Positionspapier zum Antiterrorgesetz der Bundesregierung

Kiel, 7. Dezember 2001

Unabhängiges Landeszentrum für Datenschutz
Postfach 71 16, 24171 Kiel
Tel.: 0431/988-1200, Fax: 0431/988-1223
E-Mail: mail@datenschutzzentrum.de
Internet: www.datenschutzzentrum.de

Inhalt:

I. Zu den Änderungen im Polizei- und Geheimdienstrecht

1. Artikel 1, 2 und 3 – Änderung des Bundesverfassungsschutzgesetzes, des MAD-Gesetzes und des BND-Gesetzes

1.1 Der Beobachtungsauftrag des Bundesamtes für Verfassungsschutz soll auf **Bestrebungen** erweitert werden, die **gegen den Gedanken der Völkerverständigung** gerichtet sind, auch wenn sie die sonstigen Kriterien des § 3 Abs. 1 BVerfSchG – insbesondere des gewaltgeneigten Extremismus – nicht erfüllen. Nach der Begründung des Gesetzentwurfs der Bundesregierung soll die Tätigkeit des Bundesamtes bereits weit im Vorfeld terroristischer Bestrebungen ansetzen, nämlich bei Bestrebungen, die „den Nährboden für die Entstehung extremistischer Auffassungen bilden“ können.

Bezweckt ist nach der Begründung allerdings vor allem die Lockerung des bislang vorausgesetzten Inlandsbezuges der geplanten oder durchgeführten Gewaltanwendung extremistischer Gruppierungen. Über dieses durchaus nachvollziehbare Anliegen, dem durch eine Erweiterung der Ziff. 2 und 3 des § 3 Abs. 1 BVerfSchG auf Schutzgüter im Ausland Rechnung getragen werden könnte, geht die vorgeschlagene Formulierung jedoch weit hinaus. Als Folge sind **ausufernde Datensammlungen** der Bundesverfassungsschutzbehörde zu befürchten, die gerade keine Konzentration geheimdienstlicher Aufklärung auf den eindeutig gewaltorientierten islamischen Extremismus mit sich bringen.

Auch der Aufgabenbereich des **Militärischen Abschirmdienstes (MAD)** soll entsprechend erweitert werden (Art. 2 Nr. 1 des Entwurfs). Hiergegen bestehen dieselben Bedenken.

1.2 Das Bundesamt für Verfassungsschutz soll umfangreiche **Auskunftsbefugnisse u.a. gegenüber Banken, Post-, Telekommunikations-, Flug- und Teledienste- sowie Luftfahrtunternehmen** erhalten, die die einzelnen Kontobewegungen sowie Kommunikationsverbindungen umfassen. Zwar sind die tatbestandlichen Voraussetzungen für solche Auskunftsersuchen gegenüber dem ursprünglichen Entwurf deutlich angehoben worden, indem tatsächliche Anhaltspunkte für qualifizierte Gefahren verlangt werden bzw. im Bereich der Kommunikation auf die Voraussetzungen des § 3 Abs. 1 des G 10 verwiesen wird. Dennoch bewegen sich die geplanten Befugnisse in einem typischerweise polizeilichen Bereich konkreter Ermittlungen zu individuellen Verhaltensweisen und weniger im Bereich der geheimdienstlichen Strukturinformationen. Die verfassungsrechtlich gebotene **Trennung von Polizei und Geheimdiensten** wird hierdurch – wie bereits bei den individualbezogenen Abhörbefugnissen des BND – angesichts der Übermittlungsmöglichkeiten an die Polizei weiter aufgeweicht. Außerdem sind parallele Ermittlungen und in diesem Zuge doppelte Grundrechtseingriffe durch Polizei und Verfassungsschutz zu befürchten. Zu berücksichtigen sind auch faktisch diskriminierende Auswirkungen für die Betroffenen insbesondere, wenn sich ein Geheimdienst bei Kre-

ditunternehmen über Konten und Transaktionen einer Person erkundigt, ohne dass ein strafrechtlicher Anfangsverdacht vorliegen muss.

Immerhin unterstellt der Entwurf nun die kommunikationsbezogenen Auskunftsbefugnisse zumindest partiell den Voraussetzungen des G 10. Nach der Rechtsprechung des Bundesverfassungsgerichts unterliegen auch die näheren Umstände der Kommunikation dem Fernmeldegeheimnis. Alle Eingriffsbefugnisse in Bezug auf Art. 10 GG sollten daher innerhalb des G 10 und nicht – wie hier geplant – unmittelbar im Bundesverfassungsschutzgesetz angesiedelt werden, um ein **rechtssystematisch einheitliches System** der materiellen Voraussetzungen, des Anordnungsverfahrens, der Datenverarbeitungsbefugnisse und ihrer Kontrolle zu Gewähr leisten. Auch innerhalb des G 10 sind sachgerechte Abstufungen in Bezug auf Inhalts- und Verbindungsdaten möglich.

1.3 Auch der **Militärische Abschirmdienst** und der **Bundesnachrichtendienst** (BND) sollen entsprechende Auskunftsbefugnisse gegenüber Telekommunikations- und Teledienstebetreibern sowie gegenüber Kreditinstituten, Finanz- und Finanzdienstleistungsunternehmen (BND) bekommen.

1.4 Die bislang rechtlich umstrittene Zulässigkeit des Einsatzes des sog. **IMSI-Catchers** soll auch bei bloßem Stand-by-Betrieb von Mobilfunkendgeräten durch eine entsprechende gesetzliche Befugnis des Bundesamtes für den Verfassungsschutz geregelt werden. Sie soll die Ermittlung des Standortes einer Person und der von ihr verwandten Geräte- und Kartennummer ermöglichen.

Gegen den Einsatz des IMSI-Catchers bestehen gravierende datenschutzrechtliche Bedenken. Technisch bedingt greift dieses Gerät besonders intensiv in die **Kommunikationsrechte Dritter** ein, die während der Zeit seines Einsatzes im Sendebereich des IMSI-Catchers keine Gespräche führen können und deren Daten zunächst ebenfalls mit abgefangen werden. Mit der Legitimierung des staatlichen Einsatzes von IMSI-Catchern wird eine Technik gefördert und sozusagen „salonfähig“ gemacht, die etwa im Bereich der Wirtschaftskriminalität von hohem Interesse ist, da es mit ihr nach dem gegenwärtigen technischen Standard auch möglich ist, die Verschlüsselung von Gesprächen auszuschalten und Inhalte abzuhören. Die technische Option des Abhörmodus würde im Übrigen – sofern der IMSI-Catcher auch von der Polizei eingesetzt werden dürfte, was allerdings in zunehmendem Maße bereits jetzt ohne gesetzliche Grundlage geschieht – auch absehbar zu einer weiteren Steigerung der Zahl staatlicher Telekommunikationsüberwachungen führen.

Nach der Begründung des Regierungsentwurfs soll mit dem IMSI-Catcher lediglich die Anschlussnummer für Maßnahmen der Telefonüberwachung nach dem G 10 ermittelt und damit die Voraussetzung für deren Anordnung geschaffen werden. Auch diese Befugnis soll jedoch nicht im G 10, sondern außerhalb dieses Regelungszusammenhangs in § 9 BVerfSchG eingefügt werden. Nach ihrem Wortlaut soll der IMSI-Catcher zur Ermittlung des Standorts einer überwachten Person über die Vorbereitung von G 10-Anordnungen hinaus allgemein zur Erfüllung der Aufgaben des Bundesamtes für Verfassungsschutz (mit Ausnahme des § 3 Abs. 1 Nr. 1 BVerfSchG) eingesetzt werden.

Damit wird jedoch die Regelungsintention weit überschritten.

Angesichts des hohen Ausstattungsgrades der Bevölkerung mit Mobiltelefonen wäre zu befürchten, dass die Erstellung und Auswertung von **Bewegungsbildern** von Personen mit aktiv geschaltetem Handy zu einer Standardermittlungsmethode zunächst der Verfassungsschutzbehörde würde.

Wie entsprechende Anträge im Bundesrat zeigen, würde die Befugnis zur Einsatz eines IMSI-Catchers mit hoher Wahrscheinlichkeit – wenn nicht bereits mit dem vorliegenden Sicherheitspaket – in einem nächsten gesetzgeberischen Schritt auch den **Strafverfolgungsbehörden** zuerkannt. Es ergäbe sich insgesamt eine neue Qualität der immer vollständigeren staatlichen Überwachbarkeit des Aufenthaltsortes von Personen, die durch Aktivschaltung ihres Mobiltelefons erreichbar sein wollen. Betrachtet man die heranwachsende Generation der heute Jugendlichen, dann wird deutlich, welches Ausmaß diese aus Sicht der Betroffenen unerwünschte „**Nebenwirkung**“ der **Teilnahme an der Informationsgesellschaft** bereits in wenigen Jahren erreichen würde.

