

Dr. Thilo Weichert

Datenschutz für Flüchtlinge nach der Anti-Terror-Gesetzgebung

I. EINFÜHRUNG

Das so genannte Terrorismusbekämpfungsgesetz (TeBekG) vom 9. Januar 2002 (BGBl. 2002 I, 361) hat bisher noch keinen erkennbaren Beitrag zur Bekämpfung des Terrorismus geleistet. Der Beitrag, den dieses Gesetz zum Grundrechtsabbau, zur Ausgrenzung und zur Diskriminierung von Ausländern und insbesondere von Flüchtlingen leistet, ist dagegen schon heute mit Händen zu greifen. Erstaunlicherweise war dies aber kaum Gegenstand der öffentlichen Diskussion. Die Debatte über biometrische Merkmale auf Ausweisen und Pässen für Deutsche wurde heftig geführt und brachte letztendlich für diese Pläne eine Beerdigung erster Klasse. Dass diese Pläne in Bezug auf Nicht-Deutsche weiter vorangetrieben werden, scheint kaum jemanden zu kümmern. Gegenüber den ursprünglichen Planungen des Bundesinnenministeriums blieben die Deutsche treffenden Regelungen praktisch nirgends unverändert. Im Ausländerrecht kam es dagegen kaum zu rechtsstaatlichen Eingrenzungen; ja weitere Verschärfungen wurden zur Debatte gestellt und fanden teilweise den Segen des Gesetzgebers.

Geradezu gespenstisch ist insofern nun die Diskussion um das Zuwanderungsgesetz. Es wird der Eindruck erweckt, dass hier das überkommene, teilweise noch polizeirechtlich ausgerichtete Ausländergesetz (AuslG) durch ein reines Aufenthaltsrecht abgelöst werden sollte. Tatsächlich finden sich aber sämtliche "Errungenschaften" des TeBekG in den Entwürfen zum Zuwanderungsgesetz wieder, mit der Folge, dass die polizeistaatliche, schon bisher verfassungsrechtlich angreifbare Komponente des AuslG (dazu Weichert in Huber, HdbAuslAsylR, Vorb § 75-80 AuslG Rdn. 28 ff.) nicht abgebaut, sondern weiter verstärkt wird.

Die Deutsche Vereinigung für Datenschutz (DVD e.V.) hat sich während des Gesetzgebungsverfahrens speziell der Frage des Abbaus des Datenschutzes für Ausländerinnen und Ausländer gewidmet, in ihrer ersten Stellungnahme vom 29.09.2001 (Datenschutznachrichten - DANA - 4/2001, 8 ff.) und insbesondere in einem ausführlichen Gutachten vom 15.11.2002 (Unbequem 46/47 - Dez. 2001, 22 ff., abrufbar unter www.aktiv.org/DVD/; siehe auch PE vom 16.11.2001, DANA 4/2001, 40). Auch wenn diese Kritik nicht die gewünschte Resonanz gefunden hat, so war und bleibt sie – insbesondere im Hin-

blick auf das Zuwanderungsgesetz – berechtigt und von aktueller Relevanz. Daher soll im Folgenden das TeBekG mit seinen Auswirkungen v.a. auf Flüchtlinge dargestellt und einer knappen juristischen Kritik unterworfen werden.

II. DAS DURCHLÖCHERTE ASYLGEHEIMNIS

Das Bundesamt für die Anerkennung ausländischer Flüchtlinge (BAFI) wie die Ausländerbehörden (ABH) erhalten mit § 18 Abs. 1a BVerfSchG das Recht, von sich aus den Verfassungsschutzbehörden personenbezogene Informationen über Bestrebungen nach § 3 Abs. 1 BVerfSchG zu übermitteln, "wenn tatsächliche Anhaltspunkte dafür vorliegen, dass die Übermittlung für die Erfüllung der Aufgaben der Verfassungsschutzbehörden erforderlich ist". § 3 Abs. 1 BVerfSchG beschränkt sich nicht auf Terrorismusbekämpfung oder auf gewaltbereite Bestrebungen, sondern schließt auch bloße extremistische Bestrebungen mit ein. Einfaches und legales politisches Engagement von Nichtdeutschen darf also zulässigerweise von Asyl- und Ausländerbehörden an die Verfassungsschutzbehörden weitergegeben werden. Mangels Kenntnis der geheimdienstlichen Bewertungen droht dabei ein Übermaß an Daten übermittelt zu werden.

