Entschließungsantrag

der Abgeordneten Mag. Johann Maier

und GenossInnen

betreffend Hochsicherheitspässe: Für ein EU-weit einheitliches und umfassendes Datenschutz- und IT-Sicherheitskonzept – Initiative der Österreichischen EU-Ratspräsidentschaft

Der österreichische Nationalrat hat am 01.03.2006 mehrheitlich die Novelle zum Passgesetz beschlossen, mit der nun auch biometrische Passdaten auf einem Funkchip (RFID-Chip) gespeichert werden können. Damit wurde die Verordnung (EG) Nr. 2252/2004 umgesetzt. Die Verordnung (EG) Nr. 2252/2004 über Normen für Sicherheitsmerkmale und biometrische Daten in von den Mitgliedstaaten ausgestellten Pässen und Reisedokumenten (EG-PassVO) trat bereits am 18. Jänner 2005 in Kraft. Sie legt als unmittelbar verbindliches Recht für alle EU-Bürger fest, dass in den Reisepässen der EU-Mitgliedstaaten zwei biometrische Datensätze elektronisch gespeichert werden. In neuen Pässen muss 18 Monate nach der Festlegung der technischen Formate (die im Februar 2005 erfolgt ist) ein Datensatz über das Bild des Gesichts und 36 Monate nach diesem Zeitpunkt ein Datensatz über die Fingerabdrücke enthalten sein, obwohl sich das Europäische Parlament gegen den digitalen Fingerabdruck ausgesprochen hat. Die Art. 29 Datenschutzgruppe wurde trotz der Forderung des Europäischen Parlaments (EP) in das Verfahren der technischen Normierung durch den Rat nicht einbezogen. Diese Normierung obliegt in Zukunft dem privaten internationalen Verein ICAO.

Durch die vorgenommene Novelle zum Passgesetz wird in Österreich u.a. konkret die Speicherung eines digitalen Bildes des Passinhabers als primäres biometrisches Merkmal verpflichtend vorgeschrieben. Neben dem Lichtbild ist nach der VO (EG) Nr. 2252/2004 auch der Fingerabdruck des Passinhabers als zweites biometrisches Merkmal (ca. ab 2008) vorgesehen. Diese beiden biometrischen Daten sind auf einem im Pass eingeprägten Mikrochip (RFID) zu speichern.

Verfassungsrechtlich problematisch in dieser EU-Verordnung ist aber die dynamische Verweisung auf die technischen Sicherheitsstandards der ICAO (z.B. Richtlinien, Empfehlungen etc.). Die Mitgliedsstaaten der EU sind durch die EU-VO verpflichtet, die

entsprechenden Vorgaben der ICAO einzuhalten. Da es dabei auch um die Art der Speicherung, des Zugriffsschutzes und der Verschlüsselung geht, wird in verfassungsrechtlich gewährleistete Grundrechte eingegriffen, ohne dass es eine parlamentarische Kontrolle gibt. Zu beachten ist ferner, dass es sich dabei um eine international tätige Organisation handelt, die maßgeblich unter dem Druck außereuropäischer Staaten steht (z.B. USA).

Die Entscheidung für die zwei biometrischen Merkmale wurde durch den **Europäischen Rat** (Regierungsvertreter) getroffen – und zwar entgegen der Stellungnahme des EP. Das EP hat sich u. a. ausdrücklich gegen den Fingerabdruck als zweites biometrisches Merkmal ausgesprochen. Die Mehrzahl der nationalen Parlamente in den EU-Mitgliedsstaaten wurden vor dieser Entscheidung mit den Themen Hochsicherheitspässe und Biometrie nicht befasst; weder Chancen noch Risiken, weder Aufwand noch Kosten waren vor der EU-Beschlussfassung auf den nationalen Ebenen Gegenstand ausführlicher Diskussionen.

Begründet wurde und wird die Einführung von Biometrie und biometrischen Verfahren in Pässen durch die EU-Kommission und die nationalen Regierungsvertreter mit Terrorismusbekämpfung, Dokumentenmissbrauch und vielen Sicherheitsargumenten. In Wirklichkeit kommen diese Vorgaben von der Internationalen Zivilluftfahrt-Organisation **ICAO**. Diese Regelungen dienen aber ausschließlich der Beschleunigung der Grenzkontrollen bei der Aus- bzw. Einreise und der Check-in Verfahren, nicht aber einer Erhöhung der Sicherheit bzw. der Terrorismusbekämpfung. Die MRZ-Zeile im Pass kann übrigens jederzeit über das Internet berechnet werden (ICAO 9303).

Daher wurde in einem **SP-Entschließungsantrag** im Nationalrat im Jahr 2005 auch ein Moratorium eingefordert sowie eine Kosten- und Nutzenstudie (EA 598/A(E)). Dieser EA wurde Ende 2005 im Nationalrat von allen Fraktionen **einstimmig** angenommen. Die in diesem Antrag verlangte Studie wurde vom BMI in Auftrag gegeben und wird zur Zeit im Fraunhofer-Institut erarbeitet. Auf EU-Ebene wird am Forschungsprojekt **„Biometrie Identification Technology Ethics“** gearbeitet (Fertigstellung Juni 2006).

Die Frage, ob die in den Pässen standardmäßig eingesetzte RFID-Technik dazu führen kann, dass jedes handelsübliche 13-MHz-Lesegerät die biometrischen Merkmale auslesen kann, hat beispielsweise in Deutschland zum öffentlichen Start von **OpenMRTD** geführt. Ziel des von Harald Welte ins Leben gerufenen **Open Source-Projekte** ist die Erstellung eines Toolsets,

mit dem die Daten von biometrischen Pässen gelesen und untersucht werden können. Im digitalen Zeitalter sollen nämlich aus dessen Sicht auch die Bürger ein Mittel zur Hand haben, mit dem sie die digitalen Inhalte lesen können, genau wie sie die analogen (gedruckten) Inhalte lesen können. **Insbesondere sollte es damit möglich sein, die digitale Signatur zu überprüfen und damit festzustellen, ob der Pass tatsächlich korrekt ausgestellt wurde.**

Das vom Bundesministerium für Inneres und der Österreichischen Staatsdruckerei vorgestellte Sicherheitskonzept für die österreichischen Hochsicherheitspässe wurde vom Datenschutzrat ausführlich diskutiert, begutachtet und für tauglich erachtet; gleichzeitig wurde aber ausdrücklich darauf hingewiesen, dass dieses Sicherheitskonzept durch das Bundesministerium für Inneres laufend zu überprüfen ist.

Trotz dieser gültigen EU-Verordnung sind auf europäischer Ebene viele Fragen zur Anwendung von Biometrie und über biometrische Verfahren offen geblieben und gesellschaftspolitisch in ihrer Tragweite keinesfalls ausdiskutiert worden. Darauf wurde beispielsweise auch bei der Internationalen Konferenz der Datenschutzbeauftragten in Montreux sehr klar hingewiesen (September 2005). Nach der EMRK und dem österreichischen Verfassungsrecht absolut bedenklich und abzulehnen wäre überdies eine unkontrollierte Verwendung biometrischer Passdaten durch viele Behörden wie auch durch private Unternehmen.

Zu berücksichtigen ist, dass im Privatsektor zunehmend biometrische Daten verarbeitet werden, oft auch auf freiwilliger Basis (z.B. Zutrittskontrolle). Biometrische Daten können aber auch gesammelt werden, ohne dass die betroffene Person Kenntnis davon erhält, da Personen biometrische Spuren unbewusst hinterlassen können. Die Biometrie macht den menschlichen Körper „maschinenlesbar", womit biometrische Daten als weltweit einheitlicher Indikator benutzt werden könnten. Die verbreitete Verwendung der Biometrie wird nicht nur weitreichende Folgen für die Privatsphäre und Grundrechte haben, sondern für die Weltgesellschaft insgesamt. Notwendig sind daher – neben absoluter Transparenz – wirksame Schutzmaßnahmen, die zu einem möglichst frühen Zeitpunkt Anwendung finden sollen, damit die der Biometrie inhärenten Risiken vermindert werden (z.B. Eingriff in die Privatsphäre; Identitätsdiebstahl). Neben den technischen Sicherheitsstandards sind abschreckende Strafbestimmungen vorzusehen, aber auch die Möglichkeit von zivilrechtlichen Ansprüchen sowie Staatshaftungsansprüchen.

Europaweit gibt es zur Zeit noch immer kein harmonisiertes und umfassendes **Datenschutz- und IT-Konzept** für die so genannten Hochsicherheitspässe, die Biometrieanwendung bzw. die bei Kontrollen verwendeten biometrische Verfahren. Es fehlt ein harmonisiertes technisches Sicherheitskonzept zum Schutz der im RFID-Chip gespeicherten biometrischen Daten der Passinhaber (Mindestanforderungen für biometriegestützte Pässe zur Verhinderung des Missbrauchs). Dies wurde 2005 auch durch das Europäische Parlament (EP) bestätigt. Dass es noch enorme ungelöste technische Probleme gibt, bewies im Jänner 2006 ein **Test in den Niederlanden**. Laut dem Bericht eines TV-Senders gelang es Hackern, ohne Probleme die Daten vom Funkchip des Dokuments auszulesen und rasch zu entschlüsseln. Name, Geburtsdatum und weitere persönliche Daten konnten auf diese Weise bei dem „Trockentest" ermittelt werden. Die Schwachstellen müssen aus Behördensicht nun erst ausgelotet werden.

