

Effektiv aber ungerecht? – Eine ethische Perspektive auf risikobasierte Sicherheitsstrukturen an Flughäfen

Matthias Leese

1 Einleitung

Unbegrenzte Mobilität ist das Paradigma moderner Gesellschaften.¹ Oder, wie Urry (2007) es formuliert: Bewegung ist eng verknüpft mit der Existenz von Leben an sich. Gleichzeitig werden in einem zunehmend als unsicher wahrgenommenen globalen Umfeld umfassende Sicherheitsapparate entlang der Reise- und Transportinfrastrukturen etabliert. Wie zahlreiche Autoren (etwa Lahav/Guiraudon 2000; Pallitto/Heyman 2008) betonen, haben die neueren Entwicklungen bei Grenzregimen auch in den regulären Reise- und Mobilitätsbereich Eingang gefunden und somit die intensive Überprüfung an der Landesgrenze auf öffentliche Transportknotenpunkte übertragen. Besonders in der Luftfahrt, die durch die Anschläge vom 11. September 2001 ins Zentrum der öffentlichen Aufmerksamkeit im Kampf gegen den Terrorismus gerückt wurde, zeichnen sich Intensivierungen einer bereits länger anhaltenden Versicherheitlichung ab (Lyon 2003). Der vorliegende Aufsatz untersucht die immanente Verlagerung von Sicherheitsmechanismen hin zu Risiko als Hauptparadigma im Bemühen, Passagierkontrollen in Zeiten stetig steigender globaler Reisebewegungen sowohl wirksam als auch effizient zu gestalten. Im Grunde genommen verfügen moderne Flughäfen schon seit längerer Zeit über erhebliche Sicherheits- und Überwachungsmaßnahmen, die sich zu intensiven und invasiven Kontrollen am Checkpoint zuspitzen. Hierbei handelt es sich nach Sweet (2009) um die letzte Verteidigungslinie zwischen dem öffentlich zugänglichen landseitigen Bereich und dem gesicherten luftseitigen Bereich, der für den – als harmlos eingestuft – Fluggast reserviert ist. Abhängig vom internationalen und nationalen gesetzlichen Rahmen und dem jeweiligen Flughafen finden sich hier eine große Bandbreite an Sicherheitsmaßnahmen, einschließlich Röntgentechnik für Reisegepäck, Metalldetektor-Portalen und Sicherheits- oder Körperscannern für Passagiere, ergänzt durch manuelles Abtasten, Videoüberwachung und Sprengstoffdetektion.

Insgesamt wird durch dieses Arrangement von moderner Technologie und streng reglementiertem Verhalten das Reisen für Passagiere immer unbehaglicher und stressreicher. Die Luftfahrt sieht sich dabei schwerlich kompatiblen Interessen von unterschiedlichen Stake-

¹Frühere Versionen dieses Aufsatzes wurden auf der SIRA Conference Series 3 im Mai 2012 und dem NCAS Workshop „New Passenger Security Concepts“ im Juli 2012 vorgetragen. Der Verfasser ist dankbar für alle aufschlussreichen Kommentare und Anmerkungen auf beiden Veranstaltungen sowie für das kritische Feedback von Regina Ammicht Quinn. Die zugrundeliegenden Forschungsarbeiten wurden im Rahmen des vom Bundesministerium für Bildung und Forschung (BMBF) geförderten Projekts KRETA (kreta.uni-tuebingen.de) durchgeführt.

holdern gegenüber: dem angenehmen und bequemen Reisen für die Fluggäste, dem maximalen Schutz vor Terroranschlägen und anderen Straftaten, sowie der Forderung nach Effizienz, um unnötige Kosten zu vermeiden, und dem allgemeinen Paradigma, die Luftfahrt weiterhin als schnellste Form des Reisens zu vermarkten (Adey 2006). Gerade durch die immer aufwendigeren Kontrollverfahren entsteht jedoch ein gesteigertes Unbehagen auf Seiten der Passagiere, das bei den internationalen Luftfahrtverbänden Aktionismus hervorgerufen hat. Insbesondere die International Air Transport Association (IATA) präsentiert sich ernsthaft bemüht, eine Lösung zur Entschärfung der Gegensätze zu finden und eine fundamentale Veränderung im Gesamtansatz zur Flugsicherheit herbeizuführen. Dazu der Generaldirektor und Vorstandsvorsitzende der IATA, Giovanni Bisignani, in einer Presseerklärung im Jahr 2011: „We spend 7.4 billion Dollars a year to keep aviation secure. But our passengers only see hassle. Passengers should be able to get from curb to boarding gate with dignity. That means without stopping, stripping or unpacking, and certainly not groping.“² Zwar klingt das sicherlich wie ein hehres Ziel, jedoch hat die Art der geplanten Umsetzung bei Vertretern von Bürger- und Menschenrechten zu Kritik geführt.