Von höchster grundrechtlicher Relevanz ist diese Übermittlungsbefugnis für den Bereich des BAFI, da dieses bei der Entgegennahme der Begründungen von Asylanträgen sensible politische Informationen erfährt. Diese Asylgründe gibt nun das BAFI – so das neue Gesetz – von sich aus an den Verfassungsschutz weiter. Es dürfte wenige Asylgründe geben, die nicht für die Aufgabenerfüllung des Bundesamtes für Verfassungsschutz (BfV) oder für die Landesämter (LfV) für erforderlich angesehen werden könnten. Die schutzwürdigen Belange von Asylsuchenden sind nicht erwähnt und dürfen nach dem Wortlaut des Gesetzes nicht berücksichtigt werden. Es ist nicht vorgesehen, dass die erhaltenen Daten sofort auf ihre Relevanz hin überprüft werden und bei negativer Bewertung sofort gelöscht werden müssten. Auch an eine besondere Zweckbindung (z.B. auf die Bekämpfung terroristischer Bestrebungen) oder besondere technische Sicherungen wurde nicht gedacht.

Zunächst war vorgesehen, dass diese Daten gar an die Sicherheits- und Geheimdienstorgane des Heimatstaates, der auch Verfolgerstaat sein kann, weitergegeben werden. Einziges Hindernis wäre eine Abwägung mit den schutzwürdigen Interessen der Betroffenen (§ 19 Abs. 3 S. 2 BVerfSchG) gewesen. Dieses Problem wurde zunächst von den Politikern überhaupt nicht erkannt. Nachdem klar wurde, dass für die Antragstellenden der Asylantrag damit die Grundlage

weiteren politischer Verfolgung werden könnte, wurde ein Satz 2 in § 18 Abs. 1a BVerfSchG aufgenommen, wonach die Übermittlung ins Ausland unterbleibt, "es sei denn, die Übermittlung ist völkerrechtlich geboten". Außerdem wurde nach § 19 Abs. 4 BVerfSchG die Übermittlung an "andere Stellen" davon abhängig gemacht, dass das Bundesinnenministerium vorher zustimmt. Das BfV führt einen Nachweis über Zweck, Veranlassung, Aktenfundstelle und Empfänger der Übermittlung. Außerdem wird eine Zweckänderung beim Empfänger verboten. Schließlich ist dem Betroffenen vom BfV eine Mitteilung zu machen, "sobald eine Gefährdung seiner Aufgabenerfüllung durch die Mitteilung nicht mehr zu besorgen ist". Bei den mit heißer Nadel gestrickten Formulierungen wurde aber übersehen, dass bei ausländischen Datenempfängern eine Kontrolle der zweckgemäßen Nutzung nicht vorgenommen werden kann. Außerdem berechtigt § 19 Abs. 1a BVerfSchG auch die Landesämter für Verfassungsschutz (LfV), die Bindungen des § 19 Abs. 4 BVerfSchG gelten aber nur für das BfV. Die Anknüpfung bei den Auslandsübermittlungen an das Völkerrecht stellt einen Formelkompromiss dar, da nicht offen gelegt wurde, nach welchen völkerrechtlichen Regelungen ein Datenaustausch des BfV mit ausländischen Stellen "geboten" sein könnte.

Auch nach den Eingrenzungen der Weiterübermittlung der Daten ist die neu eingeführte praktisch unbegrenzte Übermittlungsbefugnis des BfV an die Verfassungsschutzbehörden ein Verstoß gegen das aus Art. 16a GG abzuleitende Asylgeheimnis. Art. 16a GG hat auch insofern eine Schutzwirkung, dass die von ihm offenbarten Asylgründe nicht zur weiteren Verfolgung oder zu anderen gravierenden Nachteilen führen dürfen (Bäumler GK-AsylVfG § 7 Rdn. 13 f.). Gibt es einen solchen Schutz nicht, so werden die Asylsuchenden daran gehindert, sich bei der Begründung ihrer politischen Verfolgung umfassend und wahrheitsgemäß zu offenbaren. Mit der neuen Regelung muss der Asylantragsteller davon ausgehen, dass seine Asylgründe den Verfassungsschutzbehörden weitergegeben werden. Er hat auch keine Sicherheit, dass sie nicht von dort weiterübermittelt werden. Allein die durch das BVerfSchG begründete Furcht, die Asylgründe könnten für weitere Verfolgungszwecke genutzt werden, greift in den Kernschutzbereich des Art. 16a GG ein (Weichert in Huber, HdbAuslAsylR, Vorb §§ 7, 8 AsylVfG Rdn. 10 f.).

