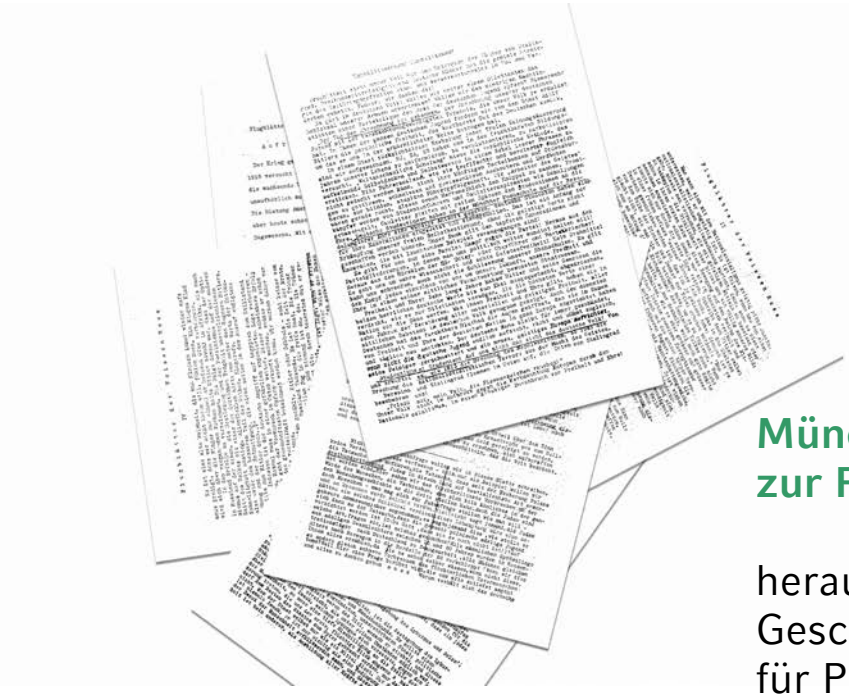
LMU LUDWIG-MAXIMILIANS-UNIVERSITÄT MÜNCHEN

GESCHWISTER-SCHOLL-INSTITUT
FÜR POLITIKWISSENSCHAFT



Münchener Beiträge zur Politikwissenschaft

herausgegeben vom
Geschwister-Scholl-Institut
für Politikwissenschaft

2015

Sina Beckstein

Die Wahrnehmung von Anti-Terror-Maßnahmen in der Europäischen Union. Versicherheitlichungsprozesse im Instrument der Fluggastdaten in interner und externer Dimension

Bachelorarbeit bei
Dr. Alexander Spencer
SoSe 2015

1 Einleitung

Die transnationale Natur des Terrorismus ist ein Fakt der europäischen und internationalen Debatte um den Kampf gegen den Terrorismus geworden. So heißt es in der aktuellsten Sicherheitsagenda der Europäischen Union (Kommission 2015a: 2): „Die Bedrohungen werden immer vielfältiger und internationaler und sind zunehmend grenz- und bereichsübergreifender Natur.“. Diese Aussage impliziert, dass Bedrohungen nicht mehr als ausschließlich von ‚innen‘ (intern) oder von ‚außen‘ (extern) stammen, sondern dass in ihrer Natur liegt, dass sie überall auftreten können (vgl. Jackson 2007: 237; Monar 2007: 298). Im politischen Diskurs äußert sich dies wie folgt: „Sicherheitsbedrohungen machen nicht an den Grenzen der EU halt. Die innere Sicherheit der EU und die globale Sicherheit bedingen einander und sind miteinander verknüpft.“ (Kommission 2015a: 6)

Die Wahrnehmung und Äußerung der terroristischen Bedrohung als ‚transnational‘ ist von politischer Relevanz, da sie bestimmte Maßnahmen vor anderen vorrangig erscheinen lässt. Der Schutz der europäischen Union an ihren Außengrenzen ist beispielsweise seit des Erstarken des Islamischen Staates und der damit verbundenen Debatte um die (Rück-)Einreise von sogenannten ‚ausländischen Kämpfern‘ erneut ein zentrales Anliegen der Union geworden (vgl. Rat 2015). Wie Transnationalität impliziert, ist nicht nur die externe Dimension von Interesse, sondern auch der Grenzschutz einzelner Staaten innerhalb des europäischen Systems. Durch das Schengen-Abkommen und die damit verbundene Abschaffung sämtlicher Kontrollen an den Grenzen, ist die Bewegungsfreiheit eines jeden einzelnen Europäers im Schengen-Raum garantiert – ungeachtet dessen, ob dieser sich zum radikalen Islamisten hat ausbilden lassen oder nicht. Der Rat der EU formulierte dies in der EU-Strategie der Terrorismusbekämpfung von 2005 wie folgt:

> Die Europäische Union ist ein Raum wachsender Offenheit, in dem die inneren und äußeren Aspekte der Sicherheit eng miteinander verknüpft sind. Sie ist ein Raum immer stärker werdender Verflechtungen, der die Freizügigkeit von Menschen, Ideen, Technologie und Ressourcen ermöglicht. Terroristen missbrauchen ein solches Umfeld, um ihre Ziele zu verfolgen. (Rat 2005: 6)

Dieser ‚Unsicherheit‘ im europäischen Umfeld möchte die EU mit dem Austausch von personenbezogenen Daten entgegenwirken – bestehende Instrumente dafür sind das das Schengener Informationssystem (SIS), das Schengener Informationssystem der zweiten Generation (SIS II) sowie das Visa-Informationssystem (VIS) (vgl. Kommission 2011a: 3).

Die Instrumente zur Sicherung der europäischen Bürgerinnen und Bürger, Normen und Werte heißen demnach Informationserhebung, -speicherung und –austausch und betreffen zunehmend die Überschreitung von nationalen Grenzen.