Bisher kommt ein regelbasierter oder bürokratischer Grundsatz (O'Malley 2006) bei der Sicherheitskontrolle zum Einsatz. Jeder Passagier muss also dieselben Kontrollmaßnahmen durchlaufen. Die aktuell zu beobachtenden Trends weisen allerdings in die entgegengesetzte Richtung. Auf der IATA-Jahreskonferenz 2011 in Singapur wurde ein Konzept für den „Checkpoint of the Future“ vorgestellt³, das die Aufmerksamkeit der Öffentlichkeit und der Medien auf sich zog. Der Kerngedanke des Vorschlags ist eine datengestützte Passagieranalyse, die die Reisenden in unterschiedliche Risikokategorien unterteilt. Dieses Konzept ähnelt verblüffend dem amerikanischen CAPPS II (Computer-Assisted Passenger Prescreening System) Ansatz, der 2004 – aufgrund von schwerwiegenden Bedenken bezüglich Privatsphäre und Bürgerrechten – von der US-Luftsicherheitsbehörde TSA (Transportation Security Authority) wieder aufgegeben wurde. Bei CAPPS II war die Errechnung einer statistischen Risikobewertung für jeden Passagier auf der Grundlage von Informationen wie z.B. soziodemographische Daten, Reiseroute, Art der Bezahlung, frühere Reisen etc., vorgesehen (vgl. Barnett 2004: 912). Die Reisenden sollten dann je nach ihrem Risikostatus als potenzielle Terroristen oder harmlose Passagiere mit unterschiedlicher Intensität kontrolliert werden. Der „Checkpoint of the Future“ greift dieses Prinzip im Wesentlichen wieder auf und sieht vor, die Passagierströme mittels einer umfangreichen Sammlung von Passagierinformationen zu klassifizieren und zu sortieren. Das IATA-Konzept ist nicht der einzige Vorschlag, in dem die Risikobewertung als Lösung für die drängenden Probleme der Luftfahrt angepriesen wird. Der Airports Council International (ACI) und die Association of European Airlines (AEA) haben ein gemeinsames Konzept mit dem Namen „Better Security“ (ACI/AEA 2011) vorgelegt, welches im Wesentlichen eine sehr ähnliche Funktionsweise beschreibt.

Es scheint, dass diese neuen Sicherheitsansätze einen Ansatz neu aufgreifen, der bereits von Bürgerrechtsaktivisten und demokratischen Entscheidungsträgern als unzureichend beurteilt wurde.⁴ In Abhängigkeit zur zugewiesenen Bedrohungsstufe würden Passagiere in risikobasierten Screening-Ansätzen Kontrolltunnel durchlaufen müssen, die imstande wären, verschiedene Sicherheitstechnologien (z.B. biometrische Identifikation, Objektdeteksi-

²<http://www.iata.org/pressroom/pr/pages/2011-06-07-01.aspx>

³<http://www.iata.org/pressroom/pr/pages/2011-06-07-01.aspx>

⁴Zu einer umfassenden Kritik an CAPPS II siehe etwa Curry (2004).

on, Materialdetektion, Sprengstoffanalyse) abhängig vom jeweiligen Risikostatus des Reisenden zu (de-)aktivieren. Damit wären Passagiere mit mehr (hohes Risiko) oder weniger (geringes Risiko) Kontrollmaßnahmen konfrontiert. Es ist zwar davon auszugehen, dass die technischen Voraussetzungen für eine solche Lösung in ihrer vollen Bandbreite erst in einigen Jahren zur Verfügung stehen werden, die IATA sieht jedoch eine stufenweise Einführung von risikobasierter Differenzierung vor. Allgemein gesprochen ist dieser Trend zur Hinwendung zu präemptiver Sicherheit, die auf Antizipation und Risiko setzt, nicht nur in der Luftfahrt, sondern auch in vielen anderen sicherheitsrelevanten Bereichen erkennbar, etwa bei Grenzkontrollen oder der Überwachung von Finanzströmen.

Der Risikobegriff wirft jedoch Fragen zu ethischen Aspekten der vorgesehenen Kontrollstrukturen auf. Im Weiteren wird argumentiert, dass die Umsetzung eines risikobasierten Screenings am Checkpoint Gefahr läuft, Menschen- und Bürgerrechte zu verletzen. Im Hinblick auf Gerechtigkeit und Diskriminierung bestehen starke Bedenken bezüglich der Auswirkung von Datenanalyse und Risikobewertung, da Risikoklassifizierung und die Sortierung von Passagierströmen dazu tendieren, Vorurteile oder soziale Kategorien zu reproduzieren. Einfacher gesagt: gewisse Eigenschaften, die dem Klischee eines Terroristen entsprechen (d.h. jung, männlich, Araber, Moslem) könnten dafür sorgen, dass entsprechende Personen mit einer höheren Wahrscheinlichkeit als Hochrisikopassagiere eingestuft werden, selbst wenn von ihnen keinerlei Bedrohung ausgeht. Durch die notwendige Geheimhaltung der von den Sicherheitsbehörden genutzten Kriterien zur Risikobewertung werden den betroffenen Einzelpersonen strukturell bedingt grundlegende Prinzipien der Privatsphäre und des Datenschutzes vorenthalten, wie z.B. die Möglichkeit der Einsicht in gespeicherte Informationen bzw. deren Aktualisierung und Korrektur. Darüber hinaus kommt es zu einer Reproduktion von ökonomischen Ungleichgewichten in der Risikobewertung, bedingt durch die zunehmende Deckungsgleichheit von privatwirtschaftlichen und behördlichen Strukturen in der Luftfahrt. Programme wie „Frequent Flier Clubs“, sowie die Möglichkeit einer Registrierung als „trusted traveler“ tragen dazu bei, die Grenzen zwischen den Informationsquellen für die Risikobewertung zu verwischen und stehen vor allem zahlungskräftigen Vielfliegern zur Verfügung. Durch die Angabe von zusätzlichen persönlichen Informationen und einem Background-Check wird es möglich, sich eine privilegierte Behandlung an bei der Sicherheitskontrolle schlichtweg zu erkaufen. Dies führt in der Konsequenz zu einer automatisierten Zuordnung in eine Niedrigriskokategorie, da „bekannte“ Reisende freiwillig genügend Informationen angegeben haben, um als harmlos eingestuft zu werden.

