

Stellungnahme zum Bundesbeschluss über biometrische Pässe und Ausweise vom 13. Juni 2008

Zusammenfassung

- Die vorgesehene Kompetenz des Bundesrates zum Abschluss von Verträgen über die Auslesung der gespeicherten Fingerabdruckmuster mit anderen Ländern ist zu wenig klar umschrieben. Insbesondere fehlen Vorgaben zu Klauseln betreffend Speicherdauer und weitere Verwendung der ausgelesenen Muster.
- Dem Wortlaut nach wird das Gesetz kein Verbot der Verwendung von ISA-Daten zu Fahndungszwecken enthalten. Vielmehr erlauben die neuen Bestimmungen einen Zugriff auf diese Daten zur Erfüllung gesetzlicher Aufgaben bzw. zur Identifikation von Personen.
- In der Gesamtbetrachtung enthalten die neuen Bestimmungen umfassende Kompetenzen des Bundesrates, privaten Unternehmen sowie Bundesbehörden im Sinne des DSG Zugriffsrechte in Bezug auf die ISA-Daten zu gewähren. Dies, obwohl die Berechtigung einer Behörde im Einzelfall aufgrund der Sensibilität der gespeicherten Personendaten jeweils in einem formellen Gesetz zu regeln wäre.
- Im Zusammenspiel mit der geplanten Änderung des Regierungs- und Verwaltungsorganisationsgesetzes könnten die auf dem Chip gespeicherten Daten bei jeder elektronischen Kontrolle als digitale Kopie gespeichert und für unbestimmte Zeit aufbewahrt werden.

1. Einleitung

Im Hinblick auf das Recht auf den Schutz vor Missbrauch der persönlichen Daten stellt die zunehmende Tendenz, persönliche Daten elektronisch zu konzentrieren, sei es in Form von Gesundheitskarten, biometrischen Reisedokumenten oder neuer Zentralregister, eine steigende Bedrohung der Privatsphäre dar. Wer heute sein Portemonnaie verliert, muss noch nicht damit rechnen, dass Drittpersonen durch unbefugtes Auslesen der darin herumgetragenen elektronischen Ausweise und Karten an sensible Informationen gelangen. Noch nicht.

Vorweg ist darauf hinzuweisen, dass die undifferenzierte Betrachtung verschiedener Kategorien von biometrischen Daten aus Datenschutzrechtlicher Sicht nicht zulässig erscheint. Die Gleichsetzung der bisher in den Ausweisen und dem Informationssystem

Ausweispapiere (ISA) gespeicherten Daten mit der geplanten Speicherung von Fingerabdruckmustern übergeht die eigentliche Problematik. Mit der Erfassung und Speicherung des Fingerabdrucks wird eine neue Kategorie biometrischer Daten erfasst und bearbeitet, deren Individualisierungsgrad und Missbrauchspotential eine neue Qualität erreichen. Dies zeigt sich beispielsweise daran, wie viel schwieriger es sein dürfte, jemanden anhand der Körpergröße zu identifizieren, als anhand eines Fingerabdrucks.

Im Übrigen birgt die Umsetzung des Notentauschs zwischen der Schweiz und der Europäischen Gemeinschaft betreffend die Übernahme der Verordnung (EG) Nr. 2252/2004 über biometrische Pässe und Reisedokumente in der vorgeschlagenen Form einige datenschutzrechtliche Probleme.

2. Verträge mit anderen Staaten über das Auslesen der Fingerabdruckmuster

Im neu einzufügenden Art. 2a (neu) AwG soll der Bundesrat befugt werden, Verträge über das Lesen der im Chip gespeicherten Fingerabdrücke abzuschliessen, sofern die betreffenden Staaten über einen Datenschutz verfügen, der dem schweizerischen gleichwertig ist. Das maschinelle Auslesen der bisher gespeicherten Daten ist bereits möglich, auch in Staaten, die anerkanntermassen nicht über ein vergleichbares Niveau an Datenschutz verfügen, wie etwa die USA. Das Problem ist insofern nicht von vorrangiger Bedeutung, als die USA keine Speicherung von Fingerabdruckmustern in den Reisedokumenten selbst verlangen.