Neben den bestehenden Instrumenten sind auch neue Maßnahmen geplant. Diese umfassen ein Einreise-Ausreise-System (EES) sowie die Erfassung und Speicherung von Fluggastdaten (Passenger-Name-Record, PNR). Mit PNR-Daten können Reisemuster, Buchungsdetails (unter anderem Kreditkartendetails) und andere Informationen von Passagieren kategorisch erfasst und zur Auswertung an betraute Institutionen weitergeleitet werden. PNR-Daten stellen als Instrument des Informationsmanagements im Bereich von Grenzübertritten einen besonderen Fall dar, da über diese postuliert wird, sie würden „hauptsächlich zur polizeilichen Erkenntnisgewinnung und w e n i g e r für Grenzkontrollzwecke verwendet. […] [Sie] dienen weniger der Bekämpfung von irregulärer Einwanderung und der Erleichterung der Grenzkontrollen als vielmehr der Bekämpfung von Terrorismus und schwerer Kriminalität." (Hervorhebung i.O.; eigene Einfügung; Kommission 2011a: 9)

Bei der Diskussion um die Erhebung von Fluggastdaten an den Außengrenzen der EU (EU-PNR) handelt es sich um kein Novum – ein Vorschlag über einen Rahmenbeschluss für interne Passagierdaten gab es bereits 2007 und vergleichbare bilaterale Abkommen bestehen mit den USA, Australien und Kanada.

Die Datenerhebung und -auswertung betrifft dabei nicht nur ‚verdächtige' Bürgerinnen und Bürger oder gar solche, die auf Anti-Terror-Listen erfasst worden sind, sondern es werden die Daten jedes Europäers genutzt, der in die USA, Australien oder Kanada fliegt und möglicherweise bald auch von jeder Person, die in die europäische Union ein- oder ausreist.

Intuitiv bedeutet das, dass jede Person, die sich als Flugreisende/r aus der europäischen Union heraus oder in die EU hinein bzw. ins Ausland bewegt, eine potentielle Sicherheitsbedrohung darstellt. Die Rolle der Grenzen an sich ist also veränderbar - Kontrollen an den Außengrenzen tragen nicht mehr nur zur Verhinderung von illegaler Migration, sondern zur Bekämpfung des Terrorismus als transnationales Phänomen bei.

Dies geschieht direkt durch Instrumente bzw. Maßnahmen der Terrorabwehr. So fand beispielsweise Brouwer (2006: 138) heraus, dass durch die Zweckveränderung der europäischen Instrumente SIS II, VIS und Eurodac, Grenz- und Immigrationskontrollen direkt mit der inneren Sicherheit und dem Kampf gegen den Terrorismus verlinkt werden. Migration als Entität wurde durch diese Prozesse also in eine wahrgenommene Sicherheitsbedrohung transformiert.

Das Bild des Terrorismus, d.h. wer oder was eine terroristische Bedrohung darstellt und wie darauf reagiert werden soll, ist folglich ein konstruiertes, veränderbares Gebilde, das sich durch bestimmte Agenten, Handlungen und Kontexte in der Bevölkerung manifestieren kann (vgl. Balzacq 2011: 35-38).

In diesem Bereich der Terrorbekämpfung betreffen PNR-Daten den Schutz des Luftverkehrs. Der oder die Flugreisende ist dadurch kein neutral besetzter Begriff mehr – Flugreisende und der gesamte Luftverkehr können durch die Legitimierung von PNR-Daten zu einer Sicherheitsbedrohung werden, da eine terroristische Intention nicht ausgeschlossen werden kann.

In der vorliegenden Arbeit wird gezeigt, dass die geäußerte Zweckausrichtung - nämlich die alleinige Bekämpfung des Terrorismus - nicht den Prozessen entspricht, die tatsächlich durch das PNR-Instrument impliziert werden. Vielmehr sind Passagierdaten ein versicherheitlichendes Instrument. Durch das Instrument selbst werden bestimmte Entitäten unter dem Deckmantel der Terrorismusbekämpfung auf verschiedene Art und Weise in einen Sicherheitskontext gerückt, d.h. sie werden in eine Sicherheitsbedrohung transformiert.

Einerseits zeigen sich diese Prozesse implizit in der Natur und den Funktionen des Instruments bzw. in deren Dynamik, andererseits explizit (d.h. geäußert) in Vorschlägen und Abkommen zu PNR-Daten.

Die Forschungsfrage leitet sich aus diesem Vorhaben ab und lautet folglich:

Wie zeigen sich Versicherheitlichungsprozesse im Instrument der Fluggastdaten (PNR) und wie reflektiert dieses direkt und indirekt bestimmte Bedrohungswahrnehmungen?

Im Sinne des Konstruktivismus entwickelten verschiedene Autoren eine Theorie der Internationalen Beziehungen, die sich genau mit der Transformation von Entitäten in einen Sicherheitsbereich befasst. Die ‚Securitization'[1] bzw. Versicherheitlichungstheorie verfolgt dabei unterschiedliche Ansätze zur Untersuchung dieser Problematiken, wovon in dieser Arbeit der soziologische Ansatz mit einem speziellen Fokus auf der Untersuchung einzelner Instrumente (Instrumente-Ansatz) nach Thierry Balzacq gewählt wurde (zu den Gründen der Auswahl dieses Ansatzes vgl. Kapitel 2.2.2).

