Daten-Freizonen" in der Europäischen Union verringern und – was vielleicht noch wichtiger ist – gewährleisten, dass Beweismittel in Form von Kommunikationsdaten zur Verfügung stehen, die die justizielle Zusammenarbeit der Strafverfolgungsbehörden erleichtern.

Parallel zur Zunahme der Bedrohung durch international operierende Straftäter und Terroristen durchlief die stark wettbewerbsgeprägte Telekommunikationsbranche einen umfassenden technologischen Wandel. Durch diese Entwicklungen stehen die Diensteerbringer unter dem Druck, den Zeitraum, in dem sie ihre Kommunikationsdaten speichern, zu verkürzen. Ein Beispiel für die neuen Technologien, das bereits Auswirkungen auf die Dauer der Vorratsspeicherung von Daten hat, ist die Entwicklung von Technologien, für die in Abhängigkeit von der Inanspruchnahme gezahlt wird. Hierbei handelt es sich um einen der wichtigsten Faktoren für die Verkürzung des Zeitraums, in dem Kommunikationdaten von der Branche gespeichert werden; darüber hinaus kann diese Zahlungsoption grundsätzlich den Umfang der überhaupt verfügbaren Daten verringern.

Diese technologischen Entwicklungen bilden einen weiteren, über den ständig zunehmenden gewerblichen Bedarf hinaus gehenden Faktor, der die Unternehmen zwingt, den Wert und die Effizienz ihrer Systeme kontinuierlich zu beurteilen und zu überprüfen. Dieser wirtschaftliche Druck zur Kostensenkung bedeutet auch, dass früher für gewerbliche Zwecke gespeicherte Daten nun gelöscht werden, weil ihr Wert gesunken ist. Es ist jedoch deutlich, dass dieser Druck zwar besteht und zunimmt, aber in vielen Unternehmen noch keinen "kritischen Wert" erreicht hat; daher lässt sich bislang noch kein dramatischer Abbau der Speicherdauer feststellen, obwohl sie zurückgeht. Dieser Rahmenbeschluss wird drastische Kürzungen verhindern. Im Übrigen deuten auch erste Untersuchungen darauf hin, dass die Einhaltung der Bestimmungen dieses Rahmenbeschlusses voraussichtlich nicht in allen Unternehmen eine längere Speicherung aller Arten von Daten erfordert, obwohl die Erbringer von Kommunikationsdiensten möglicherweise bestimmte Arten von Daten länger speichern müssen.

Daher ist der Erlass von Rechtsvorschriften, die alle Mitgliedstaaten verpflichten, verbindliche Bestimmungen über die Vorratsspeicherung von Daten zu erlassen, von entscheidender Bedeutung dafür, dass die Mitgliedstaaten einen Raum der Freiheit, der Sicherheit und des Rechts schaffen und die Kriminalität einschließlich des Terrorismus erfolgreich bekämpfen können. Dieser Rahmenbeschluss wird eingedenk dieses Ziels und unter Beachtung der Tatsache, dass es sich bei der Erbringung von Kommunikationsdiensten um ein internationales Geschäftsfeld handelt, eine Angleichung der Regelungen der Mitgliedstaaten bewirken, um sicherzustellen, dass dieses wesentliche Ermittlungswerkzeug zur Verfügung steht, wenn Verbrechen begangen oder terroristische Anschläge verübt werden.

Das Ziel dieses Rahmenbeschlusses

Die Erbringer von Kommunikationsdiensten generieren bei der alltäglichen Erbringung dieser Dienste Kommunikationsdaten. Diese Daten werden derzeit aus mehreren Gründen, zu denen die Aufdeckung von Betrugsfällen, die Erstellung von Rechnungen und die Einhaltung von Finanzbestimmungen gehören, gespeichert. Dieser Rahmenbeschluss umfasst Maßnahmen, die die Erbringer von Kommunikationsdiensten verpflichten, die Dauer der Speicherung einiger Arten von Kommunikationsdaten unverändert beizubehalten oder zu verlängern.