1.5 Schwer nachvollziehbar ist, dass in § 12 Abs. 3 S. 2 BVerfSchG die **Löschfrist** für Speicherungen über terroristische und vor allem über gegen die Völkerverständigung gerichtete Bestrebungen von zehn auf fünfzehn Jahre seit dem Zeitpunkt der letzten gespeicherten relevanten Information verlängert werden soll. Es muss bezweifelt werden, dass eine Information nach einer so langen Zeit ohne weitere hinzugekommene Erkenntnisse noch von Aktualität und Bedeutung für die Terrorismusbekämpfung sein kann. Die Anwendung einer Fünfzehn-Jahre-Frist auf die in das Extremismusvorfeld hineinreichenden Bestrebungen gegen die Völkerverständigung (s.o. 1.) erscheint besonders problematisch.

2. Art. 5 – Änderung des Sicherheitsüberprüfungsgesetzes

Durch die Einfügung von Regelungen über die **Sicherheitsüberprüfung zu Zwecken des personellen Sabotageschutzes** in das Sicherheitsüberprüfungsgesetz des Bundes (SÜG) soll im Zuständigkeitsbereich des Bundes die einfache Sicherheitsüberprüfung auf Personen erstreckt werden, die an sicherheitsempfindlichen Stellen bestimmter lebens- oder verteidigungswichtiger Einrichtungen tätig sind. Die vorgeschlagene Regelung erscheint grundsätzlich nachvollziehbar und im Verhältnis zu den Gefahren des extremistischen Terrorismus, die sich am 11. September manifestiert haben, prinzipiell angemessen. Allerdings sollten die **wesentlichen Festlegungen**, welche Bereiche innerhalb welcher Einrichtungen unter den Anwendungsbereich des SÜG fallen, **im Gesetz** selbst geleistet werden, um im Volumen ausufernden Überprüfungen im gesamten Versorgungsbereich vorzubeugen. Ferner sollte eine Einbeziehung des Lebens-/Ehepartners in die Überprüfung zu Zwecken des personellen Sabotageschutzes aus Gründen der Verhältnismäßigkeit ausgeschlossen werden. Sicherheitsbeeinträchtigende Einwirkungen des Partners auf die beschäftigte Person sind eher im Bereich des Verschlusssachenschutzes denkbar; außerdem ist der Kreis der von der Erweiterung des SÜG Betroffenen ohnehin sehr groß.

3. Art. 10 – Änderung des Bundeskriminalamtgesetzes

Gegenüber einer Erweiterung der Datenerhebungsbefugnisse des BKA innerhalb des § 7 Abs. 2 Bundeskriminalamtgesetz (BKAG) bestehen erhebliche datenschutzrechtliche Bedenken. Der Regierungsentwurf beabsichtigt, die **Funktion des BKA als Zentralstelle zu erweitern**, indem es unabhängig von den Länderpolizeien und den dort möglicherweise bereits vorhandenen Daten bei sämtlichen öffentlichen oder nichtöffentlichen Stellen Informationen originär erheben darf, um vorhandene Sachverhalte zu ergänzen oder sonst zu „Auswertungszwecken". Die Erhebung wird im Gesetz auch nicht mehr als Ersuchen bezeichnet, wodurch aufseiten der angesprochenen Stelle der Eindruck einer Verpflichtung zur Datenübermittlung erweckt wird, ohne dass dies allerdings ausdrücklich gesetzlich vorgesehen wäre.

Durch die geplante Regelung würde die Rolle des BKA in einer Weise gestärkt, die der grundgesetzlichen Kompetenzverteilung auf dem Gebiet des Polizeirechts nicht mehr entspräche. Dem BKA würde eine **Grauzone präventiver Ermittlungen** eröffnet, in der eine Koordination mit den originär zuständigen Länderpolizeien bei der Datenerhebung nicht mehr in jedem Falle stattfände. Dies ginge weit über das bisherige Verständnis der Zentralstellenfunktion des BKA hinaus und hätte zwangsläufig Doppelerhebungen personenbezogener Daten von Bund und Ländern an Stelle der notwendigen Bündelung und Koordinierung polizeilicher Informationssammlungen zur Folge. Um die Betroffenen so schonend wie möglich zu belasten, müssen innerhalb der Polizei bereits vorhandene Daten auf Grundlage der hierfür vorhandenen Übermittlungsbefugnisse des BKAG und der Landespolizeigesetze genutzt werden, bevor Anfragen an dritte Stellen getätigt werden. Zudem wird das BKA häufig nicht erkennen können, ob in einem Land bereits Strafermittlungsverfahren gegen die sie interessierende Person laufen, sodass auch die justizielle Aufsicht über Datenerhebungen gem. § 7 Abs. 2 S. 3 BKAG leerliefe.

4. Art. 18 – Änderung des Zehnten Buches Sozialgesetzbuch

Völlig inakzeptabel ist der generelle **Ausschluss des Schutzes von Sozialdaten gegenüber Maßnahmen der Rasterfahndung**, der in Gestalt eines § 68 Abs. 3 SGB X festgeschrieben werden soll: Sozialdaten gehören zu den sensibelsten Daten in staatlicher Verfügungsgewalt und reichen insbesondere im medizinischen Bereich weit in die Persönlichkeitssphäre des Einzelnen hinein. Es erscheint nicht vertretbar, diese dem besonderen Schutz des Staates anvertrauten Daten über die bisherigen, genau abgestuften Möglichkeiten polizeilicher Einzelfallermittlungen hinaus in eine Maßnahme wie die Rasterfahndung einzubeziehen, die vom Ansatz her notwendigerweise zu einem überwiegenden Anteil rechtstreue Bürger erfasst. Bei der Übermittlung von Sozialdaten an Sicherheitsbehörden müssen Einzelfallerwägungen immer eine Rolle spielen können.

Es konterkariert die **verfassungsrechtliche Aufgabe des Sozialstaates**, wenn Bürger in eine u.U. für sie folgenschwere Maßnahme wie die Rasterfahndung mit den sich anschließenden Maßnahmen polizeilicher Ermittlungen dadurch geraten können, dass sie durch die Wahrnehmung staatlicher Sozialvorsorge ein - für sie völlig intransparentes - Unterscheidungskriterium geliefert haben. Sofern Sozialdaten eine wesentliche Rolle bei der Ermittlung einer (potenziellen) Tätergruppe spielen, müssen sie nach der Phase des maschinellen Abgleiches der Rasterfahndungsdaten erforderlichenfalls in konventioneller Weise zu den relevanten Personen auf Grundlage des bestehenden § 68 Abs. 1 SGB X beigezogen und verwertet werden.

II. Zu den Vorschlägen des Bundesrates

Der Bundesrat fordert in seinem Beschluss vom 30.11.2001 noch **weitere Verschärfungen des Gesetzespakets**. Damit soll offenbar der gegenwärtige Zeitdruck, unter den das Sicherheitspaket der Bundesregierung gesetzt wird, ausgenutzt werden, um dem Gesetzgeber weitere Posten aus den Wunschzetteln der Sicherheitsbehörden abzuringen. Positiv ist allerdings zu bewerten, dass der Bundesrat eine Erweiterung der Datenerhebungsbefugnisse des BKA als Zentralstelle ablehnt.

1. Die bedeutsamsten Verschärfungen durch den Bundesrat sind:

1.1 Schon **Kinder ab 14 Jahren** sollen in den **Dateien des Verfassungsschutzes** gespeichert werden dürfen. Bislang schützt die Altersgrenze von 16 Jahren vor einer Dateispeicherung der Aktivitäten von Kindern. Ein Zusammenhang mit der Bekämpfung hochorganisierten islamischen Terrorismus ist bei diesem Vorstoß nicht erkennbar.

1.2 Die bereits im Gesetzgebungsverfahren befindliche Nachfolgeregelung zu § 12 FAG betreffend die Zulässigkeit einer Übermittlung von **Telekommunikationsverbindungsdaten** zu Strafverfolgungszwecken soll mit dem Argument auf Eis gelegt werden, dass eine Einschränkung der Auswertungsmöglichkeiten der Polizei gegenüber der bisherigen Regelung zurzeit „nicht vermittelbar" sei. Stattdessen müssten den Betreibern **Aufzeichnungspflichten** hinsichtlich der anfallenden Verbindungs- und der **Standortdaten** auch bei bloßem Stand-by-Betrieb eines Gerätes auferlegt werden.

1.3 Die **Staatsanwaltschaften** sollen Zugang zu **polizeilichen Dateien** haben. Der gesetzliche Formulierungsvorschlag erfasst über die in der Begründung aufgeführten Fahndungs-, Haft- und DNA-Dateien hinaus potenziell alle Dateien und sieht nur eine Ausschlussmöglichkeit vor. Eine Trennung der Verarbeitungszwecke Strafverfolgung und Gefahrenabwehr würde nach diesem Vorschlag faktisch nicht mehr existieren. Auf die justizielle Kontrolle von rein strafverfolgenden Daten der Polizei beschränkt wäre der Vorschlag des Bundesrates allerdings durchaus nachvollziehbar.