Die **Passkontrollen** werden an den EU-Grenzkontrollstellen (Ein- und Ausreise) bzw. Flughäfen aufgrund fehlender einheitlicher Kontroll- und Sicherheitsstandards bzw. biometrischer Verfahren in den EU-Mitgliedsstaaten äußerst unterschiedlich durchgeführt. Zum Teil werden bei der Kontrolle die im Chip gespeicherten biometrischen Passdaten mit denen der einreisenden Person (Kamerabild) verglichen, möglicherweise auch gespeichert und dann weiter verarbeitet.
Die Echtheit aller Daten des Einreisenden wird bei österreichischen Grenzkontrollen (Einreise oder Ausreise) nicht überprüft bzw. festgestellt. Österreich verwendet kein biometrisches Verfahren: Es wird nur die Authentizität (Echtheit) des Dokuments geprüft (Art. 4 Abs 3 VO). Die digitalen Bilddaten werden mit dem aufgedruckten und verschweißten Bild des Passes verglichen.

Anders beispielsweise die Situation in Deutschland: Das auf dem Chip gespeicherte Passbild soll bei der Einreise analysiert und mit dem aktuellen Kamerabild verglichen werden. Liegt der Vergleich innerhalb einer bestimmten Toleranz gilt es als sicher, dass der Reisende mit dem Passinhaber identisch ist. Diese Gesichtserkennung ist aber nicht unproblematisch (Lichtverhältnisse, Mimik, Gesichtszüge, Haaransatz etc.).
Ein Problem liegt beispielsweise bei Menschen mit asymmetrischen Gesichtern (z.B. schiefe Nase) und Kindern. Daher müssen deutsche Passinhaber auch eine sog. Lichtbilderklärung unterfertigen, um mögliche Schadenersatzansprüche auszuschließen.

„Hiermit bestätige ich, dass ich von der Ausweisbehörde über die Qualität/Beschaffenheit meines vorgelegten Lichtbildes belehrt wurde.
Ich bestehe auf Annahme dieses Lichtbildes durch die Passbehörde.
Entstehende Schadenersatzansprüche, wegen Abweisung an einer Landesgrenze oder auf Grund polizeilicher Identitätsvorstellungen, kann ich gegenüber der Passbehörde nicht geltend machen. Die Kosten für einen neuen Ausweis habe ich voll zu tragen."

Diese Situation erklärt auch die unterschiedliche rechtspolitische Diskussion in den EU-Mitgliedsstaaten zur Biometrie in Pässen insbesondere, was Fragen des Datenschutzes und der Datensicherheit betrifft.

Es gibt weltweit noch kein biometrisches Verfahren, das eine 100%ige Identifikation zulässt, die Zuverlässigkeit dieser Systeme und Verfahren ist noch gering.
Hochsicherheitspässe mit einem oder mehreren biometrischen Merkmalen führen somit nicht automatisch zu einer Verbesserung der Sicherheit (Konferenz der deutschen Datenschutzbeauftragten im Juni 2005). Tests haben bewiesen, dass biometrische Identifikationsverfahren einerseits hohe Falscherkennungsraten aufweisen und andererseits oft mit einfachsten Mitteln zu überlisten sind. **Diese Hochsicherheitspässe werden möglicherweise durch die derzeit noch unsicheren und verwendeten biometrischen Verfahren in einigen EU-Mitgliedsstaaten zum wirklichen Sicherheitsrisiko!**

Kurz vor der geplanten Einführung von neuen Reisepässen mit individuellen biometrischen Merkmalen im November des Jahres 2005 kam eine Studie des deutschen Bundesamtes für Sicherheit in der Informationstechnik (BSI) zu wenig erfreulichen Ergebnissen: Drei Erfassungstechniken biometrischer Merkmale zeigten in drei bis 23 Prozent aller Fälle fehlerhafte Ergebnisse. **Das Bundesamt bemängelt das Fehlen von Großversuchen und sah noch erheblichen Nachbesserungsbedarf.**

Auch der Beschluss der deutschen Datenschutzbeauftragten im Jahr 2005 zeigte deutlich die bestehenden Sicherheitsdefizite bei Hochsicherheitspässen auf.
Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder forderte eine objektive Bewertung von biometrischen Verfahren und trat dafür ein, die Ergebnisse entsprechender Untersuchungen und Pilotprojekte zu veröffentlichen und die Erkenntnisse mit der Wissenschaft und der breiten Öffentlichkeit zu diskutieren. Eingefordert wurden überdies

rechtliche, organisatorische und technische Maßnahmen.