Im Bereich der Erforschung von Instrumenten setzten sich einige Autoren intensiv mit der Klassifizierung und Typologisierung von Policy-Instrumenten auseinander (vgl. z.B. Schneider und Ingram 1990; Vedung 1998; Salamon 2002) während sich andere Autoren mit deren Auswahl beschäftigten (vgl. z.B. Peters 2002). Ein weiterer Forschungsbereich beschäftigt sich mit der Evaluation der Effektivität von Terrorismusbekämpfung als Policy (vgl. z. B. Lum et al. 2006; Hayes und Jones 2015) oder einzelner Maßnahmen (vgl. z. B: Bures 2006; Chistyakova 2015).

[1] ‚Securitization' wird als bestehender politikwissenschaftlicher Begriff mit ‚Versicherheitlichung' gleichgesetzt. Alle direkten und indirekten Zitate (ausgenommen von Definitionen) wurden von der Autorin aus Gründen der besseren Lesbarkeit ins Deutsche übersetzt.

Die Untersuchungen des PNR-Instruments beziehen sich zum Großteil auf den Datenschutz bzw. die Verletzung von Grundrechten (vgl. z. B. Guild und Brouwer 2006; Hailbronner et al. 2008; Brouwer 2009; Pawlak 2009; Nino 2010; Boehm 2010; Hornung und Boehm 2012; Bigo et al. 2015), sowie auf die Einflussnahme von externen Akteure auf die Ausgestaltung des (EU) Instruments (vgl. z. B. Pawlak 2009; Hobbing 2010; Kaunert et al. 2012).
Mit der Untersuchung von Versicherheitlichungsprozessen durch bestimmte Instrumente beschäftigten sich vergleichsweise wenige Autoren (vgl. z. B. Balzacq 2008), weswegen solch eine Analyse hinsichtlich PNR-Daten relevant für den Forschungsbereich ist.

Im ersten theoretischen Teil der Forschungsarbeit werden die unterschiedlichen Ansätze zur Untersuchung von Versicherheitlichung, sowie ihre Differenzen genauer beleuchtet (Kapitel 2), was eine Literaturübersicht zu diesem Thema impliziert. Nach dieser generellen thematischen Übersicht wird der in dieser Arbeit verwendete ‚Tool'-bzw. Instrumente-Ansatz im Detail dargestellt (2.2.2). Insbesondere wird herausgearbeitet, warum der Fokus auf die Substanz von Instrumenten für Studien zur Versicherheitlichung sinnvoll sein kann.
Im zweiten empirischen Teil (Kapitel 3) werden daraufhin Fluggastdaten (PNR) als ausgewähltes Instrument der Terrorismusbekämpfung sowohl in der europäischen, internen Dimension (3.2), als auch in ihrer externer Dimension (3.3) anhand des Fallbeispiels von Abkommen zwischen der Europäischen Union und den Vereinigten Staaten von Amerika (USA) untersucht. Der Fokus der Untersuchung liegt auf den Eigenschaften des PNR-Instruments, was auch seine Veränderung in unterschiedlichen Vorschlägen und Abkommen der EU beinhaltet. In beiden Dimensionen werden, aufbauend auf der Natur und den Funktionen des PNR-Instruments, letztendlich die Prozesse dargestellt, die das Instrument der Fluggastdaten zu einem versicherheitlichenden Instrument werden lassen (3.2.5, 3.3.5).
Im abschließenden Kapitel (Kapitel 4) wird die Forschungsfrage zusammenfassend beantwortet.

2 Theoretisches Konzept: Theorie der Versicherheitlichung (Securitization)

2.1 Philosophischer Ansatz (Kopenhagener Schule)

Die am meisten verbreitete Securitization-Theorie geht davon aus, dass Bedrohungen durch Sprache in einem Diskurs konstruiert werden. Dieser Theoriestrang wurde maßgeblich von der sogenannten Kopenhagener Schule entwickelt und kann als Teil der Sprachphilosophie als *philosophischer Ansatz* (vgl. Balzacq 2010a: 60) bezeichnet werden. Die Prämissen des

Sprachaktmodells wurden vor allem von Barry Buzan, Ole Waever und Jaap de Wilde (1998) vertreten und entwickelt.

Das Sprachaktmodell folgt der Annahme, dass keine Problematik von Natur aus eine Bedrohung sei, sondern erst durch den Diskurs zu einem Sicherheitsproblem werde (vgl. Balzacq 2011:1). Nur durch sogenannte ‚Sprachakte' kann Sicherheit konstruiert werden (vgl. Buzan et al. 1998: 26). Der Tradition des Poststrukturalismus folgend, postulieren die Vertreter eine ‚magische' Kraft der Sprache (vgl. Balzacq 2011: 1). Dabei ist unwichtig, ob bestimmte Aussagen die gegebene Realität abbilden (Buzan et al. 1998: 26):

> 'Security' is thus a self-referential practice, because it is in this practice that the issue becomes a security issue – not necessarily because a real existential threat exists but because the issue is presented as such a threat. (Buzan et al. 1998: 24)

Äußerungen selbst sind also Handlungen (vgl. Buzan et al. 1998: 26). Sie sind Performative und können daher (im Gegensatz zu Konstativen) nicht als wahr oder falsch beurteilt werden (vgl. Balzacq 2011: 1). Im Sicherheitsdiskurs würden Problematiken dramatisiert und als höchste Priorität eingestuft werden. Bereits durch die Verbindung eines Problems mit ‚Sicherheit' erhebt der Agent einen Anspruch auf die Behandlung desselben mit besonderen Mitteln (vgl. Buzan et al. 1998: 26).

Versicherheitlichung bezeichne dabei eine extreme Form der Politisierung, indem eine Problematik als existentielle Bedrohung dargestellt wird, für dessen Bekämpfung Notfallmaßnahmen eingesetzt und Handlungen außerhalb der ‚normalen' Politik legitimiert werden können (vgl. Buzan et al. 1998: 23f.). Bestimmte versicherheitlichende Akteure erklären dafür maßgebliche Objekte (*referent objetcts*; z.B: Staat, Nationen oder nationale Identität) als existentiell bedroht, die wiederum einen legitimen Anspruch auf Überleben haben (vgl. Buzan et al. 1998: 36).