Die Unterstützung für die Einführung bindender Regeln für die Speicherung von Kommunikationsdaten hat in den vergangenen Jahren an Kraft und Intensität zugenommen. Ihre Notwendigkeit wird nicht mehr bestritten, und die Bedeutung von Kommunikationsdaten als Ermittlungswerkzeug wird so gut wie einhellig bestätigt und ist in zahlreichen Foren anerkannt worden. Einige der möglicherweise wichtigsten Belege hierfür aus der jüngsten Vergangenheit werden nachstehend aufgeführt.

Der Rat hat am 20. September 2001 Schlussfolgerungen (Dok. SN 3926/6/01) angenommen, in denen er die Bedeutung von Kommunikationsdaten für die Verbrechens- und Terrorismusbekämpfung anerkannt hat. Darüber hinaus wurde die Kommission aufgefordert, Vorschläge zu unterbreiten, die sicherstellen, dass die Strafverfolgungsbehörden die Möglichkeit erhalten, im Zusammenhang mit kriminellen Handlungen zu ermitteln, die unter Anwendung elektronischer Kommunikationssysteme begangen wurden.

Die Bedeutung von Kommunikationsdaten wurde ferner in Artikel 15 der Richtlinie 2002/58/EG über den Schutz der Privatsphäre in der elektronischen Kommunikation gewürdigt. Die Mitgliedstaaten sind gemäß Artikel 15 berechtigt, Rechtsvorschriften zu erlassen, die die Rechte und Pflichten gemäß Artikel 5, Artikel 6, Artikel 8 Absätze 1, 2, 3 und 4 sowie Artikel 9 dieser Richtlinie beschränken, sofern eine solche Beschränkung gemäß Artikel 13 Absatz 1 der Richtlinie 95/46/EG für die nationale Sicherheit, (d. h. die Sicherheit des Staates), die Landesverteidigung, die öffentliche Sicherheit sowie die Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten oder des unzulässigen Gebrauchs von elektronischen Kommunikationssystemen in einer demokratischen Gesellschaft notwendig, angemessen und verhältnismäßig ist.

Der Rat hat auf seiner Tagung am 19. Dezember 2002 Schlussfolgerungen zum Thema Informationstechnologie und Ermittlungsarbeit und Verfolgung im Bereich der organisierten Kriminalität angenommen (Dok. 15691/02). In diesen Schlussfolgerungen brachte er die Auffassung zum Ausdruck, dass die Erhaltung und Weiterentwicklung der Union als Raum der Freiheit, der Sicherheit und des Rechts nach Artikel 2 des Vertrags über die Europäische Union und die Schaffung eines hohen Maßes an Sicherheit in diesem Raum - das allgemeine Ziel des Artikels 29 des Vertrags - voraussetzt, dass strafrechtliche Ermittlungen und die Strafverfolgung mit hinreichender Gründlichkeit und Effizienz durchgeführt werden können, wobei jedoch gemäß Artikel 6 des Vertrags über die Europäische Union die Menschenrechte und Grundfreiheiten zu achten sind.

In diesen Schlussfolgerungen wurde ferner mit Besorgnis festgestellt, dass die technologischen Innovationen im Zuge der laufenden Entwicklung des Internet und anderer elektronischer Kommunikationsdienstleistungen und des zunehmenden e–Banking parallel zu ihrem großen Nutzen für die Gesellschaft Straftätern und insbesondere kriminellen Organisationen die Möglichkeit eröffnen, diese Technologien in stärkerem Maße für ihre Zwecke auszunutzen.

Darüber hinaus wurden in den Schlussfolgerungen alle betroffenen Parteien (Regierungen, Parlamente, Strafverfolgungs- und Justizbehörden, Unternehmen, Datenschutzbehörden und andere interessierte Parteien) aufgefordert, auf nationaler und auf EU-Ebene vorrangig einen offenen und konstruktiven Dialog einzuleiten, um Lösungen für die Frage der Speicherung von Verkehrsdaten zu finden, die der Notwendigkeit eines wirksamen Instrumentariums zur Verhütung, Feststellung, Aufklärung und Verfolgung von Straftaten wie auch dem Schutz der Grundrechte und Grundfreiheiten natürlicher Personen, insbesondere ihrem Recht auf Schutz der Privatsphäre, Datenschutz und Wahrung des Fernmeldegeheimnisses, Rechnung tragen.