III. DIE RENAISSANCE DER ASYLCARD

Noch die schwarz-gelbe Regierung plante für Asylsuchende als Ausweis- und Datenübermittlungsmedium eine Prozessor-Chipkarte unter

dem Namen AsylCard einzuführen (Weichert DANA 4/1998, 28 f.). Diese Karte, über die zur eindeutigen Identifikation der mit dem Dokument ausgewiesenen Person ein Fingerabdruck-Abgleich vorgesehen war, wurde nicht realisiert, u.a. weil die damit verbundenen rechtlichen Fragen nicht gelöst werden konnten (siehe das ausführliche Gutachten des ULD Schleswig-Holstein unter www.datenschutzzentrum.de).

Nunmehr wurde der biometrische Ausweis auch für Deutsche in die Diskussion gebracht. Während dessen Einführung als Personalausweis und Reisepass aber unter Gesetzesvorbehalt steht (§ 4 Abs. 4 S. 1 PassG, § 1 Abs. 5 S. 1 PersAuswG), sind im Ausländer- und Asylrecht weiterhin vergleichbare Ausländerausweise bzw. -dokumente vorgesehen. Diese sollen u.a. neben dem Lichtbild und der eigenhändigen Unterschrift "weitere biometrische Merkmale von Fingern oder Händen oder Gesicht des Inhabers enthalten" sowie eine "Zone für das automatische Lesen". Diese Dokumente haben unterschiedliche Namen: Aufenthaltsgenehmigung (§ 5 AuslG), Ausweisersatz (§ 39 Abs. 1 AuslG), Bescheinigung über die Duldung (§ 56a AuslG), Fiktionsbescheinigung (§ 69 Abs. 2 AuslG) oder Bescheinigung über die Aufenthaltsgestattung (§ 63 AsylVfG). Die geplanten Funktionen sind identisch. Die Einzelheiten sollen vom Bundesinnenministerium "nach Maßgabe der gemeinschaftlichen Regelungen durch Rechtsverordnung" präzisiert werden (§ 5 Abs. 6 AuslG). Sämtliche öffentliche Stellen können "die in der Zone für das automatische Lesen enthaltenen Daten zur Erfüllung ihrer gesetzlichen Aufgaben speichern, übermitteln und nutzen" (§ 5 Abs. 7 AuslG).

Der Umstand, dass es zur Einführung der Ausländerausweise nur einer Rechtsverordnung bedarf, spricht dafür, dass diese als Testprojekt für die Einführung von elektronischen Ausweisen generell verwirklicht werden sollen. Hierin liegt eine Ungleichbehandlung gegenüber deutschen Staatsangehörigen, für die keine sachliche Rechtfertigung erkennbar ist, so dass mit der vorrangigen Umsetzung der biometrischen Chipkarten-Ausländerausweise ein Gleichheitsverstoß nach Art. 3 Abs. 3 GG erfolgen würde.

Die dabei erwähnten biometrischen Identifizierungsmerkmale sind als Personenkennzeichen (PKZ) verwendbar, d.h. als Merkmal, über das verschiedenste Datenbestände zusammen geführt werden können. Wegen dieses Risikos wird bisher die generelle Nutzung solcher PKZ für verfassungswidrig gehalten (Kirchberg ZRP 1977, 137; Weichert AZRG, 1998, § 3 Rdn. 5-7). Ordnungsnummern wurden im deutschen Rechtssystem bisher nur unter restriktiven Voraussetzungen zugelassen. Hier jedoch wird in § 5 Abs. 7 AuslG

eine generelle Nutzungserlaubnis eröffnet mit der erklärten Absicht "maschinelle Datenabgleiche durchführen" zu können. Diese Regelung ist schwerlich mit den verfassungsgerichtlichen Vorgaben zur informationellen Gewaltenteilung und zur Zweckbindung in Einklang zu bringen (BVerfGE 65, 46 = NJW 1984, 422).

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 insbesondere auch für polizeiliche Zwecke. Es ist davon auszugehen, dass diese Merkmale auch für polizeiliche Spurenabgleiche verwendet werden. Von besonderer Tragweite ist angesichts des zunehmenden Einsatzes von Videoüberwachung im öffentlichen Raum die Zulassung der Gesichtsgeometrie als Identifizierungsmerkmal, da mit anderweit erfassten Videobildern automatisierte Musterabgleiche vorgenommen werden können. Die Methode der Identifikation mit Hilfe gesichtsgeometrischer Daten wird übrigens schon heute im Ausländerrecht praktiziert (DANA 3/2001, 17).

