Stiftung Deutsches Forum für Kriminalprävention
Dahlmannstraße 5-7
53113 Bonn

Tel. (0228) 28044-0 Fax (0228) 28044-21
www.kriminalpraevention.de
eMail: dfk@kriminalpraevention.de

Symposium
Biometrie und Flughafensicherheit

Berlin, 31. März 2004

Inhaltsübersicht:

Vorwort

Das Symposium „Biometrie und Flughafensicherheit“ fand auf Einladung des Deutschen Forums für Kriminalprävention – DFK – am 31. März 2004 in Berlin in der Bundesdruckerei statt. Sie führte eine große Zahl von Interessierten aus der Politik, vor allem aber auch der Industrie, den Flughäfen und Fluggesellschaften, den Polizeibehörden und dem Datenschutz zusammen, um gemeinsam über den vorgelegten Diskussionsbeitrag des DFK-Arbeitskreises Kriminalprävention und Biometrie sowie damit im Zusammenhang stehende Fragen zu diskutieren.

Der Schutz vor Kriminalität und Terrorismus mit seinen zahlreichen internationalen Verflechtungen und qualitativ neuen Gefahren hat nach den Anschlägen vom 11. September 2001 in den USA und zuletzt am 11. März 2004 in Madrid eine zunehmende Bedeutung gewonnen und die westlichen Gesellschaften stark verunsichert. Das Schutzbedürfnis ist erheblich gestiegen, die Akzeptanz von normalerweise als lästig, hinderlich und bürokratisch empfundenen Kontrollen und Sicherheitsvorkehrungen hat demgegenüber deutlich zugenommen.

Bekanntlich lassen sich offensichtlich gefährdete Örtlichkeiten oftmals mit polizeilichen Maßnahmen hinreichend schützen. Bei anderen komplexen Anlagen, die als Ziel von Terroristen ins Auge gefasst werden, um die Bevölkerung wahllos zu treffen und zu einer allgemeinen Unsicherheit beizutragen, so genannten „weichen Zielen“, ist dies nur eingeschränkt möglich. Damit müssen Wege und Möglichkeiten des Selbstschutzes stark in den Vordergrund rücken. Dies gilt insbesondere für die Verkehrsinfrastruktur und innerhalb dieses Feldes wiederum besonders für die Flughäfen und den Flugverkehr.

Zum Schutz der Mitarbeiterinnen und Mitarbeiter der Flughäfen, der Fluggesellschaften, der Fluggäste und der übrigen Gäste von Flughäfen müssen wir alles tatsächlich und rechtlich mögliche tun, ohne die Freiheit jedes einzelnen und unserer Gesellschaft oder gar rechtsstaatliche Prinzipien aufzugeben. Dies ist eine Gratwanderung.

Bei dieser schwierigen und komplexen Aufgabe können technische Systeme wichtige Hilfsmittel sein. Ob und wie sie als Ergänzung zur Erhöhung der Sicherheit oder gar als Ersatz für personell aufwändigere andere Sicherungsmittel eingesetzt werden können, ist Gegenstand der Ausarbeitung des DFK-Arbeitskreises Kriminalprävention und Biometrie, die bei diesem Symposium vorgestellt, erläutert und diskutiert wurde.

Der Bundesdruckerei als vorzügliche Gastgeberin sei an dieser Stelle nochmals gedankt.

(Norbert Salmon, stellvertretender Voststandsvorsitzender des DFK)

Programm

Moderation:	Norbert Salmon, stellv. Vorstandsvorsitzender DFK
10.00 Uhr	**Begrüßung und Einführung** Norbert Salmon
	Grußwort Moritz Gerke, Geschäftsführer Bundesdruckerei
10.30 Uhr	**Vorstellung des Konzeptes Airport Security** Jürgen Junghanns, BHE Dr. Ulrich Krienen, ZVEI Norbert Küster, ZVEI
11.30 Uhr	**Leistungsfähigkeit der Biometrie-Technik – ein aktueller Überblick** Prof. Dr. Michael Behrens, Institut für biometrische Identifikationssysteme, FH Gießen-Friedberg
12.10 Uhr	**Stellungnahme Flughafenbetreiber** Dagmar Naumann, FRAPORT AG
12.30 Uhr	**Mittagspause**
13.00 Uhr	**Pressekonferenz**
13.30 Uhr	**Biometrie im Kontext der aktuellen Erfordernisse zur Flugsicherheit** Dr. Günther Beckstein, Bayerischer Staatsminister des Innern
14.00 Uhr	**Der Einsatz biometrischer Verfahren aus datenschutzrechtlicher Sicht** Peter Schaar, Bundesbeauftragter für den Datenschutz
14.30 Uhr	**Diskussion: Biometrie und Flughafensicherheit – Was fordert die Politik?**
	Moderation: Bernd Seibt, ZVEI **mit:** Dr. Günther Beckstein, STMI Bayern Clemens Binninger, MdB, CDU / CSU Dr. Max Stadler, MdB, FDP Silke Stokar, MdB, Bündnis 90/Die Grünen Dr. Dieter Wiefelspütz, MdB, SPD
15.50 Uhr	**Zusammenfassung und Ausblick** Norbert Salmon
16.00 Uhr	**Nachlese – Möglichkeit für Gespräche**

Die Veranstaltung: Zusammenfassender Bericht

Am 31. März 2004 fanden sich auf Einladung der Stiftung Deutsches Forum Kriminalprävention über 100 Teilnehmer aus Wirtschaft, Politik und Behörden in den Räumen der Bundesdruckerei Berlin ein und nahmen an einer Fachtagung zum Thema „Biometrie und Flughafensicherheit“ teil.

Die Entwicklungen in der Biometrie, der technischen Erkennung von personeneigenen Merkmalen, eröffnen neue Möglichkeiten für die Kriminalprävention, die besonders für die Sicherheit an Flughäfen von großem Nutzwert scheinen. Die gegenwärtigen Gefahren durch den internationalen Terrorismus haben bereits zu höheren Sicherheitsstandards geführt. Neben verschärften Fluggastkontrollen wird seit dem 19. Januar 2004 eine Personen- und Gepäckkontrolle für alle Mitarbeiterinnen und Mitarbeiter eines Flughafens beim Betreten der Sicherheitsbereiche verlangt. Das stellt die Flughafenbetreiber vor logistische, zeitliche und daher auch kostenwirksame Probleme. Mittels der Biometrie-Technik können diese Prozesse erleichtert werden.

Biometrie ist ein Thema, das von Erwartungen und Befürchtungen gleichermaßen besetzt ist, bei denen es vornehmlich um das notwendige Ausmaß von Sicherheitsmaßnahmen und einer angemessenen Gewährleistung datenschutzrechtlicher Belange geht. Dem DFK war es gelungen, für das Symposium Vortragende aus allen für die Diskussion relevanten Kreisen zu gewinnen, namentlich aus dem Bereich der Flughafenwirtschaft, der Wissenschaft, der Politik und des Datenschutzes. Die Veranstaltung wurde durch eine Podiumsdiskussion abgerundet, an der neben dem Bayerischen Staatsminister des Innern Dr. Günther Beckstein die Biometrie-Experten der Bundesfraktionen Silke Stokar (Bündnis 90 / Die Grünen), Clemens Binninger (CDU) und Dr. Max Stadler (FDP) sowie der Bundesbeauftragte für den Datenschutz Peter Schaar teilnahmen. SPD Innenexperte Dr. Dieter Wiefelspütz hatte seine Teilnahme kurzfristig und sehr zum Bedauern des DFK absagen müssen.

Im Mittelpunkt der Veranstaltung stand die Präsentation des im DFK-Arbeitskreis *Kriminalprävention und Biometrie* erarbeiteten Diskussionspapiers „Airport Security – Biometrische Applikationen zur Verbesserung der Sicherheit an Flughäfen“.

Das Konzept enthält Vorschläge, wie Biometrie unter kriminalpräventiven Gesichtspunkten sinnvoll im Flughafenbetrieb einzusetzen ist und beschreibt insbesondere die Einführung eines standardisierten „Flughafenausweises“ für Mitarbeiter der Flughafenbetreiber, Fluggesellschaften und sonstiger im Sicherheitsbereich eines Flughafens tätige Unternehmen. Auf dem Ausweis, der nach einer Sicherheitsprüfung ausgestellt wird, werden biometrische Daten des Benutzers gespeichert und der Zutritt zum Sicherheitsbereich dem Berechtigten nur nach maschinellem Abgleich der Daten mit den personeneigenen Merkmalen des Ausweisnutzers gewährt. Der Ausweis kann folglich nicht von Unberechtigten missbraucht werden. Die Zutrittskontrolle könnte auf diesem Wege vollautomatisch und zeiteffizient erfolgen.

Der weiterhin vorgeschlagene „Flugpass“ basiert auf der gleichen Idee wie der Flughafenausweis für Mitarbeiter, würde jedoch für Passagiere der gewerblichen Luftfahrt gelten.

In erster Linie soll das Konzept, entstanden unter Mitwirkung von potentiellen Nutzern biometrischer Verfahren, Herstellern biometrischer Systeme, Datenschützern und Vertretern der Sicherheitsbehörden „zu einer unvoreingenommen fachlichen Bewertung des präventiven Nutzen von Biometrie beitragen“, so Norbert Salmon, stellvertretender Vorsitzender des DFK und Moderator der Veranstaltung. Besonders im Spannungsfeld zum Datenschutz weist das Konzept auf noch zu lösende Konflikte hin.

Prof. Dr. Michael Behrens vom Institut für biometrische Identifikationssysteme an der FH Gießen-Friedberg verdeutlichte mit seinem Vortrag über die aktuelle Leitungsfähigkeit der Biometrie-Technik, dass die im Diskussionspapier vorgestellten biometrischen Alternativen bzw. Ergänzungen zu den Kontrollen an Flughäfen technisch durchaus umsetzbar seien.

Die Bereichsleiterin Infrastruktur, Flug- und Terminalbetrieb der Fraport AG Dagmar Naumann machte in ihrer Stellungnahme zum Konzept deutlich, dass Biometrie seitens der Flughafenbetreiber als eine gute *Ergänzung* zu den herkömmlichen Kontrollverfahren gesehen wird. Zu- und Durchgangskontrollen könnten effizient unterstützt und beschleunigt werden. Der Gesetzgeber müsse hier zügig die richtigen Vorraussetzungen schaffen. Nicht zuletzt müsse eine Kooperation auf internationaler Ebene erreicht werden, um Standardisierungen voranzutreiben.

Dass Biometrie eine sehr gute Möglichkeit ist, die Sicherheit im nicht-hoheitlichen Bereich zu gestalten, wird auch vom bayerischen Innenminister Dr. Günther Beckstein vertreten. Der Gebrauch von Biometrie sei vielmehr schon längst überfällig. Der Innenminister betonte in Bezug auf die datenschutzrechtlichen Aspekte, dass das Ziel des Einsatzes von Biometrie nicht eine Überwachung des Normalbürgers sein darf und auch nicht sein wird.

Auch der Bundesbeauftragte für den Datenschutz Peter Schaar versteht eine Reihe biometrischer Applikationen als geeignete und aus datenschutzrechtlicher Sichtweise qualifizierte Methoden zur Optimierung von Sicherheitskontrollprozessen. So bestünden bei der Verifikation von Personen anhand biometrischer Merkmale, wie im Diskussionspapier für den Mitarbeiterausweis vorgeschlagen, per se keine Bedenken aus datenschutzrechtlicher Sicht, weil die Daten dezentral auf der Ausweiskarte gespeichert werden könnten. Als problematischer bewertete Schaar die Speicherung von Daten in einer zentralen Datenbank, was im Hinblick auf eine Identifikation von Personen unvermeidlich wäre. Letztlich müsse auch darüber nachgedacht werden, wer in einem globalen System Zugang zu den Daten hätte und ggf. nicht gemäß deutscher Standards damit umginge.

Der datenschutzrechtliche Aspekt bildete auch in der anschließenden Podiumsdiskussion einen Schwerpunkt. Während der Diskussion plädierte MdB Binninger (CDU) für eine zügige Einführung von biometrischen Merkmalen in Ausweispapieren und dementspre-

chend biometrischer Verfahren bei Grenzkontrollen, durchaus aber auch im Kontext anderer Applikationen z.B. in der Fahndung. Hierfür müssten seitens des Gesetzgebers schnell die notwendigen Vorraussetzungen geschaffen werden. Silke Stokar (Bündnis 90 / Die Grünen) und Dr. Max Stadler (FDP) bewerteten den gesetzlichen Rahmen für den Biometrie-Einsatz als ausreichend. MdB Stokar warnte vor einer blinden Technikgläubigkeit. Sie betonte, dass darüber hinaus nur kooperative Verfahren, bei denen Personen selber ihre Daten zur Verfügung stellen und sich immer bewusst darüber sind, wann sie Objekt eines biometrischen Scans werden, in einer freiheitlichen Bürgergesellschaft akzeptabel seien.

