Bundesrat **Drucksache 675/02**
05.08.02

EU - In - K - R - Wi

Unterrichtung
durch die Bundesregierung

Entwurf für Schlussfolgerungen des Rates über IT-bezogene Maßnahmen im Hinblick auf die Ermittlung und Verfolgung organisierter Kriminalität

Ratsdok. 10358/02

Vertrieb: Bundesanzeiger Verlagsgesellschaft mbH, Postfach 1320, 53003 Bonn
Telefon: 0228/3820840, Telefax: 0228/3820844
ISSN 0720-2946

Übermittelt vom Bundesministerium der Finanzen am 5. August 2002 gemäß § 2 des Gesetzes über die Zusammenarbeit von Bund und Ländern in Angelegenheiten der Europäischen Union (BGBl. I 1993 S. 313 ff.).

Auf Verlangen des Freistaates Bayern gemäß § 45 a (1) GO BR erscheint die Vorlage als Drucksache des Bundesrates.

Drucksache 675/02

10358/02

Entwurf für Schlussfolgerungen des Rates über IT-bezogene Maßnahmen im Hinblick auf die Ermittlung und Verfolgung organisierter Kriminalität

Der Rat der Europäischen Union

1. BETONT, dass ein hohes Maß an Sicherheit in einem Raum der Freiheit, der Sicherheit und des Rechts voraussetzt, dass strafrechtliche Ermittlungen und die Strafverfolgung mit hinreichender Gründlichkeit und Effizienz durchgeführt werden können;

2. STELLT FEST, dass die beträchtliche Zunahme der Telekommunikationsmöglichkeiten dazu geführt hat, dass Telekommunikationsdaten heutzutage ein besonders wichtiges und hilfreiches Mittel bei der Ermittlung und Verfolgung krimineller Organisationen darstellen;

3. VERTRITT DIE AUFFASSUNG, dass der allgemeine Zugang aller Einwohner der Europäischen Union zu einer umfassenden Nutzung der Möglichkeiten, die durch die fortlaufende Entwicklung der Informationstechnologie geboten werden, eine wesentliche Komponente der wirtschaftlichen und sozialen Entwicklung in der ganzen Union ausmacht und dass dieser Zugang nur den Beschränkungen und Restriktionen unterworfen werden sollte, die im Hinblick auf die nationale Sicherheit, die Grundrechte der Bürger, die Aufklärung schwerer Straftaten oder andere gewichtige Erwägungen im Zusammenhang mit der regionalen und globalen Entwicklung erforderlich sind;

4. STELLT mit Besorgnis FEST, 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 kriminellen Organisationen in zunehmendem Maße die Möglichkeit eröffnen, diese Technologien zu missbrauchen;

5. ERINNERT daran, dass das Fernmeldegeheimnis nur insoweit beschränkt werden darf, als dies zum Schutz der nationalen Interessen oder der nationalen Sicherheit oder zum Zwecke der Aufklärung schwerer Verbrechen erforderlich ist;

6. WEIST DARAUF HIN, dass in den politischen Leitlinien des vom Rat am 28. April 1997 angenommenen Aktionsplans zur Bekämpfung der organisierten Kriminalität ausdrücklich festgestellt wird, dass es erforderlich ist, den Weg für eine Politik zu ebnen, bei der sichergestellt ist, dass die Strafverfolgungs- und Justizbehörden die Möglichkeit haben, die missbräuchliche Verwendung dieser neuen Technologien zu verhindern;

7. VERWEIST auf die Schlussfolgerungen des Rates vom 20. September 2001, in denen betont wird, dass dafür Sorge zu tragen ist, dass die Strafverfolgungsbehörden die Möglichkeit erhalten, im Zusammenhang mit kriminellen Handlungen zu ermitteln, die unter Anwendung elektronischer Kommunikationssysteme begangen wurden, dabei jedoch darauf zu achten ist, dass ein Gleichgewicht zwischen dem Schutz personenbezogener Daten und der Notwendigkeit des Zugangs der Strafverfolgungsbehörden zu Daten für strafrechtliche Ermittlungszwecke gewährleistet wird;