IV. SPRACHANALYSE

Das TeBekG erlaubt erstmalig ausdrücklich die offene Aufnahme und Auswertung des "gesprochenen Wortes" zur "Bestimmung des Herkunftsstaates oder der Herkunftsregion des Ausländers" (§ 41 Abs. 2 S. 2-4 AuslG, § 16 Abs. 2 S. 3-5 AsylVfG). Der Ausländer muss über die Erhebung vorher in Kenntnis gesetzt werden. Die Aufzeichnung wird bei der aufzeichnenden Behörde aufbewahrt. Die Sprachanalyse hat – wie die meisten sonstigen ausländerrechtlichen Änderungen – zunächst nichts mit der Bekämpfung des Terrorismus oder generell von Straftaten zu tun. Die Gesetzesnovelle war vielmehr ein willkommener Anlass, eine ohnehin geplante Änderung ohne viel Diskussion durchzusetzen. Die Sprachanalyse dient der Herkunftsbestimmung, die für die Durchsetzung aufenthaltsbeendender Maßnahmen von Bedeutung ist.

Sprach- und Dialektanalysen sind wenig aussagekräftig und wissenschaftlich fragwürdig. Eine rechtsstaatliche Hinterfragung der Ergebnisse ist kaum möglich. Es bestehen Zweifel, dass das vorgesehene "in-Kennnis-Setzen" eine ausreichende Aufklärung über mögliche Risiken beim Betroffenen und deren tatsächliche Kenntnisnahme sicherstellt.

Die Aufbewahrung der Sprachproben soll 10 Jahre lang erfolgen (§ 78 Abs. 4 Nr. 4 AuslG, § 16 Abs. 6 AsylVfG). Es ist zunächst nicht erkennbar, weshalb nach Erstellung des Herkunftsgutachtens und der Zuordnung der Sprache zu einer Region keine Löschung vorgesehen ist. Die weitere

Aufbewahrung macht nur Sinn, wenn damit später eine biometrische Sprachzuordnung, z.B. von abgehörten Telefonaten oder sonstigen Sprachaufzeichnungen, geplant ist. Tatsächlich ist gewollt, die gewonnenen Unterlagen auch zu nutzen "zur Feststellung der Identität oder Zuordnung von Beweismitteln für Zwecke des Strafverfahrens oder zur Gefahrenabwehr" (§ 78 Abs. 3 S. 1 AuslG, § 16 Abs. 5 S. 1 AsylVfG). Dies ist auch der ausschließlich weiter verfolgte Zweck. Da es sich hierbei um eine anlasslose Vorratsdatenspeicherung bzgl. insofern völlig Unverdächtiger handelt, muss die weitere Aufbewahrung der Sprachproben als verfassungswidrig angesehen werden. Die nachträglich aufgenommene Regelung zum Aufbewahrungsort der Sprachproben (nicht beim BKA, sondern bei der aufzeichnenden Stelle) ändert an der rechtlichen Bewertung nichts. Die Besonderheit dieses Eingriffs ins Persönlichkeitsrecht liegt darin, dass das Sprechen für den Menschen zur Aufrechterhaltung seiner Sozialität unabdingbar ist.

V. IDENTITÄTSSICHERUNG PER DAKTYLOSKOPIE

Schon bisher war geregelt, dass von sämtlichen Bürgerkriegsflüchtlingen (§ 41 a AuslG) und Asylsuchenden (§ 16 AsylVfG) als Identitätssicherungsmaßnahme Fingerabdrücke erhoben und zentral beim BKA gespeichert werden. Ansonsten konnte eine Maßnahme der Identitätssicherung i.d.R. nur durch Zweifel über die Person oder die Staatsangehörigkeit legitimiert werden (§ 41 Abs. 1 AuslG). Diese Praxis der Identitätssicherung wird nun durch eine Kann-Regelung nach § 41 Abs. 3 AuslG auf weitere Personengruppen ausgedehnt, ohne dass Identitätszweifel nötig wären:

1. wenn der Ausländer mit einem gefälschten oder verfälschten Pass oder Passersatz einreisen will oder eingereist ist (bisher Abs. 3 S. 1 1. Alt.),
2. wenn sonstige Anhaltspunkte den Verdacht begründen, dass der Ausländer nach einer Zurückweisung oder Beendigung des Aufenthalts erneut unerlaubt ins Bundesgebiet einreisen will (bisher Abs. 3 S. 1 2. Alt.),
3. wenn der Ausländer in einen in § 26a Abs. 2 AsylVfG genannten Drittstaat zurückgewiesen oder zurückgeschoben wird (bisher Abs. 3 S. 2),
4. wenn ein Versagungsgrund nach § 8 Abs. 1 Nr. 5 AuslG (extremistische Betätigung) festgestellt worden ist,
5. bei der Beantragung eines Visums für einen Aufenthalt von mehr als drei Monaten durch Staatsangehörige der Staaten, bei denen Rückführungsschwierigkeiten bestehen sowie in den nach § 64a Abs. 4 AuslG (besonderes Ver-

fahren bei Staatsangehörigen von "Schurkenstaaten", s.u. VI.) festgelegten Fällen.

Außerdem sind sämtliche mindestens 14-jährige Ausländer, die aus einem Drittstaat unerlaubt eingereist sind, und solche, die sich illegal und ohne Duldung im Bundesgebiet aufhalten und bei denen Anhaltspunkte für einen Asylantrag in einem anderen EU-Staat bestehen, durch die Erfassung aller zehn Fingerabdrücke zu identifizieren (§ 41 Abs. 4, 5 AuslG).

Schon die bisherige Regelung der daktyloskopischen (Fingerabdruck-) Erfassung war als Vorratsdatenspeicherung verfassungswidrig, soweit keine individuellen Gründe für Zweifel an der Identität bestanden (Grünewald in GK-AuslR § 41a Rdn. 6-10; Weichert in Huber HdbAuslAsylR § 41a Rdn. 2). Der Katalog wird nun um Fälle erweitert, bei denen von Anfang an an der Identität der Betroffenen keine Zweifel bestehen. Der Verweis darauf, dass mit dieser Regelung teilweise eine Anpassung an die europäische EUODAC-Verordnung erfolgt, ist nicht geeignet, die bestehenden verfassungsrechtlichen Bedenken zu zerstreuen.

Die angefertigten Unterlagen werden beim BKA teilweise länger, nämlich bis zu 10 Jahren aufbewahrt (§ 78 Abs. 4 Nr. 4 AuslG). Dies soll insbesondere und ausnahmslos für sämtliche Asylsuchende und evtl. für Bürgerkriegsflüchtlinge gelten (§ 16 Abs. 6 AsylVfG; siehe den entstandenen Verweisungsfehler in § 41a Abs. 3 AuslG). Damit wirkt die auf einer pauschalen Verdächtigung basierende Datenerhebung für einen außergewöhnlichen Zeitraum fort. Selbst wenn die Rückführungsschwierigkeiten in einen Staat oder der pauschale Extremismusverdacht durch politische Änderungen nicht mehr bestehen, soll dies nichts an der übermäßig langen Vorratsdatenspeicherung ändern.

Die angefertigten ED-Unterlagen dürfen generell "zur Feststellung der Identität oder der Zuordnung von Beweismitteln für Zwecke des Strafverfahrens oder zur Gefahrenabwehr" genutzt werden (§ 78 Abs. 3 AuslG, § 16 Abs. 5 S. 1 AsylVfG). Bisher bedurfte es für diese Zweckänderung bei Flüchtlingen bestimmter Tatsachen, die "die Annahme begründen, dass dies zur Aufklärung einer Straftat führen wird, oder wenn es zur Abwehr einer erheblichen Gefahr für die öffentliche Sicherheit erforderlich ist" (§ 16 Abs. 5 S. 1 AsylVfG a.F.). Mit der Neuregelung wird der polizeiliche Daten- und Spurenabgleich de facto auf sämtliche per ED-Maßnahme erfassten ausländischen Menschen ausgeweitet, ohne dass es eines konkreten Verdachtes bedürfte. Diese Menschen werden als potenzielle Straftäter behandelt. Die weiterhin vorgesehene Trennung zwischen polizeilichen und ausländerrechtlichen Datenbestän-

den beim BKA (§ 78 Abs. 2 AuslG, § 16 Abs. 4 AsylVfG) wird ad absurdum geführt.

Es gibt keinen vernünftigen Grund, (auch anerkannte) Asylsuchende oder sonstige Flüchtlinge einem höheren Kriminalitätsverdacht auszusetzen als sonstige Menschen generell. Daher verstößt die Zulassung des polizeilichen Datenabgleichs gegen den Gleichheitsgrundsatz des Art. 3 Abs. 1 GG. Zudem wird das Schutzziel des Art. 16a GG in sein Gegenteil verkehrt, wenn unabhängig vom Ausgang des Asylverfahrens die ED-Unterlagen aus dem Asylverfahren zu polizeilichen Zwecken genutzt werden.