Am 25. März 2004 hat der Europäische Rat eine Erklärung zur Terrorismusbekämpfung veröffentlicht, in der auf die Bedeutung von Rechtsvorschriften über die Aufbewahrung von Verkehrsdaten durch Diensteanbieter hingewiesen wurde. Ferner wurde erklärt, dass dieser Vorschlag vorrangig behandelt werden sollte, damit er bis Juni 2005 angenommen werden kann.

Die Rechtsgrundlage des Rahmenbeschlusses

Der Rahmenbeschluss stützt sich auf den Vertrag über die Europäische Union, insbesondere auf Artikel 31 Absatz 1 Buchstabe c und Artikel 34 Absatz 2 Buchstabe b.

Die Sicherungsspeicherung von Daten ist kein Ersatz für die Vorratsspeicherung von Daten

Die europäischen Datenschutzbeauftragten haben sich in ihrer Stellungnahme 5/2002 für die Sicherungsspeicherung von Daten anstelle der Vorratsspeicherung ausgesprochen. Als Sicherungsspeicherung von Daten wird im Unterschied zu der umfassenden Speicherung von Daten, wie sie im Rahmen einer Regelung über die Vorratsspeicherung vorgesehen ist, die Speicherung von Daten bezeichnet, die sich auf bestimmte Personen beziehen. Die Sicherheits-, Geheimdienst- und Strafverfolgungsstellen erkennen an, dass die von den Datenschutzbeauftragten vorgeschlagene Sicherungsspeicherung von Daten ein sehr nützliches Werkzeug für die Untersuchung der Handlungen von Verdächtigen ist. Sie kann jedoch keinen Beitrag zur Überprüfung von Personen leisten, die noch nicht verdächtigt werden, einer kriminellen oder terroristischen Organisation anzugehören.

Die Sicherungsspeicherung von Daten kann daher den Bedarf der Sicherheits-, Geheimdienst- und Strafverfolgungsstellen im Hinblick auf die Bekämpfung heutiger Straftäter, zu denen auch Terroristen gehören, nicht decken.

Darüber hinaus verhindert eine Regelung für die Vorratsspeicherung von Daten den unverhältnismäßigen Rückgriff auf die Sicherungsspeicherung. Hierbei handelt es sich um einen häufig nicht verstandenen zentralen Aspekt der Vorratsspeicherung: Die Vorratsspeicherung basiert auf dem Grundsatz, dass prinzipiell keine Zugriffe auf die gespeicherten Daten erfolgen. Die Strafverfolgungsbehörden können lediglich im Einzelfall beschließen, auf einen sehr begrenzten Teil dieser Daten zuzugreifen. Ohne eine solche Regelung entsteht angesichts der Bedrohung durch neue Formen der Kriminalität einschließlich des Terrorismus ein wachsender Bedarf für eine umfassendere Sicherheitsspeicherung von Daten, bei der alle Informationen, die von einer bestimmten Person ausgehen oder ihr übermittelt werden, nicht nur gespeichert werden, sondern auch von der Behörde genutzt werden können, die die Sicherungsspeicherung angeordnet hat.

2. ARTIKEL 1 - GELTUNGSBEREICH UND ZIEL

Das Ziel des Rahmenbeschlusses ist zu gewährleisten, dass die Daten, die bei der Herstellung einer Kommunikationsverbindung oder dem Eingang von Kommunikationen generiert werden, von den Erbringern der Kommunikationsdienstleistung für einen bestimmten Zeitraum gespeichert werden. Dies soll sowohl die anschließende Untersuchung der Kommunikationsdaten ermöglichen als auch die justizielle Zusammenarbeit erleichtern, sofern es einen legitimen Anlass hierfür im Sinn der Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten, einschließlich Terrorismus, gibt.