1.4 Umgekehrt soll die **Polizei Online-Zugriff auf das Zentrale Staatsanwaltschaftliche Verfahrensregister** bekommen. Zur Begründung wird schlicht auf den Bericht einer Länderarbeitsgruppe verwiesen.

1.5 Nicht nur das Bundesamt für Verfassungsschutz, sondern auch die jeweiligen **Landesämter für Verfassungsschutz** sollen die teilweise hochsensiblen und aus Asylverfahren stammenden Daten über die politische Betätigung von Ausländern in den Asyl- und Ausländerbehörden erhalten.

1.6 Vor der Erteilung von unbefristeten Aufenthaltserlaubnissen oder Aufenthaltsberechtigungen kann nicht nur, sondern muss eine **Regelanfrage** bei sämtlichen Sicherheitsbehörden durchgeführt werden, wenn dies „geboten ist".

1.7 Weitere **Löschungsfristen** sollen um viele Jahre verlängert werden, und zwar bei Menschen, die sich einbürgern ließen oder bei Visa-Antragstellern, weil dies „für die Bekämpfung politisch motivierter Ausländerkriminalität unverzichtbar" wäre.

2. Weitere Pläne in der Schublade

Mit einem **Gesetzentwurf Bayerns und Thüringens** liegen bereits weitere Forderungen nach dem Abbau von Grundrechten auf dem Tisch: Wie vorauszusehen (s.o.), sollen, sobald die Befugnis für den Verfassungsschutz durchgesetzt ist, auch Strafverfolgungsbehörden die Befugnis zum Einsatz des **IMSI-Catchers** bekommen. Außerdem sollen Telekommunikations- und Teledienstebetreiber zur **Vorratsdatenspeicherung von Verbindungsdaten** verpflichtet werden. Zu dem letzteren Vorstoß haben sich die Datenschutzbeauftragten wiederholt deutlich ablehnend geäußert. Es wäre unverantwortlich, eine solche Weichenstellung für das Verhältnis zwischen Informations- und Kommunikationsgrundrechten und Bedürfnissen der Sicherheitsbehörden im Zusammenhang der kurzfristigen Maßnahmen zur Terrorismusbekämpfung zu treffen, da eine sachgerechte Abwägung mit Betroffenenbelangen gegenwärtig kaum möglich ist. Eine Vorratsdatenspeicherung in dieser Form wäre verfassungswidrig. Auch wenn der Antrag Bayerns und Thüringens diesmal noch keine Mehrheit fand, kann nach allen bisherigen Erfahrungen davon ausgegangen werden, dass er bei jeder sich bietenden Gelegenheit solange wiederholt wird, bis das politische Klima für seine Annahme besteht.

III. Datenschutzrechtliche Positionen zu biometrischen Verfahren für den Masseneinsatz

Das ULD Schleswig-Holstein beschäftigt sich seit einigen Jahren mit dem Themenkomplex Biometrie, u.a. im Rahmen des Projektes "BioTrusT", das vom BMWi gefördert wird. **BioTrusT** untersucht biometrische Anwendungen im Bereich von Banken. Wegen der großen Anzahl von Bankkunden sind die Problemfelder des Bankenbereichs mit denen staatlicher Anwendungen zu vergleichen; die zum Einsatz kommende Technik ist ohnehin gleich.

Mit dem Begriff *Biometrie* oder *biometrische Verfahren* werden Verfahren zur automatisierten Erfassung und Auswertung personenbezogener Körpermerkmale und personenbezogenen Verhaltens von Personen bezeichnet, um diese automatisiert (wieder)erkennen zu können. Zu den zum gegenwärtigen Zeitpunkt auswertbaren Merkmalen zählen u.a. Fingerabdruck, Handflächenabdruck, Handvenenmuster, Geometrie der Hand, Irismuster (Muster der Regenbogenhaut), Retinamuster (Muster des Augenhintergrunds), Gesichtsgeometrie, Stimme, Lippenbewegung, (Unter)Schrift sowie das Tippverhalten auf einer Tastatur. Eine vollautomatische Auswertung von menschlicher DNA ist derzeit (noch) nicht möglich.

Bislang wurden beim ULD im Rahmen der Beschäftigung mit dem Themenkomplex Biometrie folgende **datenschutzrechtliche Positionen** erarbeitet:

1. Keine unbemerkte Erhebung biometrischer Daten:

Biometrische Verfahren für den Masseneinsatz müssen so konstruiert sein, dass sie die Daten nicht unbemerkt erfassen, sondern vielmehr der Betroffene Kenntnis von der Anwendung hat. Daher ist auf die verdeckte Sprecher- oder Gesichtserkennung sowie auf die verdeckte biometrische Auswertung anderer Daten (z.B. Unterschriften) zu verzichten. Dies gebietet schon das allgemeine **Transparenzgebot bei der Datenverarbeitung**; außerdem haben Betroffene andernfalls keine Chance, sich einem einwilligungsbedürftigen Verfahren zu entziehen. Es sind deshalb biometrische Verfahren vorzuziehen, die eine **aktive Mitwirkung** erfordern und dadurch eine verdeckte Erfassung biometrischer Merkmale nicht oder nur unter erschwerten Bedingungen zulassen. Dazu gehören nach derzeitigem Kenntnisstand in erster Linie solche Verfahren, die einen Körperkontakt oder eine spezielle Haltung des Körpers ("Aufnahmeposition") erfordern, etwa Hand- und Fingerabdruckverfahren, Handgeometrie, Handvenenmuster, Iris- und Retinaerkennung, sowie verhaltensbasierte Merkmale wie die Schriftdynamik. Es ist aber damit zu rechnen, dass sich die Verhältnisse durch technische Weiterentwicklung, etwa bei der Iriserkennung, ändern und weitere Merkmale unbemerkt erfasst werden können.

2. Keine Speicherung von Referenzdaten außerhalb der Verfügungsgewalt der Betroffenen

Wegen des hohen Missbrauchspotenzials und der Unabänderbarkeit[1] der biometrischen Daten sollten Referenzdaten weder zentral noch in einer anderen für Unbefugte zugänglichen Form gespeichert werden. Die **Betroffenen** müssen die **alleinige Verfügungsgewalt** über ihre Daten behalten. Dies beinhaltet auch den Verzicht auf dezentrale Register und Dateien (die technisch problemlos zusammengeführt werden könnten), aber auch auf Zwischenspeicherungen und Protokollierungen biometrischer Daten zu Kontrollzwecken. Andernfalls besteht die **Gefahr einer Zweckentfremdung** dieses Datenbestandes. Eine Speicherung biometrischer Daten bei Pass- und Ausweisbehörden (analog zu den Ausweisbildern) ist deshalb - nicht zuletzt wegen der mit der Nutzung dieser Bilder selbst in Ordnungswidrigkeitenverfahren gemachten Erfahrungen - abzulehnen. Zum Schutz gegen unerkannte Veränderungen und Verfälschungen biometrischer Referenzdaten in Ausweisen bieten sich digitale Signaturen an.

3. Nebenwirkungsfreie Verfahren

Es müssen Verfahren und Verfahrensgestaltungen gewählt werden, die nebenwirkungsfrei sind bzw. Nebenwirkungen minimieren. Dazu gehört der **Verzicht auf die Speicherung von Rohdaten** (die medizinische oder sonstige sensible Informationen enthalten können) und der Verzicht auf die Verwendung von Merkmalen, die für kriminalistische Zwecke genutzt werden können, um eine **Vermischung** dieser verschiedenen **Anwendungszwecke** von vornherein **auszuschließen**. Daraus folgt, dass biometrische Verfahren wie die Handgeometrie-, Handvenen- oder Iriserkennung der Verwendung von Finger-, Handlinien-, Gesichts- oder Sprechererkennungsverfahren vorzuziehen sind. Die Gewinnung von Zusatzinformationen bei der Durchführung von Identitätskontrollen sollte generell gesetzlich untersagt werden, da sich in Zukunft neue, heute nicht vorhersehbare Möglichkeiten ergeben werden, aus den biometrischen Daten zusätzliche Informationen zu gewinnen.