Das DFK wird sehr aufmerksam verfolgen, ob und in welchem Ausmaß sich die Biometrie als technisches Instrument zur Unterstützung von Flughafensicherheit durchsetzen wird. Ziel des DFK war es, Impulse für den öffentlichen Diskurs zu geben.

Die Inhalte des Symposiums werden dokumentiert und in Form einer Broschüre herausgegeben und als PDF-Datei unter www.kriminalpraevention.de abrufbar sein. Das Diskussionspapier „Airport Security – Biometrische Applikationen zur Verbesserung der Sicherheit auf Flughäfen“ steht dort ebenfalls als Download zur Verfügung.

Der Gastgeber: Die Bundesdruckerei GmbH

Mit ihrem Engagement als Stifter des Deutschen Forums für Kriminalprävention (DFK) hatte die Bundesdruckerei GmbH mit ihren Räumlichkeiten und der organisatorischen Unterstützung den Rahmen für das Gelingen des Symposiums „Biometrie und Flughafensicherheit“ gegeben. Die Geschäftsführer Moritz Gerke, Ulrich Haman und Klaus-Dieter Langen ließen es sich nicht nehmen, als Hausherren die Gäste zu begrüßen und persönlich zu den Teilnehmern zu gehören.

Das Unternehmen versteht sich nach der Privatisierung vor vier Jahren als ein führender Konzern der Hochsicherheitstechnologie, in dem rund 1300 Mitarbeiter beschäftigt sind und ein jährlicher Umsatz von über 220 Mio EUR erreicht wird. Die klassischen Produkte sind Banknoten, Postwertzeichen, Steuerzeichen, Ausweise und Reisepässe. Die Bundesdruckerei zählt zu den Herstellern der sichersten Personaldokumente. Für die Bundesrepublik Deutschland werden hier alle Personalausweise und Reisepässe sowie Kartenführerscheine gefertigt und somit das weltweit größte Pass- und Ausweissystem bedient.

Das Unternehmen ist auf die geplante Ausstattung von Personaldokumenten mit biometrischen Merkmalen gut vorbereitet und versteht sich als Systemlieferant, der neben den neuartigen Dokumenten auch die technischen Anlagen zum Personen-Dokumenten-Abgleich liefert.

Zu den Teilnehmern der Veranstaltung gehörten eine Reihe von Wettbewerbern, die Lösungen für die aktuellen und zukünftigen Sicherheitsherausforderungen anbieten.

Das Konzept: Airport-Security – Biometrische Applikationen zur Verbesserung der Sicherheit auf Flughäfen

von Norbert Küster (DFK), Jürgen Junghanns (BHE), Ulrich Krienen (ZVEI)

Die Stiftung DFK – Deutsches Forum für Kriminalprävention greift mit dem hier vorgelegten Konzept „Airport-Security – Biometrische Applikationen zur Verbesserung der Sicherheit auf Flughäfen“ ein Anliegen der Bundesregierung auf. Lutz Diwell, Staatssekretär im Bundesministerium des Innern, hat es in seiner Rede zum 5. Internationalen Airportforum am 11. September 2003 in Frankfurt so formuliert:

> *„Es ist mir ein Anliegen, dass zur Erhöhung der Sicherheit die uns zur Verfügung stehenden und geeigneten technologischen Entwicklungen genutzt werden. Mit der Biometrie ist in den letzten Jahren eine neue Schlüsseltechnologie entstanden, die hierbei erhebliche Sicherheitsgewinne ermöglichen kann. Biometrische Merkmale – seien es Fingerabdrücke, Lichtbilder oder Iris-Fotos – können die Identifikation einreisender Personen verbessern. Daneben sind sie ein geeignetes Hilfsmittel zur eindeutigen Zuordnung von Dokumenten zu ihren Inhabern. Mit Hilfe der Biometrie können und werden wir eine neue Sicherheitsinfrastruktur aufbauen.“*

Parallel zu dem von Staatssekretär Diwell angesprochenen Bereich hoheitlicher Kontrollen sollen mit diesem Konzept die neuen technischen Möglichkeiten der Biometrie zur Erhöhung der Sicherheit im nicht-hoheitlichen Bereich eines Flughafens gezeigt werden. Zugleich geht es darum, aktuelle Diskussionen und Vorschläge zu strukturieren.

Sicherheit ist ein Ziel aller Infrastruktureinrichtungen, da sie Grundvoraussetzung für deren wirtschaftlichen Erfolg ist. Passagiere, also Kunden, die sich nicht sicher fühlen, meiden Flugreisen so weit wie möglich oder wählen Flughäfen, die den gewünschten Sicherheitsstandard bei optimalem Komfort bieten.

Fluggesellschaften und Flughafenbetreiber sehen sich mit organisatorisch und finanziell überbordenden Aufwendungen durch neue staatliche Sicherheitsanforderungen konfrontiert. Diese führen sowohl zu höheren direkten Kosten pro Flug als auch zu deutlich verlängerten Abfertigungszeiten.

Daher müssen neue sicherheitstechnische Maßnahmen in die vorhandenen Abläufe integriert werden. Sie dürfen keine vermeidbare zusätzliche Belastung beinhalten, und mit den verwendeten Techniken sollte sich zusätzlicher Nutzen sowohl für Kunden als auch Betreiber einstellen.

Die in diesem Konzept vorgeschlagenen Maßnahmen gehen von den Auflagen aus, die von allen Betreibern von Verkehrsflughäfen in Europa aufgrund der Verordnung (EG) Nr. 2320/2002 des Europäischen Parlaments und Rates vom 16.12.2002 zur Festlegung gemeinsamer Vorschriften für die Sicherheit in der Zivilluftfahrt umgesetzt und in die Arbeitsabläufe des Flughafenbetriebs integriert werden müssen. Die volle Wirksamkeit der in der EU-Verordnung vorgesehenen Maßnahmen war bis zum 19. Januar 2004 herzustellen. Ergänzend wird Bezug genommen auf das geplante Luftsicherheitsgesetz (LuftSiGE), dessen Entwurf vom Bundeskabinett am 7.11.2003 in das parlamentarische Verfahren eingebracht wurde

Kernpunkt des DFK-Konzeptes ist die Einführung eines standardisierten „Flughafenausweises“ für Mitarbeiter und berufsbedingte Dauerbesucher von Flughafenbetreibern, Fluggesellschaften und sonstigen im Sicherheitsbereich tätigen Unternehmen. Außerdem wird die Einführung eines „Flugpasses“ für Passagiere der gewerblichen Luftfahrt auf freiwilliger Basis vorgeschlagen. Beide Ausweise tragen biometrische Merkmale ihrer berechtigten Inhaber. Damit kann an entsprechend ausgerüsteten Kontrollpunkten überprüft werden, ob der aktuelle Ausweisbenutzer der rechtmäßige Ausweisinhaber ist. Die Kontrollstellen befinden sich für Mitarbeiter dezentral über das gesamte Flughafengelände verteilt, für Passagiere an jedem Übergang vom Check-In zum Gate, insbesondere aber an allen Übergängen vom öffentlich zugänglichen zum nicht öffentlich zugänglichen Bereich, also etwa zu Sicherheitsbereichen wie der so genannten Luftzone eines Flughafens.

Der mit biometrischen Daten aufgeladene Ausweis ist ein technisch weiter entwickelter „Flughafenausweis“, wie er für alle Mitarbeiter, insbesondere jene, die im Sicherheitsbereich eines Flughafens tätig sind, durch die genannte EU-Verordnung nun vorgeschrieben ist. Fach- und Dauerbesucher sollen ihn unter den gleichen Voraussetzungen erhalten. Der Ausweis wird entsprechend den Vorgaben der EU-Verordnung nur nach vorheriger amtlicher Zuverlässigkeitskontrolle vom Flughafenbetreiber ausgegeben. Mit ihm können sich Berechtigte im für sie freigegebenen Teil der Sicherheitszone eines Flughafens ohne autorisierte Begleitung bewegen.

Auf Grund ihrer inzwischen fortgeschrittenen technischen Reife werden „prozessorgestützte Smart Cards mit RFID („Radio Frequency Identification")-Technik" vorgeschlagen. Das sind Ausweiskarten, die berührungslos mit einem entsprechenden Leser arbeiten. Aufgrund der international stark gestiegenen Anforderungen und Nachfrage hat die Entwicklung der Hard- und Software solcher Smart Cards mit integriertem RFID-Speicherchip in jüngster Zeit starke Fortschritte gemacht. Ihre Speicherkapazität liegt derzeit bei 32 KB. Außer Daten für verschiedene biometrische Verifikationsverfahren lassen sich Zugriffsberechtigungen und Sicherheitsapplikationen ebenso speichern wie Daten über Zutrittsberechtigungen zu Sicherheitsbereichen oder das ausgebende Unternehmen.

Biometrische Erkennungsmethoden und deren Integration in bestehende Sicherheitseinrichtungen dienen der „Verifikation" des Kartennutzers. „Verifikation" bedeutet in diesem Zusammenhang die Überprüfung, ob beim aktuellen Vorgang der Kartennutzer mit dem für diese Karte hinterlegten und/oder mit den auf der Karte selbst gespeicherten Kenndaten des Berechtigten identisch ist.

Diese Sicherheitseinrichtungen wiederum haben eine definierte Schnittstelle zu den prozessorientierten Systemen am jeweiligen Kontrollpunkt.

Die vorgeschlagenen Maßnahmen sollen eine Teilautomatisierung bei den sicherheitsrelevanten Prozeduren ermöglichen, die zu mehr Effizienz trotz höherer Sicherheitsstandards führen. Für Flughafenbetreiber und Fluggesellschaften soll auf diese Weise ein wirtschaftlicher Betrieb möglich bleiben. Mitarbeiter und zum Teil auch Fluggäste sollen von Prozeduren befreit werden können, die häufig als sehr lästig empfunden werden, jedoch zur Erhöhung der Sicherheit nichts Wesentliches beitragen.

Der entscheidende Vorteil eines solchen Ausweises für Mitarbeiter und Dauerbesucher liegt in der Möglichkeit einer dezentralen, automatischen Verifikation des Nutzers. Gleichzeitig erscheint denkbar, für derart ausgestattete, verifizierte Ausweisnutzer auf die sonst durch die EU-Verordnung vorgeschriebene lückenlose physische Kontrolle der Person und der Überprüfung der von ihr mitgeführten Gegenstände zu verzichten, da die Person schon amtlich auf ihre Vertrauenswürdigkeit überprüft wurde. Diese Kontrollen könnten für solche überprüften und für vertrauenswürdig befundenen Personen auf die in der Verordnung vorgesehenen „fortlaufenden, angemessenen Stichprobendurchsuchungen" beschränkt werden.

Allerdings erlaubt die gegenwärtige Regelung der EU-Verordnung seit Ablauf der Übergangsperiode am 19.01.2004 einen solchen (partiellen) Verzicht auf physische Personenkontrollen nicht. Insofern enthält das DFK-Konzept zugleich einen Vorschlag, bei der anstehenden Revision der EU-Verordnung den Mitgliedstaaten eine flexiblere Handhabung der konkreten Sicherheitsmaßnahmen zu erlauben, wenn sie durch Nutzung neuartiger Techniken das bisherige Sicherheitsniveau übertreffen können.

Der in diesem Konzept außerdem vorgeschlagene neuartige „Flugpass" für Passagiere arbeitet auf gleicher Basis, hat allerdings einen gegenüber dem Mitarbeiterausweis stark eingeschränkten und abweichenden Einsatzbereich. Zwei Aspekte sprechen für den Flug-

pass: Zur Erhöhung der Flughafensicherheit und unter kriminalpräventiven Gesichtspunkten muss zukünftig gewährleistet sein, dass die in einem Flugzeug beförderten Personen identisch sind mit denen, die eingecheckt wurden. Dies ist heute – nach Angaben von Fluggesellschaften – nicht gewährleistet und auch tatsächlich relativ häufig nicht der Fall, weil nach dem Check-In die Bordkarten getauscht oder einer anderen Person ausgehändigt werden können, die dann das Flugzeug betritt. Dies schafft immer wieder erhebliche Sicherheitsprobleme. Mit einem Flugpass, auf dem die biometrischen Daten des eingecheckten Fluggastes gespeichert sind, kann dies vermieden werden.

Ein solcher Flugpass kann unter Sicherheitsgesichtspunkten auf unterschiedliche Weise genutzt werden: Einerseits (ausschließlich) als Boardingkarte, andererseits aber – auf Grundlage vertraglicher Vereinbarungen zwischen einem Fluggast und einer oder mehreren Fluggesellschaften und/oder einem oder mehreren Flughafenbetreibern – als Dauerausweis zur Erleichterung des Check-Ins, des Boardings im Selbstabfertigungsverfahren, als Zutrittsausweis für Lounges und schließlich noch zur verstärkten Kundenbindung.