VI. SCHURKENSTAATEN-REGELUNG

Zur Feststellung von extremistischen Bestrebungen (Versagungsgründe nach § 8 Abs. 1 Nr. 5 AuslG) werden künftig bei besonders definierten Gruppen von Ausländern vor Visumerteilung Anfragen bei folgenden Einrichtungen vorgenommen: Bundesnachrichtendienst (BND), Bundesamt für Verfassungsschutz (BfV), Militärischer Abschirmdienst (MAD), BKA und Zollkriminalamt (§ 64a Abs. 1 AuslG). Das gleiche Verfahren erfolgt vor der Erteilung oder Verlängerung einer sonstigen Aufenthaltsgenehmigung (§ 64a Abs. 2 AuslG).

Die Gruppen der Betroffenen werden vom Bundesinnenministerium im Einvernehmen mit dem Auswärtigen Amt über die Staatsangehörigkeit (sog. Schurkenstaaten) oder "in sonstiger Weise bestimmt" (§ 64a Abs. 4 AuslG). Die Festlegung der Gruppen, bei denen ein Generalverdacht angenommen wird und deshalb Regelanfragen bei den Bundessicherheitsbehörden erfolgen, ist äußerst vage. Daran ändert auch der Umstand nichts, dass neben der Staatsangehörigkeit weitere Merkmale wie Alter, Geschlecht und Familienstand herangezogen werden können. Es erfolgt eine Vorratsdatenerhebung mit anschließender Vorratsdatenspeicherung. Verfahrensrechtlich äußerst problematisch ist, dass die Festlegung der Gruppen ohne jegliche Rechtsförmlichkeit, z.B. durch Erlass einer Rechtsverordnung, erfolgen soll. Die Geeignetheit geschweige denn die Erforderlichkeit der Maßnahme wurde im Gesetzgebungsverfahren nicht 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 dabei visums- oder aufenthaltsrechtlich relevante Erkenntnis ergeben werden. Bei vielen der Stellen, deren Datenerhebungsbefugnis sich auf das Bundesgebiet beschränkt, macht die Anfrage zu visumantragstellenden Personen keinen Sinn,

da diese sich mit großer Wahrscheinlichkeit noch nie in der Bundesrepublik aufgehalten haben.

Nach § 64a Abs. 3 S. 2 AuslG dürfen die Sicherheitsbehörden und Nachrichtendienste "die mit der Anfrage übermittelten Daten speichern und nutzen, wenn das zur Erfüllung ihrer gesetzlichen Aufgaben erforderlich ist". Diese materiell unbeschränkte Nutzungserlaubnis im Rahmen eines Vorfeld-Beteiligungsverfahrens durch sämtliche genannten "Bedarfsträger" verletzt den datenschutzrechtlichen Zweckbindungsgrundsatz und das Bestimmtheitsgebot; die Regelung ist unverhältnismäßig und zugleich ein Gleichheitsverstoß gegen Art. 3 Abs. 1 GG im Verhältnis zu sämtlichen Menschen, über die nicht derart leicht Daten beschafft und genutzt werden können. Systematisch hat diese Regelung auch nichts im AuslG zu suchen; sie gehört in die jeweiligen Fachgesetze.

VII. AUSLÄNDERZENTRALREGISTERGESETZ

Mit dem Ausländerzentralregister (AZR), für das es seit 1994 eine gesetzliche Grundlage gibt, wird schon bisher eine sehr weit gehende Erfassung der gesamten nichtdeutschen Bevölkerung praktiziert, die verfassungsrechtlich angreifbar ist (ausführlich Weichert, AZRG, 1998, Einf. Rdn. 13 ff.). Die verfassungsrechtliche Kritik hat nach der Zurückweisung von entsprechenden Verfassungsbeschwerden durch das BVerfG (BVerfG DuD 2002, 45 ff.) nichts an Berechtigung verloren, zumal vom BVerfG bei der rein formalen Ablehnung der Zulässigkeit ausführlich die materiell-rechtlichen Bedenken referiert wurden. Das AZRG legitimiert unverhältnismäßige Eingriffe in das Recht auf informationelle Selbstbestimmung auf Basis unbestimmter Regelungen. Die sicherheitsbehördliche Nutzung des AZR ist eine sachlich nicht begründ- und rechtfertigbare Ungleichbehandlung gegenüber den Deutschen. Statt nun diese vorhandenen Defizite abzubauen, wurden mit dem TeBekG weitere Verfassungsverstöße programmiert.