In diesem Artikel wird festgelegt, was in den Geltungsbereich dieses Rahmenbeschlusses fallen soll; darüber hinaus wird festgestellt, was nicht in seinen Geltungsbereich fällt. Dieser Rahmenbeschluss gilt nicht für die Überwachung des Inhalts von Kommunikationen. Mit anderen Worten: Der Rahmenbeschluss soll nicht abdecken, was in einer Kommunikation tatsächlich gesprochen oder geschrieben wird.

Die Zwecke, für die eine Speicherung von Kommunikationsdaten gemäß dem Rahmenbeschluss zulässig ist, wurden mit Artikel 15 der Richtlinie 2002/58/EG festgelegt. Wie bereits erwähnt, gehören hierzu die Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten.

Das Ziel der Verhütung von Straftaten ist möglicherweise das einzige Ziel, das nicht unmittelbar einsichtig ist und für eine gewisse Verwirrung sorgen kann. Der Ausdruck "Verhütung von Straftaten" bezieht sich im Rahmenbeschluss ausschließlich auf Fälle, in denen ein begründeter Verdacht auf die Planung einer Straftat vorliegt. Die Verdächtigen müssen mit anderen Worten Grund zur Befürchtung gegeben haben, dass eine Straftat begangen wird, so dass sie in der Folge Gegenstand einer Untersuchung der Strafverfolgungsbehörden werden, die die Vereitelung der Pläne bezweckt. Der im Rahmenbeschluss verwendete Ausdruck "Verhütung von Straftaten" unterliegt mit Blick auf die Arten von Straftaten, die in den Geltungsbereich des Rahmenbeschlusses fallen, keiner Einschränkung.

Im Rahmenbeschluss wird jedoch der Tatsache Rechnung getragen, dass in der Europäischen Union mit Blick auf die "Verhütung von Straftaten" als Ziel der Vorratsspeicherung von Daten unterschiedliche rechtliche Standpunkte vertreten werden. Im Rahmenbeschluss soll diesen Unterschieden dadurch Rechnung getragen werden, dass anerkannt wird, dass es für einige Mitgliedstaaten nicht zweckdienlich sein wird, den Grundsatz der Vorratsspeicherung von Daten zum Zweck der Verhütung von Straftaten anzunehmen, unter anderem deshalb, weil die Verhütung von Straftaten nicht in den Zuständigkeitsbereich der Behörden fällt, die sich mit besonderen Ermittlungstechniken beschäftigen, zu denen die Nutzung von Kommunikationsdaten gehört. Daher wurde in den Rahmenbeschluss eine Ausnahmeregelung eingefügt, die es den Mitgliedstaaten ermöglicht, die Verhütung von Straftaten als Zweck der Vorratsspeicherung von Daten aus ihren einzelstaatlichen Rechtsbestimmungen auszuklammern.

3. ARTIKEL 2 - DATENBEZOGENE BEGRIFFSBESTIMMUNGEN

Die derzeit von der Kommunikationsbranche gespeicherten Daten decken einen umfassenderen Bereich von Daten als den ab, den sie zunächst für den Betrieb ihrer Netze und die Erstellung von Rechnungen benötigen. Diese Informationen werden in Artikel 2 des Rahmenbeschlusses beschrieben und betreffen die Ermittlung des Urhebers, des Zeitpunkts, des Orts und der Art und Weise eines Vorgangs für jedes Netz beziehungsweise jeden Dienst. Einzelne Unternehmen können einen spezifischen Bedarf für die Vorratsspeicherung bestimmter Daten haben, und die Anforderungen in Bezug auf die Untersuchung krimineller und terroristischer Tätigkeiten besagen, dass die nachstehend genannten Daten für die in Artikel 1 genannten Zwecke zu speichern sind. Im Sinne des Rahmenbeschlusses bezeichnet der Ausdruck Daten somit folgende Arten von Daten: Telefonnummern, Internetadressen, Rechnungsadressen des Kunden und die Telefonnummern/Kommunikationsvorgänge, die unter Nutzung eines bestimmten Telefons/Computers angerufen bzw. stattgefunden haben.