Der Grundansatz dieses Konzeptes zielt darauf ab, die wesentlichen Bereiche des gesamten Flughafenbetriebes im Zusammenhang und die Arbeitsabläufe prozessorientiert unter Sicherheitsgesichtspunkten zu betrachten und unter vorrangig kriminalpräventiven Gesichtspunkten Vorschläge zur Erhöhung der Sicherheit des Flughafen- und Flugbetriebes durch Nutzung neuartiger technischer Möglichkeiten zu unterbreiten. Daher betrachtet dieses Konzept außer den Mitarbeitern auch andere Personengruppen, die nicht öffentlich zugängliche Bereiche eines Flughafens regelmäßig besuchen müssen, nämlich Fachbesucher verschiedener Kategorien, aber auch das allgemeine Publikum, das die öffentlich zugänglichen Ankunfts- und Abflughallen in großer Zahl benutzt.

Für alle Besucher nicht öffentlich zugänglicher Flughafenbereiche wird die konsequente Nutzung von Besucherverwaltungssystemen vorgeschlagen, die – für gelegentliche Besucher – mit Ausweisen ohne biometrische Daten der Besucher auskommen. Lediglich für Dauer- und Fachbesucher, die über längere Zeit und regelmäßig wiederkehrend den Sicherheitsbereich betreten müssen, sollen, wie für Mitarbeiter, Flughafenausweise mit biometrischen Daten des Berechtigten ausgegeben werden.

Für die Ankunfts- und Abflughallen werden Videoüberwachungsmaßnahmen vorgeschlagen, die mit biometrischen Gesichtserkennungssystemen ausgerüstet sind, die unter definierten Randbedingungen nur das Bild einer mit Hausverbot belegten und/oder gesuchten Person anzeigen, wenn diese einen der Kontrollpunkte passiert.

In dem Konzept werden – für die verschiedenen Anwendungszwecke getrennt – auch die rechtlichen, insbesondere datenschutzrechtlichen Rahmenbedingungen betrachtet und Hinweise für notwendige Klärungen gegeben. Die Prüfung der rechtlichen Rahmenbedingungen muss kursorisch bleiben und sich notwendigerweise mit Hinweisen begnügen, weil eine konkrete rechtliche Prüfung detaillierte Festlegungen der organisatorischen Abläufe und der technischen Verfahren voraussetzen würde. Das kann und soll hier nicht geleistet werden. Die Anwendung technischer Maßnahmen zur Personenkontrolle ist

politisch und rechtlich umstritten. Insbesondere von Seiten der Datenschutzbehörden des Bundes und der Länder werden immer wieder Bedenken geltend gemacht. Sie müssen in der konkreten Anwendung berücksichtigt und – bezogen auf den Einzelfall – genau geprüft werden.

Die Stiftung DFK – Deutsches Forum für Kriminalprävention beabsichtigt mit der Vorlage dieses Konzeptvorschlages, die gegenwärtig geführten vielfältigen Diskussionen um die Nutzung technischer Verfahren zur Verbesserung der Sicherheit auf Flughäfen und des Flugbetriebs zu strukturieren. So soll die weitere Diskussion auf der Fachebene und unter Fachleuten vorangebracht werden.

Dieses Konzept dient des Weiteren der Vorbereitung einer Veranstaltung des DFK zum Thema. Dazu ist es unabweisbar notwendig, Vorschläge zur Nutzung biometrischer Verfahren in technischer und organisatorischer Hinsicht zu konkretisieren.

Dies bedeutet aber nicht, dass die Stiftung DFK – Deutsches Forum für Kriminalprävention die hier zur Diskussion gestellten technischen und organisatorischen Maßnahmen für den besten oder gar einzig gangbaren Weg hält. Der Vorstand der Stiftung DFK – Deutsches Forum für Kriminalprävention und der DFK-Arbeitskreis Kriminalprävention und Biometrie, der die Erarbeitung dieses Konzeptvorschlages verantwortet, sind für weitere Anregungen und jeden Diskussionsbeitrag zum Thema dankbar.

Technische Leistungsfähigkeit und Eignung von Biometrie bei Ausweisdokumenten und Grenzkontrolle

Auszug aus dem 93. Arbeitsbericht des Büros für Technikfolgen-Abschätzung beim Deutschen Bundestag (TAB) vom Dezember 2003: „Biometrie und Ausweisdokumente – Leistungsfähigkeit, politische Rahmenbedingungen, rechtliche Ausgestaltung“ von Thomas Petermann, Constanze Scherz und Arnold Sauter*

Der Bericht „Biometrie und Ausweisdokumente“ des Büros für Technologiefolgen–Abschätzung des Deutsches Bundestages (TAB) vom Dezember 2003 fasst den Stand der Diskussion zur technischen Leistungsfähigkeit und Eignung der Handgeometrie-, Fingerabdruck- sowie Gesichts- und Iriserkennung für die Nutzung bei Ausweisdokumenten und bei Grenzkontrollen mit dem Ziel der Verifikation zusammen. Die Frage, welche biometrischen Systeme und die Nutzung welcher Merkmale geeignet bzw. vorzugswürdig sind, ist mittlerweile nicht mehr so offen wie noch vor kurzem. Erkennungssysteme, die Finger, Gesicht oder Iris (bzw. eine Kombination dieser Merkmale) nutzen, haben ihre Eignung für Verifikationsanwendungen bei Ausweisdokumenten grundsätzlich unter Beweis gestellt – auch wenn ihre Performanz und Leistungsfähigkeit je nach Kontext und Systemanforderung teilweise noch verbesserungswürdig sind.

Bei der Prüfung entlang verschiedener Kriterien stellt sich die Situation wie folgt dar:

– Im Falle einer biometrischen Ausrüstung der Ausweisdokumente muss sichergestellt sein, dass das vorgesehene Merkmal möglichst *keine oder nur eine sehr geringe Zahl von Bürgern von der Anwendung ausschließt.* Fingerabdruck-Verfahren werden dieser Anforderung nur bedingt gerecht. Vorliegende Tests und Erfahrungen zeigen, dass hier bei etwa 2 % der Gesamtbevölkerung Probleme bei der biometrischen Erfassung (enrollment) auftreten. Die Enrollment-Ausfallraten von Hand- und Iriserkennungs-Verfahren sind zwar geringer als die des Fingerabdrucks, bei bestimmten Nutzergruppen bleiben aber Probleme aufgrund ihres Alters oder ihrer Ethnie. Die Nutzerausfallrate für die Gesichtserkennung ist marginal.

– Die Handgeometrieerkennung erweist sich im Hinblick auf die Anforderung der *Unterscheidbarkeit* – besonders bei umfangreichen Anwendungen – als weniger geeignet. Die Unterscheidbarkeit bei Iris, Finger und Gesicht ist aufgrund der hohen Anzahl an eindeutigen Informationen grundsätzlich besser gewährleistet. Seriöse Qualitätstests belegen die hohe Einzigartigkeit der Merkmale Finger und Gesicht auch bei großen Datenbeständen. Für die Iris liegen hierzu Belege aus Großanwendungen bislang nicht vor.

---

* Beitrag von Prof. Dr. Behrens „Leistungsfähigkeit der Biometrie-Technik: ein aktueller Überblick“ stand für die Dokumentation leider nicht zur Verfügung. Mit freundlicher Genehmigung wird aus dem Bericht des TAB zitiert.

– Für biometrische Anwendungen ist es wichtig, dass das Merkmal sich nicht in kurzen Zeitabständen verändert. Unter dem Gesichtspunkt der *Stabilität* ist der Einsatz von Fingerabdruck-Verfahren aufgrund bestimmter Einschränkungen kritisch zu beurteilen. Nachteilig bei der Handgeometrieerkennung ist die späte Stabilisierung des Merkmals erst im Alter von 20 Jahren. Die Stabilität des Gesichtes ist für die Ausweisanwendung ausreichend, da Veränderungen dieses Merkmals innerhalb größerer Zeitabstände erfolgen, so dass mit vertretbarem Aufwand „Neuregistrierungen" vorgenommen werden könnten. Die Iris dürfte in Bezug auf das Kriterium der Stabilität am unproblematischsten sein.

– Bisher durchgeführte Studien deuten auf eine hohe *Erkennungsleistung* von Iriserkennungs-Verfahren hin, die es aber noch in Großanwendungen zu überprüfen gilt. Die Handgeometrieerkennung erzielt zwar in Kleinszenarien gute Erkennungsraten, die Problematik der nicht eindeutig unterscheidbaren Identität von Handgeometriemustern in größeren Anwendungen müsste allerdings erst in umfangreichen Teststudien widerlegt werden. Fingerabdruck- und Gesichtserkennungs-Verfahren haben in aktuellen und unabhängigen Studien ihre Erkennungsleistung auch bei umfangreichen Datenmengen unter Beweis gestellt. Die augenblicklich erreichbare Leistung der beiden Verfahren bei *Verifikationsanwendungen* ist dabei ungefähr gleich einzustufen.

  Sowohl Fingerabdruck- als auch Gesichtserkennungs-Verfahren sind heute so weit ausgereift und leistungsstark, dass ihr Einsatz im Vergleich zur bisherigen Situation eine Effektivierung der Grenzkontrollen im Verifikationsmodus verspricht. Die Frage, ob die hier erwartbare Erkennungsleistung eine hinreichende Sicherheit gewährleisten wird und ob die erhofften Verbesserungen bei der Grenzkontrolle den hierzu erforderlichen Aufwand rechtfertigen, muss politisch entschieden und begründet werden. Dabei sollte offen diskutiert werden, dass es – trotz eindrucksvoll geringer Fehlerraten – in der Praxis eines Masseneinsatzes nur zu einem relativen Sicherheitszugewinn kommen kann, da Falschidentifikationen in einem gewissen Umfang weiter erfolgen werden.

– Für die Ausweisanwendung sind *Verfahren mit niedrigem Bedienungsaufwand* und hoher Verständlichkeit *günstig*. Vorteile bieten hier Gesichtserkennungs-Verfahren als kontaktloses Verfahren ohne großen Positionierungsaufwand. Fingerabdruck-Verfahren sind zwar bequem nutzbar, erfordern aber eine, wenn auch kurze, Einlernzeit. Auch bei der Handgeometrieerkennung treten Bedienungsfehler eher selten auf. Die Iriserkennung ist im Hinblick auf den Bedienungsaufwand im Vergleich weniger günstig einzuschätzen, da sie genaue Verhaltensvorschriften und eine gewisse Einlernzeit erfordert.

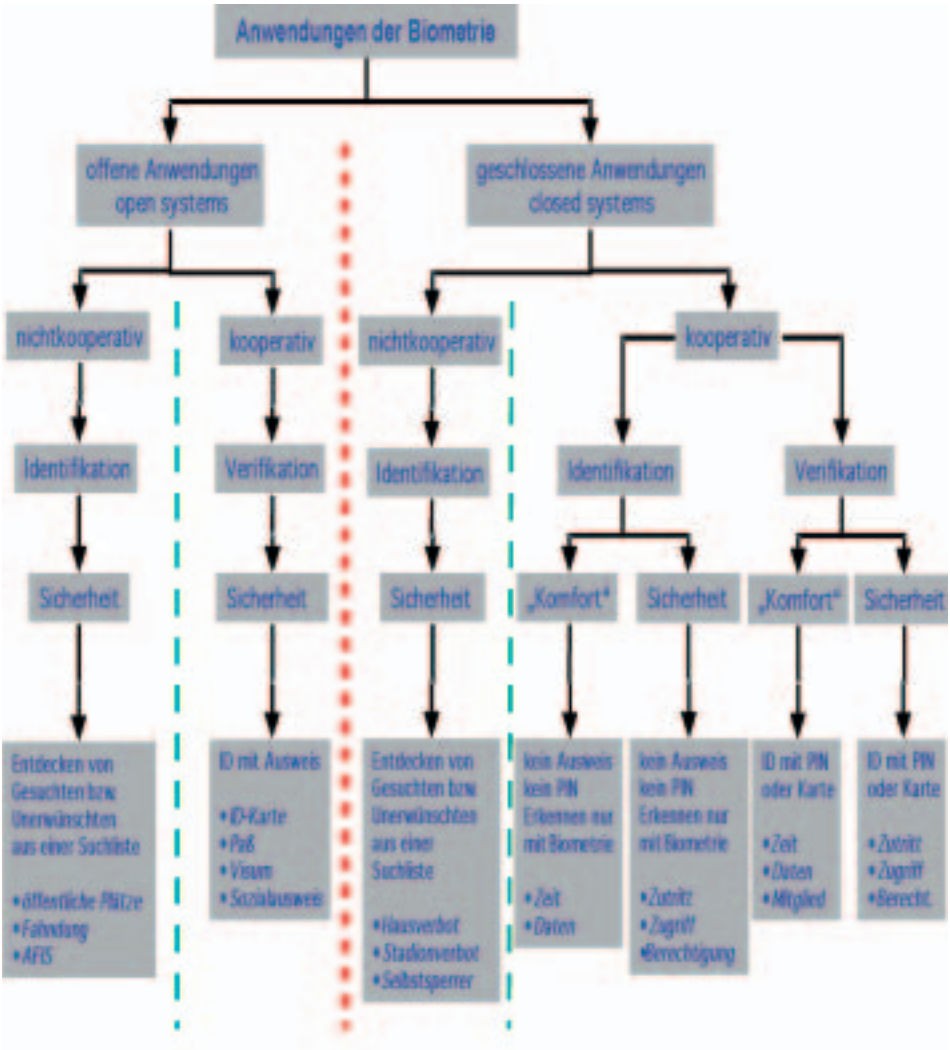
– Der bei allen Verfahren erforderliche Aufwand beim Enrollment und bei der Kontrolle dürfte grundsätzlich den bisher üblichen Zeitrahmen der Ausweisbeantragungs- und Kontrollprozesse nicht entscheidend verändern. Für eine umfassende Einschätzung müssen aber weitere Aspekte wie die Systemumgebung sowie bauliche, infrastrukturelle und organisatorische Aspekte mit herangezogen werden. Ob beispielsweise im Falle der Ausweiskontrolle an Flughäfen mehr Zeit erforderlich wäre oder ob biometrische

Verfahren längerfristig zu Zeiteinsparungen führen könnten, hängt von den konkreten Systembedingungen und Leistungsanforderungen vor Ort ab.

