Brüssel/Berlin, 21. Februar 2006

EU-Justizminister beschließen Richtlinie zur Vorratsdatenspeicherung

Der Rat der europäischen Justizminister hat heute in Brüssel die Richtlinie des Europäischen Parlaments und des Rates über die so genannte Vorratsdatenspeicherung beschlossen.

„Die Richtlinie ist ein gutes Beispiel für einen sachgerechten Interessenausgleich zwischen den Freiheitsrechten der Bürgerinnen und Bürger und dem Interesse an einer effektiven Strafverfolgung. Bei der Aufklärung erheblicher Straftaten ist es für die Strafverfolgungsbehörden außerordentlich wichtig auf Daten zugreifen zu können, die bei Telefon- und Internetverbindungen entstehen und von Telekommunikationsunternehmen gespeichert werden. Aus diesen Daten können wichtige Hinweise gewonnen werden, z. B. wer wann mit wem Verbindung aufgenommen hat. Deutschland hat in intensiven Verhandlungen durchgesetzt, dass die Speicherpflicht im Interesse der Freiheitsrechte von Bürgerinnen und Bürger auf ein Mindestmaß beschränkt wird. Das gilt nicht nur für die Datenarten, die gespeichert werden müssen, sondern auch für die Speicherdauer, die jetzt mindestens sechs Monate beträgt. Andere Mitgliedstaaten hatten vehement für eine Mindestspeicherfrist von einem Jahr plädiert. In Rede stand auch die Speicherpflicht von Standortdaten während und am Ende einer Mobilfunkverbindung und Daten bei erfolglosen Anrufversuchen. Beides halte ich für unverhältnismäßig und bin daher sehr zufrieden, dass wir die deutsche Position in Brüssel durchsetzen konnten“, sagte Bundesjustizministerin Brigitte Zypries.

Die europäischen Justizministerinnen und Justizminister hatten sich bereits am 2. Dezember 2005 auf die Inhalte der Richtlinie verständigt, verschiedene Staaten hatten ihre Zustimmung aber unter Parlamentsvorbehalt gestellt. Auch Bundesjustizministerin Brigitte Zypries legte Wert darauf, vor einer endgültigen Zustimmung Deutschlands zunächst den Deutschen Bundestag zu befassen. Auf Antrag der Koalitionsfraktionen hat der Deutsche Bundestag am 16. Februar 2006 eine Entschließung (BT-Drs. 16/690) verabschiedet und den Inhalt der Richtlinie begrüßt.

Der Inhalt der Richtlinie im Wesentlichen:

1. Die Mitgliedstaaten verpflichten sich, den Telekommunikationsdiensteanbietern eine Speicherungsfrist von mindestens sechs Monaten für im Einzelnen aufgeführte Telekommunikationsbestands- und –verkehrsdaten aufzuerlegen. Den Mitgliedstaaten steht es frei, diese Frist im nationalen Recht bis auf 24 Monate auszudehnen. Bestandsdaten sind beispielsweise Name und Anschrift eines Anschlussinhabers, Verkehrsdaten sind diejenigen, die beim Zustandekommen der Verbindung anfallen (z.B. die angerufene Nummer oder die Uhrzeit des Telefonats).

2. Zweck der Speicherung ist die Ermittlung, Aufdeckung und Verfolgung schwerer Straftaten, zu denen auch alle mittels Telekommunikation begangene Straftaten gehören. Den Zugang der Strafverfolgungsbehörden zu diesen Daten müssen die Mitgliedstaaten unter Beachtung der Verhältnismäßigkeit, des Rechts der europäischen Union und des Völkerrechts, insbesondere der Europäischen Menschenrechtskonvention regeln. Wie bislang schon wird auch künftig der Zugang zu solchen Daten grundsätzlich nur aufgrund eines richterlichen Beschlusses zulässig sein.

3. Um die Kosten für die Speicherung möglichst niedrig zu halten, müssen Verkehrsdaten von erfolglosen Anrufversuchen nur dann gespeichert werden, wenn die Unternehmen diese Daten ohnehin speichern. Aus demselben Grund müssen Standortdaten im Mobilfunk nur für den Beginn, nicht aber auch für das Ende der Mobilfunkverbindung gespeichert werden. So wird zudem verhindert, dass nachträglich engmaschige Bewegungsprofile der Mobilfunknutzer erstellt werden können.

4. Im Bereich des Internets sind neben den Einwahldaten (IP-Adresse und Zeitpunkt) die Verkehrsdaten zu E-Mails und Internettelefonie zu speichern.

5. Daten, die Aufschluss über den Inhalt einer Kommunikation (z.B. Email oder Telefongespräch oder Seiten, die ein Nutzer aufgerufen hat) geben, dürfen nach der Richtlinie nicht gespeichert werden.

6. Die Richtlinie enthält Vorgaben für Regelungen zum Datenschutz und zur Datensicherheit, die mit Sanktionen bewehrt werden müssen. Die Sanktionen sollen insbesondere einen unbefugten Zugriff oder Umgang mit den Daten verhindern und die Einhaltung der Datenschutzbestimmungen sichern.