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

4. ARTIKEL 3 – VORRATSSPEICHERUNG VON DATEN

In diesem Artikel wird festgestellt, dass alle Mitgliedstaaten diese Maßnahmen annehmen müssen, um die internationale justizielle Zusammenarbeit zu erleichtern, die für die Bekämpfung von Straftaten einschließlich des Terrorismus in den Fällen erforderlich ist, in denen strafbare Handlungen oder Belege für Kriminalität mehr als einen Staat betreffen.

5. ARTIKEL 4 – FRISTEN FÜR DIE VORRATSSPEICHERUNG VON DATEN

Dieser Artikel bildet die Grundlage für die Einführung von Rechtsvorschriften betreffend die Vorratsspeicherung von Kommunikationsdaten für mindestens 12 und höchstens 36 Monate in allen Mitgliedstaaten. Eine Mindestfrist für die Vorratsspeicherung ist als gemeinsame Regelung für die Verbesserung der justiziellen Zusammenarbeit in Strafsachen erforderlich.

Der Artikel enthält ferner eine Ausnahmeregelung, der es einzelnen Mitgliedstaaten ermöglicht, diese Dauer bei Vorliegen bestimmter Umstände unter Bezugnahme auf besondere Technologien mit Ausnahme der Telefonie abzuwandeln. Zu diesen Technologien gehören beispielsweise Textmitteilungen und E-Mail. Die Dauer der Vorratsspeicherung bei diesen Technologien kann von den Mitgliedstaaten, die die Ausnahmeregelung anwenden, sowohl verlängert als auch verkürzt werden.

6. ARTIKEL 5 – ZUGRIFF AUF DATEN

Dieser Artikel soll den Rückgriff auf die Instrumente der justiziellen Zusammenarbeit, an der die Mitgliedstaaten bereits beteiligt sind, ermöglichen, die auf unter den Rahmenbeschluss fallende Fragen anwendbar sind. Dies betrifft insbesondere das Übereinkommen über die Rechtshilfe in Strafsachen zwischen den Mitgliedstaaten der Europäischen Union, das am 29. Mai 2000 unterzeichnet wurde (der Europäische Rat hat die Mitgliedstaaten in seiner Erklärung vom 26. März 2004 aufgerufen, die Ratifikation vor Ende des Jahres 2004 abzuschließen).

7. ARTIKEL 6 – DATENSCHUTZ

Dieser Artikel stellt einen sehr wichtigen Bestandteil des Rahmenbeschlusses dar, mit dem nicht nur die Wirksamkeit unserer einzelstaatlichen Systeme der Verbrechensbekämpfung verbessert, sondern auch ihre Vereinbarkeit mit den Prinzipien der Privatsphäre und des Datenschutzes gewährleistet werden soll.

Der Artikel lehnt sich an die Datenschutzgrundsätze in anderen Instrumenten der EU und internationalen Instrumenten an, insbesondere an die der Richtlinie 95/46/EG. Er gewährleistet, dass der Notwendigkeit und Verhältnismäßigkeit des angestrebten Abrufs von Daten sowie dem Erfordernis Rechnung getragen wird, Beschlüsse über den Zugriff auf Kommunikationsdaten von Fall zu Fall und im Einklang mit den Rechtsvorschriften des jeweiligen Mitgliedstaats zu fassen.

8. ARTIKEL 7 – DATENSICHERHEIT

Dieser Artikel bezieht sich auf die Integrität der auf Vorrat gespeicherten Kommunikationsdaten und die Möglichkeit, ihre dauerhafte Integrität zu gewährleisten. Es ist von entscheidender Bedeutung, dass die Kommunikationsdaten während der gesamten Dauer der Vorratsspeicherung im Netz des Diensteerbringers in unveränderter Qualität gespeichert werden. Ferner ist in diesem Artikel vorgesehen, dass der Zugriff auf diese Daten in den einzelstaatlichen Rechtsvorschriften des betreffenden Mitgliedstaats eindeutig geregelt wird.

9. ARTIKEL 8 – UMSETZUNG

In diesem Artikel wird klargestellt, dass es während des Umsetzungsprozesses darauf ankommt, dass die einzelnen Mitgliedstaaten mit den Erbringern von Kommunikationsdiensten in ihrem Hoheitsgebiet in einen Dialog über die Bestimmungen des Rahmenbeschlusses eintreten.