Es zeigen sich bei jeder Technologie sowohl gewisse Stärken als auch Schwächen. So erweist sich die *Gesichtserkennung* bei zwei Kriterien als führend (Enrollment-Ausfallrate, Bedienungsaufwand/Verständlichkeit), sie ist aber bei der Erkennungsleistung schwächer zu bewerten. Die *Iriserkennung* ist bei der Erkennungsleistung führend. Sie weist allerdings schwächere Werte beim Bedienungsaufwand auf. Die *Handgeometrieerkennung* weist insgesamt durchschnittliche Leistungen, allerdings eine hohe Falschakzeptanzrate auf. Die *Fingerabdruckerkennung* ist bei keinem Kriterium den anderen Verfahren überlegen, weist aber im Durchschnitt gute Werte auf, sieht man von einer nicht zufrieden stellenden Enrollment-Ausfallrate ab. Die Unterschiede, die sich bei den einzelnen Kriterien ergeben, sind allerdings nicht sehr gravierend.

Insgesamt ist deshalb der Schluss zu ziehen, dass *drei Verfahren* – Gesichts-, Iris- und Fingerabdruckerkennung – über *eine in etwa vergleichbare technische Leistungsfähigkeit* verfügen. Die Handgeometrie fällt demgegenüber etwas ab. Zur Entscheidung für oder gegen eine Technologie müssten weitere Kriterien und Fragestellungen in die Abwägung mit einbezogen werden.

Übersicht zur Kategorisierung biometrischer Verfahren



(Jürgen Junghanns, BHE)

Die Sichtweise eines Flughafenbetreibers: Biometrie zur Optimierung der Ablauforganisation

von Dagmar Naumann, Bereichsleiterin Infrastruktur für den Flug- und Terminalbetrieb der Frankfurt Airport Services Worldwide (Fraport AG)

Das vorgestellte Konzept *„Airport Security – Biometrische Applikationen zur Verbesserung der Sicherheit auf Flughäfen“* enthält eine Vielzahl von Ansätzen, am Frankfurter Flughafen mittels biometrischer Verfahren die Ablauforganisation und damit die Sicherheit und Wirtschaftlichkeit zu verbessern.

Aufgrund der strengeren Sicherheitsanforderungen an Flughäfen, wie etwa die 100 % Reisegepäckkontrolle (seit Januar 2003) oder die 100 % Waren- und Mitarbeiterkontrolle (seit Januar 2004) sehen sich die Flughafenbetreiber vor immer größere Aufgaben gestellt und somit auch vor neue Anforderungen an einen effizienten Ablauf der Kontrollprozesse am Flughafen. Dies steht in unmittelbarem Zusammenhang mit einem hohen Wettbewerbs- und Kostendruck. Bei der Einführung neuer Technologien sollte den entstehenden Kosten ein entsprechender Nutzen gegenüberstehen.

Biometrie kann, im Kontext einer Vielzahl von Abläufen gesehen, eine Ergänzung zu den herkömmlichen Verfahrensweisen darstellen und wird somit zukünftig eine Rolle spielen, um Zu- und Durchgangskontrollen effizient zu unterstützen und zu beschleunigen. Um dieses Ziel zu erreichen gelten seitens der Flughafenbetreiber folgende Anforderungen an die Leistungsfähigkeit der biometrischen Systeme:

- Zuverlässigkeit auch bei großen Datenmengen
- Ausfallsicherheit
- Beschleunigung von Prozessen
- Einfachheit in der Nutzung
- Hohe Akzeptanz bei den Nutzern
- Überwindungssicherheit

Für Flughafenbetreiber sind folgende Anwendungsbereiche der Unterstützungen durch biometrische Systeme von Relevanz:

- Die *Automatisierung der Grenzkontrolle*, also einer hoheitlichen Aufgabe, durch international standardisierte und global interoperable biometriegestützte Reisedokumente und Ausweise ermöglicht es einer großen Anzahl von Passagieren, von einer Beschleunigung der Prozesse zu profitieren. Den Flughafenbetreibern sollten durch den Betrieb entsprechender Anlagen keine zusätzlichen Kosten entstehen. Die verschiedenen *Passagierprozesse* am Flughafen, namentlich Check-In, Boarding und Grenzkontrolle könnten anhand biometrischer Systeme miteinander verbunden werden. Eine folglich stärkere informationstechnische Kopplung der Airline- und Behördensysteme erlauben eine Erhöhung der Sicherheit sowie der Prozessgeschwindigkeit. In diesem Fall sind standardisierte Systemplattformen eine Notwendigkeit.

– Durch eine *biometrisch gestützte Zutrittskontrolle für Mitarbeiter der Flughäfen* sowie ansässiger Drittfirmen könnte ein deutlicher Sicherheitsgewinn erreicht werden. Physische Checks können aber nur ergänzt, nicht substituiert werden. Die entstehenden Kosten für die Flughafenbetreiber durch Installation und Betrieb der biometrischen Systeme müssen an anderer Stelle wieder eingespart werden. Wichtig ist, dass den einzelnen Flughäfen die Freiheit erhalten bleibt, sich individuell für eine geeignete Technologie zu entscheiden. Technische Verfahren sollten für diesen Bereich nicht verordnet werden. Flughäfen unterscheiden sich in ihrer Infrastruktur voneinander, was zu unterschiedlichen Bedingungen für die Gewährleistung von Sicherheit und effizienten Prozessen führt. Der Gesetz- bzw. Verordnungsgeber sollte hier entsprechende Spielräume ermöglichen und nur ein Mindestmaß an Vorgaben machen.
– In Bezug auf die Ausführungen im DFK-Konzept zum *Standardisierten Mitarbeiterausweis* ist eine Standardisierung eines solchen Ausweises über den jeweiligen Standort des Flughafens hinaus nicht notwendig. Die Rahmenbedingungen der einzelnen Flughäfen sind zu unterschiedlich, als dass hier der Einsatz eines einheitlichen biometrischen Systems sinnvoll erscheint.
– *Automatisierte Überwachungssysteme (CCTV)* könnten bei biometrischer Identifikation von Personen zur Überwachung von Terminals und Betriebsbereichen beitragen. Der Einsatz solcher Systeme ist aber mit den zur Zeit geltenden Regelungen des Datenschutzes nicht erreichbar.
– Eine *Aufnahme von biometrischen Merkmalen in die Smartcard für Vielfliegerprogramme* ist denkbar, kann aber nur im Rahmen einer standardisierten Infrastruktur geschehen. Die Frage, wer hierbei eine Standardisierung vorantreibt bzw. die Kosten trägt, bleibt offen. Statt in eine solche durch Biometrie erweiterte Vielflieger Smartcard zu investieren, sollte über die Möglichkeiten der Nutzung von Reisepässen bzw. Ausweisen mit biometrischen Merkmalen nachgedacht werden, deren zukünftiger Gebrauch ohnehin zu erwarten ist. Der Gesetzgeber sollte in diesem Zusammenhang die Möglichkeit schaffen, dass die behördlichen Dokumente auch durch Fluggesellschaften und Flughäfen ausgelesen werden können.

Eine Kooperation aller beteiligten Akteure bei der Schließung noch vorhandener Sicherheitslücken sollte schnell erreicht werden. Dabei ist auch eine verstärkte Zusammenarbeit der Behörden auf internationaler Ebene unumgänglich. So steht bisher z.B. immer noch eine einheitliche EU-weite Definition der „Critical Parts“ eines Flughafens aus.

Zum Umgang mit Risiken

von Wolfgang Kahl, Mitarbeiter der DFK-Geschäftsstelle

Der Luftverkehr hat sich durch die Flugzeugentführungen internationaler Terrorgruppen in den 1970er Jahren und besonders mit der Katastrophe am 11. September 2001 in New York zu einem sehr sensiblen Bereich für die Sicherheit der Bürger entwickelt und kann gewissermaßen als Gradmesser für die terroristische Bedrohungslage gelten.

Biometrie als Instrument der Kriminalprävention scheint ein innovativer technischer Ansatz zu sein, um Sicherheitsrisiken in bestimmten Situationen und Abläufen minimieren zu können.

Das Deutsche Forum für Kriminalprävention (DFK) setzt sich zum Ziel, eine Vielzahl von Akteuren zu gemeinsamer Verantwortung bei der Prävention von Sicherheitsrisiken für die Gesellschaft zusammenzuführen, und hat den Ansatz der Vernetzung in einem Arbeitskreis verwirklicht, der die kriminalpräventiven Möglichkeiten der Biometrie möglichst umfassend beleuchten soll. Es sind Vertreter des Datenschutzes, der Wissenschaft, der Behörden, der Fachverbände und anderer interessierter Vereinigungen eingebunden.

Die technische Leistungsfähigkeit / Reife ist Grundvoraussetzung für eine Diskussion über den praktischen Einsatz von Biometrie, eine Diskussion die dann im Spannungsfeld zwischen Sicherheitserfordernissen und dem Schutz der Privatsphäre steht.

Flug(hafen)sicherheit als herausragende Sicherheitsaufgabe fordert geradezu heraus, innovative technische Ansätze zur Verbesserung der Sicherheit zu untersuchen und im akzeptablen Rahmen zu fördern.

Die Bedrohungslage wird besonders durch die Entwicklungen im nahen und mittleren Osten beeinflusst. Ermittlungs- und Fahndungserfolge werden weltweit erzielt, dennoch bleibt die schwierige Frage, welche Sicherheitsgewinne dadurch letztlich erreicht werden, momentan offen. Die Gefährdungslage ist schwer kalkulierbar und von einem entsprechend hohen Niveau muss weiter ausgegangen werden.

Bekanntermaßen gibt es eine Vielzahl von besonders schutzwürdigen Lebensbereichen und Infrastrukturen, die aber nicht alle gleichermaßen und vor allem auch nicht zu jeder Zeit und gegenüber allen Gefahren und Bedrohungen geschützt werden können. Beispiele sind – neben dem Flugverkehr – der Bahnverkehr, Sportstadien, Leitungsnetze, Krankenhäuser, Rechenzentren und Kraftwerke. Die Liste lässt sich fortsetzen. Hinzu kommen die Gefährdungen so genannter „weicher Ziele“, deren gemeinsames Merkmal die Verwundbarkeit einer hohen Zahl von Menschen ist und die überall im urbanen Leben vorzufinden sind.

Der Begriff des Restrisikos ist aus der Diskussion um die Nutzung der Kernenergie bekannt. Er gilt aber auch im Hinblick auf andere Gefahren für die Sicherheit unserer Gesellschaft. Insofern wäre es falsch, wenn man bei allen Bemühungen um technische und andere Prävention von der Vorstellung, einen 100prozentigen Schutz erreichen zu können,

ausgeht. Realistischer Weise sollten die verbleibenden Risiken bewusst bleiben. Absolute Sicherheit durch vermeintlich perfekte Schutzmaßnahmen wäre eine illusionäre Zielstellung.

In der Diskussion, welches Verfahren, welche Technik, welche Dienstleistung das erreichbare Optimum akzeptabler Sicherheit bietet, kommt man schnell zu dem Ergebnis, dass nicht eine einzelne isolierte Vorgehensweise den richtigen Weg beschreibt sondern ein aufeinander abgestimmtes System von Maßnahmen und Technikeinsatz, ein „Sicherheitsmix“ also, der richtige konzeptionelle Ansatz ist. Dazu kann und sollte auch die Biometrie zählen. Ob und wie gut ein System am Ende geeignet ist, definiert sich nicht durch eine einzelne Komponente, sondern durch die Schlüssigkeit der Integration aller Bestandteile eines Sicherheitskonzeptes.

