330/AB XXII. GP

Eingelangt am 16.06.2003

BM für Justiz

Anfragebeantwortung

Die Abgeordneten zum Nationalrat Mag. Johann Maier, Kolleginnen und Kollegen haben an mich eine schriftliche Anfrage betreffend „weltweites totales USA-Überwachungsprojekt „Information Awareness Office (IAO)" - Auswirkungen auf Österreich und Europa" gerichtet.

Ich beantworte diese Anfrage wie folgt:

Zu 1 bis 3:

Das Thema ist aus den Medien bekannt. Eine Kontaktaufnahme oder Information durch amerikanische Dienststellen ist bisher nicht erfolgt.

Zu 4:

Ich verweise auf die Beantwortungen der Anfragen durch den Herrn Bundesminister für Inneres zur Zahl 318/J-NR/2003 und den Herrn Bundeskanzler zur Zahl 323/J-NR/2003.

Zu 5:

Mangels einer offiziellen Information ist das in der Anfrage näher bezeichnete Überwachungsprojekt weder mir noch den Beamten des Bundesministeriums für Justiz ausreichend bekannt, sodass ich diese Frage nur sehr allgemein beantworten kann.

Von Bedeutung ist im gegebenen Zusammenhang die Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen

Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation), ABI. Nr. L 201/37 vom 31.7.2002. Deren Artikel 5 verpflichtet die Mitgliedstaaten dazu, die Vertraulichkeit der mit öffentlichen Kommunikationsnetzen und öffentlich zugänglichen Kommunikationsdiensten übertragenen Nachrichten und der damit verbundenen Verkehrsdaten durch innerstaatliche Vorschriften sicherzustellen. Insbesondere untersagen sie das Mithören, Abhören und Speichern sowie andere Arten des Abfangens oder Überwachens von Nachrichten und der damit verbundenen Verkehrsdaten durch andere Personen als die Nutzer, wenn keine Einwilligung der betroffenen Nutzer vorliegt.

In grundrechtlicher Hinsicht wäre auf Art. 10a StGG zu verweisen, wonach das Fernmeldegeheimnis verfassungsmäßig verankert und durch § 119 StGB auch strafrechtlich geschützt ist. Es kann nur auf Grund einer gerichtlichen Anordnung durchbrochen werden (§ 149a ff. StPO). Einfachgesetzlich ist das Fernmelde-geheimnis in § 87 TKG geregelt, wodurch auch klargestellt wird, dass es sich auf Vermittlungsdaten bezieht. Zum Grundrecht auf Datenschutz verweise ich auf § 1 DSG 2000 und auf Art. 8 EMRK.

Die Zulässigkeit der Übermittlung personenbezogener Daten an Sicherheits-organisationen oder ausländische Sicherheitsbehörden wird in § 8 des Polizei-kooperationsgesetzes geregelt; dessen Anwendung fällt wiederum in den Vollzugsbereich des Bundesministeriums für Inneres. Gleiches gilt im Übrigen für die Datenschutzregelung des Europolübereinkommens und des Schengener Durchführungsübereinkommens. Für beide Bereiche kann allgemein bemerkt werden, dass jede Vertragspartei die Verpflichtung übernommen hat, spätestens bis zum jeweiligen Inkrafttreten der Übereinkommen in ihrem nationalem Recht in Bezug auf die Verarbeitung personenbezogener Daten in Dateien im Rahmen der Anwendung der Übereinkommen die erforderlichen Maßnahmen zur Gewährleistung eines Datenschutzstandards zu treffen, der zumindest dem entspricht, der sich aus der Verwirklichung der Grundsätze des Übereinkommens des Europarates vom 28. Januar 1981 ergibt, und dabei die Empfehlung R(87) 15 des Ministerkomitees des Europarates vom 17. September 1987 über die Nutzung personenbezogener Daten im Polizeibereich zu beachten (siehe z.B. Art. 14 Abs. 1 des Europol-Übereinkommens).