2 Disziplin und Einschüchterung: Der Flughafen

Fuller und Harley (2004) haben den Flughafen als gesellschaftliches Labor beschrieben, von dem aus Entwicklungen speziell bezüglich Sicherheitsmaßnahmen auch auf gesellschaftliche Bereiche übergreifen können. Flughäfen setzen die affektive Dimension sehr geschickt ein, um spezielle Stimmungen und Wahrnehmungen zu erzeugen, so etwa Unwohlsein und Bedrohlichkeit (Adey 2009), die nur durch die die strenge Einhaltung der Sicherheits- und Verhaltensregeln aufgelöst werden können. Auf diese Weise werden Flughäfen zu Orten extremer Disziplin (Lyon 2003), die das Individuum einem umfassenden Sicherheitsparadigma unterordnen. Invasive Sicherheitsmaßnahmen werden daher auf Flughäfen eher akzeptiert als andernorts (Lüdemann/Schlepper 2010). Diese Akzeptanz ist im deutschen Kontext unter

anderem der Angst vor Terroranschlägen zugeschrieben worden (Leese 2013), beruht aber auch auf den charakteristischen Eigenschaften von speziellen Transit-Orten wie Flughäfen, die Augé (2006) als „Nicht-Orte“ beschrieben hat. Diese Orte existieren nur für den alleinigen Zweck der Mobilität und zeichnen sich durch das Fehlen dauerhafter Bewohner und regulärer sozialer Interaktionen aus. An einem Ort wie dem Flughafen, wo jeder im Prinzip ein Fremder bleibt und Reisende sich permanent fortbewegen, kann kein traditionelles Vertrauensverhältnis aufgebaut und gefestigt werden, das zu einer Bewertung der Harmlosigkeit des Einzelnen führen könnte. Wie Bauman (2003: 106) betont: Es ist nicht möglich, die Absichten des Fremden zu kennen, der daher den unbekanntem Teil einer jeden sozialen (Sicherheits-)Gleichung darstellt. In einem Umfeld wie dem des Flughafens, das allgemein stark auf rationalisierte Strukturen und Risikomanagement setzt (Lyon 2006; Adey 2008; Salter 2008a), wird dies zum Problem. Um der Ungewissheit zu begegnen, die der reisende Fremde verursacht, soll eine größtmögliche Menge an persönlichen Informationen über Passagiere helfen, ihre Geschichte und Persönlichkeit zu rekonstruieren, sowie – am allerwichtigsten – ihre Absichten enthüllen (Curry 2004). Auf Flughäfen wird das Wissen über die Reisenden mittels einer digitalen Datenspur erzeugt, die mit dem Kauf eines Flugtickets beginnt (Bennett 2005, 2008) und sich über Check-in und Sicherheitskontrolle und gegebenenfalls bis hin zur Einreiseprozedur am Zielflughafen fortsetzt. Sicherheit wird in der Konsequenz über die digitale Dopplung von Identitäten in Datenbanken realisiert (Haggerty/Ericson 2000).

Die Abkopplung der digitalisierten Informationen von der realen Person ermöglicht es den Sicherheitsbehörden, den Passagier im Namen der Sicherheit in seine einzelnen informationellen Bestandteile zu zerlegen, zu überprüfen, neu zu arrangieren, zu berechnen, zu übermitteln und schließlich wieder zu rekonstruieren. Wie Lyon (2006) anmerkt, hat Flughafensicherheit seit jeher das Ziel, gefährliche Personen und Gegenstände aus dem massiven Strom von Reisenden, die jeden Tag die Sicherheitskontrollen passieren, auszusortieren. Mechanismen der Risikobewertung können nur dann effektiv arbeiten, wenn sie die verfügbaren Datenquellen maximal ausnutzen und kombinieren und auf diese Art große Mengen an Passagierinformationen sammeln, die in einem zweiten Schritt mit Hilfe von Algorithmen analysiert und mit anderen Datenbanken abgeglichen werden. In Bezug auf eine Bewertung der (beabsichtigten oder unbeabsichtigten) ethischen Auswirkungen von risiko-basierten Passagierkontrollen muss die sich verändernde Praxis Informationsbeschaffung, -verarbeitung und -auswertung sorgfältig untersucht werden.

In seinen Überlegungen zu diesen Mechanismen bezeichnet Lyon (2006) Flughafensicherheit als Musterbeispiel für eine soziale Sortierung und identifiziert die bedenkliche Tendenz eines technokratischen Imperativs, nach dem verfügbare Sicherheitstechnologie ungeachtet ihrer Angemessenheit an Flughäfen zum Einsatz gebracht wird. Lyons Definition von zeitgenössischer Überwachung, die er als „routine and focused attention to personal details for the purpose of influence, management, care, and control“ (ebd.: 403) beschreibt, trifft den Kern des zu beobachtenden Paradigmenwechsels in der Luftfahrt und die Praktiken von risikobasierten Kontrollstrukturen. Wie Jones (2009: 98) anmerkt, fungierte die Sicherheitskontrolle am Flughafen bisher als eigenständige Maßnahme, wird aber nun verstärkt mit Informationstechnologie und datenbasierter Überwachung verknüpft. Um die komplementären, aber doch unterschiedlichen Dimensionen zu verdeutlichen, haben Byrne und Marx (2011) Sicherheitstechnologie idealtypisch in zwei Kategorien eingeteilt und unterscheiden dabei zwischen harten („hard“) und weichen („soft“) Technologien. Harte Technologien am

Flughafen, wie etwa Röntgengeräte, Metalldetektoren oder Körperscanner, beziehen sich auf eine sich bereits materialisierende Dimension der Bedrohung, also auf den Fall in dem bereits ein verbotener Gegenstand im Gepäck oder am Körper des Passagiers entdeckt wurde. In diesem Szenario liegt bereits in einer konkreten Situation ein Regelbruch vor und die Sicherheit ist manifest bedroht.

Die Einführung von Risiko als Beurteilungskategorie von Individuen bricht diese Kausalkette jedoch auf. Um die Praxis der situativen Kriminalprävention mit vorgelagerten elektronischen Entscheidungshilfen zu unterstützen, analysieren „weiche“ Sicherheitstechnologien wie Risikobewertungsalgorithmen den Passagier bereits im Vorfeld. Datengestützte Risikokalkulation ergänzt im Wesentlichen die materielle Dimension, also die Suche nach gefährlichen Gegenständen, mit Hinweisen darüber, wo das Screening intensiviert werden sollte und wo die Intensität zugunsten einer erhöhten Schnelligkeit und größerer Bequemlichkeit für die Passagiere reduziert werden kann.