Und noch ein Gedanke: Bei allem, was für die Sicherheit der Bürger getan werden kann und soll, darf nicht vergessen werden, den Bürger auch in seiner Eigenverantwortung anzusprechen und mitzunehmen. Das bedeutet nicht nur die Förderung von Wachsamkeit sondern auch das weite Feld einer die Wurzeln vieler Übel anpackenden und wertorientierten Verantwortlichkeit der Bürger z.B. für die Erziehung zu Toleranz, Mitmenschlichkeit, Hilfsbereitschaft und Solidarität.

Biometrie und Flughafensicherheit

von Dr. Günther Beckstein, Bayerischer Staatsminister des Innern

Sehr geehrte Damen und Herren,

sehr gerne bin ich der Einladung des Deutschen Forums für Kriminalprävention hierher nach Berlin gefolgt.

Die Flughafensicherheit hat nach den Anschlägen vom 11.September 2001 besondere Bedeutung erlangt. Man hat angesichts der angespannten Sicherheitslage weltweit mannigfaltige Anstrengungen unternommen, um die Sicherheit im gesamten Luftfahrtbereich durch technische Innovationen, gesetzliche Änderungen sowie organisatorische und personelle Anpassungen bei Polizei, Flughafenbetreibern, Fluggesellschaften und der internationalen Kooperation zu verbessern.

Es freut mich, heute in diesem Zusammenhang anlässlich des Symposiums vor einem Fachpublikum zum Thema „Biometrie und Flughafensicherheit“ referieren zu können.

I. Bayerische Sicherheitsstrategie

Verehrte Damen und Herren, lassen Sie mich zu Beginn meiner Ausführungen kurz auf die bayerische Sicherheitsstrategie zu sprechen kommen:

Bayern steht dazu, dass Sicherheit zu den elementarsten Grundbedürfnissen der Menschen gehört und wesentlicher Bestandteil ihrer Lebensqualität ist. Innere Sicherheit hat für mich deshalb den Stellenwert eines sozialen Grundrechts. Sie ist Voraussetzung für die Stabilität unseres Gemeinwesens. Nur in einem Land, in dem die Bürger sicher leben, können sie ihre Freiheit wirklich entfalten.

Wir verfolgen in Bayern eine langfristig angelegte Sicherheitsstrategie, die sich als sehr erfolgreich erweist. Wir gehen gegen Kriminalität aller Art konsequent vor, dulden keine rechtsfreien Räume und wollen durch umfassende Kriminalprävention dafür sorgen, dass Straftaten erst gar nicht begangen werden. Hierbei setzen wir auch auf umfassende und gesamtgesellschaftliche Sicherheitspartnerschaften.

II. Sicherheitslage Terrorismus

Wie die schrecklichen Ereignisse in der Vergangenheit deutlich gemacht haben, mündet extremistisches Gedankengut im schlimmsten Falle in terroristische Handlungen, mit denen auf menschenverachtende Art und Weise Forderungen durchgesetzt oder in den Blickpunkt der Öffentlichkeit gerückt werden sollen. Das haben uns nicht nur die Anschläge vom 11. September 2001 vor Augen geführt.

Mit den Anschlägen von Istanbul war der internationale Terrorismus bereits sehr nahe an uns herangerückt. Wenn die Anschläge in Madrid der Al Qaida zuzurechnen sind – wofür vieles spricht –, dann verdeutlicht dies unsere unmittelbare Bedrohungslage in Europa.

Wir müssen feststellen, dass der islamistische Fundamentalismus und insbesondere die arabischen Mudschaheddin im Umfeld der Organisation Al Qaida derzeit die akuteste Bedrohung der Inneren Sicherheit in Deutschland darstellen. Internationale Netzwerkstrukturen der Al Qaida sind trotz Erfolgen der Sicherheitsbehörden und der militärischen Maßnahmen der Antiterrorallianz weiterhin existent und funktionsfähig.

Eine nachhaltige Schwächung des islamistischen Terrorismus ist leider bisher trotz weltweiter Anstrengungen der Sicherheitsbehörden noch nicht eingetreten. Grundsätzlich müssen wir davon ausgehen, dass Angehörige islamistischer Netzwerke willens und in der Lage sind, zukünftig Anschläge durchzuführen. Auch in Deutschland haben wir ein nicht unerhebliches Potenzial islamistischer Fundamentalisten und Unterstützer mit vielfältigen internationalen Verbindungen in alle Teile der Welt.

Wie die kürzlichen Hinweise auf geplante Anschläge gegen die US-Militärbasis in Frankfurt/Main und ein Militärkrankenhaus in Hamburg gezeigt haben, ist Deutschland nicht nur als Vorbereitungsraum, sondern durchaus auch als möglicher Ausführungsraum terroristischer Gewaltakte einzustufen. Den Sicherheitsbehörden liegen zwar derzeit keine Hinweise auf unmittelbar bevorstehende Anschläge islamistischer Terroristen in Deutschland vor. In jedem Fall müssen wir aber äußerst wachsam sein.

Wir müssen alles tun, um dieser Bedrohung gezielt zu begegnen. Angesichts der jüngsten Anschläge müssen wir uns vor Augen halten, dass zunehmend so genannte „weiche“ Ziele in das Visier der Terroristen geraten können, also von vornherein nicht als konkret gefährdet eingestufte Örtlichkeiten und Objekte.

Bayern hat nach dem 11. September das größte Sicherheitspaket aller deutschen Länder verabschiedet.

Zur effektiven Kriminalitätsbekämpfung nutzen und erproben wir modernste Technik. So führen wir derzeit auch ein neues Gerät zur „elektronischen“ Abnahme von Fingerabdrükken ein, den sogenannten „Livescan“.

Auch die Bundesregierung hat auf die terroristische Bedrohung reagiert und zwei Sicherheitspakete beschlossen. Im Interesse einer größtmöglichen Sicherheit unserer Bürgerinnen und Bürger sehe ich aber bei der Terrorismusbekämpfung noch deutlichen Nachbesserungsbedarf. [...] Zwar begrüße ich es grundsätzlich, dass die Bundesregierung inzwischen den Entwurf eines Luftsicherheitsgesetzes auf den Weg gebracht hat. Was aber leider nach wie vor fehlt, sind ein Gesamtkonzept und die notwendige verfassungsrechtliche Absicherung.

III. Bedeutung der Biometrie

Neben den vorangestellten Forderungen habe ich mich auch nachdrücklich für die Speicherung biometrischer Daten in Ausweispapieren eingesetzt.

In nicht-hoheitlichen Anwendungsfeldern sind biometrische Verfahren bereits deutlich auf dem Vormarsch. Vor allem in den Bereichen der Zugangs-, Zutritts- und Zugriffssiche-

rung sind biometrische Verfahren schon jetzt kaum mehr aus der Privatwirtschaft wegzudenken.

Auch zu Gunsten der Flughafensicherheit können die seit Jahren positiven Ergebnisse bei der Nutzung biometrischer Verfahren – sei es bei Iris, Gesicht oder Finger – zur Automatisierung von Zutrittskontrollen erfolgreich genutzt werden; ich nenne hier nur die Mitarbeiter des Flughafenbetreibers in besonders gefährdeten Gebäudeteilen.

Die konventionelle Sicherheitstechnik mit Passwörtern oder PIN-Chipkarten überprüft zwar die verwendeten Daten, nicht aber den rechtmäßigen Benutzer oder Inhaber. Durch die Personenauthentifizierung mittels biometrischer Verfahren ist das sehr wohl möglich. Darüber hinaus können z.B. das Finger-, Iris- oder Gesichtsbild weder verloren noch vergessen oder einfach gestohlen werden.

Aber auch im hoheitlichen Anwendungsbereich – wie der polizeilichen Nutzung biometrischer Verfahren – schlummert meiner Überzeugung nach ein enormes Potenzial zur Optimierung der Kriminalitätsbekämpfung.

Sobald der polizeiliche Einsatz biometrischer Verfahren wie die Gesichtserkennung das nötige Maß an Alltagssicherheit und technischer Zuverlässigkeit erreicht hat, wäre dies eine hervorragende Fahndungsunterstützung für unsere Polizeikräfte.

Außerdem könnte der Einsatz biometrischer Verfahren eine hohe generalpräventive Wirkung entfalten, da das Entdeckungsrisiko für Straftäter massiv steigen würde.

Lassen Sie mich festhalten: Die umsichtige Nutzung biometrischer Verfahren wäre ein Quantensprung für die Kriminalprävention und Repression!

Seit den Terroranschlägen des 11. September 2001 befassen wir uns in Bayern im Rahmen von strategischen Sicherheitsüberlegungen noch intensiver mit innovativen Technologien. Ich nenne hier insbesondere die biometrischen Verfahren zur Optimierung der polizeilichen Fahndungs- und Ermittlungsarbeit.

Als ein Baustein des Sicherheitskonzepts Bayern haben wir bereits am 1. Januar 2002 das Strategische Innovationszentrum der Bayerischen Polizei (SIZ) als Wissensverbund von hochqualifizierten Akademikern und Polizeipraktikern eingerichtet.

Die Mitarbeiter des Strategischen Innovationszentrum erheben im Rahmen einer Marktanalyse weltweit fortlaufend Erkenntnisse zu neuartigen Kriminalitätsformen sowie Ansätze für innovative Bekämpfungsstrategien und modernste Einsatztechnologien.

Unser Ziel ist dabei, zeitnah und zentral den polizeilichen Nutzen und zielführende Einsatzfelder dieser innovativen Technologien zu prüfen.

In diesem Zuständigkeitsbereich hat das Strategische Innovationszentrum der Bayerischen Polizei in den letzten zwei Jahren einen besonderen Tätigkeitsschwerpunkt auf die Prüfung des polizeilichen Nutzens von biometrischen Verfahren gelegt, so z.B. auf die Gesichts-, Finger- und Iriserkennung.

Als besonders vielversprechend gilt die biometrische Gesichtserkennung. Sie könnte im Gegensatz zum Fingerbild oder zur Iriserkennung auch aus größerer Entfernung die polizeiliche Fahndungs- und Ermittlungsarbeit optimieren.

Auch weltweit führende Sicherheitsexperten haben nach den Anschlägen des 11. September 2001 die biometrische Gesichtsfelderkennung zunächst als wegweisende Lösung zur Erhöhung des Sicherheitsstandards dargestellt.

Unsere internationale Marktanalyse führte aber bereits damals zu der Vermutung, dass die biometrische Gesichtserkennung – gerade in dynamischen Situation wie bei der Personenfahndung im öffentlichen Raum – schnell an ihre technische Leistungsgrenzen stößt. Deshalb ist sie unter polizeilichen Rahmenbedingungen noch nicht einsetzbar.

Angesichts dieser Erkenntnisse haben wir uns in Bayern schon vor knapp zwei Jahren überlegt, wie wir die Gesichtserkennung trotzdem kurzfristig beispielsweise im Bereich Flughafensicherheit und Grenzkontrolle polizeilich nutzbar machen können.

Diese Überlegungen führten uns zu der Entscheidung, nicht die technisch hoch komplizierte Personenidentifikation durch Abgleich eines Gesichts aus gewisser Entfernung mit einer Fahndungsdatei zu erproben. Vielmehr verlagerten wir unsere Versuche auf den 1:1-Vergleich durch einen Abgleich des Gesichts mit dem vorgelegten Passbild.

Ab August 2002 testeten wir für vier Monate am Flughafen Nürnberg und für sechs Monate am Grenzübergang Waidhaus die technische Leistungsfähigkeit von Gesichtserkennungssoftware im eng begrenzten Anwendungsbereich des Personendirektvergleichs bei der polizeilichen Passkontrolle.

Mit Hilfe zuverlässig arbeitender biometrischer Verfahren sollten unserer Einschätzung nach die polizeilichen Personenkontrollen in Flughäfen und an den Grenzen wesentlich optimiert werden können.

Ein polizeiliches Ziel war es unter anderem, durch diese Technologie den von international agierenden Straftätern praktizierten Ausweismissbrauch gezielt zu bekämpfen.

An die Systeme wurden hohe technische Anforderungen gestellt, weil sie bei jeder Überprüfung mit einem neuen Bild konfrontiert wurden. Das ist bei Zutrittskontrollen eines geschlossenen Benutzerkreises im nicht-hoheitlichen Bereich oder auch bei Vielfliegern im Rahmen der automatisierten Grenzkontrolle nicht der Fall.

Das wichtigste Ergebnis unserer Pilotversuche war, dass die biometrische Gesichtserkennung auch bei stationären polizeilichen Rahmenbedingungen und der Zielrichtung Personenverifikation noch keine zuverlässige technische Unterstützung polizeilicher Kontrollen darstellt.

Ich werte unsere Pilotversuche zur Erprobung der Gesichtserkennung aber trotzdem als Erfolg, weil wir damit erstmals diese Technologie unter polizeilichen Alltagsbedingungen testen konnten. Seitdem wissen wir aus eigener Erfahrung, dass die technische Leistungsfähigkeit der biometrischen Gesichtserkennung noch nicht unseren polizeilichen Anforderungen entspricht.

Das wesentliche Problem für die polizeiliche Nutzung von biometrischen Verfahren wie der Gesichts- und im besonderen Maße der Iriserkennung ist, dass sie einer hohen Kooperationsbereitschaft des Betroffenen bedarf – die bei einer polizeilichen Personenkontrolle sicher nicht in jedem Fall vorausgesetzt werden kann.

Dazu kommt, dass im polizeilichen Einsatz nicht rund um die Uhr und an jeder Örtlichkeit Optimalbedingungen für diese Technologie herrschen. Wir können nicht wie in der privatwirtschaftlichen Nutzung eine „Laborsituation“ schaffen.

Innovative Technologie muss, um polizeiliche Maßnahmen wirkungsvoll zu unterstützen, in jeder Situation zuverlässig funktionieren. Und zwar unabhängig von den Lichtverhältnissen, der Kopfneigung, des dynamischen Hintergrunds oder der Qualität des vorgelegten Ausweisdokuments. Die Technik der biometrischen Verfahren muss hier noch deutlich verfeinert werden.

Wir werden in Bayern fortlaufend die Entwicklung biometrischer Verfahren verfolgen. Dabei hoffe ich auf den rasanten technologischen Fortschritt, damit unserer Polizei in naher Zukunft biometrische Verfahren zur Optimierung der polizeilichen Fahndungs- und Ermittlungsarbeit zuverlässig zur Verfügung stehen.

Eine wegweisende Entscheidung ist diesbezüglich die Aufnahme von biometrischen Merkmalen in amtliche Ausweisdokumente und Aufenthaltstitel, um zielgerichteter den Ausweismissbrauch bekämpfen zu können.

Sobald hier, wie von mir nachdrücklich gefordert, eine Entscheidung getroffen wurde, muss jeder Bundesbürger und Visumpflichtiger sein biometrisches Merkmal schon technisch aufbereitet im amtlichen und fälschungssichereren Dokument mit sich führen.

Leider hinken Deutschland und Europa in diesem Bereich weit hinterher. Ob in Bosnien-Herzegowina, Botswana, Jemen, Australien oder in Malaysia, viele Länder haben das, was die Bundesregierung seit Jahren verkündet, durch biometrische Merkmale in Ausweisdokumenten längst umgesetzt.

Überdies ist für mich nicht nachvollziehbar, dass im Gesetzeswerk der Bundesregierung ausdrücklich festgeschrieben ist, für die biometrischen Daten keine bundesweite Datei einzurichten.

Im Sinne einer erfolgreichen Gewährleistung der Inneren Sicherheit dürfen wir hier nicht auf halbem Wege stehen bleiben. Der Zugriff auf eine zentrale biometrische Datei würde polizeiliche Fahndungsmaßnahmen wesentlich erleichtern und beschleunigen. Gerade im Visumverfahren könnten wir mit der Speicherung biometrischer Daten Extremisten aus dem islamisch-fundamentalistischen Bereich sicher und schnell identifizieren.

Beispielsweise trat einer der Hauptattentäter der Anschläge des 11. September 2001, nämlich Mohammed Atta, mit unterschiedlichsten Namen und Namensschreibweisen sowie einer Vielzahl von Personaldokumenten in Erscheinung.

Meiner Meinung nach führt es gerade im Hinblick auf die aktuelle Bedrohungslage in Europa zu einem unverantwortlichen Sicherheitsdefizit, wenn wir in Deutschland dauer-

haft auf eine solche bundesweite biometrische Datei zur polizeilichen Nutzung verzichten müssen.

IV. Hoheitlicher Bereich der Flughafensicherheit

Meinen Ausführungen möchte ich auch einige Aspekte zum hoheitlichen Bereich der Flughafensicherheit anfügen:

Der Sicherheitsstandard an deutschen Flughäfen geriet durch die Medien in jüngster Vergangenheit wieder in den Blickpunkt der Öffentlichkeit.

Prinzipiell ist die Luftaufsicht Aufgabe der Luftfahrtbehörden und der für die Flugsicherung zuständigen Stellen. Im Luftverkehrsgesetz sind Regelungen zur Abwehr von Gefahren für die Sicherheit des Luftverkehrs sowie für die öffentliche Sicherheit und Ordnung durch die Luftfahrt festgeschrieben. Es sind auch Bestimmungen zum Schutz vor Angriffen auf die Sicherheit des Luftverkehrs enthalten.

Die Zuständigkeit der Luftfahrtbehörden ist jedoch nur auf das unmittelbare Flugplatzgelände beschränkt. Insoweit bleibt die gefahrenabwehrende Aufgabe der Polizei außerhalb des räumlich begrenzten Bereiches bestehen.

Wie sehen nun die Maßnahmen der Polizei aus?

Die polizeilichen Maßnahmen werden umsichtig der jeweiligen Lage angepasst. Insbesondere wurden nach den Terroranschlägen vom 11. September 2001 deutlich sensiblere und umfassendere Sicherheitskonzepte erarbeitet und inzwischen durchgeführt.

Am Beispiel bayerischer Flughäfen bedeutet dies: Die Bayerische Polizei nimmt neben den allgemeinpolizeilichen Maßnahmen auch grenzpolizeiliche Aufgaben zur umfassenden Gewährleistung der Sicherheit wahr. So werden zum Beispiel am Flughafen Nürnberg grenzpolizeiliche Kontrollen durchgeführt, um den grenzüberschreitenden Verkehr auch im Hinblick auf die Erfüllung des Schengener Durchführungsübereinkommens zu überprüfen.

Eine Ausnahme stellt der Flughafen München dar. Dort werden die grenzpolizeilichen Maßnahmen aufgrund eines Verwaltungsabkommens zwischen dem Freistaat Bayern und dem Bund vom Bundesgrenzschutz übernommen.

In diesem Kontext möchte ich nochmals die „Sicherheitslücken“ am Münchener Flughafen aufgreifen.

Aufgabe des Bundesgrenzschutzes ist es, die Sicherheit der Grenzen zu garantieren. Der Bund ist dringend aufgefordert, dafür zu sorgen, dass der Bundesgrenzschutz seiner Aufgabe auch am Flughafen München gerecht wird. Dazu muss dem Bundesgrenzschutz ausreichend Personal zugewiesen werden und auch tatsächlich zur Verfügung stehen. Es kann und darf nicht sein, dass in München ankommende Flüge wegen Personalmangel von der Kontrolle ausgenommen werden. Zumal in München auch Maschinen aus Ländern des Nahen und Mittleren Ostens landen. Schon deshalb haben wir ein massives Interesse dar-

an, dass jeder Einzelne, der aus einem Nicht-Schengen-Staat einreist, auch kontrolliert wird!

Gerade unter präventiven Gesichtspunkten kommt der Durchführung der Kontrollen an den Schengen-Außengrenzen eine prioritäre Bedeutung zu.

V. Schlussworte

Damit komme ich zum Ende meiner Ausführungen. Ich danke dem Deutschen Forum für Kriminalprävention für die hervorragende Organisation dieses Symposiums.

Insbesondere die Einbindung aller von dieser Thematik betroffenen Stellen gewährleistet meiner Meinung nach professionelle Ergebnisse; Ergebnisse, die geeignet sind, das Präventionsforum als kompetenten Ansprechpartner und Plattform für sicherheitstechnische Angelegenheiten öffentlich zu profilieren.

Daneben sind solche Veranstaltungen gut geeignet, unbegründete Ängste vor der Erhebung, Speicherung und Nutzung von biometrischen Merkmalen abzubauen. Ein breites Verständnis für den sachgerechten Einsatz dieser Technologie im Sicherheitsbereich würde uns auf dem Weg zu einer effizienteren Kriminalitäts- und insbesondere Terrorismusbekämpfung ein gutes Stück voranbringen!

Ich danke Ihnen für Ihre Aufmerksamkeit!

Der Einsatz biometrischer Verfahren aus datenschutzrechtlicher Sicht

von Peter Schaar, Bundesbeauftragter für den Datenschutz

Meine Damen und Herren,

in diesen unruhigen Zeiten erleben wird das Wiederaufleben der Diskussion um das Verhältnis von Sicherheit und Datenschutz. Diese Debatte sollte sachlich und möglichst konkret geführt werden, denn pauschale Forderungen und Schuldzuweisungen nützen weder der Sicherheit noch dem Datenschutz. Vielmehr kann die sachliche Auseinandersetzung zu Lösungen führen, die sowohl die Sicherheit verbessern als auch den Datenschutz voranbringen.

Ich bin Ihnen auch deshalb dankbar, dass Sie mir die Gelegenheit gegeben haben, mich hier zu dem Konzept Airport Security zu äußern. Es handelt sich dabei um einen interessanten Ansatz in dem weiten Feld möglicher praktischer Anwendungen von biometrischen Verfahren. Aus datenschutzrechtlicher Sicht enthält es eine Reihe von Elementen, die erwägenswert sind, aber auch Punkte, zu denen ich als Datenschützer ein klares „nein“ sage. Viele für den Datenschutz interessante Fragen bleiben in dem Konzept aber auch zunächst offen und werden sich konkret erst bei einer möglichen Umsetzung stellen. Ich möchte deswegen auch gar nicht in die Details des heute vorgestellten Konzepts gehen, sondern die Gelegenheit nutzen, um generell etwas zum Verhältnis zwischen Datenschutz und biometrischen Verfahren zu sagen, was dann natürlich auch für das Konzept „Airport-Security“ gilt.

Dabei möchte ich zunächst noch etwas Grundsätzliches zur Biometrie und den verwandten Begriffen sagen, denn in der öffentlichen Diskussion über Segen oder auch Gefahren biometrischer Verfahren scheinen manchmal die technischen Realitäten etwas zu kurz zu kommen.

Biometrie ist eigentlich das Vermessen von individuellen Körpermerkmalen von Lebewesen und die Nutzung dieser Merkmale, um Unterscheidungen vornehmen zu können. Neuerdings benutzen wir den Begriff „Biometrie“ überwiegend im Zusammenhang mit der automatischen Vermessung dieser Merkmale und den daraus resultieren Erkennungsverfahren und dem rechnergestützten Vergleich der Daten.

In der Biometrie unterscheidet man zwischen statischen (physiologischen) und dynamischen (verhaltenstypischen) Merkmalen. Die statischen Merkmale, die bei den derzeitigen Verfahren genutzt und eingesetzt werden, sind die der Finger, Hände oder des Gesichts, einschließlich der Augen. Bei den dynamischen Merkmalen sind es u.a. die Unterschriftendynamik oder das Tippverhalten beim Schreiben auf einer Tastatur, um einige Verfahren zu benennen.

Mit Hilfe der Biometrie ist es möglich, dass eine Person anhand ihrer charakteristischen Körpermerkmale von einem entsprechenden System automatisch, also ohne Mithilfe eines Menschen erkannt wird, wenn die Merkmale vorher im System gespeichert wurden.

In diesem Zusammenhang fallen häufig die Begriffe Verifikation und Identifikation; sie werden aber nicht sauber auseinandergehalten, was vielfach zu erheblicher Verwirrung führt. Unter Verifikation versteht man den 1:1 Vergleich, d.h. es wird nur überprüft, ob das abgespeicherte Merkmal mit dem aktuell aufgenommenen Merkmal übereinstimmt, eine Identifizierung der betroffenen Person, d.h. Feststellung der tatsächlichen Identität, findet aber nicht statt. Dies ist bei der Identifikation anders, bei der ein sogenannter 1:n Vergleich vorgenommen wird, das aktuell aufgenommene Merkmal also mit einer vorher in einer Datenbank abgespeicherten Datenmenge verglichen wird, um die Identität des Merkmalinhabers zu ermitteln.

Diese Unterscheidung ist auch datenschutzrechtlich von erheblicher Bedeutung. Während bei einer Verifikation die Verarbeitung auf der Karte oder dem Ausweis vorgenommen werden kann, so dass der Karteninhaber Herr seiner Daten bleibt und vom Aufbau mehr oder weniger umfangreicher Referenzdateien abgesehen werden kann, setzt eine Identifikation immer voraus, dass ein Abgleich mit zu diesem Zweck bereitgehaltenen Dateien vorgenommen wird, was eine Reihe von datenschutzrechtlichen Problemen zur Folge hat.

Von großer Bedeutung ist dabei auch die Fehlerhäufigkeit.