In einer unsinnigen, zugleich aber gefährlichen Regelung erlaubt § 3 Nr. 5 AZRG die Speicherung von "freiwillig gemachten Angaben zur Religionszugehörigkeit". Die Zugehörigkeit zu einer nicht besonders privilegierten Religionsgemeinschaft ist für deutsche Behörden nur aus Gründen der Gefahrenabwehr und Strafverfolgung von Interesse. Es macht keinen Sinn, freiwillig Daten zu erbitten, die dann zum Nachteil der Betroffenen genutzt werden sollen. Weshalb sollte ein religiös motivierter potenzieller Straftäter Angaben zu seinem Glauben machen, wenn er davon ausgehen muss, dass diese Information polizeilich gegen ihn genutzt wird? Es ist zu befürchten, dass faktisch die Datenerhebung über die Ausländer-

behörden in einer Form erfolgen wird, die Zweifel an der Freiwilligkeit begründet.

Voraussetzung für die sicherheitsbehördliche Rasterfahndung mit AZR-Daten soll nicht mehr eine "im Einzelfall bestehende Gefahr" sein, sondern generell der Zweck der "Abwehr einer Gefahr". Die Rasterfahndung für den BND ist künftig auch erlaubt 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 G-10-G). Zudem fiel der Ausschluss sicherheitsbehördlicher Rasterfahndungen bei Personen mit einem gesicherten Aufenthaltsstatus (Aufenthaltsberechtigung oder unbefristete Aufenthaltserlaubnis) weg (§§ 12, 31 AZRG).

Rasterfahndungen betreffen generell eine große Zahl unverdächtig Personen, bei denen im Fall des Vorliegens der Rastermerkmale durch die sicherheitsbehördliche Ausermittlung im Einzelfall sehr intensive Grundrechtseingriffe erfolgen können. Es ist unverhältnismäßig, diese intensiven Grundrechtseingriffe schon mit der Annahme einer allgemeinen Gefahrenlage zu rechtfertigen. Der Gesetzeswortlaut steht im Widerspruch zur amtlichen Begründung, wo auf die besonders schwerwiegenden Gefahren der Begehung terroristischer Anschläge verwiesen wird. Weshalb sämtliche Geheimdienste die Befugnis zur Durchführung von Rasterfahndungsmaßnahmen erhalten, ist nicht nachvollziehbar. Die Gefahr paralleler, nicht abgestimmter Maßnahmen ist augenscheinlich.

In § 15 AZRG wird die Befugnis des AZR-Datenabrufs für Zwecke der Zuverlässigkeitsprüfung nach § 29d LuftVerkehrsG durch die Landesluftfahrtbehörden eröffnet. Damit wird das AZR erstmals direkt für Zwecke der Sicherheitsüberprüfungen nutzbar gemacht. Angesichts der ohnehin vorgesehenen Abfrage bei Polizei, Geheimdiensten, Bundeszentralregister sowie im Bedarfsfall bei anderen Stellen ist nicht erkennbar, welchen zusätzlichen Erkenntniswert die AZR-Daten haben sollen, zumal diese i.d.R. genau von den Behörden stammen, die ohnehin schon bei der Überprüfung eingeschaltet werden. Die meisten AZR-Daten sind für Zuverlässigkeitsprüfungen nicht relevant. Dessen ungeachtet wird deren Übermittlung für diese Zwecke ohne Einschränkung erlaubt.

Bisher konnten Geheimdienste im AZR nur auf Personalien und Verwaltungsdaten online zugreifen. Jetzt erlaubt § 22 Abs. 1 Nr. 8 AZRG den umfassenden geheimdienstlichen Zugriff im automatisierten Abrufverfahren. Auch die Beschränkung auf eilbedürftige Fälle und die Verpflichtung, diese Eilbedürftigkeit zu protokollieren

(§ 22 Abs. 2 S. 2, 3 AZRG a.F.) ist weggefallen. Mit dieser "Erleichterung" wird die Trennung zwischen Geheimdienste und Verwaltung ausgehöhlt. Die Begründung, die Daten würden "effektiv und zügig" benötigt und die konventionelle Auskunft "behindere die Arbeit der Dienste", wird weder belegt noch ist sie plausibel. Mit ihr ließe sich die Aufhebung jeder verfahrensrechtlichen Begrenzung personenbezogener Datenverarbeitung rechtfertigen. Protokollierungs- und Begründungsverpflichtungen zielen auf eine Verbesserung der Kontrolle und eine Erhöhung der Rationalität von Verwaltungsentscheidungen. Das Vieraugenprinzip bei Datenübermittlungen, das bei dem automatisierten Abrufverfahren entfällt, ist ein zentrales Instrument der Sicherung der Rechtmäßigkeit von Datenübermittlungen.