Für den Bereich des Justizressorts setzt daher die Überwachung der Kommunikation eine gerichtliche Anordnung nach den §§ 149a ff. StPO voraus. In materieller

Hinsicht würden generelle Abhörmaßnahmen auch den Strafbestimmungen der §§ 118a (Widerrechtlicher Zugriff auf ein Computersystem"), 119 („Verletzung des Telekommunikationsgeheimnisses") und 119a („Missbräuchliches Abfangen von Daten) bzw. 120 (Missbrauch von Tonaufnahme- oder Abhörgeräten) StGB zuwiderlaufen.

Zu 6 und 9 bis 11:
Diese Fragen betreffen keinen Gegenstand der Vollziehung des Bundesministers für Justiz.

Zu 7 und 8:
Nein.

Zu 12 und 13:
EUROJUST wurde mit Beschluss des Rates vom 28. Februar 2002, ABI L 063 vom 6. 3. 2003, gegründet. Art 27 dieses Beschlusses regelt die Beziehungen von EUROJUST zu den für Ermittlungen und Strafverfolgungsmaßnahmen zuständigen Behörden von Drittstaaten. Für die Zusammenarbeit mit Drittstaaten kann EUROJUST Vereinbarungen über die Zusammenarbeit abschließen, die vom Rat gebilligt werden müssen. Enthalten diese Vereinbarungen Bestimmungen über den Austausch personenbezogener Daten, ist die gemeinsame Kontrollinstanz von EUROJUST zu hören.

Bevor EUROJUST Informationen mit Drittstaaten austauscht, ist die Genehmigung des nationalen Mitglieds jenes Mitgliedsstaates einzuholen, der die Informationen vorgelegt hat. Überdies darf EUROJUST personenbezogene Daten an Behörden von Drittstaaten, die nicht Mitgliedsstaaten des Übereinkommens des Europarats vom 28. Jänner 1981 sind, nur weiterleiten, wenn ein vergleichbares angemessenes Datenschutzniveau gewährleistet ist. Auch die Einhaltung dieser Vorschrift ist von der Gemeinsamen Kontrollinstanz zu überwachen. Für eine Übermittlung von personenbezogenen Daten bei unmittelbar drohender ernster Gefahr für eine Person oder die öffentliche Sicherheit bestehen in der Verantwortlichkeit des nationalen Mitglieds Sondervorschriften.

Die Übermittlung personenbezogener Daten an Drittstaaten wird durch den Beschluss zur Schaffung von EUROJUST ausführlich im Hinblick auf die Einhaltung eines angemessenen Datenschutzniveau durch Drittstaaten geregelt.

Werden keine personenbezogenen Daten an Drittstaaten weitergeleitet, kann eine Zusammenarbeit mit Behörden von Drittstaaten auch eine ohne vorherige Vereinbarung zwischen EUROJUST und dem Drittstaat stattfinden.

Zu 14 und 15:

Bei der Informationssuche im Internet ist es vielfach unvermeidlich auch auf personenbezogene Daten zu stoßen. Dabei kann es freilich auch vorkommen, dass gezielt nach personenbezogenen Daten gesucht wird, wenn etwa in einem Internet-Verzeichnis die Telefonnummer eines Ansprechpartners erhoben wird.

Zu 16 und 17:

Das Bundesministerium für Justiz betreibt außer dem Kanzleiinformationssystem und der im Netzwerk Justiz den Gerichten zugänglichen Listen der Revisoren nach dem Genossenschaftsgesetz 1997 selbst keine Datenbanken. In größerem Umfang wird dies im Auftrag der Gerichte bzw. des Bundesministeriums für Justiz im Bundesrechenzentrum durchgeführt (Verfahrensautomation Justiz, Ediktsdatei, Firmenbuch, Integrierte Vollzugsverwaltung (IW)). Nähere Informationen können dem öffentlich zugänglichen Datenverarbeitungsregister entnommen werden.

Darüber hinaus bestehen Datenbanken mit personenbezogenen Daten bei den Justizanstalten (zum Beispiel Diensteinteilungsprogramme). Die Justizanstalten sind angewiesen diese Datenverarbeitungen selbstständig zu melden (siehe Erlass JMZ 42701/19-V.3/2000 vom 4.5.2000).

Zu 18 bis 21:

Rechtsgrundlage sind die jeweiligen Materiengesetze. Details können dem zuvor erwähnten Datenverarbeitungsregister entnommen werden.