Bei den biometrischen Merkmalen sind nämlich unterschiedliche Wiedererkennungsraten gegeben. Dies hängt sowohl von dem Ausprägungsgrad des einzelnen Merkmals wie auch von der eingesetzten Technik ab. Nicht nur im Hinblick auf die Funktionsfähigkeit der Systeme, sondern auch datenschutzrechtlich sind solche Merkmale und Verfahren zu bevorzugen, die eine niedrige Fehlerrate aufweisen, denn die Zulässigkeit der Erhebung und Verarbeitung personenbezogener Daten knüpft zentral daran an, dass die Daten für die Aufgabenerfüllung erforderlich sind. Systeme mit hoher Fehlerrate sind jedoch nicht oder nur eingeschränkt verwendbar und die Datenerhebung mittels unzureichender Systeme für die Aufgabenerfüllung nicht geeignet und mithin im Regelfall unzulässig.

Fehlerhafte Ergebnisse biometrischer Verfahren werden danach unterschieden, ob eine fehlerhafte Erkennung einer unberechtigten Person (Falschakzeptanz) oder eine fehlerhafte Nicht-Erkennung eines Berechtigten (Falschzurückweisung) erfolgt. Der Anteil der fehlerhaften Ergebnisse wird als FAR *(false acceptance rat*e) oder FMR *(false match rat*e) bzw. FRR *(false rejection rat*e) oder FNMR *(false non match rat*e) bezeichnet.

In einem kürzlich veröffentlichten Test von Gesichtserkennungssystemen wurden aktuelle Zahlen über Falscherkennungen publiziert. Bei einer angenommen Falschakzeptanzrate (FAR) von 1 % wurden von den besten Geräten bei einem 1:1 Vergleich (Verifikation) ca. 90 % der Berechtigten erkannt und 10 % abgewiesen. Dies entspricht einer Falschzurückweisungsrate (FRR) von 10 %. Die Ergebnisse beziehen sich auf einen Datensatz von Frontalaufnahmen. Beim Vergleich gleichtätiger Innenaufnahmen betrug die Erkennungsrate bis zu 95 % (bei 1 % Falschakzeptanzrate); wurden Innen- und Außenaufnahmen gemischt, sank die Rate auf 50 %. Im Bereich der Fingerabdruckverfahren lagen die besten Ergebnisse bei einer 1 %igen FAR bei ca. 0,15 % Falschzurückweisungen.

Die bisher eingesetzten Verfahren sind alle im Bereich der Verifikation anzusiedeln. Nur dort ist – auch durch das kooperative Verhalten der Nutzer bedingt – eine akzeptable Fehlerrate gegeben bzw. die Einschränkungen für die Nutzer vertretbar. Alle im Bereich der Identifikation getesteten Verfahren haben zu hohe Fehlerraten und somit keine zufriedenstellenden Ergebnisse erzielt. Allerdings ist auch klar, dass bei größeren Datenbeständen auch die Fehlerrate entsprechend ansteigt, insbesondere bei einem Aufbau riesiger Referenzdateien. Es ist jedoch zu erwarten, dass in Zukunft durch den Fortschritt der Technik die Fehlerraten deutlich reduziert werden können. So sind weitere Versuche geplant um herauszufinden, unter welchen Bedingungen Erfolg versprechende Ergebnisse erzielt werden können.

Eine hohe Falscherkennung bzw. Falschakzeptanz wären bei einem biometrischen System unter Sicherheitsaspekten Ausschlusskriterien, insbesondere für einen Masseneinsatz wäre es ungeeignet. Fehlerhafte Rückweisungen hätten hingegen für die Betroffenen diskriminierende Auswirkungen und würden zu einer schlechten Akzeptanz des Verfahrens beim Nutzer führen: So geraten Personen, die durch das System zurückgewiesen werden, unter Druck, sich zu rechtfertigen und sie würden Gegenstand erweiterter Überprüfungen. Da sich das ganze in der Öffentlichkeit abspielt, könnten Mitreisende den Eindruck gewinnen, dass mit den Zurückgewiesenen etwas „nicht stimmt“.

Die Falschrückweisungsproblematik lässt sich auch nicht durch Kombination verschiedener biometrischer Merkmale, etwa Fingerabdruck und Gesichtserkennung, lösen; vielmehr würde eine Person bereits dann zurückgewiesen, wenn ein biometrisches Merkmal nicht passt. Im Ergebnis würde sich dadurch die Falschrückweisungsquote deshalb sogar erhöhen.

Welches biometrische Verfahren zum Einsatz kommt, ist aus datenschutzrechtlicher Sicht nicht gleichgültig. Es werden bereits sehr unterschiedliche Merkmale getestet. Hierzu gehören z.B. Gesicht, Iris, Retina, Finger, Handgeometrie, Venenmuster auf dem Handrücken, Ohr, DNA, und Unterschrift, Gang, Tippverhalten an der Tastatur sowie Stimme und Sprechverhalten.

Viele Merkmale haben in den jeweiligen Anwendungen Vor- und Nachteile. So hängt es u.a. von den Umgebungsbedingungen ab, wo die Erkennung vorgenommen wird. Für viele Verfahren sind entsprechende Lichtverhältnisse wichtig, während andere wie z.B. die Fingererkennung dieses Kriterium nicht benötigt, dafür aber andere Erkennungsprobleme auftreten können.

Aus diesem Grunde kann ich auch keine generelle Empfehlung für ein bestimmtes Verfahren aussprechen, da bei jeder Anwendung die jeweiligen Randbedingungen beachtet werden müssen.

Ich will aber nicht verhehlen, dass ich die Iris-Erkennung am ehesten für ein Verfahren halte, das datenschutzrechtlichen Anforderungen genügen kann, weil die aktive Mitwirkung der Betroffenen dafür unerlässlich ist. Eine heimliche Überwachung, wie sie etwa Verfahren der Gesichtserkennung möglich – und damit wohl leider auch wahrscheinlich

– machen würden, wäre hier ausgeschlossen. Die Betroffenen können sicher sein, dass jede Maßnahme der Verifikation oder gegebenenfalls auch der Identifikation von ihnen als solche wahrgenommen wird, weil sie sich aktiv daran beteiligen.

Damit komme ich zum nächsten datenschutzrechtlichen Aspekt, nämlich dem der Datenerfassung:

Sensoren erfassen ein biometrisches Referenzmuster (Rohdaten) elektronisch und speichern dieses Muster im System („Enrollment"). Dies kann auch ohne Kenntnis der Person erfolgen, z.B. bei der Auswertung von Fingerabdrücken oder bei Gesichtsaufnahmen von Fotos oder bei der Videobeobachtungen. Bei dem Erkennungsvorgang werden dann erneut die Merkmale (Rohdaten) erfasst, die spezifischen Merkmale (z.B. Koordinaten von Verzweigungen oder Enden von Fingerabdrucklinien) herausgelesen und mittels eines mathematischen Verfahrens in einen reduzierten Datensatz (Template) umgewandelt und mit den bereits gespeicherten Referenzdaten verglichen. Bei einer Übereinstimmung ist die Erkennung erfolgreich.

Bei geschlossenen Systemen reicht es aus, das nur noch das Template gespeichert wird, es enthält die für einen Vergleich notwendigen Daten, erlaubt aber üblicherweise Rückschlüsse auf die Person nur in eingeschränktem Umfang.

Weder für die Verifikation noch für die Identifikation mittels biometrischer Verfahren ist es erforderlich, biometrische Rohdaten zu speichern.

Hier ist zwischen geschlossenen und offenen Anwendungen zu unterscheiden:

Bei geschlossenen Anwendungen ist die Umgebung, das zugrundeliegende System und der Personenkreis, der an der Anwendung teilnimmt, vorgegeben. Ein Einsatzschwerpunkt ist derzeit sicherlich die Zutritts- bzw. Zugangskontrolle. Je nach Anwendung werden Verifikations- oder auch Identifikationssysteme eingesetzt.

Zu den offenen Anwendungen sind sicherlich die im hoheitlichen Bereich durchgeführten Verfahren zu zählen. Hier ist die Aufnahme von biometrischen Merkmalen in den Pass das beste Beispiel. Bei dieser Anwendung ist das biometrische Merkmal und die Ausweis-Lesetechnik vorgegeben. Die Systeme, die die biometrischen Daten des Ausweises mit den aktuell (live) aufgenommenen Daten vergleichen, um so eine Erkennung vornehmen zu können, können unterschiedlich sein. Soweit in derartigen Systemen biometrische Rohdaten verwendet werden, könnten Staaten, die unseren rechtsstaatlich-demokratischen Vorstellungen nicht entsprechen, unter Einsatz der entsprechenden Technik ungehinderten Zugang zu den vollständigen biometrischen Daten erhalten. Gerade bei Massenanwendungen, wie z.B. Pässen, sind viele Stellen und Nationen in die Sicherheitskette eingebunden und über Sicherheitsalgorithmen (Verschlüsselungstechniken) informiert.

Deswegen muss hier sehr bedacht vorgegangen werden. Größtmögliche Transparenz ist sowohl hinsichtlich der gespeicherten Daten als auch in Bezug auf die Sicherungsmaßnahmen erforderlich. Der rechtliche Rahmen, die Implementierung solcher Systeme und die dafür wahrscheinlich erforderliche Standardisierung dürfen nicht in mehr oder weni-

ger geheimen Zirkeln unter Ausschluss der Öffentlichkeit ausgehandelt werden. Ich halte nichts von dem Prinzip „Security by Obscurity“, bei dem die Sicherheit des Systems von der Geheimhaltung seiner Funktionsweise abhängig ist. Sicherheitsmaßnahmen müssen effektiv und nachprüfbar gestaltet werden, die Sicherheits-Algorithmen dürfen nicht geheim bleiben. Offenheit bedeutet hier nachgewiesene Sicherheit. Zieht man die Zahl der beteiligten Staaten und Institutionen in Betracht, die mit Reisedokumenten umgehen sollen, wäre eine Geheimhaltung der Sicherheitsmechanismen bei biometrischen Verfahren zur Verifikation in diesem Bereich darüber hinaus auch völlig unrealistisch.

Meine Damen und Herren, nach diesen eher allgemeinen Ausführungen zu Biometrie und Datenschutz möchte ich zum Abschluss noch einmal konkret zusammenfassen, welche Anforderungen der Datenschutz an biometrische Systeme und Verfahren stellt:

– Die Speicherung der biometrischen Daten hat ausschließlich so zu erfolgen, dass sie in der Verfügungsgewalt der Betroffenen (dezentrale Speicherung, z.B. Chip) bleiben und nicht durch Dritte ausgelesen werden können.

– Biometrische Daten dürfen nur in verschlüsselter Form gespeichert werden.

– Die Datensätze dürfen nur in einer gesicherten Umgebung (Netzwerk, Datenbank) aufgenommen und verarbeitet werden.

– Beim Datentransfer und insbesondere bei der Verwendung von Funkübertragungsstrekken (z.B. Nutzung von RFID-Chips als Speicher) sind die Daten verschlüsselt zu übertragen.

– Nur die für den späteren Vergleich notwendige Merkmale und keine Überschussinformationen dürfen aufgenommen und gespeichert werden, nach Möglichkeit sind nur Templates zu speichern.

– Eine strenge Zweckbindung der Daten ist sicherzustellen.

– Nur kooperative biometrische Verfahren sind einzusetzen (die zu überprüfende Person muss aktiv in die Prüfung einbezogen werden, keine verdeckte Erfassung).

– Auch bei den Lesegeräten muss eine größtmögliche Datensicherheit erzeugt werden.

– Keine zentrale Speicherung der Daten.

– Zustimmung der Beteiligten, wenn keine gesetzlichen Vorgaben vorhanden sind.

– Nur solche Verfahren dürfen zum Einsatz kommen, die eine Benachteiligung bestimmter Personengruppen weitgehend ausschließen. Für Menschen, die das verwendete biometrische Merkmal nicht nutzen können, bedarf es praktikabler, diskriminierungsfreier Ersatzlösungen.

Konkret für das heute vorgestellte Konzept Airport-Security bedeutet dies, dass aus datenschutzrechtlicher Sicht gegen einen lokalen biometrischen Flughafenausweis für all diejenigen, die Zutritt zu den nicht für jedermann zugänglichen Bereichen eines Flughafens haben müssen, keine grundlegenden Bedenken bestehen.

Ein Flugpass für Passagiere, der ja über den Bereich eines bestimmten Flughafens hinaus Anwendung finden müsste, setzt eine entsprechende Infrastruktur voraus, die je nach Ausgestaltung erhebliche datenschutzrechtliche Probleme aufwerfen könnte. Auf jeden Fall wäre ein solches Verfahren nur auf Basis der Einwilligung der Flugpassagiere zulässig. Wirksame Einwilligungserklärungen setzen eine umfassende Information der Betroffenen voraus. Vor allem muss die tatsächliche Freiwilligkeit gewährleistet sein, d.h. der Service oder konkret: die Abfertigung darf nicht daran gebunden werden, dass der Betroffene in die Verwendung seiner biometrischen Daten einwilligt.

Schließlich muss technisch und organisatorisch gewährleistet sein, dass die biometrischen Flugpass-Daten nicht unbefugt verwendet werden und dass sie nicht in zentralen Dateien gespeichert werden, sondern ausschließlich in dem Dokument selbst. Damit würden sich auch weitere Datenschutzprobleme vermeiden lassen, die sich bei dateimäßiger Speicherung ergeben würden: Ich denke hier insbesondere an die Problematik der Übermittlung personenbezogener Daten in das Ausland, die ja nur unter sehr restriktiven Bedingungen zulässig ist.

Die ebenfalls in dem Papier vorgeschlagene Verwendung der zur Identitätsfeststellung erhobenen digitalisierten Gesichtsbilder für die Videoüberwachung mit automatischem Bildabgleich lehnen wir Datenschützer ab, weil dies zu einer unkontrollierbaren, personenbezogenen Rundumbeobachtung führen würde. Zudem würde es sich dabei um eine Zweckänderung handeln, die mit den Primärzwecken der Erhebung der Daten, der Verifikation der Flugdokumente, nicht kompatibel wäre. Dieser Mangel könnte auch nicht durch eine Einwilligungslösung „geheilt“ werden, da die Überwachung nicht nur die Inhaber von Flugpässen und Flughafenmitarbeiter, sondern auch sonstige Dritte betreffen würde.

Kommen wir zurück zum Ausgangspunkt: Biometrische Verfahren können unter bestimmten Rahmenbedingungen die Sicherheit verbessern und zugleich den Datenschutz wahren. Insoweit besteht auch in der Biometrie zwischen beiden Zielen kein unauflösbarer Widerspruch. Die Grenze des Zulässigen und Sinnvollen ist aber nicht notwendigerweise identisch mit dem technisch Machbaren. Dessen sollten sich alle Beteiligten bewusst sein. Andernfalls würde der Erfolg solcher Systeme in Frage gestellt, nicht zuletzt mangels Akzeptanz der Betroffenen, aber auch im Hinblick auf die Wahrung unserer demokratischen Errungenschaften.

Ich danke für Ihre Aufmerksamkeit.

Die Diskussion:
Was fordert die Politik und was wird von der Politik gefordert?

Zum Abschluss diskutierten der *bayerische Innenminister Dr. Beckstein, die Mitglieder des Deutschen Bundestages Silke Stokar (Bündnis 90 / Die Grünen), Clemens Binninger (CDU) und Dr. Max Stadler (FDP) sowie der Bundesbeauftragte für den Datenschutz Peter Schaar* eine Vielzahl von Aspekten des Biometrie-Einsatzes.

Die Moderation bezog dabei auch eine Reihe von Fragen aus dem Publikum mit ein.

Während *Silke Stokar* vor einer zu großen Technologiegläubigkeit warnt und biometrische Verfahren als Ergänzung zu konventionellen Überprüfungsabläufen sieht, fordert *Clemens Binninger* vor dem Hintergrund der wachsenden Herausforderungen bei der Bekämpfung von Terrorismus und Kriminalität eine Entlastung des Sicherheitspersonals durch geeignete technische Möglichkeiten, zu denen biometrische Kontrollverfahren mittlerweile gehören. Biometrie zu vernachlässigen sei seiner Meinung nach „unverantwortlich."

Dr. Stadler und vor allem auch der *Bundesdatenschutzbeauftragte Schaar* betonen das Erfordernis, den Bürger vor ausufernder und missbräuchlicher Nutzung seiner biometrischen Daten zu schützen. Durch Biometrieeinsatz erreichbare Sicherheitszugewinne sollten nicht alleiniger Maßstab der Entscheidungsfindung sein. Zugleich gelte es, die Kontrolle über zulässige biometrische Datenerfassungen und Abgleiche zu behalten. *Stokar* ergänzte, dass es dem Bürger immer bewusst sein müsse, wann er Objekt eines biometrischen Scans wird.

Übereinstimmend waren die Auffassungen, dass sowohl die Tauglichkeit als auch die Datenschutzaspekte in weiteren Pilot-Anwendungen mit unterschiedlichen technischen Verfahren zu prüfen seien.

Zur Frage, inwieweit der Einsatz hoheitlicher Ausweisdokumente auch zur Authentisierung von Berechtigten im privatrechtlichen Bereich zur Anwendung kommen können, sind die Meinungen geteilt. *Silke Stokar* sieht wenig Spielräume, während aus Sicht der Flughafenbetreiber dadurch effiziente Abläufe erreichbar wären.

Gegensätzlichkeit bestand auch bei der Frage, ob Abgleiche biometrischer Daten im so genannten Identifikationsverfahren erfolgen können. Im Gegensatz zum Verifikationsverfahren, bei dem ein Datenabgleich von Ausweis und Person erfolgt, wird – zum Zweck der Identifikation – die Berechtigung einer Person mit den entsprechenden biometrischen Daten in einer Datenbank hinterlegt, so dass für den Abgleich im Rahmen einer Zugangskontrolle ein Ausweis entbehrlich wird. *Minister Beckstein* hält ein solches Verfahren für zweckmäßig (Ausweise können verloren gehen oder vergessen werden). Gegen das Identifikationsverfahren sprechen aus Sicht von *Stadler, Schaar und Stokar* datenschutzrechtliche Erwägungen, insbesondere die Gefahr missbräuchlicher Nutzungen. Seitens der *Flughafenbetreiber* wird die Beibehaltung von sichtbar getragenen Mitarbeiterausweisen befürwortet, weil damit die Erkennbarkeit eines Berechtigten auch im Sicherheitsbereich erleichtert sei.

Binninger und Beckstein befürworten darüber hinaus im Bereich der hoheitlichen Fahndung nach Gefährdern und Straftätern Videoüberwachungsmaßnahmen mit Datenabgleichen im Identifikationsmodus. In engen Grenzen könnte trotz datenschutzrechtlicher Vorbehalte einem solchem Vorschlag auch aus Sicht der *anderen Diskutanten* zugestimmt werden.

Schließlich wird seitens *einiger Wirtschaftsvertreter* eine engere und schnellere Kooperation von Politik und Wirtschaft im Hinblick auf die Umsetzung innovativer technischer

Verfahren eingefordert. Für die Regierungsfraktionen erklärte *Silke Stokar*, dass nicht Wirtschaftsinteressen allein den Verlauf politischer Entscheidungsprozesse, die hier zudem sensibel im Hinblick auf die Wahrung von Bürgerrechten einzuschätzen sind, bestimmen dürfen. Das Parlament müsse seiner Verantwortung in angemessener Weise Geltung verschaffen.

Die Diskussion hat am Ende gezeigt, dass Kriminalprävention und Biometrie ein Thema mit Zündstoff in der gesellschaftlichen und politischen Diskussion bleiben wird. Das DFK wird weiterhin ein Forum für aktuelle Debatten um realisierbare Sicherheitszugewinne und berechtigte Datenschutzinteressen der Bürger sein.

Pressemitteilung des DFK

DFK stellt Konzept zur Verbesserung der Sicherheit auf Flughäfen vor

Bonn, 31. März 2004 – Das Deutsche Forum für Kriminalprävention (DFK) stellt heute in Berlin mit seinem Konzept „Airport Security – Biometrische Applikationen zur Verbesserung der Sicherheit an Flughäfen" den präventiven Nutzen biometrischer Verfahren im nicht-hoheitlichen Bereich zur Erhöhung der Sicherheit auf Flughäfen dar.

Das Konzept wird im Rahmen des Symposiums „Biometrie und Flughafensicherheit" präsentiert. Das DFK leistet mit der Einrichtung des Arbeitskreises „Kriminalprävention und Biometrie" einen wichtigen gesellschaftlichen Beitrag und schlägt den Bogen zwischen dem allgemeinen Sicherheitsbedürfnis einerseits und dem Schutz der individuellen Privatsphäre andererseits.

Der mit dem vorgelegten Diskussionsbeitrag verfolgte Grundansatz ist die Erhöhung der Sicherheit des (privat-rechtlichen) Flughafen- und Flugbetriebes einschließlich des stattfindenden Personenverkehrs unter kriminalpräventiven Gesichtspunkten durch Nutzung biometrischer Verfahren. Ein Kernpunkt hierbei ist die Einführung eines standardisierten „Flughafenausweises" für Mitarbeiter der Flughafenbetreiber, der Fluggesellschaften und sonstiger im Sicherheitsbereich eines Flughafens tätiger Unternehmen sowie eines neuartigen „Flugpasses" für Passagiere der gewerblichen Luftfahrt. Wesentlicher Bestandteil der Ausweise werden die biometrischen Merkmale der jeweils berechtigten Inhaber sein. Somit wird zweifelsfrei sichergestellt, dass auch nur der tatsächlich berechtigte Ausweis-

träger den jeweiligen Sicherheitsbereich des Flughafens betritt und der Flugreisende mit der für den Flug eingecheckten Person identisch ist (Verifikation).

Für die Ankunfts- und Abflughallen werden Videoüberwachungsmaßnahmen vorgeschlagen, die mit biometrischen Gesichtserkennungssystemen ausgerüstet sind, die nur Bilder von mit Hausverbot belegten und/oder gesuchten Personen anzeigen, wenn diese einen der Kontrollpunkte passieren (Identifikation).

In dem Konzept werden – für die verschiedenen Anwendungszwecke getrennt – auch die rechtlichen, insbesondere datenschutzrechtlichen Rahmenbedingungen betrachtet und Hinweise für notwendige Klärungen gegeben.

Der bayerische Staatsminister des Innern Dr. Günther Beckstein erklärt in seinem Vortrag: „Auch zu Gunsten der Flughafensicherheit können die seit Jahren positiven Ergebnisse bei der Nutzung biometrischer Verfahren zur Automatisierung von Zutrittskontrollen zum Beispiel von Mitarbeitern des Flughafenbetreibers in besonders gefährdeten Gebäudeteilen erfolgreich genutzt werden. Aber auch im hoheitlichen Anwendungsbereich wie der polizeilichen Nutzung biometrischer Verfahren schlummert meiner Überzeugung nach ein enormes Potenzial zur Optimierung der Kriminalitätsbekämpfung. Die umsichtige Nutzung biometrischer Verfahren wäre ein Quantensprung für die Kriminalprävention und Repression!“

Im weiteren Verlauf des Symposiums diskutieren eine Reihe ausgewiesener Experten aus Politik und Wirtschaft die aufgezeigten Möglichkeiten, Biometrie im Flughafenbetrieb zur Erhöhung der Sicherheit einzusetzen. Teilnehmer sind neben Staatsminister Dr. Beckstein u. a. Clemens Binninger (MdB, CDU), Dr. Dieter Wiefelspütz (MdB, SPD), Dr. Max Stadler (MdB, FDP) und Silke Stokar (MdB, BÜNDNIS 90 /DIE GRÜNEN). Neben der Beleuchtung des Themas aus der Perspektive von Flughafenbetreibern und Luftfahrtgesellschaften werden auch datenschutzrechtliche Aspekte aufgegriffen: Der Bundesbeauftragte für den Datenschutz Peter Schaar referiert über den „Einsatz biometrischer Verfahren aus datenschutzrechtlicher Sicht“.

„Wir freuen uns sehr, auf unserem Symposium ein so breites Themenspektrum mit Experten aus Politik und Wirtschaft bieten zu können“, so Norbert Salmon, stellvertretender Vorstandsvorsitzender des DFK. „Wir hoffen, mit Hilfe dieser Veranstaltung den Nutzen neuer Technologien zur Kriminalitätsprävention aufzeigen und die öffentliche Akzeptanz nachhaltig fördern zu können. Außerdem wollen wir zu einer unvoreingenommenen fachlichen Bewertung des präventiven Nutzens von Biometrie beitragen.“

Über das Deutsche Forum für Kriminalprävention (DFK)

Das Deutsche Forum für Kriminalprävention wurde 2001 auf Initiative der Innenministerkonferenz (IMK) als gemeinnützige privatrechtliche Stiftung von Bund und Länder gegründet.

Intention des DFK ist es, durch Vernetzung und Kooperation, Bündelung von Präventionsaktivitäten, Wissenstransfer sowie Sensibilisierung einer breiten Öffentlichkeit eine nach-

haltige Kriminalprävention zu stärken und im Rahmen eines gesamtgesellschaftlichen Ansatzes bundesweit staatliche und gesellschaftliche Kräfte in gemeinsamer Verantwortung zusammen zu führen.

Ziel ist es, der Kriminalität durch vorbeugende Maßnahmen Einhalt zu gebieten, die durch Kriminalität entstehenden Schäden zu verringern und das Sicherheitsgefühl der Bevölkerung zu stärken. Alle gesellschaftlichen Kräfte sind aufgerufen, hierzu ihren Beitrag zu leisten.