VIII. SCHLUSS

Während es sich bei den meisten sonstigen Normen des Terrorismusbekämpfungsgesetzes um Schläferregelungen handelt, also um Befugnisse, die über Jahre hinweg schlummern können, ohne eine praktische Relevanz zu erhalten, gilt dies für die Änderungen des Asyl- und Ausländerrechts fast durchgängig nicht. Die Anwendung der Normen bedingen sofortige und teilweise schwerwiegende Grundrechtseingriffe. Dies gilt nicht nur für die oben beschriebenen Gesetze, sondern z.B. auch für die vor dem 11. September nur von Bayern praktizierte Regelanfrage bei den Ämtern für Verfassungsschutz im Fall von Einbürgerungen, dem nachzuahmen sich nach den Anschlägen sofort sämtliche Länder beeilten (§ 86 Nr. 2 AuslG; zur Regelanfrage Berlitz in GK-StAR § 86 AuslG Rdn. 138; kritisch DANA 1/1999, 34 f.).

Um so bedauerlicher ist es, dass sich der Gesetzgeber gerade hier nicht – wie an anderer Stellen (§ 8 Abs. 10 BVerfSchG) – zu einer klaren Evaluierungsregelung durchringen konnte. Eine nicht ganz durchsichtige Funktion erfüllt insofern Art. 22 Abs. 3 TeBekG, der nahe legt, dass auch die Übermittlung von asyl- und ausländerbehördlichen Daten vor Ablauf der Gültigkeitsfrist der Änderungen des BVerfSchG am 11. Januar 2007 zu evaluieren ist. Dies ist aber nur möglich, wenn vom Inkrafttreten des TeBekG an über sämtliche

Datenübermittlungen nach § 18 Abs. 1a BVerfSchG an das BfV wie an die LfV eine Dokumentation angelegt und deren Wirksamkeit für die Aufgabenerfüllung protokolliert wird. Ob der Gesetzgeber die Evaluierungspflicht auch auf die Geheimdienstbefugnisse etwa nach dem Ausländerrecht (z.B. § 64a Abs. 1, 2 AuslG, § 22 Abs. 1 Nr. 8 AZRG) erstrecken wollte, ist nicht eindeutig erkennbar. Vom Sinn und Zweck der Evaluierungsregelung muss davon ausgegangen werden. Leider nicht erfasst sind eindeutig sämtliche in ausländer- und asylrechtlichen Regelungen enthaltenen Vorratsdatensammlungen für polizeiliche Zwecke.

Von kurzfristig hoher praktischer Relevanz für viele Ausländerinnen und Ausländer sind die aktuell durchgeführten Rasterfahndungen nach Landesrecht, bei denen es zumindest bei den polizeilichen Trefferfällen zu Speicherungen in polizeilichen Datenbanken kommt. Zwar dürften diese Daten nicht für asyl- und ausländerrechtliche Zwecke genutzt werden, solange sich hieraus nicht ein konkreter Tatverdacht ergeben hat. Dass diese klare Rechtslage von Seiten der Polizei nicht erkannt wird, lässt für viele der Betroffenen aus ausländerrechtliches Unbill befürchten.

Schon der Erlass der neuen Regelungen und in verstärktem Maße deren Anwendung sind geeignet, bei dem deutschen wie beim ausländischen Teil unserer gemeinsamen Bevölkerung vor einander Angst, Abwehr und Aggression zu schüren. Damit wird keine Sicherheit geschaffen. Auch wenn dem Gesetzgeber dies vielleicht nicht bewusst war, so hat er Gesetze gemacht, die ein Klima schaffen, das dem Terrorismus förderlich ist. Im Rahmen der Zuwanderungsgesetzgebung wäre es möglich gewesen, elegant und ohne großen Gesichtverlust, einen gewaltigen politischen Fehler zurückzunehmen. Nur scheint auch das bisher von den deutschen Politikern bisher nicht erkannt worden zu sein.

Der Autor ist Vorsitzender der Deutschen Vereinigung für Datenschutz e.V., Stellv. Leiter des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein