Der Landesbeauftragte für den Datenschutz Schleswig-Holstein

11. November 1998

Stellungnahme zur Machbarkeitsstudie zur geplanten Einführung einer AsylCard

Ende 1994 hat eine Bund/Länder-Arbeitsgruppe zur Harmonisierung der Verwaltungsabläufe im Asylverfahren einen umfangreichen "Zwischenbericht" erstellt, in dem erstmals der Vorschlag gemacht wurde, entsprechend einem Vorbild aus den Niederlanden eine prozessorgestützte Chip-Karte "zur Vereinfachung der Organisation und Administration" des Asylverfahrens einzuführen. Die Arbeitsgruppe plante, hierzu eine Machbarkeitsstudie in Auftrag zu geben. Trotz vielseitiger datenschutzrechtlicher Kritik an der vorgelegten Leistungsbeschreibung erfolgte am 1.5.1997 die entsprechende öffentliche Ausschreibung. Den Zuschlag für die Erstellung der Machbarkeitsstudie erhielt die Fa. ORGA Consult GmbH, An der Kapelle 2, 33104 Paderborn, gemeinsam mit dem Forschungsverbund ikoplan-Institut für Kommunikation, Organisation & Planung, Kooperationsstelle Wissenschaft - Arbeit - Gesellschaft/Soziologie Universität Paderborn und der Kanzlei Dr. G., Paderborn. Die Studie wurde in Form eines Abschlußberichts im Juni 1998 von der Auftragnehmerin ORGA-Consult GmbH dem Bundesministerium des Innern (BMI) vorgelegt. Das BMI leitete diese mit der Bitte um Stellungnahme an das Bundesamt für die Anerkennung ausländischer Flüchtlinge (BAFl) weiter.

Eine Kopie der Machbarkeitsstudie liegt mir vor. Eine öffentliche Vorstellung ist bisher nicht erfolgt. In der folgenden Stellungnahme werden die wesentlichen Aussagen der Studie wiedergegeben und aus Datenschutzsicht bewertet (Seitenangaben sind solche der Studie).

I. Allgemeine Bemerkungen

Die Lesbarkeit der Studie wird dadurch erschwert, daß deren **Aufbau** schwer nachvollziehbar ist und in verschiedenen Teilen **Begrifflichkeiten**, Abkürzungen usw. verwendet werden, die nicht mit anderen Teilen der Studie korrespondieren. Einige Beispiele: die Begriffe "Anonymisieren" und "Pseudonymisieren" werden teilweise fälschlich synonym genutzt; dann ist gar von "Einweganonymisierung" die Rede (S. 82). Es wird von einer Ausweisnummer gesprochen (z.B. S. 126, 170), die im Datenschema der Karte nicht vorgesehen ist und als Personenkennzeichen ausdrücklich abgelehnt wird (S. 128). Ob dabei die Kartennummer (S. 102, 106), die eben eine solche Funktion erfüllt (siehe unten) gemeint ist, kann aus dem sonstigen Kontext heraus nur vermutet werden. Der Begriff Hintergrundsystem (HGS) wird regelmäßig für das beim BAFl geführte DV-System zur AsylCard verwendet; dann aber taucht dieser Begriff im Plural auf, wobei nur vermutet werden kann, daß damit lokale DV-Systeme gemeint sind (S. 136, 148). Es bleibt aber unklar, welche Aussagen zu Hintergrundsystemen auf die lokalen Systeme anwendbar sein sollen. Die offensichtlich von verschiedenen Personen und Stellen erarbeiteten Studienteile sind ungenügend aufeinander abgestimmt.

Bzgl. der Ausführungen zur **Datensicherheit** ist festzustellen, daß Behauptungen aufgestellt werden, die sich bei der Lektüre weiterer technischer oder organisatorischer Ausführungen als fragwürdig, widersprüchlich oder als nicht näher begründet erweisen. Wenn es z.B. heißt, bei komplexeren Zugriffen würden "applikationsspezifische Befehle benutzt, die nicht in der ISO Norm spezifiziert sind," und damit werde "dem hohen Anspruch an funktionale Sicherheit und dem hohen Datenschutzbedürfnis Rechnung getragen" (S. 135), ohne daß ein weiteres Wort über diese spezifischen Befehle verloren wird, so erscheint dies wenig seriös. Es entsteht der Eindruck, daß hier "security by obscurity" erreicht werden soll. Weitere nicht näher erläuterte Aussagen sind z.B.:

- "Das Hintergrundsystem verfügt über eine zu spezifizierende administrative Komponente, mit der die Zuverlässigkeit und Verfügbarkeit des Systems sichergestellt wird" (S. 148).
- "Die Anwendung der Smart-Card ergänzt die üblichen Kommunikationswege zum Austausch von Daten und Informationen zwischen den Behörden. Der Informationstaustausch wird durch den Einsatz der Karte auf ein höheres Qualitätsniveau gebracht" (S. 174).

Maßnahmen werden vorgeschlagen, ohne daß deren Zweck im konkreten Kontext erkennbar ist (z.B. digitale Signatur nach Signaturgesetz, S. 166). Zwar wird die technische Machbarkeit bestimmter Sicherheitsanforderungen erläutert. Die technischen und tatsächlichen Konsequenzen der Maßnahmen werden aber regelmäßig nicht offengelegt.

Für die Studie ist weiterhin kennzeichnend, daß auf bekannte **datenschutzrechtliche Argumente** zur AsylCard (S. 299 ff.) nur unpräzise oder gar nicht eingegangen wird (S. 320 ff.). Die rechtlichen

Ausführungen nehmen nur vage Bezug auf die konkreten technischen Systemvorschläge und erschöpfen sich in allgemeinen rechtlichen Ausführungen.

In der Studie wird dargestellt, den Datenschutzbeauftragten des Bundes und der Länder sei von der Projektgruppe das Angebot gemacht worden, die entwickelten Lösungsvorschläge zu präsentieren und zur Diskussion zu stellen. Von diesem Angebot hätten die **Landesbeauftragten** aber keinen Gebrauch gemacht. Meines Wissens haben einige Landesbeauftragte an einer Diskussion ihr Interesse bekundet. Diese ist aber aus nicht von ihnen zu vertretenden Gründen nicht zustande gekommen.

II. Darstellung der wesentlichen Inhalte der Studie

Die Studie verwendet statt des bisher geläufigen und in dieser Stellungnahme weiterhin verwendeten Begriff "**AsylCard**" die Bezeichnung "**Smart-Card**". Diese soll eine bundesweit einheitliche Ausweiskarte im Scheckkartenformat mit einem Mikroprozessor-Chip sein. Sie dient dem Träger als Identifikationsnachweis und erlaubt die vereinfachte Kommunikation mit den am Asylverfahren beteiligten Stellen.

Die **optische Personalisierung** der Karte soll folgende Daten umfassen: Name, Vorname, Geburtsdatum, Staatsangehörigkeit, Lichtbild und Unterschrift. Als Kartenmerkmale sind eine eindeutige Kartennummer und ein Gültigkeitsdatum vorgesehen (S. 68).

