357 /J

2003 -04- 29

ANFRAGE

der Abgeordneten Mag. Johann Maier
und GenossInnen
an den Bundesminister für Landesverteidigung
betreffend **weltweites totales USA-Überwachungsprojekt „Information Awareness Office" (IAO) – Auswirkungen auf Österreich und Europa**

Medienberichten zufolge plant die USA das totalste Überwachungsprojekt der Geschichte: „Information Awareness Office" (IAO).
Entstanden ist es als Reaktion auf die Terroranschläge des 11. September 2001. Beim seit Anfang des Jahres 2002 bestehenden IAO laufen eine ganze Reihe von Aktivitäten zusammen, deren Ziel es ist, alle irgendwie zugänglichen Daten von Bürgern miteinander zu verknüpfen. **Weltweit und nicht auf die USA beschränkt.**

Die moderne Kommunikation wird von den USA als Gefahrenquelle gesehen. Die technologische Revolution habe in den Bereichen Information und Kommunikation zu einer Machtverschiebung von Regierungen und Staaten hin zu Individuen und Gruppen geführt. Terroristische Gefährdung könne daher nur durch eine entsprechende Kontrolle und Überwachung der modernen Kommunikation präventiv gekämpft werden, lautet nun die amerikanische Philosophie und Weltpolitik.

Damit wird einerseits das Datenschutzniveau reduziert, andererseits das Recht auf Privatsphäre (Privacy) als Grund- und Menschenrecht in Frage gestellt.

Datenschutz ist als Grund- und Menschenrecht auch in Europa unterschiedlich ausgeprägt (zB Umsetzung, Registrierung, Zustimmung, Rechtsdurchsetzung, Information). Trotzdem stellt die EU-Datenschutzrichtlinie – ungeachtet aller Vorbehalte und Mängel – ein Vorbild für andere Staaten dar. Problematisch ist nur, dass durch die EU der Bereich der äußeren und inneren Sicherheit ausgeklammert wurde. Dafür gelten jeweils (nationale) Sonderbestimmungen.

Noch ist „IAO" ein zunächst auf fünf Jahre befristetes Forschungsprojekt mit dem Ziel der Schaffung des Prototyps eines solch allwissenden, göttlichen Auges der USA. Fest steht aber, dass derzeit bereits 200 Millionen Dollar jährlich dafür budgetiert sind.

Die Stoßrichtung des Programms zielt zunächst einmal auf die **Einbindung staatlicher und privater Datenbanken weltweit**: Flugbuchungen, Kreditkartenumsätze, Bücherkäufe,

Medikamentenverschreibungen, Führer- und Pilotenscheine, Kontobewegungen, Autovermietungen, Visa- und Asylinformationen, Krankenkassen-Register, die Daten von Geheimdiensten und Strafverfolgern – alles, was irgendwo und irgendwann elektronisch erfasst ist, jede Informationsquelle der Welt soll zugänglich gemacht, verknüpft und automatisiert ausgewertet werden.

Doch damit nicht genug: Dazu kommt jener Bereich, der bisher schon von „Echelon" abgedeckt ist, nämlich alles, was mit **Kommunikation** zu tun hat: Telephonate, Faxe, E-Mails, Datenströme werden – in einem weitgehend rechtsfreien Raum – abgehört, gescannt und ebenfalls dem auszuwertenden Mega-Daten-Pool hinzugefügt.

Weiters sollen **alle Varianten biometrischer Erkennungssysteme** einbezogen werden. Dazu gehören einerseits bestehende Datenbanken – etwa mit DNA-Informationen oder Fingerabdrücken (von Ausländern aus bestimmten arabischen Ländern werden bei der Einreise in die USA bereits seit Oktober vergangenen Jahres Fingerabdrücke genommen). Ebenso sollen neue biometrische Erkennungsmethoden weiterentwickelt und integriert werden. Eines dieser Projekte nennt sich etwa „Human ID at a Distance". Dabei geht es um die Identifizierung von Personen via Video-Daten, wie sie beispielsweise bei den zahlreichen Überwachungskameras in Flughäfen oder Geschäften anfallen (aus der Presse 2.12.2002).

Bei diesen amerikanischen Überwachungsvorstellungen stellt sich natürlich auch die Frage, inwieweit jetzt bereits die USA und andere Drittstaaten Daten aus dem „Schengener Informationssystem" und anderen öffentlichen Datenbanken der EU-Mitgliedsstaaten erhalten.

Den ersten Eindruck von diesem Überwachungsprojekt bekamen die Europäer jüngst zu spüren, als die USA den vollen Zugriff auf alle Fluggastdaten bzw. Buchungssysteme der europäischen Airlines verlangten. Angedroht wurde die Entziehung der Landerechte und den USA. Rechtsgültige europäische Datenschutzbestimmungen sollten damit ausgehebelt werden.