4. Rechtsfolgen

Es muss beachtet werden, dass die Entscheidungen biometrischer Verfahren nur im Rahmen einer gewissen Schwankungsbreite korrekt sind. Die Genauigkeit hängt vom biometrischen Merkmal, dem eingesetzten Verfahren und nicht

[1] Auch die sogenannten verhaltensbasierten Merkmale wie Schriftdynamik und Sprache, die durch Schreiben oder Sprechen verschiedener Worte verändert werden können, weisen unveränderbare personenspezifische Anteile auf.

zuletzt von den Parametereinstellungen ab. Es darf deshalb **kein blindes Vertrauen** in die **biometrische Technik** geben. Insbesondere müssen die Ergebnisse biometrischer Entscheidungen überprüft werden (können), wenn sich negative rechtliche Folgen (z.B. Abschiebung von Asylbewerbern) ergeben. Notwendig ist deshalb ein Recht des Nutzers auf Zugang zu seinen Daten und die Möglichkeit der Überprüfung, ob es sich um *seine* Datensätze handelt. Anders als die in herkömmlichen Ausweisen verwendeten Daten (Name, Lichtbild, Unterschrift, etc.) lassen sich biometrische Merkmale in den meisten Fällen nicht manuell überprüfen. Für eine wirksame Überprüfung durch den Nutzer müssen ihm deshalb genau die technischen Verfahren (mit gleichen Parametereinstellungen) zur Verfügung gestellt werden, die auch sonst bei der Identitätsüberprüfung eingesetzt werden.

5. Systemsicherheit und Revisionsmöglichkeiten

Es ist zu erwarten, dass biometrische Verfahren in den kommenden Jahren auch außerhalb des Zwecks der Identitätsfeststellung zur Anwendung kommen. Denkbar und zum Teil umgesetzt sind die Zugangssicherung zu Computern und Geldautomaten und der Einsatz im Rahmen von digitalen Signaturen. Ein Einsatz biometrischer Daten zu Zwecken der Datensicherheit kann aus Datenschutzgründen sogar sinnvoll sein, weil sie wegen ihrer bequemen Anwendung auf eine hohe Akzeptanz stoßen könnten. Ein **Missbrauch** biometrischer Verfahren und Daten kann für die Betroffenen aber **fatale Folgen** haben. Deshalb und weil biometrische Verfahren nicht automatisch sicherer sind (ihre Sicherheit hängt zum einen von der Sicherheit des Gesamtsystems, aber auch entscheidend von Parametereinstellung und Konfiguration ab), sind **Revisionsmöglichkeiten** vorzusehen, um Manipulationen entdecken oder verhindern zu können.

6. Rückfallpositionen und Auswege aus biometrischen Verfahren

Es müssen sinnvolle Alternativen vorgesehen sein, wenn biometrische Verfahren nicht so wie vorgesehen funktionieren oder Fehlentscheidungen produzieren. Dazu gehören **Ausweichverfahren**, wenn einzelne biometrische Merkmale von Personen nicht erfassbar sind (Vermeidung von Diskriminierungen), aber auch Prozeduren, die mit Falscherkennungen und Fehlfunktionen der biometrischen Systeme umgehen. Generell müssen Systeme und Abläufe so gestaltet werden, dass **Alternativen** möglich sind, wenn sich eingeführte biometrische Verfahren als ungeeignet (z.B. durch mangelnde Robustheit, erheblich höhere Kosten als erwartet, etc.) erweisen; es darf nicht aus Mangel an Alternativen an ungeeigneten oder risikobehafteten Verfahren festgehalten werden.

7. Fazit

Zusammenfassend lässt sich feststellen, dass den großen Risiken, die biometrische Massenverfahren bergen können, nur durch eine sinnvolle, abwägende Auswahl der biometrischen Merkmale und durch sorgfältige Gestaltung des technischen und organisatorischen Umfeldes begegnet werden kann. Von den betrachteten biometrischen Merkmalen scheinen unter Datenschutzgesichtspunkten die **Handgeometrie** und die **Schriftdynamik** die wenigsten riskanten Nebenwirkungen aufzuweisen.

IV. Hintergrundinformationen zu biometrischen Verfahren

1. Technik

Die Erfassung biometrischer Merkmale erfolgt mit Hilfe sensorähnlicher Geräte (z.B. Kameras, Mikrofonen, Tastaturen, Fingerabdrucksensoren). Ein Teil der dabei erzeugten **Rohdaten** (z.B. Tonaufnahmen, Videoaufnahmen) erlaubt eine unmittelbare Wiedererkennung durch Menschen – z.B. beim Anhören von Sprachaufnahmen mit Lautsprechern oder dem Betrachten von Videoaufnahmen eines Gesichts. Für eine weitere Gruppe von Rohdaten ist eine unmittelbare Interpretation nur bedingt möglich (z.B. bei Bildern von Fingerabdrücken, die eine Identifizierung erst mit Hilfe von Vergleichsmustern ermöglichen). Wieder andere Rohdaten können nicht direkt interpretiert werden, z.B. Thermo-Gesichtsaufnahmen oder die Sensordaten eines (Unter-) Schriftensensors, der Schreibdruck und der Schreibgeschwindigkeit erfasst.

Die so gewonnen Rohdaten werden weiterverarbeitet und ein sog. **Template** erzeugt. Dies ist ein kleiner Datensatz, der Parameter eines mathematischen Modells der Rohdaten enthält, beispielsweise Koordinaten von sog. Minutien (u.a. Verzweigungen oder Enden von Fingerabdrucklinien) bei Fingerabdrükken. Er enthält (in komprimierter Form) die für einen Vergleich notwendigen Daten, erlaubt aber üblicherweise keine unmittelbaren Rückschlüsse auf die Rohdaten der Person. Ein solches Template wird bei der erstmaligen Benutzung des Gerätes, dem **Einlernen (Enrollment)**, gespeichert. Bei allen weiteren Benutzungen des Gerätes werden wiederum Rohdaten erfasst und aus ihnen ein Template berechnet. Ein Vergleichsalgorithmus überprüft, ob dieses Template mit dem abgespeicherten übereinstimmt. Ist dies der Fall, meldet das Gerät ein positives Ergebnis.

Es gibt zwei grundsätzliche Betriebsarten, die stark mit der jeweiligen Anwendung zusammenhängen: **Verifikation** und **Identifikation**: Bei der *Verifikation* wird in einem 1:1-Vergleich die Identität eines Benutzers geprüft, indem die aktuell präsentierten Daten mit *(s)einem* Template verglichen werden. Die *Identifikation* vergleicht das Template des aktuellen Benutzers mit *allen* gespeicherten Templates aller eingelernten Benutzer (1:n-Vergleich) und liefert als Ergebnis die Nutzerkennung (Identitätsnummer o.ä.) desjenigen Benutzers aus dem Datenbestand zurück, dessen Template am besten mit dem des aktuellen Benutzers übereinstimmt; ggf. wird eine Auswahl zur manuellen Entscheidung vorgelegt.

Für Identifikationsverfahren ist eine **zentrale Speicherung** aller biometrischen Daten in einer Datenbank erforderlich, da beim Vergleich auf alle Daten zurückgegriffen werden muss. Für Verifikationsverfahren, die einen 1:1-Vergleich vornehmen, genügt eine dezentrale Speicherung auf Datenträgern (z.B. auf Chipkarten, Ausdruck eines Barcodes etc.), die im Einflussbereich der Benutzer verbleiben können.

2. Ziele und Einsatzbereiche

Die Ziele bei der Anwendung biometrischer Verfahren sind mannigfaltig:

- Rationalisierung durch Automatisierung
  - Beschleunigung (z.B. schnellere Personenkontrolle an Flughäfen)
  - Ausweitung von Kontrollen und Überwachungen (z.B. automatisierter Datenabgleich zur Vermeidung mehrfacher Inanspruchnahme von Leistungen, automatisierte Fahndung nach Personen in Menschengruppen)
- Erhöhung der Sicherheit im Vergleich zu einem manuellen Abgleich biometrischer Daten [z.B. Passbild] oder anderen Zugangskontrollverfahren [PINs, Passwörter, Ausweise etc.] Gefahr der Weitergabe!)
- Komfortgewinn (kein Merken von Passwörtern oder Mitführen von Codekarten)

Ebenso zahlreich sind die (potenziellen) Anwendungsgebiete biometrischer Verfahren:

- Automatisierung/Beschleunigung von Ausweiskontrollen [Zutrittskontrollen zu Flughafenbereichen, (Hoch)Sicherheitsbereichen, Grenzkontrollen etc.]
- Ausgabe von Ausweisen, Visa etc. [Vermeidung von Doppelausgaben]
- automatisierte Überwachung [z.B. Kopplung von Videoanlagen mit Gesichtserkennungsverfahren, sowohl im öffentlichen als auch im privaten Bereich]
- Zugang zu Computern und Dateien; Freischaltung elektronischer Signaturen
- Eintritt zu Vergnügungsparks für Dauerkarteninhaber [Unterbindung der Weitergabe von Dauerkarten]
- Online-Verkauf von Tickets [ticketlose biometrische Zugangserlaubnis nach Online-Abwicklung von Geschäften]