Hingegen wird im Rahmen der Umsetzung der Schengen-Ordnung ein Austausch von Leserechten mit den angeschlossenen Staaten sehr wahrscheinlich. Die Übertragung der Abschlusskompetenz auf den Bundesrat ist hierbei problematisch, da das neue AwG keine Vorschriften darüber enthält, die einen Rahmen für den möglichen Inhalt solcher Verträge bieten würden. Diese Frage stellt sich insbesondere im Hinblick auf die Bearbeitung, (Zwischen-)Speicherung und allfällige weitere Verwendung der Fingerabdruckmuster durch die Vertragsparteien.

3. Speicherung der Daten im ISA und Bearbeitung zu Fahndungszwecken

In der Botschaft und in den Abstimmungsunterlagen des Bundes wird betont, die Verwendung der im ISA gespeicherten Fingerabdruckmuster zu Fahndungszwecken sei verboten. Die Zugriffsberechtigungen und rechtmässigen Bearbeitungszwecke der im ISA gespeicherten Daten wurden vom Bundesrat in Art. 28 der Verordnung zum Ausweisgesetz (SR 143.111) als nicht abschliessende Aufzählung geregelt. Dies ist aus der Verwendung der Formel "insbesondere" klar ersichtlich. Die Verordnungsbestimmung stützt sich ihrerseits auf Art. 15 AwG, der dem Bundesrat eine umfassende Kompetenz zur Regelung der Zugriffs- und Bearbeitungsberechtigungen zuweist. Dies bedeutet, dass die ISA grundsätzlich für weitere Zugriffsberechtigungen offen ist, die jeweils durch den Bundesrat erteilt würden.

Solche neuen Zugriffsrechte sind im Änderungsvorschlag zum Ausweisgesetz vorgesehen. Der neue Art. 12 AwG gewährt zunächst in Abs. 2 lit. a dem Bundesamt für Polizei (Fedpol)

Zugriff auf sämtliche Daten, soweit diese der Erfüllung einer gesetzlichen Aufgabe dienen. Damit können auch andere Aufgaben gemeint sein, als jene, die in der nicht abschliessenden Liste von Art. 28 VAWG aufgezählt sind. Im Übrigen wäre eine Beschränkung des Begriffs der gesetzlichen Aufgabe im Sinne von Art. 12 Abs. 2 lit. b (neu) AwG durch eine Verordnung ohnehin rechtlich nicht möglich - diese müsste bereits im Ausweisgesetz selber vorgenommen werden.

Die Aufgaben und Funktionen des Fedpol sind in Art. 9, 10 und 11 der Organisationsverordnung vom 17. November 1999 für das Eidgenössische Justiz- und Polizeidepartement (OV-EJPD, SR 172.213.1) geregelt und beinhalten wenig genau umschriebene Kompetenzen in den Bereichen Staatsschutz, Wahrung der inneren Sicherheit der Schweiz, Bekämpfung der Kriminalität im Rahmen der Bundeszuständigkeit, Pflege von Kontakten zu ausländischen Polizei-, Sicherheits- und Strafverfolgungsbehörden, Gerichtspolizei, Unterstützung interkantonalen und internationalen Ermittlungen, Sicherheits-, Polizei- und Strafverfolgungsbehörden von Bund und Kantonen, Führung des Bundessicherheitsdienstes, Leitung der Koordinationsstelle gegen Menschenhandel und Menschen schmuggel, fremdenpolizeilicher Aufgaben in Bezug auf die innere Sicherheit, sowie der Betreibung von Informationssystemen im Bereich der Polizei, der Strafverfolgung und der inneren Sicherheit, der Bearbeitung von Anfragen und Auskunftsgesuchen in Polizeisachen und der Leitung von Nachforschungen nach dem Aufenthalt von Personen und Sachen sowie nach vermissten Personen im In- und Ausland.

