2398/AB XXIII. GP

Eingelangt am 25.01.2008
Dieser Text wurde elektronisch übermittelt. Abweichungen vom Original sind möglich.

BM für Justiz

Anfragebeantwortung

DIE BUNDESMINISTERIN
FÜR JUSTIZ

BMJ-Pr7000/0127-Pr 1/2007

An die

Frau Präsidentin des Nationalrates

W i e n

zur Zahl 2589/J-NR/2007

Die Abgeordneten zum Nationalrat Mag. Johann Maier und GenossInnen haben an mich eine schriftliche Anfrage betreffend „Cybercrime-Konvention: Weltweiter Lagerverkauf der TK-Vorratsdaten?“ gerichtet.

Ich beantworte diese Anfrage wie folgt:

Zu 1:
Die in der Anfrage zitierte Darstellung des Arbeitskreises „Vorratsdatenspeicherung“ ist etwas missverständlich. Art. 15 des erwähnten Übereinkommens (ETS Nr. 185) stellt – als zentrale verfahrensrechtliche Bestimmung – die Anwendung der vorgesehenen prozessualen Maßnahmen unter Bedingungen und Garantien. Ganz allgemein steht daher die Umsetzung des Übereinkommens unter dem Vorbehalt der Einhaltung jener Bedingungen und Garantien, die zum Schutze der Grundrechte

Dieser Text wurde elektronisch übermittelt. Abweichungen vom Original sind möglich.

nach innerstaatlichem Recht vorgesehen sind. Die Vertragsparteien sind auch verantwortlich, dass die Verpflichtungen nach der Menschenrechtskonvention 1950 (hier insbesondere Artikel 8 EMRK) und dem Internationalen Pakt der UNO über bürgerliche und politische Rechte von 1966 sowie nach anderen völkerrechtlichen Verpflichtungen eingehalten werden. In diesem Zusammenhang werden insbesondere eine gerichtliche Kontrolle sowie aus dem Verhältnismäßgikeitsgrundsatz ableitbare Verfahrensgarantien, wie Begründung des Eingriffs und Begrenzung des Umfangs und der Dauer des Eingriffs hervorgehoben.

Die einzelnen prozessualen Befugnisse dürfen gemäß Art. 14 nur für Zwecke spezifischer strafrechtlicher Ermittlungen oder Verfahren in Bezug auf die nach Art. 2 bis 11 des Übereinkommens aufgelisteten Straftaten, sowie andere mittels Computersystem begangener Straftaten und die Erhebung von Beweismaterial in elektronischer Form umgesetzt werden. Die Erhebung von Verkehrsdaten in Echtzeit (Art. 20 = Auskunft über Daten einer Nachrichtenübermittlung, s. §§ 134 Z 2 und 135 Abs. 2 StPO nF) kann mittels Vorbehalt auf gewisse Straftaten eingeschränkt werden, doch darf diese Maßnahme nicht enger gefasst sein als die Maßnahme der Erhebung der Inhaltsdaten in Echtzeit (Art 21 = Überwachung von Nachrichten gemäß §§ 134 Z 3 und 135 Abs. 3 StPO nF).

Die Bestimmungen der §§ 134 ff. StPO idF BGBl. I Nr. 19/2004 und BGBl. I Nr. 93/2007 über die Auskunft über Daten einer Nachrichtenübermittlung und die Überwachung von Nachrichten entsprechen voll und ganz den vorgesehenen Garantien (richterliche Bewilligung, Befristung; Bindung an den Verhältnismäßigkeitsgrundsatz; Regelung von Verwertungsverboten, Schutz von Berufsgeheimnissen sowie Löschungsverpflichtungen).

Zu 2:

Das Cybercrime-Übereinkommen wurde bisher von 21 Staaten ratifiziert; eine Ratifikation durch Österreich ist bisher nicht erfolgt. Aber auch nach erfolgter Ratifikation des Übereinkommens durch Österreich kommt die Übermittlung nationaler Kommunikationsdaten grundsätzlich nur über entsprechendes Rechtshilfeersuchen in Zusammenhang mit einem im ersuchenden Staat anhängigen gerichtlichen Strafverfahren in Betracht, dessen Vollstreckung sich nach nationalem Recht richtet, wobei die nach nationalem Recht oder nach den anwendbaren Rechtshilfeverträgen vorgesehenen Ablehnungsgründe bestehen.

Dieser Text wurde elektronisch übermittelt. Abweichungen vom Original sind möglich.

Ein unmittelbarer Zugriff eines anderen Vertragsstaats auf österreichische Kommunikationsdaten ist nach Art. 32 des Übereinkommens nur im Fall öffentlich zugänglicher gespeicherter Computerdaten oder mit Zustimmung des Betroffenen vorgesehen.

Zu 3:

Zu den Grundsätzen der Rechtshilfe sowie zum Datenzugriff nach Artikel 32 der Cyber Crime Konvention darf zunächst auf die Beantwortung zu Frage 2 verwiesen werden.

Artikel 23 der Cyber Crime Konvention, der die allgemeinen Grundsätze der internationalen Zusammenarbeit festlegt, bezieht sich auf “Straftaten in Zusammenhang mit Computersystemen und –daten” sowie auf die „Erhebung von Beweismaterial in elektronischer Form für eine Straftat“. “Straftaten in Zusammenhang mit Computersystemen und –daten” sind die in Artikel 14 Abs. 2 lit. a und b genannten Straftaten, das sind einerseits (lit. a) die nach den Artikeln 2 bis 11 umschriebenen Straftaten (Artikel 2 – Rechtswidriger Zugang, Artikel 3 – Rechtswidriges Abfangen, Artikel 4 – Eingriff in Daten, Artikel 5 – Eingriff in ein System, Artikel 6 – Missbrauch von Vorrichtungen, Artikel 7 – Computerbezogene Fälschung, Artikel 8 – Computerbezogener Betrug, Artikel 9 – Straftaten mit Bezug zu Kinderpornographie, Artikel 10 – Straftaten in Zusammenhang mit Verletzungen des Urheberrechts und verwandter Schutzrechte, Artikel 11 – Versuch und Beihilfe oder Anstiftung) und andererseits (lit. b) andere mittels eines Computersystems begangene Straftaten.

Das bedeutet nach Paragraph 243 des erläuternden Berichts zur Cyber Crime Kovnention zusammenfassend, dass die Regeln nach Kapitel III der Konvention (Internationale Zusammenarbeit) dann zur Anwendung gelangen können, wenn eine Straftat mittels eines Computersystems begangen wurde oder wenn bei einer „gewöhnlichen“, dh. ohne Verwendung eines Computersystems begangenen Tat (der erläuternde Bericht nennt hier als Beispiel Mord) Beweismaterial in elektronischer Form eine Rolle spielt.

Die Artikel 24 (Auslieferung), 33 (Rechtshilfe bei der Erhebung von Verkehrsdaten in Echtzeit) und 34 (Rechtshilfe bei der Erhebung von Inhaltsdaten in Echtzeit) erlauben den Mitgliedstaaten jedoch einen abweichenden Anwendungsbereich.

Im nationalen Recht darf die Auskunft über Daten einer Nachrichtenübermittlung (§ 135 Abs. 2 StPO nF) – abgesehen von den Fällen der Zustimmung des Inhabers

Dieser Text wurde elektronisch übermittelt. Abweichungen vom Original sind möglich.

der technischen Einrichtung – nur angeordnet werden, wenn zu erwarten ist, dass dadurch die Aufklärung einer vorsätzlich begangenen Straftat, die mit Freiheitsstrafe von mehr als einem Jahr ist, und auf Grund bestimmter Tatsachen anzunehmen ist, dass dadurch Daten des Beschuldigten ermittelt werden können. Die Überwachung von Nachrichten (§ 135 Abs. 3 StPO nF) setzt darüber hinaus voraus, dass der Inhaber der technischen Einrichtung der Tat dringend verdächtig ist oder anzunehmen ist, dass sich ein der Tat dringend Verdächtiger mit dem Inhaber der überwachten Einrichtung in Verbindung setzen werde.

Zu 4:

Sollte die Richtlinie zur Vorratsdatenspeicherung umgesetzt werden, so bleibt es dabei, dass ein Zugriff auf die gespeicherten Daten (bzw. einzelne, genau konkretisierte Daten davon) nur auf Grund einer gerichtlichen Bewilligung zulässig ist. Eine Weitergabe solcher Daten ist nur im Einzelfall auf Grund eines Rechtshilfeersuchens (innerhalb der EU nach Maßstab des EU- Rechtshilfeübereinkommens) zulässig.

Zu 5:

Dazu verweise ich zunächst auf die Beantwortung von Frage 2. Eine Verpflichtung zur lebenslangen Speicherung nationaler Kommunikationsdaten ist im Cybercrime-Übereinkommen nicht enthalten; vielmehr werden die nationalen Speicherfristen durch das Übereinkommen nicht berührt.

Was die allfällige Weitergabe übermittelter Kommunikationsdaten durch den ersuchenden Staat betrifft, so ist die Bestimmung des Art. 28 Abs. 2 lit. b des Übereinkommens zu beachten; danach kann der ersuchte Staat anlässlich der Datenübermittlung die Bedingung stellen, dass diese nur für die im Ersuchen angeführten Untersuchungen und Verfahren verwendet werden dürfen (Spezialitätsbindung). In einem derartigen Fall kommt deren Weitergabe durch den ersuchenden Staat nicht in Betracht.

. Jänner 2008

(Dr. Maria Berger)

Dieser Text wurde elektronisch übermittelt. Abweichungen vom Original sind möglich.