Betroffen von diesem US-Überwachungskonzept sind nicht nur private, sondern auch alle öffentlichen – auch österreichischen - Datenbanken, gleichgültig welches Bundesministerium im Einzelfall Betreiber ist. Damit geht es um die Frage, wie sicher sind private und öffentliche Datenbanken in Österreich. Bei Datenbanken von Unternehmen, die grenzüberschreitend tätig sind (z.B. Banken) gab es nie eine hundertprozentige Sicherheit, dass datenschutzrechtliche Bestimmungen auch eingehalten werden. Bei privaten Datenbanken und im Internet sind die Defizite bekannt und offensichtlich. Moderne Suchmaschinentechnologien beispielsweise geben Privatpersonen und Firmen Daten aus dem Netz, die missbräuchlich verwendet werden

können. Suchmaschinenerzeuger wie Quigo Technologies brüsten sich auf ihrer Homepage, automatische Tools für Business und Militär zu erzeugen, um Kunden- oder Personenprofile zu erstellen (indizierte Datenbanken).

Bereits in den letzten Jahren gab es Auseinandersetzungen mit den Vereinigten Staaten von Amerika über datenschutzrechtliche Schutzstandards. Die mit der EU-Kommission aus wirtschaftlichen Gründen vereinbarten „Safe Harbour-Grundsätze" sollen bestimmte Mindeststandards sichern, sind aber gesetzlich nicht abgesichert und durchsetzbar. Die Artikel 29 Datenschutzgruppe der EU – der alle Mitgliedstaaten angehören – hat dazu grundsätzliche Bedenken angemeldet und Verbesserungen eingefordert (z.B. Weitergabe von Daten an Dritte in den USA, Rechtsdurchsetzung, Ausnahmen).

Die unterzeichneten Abgeordneten richten daher an den Bundesminister für Landesverteidigung nachstehende

Anfrage:

1. Ist Ihnen dieses zitierte weltweite Überwachungsprojekt der USA bekannt?
2. Sind Sie von der amerikanischen Administration bereits darüber informiert worden? Wenn ja, wann?
3. Wann ist die USA (bzw. die US-Administration wie zB die Botschaft) an Sie oder an eine nachgeordnete Dienststelle Ihres Bundesministeriums herangetreten, an diesem Projekt mitzuwirken?
4. Welche Haltung nimmt das Bundesministerium für Inneres bzw. die Österreichische Bundesregierung zu diesem weltweiten Überwachungsprojekt der USA ein?
5. Gegen welche bestehenden gültigen europäischen und nationalen Vorschriften würde bei einer Übernahme bzw. Teilnahme an diesem Projekt durch Österreich verstoßen werden?
   Welche geltenden Bestimmungen verbieten dies?
6. Welche Haltung nehmen die zuständigen Gremien der EU-Kommission bzw. das Europäische Parlament zu diesem weltweiten Überwachungsprojekt der USA ein?
7. War Ihr Bundesministerium auf EU-Ebene in Gesprächen und/oder Verhandlungen bereits dazu eingebunden?
8. Wenn ja, was war das Ergebnis?
9. Sind Ihnen Verhandlungen der EU-Kommission mit den USA bezüglich IAO bekannt?
10. Wenn ja, wie ist der Verhandlungsstand?
11. Wenn ja, inwieweit sind die Mitgliedstaaten und konkret Ihr Ressort eingebunden?
12. Erhält die NATO Daten, aus dem „Schengener Informationssystem"?

13. Wenn ja, welche Daten unter welchen Voraussetzungen und aufgrund welcher Bestimmungen?
14. Wurden bzw. werden von ihrem Bundesministerium personenbezogene Daten über Suchmaschinen abgefragt bzw. bezogen (z.B. google)?
15. Wenn ja, seit wann? Welche?
    Was war jeweils der Anlass dafür?
16. Welche Datenbanken betreibt Ihr Ministerium? Welche davon werden als Informationsverbundsystem geführt?
    Wann wurden diese bei der Datenschutzkommission registriert?
17. Welche „Nichtbehörden" (z.B. Unternehmen) haben für diese Daten oder Teile davon eine Zugriffsberechtigung?
18. In welchen Rechtsmaterien ist dies jeweils geregelt?
    Welche Voraussetzungen müssen dafür jeweils erfüllt sein?
19. Welche „beliehene Unternehmen" haben Zugriff auf Daten aus diesen Datenbanken im Rahmen der ihnen vom Gesetz übertragenen Aufgaben (ersuche um Aufzählung dieser Unternehmen)?
20. Können (sensible) Daten aus diesen öffentlichen Datenbanken ausländischen Stellen bzw. europäischen Dienststellen übermittelt werden?
21. Wenn ja, welche Daten und aufgrund welcher Rechtsgrundlage?
22. Sind Datenübertragungen im Rahmen der Petersberger Beschlüsse vorgesehen?
    Wenn ja, welche Daten unter welchen Voraussetzungen und aufgrund welcher Bestimmungen?
23. Sind Datenübertragungen im Rahmen der „Partnerschaft für den Frieden" vorgesehen?
    Wenn ja, welche Daten unter welchen Voraussetzungen und aufgrund welcher Bestimmungen?
24. Gibt es Datenübertragungen im Rahmen der Sicherheits- und Verteidigungspolitik?
    Wenn ja, welche Daten unter welchen Voraussetzungen und aufgrund welcher Bestimmungen?
25. Gibt es Datenübertragungen im Rahmen des KSE-BVG?
    Wenn ja, welche Daten unter welchen Voraussetzungen und aufgrund welcher Bestimmungen?