Empirisch ist die Erhebung von Passagierinformationen bereits in einer Vielzahl von unterschiedlichen Formen zu finden – von Fluggastdatensätzen, zu deren Erstellung und Weitergabe die Fluggesellschaften abhängig vom Zielland des Flugs verpflichtet sind (etwa Passenger Name Record (PNR)- und Advance Passenger Information (API)-Dateien) über behördliche Gefährder-Listen (etwa die deutsche Antiterrordatei) und kommerzielle Ausschlusslisten der Airlines („no-fly lists“) bis hin zu „trusted traveler“ oder „registered passenger“ Konzepten, die häufig Mischformen der Kooperation von kommerziellen und staatlichen Akteuren darstellen und den Zugang zur Sicherheitskontrolle oder EinreiseprozEDUREN für zahlende Kunden erleichtern und beschleunigen. Im Gegensatz zu automatisierten und unsichtbaren (Bellanova/Duez 2012) Verfahren wie der Erstellung von Fluggastdatensätzen oder Ausschlusslisten, wählen „trusted traveler“ Programme einen anderen Ansatz. Die Datenerfassung geht hier offen sichtbar vonstatten und beruht auf freiwillig erteilten Angaben, einschließlich eingehender Background-Checks und biometrischer Daten, etwa zur Retina- oder Handvenenerkennung. Am Flughafen Schiphol in Amsterdam, einem der größten Drehkreuze für Flugreisen in Europa, können Vielflieger sich für eine jährliche Gebühr von 119 Euro im PRIVIUM-Programm registrieren lassen. Als Gegenleistung erhalten zahlende Kunden neben anderen Vergünstigungen auch die Möglichkeit, das Grenzkontrollverfahren zu beschleunigen, indem sie einen maschinellen Irisscan durchlaufen, anstatt sich anzustellen und einem Grenzbeamten ihren Personalausweis oder Reisepass vorzuzeigen.⁵ Gekoppelt an solche Verfahren sind oft auch andere Vergünstigungen, wie etwa der Zugang zu Lounges, ausgewiesene Parkplätze, oder die Benutzung einer exklusiven „fast lane“, die schnelleren Zugang zur Sicherheitskontrolle sicherstellt.

In Anlehnung an Foucault hat Salter (2007) die Praxis des informationellen Offenbarungseids am Flughafen als „confessionary complex“ bezeichnet, im Zuge dessen für die Berechtigung, den Sicherheitsbereich betreten zu dürfen, alle notwendigen Informationen preisgegeben werden – entweder durch freiwillige Angabe oder durch eine automatisierte Abfrage. Für die Luftfahrt bitten Konzepte wie „trusted traveler“ oder „registered passenger“ einen doppelten Vorteil. Neben der Kundenbindung und einer zusätzlichen Einnahmequelle geben Reisende eine ganze Bandbreite an Informationen freiwillig preis und können tragen auf diese Weise selbst zu einer besseren Fundierung von Risikobewertungsmechanismen bei. Lyon (2003) hat eine solche verstärkte Konvergenz von ehemals separaten privatwirtschaftlichen

⁵<http://www.schiphol.nl/Travellers/AtSchiphol/Privium/PriviumBenefits/FastBorderPassage.htm>

und sicherheitsbehördlichen Datenbanken in der Entwicklung der Flughafensicherheit nach den Anschlägen des 11. September 2001 prognostiziert, indem er moderne Flughäfen als „decentralized, rhizomic system of surveillance, in which travelers are constructed as manipulable entries in remote databases“ (ebd.: 15) beschreibt.

Bennett (2005, 2008) hat die durch den einfachen Kauf eines Flugtickets ausgelösten Kaskadeneffekte des Sammelns, Verarbeitens und Weitergebens von Passagierdaten analysiert. Dabei konzentriert er sich auf bilaterale PNR-Abkommen (siehe auch Bellanova/Duez 2012) und Flugverbotslisten und verweist darauf, dass Daten abhängig von kontextuellen Faktoren verarbeitet werden, welche das Land der Abreise, das Zielland und die Flugroute umfassen und die auch zwischen verschiedenen Flughäfen eines Landes variieren können. Die unterschiedlichen Verfahrensweisen hinsichtlich der Sammlung, Verarbeitung, Speicherung und Weitergabe von Informationen liegen dabei bis zu einem gewissen Grad auch in der starken Fragmentierung der Luftfahrt begründet. Bindende Vorschriften verschiedener internationaler Organisationen (IATA, ICAO⁶) ergänzen dabei nationale sowie supranationale europäische gesetzliche Regelungen (Barros 2012). Darüber hinaus bestehen zwischen zahlreichen Ländern besagte bilaterale Vereinbarungen über die Weitergabe von Daten.

Zur unübersichtlichen rechtlichen Situation kommt hinzu, dass Flughäfen als die eigentlichen Orte der Sicherheitskontrolle häufig hybride Konstrukte sind, die aus einer Vielzahl von privaten Unternehmen und staatlichen Behörden bestehen, die teilweise kooperieren, teilweise aber auch Verantwortung durch Outsourcing an dritte Parteien weitergeben, im Falle der für die Sicherheitskontrollen verantwortlichen Bundespolizei etwa an private Sicherheitsfirmen (Lippert/O'Connor 2003; O'Malley 2006; Salter 2008b). Empirisch gesehen sind also bereits heute Praktiken der Erhebung und Verarbeitung von Passagierdaten festzustellen, die allerdings eine erhebliche Bandbreite an Variationen aufweisen. Ist die Einführung von risikobasierten Passagierkontrollen, wie von IATA und ACI/AEA vorgeschlagen, also die logische Konsequenz eines langfristigen Trends (Lyon 2006), beziehungsweise die Institutionalisierung von Praktiken, die bereits heute angewendet werden (O'Malley 2006)? Und welche Konsequenzen ergeben sich dadurch für eine ethische Bewertung der aktuellen Entwicklungen?