Auch im Memorandum der Europäischen Datenschützer in Montreux (30.09.2005) wird auf nicht gelöste Probleme hingewiesen.

„The Commission decision of 28 February 2005 is not appropriate to safe the rights of the citizens, since the contact between the RFID-chip and the reader is able to eavesdropped and the information can be skimmed."

Als österreichische Initiative der EU-Ratspräsidentschaft sollte ein harmonisiertes und umfassendes Datenschutz- und IT-Sicherheitskonzept für die An- und Verwendung von biometrischen Daten in Hochsicherheitspässen sowie die bei Kontrollen angewandten biometrischen Verfahren vorgeschlagen und in den EU-Gremien vertreten werden.

Die unterzeichneten Abgeordneten stellen daher folgenden

Entschließungsantrag:

Der Nationalrat wolle beschließen:

„Die jeweils zuständigen Mitglieder der österreichischen Bundesregierung werden aufgefordert, im Rahmen der EU-Ratspräsidentschaft Österreichs in den jeweils zuständigen EU-Gremien und Ministerräten Initiativen dahingehend zu setzen, dass

- in der Europäischen Union die biometrischen Merkmale (Daten) ausschließlich von den für die Passkontrollen zuständigen Behörden für hoheitliche Zwecke genutzt werden,
- der Zugriff für Private auf diese biometrischen Daten (Passdaten) generell ausgeschlossen wird,
- biometrische Daten, die auf der Grundlage gesetzlicher Verpflichtungen zu öffentlichen Zwecken (siehe Passgesetz) gespeichert werden, und solchen, die mit ausdrücklicher Einwilligung von Personen zu Vertragszwecken gesammelt und gespeichert werden, strikt getrennt bleiben,
- die in Ausweisen gespeicherten Daten mit biometrischen Daten nicht als Referenzdaten genutzt werden, um Daten aus unterschiedlichen Systemen und Kontexten zusammenzuführen,

- keine zentralen oder vernetzten Biometriedatenbanken geschaffen werden und die biometrischen Identifizierungsdaten ausschließlich nur auf dem jeweiligen Ausweisdokument gespeichert werden dürfen,
- keine europäische Passdatei mit biometrischen Daten der EU-BürgerInnen angelegt wird,
- die Verwendung biometrischer Daten in Pässen auf den Zweck der Identifizierung durch Vergleich der Daten des Dokuments mit Daten des Dokumentinhabers im Moment der Dokumentvorlage technisch beschränkt wird,
- die maschinelle Auslesung von biometrischen Daten auf Pässen nur an den EU-Grenzkontrollstellen und Flughäfen bzw. Häfen erfolgt,
- die für die Ausstellung und das Auslesen von biometrischen Merkmalen verwendeten Lesegeräte nach internationalen Standards von einer unabhängigen Stelle zertifiziert und diese in regelmäßigen zeitlichen Intervallen durch eine zentrale Einrichtung authentisiert werden,
- harmonisierte Verfahren in der EU festgelegt werden, die einen Datenmissbrauch beim Auslesen von biometrischen Daten verhindern und diese Verfahrensfestlegung durch eine unabhängige Stelle regelmäßig evaluiert wird,
- Passlesegeräte bei den nationalen Ausgabestellen (d.s. Passbehörden) kostenfrei aufgestellt werden, damit jeder Bürger überprüfen kann welche Daten auf dem Chip gespeichert sind und
- Schadenersatzregelungen bzw. Amtshaftungsregeln für den Fall der Nichtidentifikation bzw. Nichtverifikation (Biometrie funktioniert nicht) und damit verbundener Schäden festgelegt sowie
- abschreckende Strafbestimmungen für das illegale Auslesen, Verarbeiten, Verwenden oder für die rechtswidrige Übermittlung und Verwertung von biometrischen Daten normiert werden (Umgehung der IT-Sicherheitstechnik bzw. der Verschlüsselung). Dies gilt insbesondere für den Fall des Identitätsdiebstahles.

Zuweisungsvorschlag: Ausschuss für innere Angelegenheiten