3. Problemfelder

3.1 Entscheidungsqualität

Da die Rohdaten mit Messfehlern behaftet sind oder sich im Laufe der Zeit ändern (Stimmbruch, Frisuränderung, Verletzung am Finger etc.), sind auch

die entsprechenden Templates nicht hundertprozentig gleich. Beim Vergleich (**Matching)** muss dies berücksichtigt werden: Mittels eines Parameters kann eingestellt werden, ab welchem Übereinstimmungsgrad eine positive Identifikation gemeldet werden soll.[2] Die **Wahl dieses Parameters** beeinflusst ganz entscheidend die Güte der biometrischen Erkennung, d.h. den Prozentsatz von Falschentscheidungen. Die gemeldeten Ergebnisse des Vergleiches können in zweierlei Hinsicht fehlerhaft sein:

- die Messwerte *einer* Person unterscheiden sich so stark, dass der Vergleichsalgorithmus fälschlicherweise „*keine Übereinstimmung"* meldet (Falschzurückweisung)

- die Messwerte *zweier* Personen ähneln sich so sehr, dass der Vergleichsalgorithmus fälschlicherweise „*Übereinstimmung"* meldet. (Falscherkennung)

Man kann durch Parameterwahl das System auf „scharf" (wenig Falscherkennungen, viele Falschzurückweisungen) oder auch „nicht so scharf" (wenig Falschzurückweisungen, viele Falscherkennungen) stellen. Wählt man den Parameter so, dass die Rate beider Fehler gleich ist, so ergeben sich bei vergleichenden Anwendungstests Fehlerraten zwischen 0.2 und 7% bei den meisten biometrischen Systemen, wenn man bis zu zwei Fehlversuche zulässt.[3]

Es ist zu beachten, dass nicht alle Menschen in alle Systeme eingelernt werden können: Abgesehen von offensichtlichen Fällen (wenn das biometrische Merkmal, wie etwa Sprechfähigkeit, nicht vorliegt) gibt es beispielsweise Probleme bei Fingerabdruckverfahren, weil sich die Fingerabdrücke bestimmter Personen nicht aufnehmen lassen. Dies kann temporär (z.B. aufgrund von körperlicher Arbeit), aber auch dauerhaft (Veränderungen der Haut) der Fall sein. Experten gehen von bis zu 2% **Problemfällen** aus.[4]

3.2 Zusatzgehalt biometrischer Daten

Aus biometrischen Rohdaten wie Aufnahmen von Gesicht, Sprache, Iris, Augenhintergrund und Fingerabdruck können **weitere Informationen über die betreffende Person** abgeleitet werden: Anhand des Gesichtes und der Sprache lassen sich Geschlecht, ungefähres Alter und Hinweise auf die ethnische Herkunft gewinnen. Aufnahmen des Augenhintergrundes lassen u.U. Diagnosen auf Krankheiten wie Arteriosklerose, Diabetes oder Bluthochdruck[5] zu. Bei

---

2 Dieses Verfahren wird auch in der Daktyloskopie angewendet: Zwei Fingerabdrücke gelten als gleich, wenn eine bestimmte Anzahl von Minutien, abhängig von der Größe und Qualität der Abdrücke übereinstimmt.

3 CESG/BWG Biometric Test Programme: Biometric Product Testing Final Report, abrufbar unter http://www.cesg.gov.uk/technology/biometrics/media/Biometric%20Test%20Report%20pt1.pdf [Stand 19.11.2001]

4 *Mansfield, T.*, „How to achieve test results in real-life", Vortrag bei der Biometrics 2000, 6.-8.11.2000, London: Fehlerraten bei der Rohdatenerfassung beim Enrollment und Betrieb 0-2%.

5 *Woodward, John D.* Biometric Scanning, Law & Policy: Identifying the concerns – drafting the Biometrics Blueprint. University of Pittsburgh Law Review, 1997, Fußnoten 70-72. Abrufbar unter http://lawreview.law.pitt.edu/index.htm

Fingerabdrücken scheint es statistische Korrelationen von Finger- und Handabdruckmustern mit Krankheiten wie chronische Magen-Darm-Beschwerden (CIP), Leukämie, Brustkrebs[6] und bestimmten vererbbaren Krankheiten[7] zu geben. Ebenso werden verschiedentlich Zusammenhänge zwischen bestimmten Fingerabdruckmustern und Homosexualität diskutiert. Auch wenn derartige Beziehungen nicht wissenschaftlich gesichert sind bzw. nur Aussagen hinsichtlich erhöhter Wahrscheinlichkeiten zulassen, können sie Diskriminierungen bewirken.

3.3 Eindeutige Personenkennziffer

Da biometrische Merkmale dauerhaft und willkürlich nur schwer veränderbar sind,[8] können sie als eine Art Personenkennziffer verwendet werden. Werden bei einer zentralen Speicherung personenbezogene Daten einer Person zusammen mit den jeweiligen Templates in verschiedenen Datenbanken gespeichert, so ist eine **Verknüpfung und Zusammenführung dieser Daten** mit Hilfe der Templates nicht ausgeschlossen – zumindest wenn die Templates auf gleiche biometrische Charakteristika (beispielsweise Fingerabdrücke) zurückgehen und mit Hilfe gleicher Algorithmen erstellt wurden oder ineinander konvertierbar sind. Werden Rohdaten direkt gespeichert, ist eine Konvertierung nicht notwendig, denn die Rohdaten in verschiedenen Datenbanken können direkt miteinander verglichen werden.

3.4 Sicherheitsproblematik

Die biometrischen Verfahren müssen gegen die Verwendung von gefälschten biometrischen Merkmalen, z.B. die Verstellung der Stimme, das Nachmachen einer Unterschrift, aber auch gegen **künstliche Fälschungen** (Artefakte) wie Fotos für Gesichtserkennungssysteme, Tonbandaufnahmen, Silikonabgüsse von Fingerabdrücken, Kontaktlinsen mit fremden Irismustern gesichert sein. Daneben müssen die Systeme gegen technische Angriffe, z.B. das Belauschen und Wiedereinspielen von biometrischen Daten in Datenleitungen des Systems, Manipulationen an den Erkennungsalgorithmen, Toleranzschwellen und Identitätsdaten der Benutzer geschützt werden.

---

6 *Woodward, John D.*, Identifying Law & Policy Concerns, S. 393, in*: Jain, A./Bolle, R./Pankati, S.* Biometrics: Personal Identification in Networked Society, Norvell 1999, S. 385-405.

7 z. B. Baffoe-Bonnie, B.: Dermatoglyphische Untersuchungen an Kindern mit Astma bronchiale und Neurodermitis. Mainz 1978, und Müller, E.: Dermatoglyphische Befunde bei Patienten mit fragilem X-Chromosom im Rahmen ihres klinischen Bildes. Hamburg 1985.

8 bestimmte, sog. *verhaltensbasierte Verfahren,* erfassen Merkmale wie die Aussprache oder Schreibweise von Worten; die Referenzdaten verändern sich mit der Änderung der Worte. Es gibt aber auch Spracherkennungsverfahren, die wortunabhängig arbeiten, vgl. auch Fußnote 1.

V. Biometrie auf Ausweisen: Möglichkeiten und Grenzen

1. Biometrische Informationen im derzeitigen Ausweissystem

Um die Auswirkungen der Ausstattung von Ausweispapieren mit biometrischen Merkmalen zu beurteilen, wird ein Vergleich mit dem heutigen Stand vorgenommen: Im Ausweis sind neben persönlichen Angaben wie Name, Geburtsdatum etc. auch Angaben über den Körper (Größe, Augenfarbe), ein Foto sowie eine Unterschrift enthalten. Dieselben Daten liegen als Kopie bei der ausstellenden Behörde (also dezentral) in einem Register vor und werden bei Auskunftsersuchen in bestimmtem Umfang übermittelt. Häufig werden dafür Datenbanken verwendet; je nach verwendeter Software kann dieses Register in unterschiedlichem Umfang (z.B. incl. Abbildung von Foto und Unterschrift) elektronisch geführt werden.

2. Denkbare Entwicklungen

Die Aufnahme biometrischer Daten in Ausweispapiere ist in unterschiedlichem Umfang denkbar:

- Biometrische Merkmale werden ausschließlich im Ausweis gespeichert.
- Biometrische Merkmale werden im Ausweis gespeichert, zusätzlich erfolgt eine dezentrale Speicherung bei den Melde- bzw. Ausländerbehörden in (elektronischen) Registern.
- Biometrische Merkmale werden im Ausweis gespeichert, zusätzlich erfolgt eine zentrale Speicherung der Daten.

Für die übrigen Daten (persönliche Angaben, Foto, Unterschrift) wird der derzeitige Stand (dezentrale Speicherung in Registern und Weitergabe von Daten nach bisherigen Verfahrensregeln) angenommen.

3. Mögliche Auswirkungen der Aufnahme biometrischer Daten in Ausweisen

Die Speicherung biometrischer Daten in **dezentralen Registern** würde die Verwendung zu strafrechtlichen Ermittlungszwecken und sog. "Rasterfahndungen" ermöglichen. Dies würde aber im Vergleich zu einer zentralen Speicherung kompliziertere technische Abläufe bedingen, da die vorhandenen Daten entweder dezentral ausgewertet werden oder zentral zusammengeführt werden müssten.

Eine wirksame Unterbindung von Ausweis-Doppelausstellungen ist allenfalls mit einem **zentralen Datenbestand** denkbar. Ein solches Verfahren findet heute schon als automatisiertes Fingerabdruckidentifikationssytsem (AFIS) Verwendung im Asylbereich. Parallelen gibt es auch mit der DNA-Datenbank des BKA - mit dem Unterschied, dass die Daten *aller* Bürger gespeichert wären und - wie eine Personenkennziffer - zur lückenlosen Identifizierung verwendet werden könnten.

Mit den zunehmenden Möglichkeiten einer Strafverfolgung durch umfassendere Datenbestände steigt das **Missbrauchs- und Schadenspotenzial**, etwa durch unbefugte Zugriffe auf die Datenbanken ("Hacking"). Werden zentrale Datenbestände angelegt, ist damit zu rechnen, dass nicht nur Strafverfolgungsbehörden, sondern auch Unbefugte Zugriff auf diese Bestände haben werden. Zusätzlich muss bedacht werden, dass sich einige Missbrauchs- und **Fälschungsmöglichkeiten** nicht auf technischem Wege ausschließen lassen (z.B. bewusste Fehleingaben) und wegen der Vielzahl der Beteiligten (etliche tausend Mitarbeiter bei den Meldebehörden etc.) nicht ausgeschlossen werden kann, dass es auf dem Wege der Erpressung oder Bestechung zur Ausstellung falscher Ausweise kommt.

Ein einigermaßen wirksames System zur (internationalen) Terrorismusbekämpfung ist außerdem nur im **weltweiten Verbund** denkbar; dies würde die Vernetzung aller nationalen Behörden erfordern oder die Erhebung und Speicherung biometrischer Daten bei allen denjenigen ausländischen Einreisenden, die keine biometrischen Informationen in ihren Reisepapieren gespeichert hätten.

Aus den seit den 70-er Jahren im Bereich der Terrorismusfahndung gewonnenen Erfahrungen lässt sich die Erwartung ableiten, dass ein einmal eingerichteter öffentlicher oder überregionaler Datenbestand trotz zunächst enger Zweckbestimmung auf Dauer **auch für andere Zwecke** genutzt wird. Druck der Medien als auch außenpolitischer Druck kann dazu führen, dass derzeit kaum vorstellbare und in der Öffentlichkeit nicht konsensfähige Verwendungen in Betracht kommen. Zusammenfassend läßt sich feststellen, dass für eine automatisierte Ausweisprüfung und eine verbesserte Zuordnung von Personen und vorgelegten Ausweisen eine Speicherung der biometrischen Daten **allein auf dem Ausweis** ausreichend ist.

VI. Zu den Änderungen im Bereich des Ausländerrechts

1. Grundsätzliches

Der Entwurf enthält keinen Vorschlag für **technisch oder sozial wirkende Prävention**. Mit solchen Vorschlägen wären nicht zwangsläufig Grundrechtseingriffe verbunden; ihre Wirksamkeit zur Terrorismusbekämpfung wäre jedoch kaum zu überschätzen.

Die Gesetzesbegründung verweist an vielen Stellen auf die **Resolution des UN-Sicherheitsrates** vom 28.09.2001 (Nr. 1373), die u.a. fordere, durch geeignete Maßnahmen

- die Identifizierung von Terroristen vor der Einreise,
- den Schutz von Identitätspapieren vor deren missbräuchlicher Verwendung,
- einen beschleunigten nationalen und grenzüberschreitenden Informationsaustausch über Terroristen und deren Bewegungen sowie über gefälschte Dokumente und
- die Verhinderung des Missbrauchs des Flüchtlingsstatus für terroristische Aktivitäten

sicherzustellen. Diese Resolution hat keine rechtliche Bindungswirkung für den nationalen Gesetzgeber. Sie ist derart allgemein gehalten, dass für deren Umsetzung unterschiedliche Wege beschritten werden können. In keinem Fall ist die Resolution in der Lage, die grundrechtlich und rechtsstaatlich begründeten Bindungen der deutschen Verfassung aufzuheben.

2. Artikel 1 – Änderung des Bundesverfassungsschutzgesetzes

Datenübermittlung vom Bundesamt für die Anerkennung und von den Ausländerbehörden an Verfassungsschutzbehörden (§ 9 Abs. 1a BVerfSchG)

Das Bundesamt für die Anerkennung ausländischer Flüchtlinge (BAFl) und die Ausländerbehörden (AuslB) der Länder sollen das Recht erhalten, von sich aus den Verfassungsschutzbehörden personenbezogene Informationen über Bestrebungen nach § 3 Abs. 1 BVerfSchG zu übermitteln, wenn sie Anhaltspunkte dafür haben, dass diese dort **zur Aufgabenerfüllung erforderlich** sind.

§ 3 Abs. 1 BVerfSchG beschränkt sich nicht auf die Terrorismusbekämpfung oder gewaltbereite Bestrebungen, die „auswärtige Belange der Bundesrepublik

Deutschland gefährden“, sondern schließt auch **bloße extremistische Bestrebungen** mit ein. Damit würde schon einfaches und legales politisches Engagement von Nichtdeutschen eine Datenweitergabe legitimieren. Mangels konkreter Kenntnis der geheimdienstlichen Gefährdungslagen besteht das Risiko, dass die Asyl- und Ausländerbehörden eher ein Übermaß an Daten übermitteln.

Von hoher Brisanz wäre diese Übermittlungsbefugnis für den Bereich des BAFl, da dieses bei der Entgegennahme der Begründungen von Asylanträgen sensible politische Informationen erfährt. Die Regelung würde die Befugnis eröffnen, die **Begründungen aus Asylanträgen** den deutschen Inlandsgeheimdiensten weiterzugeben. Die schutzwürdigen Belange von Asylsuchenden werden im Entwurf nicht erwähnt und müssten daher nicht berücksichtigt werden. Bei den Empfängern sollen diese sensiblen Daten keinen besonderen rechtlichen Regeln unterliegen. So ist nicht etwa vorgesehen, dass die erhaltenen Daten sofort auf ihre Relevanz geprüft und anderenfalls sofort gelöscht werden müssten. Eine besondere Zweckbindung (z.B. auf die Bekämpfung terroristischer Bestrebungen) oder ein Weiterübermittlungsverbot sind nicht vorgesehen.

Die erhaltenen Daten könnten so sogar an die Sicherheits- und Geheimdienstorgane des Heimatstaates, der auch der Verfolgerstaat sein kann, weitergegeben werden. Der Verweis auf die Generalklausel der überwiegenden schutzwürdigen Interessen der Betroffenen (§ 13 Abs. 3 S. 2 BVerfSchG) ist nicht geeignet, diese Gefahr zu bannen. Damit wird der in Art. 16a GG garantierte Schutz vor politischer Verfolgung verletzt. Wegen des Verstoßes gegen das aus dem Asylgrundrecht abzuleitenden **Asylgeheimnis** ist die geplante Regelung verfassungsrechtlich in dieser Form abzulehnen.

Der Übermittlungsbefugnis sollen keine adäquaten **Rechte der Betroffenen** gegenüber stehen. So sind z.B. die Auskunftsrechte der Betroffenen sehr beschränkt; eine Benachrichtigung soll nicht erfolgen.

3. Artikel 9, 12 – Änderung des Ausländergesetzes und des Asylverfahrensgesetzes

3.1 Ausländerausweise (§§ 5, 39 Abs. 1, 56a, 69 Abs. 2 AuslG, § 63 AsylVfG)

Als Aufenthaltsgenehmigung, als Ausweisersatz für Ausländer ohne Passpapiere, als Bescheinigung über die Duldung, als Bescheinigung einer Genehmigungsfiktion sowie als Bescheinigung über die Aufenthaltsgestattung für Asylsuchende sind nach vergleichbaren Gesichtspunkten geregelte **neue Dokumente** vorgesehen.

Diese Ausweisdokumente sollen unterschiedliche identifizierende Merkmale enthalten, u.a. neben dem Lichtbild und der eigenhändigen Unterschrift auch “**weitere biometrische Merkmale von Fingern oder Händen oder Gesicht**”

sowie eine "**Zone für das automatische Lesen**". Die Einzelheiten sollen vom Bundesinnenministerium „nach Maßgabe der gemeinschaftsrechtlichen Regelungen durch **Rechtsverordnung**" geregelt werden. Alle öffentlichen Stellen sollen die **Befugnis** erhalten, sämtliche automatisch lesbaren Daten zur Aufgabenerfüllung zu "speichern, übermitteln und nutzen".

Während für die Einführung von Ausweisdokumenten mit biometrischen Merkmalen bei Deutschen ein Gesetzesvorbehalt (z.B. § 1 Abs. 5 PersAuswG-E) vorgesehen ist, ist dies bei den Dokumenten der Ausländer nicht der Fall. Es ist zu vermuten, dass so der Ausländerausweis als Testprojekt für die Einführung von elektronischen Ausweisen generell verwirklicht werden soll. Für diese **ungleiche Behandlung** ist kein sachliche Rechtfertigung erkennbar.

Biometrische Identifizierungsmerkmal können wie **Personenkennzeichen** (PKZ) genutzt werden, die dazu geeignet sind, unterschiedlichste Datenbestände zusammen zu führen. Wegen der damit verbundenen Risiken wurde die generelle Nutzung solcher PKZ bisher als verfassungswidrig angesehen. Während sonstige Ordnungsnummern im deutschen Rechtssystem bisher nur unter restriktiven Voraussetzungen zugelassen sind, besteht hier ausdrücklich die Absicht, durch die Nutzung der einheitlichen Ausweisdaten „maschinelle Datenabgleiche durchführen" zu wollen (s.o. III.3.3).

Der Begriff "**biometrische Merkmale**" umschließt vor allem Fingerabdrücke, Gesichts- und Handgeometrie. Die beiden erstgenannten Merkmale fallen bei den Menschen in Alltagssituationen unwillkürlich an. Diese Daten eignen sich daher auch für andere als ausländerrechtliche Identifizierungszwecke, insbesondere für polizeiliche Zwecke. Es ist davon auszugehen, dass diese Merkmale für Spurenabgleiche mit - z.B. an Gläsern hinterlassenen - Fingerabdrükken genutzt werden. Von besonderer Tragweite ist angesichts des zunehmenden Einsatzes von Videoüberwachung im öffentlichen Raum die Zulassung der Gesichtsgeometrie als Identifizierungsmerkmal, da mit anderweitig erfassten Videobildern automatisierte Musterabgleiche vorgenommen werden können (dazu allgemein und ausführlich II-IV).

Alle wesentliche Fragen sollen vom Bundesinnenministerium nach Maßgabe gemeinschaftsrechtlicher Regelungen durch **Rechtsverordnung** geregelt werden. Dies gilt für die Wahl eventuell mehrerer biometrischer Merkmale, die Aufnahme und die Abspeicherung – auch des Lichtbilds – im Rahmen des Erstellungsvorgangs oder das Führen von Referenzdateien sowie die Nutzung dieser Daten. Die Regelung in einer Rechtsverordnung ist nicht vereinbar mit dem verfassungsrechtlichen Grundsatz, wonach bei Grundrechtseingriffen das Wesentliche durch das Parlament zu regeln ist.

Die **pauschale Verarbeitungsbefugnis** für alle öffentlichen Stellen "zur Erfüllung ihrer gesetzlichen Aufgaben" erlaubt ein Übermaß an Datenverarbeitung. Mangels genauerer Festlegung der Zwecke der Datennutzung besteht ein Widerspruch zum verfassungsrechtlichen Bestimmtheitsgebot. Systematisch gehört die allgemeine Verarbeitungsnorm des § 5 Abs. 7 auch nicht ins AuslG, da dieses die Datenverarbeitung der Ausländerbehörden, nicht aber anderer öffentlicher Stellen normiert.

3.2 Herkunftsfeststellung durch Sprachanalyse (§§ 41 Abs. 2 S. 2, 78 Abs. 3, 4 AuslG; § 16 Abs. 1 S. 3, Abs. 5, 6 AsylVfG)

Zur „Bestimmung des Herkunftsstaates oder der Herkunftsregion des Ausländers" wird die offene Aufnahme und Auswertung des "gesprochenen Wortes" erlaubt. Diese **Sprachanalyse** hat unmittelbar nichts mit der Bekämpfung von Terrorismus oder generell von Straftaten zu tun, sondern in erster Linie mit der ausländerrechtlich relevanten Herkunftsbestimmung, die v.a. bei aufenthaltsbeendenden Maßnahmen von Bedeutung ist. Die Sprach- und Dialektanalyse ist wenig aussagekräftig und wissenschaftlich fragwürdig. Eine rechtsstaatliche Hinterfragung der Ergebnisse ist kaum möglich. Es bestehen zudem Zweifel, dass das vorgesehene „in-Kenntnis-Setzen" der betroffenen Ausländer eine ausreichende Aufklärung über mögliche Risiken beim Betroffenen und eine Kenntnisnahme sicherstellt.

Es ist zunächst nicht erkennbar, weshalb nach Erstellung des Herkunftsgutachtens und der Zuordnung der Sprache zu einer Region keine sofortige Löschung vorgesehen ist. Vielmehr sollen diese Sprachproben für 10 Jahre aufbewahrt werden. Dies macht nur Sinn, wenn damit eine **biometrische Sprachzuordnung** z.B. von abgehörten Telefonaten oder sonstigen Sprachaufzeichnungen geplant ist. Eine solche zweckoffene Vorratsdatenspeicherung auch bzgl. völlig Unverdächtiger ist unzweifelhaft verfassungswidrig. Dies gilt um so mehr, als das Sprechen für den Menschen zur Aufrechterhaltung seiner Sozialität unabdingbar ist.

3.3 Identitätssicherung durch Fingerabdrücke (§§ 41 Abs. 3-6, 78 Abs. 2-4 AuslG, § 16 AsylVfG)

Schon bisher ist geregelt, dass von sämtlichen Bürgerkriegsflüchtlingen und Asylsuchenden als Identitätssicherungsmaßnahme Fingerabdrücke erhoben und beim Bundeskriminalamt (BKA) zentral gespeichert werden. Dies soll bzgl. sonstiger Ausländer in **weiteren Fällen** erlaubt werden:

- bei Zurückweisung bzw. Zurückschiebung in einen Drittstaat (nach § 26 Abs. 2 AsylVfG),

- wenn Gründe zur Versagung einer Aufenthaltsgenehmigung wegen eines Extremismusverdachtes festgestellt wurden (Verweis auf § 8 Abs. 1 Nr. 5 AuslG),

- im Rahmen der Visumsbeantragung bei Staaten mit "Rückführungsschwierigkeiten" sowie in den Fällen des neuen § 64a (zusätzliche lagespezifische Visaermittlungen).

Sämtliche mindestens 14-jährige Ausländer, die aus einem Drittstaat unerlaubt eingereist sind, sollen erkennungsdienstlich (ED) behandelt werden. Das Gleiche gilt, wenn keine Aufenthaltsgenehmigung oder Duldung besteht und Anhaltspunkte dafür bestehen, dass ein Asylantrag im EU-Ausland gestellt wurde.

Schon die bestehende Regelung wurde als verfassungsrechtlich unzulässige **Vorratsdatenspeicherung** kritisiert, weil sie ohne Berücksichtigung des Einzelfalls auf der gesetzlichen Vermutung basiert, dass bestimmte Personen künftig aus ausländerrechtlichen Gründen ihre Identität verschleiern würden. Dieser Katalog soll nun um Fälle erweitert werden, bei denen von Anfang an keine Zweifel an der Identität der Betroffenen bestanden haben. Der Verweis darauf, dass mit der Regelung teilweise eine Anpassung an die europäische **EURODAC-Verordnung** erfolgen würde, ist nicht geeignet, die bestehende verfassungsrechtliche Fragwürdigkeit zu beseitigen.

3.4 Aufbewahrung und Nutzung von ED-Unterlagen (§ 78 Abs. 2-4 AuslG, § 16 Abs. 5, 6 AsylVfG)

Die angefertigten ED-Unterlagen sollen beim BKA **10 Jahre lang aufbewahrt** werden. Die **Nutzung der ED-Unterlagen** soll generell „zur Feststellung der Identität oder der Zuordnung von Beweismitteln für Zwecke des Strafverfahrens oder zur Gefahrenabwehr" erlaubt werden.

Die auf einer pauschalen Verdächtigung basierende Datenerhebung soll für einen außergewöhnlich langen Zeitraum fortwirken. Eindeutig nicht mehr erforderlich – selbst im Sinne weitester Vorfeldbefugnisse – ist z.B. die Datenspeicherung, wenn die Rückführungsschwierigkeiten in einen Staat durch politische Änderungen behoben sind oder ein Extremismusverdacht bei der Personengruppe nicht mehr unterstellt werden kann. Eine generell, aber insbesondere für diese Fälle wirksame **Fristverkürzung** ist dringend geboten.

Über die Zulassung der Nutzung der ED-Unterlagen ohne konkreten Verdacht für jeglichen polizeilichen Daten- und Spurenabgleich würden de facto sämtliche mit ED-Maßnahmen erfassten ausländischen Menschen als potenzielle Straftäter behandelt. Die geetzlich vorgesehene Trennung zwischen polizeilichen und ausländerrechtlichen Daten beim BKA würde ad absurdum geführt. Es gibt keinen Grund, z.B. (auch anerkannte) Asylsuchende einem höheren Kriminalitätsverdacht auszusetzen als sonstige Ausländer oder Menschen generell. Das **Schutzziel des Art. 16a GG** würde in sein Gegenteil verkehrt, wenn unabhängig vom Ausgang des Asylverfahrens die ED-Unterlagen zu polizeilichen Identitätssicherungs- und -zuordnungszwecken genutzt werden dürften.

3.5 Beteiligungserfordernisse im Visumverfahren (§ 64a AuslG)

Zur Feststellung von extremistischen Bestrebungen (Versagungsgründe nach § 8 Abs. 1 Nr. 5) soll künftig bei **besonders definierten Gruppen von Ausländern** vor Visumserteilung eine **Anfrage** bei folgenden Einrichtungen erfolgen: Bundesnachrichtendienst (BND), Bundesamt für Verfassungsschutz (BfV), Militärischer Abschirmdienst (MAD), BKA und Zollkriminalamt. Die Gruppen der Betroffenen sollen vom Bundesinnenministerium im Einvernehmen mit dem Auswärtigen Amt über die Staatsangehörigkeit oder "in sonstiger Weise bestimmt" werden. Die über die Anfrage in Erfahrung gebrachten Daten sollen von den Sicherheitsbehörden ohne Einschränkung „zur Erfüllung ihrer gesetzlichen Aufgaben" weiter genutzt werden dürfen.

Die Festlegung der Gruppen, bei denen ein Generalverdacht angenommen wird und deshalb Regelanfragen bei den Bundessicherheitsbehörden erfolgen sollen, ist äußerst unbestimmt. Daran ändert auch nichts der Umstand, dass neben der Staatsangehörigkeit weitere Merkmale wie Alter, Geschlecht und Familienstand herangezogen werden können. Es erfolgt eine **Vorratsdatenerhebung** und darauf folgend eine Vorratsspeicherung. Die Geeignetheit und Erforderlichkeit der Maßnahme ist nicht einmal ansatzweise plausibel begründet.

Die Anfragen bei den genannten Sicherheitsbehörden verursachen einen **gewaltigen Verwaltungsaufwand** und lassen dort große Datenmengen anfallen, die ausgewertet und verwaltet werden müssen. Es bestehen keine Hinweise, dass sich hierdurch visumsrelevante Erkenntnisse ergeben. Bei vielen der Stellen, deren Datenerhebungsbefugnis sich auf das Gebiet der Bundesrepublik beschränkt, macht die Anfrage zu Personen keinen Sinn, die sich mit großer Wahrscheinlichkeit noch nie in der Bundesrepublik aufgehalten haben.

Verfahrensrechtlich äußerst problematisch ist, dass die Festlegung der besonderen Gruppen **ohne jegliche Rechtsförmlichkeit** erfolgen soll. Wegen der damit verbundenen Eingriffe in das Recht auf informationelle Selbstbestimmung bedürfte es zumindest einer Festlegung durch Rechtsverordnung.

Unverhältnismäßig ist zudem die Befugnis für die beteiligten Sicherheitsbehörden, die im Rahmen des Vorfeld-Beteiligungsverfahrens erhaltenen Daten für eigene Zwecke **unbegrenzt weiter zu nutzen**. Systematisch gehört eine solche Regelung zudem nicht ins Ausländerrecht.

4. Zu Art. 11 – Änderung des Ausländerzentralregistergesetzes (AZRG)

Das Ausländerzentralregister (AZR), für das seit 1994 eine gesetzliche Grundlage besteht, sieht schon heute eine sehr weit gehende Erfassung der gesamten nichtdeutschen Bevölkerung vor, die **verfassungsrechtlich** sehr problematisch ist. Es erfolgen nicht verhältnismäßige Eingriffe in das Recht auf informationelle Selbstbestimmung auf unbestimmten rechtlichen Grundlagen. Die sicherheitsbehördliche Nutzung des AZR stellt eine sachlich nicht begründ- und rechtfertigbare Ungleichbehandlung gegenüber Deutschen dar. Deswegen im Jahr 1995 eingereichte Verfassungsbeschwerden sind bis heute vom Bundesverfassungsgericht nicht behandelt.

4.1 Speicherungsinhalt (§ 3 AZRG)

Im AZR sollen künftig zusätzlich die **freiwillig gemachten Angaben zur Religionszugehörigkeit** gespeichert werden. Deren Erforderlichkeit ist nicht begründet. Es ist nicht davon auszugehen, dass religiös motivierte künftige Straftäter in Kenntnis des Umstandes, dass die ausländerrechtlich mitgeteilte Religionsangabe zu polizeilichen Zwecken genutzt werden kann, diese mitteilen werden.

4.2 Gruppenauskunft - Rasterfahndung (§§ 12, 31 AZRG)

Voraussetzung für eine sicherheitsbehördliche Rasterfahndung mit AZR-Daten (auch aus der Visa-Datei) soll nicht mehr eine "**im Einzelfall bestehende Gefahr**" sein; sondern generell der Zweck der "**Abwehr einer Gefahr**". Die Rasterfahndung für den **Bundesnachrichtendienst** (BND) soll künftig zusätzlich auch durchgeführt werden bei der Gefahr eines bewaffneten Angriffs, bei der Beeinträchtigung der Geldwertstabilität durch ausländische Geldfälschungen und bei internationaler Geldwäsche (Katalog des § 5 Abs. 1 S. 3 G10). Zudem soll der Ausschluss sicherheitsbehördlicher Rasterfahndungen bei Personen mit einem **gesicherten Aufenthaltsstatuts** (Aufenthaltsberechtigung oder unbefristete Aufenthaltserlaubnis) künftig wegfallen.

Durch den Wegfall des Erfordernisses einer konkreten Gefahr besteht die Möglichkeit der Durchführung von Gruppenauskünften zum Zweck der Rasterfahndung schon bei äußerst **vagen Verdächten** und Vermutungen. Rasterfahndungsmaßnahmen betreffen generell eine große Zahl unverdächtiger Personen, bei denen im Fall des Vorliegens der Rastermerkmale durch die sicherheitsbehördliche Ausermittlung im Einzelfall sehr intensive Grundrechtseingriffe erfolgen können. Es erscheint unverhältnismäßig, solche Eingriffe schon mit der Annahme einer allgemeinen Gefahrenlage zu rechtfertigen. Erforderlich wäre im Gesetzestext eine Eingrenzung auf besonders schwerwiegende Gefahren der Begehung terroristischer Anschläge gewesen, so wie in der Begründung argumentiert wird.

Die auch für **sämtliche Geheimdienste** vorgesehene Befugnis zur Durchführung von Rasterfahndungsmaßnahmen ist sachlich kaum begründbar und beinhaltet das Risiko paralleler, nicht abgestimmter Maßnahmen.

4.3 Datenübermittlung an Landesluftfahrtbehörden (§ 15 AZRG)

Es ist geplant, zum Zweck der Sicherheitsüberprüfung (**Zuverlässigkeitsprüfung**) nach § 29d LuftVerkehrsG den zuständigen Landesluftfahrtbehörden auf Ersuchen unbegrenzte Auskunft aus dem AZR zu geben.

Damit würde das AZR erstmals direkt für **Sicherheitsüberprüfungen** nutzbar gemacht. Angesichts der ohnehin vorgesehenen Abfrage bei Polizei, Geheimdiensten, dem Bundeszentralregister sowie im Bedarfsfall bei anderen Stelle ist nicht erkennbar, welchen zusätzlichen Erkenntniswert die AZR-Daten haben sollen. Obwohl im AZR weit überwiegend für Zuverlässigkeitsprüfungen irrelevante Daten gespeichert sind, lässt die vorgesehene Regelung auch die Übermittlung dieser Daten ohne Einschränkung zu.

4.4 Abruf im automatisierten Verfahren (§ 22 AZRG)

Bisher konnten die **Geheimdienste** online nur auf Personalien und Verwaltungsdaten im AZR zugreifen. Jetzt ist vorgesehen, dass ein unbegrenzter Abruf möglich ist. Die Beschränkung der Abrufbefugnis für die Geheimdienste auf Eilfälle und die Pflicht, die Eilbedürftigkeit zu begründen, sollen gestrichen werden.

Mit dem unbegrenzten Online-Zugriff von Geheimdiensten auf einen Verwaltungsdatenbestand wird die **Trennung zwischen Polizei bzw. Verwaltung und Diensten** ausgehöhlt. Die dafür vorgebrachte Begründung, die Daten würden benötigt und zwar “effektiv und zügig” und die konventionelle Auskunft “behindere die Arbeit der Dienste”, lässt wichtige Gesichtspunkte außer Acht. Protokollierungs- und Begründungsverpflichtungen zielen auf eine Verbesserung der Kontrollierbarkeit und auf eine Erhöhung der Rationalität von Verwaltungsentscheidungen ab. Das Vieraugenprinzip bei Datenübermittlungen, das bei Online-Abfragen entfällt, ist ein zentrales Instrument zur Sicherung der Rechtmäßigkeit von Datenübermittlungen.