3 Risiko vs. Ethik?

Im Umgang mit Risikobewertungsmechanismen und ihren ethischen Implikationen muss die Analyse mit dem Begriff des Risikos in sozialen Kontexten beginnen. Bedingt durch ihren Ursprung in der Statistik und der Technik (Zedner 2006: 424) sieht sich die Risikobewertung mit erheblichen Hürden konfrontiert, wenn nicht genügend Informationen für eine robuste Kalkulation vorhanden sind. Dies wird im Hinblick auf menschliches Verhalten schwerlich jemals der Fall sein. Da das Grundprinzip von Risikobewertung auf die Zukunft ausgerichtet ist und im Fall von Sicherheitskontrollen anstrebt, die Absichten von Individuen auf der Grundlage von Informationen über die Vergangenheit einzuschätzen, kann letztlich immer nur eine probabilistische Aussage getroffen werden. Die Berechnung von Risikokategorien kann also keine gesicherte Vorhersage über die tatsächliche Gefährdung geben, die von einem Passagier ausgeht. Im Falle einer solchen Fehleinschätzung („false positive“) kann dies zu einer diskriminierendem Aussortierung von Individuen aus dem Passagierstroms führen,

⁶International Civil Aviation Organization (Internationale zivile Luftfahrtsorganisation).

basierend nur auf einer Aussage über eine von multiplen möglichen Zukunften. So muss jemand, der sich vollkommen harmlos verhält, invasivere Kontrollverfahren erdulden als andere und wird möglicherweise sogar zusätzlich durch Sicherheitskräfte befragt. Und das obwohl sich der Reisende keines manifesten Vergehens, keines abweichenden Verhaltens oder gar einer kriminellen oder terroristischen Handlung schuldig gemacht hat. Die bloße Vermutbarkeit eines abweichenden Verhaltens des Reisenden aufgrund von Risikofaktoren wird zur Legitimation für eine Ungleichbehandlung. Die Abwendung von situativer Kriminalprävention und die Hinwendung zur Zukunft führt zu „construction, interpretation and management of contingency“ (Aradau et al. 2008: 148) – Sicherheitskonzepte gehen nunmehr davon aus, ständig den schlimmsten Fall anzunehmen, ihn zu konstruieren und zu simulieren und sich dann entsprechend darauf vorzubereiten.

In diesem Zusammenhang ist auch die Fokussierung auf Passagierinformationen zu sehen. Da alle Passagiere zu potentiellen Attentätern werden, kann sich das Individuum nur durch (die richtigen) Informationen von dem Verdacht reinwaschen, Böses im Schilde zu führen. Die datengestützte Sicherheitskontrolle nutzt nicht länger die disziplinierenden und normalisierenden Eigenschaften von Benthams (1995) Konzept des Panoptikums – stattdessen wird der Passagierstrom nach bestimmten Charakteristika zu sortieren. Sicherheit wandelt sich vom Panoptikum zum „ban-opticon“ (Bigo 2002), das über statistische Verfahren die unerwünschten Elemente von den erwünschten abtrennt, „using known data to theorise the unknown“ (Adey 2009: 278). Was an der Grenzkontrolle der illegale Migrant ist, wird im Fall der Sicherheitskontrolle am Flughafen derjenige, dessen Datenprofil dem ähnelt, was als gefährlich konstruiert wird. Der wesentliche Punkt bei einer Ungleichbehandlung auf der Grundlage von antizipatorischen Szenarien liegt also in der Etablierung eines plausiblen Narrativs der negativen Absichten des Hochrisiko-Passagiers. Ein solches Szenario wird jedoch letztlich in der Regel einen Fall prognostizieren, der noch nie aufgetreten ist, und dem Passagier ein Verhalten unterstellen, das die Person noch nie zuvor praktiziert hat (Curry 2004). In Bezug auf eine „Ethik der Sicherheitskontrolle“ werfen die aufgezeigten Entwicklungen in zweierlei Hinsicht Bedenken auf: (1) Die Kriterien, die für die Konstruktion der Risikoprofile und damit für die Etablierung von Zukunften angelegt werden, sind nicht transparent, was im Fall von Diskriminierung dafür sorgen kann, dass diese überhaupt nicht bemerkt wird, oder nicht nachgewiesen werden kann. (2) Wie bereits weiter oben verdeutlicht, kann je nach Konstruktionsart der Risikoprofile eine Reproduktion sozialer und ökonomischer Ungleichheiten auftreten, die sich in der Intensität der Kontrollmaßnahmen niederschlägt. Wer zahlt, erfährt eine angenehmere Behandlung. Wer nicht zahlen kann oder will, wird eher invasivere Kontrollmaßnahmen durchlaufen.