Die Ausgabe der Karte soll durch das BAFl als Systembetreiber (S. 156) erfolgen, das auch die sog. Basisanwendung betreibt. Die **Basisanwendung** (auch als Kinderkarte) soll folgende Funktionen erfüllen: Identitätsnachweis, Ausweis, Nachweis der Aufenthaltsgestattung (S. 72). Folgende elektronisch gespeicherten Daten gehören zu dieser Anwendung: Familienname, Geburtsname, Vorname, Geburtsdatum, Staatsangehörigkeit, Kartennummer, Gültigkeitsdauer der Karte, biometrisches Merkmal, Sprachkenntnisse, Status des Dokuments, Gültigkeitsdauer des jeweiligen Status, Unterschrift. Hierauf erhalten alle beteiligten Stellen einen lesenden Zugriff (S. 91).

Zum zweifelsfreien Identitätsnachweis werden als biometrische Angaben auf der Karte elektronisch wesentliche **Fingerabdruck-Merkmale** (Minuzien) abgelegt, die mit an Terminals opto-elektronisch erfaßten Fingerabdrücken der Asylsuchenden verglichen werden können (S. 123, 142).

Neben der Basisanwendung sind sog. **zweckgebundene Anwendungen** folgender beteiligter Behörden (sog. Systemanwender, S. 157) vorgesehen: BAFl, Ausländerbehörden (ABH), Aufnahmeeinrichtungen (AE), Sozialbehörden (SOZ), Meldebehörden (MEL), Arbeitsämter (ARB). Die Speicherung der Kartendaten wird von diesen Trägern übernommen (vgl. Anlage, Kopie von S. 91). Zugleich steht ihnen die Nutzung der Basisanwendung frei. Außerdem haben die Behörden Zugriff auf Datenfelder der sog. zweckgebundenen Anwendungen anderer Behörden (sog. verteilte Lesezugriffe). Ohne daß dies näher erläutert wird, soll außerdem die Polizei Zugriff auf diese Datenbereiche haben.

Folgende **Zugriffe** auf fremde sogenannte zweckgebundene Anwendungen sind vorgesehen (S. 94 ff.):

- BAFl: Zuständige ABH, letzte Änderung ABH, zugewiesene Anschrift, AZ-AE, zuständige AE,

letzte Änderung AE, Anschrift/Zimmernachweis (aktuell),

- ABH: sämtliche BAFl-, ARB- und MEL-Daten, AZ-AE, zuständige AE, letzte Änderung AE, Anschrift/Zimmernachweis (aktuell),
- AE: sämtliche MEL-Daten, AZ-BAFL, letzte Änderung BAFl, Volkszugehörigkeit, Geschlecht, Familienstand, Familienverbund J/N, Datum Antragstellung, zuständige BAFl-AS, abweichende Personaldaten J/N, Sprache, Religionsbekenntnis, bestellter Vertreter J/N,
- SOZ: sämtliche AE- und ARB-Daten, letzte Änderung BAFl, Geschlecht, Familienstand, Familienverbund J/N, abweichende Personaldaten J/N, bestellter Vertreter J/N, zuständige ABH, letzte Änderung AHB, Arbeitsberechtigung J/N, zugewiesene Anschrift,
- ARB: sämtliche SOZ-Daten, letzte Änderung BAFl, Geschlecht, bestellter Vertreter J/N, zuständige ABH, letzte Änderung ABH, Arbeitsberechtigung J/N, zugewiesene Anschrift,
- MEL, letzte Änderung BAFl, Geschlecht, Geburtsort, Familienstand, bestellter Vertreter J/N, zuständige ABH, letzte Änderung ABH, zugewiesene Anschrift.

Etwas versteckt und unkommentiert wird der **polizeiliche Zugriff** (POL) auf folgende AsylCard-Daten vorgesehen: Famlienname, Geburtsname, Vorname, Geburtsdatum, Staatsangehörigkeit, Kartennummer, Lichtbild, Gütigkeitsdauer der Karte, biometrisches Merkmal, Sprachkenntnisse, Status des Kartendokuments, Gültigkeit des jeweiligen Status, Unterschrift, letzte Änderung BAFl, Geschlecht, Familienstand, Familienverbund J/N, abweichende Personaldaten J/N, Sprache, bestellter Vertreter J/N, zuständige ABH, letzte Änderung ABH, vollziehbare Ausreisepflicht, Vollstreckungs- u. Abschiebungshindernisse, räumliche Beschränkung, zugewiesene Anschrift, AZ-AE, zuständige AE, letzte Änderung AE, Anschrift/Zimmernachweis (aktuell), AZ-ARB, zuständiges ARB, letzte Änderung ARB, Arbeitserlaubnis bei Firma, Dauer Arbeitserlaubnis, Arbeitslosengeld J/N, Arbeitslosenhilfe J/N, (S. 93, 102 ff., 157).

Schließlich sind für die Ausländerbehörden (AZ-ABH), die Aufnahmeeinrichtungen (Gesundheitsuntersuchung J/N, An- und Abwesenheitsnachweis AE und später, unentgeltliche Verpflegung J/N, AE spezifisches Datum für individuelle Nutzung) und die Sozialbehörde (Leistungen nach AsylBLG bzw. BSHG, erhalten am?) **exklusive Lesezugriffe** vorgesehen (S. 91).

Die sog. zweckgebundenen Anwendungen können durch **behördentypische Bereiche** ergänzt und regional unterschiedlich eingesetzt werden.

Folgende Funktionen werden besonders dargestellt:

- Verfahren zur Aufenthaltssteuerung,
- Regelung und Kontrolle des Leistungsbezugs,
- unterstützende Verfahren zum Meldewesen,
- unterstützende Verfahren beim Zugang zum Arbeitsmarkt.

Das Verfahren zur **Aufenthaltssteuerung** (S. 74 f.), betrieben von den Ausländerbehörden, soll die Erreichbarkeit des Asylbewerbers verbessern, was "zur Zustellung von Bescheiden und zur Verhinderung der illegalen Arbeitsaufnahme" erwünscht sei (S. 74). "Die Aufenthaltssteuerung geschähe durch

sekundäre Systeme (wie z.B. Meldesäulen), welche diese Daten und die Basisanwendung nutzen. Die konkrete Ausgestaltung dieses Verfahrens würde durch die einzelne Institution definiert und lokal implementiert" (S. 75).

Die Regelung und Kontrolle des **Leistungsbezugs** soll von den zuständigen Sozialbehörden betrieben werden, "um eine effizientere Regelung des Leistungsbezugs durchzuführen, aber auch den Leistungsmißbrauch zu verhindern" (S. 75).

Das unterstützende **Verfahren zum Meldewesen** soll von den Einwohnermeldeämtern betrieben werden und sieht "die kartengestützte An-, Ab- und Ummeldung von Asylbewerbern" vor (S. 75).

Als eine weitere Teilapplikation ist das unterstützende Verfahren beim **Zugang zum Arbeitsmarkt** durch die Arbeitsämter vorgesehen, womit "andere involvierte Behörden" informiert würden (S. 76).