8. BEKRÄFTIGT die Verpflichtung, bei der Durchführung von Überwachungsmaßnahmen im Telekommunikationsverkehr das im einzelstaatlichen Recht der Mitgliedstaaten verankerte Recht auf Privatsphäre zu achten, und verweist in diesem Zusammenhang auf die vom Europäischen Parlament und vom Rat am 15. Dezember 1997 erlassene Richtlinie 97/66/EG über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation;

9. FORDERT DAZU AUF, schon in nächster Zukunft bindende Regeln für die Angleichung der Vorschriften der Mitgliedstaaten über die Pflicht der Telekommunikationsbetreiber, Telekommunikationsdaten aufzubewahren, festzulegen, damit sichergestellt ist, dass diese Daten verfügbar sind, wenn diese für strafrechtliche Ermittlungen von Bedeutung sind;

10. IST in diesem Zusammenhang DER ANSICHT, dass bei der Festlegung solcher bindenden Regeln die Anforderungen betreffend den Schutz der Privatsphäre und die Verarbeitung personenbezogener Daten zu berücksichtigen sind, die sich aus der Europäischen Menschenrechtskonvention vom 4. November 1950, aus dem Übereinkommen des Europarates vom 28. Januar 1981 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten und aus der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr ergeben;

11. EMPFIEHLT, die erforderlichen Mechanismen zur Überwachung der Entwicklungen im Bereich der Informationstechnologie einzuführen, damit möglichst bald Vorschläge für Maßnahmen und Initiativen vorgelegt werden können, mit denen sichergestellt wird, dass die Strafverfolgungsbehörden unmittelbar und effizient auf die neuen Herausforderungen reagieren können, welche die künftige Entwicklung der Möglichkeiten der Informationstechnologie mit sich bringt;

12. EMPFIEHLT, dass die Mitgliedstaaten so weit wie möglich die Entwicklung im Bereich der Kommunikations- und Informationstechnologie verfolgen und ständig sicherstellen, dass die Angehörigen der Strafverfolgungsbehörden eine Weiterbildung in diesem Bereich erhalten;

13. FORDERT DAZU AUF, dass die Mitgliedstaaten verstärkt Anstrengungen unternehmen, um sicherzustellen, dass Beschlüsse über die Überwachung des Telekommunikationsverkehrs und den Zugang zu Telekommunikationsdaten so rasch wie möglich getroffen werden, insbesondere bei mobilem Telekommunikationsverkehr, bei dem die miteinander kommunizierenden Parteien ohne Vorankündigung das Land wechseln können, wodurch sich das Erfordernis einer engen und raschen Zusammenarbeit zwischen den Mitgliedstaaten ergibt;

14. EMPFIEHLT, dass die Mitgliedstaaten und die Union fortlaufend nach möglichen Lösungen für die Probleme suchen, die sich für die Strafverfolgungsbehörden durch die zunehmende Anwendung von Verschlüsselungsmöglichkeiten ergeben, so dass sowohl dem legitimen Interesse der Bürger an der Vertraulichkeit ihrer Kommunikation sowie den Möglichkeiten der Strafverfolgungsbehörden, im Falle organisierter Kriminalität effiziente Ermittlungs- und Verfolgungsmaßnahmen zu ergreifen, gebührend Rechnung getragen wird.