An der Sicherheitskontrolle prallen also behördliche Anforderungen und ethische Argumente aufeinander, gepaart mit wirtschaftlichen Zwänge einer Branche, die zunehmend mit geringeren Gewinnmargen zu kämpfen hat, aber gleichzeitig eine große Bedeutung für nationale und internationale Sicherheit aufweist. Sicherheitsbehörden und Nachrichtendienste können ihre operativen Kriterien im Kampf gegen den Terrorismus nicht öffentlich machen, und das gilt natürlich auch für die Sicherheitskontrolle am Flughafen, die nach §5 des deutschen Luftsicherheitsgesetzes der Bundespolizei untersteht. Aus Sicht der Sicherheitsbehörden bietet die Einführung von Risiko sogar einen doppelten Vorteil. Nicht nur wird durch die Fokussierung auf Passagierinformationen der unbekannte Fremde in ein zumindest teilweise bekanntes Datenprofil codiert, sondern durch die Risikokategorisierung wird die Sicherheitskontrolle selbst in den Bereich der Kontingenz gerückt. Der potentielle

Terrorist weiß nun nicht mehr, welche Sicherheitsmaßnahmen ihn erwarten – die Kontrolle ist ihrerseits dynamisch geworden durch zu- und abschaltbare Sensoren. Der Grundsatz „terrorists are in the business of uncertainty“ (Ericson 2006: 347) wird so ins Gegenteil verkehrt, stattdessen verkörpert nun der Checkpoint selbst Ungewissheit. Das Umdrehen der Kräfteverhältnisse in einem asymmetrischen Konflikt und damit die letztlich die Bekämpfung von Kontingenz mithilfe von Kontingenz (Adey 2009: 289) ist es, was Risiko als Sicherheitskonzept so attraktiv macht. Auf der anderen Seite bedeuten die Entwicklungen aber auch, dass sich die Lücke zwischen situativer Kriminalprävention und einer lückenlosen Überwachung und Protokollierung des Individuums am Flughafen unweigerlich schließt.

Diskriminierende Effekte von Risiko müssen nicht zwangsläufig beabsichtigt sein, sondern können als unbeabsichtigte Nebenfolgen auftreten. Risikokategorien neigen dazu, soziale, ökonomische und politische Kategorien zu reproduzieren und Passagierströme stereotypisch zu sortieren, etwa in Bezug auf „den Anderen“, „den Ausländer“, „den Verzweifelten“ oder „den Armen“ (Pallitto/Heyman 2008: 321). Ungleichheiten auf der Grundlage von Charakteristika wie Klassenzugehörigkeit, Nationalität, Ethnie, Geschlecht oder Religion können sich leicht auf Mechanismen der Risikobewertung übertragen. Kausale Unterstellung dieser Art können dabei bereits im Bereich von Forschung und Entwicklung zu finden sein, da Entwickler Bewertungsalgorithmen auf explizite Annahmen bezüglich des Verhältnisses zwischen Risiko und verfügbaren Informationen über den Passagier stützen müssen. Lyon (2006: 406) weist in diesem Zusammenhang darauf hin, dass auch die Sicherheitsindustrie verstärkt in den Fokus gerückt werden sollte. Und auch die mathematische Kalkulation von Risikoprofilen selbst kann „profilierende“ Wirkung entfalten (de Vries 2010).

Um daher Verletzungen von Gerechtigkeits- und Gleichbehandlungsprinzipien zu vermeiden, müssten theoretisch Details zu den verarbeiteten Informationen und zu den Kriterien für die Risikobewertung und die Konstruktion von Profilen offengelegt werden. In Bezug auf die private Wirtschaft hat Gandy (1993) den Begriff „panoptic sorting“ verwendet um zu verdeutlichen, wie Konzerne versuchen zu Marketingzwecken mittels „data-mining“ ein möglichst umfassendes Bild von Konsumenten zu erlangen. Risikobasierte Kontrollmechanismen zielen vordergründig nicht darauf ab, finanzielle Vorteile aus Passagierdaten zu ziehen, sondern auf eine Maximierung des Sicherheitsniveaus. Andererseits ist die Trennung zwischen Sicherheitsbehörden und Privatwirtschaft innerhalb der Luftfahrt verschwommen. Aus ethischer Perspektive werfen insbesondere die Möglichkeiten zu einem „opt-in“ Bedenken auf. „Trusted traveler“ oder „registered passenger“ Programme sind vornehmlich der wohlhabenden globalen Elite vorbehalten und können dazu führen, dass selbst bei einem Screeningansatz, der authentisch auf Risikokriterien beruhen sollte, es in Wirklichkeit sehr wohl die Kreditkarte sein kann, welche den Zugang zur Kategorie mit dem niedrigeren Risiko gewährt. Die Mobilität der Elite sollte möglichst nicht eingeschränkt werden, oder anders gesprochen: „risk profile corresponds to income profile“ (Pallitto/Heyman 2008: 324).

4 Schlussbemerkung

Betrachtet man die allgemeinen Tendenzen in der Ausgestaltung von Sicherheitsmaßnahmen, passen sich die jüngsten Entwicklungen in der Luftfahrt nahtlos in das Bild ein. Risikobasierte Modelle für die Passagierkontrolle können als ein weiterer Schritt hin zur Etablierung von präemptiven und antizipatorischen Strukturen gesehen werden, die sich in zunehmendem Umfang auf Datenverarbeitung und Informationsgewinnung stützen. Diese Entwicklung wird auch im europäischen Kontext deutlich, wo im Zuge des Stockholm-Programms ein stärkerer Informationsaustausch zwischen Behörden und die verbesserte Verknüpfung von Datenbanken gefördert wird (Bellanova/Duez 2012). Insbesondere in Transitinfrastrukturen wie dem Flughafen scheint das Sammeln von Passagierinformationen als Weg vorherbestimmt zu sein, um Identitäten digital zu codieren und zu verarbeiten. Risiko übersetzt Passagiere „into regimes of identification and authentication – through profiles, screens, anticipations and rules“ (Adey et al. 2012: 173). Nichtsdestotrotz scheinen Bürger eher gewillt zu sein, Einschränkungen in Fragen von Gerechtigkeit und Privatsphäre in einem Umfeld zu akzeptieren, das so einschüchternd und disziplinierend (Lyon 2006) wirkt wie der Flughafen. Viele Reisende sind sogar bereit, „false positives“ oder eine Zuweisung zu höheren Risikokategorien als notwendig zu akzeptieren. Modelle wie der "Checkpoint of the Future" der IATA und "Better Security" von ACI/AEA haben zur Folge, dass die (ohne schon minimale) Lücke zwischen situativer Kriminalprävention und einem umfassenden Überwachungsapparat weiter geschlossen wird. Das Konzept einer „surveillant assemblage“ (Haggerty/Ericson 2000) aufgreifend, werden risikobasierte Sicherheitsmaßnahmen für Kontrollpunkte angetrieben von dem Bestreben nach vertiefter Integration von Datenquellen, oder wie es Haggerty und Ericson (ebd.: 610) formulieren: „to bring systems together, to combine practices and technologies and integrate them into a larger whole“.

Die Konvergenz von Kommerz und nationaler Sicherheit (Lyon 2003, 13) wirft dabei erhebliche Bedenken auf hinsichtlich einer schleichenden Aufweichung der Zweckbestimmung der Passagierinformationen sowie der teilweise undurchschaubaren Strukturen der Datenerhebung (Bellanova/Duez 2012). Die Möglichkeit für den Passagier, auf die eigenen Daten zuzugreifen zwecks deren Prüfung, Aktualisierung und Korrektur, ist in diesem Kontext als nicht sehr wahrscheinlich einzustufen (Lyon 2003: 17). Wie Aradau und Van Munster (2007: 104) anmerken, liegt dies in der undurchsichtigen operativen Kriterien von Sicherheitsbehörden begründet, die die ausschlaggebenden Faktoren und deren Gewichtung nicht öffentlich zugänglich machen (können). Mit der Implementierung von Risiko als Kernprinzip in modernen Sicherheitsarchitekturen werden Kontrollmaßnahmen zunehmend als unvorhersehbar und dynamisch konzipiert (Adey 2009: 289). Aus funktioneller Sicht trägt dies maßgeblich zu einer gesteigerten Effizienz der Passagierkontrolle bei, und kann als Nebeneffekt sogar zur Identifizierung und Festnahme von anderweitig gesuchten, „regulären“ Straftätern führen, wie Adey etwas zynisch anmerkt (ebd.: 291).

Aus ethischer Sicht beeinträchtigen risikobasierte Kontrollverfahren Passagiere allerdings sowohl in ihren Bürgerrechten als auch in ihrer individuellen Reisegeschwindigkeit. Eine Unterscheidung zwischen privilegierten Reisenden (niedriges Risiko, viele Rechte, rasche Geschwindigkeit) und nicht privilegierten Reisenden (hohes Risiko, wenig Rechte, langsame Geschwindigkeit) (Pallitto/Heyman 2008: 316) spiegelt soziale Ungleichheiten und gesellschaftliche Statusunterschiede wider und untergräbt die Prinzipien von Gerechtigkeit und Gleichbehandlung. Wie Salter (2008a) anmerkt, kann durch die Fokussierung auf Risi-

ken und die damit zusammenhängende Hinwendung zu quantitativen und probabilistischen Verfahren zwar dazu beitragen, einige der prägenden Konflikte der Luftfahrt (Geschwindigkeit, Sicherheit, Komfort) zu entschärfen – allerdings wird das Spannungsfeld dadurch nur verlagert. Im Hinblick auf ethische Kriterien läuft risikobasiertes Screening Gefahr, Benachteiligungen zu reproduzieren und Individuen oder Gruppen strukturell invasiveren und unangenehmeren Kontrollen auszusetzen. In diesem Sinne wird ein neuer Konflikt konstruiert, bei dem sich Risiko und Ethik am Flughafen in gewisser Weise diametral entgegenstehen. Oder, wie Ericson (2006: 355) warnt: „frantic efforts at risk management in the name of precaution can tear at the social fabric“.

Literatur

- ACI/AEA (2011): Better Security. Association of European Airlines/Airports Council International Joint Briefing – Aviation Security: 10 years from 9/11. http://files.aea.be/News/Joint_ACI_AEA.pdf
- Adey, Peter (2006): "Divided we Move": The Dromologies of Airport Security and Surveillance. In: Monahan, Torin (Hrsg.): Surveillance and Security. Technological Politics and Power in Everyday Life. New York/London: Routledge
- Adey, Peter (2008): Airports, Mobility and the Calculative Architecture of Affective Control. In: Geoforum 39 (1), S. 438–451
- Adey, Peter (2009): Facing Airport Security: Affect, Biopolitics, and the Preemptive Securitisation of the Mobile Body. In: Environment and Planning D: Society and Space 27 (2), S. 274–295
- Adey, Peter/Bissell, David/McCormack, Derek/Merriman, Peter (2012): Profiling the Passenger: Mobilities, Identities, Embodiments. In: Cultural Geographies 19 (2), S. 169–193
- Aradau, Claudia/Lobo-Guerrero, Luis/van Munster, Rens (2008): Security, Technologies of Risk, and the Political: Guest Editors' Introduction. In: Security Dialogue 39 (2-3), S. 147–154
- Aradau, Claudia/van Munster, Rens (2007): Governing Terrorism Through Risk: Taking Precautions, (un)Knowing the Future. In: European Journal of International Relations 13 (1), S. 89–115
- Augé, Marc (2006): Non-places: Introduction to an Anthropology of Supermodernity. London: Verso
- Barnett, Arnold (2004): CAPPS II: The Foundation of Aviation Security? In: Risk Analysis 24 (4), S. 909–916
- Barros, Xiana (2012): EU Counterterrorism and Aviation Security: Supranational Rules but Intergovernmental Politics? In: European Foreign Affairs Review 17 (1-2), S. 53–69
- Bauman, Zygmunt (2003): Liquid Love. On the Frailty of Human Bonds. Cambridge: Polity Press
- Bellanova, Rocco/Duez, Denis (2012): A Different View on the 'Making' of European Security: The EU Passenger Name Record System as a Socio-Technical Assemblage. In: European Foreign Affairs Review 17 (1-2), S. 109–124
- Bennett, Colin J. (2005): What Happens When You Book an Airline Ticket? The Collection and Processing of Passenger Data Post-9/11. In: Zureik, Elia/Salter, Mark B. (Hrsg.): Global Surveillance and Policing. Borders, Security, Identity. Cullompton/Portland: Willan
- Bennett, Colin J. (2008): Unsafe at Any Altitude. The Comparative Politics of No-Fly Lists in the United States and Canada. In: Salter, Mark B. (Hrsg.): Politics at the Airport. Minneapolis/London: University of Minnesota Press
- Bentham, Jeremy (1995): Panopticon. In: Božovič, Miran (Hrsg.): The Panopticon Writings. London: Verso
- Bigo, Didier (2002): Security and Immigration: Toward a Critique of the Governmentality of Unease. In: Alternatives: Global, Local, Political 27 (1), S. 63–92