Die Konfiguration der **Zugriffsmatrix** wird systemweit fest codiert und bei der Kartenproduktion unveränderlich festgelegt. Eine Umgehung der Zugriffsbeschränkung soll durch die Verwendung von starken kryptografischen Mechanismen verhindert werden (S. 69). Unbefugter Zugriff soll durch die aktive Zugriffskontrolle der Karte gesichert werden (S. 90).

Die für die Administration des Kartensystems notwendige Referenz-Datenbank speichert die Daten unter einem Pseudonym. Fälschlicherweise verwendet die Studie jedoch statt dessen regelmäßig den Begriff der Anonymität. Die Verbindung zwischen der Person und den in einem **Hintergrundsystem** (HGS) beim BAFl gespeicherten Daten soll nur über das mit kryptografischen Methoden erstellte Pseudonym oder unter Verwendung der Karte hergestellt werden können (S. 70). Das Hintergrundsystem soll auch Änderungsmeldungen bearbeiten, die ohne Vorlage der Karte erzeugt werden. Diese Meldungen werden dort in einer Warteschlange abgelegt und bei der nächsten on-line-Autorisierung in die Karte überspielt. Die auf der Karte gespeicherten Informationen sollen also kein zeitgenaues Abbild der DV-Bestände sein, sie spiegeln vielmehr den Zustand seit der letzten Synchronisation mit diesen jeweiligen Beständen wieder (S. 82, 86 f., 90, 100).

Hintergrundsysteme sollen auch bzgl. der sog. zweckgebundenen Anwendungen von den jeweils dafür zuständigen Behörden geführt werden (sogenannte **lokale DV-Systeme**). Die Verantwortung hierfür tragen ausschließlich die jeweiligen Stellen (S. 127, 157).

Gehen die in der AsylCard gespeicherten Daten aus irgend einem Grunde verloren (z.B. Zerstörung), so ist deren **Rekonstruktion** aus dem entsprechenden zentralen Bestand (HGS) und den lokalen Datenbeständen vorgesehen (S. 90).

Das Hintergrundsystem soll als verläßliche Datenbasis auch für **statistische Zwecke** zur Verfügung stehen (S. 71).

Die auf der Karte gespeicherten Daten werden, soweit sie auch im Ausländerzentralregister (AZR) und/oder im BAFl-System Asylon (Asylverfahren-Online) gespeichert sind, dort **automatisch aktualisiert**. Bisher bestehende organisatorische Defizite sollen durch gezielte technische Maßnahmen kompensiert werden. "Hierzu soll die Leistungsfähigkeit der Kommunikationsinfrastruktur zwischen den Datenbeständen verbessert werden". Durch regelmäßige Plausibilitätskontrollen (Datenabgleiche) soll die Fehlerquote in den einzelnen Systemen abgebaut werden (S. 66 f.).

Nach den Vorstellungen der Studie soll die ED-Identifizierung über das Automatisierte

Fingerabdruck-Identifikationssystem (**AFIS**) beim BKA und die Fingerabdruckerfassung für die Erstellung der AsylCard unabhängig voneinander erfolgen (S. 79 f.). Die Studie weist jedoch darauf hin, daß die Nutzung eines eigenen AFIS-Systems durch das BAFl die Anzahl der Schnittstellen vermindern und "wesentlich kürzere Bearbeitungszeiten bei der ED-Auswertung" erlauben würde (S. 89). "Insbesondere im Hinblick auf eine europaweite AFIS-Nutzung für Asylsuchende (EURODAC)" sollte Effizienz mit kurzen Antwortzeiten garantiert werden (S. 159).

Die AsylCard soll nicht in jedem Fall als Datenübermittlungsmedium genutzt werden. Bei der Verteilung in eine andere Aufenthaltseinrichtung (AE) oder auch bei sonstigen Zuständigkeitsänderungen soll die betroffene Person sich zwar per Karte "auschecken". Die **An - und Abmeldung** bei der Sozialbehörde oder der Meldebehörde soll jedoch "im Rahmen eines automatisierten Verfahrens" erfolgen. Änderungen in den Speicherungsbereichen der Sozial- oder Meldebehörde sollen "durch online-Zugriffe auf deren Hintergrundsystem realisiert werden". Automatisiert aktualisiert werden soll zudem das AZR durch die Ausländerbehörde oder die Aufenthaltseinrichtung (S. 84 f.).

Die AsylCard soll mit einer Persönlichen Identifikationsnummer (PIN) versehen werden, die nur dem jeweiligen Asylbewerber mitgeteilt wird. Über diese PIN soll dem Betroffenen "das umfassende **Recht zur Einsicht** in die zu seiner Person gespeicherten Daten gegeben werden". Mit der PIN erfolgt ein uneingeschränkter Lesezugriff auf sämtliche gespeicherten Daten. Die PIN wird "dem Karteninhaber auf Anfrage freigegeben", und zwar durch das BAFl als Systembetreiber (S. 93, 121).

Die Studie schlägt vor, ein **Smart-Card Kompetenzzentrum** einzurichten, das in Zusammenarbeit mit einer Bund/Länderarbeitsgruppe die konkreten Anwendungen (sog. Module) entwickelt (S. 74). Primäre Aufgabe dieses Kompetenzzentrums soll die Systemunterstützung und die Weiterentwicklung des Systems sein. Landes- und behördenübergreifend solle dort über die Nutzung der Smart-Card hinaus eine Harmonisierung der Verfahrensabläufe bewirkt werden (S. 161 f.).

Hinsichtlich der **rechtlichen Voraussetzungen** für die Einführung der AsylCard wird festgestellt, daß diese einer gesetzlichen Grundlage bedarf (S. 228), wobei aber eine Ermächtigung nach dem Vorbild des § 291 SGB V (Krankenversichertenkarte) für ausreichend angesehen wird (S. 233). Eine Bewertung der einzelnen durch die Karte ermöglichten Formen der Datenkommunikation erfolgt nicht. Nach einem Verweis auf § 8 AsylVfG heißt es vielmehr: "Im Hinblick auf die differenzierte und dem Verhältismäßigkeitsgrundsatz Rechnung tragende Konzeption des Datenmanagements im Systemmodell empfiehlt es sich, die dort vorgesehenen Befugnisse der jeweiligen Stellen für das Lesen/Erfassen/ Schreiben/Ändern der Daten im Wege einer untergesetzlichen Regelung zu normieren. Einer Regelung im Gesetz bedarf es dafür nicht" (S. 237).

Entsprechend den Vorgaben der Leistungsbeschreibung macht die Studie Vorschläge für die optionale **Weiterentwicklung** im Hinblick auf die Reichweite wie weiterer Funktionen (S. 176).

III. Datenschutzrechtliche Bewertung

Die oben skizzierte AsylCard-Konzeption der Studie stößt aus Datenschutzsicht auf Bedenken.

1. Allgemeine Aspekte

Bevor auf einzelne rechtliche und technische Fragen eingegangen wird, soll auf eine eher grundsätzliche Fragestellung hingewiesen werden: Der datenschutzrechtlich gebotene Vorrang der Datenerhebung beim Betroffenen wird hier durch den Technikeinsatz ab absurdum geführt. Die Datenerhebung erfolgt nicht mehr durch die persönliche Befragung der Betroffenen, sondern durch Befragung von deren AsylCard. Die menschliche wird durch die technische Kommunikation ersetzt. Dies hat eine **Entpersönlichung** der Datenerhebung zur Folge und einen Verlust an Transparenz für die Betroffenen. Beim Lesen der Chipkarte durch eine leseberechtigte Stelle erkennt der Betroffene nicht mehr, was zur Kenntnis genommen wird und was letztendlich auf die lokale EDV übertragen wird.

Mit dem Ersetzen der Mensch-Mensch-Kommunikation durch eine Maschine-Maschine-Kommunikation lassen sich gewiß **Rationalisierungseffekte** erreichen. Angesichts knapper Kassen und der restriktiven allgemeinen Asylpolitik ist es unwahrscheinlich, daß die bewirkten Rationalisierungsgewinne dazu genutzt werden, die soziale Betreuung und Versorgung dieser Menschen zu verbessern. Angesichts der auch in der Studie dokumentierten Überwachungsvorstellungen von seiten der Verwaltung (S. 13 ff.) ist vielmehr mit einer Erhöhung der Kontrolldichte in allen Lebensbereichen der Asylsuchenden zu rechnen.

Mit der Einführung einer AsylCard, wie sie in der Studie vorgeschlagen wird, wären neue massive Eingriffe ins Grundrecht auf informationelle Selbstbestimmung verbunden. Solche Eingriffe sind nur bei Vorliegen eines **überwiegenden Allgemeininteresses** gerechtfertigt (BVerfGE 65, 1 ff. = NJW 1984, 419 ff.). Zwar konstatiert die Studie Defizite hinsichtlich der Richtigkeit und Aktualität der sich auf Asylsuchende beziehenden Daten (S. 21 ff., 26 f., 55 f.). Diese beruhen darauf, daß die bestehenden informationstechnischen Instrumente nicht sorgfältig gepflegt und nicht ordnungsgemäß gehandhabt werden. Die Studie überprüft nicht, inwieweit die behaupteten, nicht näher belegten Defizite abgebaut werden können. Auch die Gründe für die ungenügende Datenqualität werden nicht näher untersucht. Vielmehr wird ein weiteres Kontroll- und Erfassungssystem vorgeschlagen, das nicht an die Stelle der bisherigen, sondern ergänzend hinzu treten soll. Asylsuchende sind schon heute die wohl am besten informationell erfaßte Bevölkerungsgruppe in Deutschland. Erstaunlich ist, daß die Studie zwar umfangreich die Akzeptanzverbesserung einer AsylCard untersucht. Nicht erwähnt werden aber mögliche Fehlerquellen beim Einsatz der AsylCard.

2. Ausgestaltung der AsylCard

Die Studie entscheidet sich als Instrument zur sicheren persönlichen Zuordnung der AsylCard für die Nutzung eines **biometrischen Verfahrens**. Inwieweit dieser Einsatz aus Gleichheits- und Verhältnismäßigkeitsgründen legitim ist, wird nicht erörtert. Statt ein Verfahren geringerer Fehlerrate und geringeren Zweckentfremdungsrisikos (Augenerkennung/Netzhaut/Iris) zu wählen, schlägt die Studie die fehleranfällige klassische Methode des Fingerabdruckverfahrens vor. Der Umstand, daß dieses Verfahren erfolgreich durch das Bundeskriminalamt genutzt wird (S. 114), ist für sich noch kein Grund, dieses Verfahren zu verwenden. Er ist (wegen der Möglichkeit des zweckwidrigen Einsatzes) vielmehr Anlaß, ein anderes Verfahren zu wählen. Die Nutzung eines Verfahrens der Augenerkennung hätte den Vorteil, daß eine Identifizierung nur durch eine gezielte Handlung der betroffenen Person ausgelöst werden kann, wodurch auch das Mißbrauchsrisiko verringert würde.

Die **Erforderlichkeit** der vorgesehenen Datensätze und des Übermittlungsumfangs ist in Frage zu

stellen. Der in der Studie vorgesehene Datenumfang ist geprägt von der informationellen Begehrlichkeit der einzelnen Verwaltungsbereiche und nicht von dem, was im Sinne des verfassungsrechtlichen Verhältnismäßigkeitsprinzips als erforderlich angesehen werden kann. Er geht nicht nur weit über das derzeit rechtlich zulässige Maß hinaus, sondern auch über das, was im Rahmen der konkreten Anwendung erforderlich sein könnte. Dies gilt schon für die Basisdaten, zu denen z.B. die Sprachkenntnisse gehören sollen. Es ist nicht erkennbar, weshalb z.B. die Polizei einen derart umfassenden Datenzugriff erhalten soll. Der Umstand anwaltlicher Vertretung oder räumliche Beschränkungen haben die Meldebehörde nicht zu interessieren.

Zu berücksichtigen ist, daß durch die technikspezifischen Eigenschaften der Chipkarte **keine Einzelfallprüfung** der Erforderlichkeit der Datenabfrage erfolgen kann. Vielmehr erhalten die jeweiligen Behörden umfassenden Einblick in die für diese freigeschalteten Datensegmente, wenn eine Lesevorgang stattfindet. Untauglich ist der Versuch, dem Erforderlichkeitsgrundsatz durch die technische Zugriffsorganisation gerecht zu werden (S. 237), da Technik nicht in der Lage ist, eine auf den Einzelfall abstellende materielle Rechtsprüfung zu ersetzen.

Ein zentrales Problem des Studienkonzepts besteht darin, daß unter dem Begriff der zweckgebundenen Datenanwendung umfassend zweckwidrige Datennutzungen durch andere Behörden vorgesehen werden. Der verfassungsrechtlich gebotenen Begründungspflicht und der gesetzlichen Regelungspflicht bei **Zweckänderungen** wird nicht Rechnung getragen.

Die Studie schafft keine Klarheit über **grundlegende datenschutzrechtliche Begriffe**. Es bleibt offen, ob die Daten in die Karte eingebenden Stellen "verarbeitende Stellen" im Sinne des Datenschutzrechts sind, bzw. wer die Verantwortung für die Richtigkeit und Aktualität dieser Daten trägt. Unerwähnt bleibt, daß die jeweils anderen Stellen, die Daten auf der Karte speichern dürfen, datenschutzrechtlich als Dritte zu behandeln sind. Das Lesen in anderen sog. zweckgebundenen Anwendungen (Segmenten) ist eine rechtlich legitimationsbedürftige Datenübermittlung. Selbst das Lesen durch eine andere als die eingebende Behörde des selben Verwaltungszweiges stellt eine solche Datenübermittlung dar. Es wird lediglich festgestellt, daß bzgl. der sog. Basisdaten, auf die ein allgemeiner Lesezugriff erteilt werden soll, die Beachtung des Zweckbindungsgrundsatzes "relativ unproblematisch" sei, da "alle am Asylverfahren beteiligten Stellen den gleichen Zweck verfolgen (Feststellung der Identität)" (S. 236). So richtig vielleicht das Ergebnis sein mag (Zulässigkeit der gemeinsamen Nutzung der Ausweisfunktion), so falsch ist die Annahme, daß die Feststellung der Identität der gemeinsame Zweck aller Behörden im Sinne der datenschutzrechtlichen Zweckbindung wäre.

Ohne zu prüfen, wie weit die Übermittlungsregelung des **§ 8 AsylVfG** reicht und ohne die Erforderlichkeit und Angemessenheit der vorgesehenen Datentransfers zu prüfen, werden diese als verhältnismäßig und als auf untergesetzlicher Ebene konkretisierbar deklariert. Unabhängig von der Frage, inwieweit § 8 Abs. 3 AsylVfG hinreichend bestimmt und damit verfassungsgemäß ist (dagegen Weichert, Inf-AuslR 1993, 386), lassen sich die mit der AsylCard verfolgten Zwecke nicht auf die Ausführung des AuslG, gesundheitliche Betreuung und Versorgung sowie Aufdeckung und Verfolgung unberechtigten Leistungsbezugs reduzieren. Dies gilt z.B. für sämtliche Datenweitergaben an die Meldebehörden sowie in großen Teilen an die Arbeitsämter. Eine Normierung der Datenzugriffe auf untergesetzlicher Ebene (S. 237) würde dem Gesetzesvorbehalt bei Grundrechtseingriffen zuwiderlaufen.

Zu begrüßen ist, daß entgegen den Vorgaben der Leistungsbeschreibung auf die Verwendung eines für das gesamte Asylverfahren und alle beteiligten Behörden geltenden Zuordnungskriteriums verzichtet

werden sollte. Ein solches **Personenkennzeichen** wäre aus datenschutzrechtlicher Sicht nicht akzeptabel. Die Datensatz-Beschreibung läßt dann aber erkennen, daß die Karten-/Ausweisnummer (S. 131, 170) genau die Funktion eines Personenkennzeichens erfüllen soll: Diese im Hintergrundsystem gespeicherte und auf der Karte optisch wie elektronisch lesbare Nummer darf von allen beteiligten Behörden gelesen und weitergenutzt werden, ja selbst von der zugriffsberechtigten Polizei (S. 102, 106).

Ein für die AsylCard ins Feld geführtes Argument ist, mit ihr solle und könne **Leistungsmißbrauch** verhindert werden (S. 17 f., 64, 67, 75). Nicht dargelegt wird, wie dieses Ziel konkret realisiert werden soll und mit welchen Ausweichstrategien der betroffenen Personen zu rechnen wäre. Angesichts der rereits realisierten vollständigen daktyloskopischen Erfassung aller Asylsuchenden in AFIS ist nicht erkennbar, weshalb zusätzliche Maßnahmen erforderlich sein sollen.

Unbeantwortet bleibt in der Studie die Frage nach dem **zwingenden bzw. nachgiebigen Charakter** der Kartennutzungen für die Betroffenen. Zwar geht sie stillschweigend davon aus, daß praktisch die gesamten Anwendungen für die Asylsuchenden obligatorisch sein sollen. Dies wird aber nicht ausgesprochen; die notwendigen rechtlichen (gesetzliche Regelung) und praktischen (Sanktionsbe-wehrtheit und Erzwingung) Konsequenzen werden nicht thematisiert. Daß den Betroffenen Mitwirkungspflichten obliegen und inwieweit die bestehenden Regelungen (§ 15 AsylVfG) ausreichen, wird nicht erörtert.

Von der Studie unerwähnt bleibt die damit zusammenhängende Problematik der **Ausweispflicht**, die sich nicht nur bei der Aufenthaltskontrolle stellt, sondern bei allen sonstigen mit der AsylCard vermittelten Aktivitäten. Ein umfassender Ausweiszwang ist in der deutschen Rechtsordnung bisher nicht vorgesehen. Offensichtlich geht die Studie jedoch davon aus, daß bestimmte existentielle Vorgänge (soziale und gesundheitliche Leistungsgewährung) bzw. rechtliche Pflichten (z.B. Meldepflicht) nur mit der Karte möglich sein sollen. Die Klärung dieser Frage ist von großer datenschutzrechtlicher Bedeutung.

Während die Leistungsbeschreibung die Zwecke der **Aufenthaltskontrolle** ungeschminkt benennt (Erkennen illegaler Aufenthalte, Erzwingung räumlicher Aufenthaltsbeschränkungen, Vermeidung mehrfacher Leistungsgewährung, Verhinderung illegaler Arbeitsaufnahme), findet die Motivation der Erhöhung der Kontrolldichte in der Studie keinen entsprechenden Niederschlag (S. 65, 74 f.). Die Verantwortung für diese Funktion wird auf den lokalen Bereich herabgezont. Aus Gründen des Gesetzesvorbehalts wie aus Gleichheitsgründen ist es fraglich, ob eine solche Dezentralisierung der Aufenthaltskontrolle zulässig wäre. Die Konzeption der AsylCard ist aber so angelegt, daß sie alle von der Leistungsbeschreibung geforderten Funktionen (Zwecke) erfüllt. Sie ermöglicht es, Asylsuchende zu zwingen, sich mehrfach am Tag zum Aufenthaltsnachweis an Meldesäulen einzufinden. Nach mir vorliegenden Informationen wird dieses Instrument in Holland angewandt. Das mit der AsylCard vergleichbare "Vreemdelingendocument" wird zur Kontrolle einer bis zu vier Mal täglich bestehenden Meldepflicht genutzt; bei zweimal unentschuldigt unterlassenem Aufenthaltsnachweis kann das Asylverfahren beendet werden. Eine solche Anwendung wird in der Studie nicht durch technische oder organisatorische Vorkehrungen auszuschließen versucht. Insofern werden auch keine rechtlichen Vorgaben diskutiert. Die vorgeschlagene Technik ist grundsätzlich dazu geeignet, eine praktisch totale Aufenthaltskontrolle der Asylsuchenden zu verwirklichen - eine Art "Gefängnis ohne Mauern".

In der Studie wird die Zulässigkeit des mit der AsylCard eingeführten Kontrollinstrumentariums an Art. 1 Abs. 1 GG (**Menschenwürde**) gemessen. Sie führt aus, "der Rechtsbegriff der Menschenwürde (sei)

generell anfällig für eine floskelhafte Handhabung" (S. 242). Diese wird dann mit der Feststellung praktiziert, daß die "gegenständlichen Freiheitsbeschränkungen im Zusammenhang mit der Chipkarte" nicht vergleichbar seien mit "Sklaverei, Folter, medizinischen Manipulationen ...". Da der Verhältnismäßigkeitsgrundsatz im Bereich der Datenverarbeitung beachtet werde und eine Verknüpfung der AsylCard-Anwendung mit der materiellen Entscheidung über den Asylantrag nicht erfolge, könne von einem Verstoß gegen Art. 1 Abs. 1 GG nicht die Rede sein. Die AsylCard solle als "verfahrensrechtliches Instrument" genutzt werden, nicht zur "materiellrechtlichen Ausgestaltung des Asylverfahrens" (S. 243 f.). Die Studie bemüht sich zweifellos um eine grundrechtlich bedingte Eingrenzung der Kartennutzung. Dabei ist sie jedoch nicht erfolgreich, da das Thema zwar angesprochen wird, die Konkretisierung unzulässiger Datennutzungen aber unterbleibt. Angesichts des Umstandes, daß die Verfassungsverträglichkeit der konzipierten AsylCard von Rahmenbedingungen (Verhältnismäßigkeit, Zweckbindung, Gesetzesvorbehalt, kein Einfluß auf Asylverfahren) abhängig gemacht wird, die von der Studie nicht gesichert werden, gibt die Studie selbst Hinweise auf die Nichtvereinbarkeit ihres Konzeptes mit dem Grundgesetz.

Zugriff auf die Daten der AsylCard sollen "am Asylverfahren beteiligte Behörden haben", die sich über einen elektronischen Schlüssel authentisieren, "der genau dieser Fachbehörde zugewiesen ist" (S. 92, 137). Da die Zugriffsmatrix fest in die Karte eingebracht werden soll (S. 136), ist davon auszugehen, daß nicht nur die örtlich und sachlich zuständigen Behörden Zugriff zu den Daten erhalten sollen, sondern alle einem bestimmten Sektor (z.B. Ausländerbehörden - ABH) zugeordneten Stellen. Gegen unbefugte Zugriffe innerhalb des jeweiligen Sektors sind keine Vorkehrungen vorgesehen. Da auf der Karte keine Zugriffsprotokollierungen geplant sind, ließen sich diese unzulässigen Zugriffe auch nachträglich nicht nachvollziehen. Ebenso nicht nachvollzogen werden könnten Abrufe nicht berechtigter Stellen, die sich über einen Schlüssel unzulässigerweise als berechtigte Stelle ausgeben. Dies gilt auch für die schreibenden Zugriffe. Es wird technisch nicht verhindert, daß eine unzuständige Stelle aus dem selben Sektor das Beschreiben der Karte vornimmt. Zwar ist die Speicherung der jeweiligen Stelle vorgesehen; hierbei wird aber nicht ein eindeutiger nur einer Stelle zugeteilter Schlüssel abgefragt oder gespeichert.

Der Klarheit des vorgestellten technischen Verfahrens ist es nicht gerade förderlich, daß zwar davon die Rede ist, daß die Schlüssel der berechtigten Stellen auf der Karte abgelegt sein sollen, dies aber nicht bei der Berechnung des Speicherbedarfs der Karte berücksichtigt wurde (S. 138 f.). Es ist die Rede von einem **hierarchischen Schlüsselmanagement**, bei dem höherwertige Schlüssel (Master Keys) vergeben werden. Die Schlüssel sollen mit gesonderten Chipkarten verwaltet werden (S. 154). Die datenschutzrechtlich relevante Frage, von der die Bewertung des Schlüsselmanagements abhängt, wem welche Schlüssel in welcher Hierarchiestufe durch wen zugewiesen werden, bleibt unbeantwortet. Dies wird lapidar damit begründet, daß Schlüsselmanagement-Systeme heute schon im Bankenbereich (z.B. Geldkarte) eingesetzt würden (S. 118). Es wird nicht erwogen, daß das Schlüssel-Management bei einer multifunktionalen hoheitlichen Anwendung unter Umständen anders ausgestaltet werden muß als bei eine monofunktionalen privaten Anwendung.

3. Hintergrundsysteme

Mit der AsylCard soll nicht nur ein neues Informations- bzw. Datentransportmedium eingeführt werden. Dessen Einführung setzt die Schaffung neuer Datenbanken (als Back-Up) voraus, die die bestehenden nicht ersetzen, sondern ergänzen sollen. Hierbei handelt es sich zunächst um das **Hintergrundsystem**

(HGS) des BAFl, das weitgehend einen redundanten Datenbestand zum AZR und zu Asylon enthalten soll. Problematisch ist bei diesem HGS, daß es nicht nur als Back-Up (Datensicherung, Aktualisierung) genutzt werden soll, sondern offensichtlich auch zu anderen Zwecken. Mit einer Nutzung zu statistichen Zwecken tritt das HGS z.B. in Konkurrenz zur gesetzlich geregelten Funktion des AZR (§ 23 AZRG).

Daneben sollen (optional) hinsichtlich der sog. zweckgebundenen Anwendungen (z.B. beim Sozialamt, der Meldebehörde, der Ausländerbehörde) **lokale "Hintergrundsysteme"** eingerichtet werden, die zu den dort derzeit existierenden Systemen hinzukommen. Unbefriedigend ist, daß die Schnittstellen zwischen den Back-Up-Systemen und den bestehenden Verwaltungsdatenbanken nicht näher beschrieben werden (S. 100, 127, vgl. S. 163: HGS als Referenz zu den dezentralen Datenbeständen). In den lokalen Systemen sollen teilweise besonders sensible Daten verarbeitet werden, für die eigenständige Regelungen und besondere Vertraulichkeiten (Sozialgeheimnis gem. § 35 SGB I, Meldegeheimnis gem. § 5 MRRG) gelten. Dies bleibt aber von der Studie unberücksichtigt.

Die Studie behauptet, die für die Administration des Kartensystems notwendigen **Referenzdatenbank(en)** (S. 146) würde(n) die Daten anonym speichern (S. 70). Dies ist unrichtig. Später wird ausgeführt, daß Name, Vorname und ein Differenzierungsmarkmal durch eine Einwegverschlüsselung zu einem **Pseudonym** führen, unter dem die im Klartext im HGS gespeicherten Daten abgelegt sind. Unrichtig ist zudem die Behauptung, daß die Verbindung der HGS-Datensätze zu einer Personenidentität "nur über die Karte selbst hergestellt werden" könne (S. 70). Richtig ist vielmehr, daß dies auch mit der Kartennummer (S. 126), mit einem begrenzten Merkmals-Set wie auch mit Kenntnis von Namen und Schlüssel möglich ist.

Die Aussagen zum Verschlüsselungsverfahren (Pseudonymisierung und Zugriffsmanagement) bleiben leider auf einem sehr allgemeinen Niveau (S. 115 ff., 120). Angesichts des Umstandes, daß das BAFl sowohl Betreiber von Asylon, des HGS wie auch Verwalter des **Pseudonymisierungsschlüssels** (S. 157) sein soll, stellt sich die Frage, wozu hier überhaupt eine Verschlüsselung vorgenommen wird. Dies gilt umso mehr, als selbst die Speicherung des "Differenzierungsmerkmals" als Eingangsparamenter für die Pseudonymisierung (neben Name und Vorname) in Asylon geplant ist (S. 122).

Offensichtlich ausgehend von der falschen Annahme, beim HGS handele es sich um ein anonymes System, erklärt die Studie es für möglich, "das Hintergrundsystem von einem DV-Dienstleister im Auftrag des BAFl betreiben zu lassen" (S. 163). Die Studie geht nicht auf die Problematik der Verarbeitung hoheitlicher Daten durch **private Auftragnehmer** ein (Begrenzung und Konkretisierung der Auftragsdatenverarbeitung nach § 11 BDSG, Sicherung der Verschwiegenheitspflicht, der Datenschutzkontrolle, der Zweckbindung und der technischen Abschottung).

Wer **Zugriffsrechte auf das HGS** bekommen soll, bleibt im Dunkeln. Der Umstand, daß damit auch statistische Auswertungen vorgenommen werden sollen (S. 71), läßt darauf schließen, daß dies nicht nur Systemadministratoren und im eingeschränkten Maße BAFl-Mitarbeiter (Aktualisierung) sein sollen.

Beim HGS handelt es sich zweifellos um den sensibelsten Bestandteil der gesamten konzipierten AsylCard-Architektur. Eine Manipulation dieses Datenbestandes bzw. der Kommunikation mit diesem würde bundesweit die gesamten Basis- und BAFl-Anwendungen gefährden (S. 100). Es verwundert, daß dennoch **keine konkreten Sicherheitsvorkehrungen** benannt werden. Es wird lediglich auf die Verantwortung des BAFl als Systembetreiber für die Sicherheitsmodule hingewiesen (S. 157).

Der Mangel an Sicherheitsbewußtsein erweist sich bei den Ausführungen zur

Kommunikationsanbindung. Hierbei werden nebenbei als sich ergänzende Teile genannt: BAFl-Netz, landes- und bundesweite Behördennetze und schließlich öffentliche Datennetze. Dies sollen auch "andere öffentliche Netze wie Internet oder Datex J" sein können. Als ausreichende Abschirmung vor externen Angriffen werden Firewalls präsentiert. Die Problematik von Spezifizierung, Administration und Pflege von Firewalls wird nicht angedeutet (S. 147 f.). Die Notwendigkeit spezifischer Verschlüsselung bei der netzgestützten Datenübermittlung wird nicht erwähnt.

Zu den offenen Punkten gehören die Ausführungen zur **Kartensperrung**, die im HGS vorgenommen werden und irreversibel sein soll (S. 136, 170). Es ist nicht erkennbar, wie die Sperrung im HGS vorgenommen werden soll (S. 106), durch wen und nach welchem Verfahren.

Die **Protokollierung** der elektronischen Datenkommunikation ist aus Gründen der Nachvollziehbarkeit von Verarbeitungsvorgängen, zur Klärung von Verantwortlichkeiten und u.U. zur Datenrekonstruktion von großer Wichtigkeit. Umso verwunderlicher ist es, daß die Protokollierung in der Studie nur an zwei Stellen erwähnt wird (Anwender: S. 152, HGS: S. 153), ohne daß die wesentlichen Fragen beantwortet würden: Welche Daten, aus welchen Anlässen, in welchem Umfang und wie lange wird protokolliert, welche Nutzung der Protokolldaten wird wem erlaubt? Aus dem Datenschema der AsylCard selbst ist zu entnehmen, daß eine Protokollierung auf der Karte selbst offensichtlich nicht geplant ist.

4. Vernetzung

Ebenso wie die Leistungsbeschreibung geht auch die Studie von einer derzeit nicht existenten und rechtlich nicht vorgesehenen **Vernetzung** einzelner Stellen aus. So werden anlaßunabhängige online-Übermittlungen von den Ausländerbehörden an Melde- und Sozialbehörden erwähnt (S. 84 f.). Zwischen Ausländerbehörden und BAFl wird offensichtlich ein elektronischer Datenaustausch außerhalb der Kartenkommunikation vorausgesetzt, ebenso zu Asylon und AZR (S. 71, 81). Es wird ausgeführt, "die Leistungsfähigkeit der Kommunikationsinfrastruktur zwischen Datenbeständen" müsse verbessert werden, indem diese "regelmäßig gegeneinander auf Plausibilität gepüft werden. Dieser Abgleich von Daten soll solange erfolgen, wie die Weitergabe von Daten in diesen Systemen mit einer hohen Fehlerquote behaftet ist" (S. 66 f.). Dadurch wird die Grundidee der AsylCard "Karte statt Netz" konterkariert. Die vorgesehene Konzeption "Karte und Netz" bewirkt eine nicht nur aus Verhältnismäßigkeits-, sondern auch aus Transparenzgründen problematische informationelle Verflechtung und eine Diffussion von Verantwortlichkeiten.

Rechtlich wird die Vernetzung wie auch der Datenabgleich über die AsylCard mit einer "**Verpflichtung für eine Synchronisation** der Datenbestände" begründet (S. 237 f.). Diese rechtlich nicht begründete, sondern behauptete Verpflichtung steht im diametralen Widerspruch zum vom Bundesverfassungsgericht dargelegten Grundsatz der (unter Gesetzesvorbehalt stehenden - amtshilfefesten) informationellen Gewaltenteilung (BVerfGE 65, 46, 69). Rechtlich wenig überzeugend ist auch die Darstellung, daß die automatisierte "Aktualisierung von Daten in AZR/ Asylon" durch die Regelungen zur Datensicherheit im AZRG rechtlich legitimiert sei (S. 238). Dabei wird ignoriert, daß das AZRG keine Regelung zu Asylon enthält. Hinzu kommt, daß die in § 7 AZRG zugelassene Veränderung von AZR-Daten im Wege der Direkteingabe eine gezielte Transaktion voraussetzt (§ 8 AZRG). Ein automatisierter Datenabgleich, wie ihn die Studie vorsieht, wird vom AZRG nicht erlaubt.

5. Bereichsspezifische Anwendungen

Die Studie nimmt keine Rücksicht auf außerhalb des Asylverfahrens bestehende rechtliche Strukturen (S. 75 f.). Bei der rechtlichen Bewertung wird übersehen, daß für eine Einführung der AsylCard nicht nur eine Änderung asylrechtlicher Regelungen notwendig wäre. Vielmehr bedürften eine Vielzahl von rechtlich bisher nicht vorgesehenen Übermittlungen und Speicherungen jeweils einer **gesetzlichen Grundlage**.

So geht die Studie z.B. im **Meldebereich** von einem Datensatz aus, der den des Melderechtsrahmengesetzes überschreitet, ohne dies auch nur ansatzweise zu thematisieren.

Völlig unberücksichtigt blieben die Besonderheiten des **Sozialrechtes** und die Differenzierungen der Leistungsgewährung oder des Datenschutzrechts nach dem BSHG und dem AsylBLG (vgl. S. 86).

Äußerst unpräzise sind die Vorstellungen der Studie zur Unterstützung beim "Zugang zum Arbeitsmarkt". Hier - wie auch in vielen anderen Bereichen - wird die Notwendigkeit der Datenübermittlungen von anderen Behörden an die **Arbeitsämter** und umgekehrt sowie zwischen den Arbeitsämtern nicht begründet. Ein Indiz für die fehlende Reflektiertheit der Ausführungen ist, daß das Arbeitsamt als "beteiligte kommunale Stelle" geführt wird (S. 76).