Aufgrund des vorgeschlagenen Gesetzeswortlauts in Art. 12 (neu) AwG könnte das Fedpol die gespeicherten Daten demnach zur Identifikation von Personen in sämtlichen erwähnten Tätigkeitsbereichen verwenden. Zu diesem Zweck stünde mit der Zeit eine Datenbank zur Verfügung, welche die Muster der Fingerabdrücke jeder Person enthielte, die über 12 Jahre alt ist und der ein Schweizer Reisedokument oder ein Schweizer Passdokument ausgestellt wurde. Aus Sicht des Datenschutzes ist insbesondere fraglich, ob dies mit dem in Art. 4 Abs. 3 DSG ausdrücklich verankerten Gebot der transparenten Datenbearbeitung vereinbar ist. Zudem erscheint der Unterhalt einer Datenbank mit Fingerabdruckmustern eines überwiegenden Teils der registrierten Bevölkerung als schwerwiegender Eingriff in das Recht auf informationelle Selbstbestimmung und ist daher verfassungsrechtlich als höchst problematisch zu qualifizieren.

Neben dem Fedpol erhalten das Grenzwachtkorps sowie die vom Bund und den Kantonen bezeichneten Polizeistellen eine Zugriffsberechtigung zur Erfüllung gesetzlicher Aufgaben, wobei wiederum nicht klar geregelt ist, welche gesetzlichen Aufgaben gemeint sind. Diese Zugriffsberechtigungen werden insofern eingeschränkt, als sie ausschliesslich zur Identitätsabklärung zu nutzen sind. Unklar ist, ob damit die Bestätigung einer behaupteten Identität, etwa im Rahmen der Bearbeitung eines Antrags auf einen neuen Pass, oder die Identifizierung aufgrund von Tatortspuren im Rahmen einer Fahndung gemeint ist.

Die Botschaft äussert sich dahingehend, dass diese Artikel nicht als Rechtsgrundlage für einen Zugriff zu Fahndungszwecken interpretiert werden dürften. Nach Ansicht der Schweizerischen Datenschützer ist jedoch eine ausdrückliche Regelung dieser Einschränkung im Gesetz erforderlich. Aus dieser Sicht bedeutet die Formulierung "ausschliesslich zur

Identitätsabklärung" keine Einschränkung der in Art. 12 Abs. 2 lit. c, d und f (neu) AwG erteilten Zugriffsbefugnisse zur Erfüllung gesetzlicher Aufgaben.

Zusammenfassend muss daher festgestellt werden, dass weder das bisherige Recht noch die vorgeschlagenen Gesetzesänderungen ein ausdrückliches Verbot der Bearbeitung von ISA-Daten zu Fahndungszwecken enthalten.

4. Kompetenzdelegation an den Bundesrat

In Art. 2a Abs. 3 (neu) AwG soll dem Bundesrat die Kompetenz verliehen werden, Transportunternehmen, Flughafenbetreibern und anderen geeigneten Stellen, welche die Identität einer Person überprüfen müssen, auf die in den Pässen gespeicherten Daten zuzugreifen. Dies ist aus Sicht des Datenschutzesrechts heikel.

Aufgrund von Art. 17 Abs. 1 DSG (Bund) dürfen Behörden Daten bearbeiten, soweit eine gesetzliche Grundlage besteht. Die Bearbeitung besonders schützenswerter Personendaten, zu denen jene biometrische Daten, die aufgrund ihrer Einzigartigkeit Rückschlüsse auf das Individuum erlauben, zweifelsohne gehören, erfordert grundsätzlich eine Grundlage in einem formellen Bundesgesetz. Die gesetzliche Aufgabe, die Identität von Personen prüfen zu müssen, kann ohne weiteres ohne den elektronischen Zugriff auf sämtliche individualisierende biometrische Daten erfüllt werden. Die Aufgabe der Identifikation ist nicht gleichzusetzen mit den Mitteln der Identifikation. Da mildere Mittel zur Identifikation, etwa die Identifikation anhand eines Bildes üblicherweise ausreichen, ermächtigt eine gesetzliche Aufgabe zur Identifikation von Personen die Behörde grundsätzlich zur einfachen Ausweiskontrolle als mildestes erforderliches Mittel. Dies muss auch für Private gelten.