- Byrne, und Gary T. Marx, James (2011): Technological Innovations in Crime Prevention and Policing. A Review of the Research on Implementation and Impact. In: de Pauw, Evelien/Ponsaers, Paul/van der Vijver, Kees/Bruggeman, Willy/Deelman, Piet (Hrsg.): *Technology-led Policing*. Antwerpen/Apeldoorn/Portland: Maklu
- Curry, Michael R. (2004): The Profiler's Question and the Treacherous Traveler: Narratives of Belonging in Commercial Aviation. In: *Surveillance & Society* 1 (4), S. 475–499
- de Vries, Katja (2010): Identity, Profiling Algorithms and a World of Ambient Intelligence. In: *Ethics and Information Technology* 12 (1), S. 71–85
- Ericson, Richard V. (2006): Ten Uncertainties of Risk-Management Approaches to Security. In: *Canadian Journal of Criminology and Criminal Justice* 48 (3), S. 345–357
- Fuller, Gillian/Harley, Ross (2004): *Aviopolis. A Book about Airports*. London: Black Dog
- Gandy, Oscar H. (1993): *The Panoptic Sort: A Political Economy of Personal Information*. Boulder: Westview
- Haggerty, Kevin D./Ericson, Richard V. (2000): The Surveillant Assemblage. In: *British Journal of Sociology* 51 (4), S. 605–622
- Jones, Richard (2009): Checkpoint Security. Gateways, Airports and the Architecture of Security. In: Katja Franko Aas/Gundhus, Helene Oppen/Lomell, Heidi Mork (Hrsg.): *Technologies of InSecurity. The Surveillance of Everyday Life*. London: Routledge-Cavendish
- Lahav, Gallya/Guiraudon, Virginie (2000): Comparative Perspectives on Border Control: Away from the Border and outside the State. In: Andreas, Peter/Snyder, Timothy (Hrsg.): *The Wall Around the West. State Borders and Immigration Controls in North America and Europe*. Lanham: Rowman & Littlefield
- Leese, Matthias (2013): The Perceived Threat. Determinants and Consequences of Fear of Terrorism in Germany. In: Flammini, Francesco/Setola, Roberto/Franceschetti, Giorgio (Hrsg.): *Effective Surveillance for Homeland Security: Balancing Technology and Social Issues*. London: Chapman and Hall
- Lippert, Randy/O'Connor, Daniel (2003): Security Assemblages: Airport Security, Flexible Work, and Liberal Governance. In: *Alternatives: Global, Local, Political* 28 (3), S. 331–358
- Lüdemann, Christian/Schlepper, Christina (2010): „Willingness to Pay for Security“ bei Passagierkontrollen am Flughafen - Zu den individuellen Kosten öffentlicher Sicherheit. In: *Soziale Probleme* 21 (1), S. 117–135
- Lyon, David (2003): Airports as Data Filters: Converging Surveillance Systems after September 11th. In: *Journal of Information, Communication and Ethics in Society* 1 (1), S. 13–20
- Lyon, David (2006): Airport Screening, Surveillance, and Social Sorting: Canadian Responses to 9/11 in Context. In: *Canadian Journal of Criminology and Criminal Justice* 48 (3), S. 397–411
- O'Malley, Pat (2006): Risks, Ethics, and Airport Security. In: *Canadian Journal of Criminology and Criminal Justice* 48 (3), S. 413–421
- Pallitto, Robert/Heyman, Josiah (2008): Theorizing Cross-Border Mobility: Surveillance, Security and Identity. In: *Surveillance & Society* 5 (3), S. 315–333
- Salter, Mark B. (2007): Governmentalities of an Airport: Heterotopia and Confession. In: *International Political Sociology* 1 (1), S. 49–66
- Salter, Mark B. (2008a): Imagining Numbers: Risk, Quantification, and Aviation Security. In: *Security Dialogue* 39 ((2-3)), S. 243–266
- Salter, Mark B. (2008b): Introduction: Airport Assemblage. In: Salter, Mark B. (Hrsg.): *Politics at the Airport*. Minneapolis/London: University of Minnesota Press
- Sweet, Kathleen M. (2009): *Aviation and Airport Security. Terrorism and Safety Concerns*. Boca Raton/London/New York:: CRC Press
- Urry, John (2007): *Mobilities*. Cambridge: Polity Press
- Zedner, Lucia (2006): Neither Safe Nor Sound? The Perils and Possibilities of Risk. In: *Canadian Journal of Criminology and Criminal Justice* 48 (3), S. 423–434

Zitierweise:

Matthias Leese: Effektiv aber ungerecht? – Eine ethische Perspektive auf risikobasierte Sicherheitsstrukturen an Flughäfen; in: Wagner, Katrin/Bonß, Wolfgang: *Risikobasiert versus One Size Fits All - Neue Konzepte der Passagierüberprüfung im Luftverkehr*, Neubiberg 2014: Universitätsverlag, S. 45-55.