Die vorgesehene umfassende **Zugriffsbefugnis der Polizei** bzw. des Bundesgrenzschutzes wird nicht andeutungsweise erläutert (S. 93, 102 ff.). Eine Differenzierung nach bestimmten Aufgaben und nach dem Zweck des polizeilichen Zugriffs (konkreter Anlaß, Gefahrenabwehr/Strafverfolgung) wird konsequenterweise unterlassen. Die polizeiliche Kartennutzung ist wie ein polizeilicher Selbstbedienungsladen ausgestaltet.

6. Transparenz

Datenschutzrechtlich notwendig und insofern zu begrüßen ist es, daß das **Auskunftsrecht der Betroffenen** über die zu ihrer Person gespeicherten Daten technisch umgesetzt werden soll. Dies erfolgt in der Form, daß die oder der Asylsuchende eine PIN mitgeteilt erhält, die nur ihr bzw. ihm bekannt ist und mit der auf "Anfrage durch den Systembetreiber" alle Daten auf der Karte freigeschaltet und damit beauskunftet werden können (S. 121). Leider gibt die Studie jedoch keine Auskunft darüber, wer den Asylsuchenden in welcher Form die PIN mitteilt. Länge und Aufbau der PIN werden nicht vorgegeben. Soll die PIN nur den Betroffenen bekannt sein, so muß vorgesorgt werden, wie verfahren wird, wenn diese ihre PIN verlieren bzw. vergessen. Den Besonderheiten des Asylverfahrens, an dem Menschen teilhaben, die i.d.R. keine Kenntnis von technischen und administrativen Abläufen haben, wird in der Studie keine Aufmerksamkeit gewidmet. Ungeklärt ist, ob Unberechtigte in Kenntnis der PIN die Daten aus der Karte auslesen können. Problematisch ist zudem, daß die Wahrnehmung des Auskunftsrechts von einer Freischaltung durch den Systembetreiber abhängig ist. Unbeantwortet bleibt dabei die Frage, wie verhindert wird, daß das BAFl anläßlich der Auskunftserteilung unzulässig die beauskunfteten Daten zur Kenntnis erhält.

Die Studie legt nicht dar, wie die **Transparenz** bzgl. der Datenkommunikation mit der Karte für die Betroffenen hergestellt werden soll. Würden die Betroffenen selbst über die AsylCard als Informationsmittler in Anspruch genommen, so wäre es im Interesse informationeller Selbstbestimmung

notwendig, daß ihnen auch zur Kenntnis gebracht wird, wer über die Karte welche Daten über sie verarbeitet. Derartiges ließe sich durch ein Belegverfahren, durch Informationsblätter oder durch Display-Anzeigen realisieren. Entsprechendes ist aber nicht vorgesehen.

Zwar hält die Studie zur Einführung der AsylCard eine **spezialgesetzliche Grundlage** für notwendig (S. 246). Leider bleiben die dazu gemachten Vorschläge - es wird eine Orientierung an der Krankenversichertenkarte (KVK) nach § 291 SGB V empfohlen - hinter den rechtlichen Erfordernissen zurück. Anders als bei monofunktionalen Karten wie der KVK bedarf es zur Sicherung des Datenschutzes bei komplexen Systemen ergänzender verfahrensrechtlicher Vorkehrungen (z.B. Aufklärungs- und Belehrungspflichten, vgl. BVerfGE 65, 59). Insbesondere hinsichtlich der Transparenz für die Betroffenen entstehen beim Einsatz von multifunktionalen Chipkarten Defizite, die durch gesetzliche Regelungen kompensiert werden müssen. Hierzu macht die Studie keine Angaben.

7. Föderalismus

Zwar verfolgt die Realisierung einer AsylCard nicht das Ziel einer informations-technischen Gesamtlösung bzgl. aller administrativen Verfahren, die Asylsuchende betreffen (S. 12, 61). Es dürfte aber offensichtlich sein, daß von einer durch die Karte integrierten Kommunikationsstruktur **Standardisierungseffekte** ausgehen würden, die länderspezifische oder lokale informationstechnische Verfahren prägen oder gar festlegen. Die föderale Eigenständigkeit würde nicht nur durch gemeinsame verfahrensrechtliche, sondern auch durch systemtechnische Vorgaben eingeschränkt (S. 162, ausdrücklich S. 172).

Wie oben dargestellt, verfolgt die Konzeption auch das Ziel der Veränderung des melderechtlichen Verfahrens bei Asylsuchenden. Während die sonstigen betroffenen Verfahren vom Bundesgesetzgeber allein geregelt werden können (AuslG, AsylVfG; AFG, SGB, AsylBLG), gilt dies nicht für das Melderecht. Hier liegt - ebenso wie beim Ausweisrecht - auch eine **Gesetzgebungskompetenz** bei den Ländern; dem Bund kommt nur eine Rahmenbefugnis zu (Art. 75 Nr. 5 GG).

IV. Ergebnis

Trotz gewisser Unstimmigkeiten und Unklarheiten ergibt die Studie, daß die Einführung einer AsylCard **technisch machbar** ist. Das in der Studie vorgesehene Systemdesign birgt jedoch Sicherheitsrisiken, die eine Umsetzung in der dargelegten Form verbieten. Aber auch eine modifizierte Realisierung würde den Preis der möglichen Vollüberwachung der betroffenen Asylsuchenden kosten. Daß eine solche Totalüberwachung in anderen Ländern, u.U. mit anderen Mitteln, praktiziert oder angestrebt wird (neben der Praxis in den Niederlanden gibt es in Großbritannien Pläne einer elektronischen Markierung von Flüchtlingen mit Hilfe von Ortungssystemen, vgl. FR und SZ v. 28.10.1998), ist kein Indiz für die Verfassungsverträglichkeit solcher Maßnahmen. **Aus datenschutzrechtlicher Sicht** ist daher von der Verwirklichung der vorgesehenen AsylCard **dringend abzuraten**.

Von der Studie nicht geprüft wurden Alternativen zur AsylCard, die mit dem Grundrecht auf informationelle Selbstbestimmung vereinbar sind. Aus meiner Sicht ließen sich die Hauptprobleme bei

der Datenverarbeitung im Asylverfahren (mangelnde Übereinstimmung bzgl. Identifizierungsdaten, Unsicherheit bei der Identifizierung, S. 14 ff., 27, 62 ff.) mit einem **opto-elektronisch lesbaren Flüchtlingsausweis** beseitigen, der in Form und Ausgestaltung dem deutschen Personalausweis nachempfunden sein könnte. Die bei der Realisierung eines solchen Identitätspapieres auftretenden datenschutzrechtlichen Fragestellungen wären relativ einfach lösbar. Kosten würden in einem erheblich geringeren Umfang anfallen, zumal zumindest teilweise auf eine schon bestehende Infrastruktur zurückgegriffen werden könnte. Zugleich könne damit dem Eindruck bzw. der Gefahr der Diskriminierung von Flüchtlingen und der ungerechtfertigten Ungleichbehandlung gegenüber sonstigen Menschen, vor allem deutschen Staatsangehörigen, begegnet werden.

Zurück zur Startseite