10405/02

Entwurf von Schlussfolgerungen des Rates zur Informationstechnologie und zur Ermittlungsarbeit und Verfolgung im Bereich der organisierten Kriminalität

EINLEITUNG

Die organisierte Kriminalität stellt eine ernsthafte Bedrohung der Sicherheit und der Freiheit der Bürger der Europäischen Union dar. Die neuen Technologien und die Produkte in diesem Bereich werden in zunehmendem Maße zu wirkungsvollen Werkzeugen in den Händen von kriminellen Vereinigungen. Die durch die neuen Technologien eröffneten Möglichkeiten machen es leicht, das Betätigungsfeld für illegale Aktivitäten zu erweitern. In Anbetracht dessen legt die dänische Delegation der Multidisziplinären Gruppe "Organisierte Kriminalität" den in Dokument 10358 CRIMORG 49 MI 119 wiedergegebenen Entwurf für Schlussfolgerungen vor, deren Zweck es in erster Linie ist, die Aufmerksamkeit der Mitgliedstaaten und der Institutionen der Europäischen Union auf eine Reihe besonders wichtiger Themen zu lenken, die mit der ständigen Weiterentwicklung der modernen Informationstechnologien und den damit verbundenen Problemen und Möglichkeiten zusammenhängen.

Die dänische Initiative steht im Einklang mit dem am 28. April 1997 vom Rat angenommenen Aktionsplan zur Bekämpfung der organisierten Kriminalität, in dem hervorgehoben wird, dass den Strafverfolgungs- und Justizbehörden die Möglichkeit gegeben werden muss, den Missbrauch neuer Technologien zu verhindern und zu bekämpfen, und dass in diesem Zusammenhang sowohl illegalen Praktiken als auch illegalen Inhalten besondere Aufmerksamkeit geschenkt werden sollte.

Konkret zielt die dänische Initiative auf das Speichern von Telekommunikationsverkehrsdaten, auf die Einführung von Mechanismen für die Überwachung der fortlaufenden Entwicklung innerhalb der modernen Informationstechnologien und für die Konzipierung angemessener Maßnahmen als Reaktion auf diese Entwicklungen, auf die Effizienz einzelstaatlicher Verfahren zum Erwirken von Beschlüssen der Justizbehörden für das Abhören und Zurückverfolgen von Telekommunikationsvorgängen und schließlich auf die Herausforderungen der Verschlüsselung ab.

Abgesehen von spezifischen Fragen, die geklärt werden müssen, um die Effizienz der Strafverfolgungsmaßnahmen zu gewährleisten, muss auch dem Grundsatz der Verhältnismäßigkeit Rechnung getragen werden, wenn es um die Durchführung neuer Maßnahmen in diesem Bereich geht. In dem Aktionsplan von 1997 sind die Ziele der europäischen Maßnahmen in diesem Bereich wie folgt dargestellt: "Unter Vermeidung unnötiger Beschränkungen sollten die Strafverfolgungs- und Justizbehörden in Ergänzung der spezifischen Verantwortlichkeiten der Technologie- und Diensteanbieter über Mittel zur Verhinderung und Bekämpfung des missbräuchlichen Einsatzes dieser neuen Technologien verfügen. Die Aufmerksamkeit sollte sowohl illegalen Praktiken (wie der Verwendung dieser Technologien durch kriminelle Vereinigungen zur Erleichterung ihrer Aktivitäten) als auch illegalen Inhalten (wie Kinderpornografie oder Verbreitung von Anleitungen für die Herstellung synthetischer Drogen) gelten."

Die Initiative dürfte damit auch den Intentionen der am 20. September 2001 angenommenen Schlussfolgerungen des Rates entsprechen, in denen der Rat die Europäische Kommission ersucht, Vorschläge zu unterbreiten, mit denen dafür Sorge getragen wird, dass die Strafverfolgungsbehörden die Möglichkeit erhalten, im Zusammenhang mit kriminellen Handlungen zu ermitteln, die unter Anwendung elektronischer Kommunikationssysteme begangen wurden, und Maßnahmen gegen die Urheber zu ergreifen. In diesem Rahmen wird der Rat besonders darauf achten, dass ein Gleichgewicht zwischen dem Schutz personenbezogener Daten und der Notwendigkeit des Zugangs der Strafverfolgungsbehörden zu Daten für strafrechtliche Ermittlungszwecke gewährleistet wird.