Weder die Entwürfe des AwG noch der VAwG enthalten jedoch Bestimmungen, welche diese neue Kompetenz des Bundesrates näher umschreiben. Der reine Wortlaut des Gesetzes ermächtigt ihn vielmehr dazu, beliebigen Privaten und Behörden, welche das Erfordernis der Prüfungspflicht bezüglich der Identität beliebiger Personen erfüllen, die Zugriffsbewilligung für biometrische Daten zu erteilen. Wer als solche "Stelle" gilt und unter welchen Voraussetzungen diese Stellen als solche gelten, welche "die Identität von Personen prüfen müssen", ist ebenso unklar wie der Kreis der möglicherweise betroffenen Personen. Damit bildet der Entwurf des AwG keine ausreichend bestimmte Delegationsnorm, mittels der dem Bundesrat eine Befugnis zur Erteilung von Zugriffsberechtigungen für die Bearbeitung von biometrischen Daten durch andere Stellen als die in Art. 12 (neu) AwG ausdrücklich zur Bearbeitung und Bekanntgabe sämtlicher Ausweisdaten ermächtigt würde.

Eine Ersatzgrundlage in Form einer bundesrätlichen Bewilligung, wie sie der Entwurf des AwG vorsieht, ist sodann gemäss Art. 17 Abs. 2 lit. b DSG (Bund) im Einzelfall bloss ausnahmsweise möglich und nur soweit sie die Rechte der Betroffenen nicht gefährdet. Dies bedeutet insbesondere, dass im Hinblick auf vorhersehbare, künftige und regelmässige Datenbearbeitungen eine genügende gesetzliche Grundlage zwingend vorgeschrieben ist. Dazu müsste die im Entwurf des AwG enthaltene Delegationsnorm entsprechend präzisiert werden.

5. Speicherung der Daten nach der geplanten Revision des RVOG

Im Entwurf zur Änderung des Regierungs- und Verwaltungsorganisationsgesetzes vom 12. Dezember 2008 (RVOG) ist die generelle Befugnis von Bundesbehörden sowie von Privatpersonen mit hoheitlicher Aufgabenerfüllung vorgesehen, sämtliche Personendaten, die bei der Nutzung ihrer oder der in ihrem Auftrag betriebenen elektronischen Infrastruktur entstehen, aufzuzeichnen und als Sicherheitskopie zu speichern. Sodann wird dem Bundesrat eine allgemeine Kompetenz zur Gewährung von Zugriffs- und Bearbeitungsrechten in Bezug auf diese gespeicherten Daten übertragen.

Die auf dem Chip gespeicherten Daten der Passinhaberin oder des Passinhabers sind elektronisch gespeichert und werden beim Grenzübertritt elektronisch erfasst. Beim Auslesen dieser Daten entsteht notwendigerweise eine Kopie des Datensatzes, die sodann auf einem Bildschirm dargestellt, ausgedruckt oder auf andere Weise bearbeitet werden kann. Gemäss der vorgesehenen Revision des RVOG würde dieser Datensatz zudem auf unbestimmte Zeit irgendwo gespeichert und so für eine spätere Bearbeitung bereit liegen.

Nach dem Wortlaut des Entwurfs RVOG läge die Regelung darüber, ob und allenfalls durch wen und in welchem Umfang diese Daten später bearbeitet werden dürften, in der alleinigen Kompetenz des Bundesrates.

6. Schlussfolgerung

In der Gesamtschau sieht der Bundesbeschluss vom 13. Juni 2008 aus datenschutzrechtlicher Sicht ungenügende gesetzliche Grundlagen für die im Zusammenhang mit der Übernahme der europäischen Vorgaben notwendigen administrativen, technischen und rechtlichen Massnahmen vor. Zudem gehen die geplanten Massnahmen in unnötiger und unverhältnismässiger Weise über die europäischen Vorgaben hinaus. Insbesondere die Bestimmungen bezüglich der Auslesung, Speicherung und Bearbeitung der Fingerabdruckmuster sind zu wenig bestimmt, um der Schwere des damit verbundenen Eingriffs in die Privatsphäre des Einzelnen gerecht zu werden.

Im Übrigen ist festzustellen, dass die vorgesehenen Bestimmungen die Entscheidungskompetenz über die Zugriffs- und Bearbeitungsberechtigungen in Bezug auf die ISA-Daten vom Parlament auf den Bundesrat verlagern sollen. Dabei würden nach Ansicht der Schweizerischen Datenschutzbehörden die verfassungsmässigen Gebote der Gewaltenteilung und des Legalitätsprinzips zu wenig beachtet.