Die alleinige Erklärung, bzw. der Diskurs kreiert Versicherheitlichung aber nicht von sich aus, dies stellt nur eine versicherheitlichende Handlung dar. Erst durch die Akzeptanz einer bestimmten Zuhörerschaft ist es möglich, dass eine Problematik vollständig versicherheitlicht wird (vgl. Buzan et al. 1998: 25).

Aufgrund der Zentralität der Sprache als performativem Akt wählen die Vertreter der Kopenhagener Schule hauptsächlich die Diskursanalyse (vgl. Buzan et al. 1998: 25), um Versicherheitlichung zu untersuchen.

2.2 Soziologischer Ansatz

2.2.1 Grundannahmen

Einen weiteren Ansatz, der als *soziologischer Ansatz* bekannt ist, verfolgen insbesondere Thierry Balzacq und Didier Bigo (vgl. z.B. Bigo 2008; Balzacq 2010a: 63; Balzacq 2011). Bedrohungswahrnehmungen seien demnach insbesondere durch Praktiken, Kontexte und Machtbeziehungen konstruiert (vgl. Balzacq 2011: 1). Eine ‚Erweiterung' des philosophischen Ansatzes zeigt sich bereits in der Zusammenfassung der Analyseeinheiten von Buzan et al. (1998) in das Level des ‚Agenten', das neben den Levels der Handlungen und des Kontexts besteht. (vgl. Balzacq 2011: 35)

Die Kernargumentation (im Gegensatz zur Kopenhagen Schule) folgt hier der Annahme, dass diskursive Untersuchungen dazu beitragen können, wie sich manche Sicherheitsprobleme entwickeln, andere aber kaum durch diskursive Elemente entstehen und diese Methode somit unzureichend sei. Das Sprachaktmodell betone das Aufkommen bzw. die Erschaffung von Sicherheitsproblemen, nicht aber deren Konstruktion (vgl. Balzacq 2011: 18). Es vernachlässige die Raum/Zeit-Strukturierung, die ein Ereignis teilweise erst möglich mache, da die Fixierung auf die Gegenwart überwiege (vgl. Bigo 2014: 211). Insgesamt habe internationale Sicherheit keine spezifische Agenda, die sich nach dem Überleben richtet und die durch Politiken außerhalb des Normalfalls, also Ausnahmepolitiken, gedeutet werden können. Vielmehr seien Ver(un)sicherheitlichungsprozesse nicht nur mit einem erfolgreichen Sprachakt unter den genannten Umständen verbunden, sondern mit Routinen der relevanten Akteure, die alles umrahmen (vgl. Bigo und Tsoukala 2008: 5).

Versicherheitlichung kann demzufolge „diskursiv und nicht-diskursiv, intentional und nicht-intentional; performativ, aber keine ‚Handlung in sich selbst'" sein (Balzacq 2011: 2).

Grundlegende Unterschiede zum philosophischen Modell ergeben sich bereits in der Interpretation des Diskurses selbst. Die Vertreter des soziologischen Ansatzes kritisieren, dass das Sprachaktmodell universelle Prinzipien und Regeln entwickeln will, welche unabhängig von Kontext, Kultur und relativen Machtbeziehungen zwischen den Akteuren gelten sollen. Sie bezeichnen diese Sichtweise als ‚universelle Pragmatik' und folgern für sich, dass Sicherheit eine „pragmatische Handlung" sei (Balzacq 2010a: 64). Pragmatisch bedeutet, dass die Verwendung von Sprache als strategisches Mittel der Überzeugung dient (perlokutiver Akt) (vgl. Balzacq 2005: 184). Strategisch, da durch den argumentativen Sprachprozess ein bestimmtes Ziel erreicht werden soll. Durch die Beschreibung von Sicherheit als

‚pragmatischem Akt' kann Versicherheitlichung eben keine selbstreferentielle (vgl. Balzacq 2005: 178), sondern eine intersubjektive Praktik sein (vgl. Balzacq 2011: 3).
Versicherheitlichung wird dadurch als Prozess verstanden, der während und als Teil der Konfiguration von Umständen oder Gegebenheiten entsteht und dadurch keine konventionelle Prozedur sein kann.
Die Erweiterung des Modells von Buzan et al. (1998) um das Element des Kontexts sowie die Zentralität der Zuhörerschaft sind dafür hervorzuheben (vgl. Balzacq 2011: 35):
Die ermächtigte Zuhörerschaft ist keine formale, gegebene Entität, wie am philosophischen Ansatz kritisiert wird, sondern eine erst auftretende, empirisch zu beurteilende Kategorie, die sich durch die gegenseitige Beziehung zwischen versicherheitlichendem Akteur und Zuhörerschaft ergibt. Weiterhin betreibe die ‚traditionelle' Versicherheitlichungstheorie eine „Dekontextualisierung" bezüglich der sozialen Universen, aus denen Sicherheitsakteure stammen (vgl. Bigo 2014: 211). Um dem Diskurs überhaupt erst Bedeutung zu verleihen, muss dieser historisch und sozial eingebettet werden.

Balzacq (2011: 3) definiert Versicherheitlichung aufgrund der genannten Annahmen wie folgt:

> Securitization [is] an articulated assemblage of practices whereby heuristic artefacts (metaphors, policy tools, image repertoires, analogies, stereotypes, emotions, etc) are contextually mobilized by a securitizing actor, who works to prompt an audience to build a coherent network of implications (feelings, sensations, thoughts, and intuitions), about the critical vulnerability of a referent object, that concurs with the securitizing actor's reasons for choices and actions, by investing the referent subject with such an aura of unprecedent threatening complexion that a customized policy must be undertaken immediately to block its development.

Für eine erfolgreiche Versicherheitlichung benötigt ein versicherheitlichender Akteur die Zustimmung derer, für die eine „*direkte kausale Verbindung*" mit der Problematik auf moralischer und formaler Ebene besteht (Hervorhebung i.O; Balzacq 2005: 185). Moralische Unterstützung bedeutet die Zustimmung der ermächtigten Zuhörerschaft, während sich die formale Zustimmung auf das institutionelle Regelwerk (z.B. die Zustimmung des Parlaments) bezieht. Die moralische Zustimmung ist zwar notwendig, aber ohne die formale Zustimmung nicht hinreichend, um das gewünschte Ziel zu erreichen. Je kongruenter die beiden Formen sind, desto wahrscheinlicher wird die Versicherheitlichung (vgl. Balzacq 2005: 184f.).

Die Kritik am philosophischen Ansatz rechtfertigt für die Vertreter des soziologischen Ansatzes die Verwendung von weiteren Methoden als die Diskursanalyse. Diese stellt dennoch ein zentrales Analysemittel der soziologischen Theorieschule dar, wobei die

Methodenerweiterung eher als Vervollständigung der Zentrierung auf die Diskursanalyse des philosophischen Ansatzes zu bewerten ist (vgl. Balzacq 2005: 179; Bigo 2008: 129; Balzacq et al 2010: 3).

2.2.2 Instrumente-Ansatz

Ein Analyseelement der soziologischen Theorieschule bildet die *Untersuchung der Natur und der Funktionen von Policy-Instrumenten*. Diese können bedeutend zur Erforschung von Versicherheitlichung beitragen, da es immer schwieriger wird, Diskurse und Ideologien in Sicherheitsprogrammen zu entschlüsseln sowie die Unterschiede zwischen versicherheitlichendem Akteur und der Zuhörerschaft auszumachen (vgl. Balzacq 2011: 15).
Durch den Instrumente- (bzw. ‚Tool'-) Ansatz soll untersucht werden, wie Versicherheitlichungsprozesse durch ein Instrument auftreten, d.h. wie diese zu versicherheitlichenden Instrumenten werden können. Um dies herauszufinden, wird dargestellt, wie Instrumente der Versicherheitlichung definiert werden können, welche Charakteristika und Eigenschaften diese aufweisen und welche Arten von Instrumenten existieren, bzw. wie PNR-Daten in dieses Schemata eingeordnet werden können.

DEFINITION VON INSTRUMENTEN

Viele Autoren versuchten sich bereits an einer hinreichenden Definition von Instrumenten, (vgl. z. B. Instrumente als Objekt oder Aktivität, de Bruijn und Hufen 1998: 13f.).
Balzacq (2008: 79) argumentiert diesbezüglich, dass die Definition als Objekt oder Aktivität unvollständig sei, da sie nicht ausreiche um die Substanz von Instrumenten zu verstehen. Instrumente könnten nicht auf ihre inhärenten, technischen Funktionen reduziert werden, da sie ein spezifisches Dispositiv (im Sinne Foucaults)[2] initiieren und Praktiken verkörpern (vgl. Balzacq 2011: 15f.). Dadurch könnten Instrumente der Versicherheitlichung grundlegend zum Auftreten eines Sicherheitsbereichs und der Routinisierung von Praktiken (Habitus) beitragen (vgl. Balazcq 2011: 16). Sicherheitsinstrumente sind die „sozialen Mittel, durch die Experten der (Un)Sicherheit über eine Bedrohung nachdenken" (Balzacq 2011: 16). Durch sie wird bereits ein bestimmtes Hintergrundwissen vermittelt, sowie eine bestimmte Handlungsweise zur Bedrohungsbekämpfung impliziert. Instrumente der Versicherheitlichung sind also "*an identifiable social and technical ‚disositif' or device embodying a specific threat image*

[2] Michel Foucault (1978: 119f.) definiert ein ‚Dispositiv' als ein „entschieden heterogenes Ensemble, das Diskurse, Institutionen, architekturale Einrichtungen, reglementierende Entscheidungen, Gesetze, administrative Maßnahmen, wissenschaftliche Aussagen, philosophische, moralische oder philanthropische Lehrsätze, kurz: Gesagtes ebensowohl wie Ungesagtes umfaßt."

through which public action is configured in order to address a security issue." (Hervorhebung i.O.; Balzacq 2008: 79)

EIGENSCHAFTEN VON INSTRUMENTEN

Wie dargestellt, ist die Definition von Instrumenten der Versicherheitlichung äußerst komplex und eine eindeutige Definition schwer zu finden. Instrumente können deshalb vielmehr als ‚Bündel' von Eigenschaften definiert werden (vgl. Salamon 2002: 20), welche folgendes beinhalten:

a. Art von Gut/Ware oder Aktivität (z.B. eine Maßnahme)
b. Übermittlungsmechanismus für dieses Gut oder Aktivität (z.B. elektronisch, medial)
c. Übermittlungssystem aus Organisationen, die das Gut, die Aktivität oder den Service zur Verfügung stellen (z.B. Institutionen, Fluggesellschaften, administrative Abteilungen)
d. Regelsystem, formell oder informell, welches die Beziehungen zwischen den Entitäten die das Lieferungssystem bilden, definiert (z.B. EU-Richtlinien)

CHARAKTERISTIKA VON INSTRUMENTEN

Durch die Definition von Instrumenten der Versicherheitlichung ergeben sich nach Balzacq (2008: 80) weiterhin vier Charakteristika für diese:

Zu Anfang ist eine grundlegende Unterscheidung bezüglich der Definition und des Untersuchungsgegenstandes von Sicherheitsinstrumenten nötig: *Instrumente der Versicherheitlichung und versicherheitlichende Instrumente sind nicht miteinander gleichzusetzen*. Erstere erschaffen nicht automatisch eine Bedrohung, sondern sollen eine bereits akzeptierte Bedrohung bekämpfen oder vermindern. Im Gegensatz dazu transformieren die versicherheitlichenden Instrumente durch ihre inhärenten Eigenschaften (Natur und Funktion) das von ihnen benannte, bestimmte Wesen in eine Bedrohung. Für die Unterscheidung ist also das ‚aktive' Element zentral, was ein Instrument also tatsächlich selbst ‚tut'. Versicherheitlichende Instrumente tun etwas, indem sie Entitäten versicherheitlichen. Durch dieses Eigenleben könnten sie selbst die diskursive Logik der Versicherheitlichung ersetzen. (vgl. Balzacq 2008: 80)

Zusammengefasst können sie wie folgt definiert werden: „[…] a securitizing tool is *an instrument which, by its very nature or by its very functioning, transforms the entity (i.e. subject or object) it processes into a threat*." (Hervorhebung i.O.; Balzacq 2008: 80)

Bezüglich des europäischen Grenzmanagements durch Daten- und Informationsaustausch illustriert Bigo (2014: 219; Umstellung d. Verf.) diesen Punkt sehr deutlich, indem er

ausführt, dass „durch die Logik der Datenaufspaltung und seiner Rückzusammenfügung in anonymisierte Profile, Datendoubles ein Leben für sich selbst annehmen [können]. Sie können Fremde werden, die du niemals getroffen hast. Ein Detail wie ein vertippter Buchstabe kann dein Leben verändern."

Die prinzipielle Daseinsberechtigung versicherheitlichender Instrumente sei meist indiskutabel. Trotzdem können Instrumente dynamisch bzw. instabil sein (vgl. Peters und van Nispen 1998: 2). In diesem Prozess werden Veränderungen meist als ‚Verbesserungen' des Instruments klassifiziert. (vgl. Balzacq 2008: 80)

Eine Analyseebene tiefer hat nun auch jedes einzelne Instrument spezielle *definierende und Design Eigenschaften*, welche es mit anderen Instrumenten vergleichbar und einzigartig macht bzw. welche je nach Programm variieren können. Das Unterscheidungskriterium stellt die *Natur des Instruments* dar: die Art, wie das spezielle Instrument beschaffen ist bzw. was es individuell charakterisiert, entspricht also seiner Natur.

Bei Instrumenten, die Informationen betreffen, sammelt, speichert und tauscht jedes einzelne Instrument Informationen (*Design-Eigenschaft*). Sie unterscheiden sich aber untereinander grundlegend in der Art der Daten, der Speicherungsdauer oder ihren Zugangsbedingungen (*definierende Eigenschaften*). (vgl. Balzacq 2011: 16)

Diese Natur kann sich aufgrund der Instabilität von versicherheitlichenden Instrumenten verändern. Schrittweise kann sich eine schleichende Funktions- oder Zweckausweitung der Instrumente (‚*function-creep*'-Effekt) einstellen, was bedeutet, dass die genutzten Mittel nicht mehr dem *ursprünglich* für sie vorgesehenen Verwendungszweck und damit nicht mehr seiner ursprünglichen Natur entsprechen (vgl. Balzacq 2008: 87).

Beispielsweise konnte sich Eurodac durch seine dynamische Entwicklung von einem ursprünglichen Instrument der Abwehr von ‚Asyl-Shopping', d.h. einem Kontrollinstrument, hin zu einem investigativen Mittel (u.a) der Terrorabwehr entwickeln. Es veränderte so also seine Natur (vgl. Balzacq 2008: 87f.).

Drittens ist jedes Policy-Instrument eine *Art von Institution*. Als Institution strukturieren Instrumente Handlungen, indem sie die die eingebundenen Akteure, deren Rollen und ihre Beziehungen untereinander definieren (vgl. Salamon 2002: 19). Folglich sind diese Beziehungen nicht mehr formlos, sondern „institutionalisiert" (Salamon 2002: 19).

Die Handlung, die strukturiert wird, ist die ‚kollektive Handlung'. ‚Kollektiv' soll verdeutlichen, dass alle Entitäten eingebunden werden, deren Handlungen durch das Instrument strukturiert werden (da dies häufig nicht nur das gouvernementale Handeln betrifft) (vgl. Salamon 2002: 20).

Beispielsweise kann sich ein Abkommen zum Datenaustausch nicht nur dadurch auszeichnen, dass ein Staat durch dieses einen Sicherheits-oder Machtgewinn erlangt, sondern auch dadurch, dass sich die (Nicht-)Abschließung von einem Abkommen gezielt auf die Beziehung der Staaten zueinander und damit auf das internationale Gefüge auswirkt[3].
Letztens reflektieren Instrumente *ein spezifisches Bedrohungsbild* und die Auswahl der Bekämpfungsart bzw. die Effekte des genutzten Instruments. Diese Effekte können sich direkt oder indirekt in der Natur des Mittels zeigen.
Bezüglich des Informationsaustauschs werden in Datenbanken nicht nur die Ein- und Ausreise-Aktivitäten von Individuen gespeichert, sondern zusätzlich kategorisiert und strafrechtlich bzw. polizeilich verfolgt (vgl. Brouwer 2006: 148).

Zusammenfassend geht Balzacq davon aus, dass die Reduzierung der Sicherheitsinstrumente auf operationale Faktoren die symbolischen und politischen Elemente, die diese beinhalten, außen vor ließe (vgl. Balzacq 2011: 17). Einerseits zeigen sich politischen Elemente deutlich, da die Auswahl, Nutzung und Effekte von Sicherheitsinstrumenten durch politische Faktoren und Mobilisierung geprägt sind, sogar von diesen abhängig sind (vgl. Peters und van Nispen 1998: 3; Peters 2002: 552). Andererseits zeigt sich in Policy-Instrumenten eine eingebaute Symbolik, durch die die Denkweise des versicherheitlichenden Akteurs sowie die kollektive Wahrnehmung von Problemen erkannt werden kann (vgl. Peters und van Nispen 1998: 3), sowie deren Intentionen (vgl. de Bruijn und Hufen 1998: 12).

ARTEN VON INSTRUMENTEN

In der Literatur wurde bereits eine Vielzahl von Typologien für Instrumente entwickelt. Schneider und Ingram (1990: 513) versuchen in ihrer Typologie Policy-Tools bezüglich der von ihnen bewirkten Verhaltensänderung zu klassifizieren. Eine Verhaltensänderung kann sich dabei auf gesellschaftliche Akteure beziehen (extern) oder die Änderung von Arbeitsweisen innerhalb der EU betreffen (intern) (vgl. Salamon 2002: 20).
Die detailliertere Kategorisierung bezieht sich auf fünf unterschiedliche Maßnahmen: Autoritätsmittel, Anreiz schaffende Mittel, inhaltliche Maßnahmen, symbolische und lernende Maßnahmen (vgl. Schneider und Ingram 1990: 514-521).

[3] Noch deutlicher zeigt sich dies beim staatlichen Besitz von Nuklearwaffen (vgl. Balzacq 2008: 16): Nuklearwaffen zeichnen sich beispielsweise nicht nur dadurch aus, dass ein Staat einen Sicherheits-oder Machtgewinn durch diese erlangt, sondern auch durch die inhärente Eigenschaft des Instruments, die Beziehungen zwischen Staaten und damit das internationale Gefüge zu transformieren .

Die inhaltlichen Maßnahmen sind die relevanten der Forschungsarbeit, da ein Instrument des Spektrums der Information (Fluggastdaten) untersucht wird.

Wie Schneider und Ingram (1990: 517) zeigen, bestehen inhaltliche Maßnahmen aus Informationen, Training, Bildung und Ressourcen, um bestimmten Akteuren Entscheidungen oder Aktivitäten zu ermöglichen. Dabei beinhaltet die Instrumente spezifische Modalitäten, um externe Disziplin von Individuen und Gruppen zu verlangen (vgl. Balzacq 2011: 17).

PNR-Informationen sollen es Regierungen und strafrechtlichen bzw. polizeilichen Institutionen möglich machen, Terroristen und Schwerkriminelle (präventiv) zu erkennen und zu bekämpfen. Durch die Daten sollen mögliche Straftaten verhindert werden, da die Erkennung von potentiellen Täten wahrscheinlicher würde und diese so diszipliniert werden können. Somit betrifft die gezielte Verhaltensänderung insbesondere gesellschaftliche Akteure, wodurch das Instrument in die externe Dimension eingeordnet werden kann.

Inhaltliche Maßnahmen können häufig besonders instabil sein, wodurch die Transformation in ein versicherheitlichendes Instrument überhaupt erst möglich sei:

> It is this possibility of securitization tools being vested with new functions (that would otherwise not be accepted), through the invocation of ‘exceptional circumstances‘, that turns them into securitizing tools. (Balzacq 2008: 82)

Balazcq folgt mit dieser Betonung der ‚besonderen Umstände‘, d.h. einer ‚Politik außerhalb des Regelfalls‘, die zu Versicherheitlichung führt, der Lesart der Kopenhagener Schule. Beispielsweise betrifft das eine starke Geheimhaltung der Funktionsweise des Instruments, das Fehlen einer öffentlichen Debatte über das fragliche Instrument und dessen Beschließung unter Zeitdruck. (vgl. Balzacq 2008: 93f.)

3 Empirische Untersuchung des Fluggastdaten – Instruments

Die Untersuchung des PNR-Instruments erfolgt in zwei Dimensionen: die interne Dimension wird anhand der EU-PNR Vorschläge beleuchtet während die externe Dimension durch Abkommen der EU mit den USA (EU-USA PNR) dargestellt wird.

Gerade in der dynamischen, evolutionären Entwicklung des Instruments, d.h. durch die Untersuchung der verschiedenen Entwürfe, Vorschläge und Abkommen zu PNR Daten, kann teilweise auf Intentionen der versicherheitlichenden Akteure geschlossen werden, weswegen unterschiedliche Dokumente in die Analyse aufgenommen werden.

Dem Instrumente-Ansatz folgend, werden die Dimensionen jeweils in fünf Ebenen untersucht: zuerst wird die Struktur, d.h. die Natur und Funktionen, des Instruments detailliert dargestellt. Dies beinhaltet dessen definierende und Design- Eigenschaften. Daraufhin wird

herausgestellt, wie kollektive Handlungen durch Passagierdaten strukturiert und somit Beziehungen zwischen Akteuren institutionalisiert werden können. Viertens wird untersucht, welches Bedrohungsbild das jeweilige Instrument direkt und indirekt reflektiert. Letztendlich soll durch die Untersuchung gezeigt werden, wie sich ein versicherheitlichendes Instrument durch die dargestellten Analyseebenen herausbildet. Dies beinhaltet alle vorherigen Analyselevel inklusive der Transformation des spezifischen Bedrohungsbildes in das Instrument der Fluggasdaten.

PNR als Instrument beinhalten die Informationssammlung, -speicherung, -übermittlung, sowie den Austausch von Fluggastdaten in und zwischen Mitglieds- und Drittstaaten sowie zwischen Institutionen. Das Instrument verarbeitet personenbezogene Daten, das betroffene Subjekt ist also der/ die Flugreisende. Die Auswertung der Daten verfolgt den Zweck, Terrorismus und schwere oder organisierte Kriminalität zu bekämpfen (vgl. Kommission 2007; 2011a; Rat 2012).
Das Regelsystem, welches die Beziehungen zwischen den Entitäten beschreibt, besteht aus formalen europäische Rahmen- sowie Richtlinienvorschlägen bzw. bilateralen Abkommen der EU und einzelner Drittstaaten (USA, Australien, Kanada). Des Weiteren gehören zu diesem Regelsystem verschiedene Mitteilungen einzelner EU-Institutionen, Datenschutzrichtlinien und Erklärungen der Fluggesellschaften als Übermittlungssystem.

PNR-Daten sind prinzipiell Informationen über Personen, die Beförderungsmittel nutzen. Trotz der Übersetzung als ‚Fluggastdaten' kann sich dies auch auf Züge und Schiffe beziehen, welche oftmals aber keine Buchungssysteme wie Fluggesellschaften besitzen (vgl. Kommission 2011b: 16). Die EU bezieht sich in ihren Vorschlägen und Abkommen nur auf den Flugverkehr.
In diesem Bereich ist zwischen Advanced-Passenger-Information (API) und Passenger-Name-Records (PNR) zu unterscheiden. API- Daten beziehen sich auf maschinell einlesbare Reisepass-Informationen, wie Staatsangehörigkeit, Name oder Geburtsdatum und werden in der europäischen Union bereits erhoben (vgl. Rat 2004). Folglich werden sie zur Identitätsfeststellung verwendet und verfolgen damit den Zweck, „Grenzkontrollen zu verbessern und die illegale Einwanderung zu bekämpfen." (Rat 2004: Art. 1)
Im Gegensatz dazu beziehen sich PNR-Daten auf Informationen, die der Flugreisende während der Reservierung getätigt hat und auf die die Fluggesellschaft durch die Buchung oder durch Übermittlung einer Reiseagentur Zugriff hat. Sie gehen also insofern über die API-

Daten hinaus, als dass sie sich nicht ausschließlich auf die Identität des Reisenden, sondern auch auf den Flug selbst beziehen: Flugrouten, Sitzplatznummer, Mitreisende, Gepäckinformationen, Essenswünsche usw. Folglich sollen sie Aufschluss über Gewohnheiten und Hintergrundinformationen der Flugreisenden geben (vgl. Brouwer 2009: 3; Kommission 2007: Art.3 V).

Die Fluggastdaten aller ‚Erheber' (Fluggesellschaften, Reiseagenturen) werden vorerst in deren Buchungssystem gespeichert. Der institutionelle Zugriff kann sich zentral – auf eine Institution (z.B. Europol) – oder dezentral – auf verschiedene Institutionen der Mitgliedsstaaten- gestalten. Diese bestimmten Institutionen können daraufhin durch ein ‚Push'- oder ein ‚Pull' – System auf die PNR-Daten zugreifen.
Bei Nutzung der ‚Pull'-Methode können die betrauten Behörden direkt auf das Buchungssystem der Fluggesellschaften zugreifen und Kopien der Daten erstellen, während mit der ‚Push'-Methode die PNR-Daten an die jeweilige Behörde übermittelt werden, ohne direkten Zugriff auf das IT-System zu haben (vgl. Rat 2012: 8).

Die Details der Ausgestaltung dieser allgemeinen Rahmenbestimmungen unterscheiden sich je nach Instrument und involvierten Akteuren.

3.1 Daten und Informationssysteme

Vorab ist zu erläutern, was ‚Daten' bzw. ‚Datenbanken' überhaupt bedeutet. Sobald gesammelte Informationen in einem automatisierten oder nicht automatisierten System gesammelt und gespeichert werden, werden sie zu Daten. Diese Sammlung innerhalb eines Systems kann auch als Datenbank bezeichnet werden, die unterschiedlich programmiert werden kann. Daten in einer Datenbank werden in jedem Fall miteinander in Beziehung gesetzt, sie existieren nicht unabhängig voneinander sondern sind „logisch miteinander verbunden" (Balzacq 2008: 83). Man könnte sie auch als „Körper des Wissens" (Balzacq 2008: 83) oder als ein „Datendouble" (Bigo 2014: 217) der dahinter verborgenen Person bezeichnen. Datenbanken und die Speicherung und Sammlung von Daten sind überhaupt erst sinnvoll, wenn diese kategorisiert werden und ihnen eine Art Bedeutung verliehen wird. Diese Bedeutung kann ihnen auch durch die Erkennung von Trends oder Querverbindungen

verliehen werden, die auf der computergestützten Analyse solcher Daten basiert (Data-Mining[4]).

Im Sicherheitsbereich sagt die Auswahl der gesammelten Daten also bereits viel darüber aus, was wichtig ist, um eine Sicherheitsbedrohung zu erkennen und zu bekämpfen. Die Erstellung von Querverbindungen und die Auswertungsmethoden der Daten lassen dadurch Schlüsse über die Bedrohungswahrnehmung der versicherheitlichenden Akteure zu.

3.2 Interne Dimension von PNR Daten

Im ersten Abschnitt wird die interne (europäische) Dimension von PNR-Daten insbesondere durch die Untersuchung von Rahmenbeschluss- und Richtlinienvorschlägen der EU von 2007 (Kommission 2007), 2011 (Kommission 2011a) und 2012 (Rat 2012) dargestellt.
‚Intern' bedeutet dabei die Erfassung von Passagierdaten bei Übertritt der Außengrenzen der EU sowie die Möglichkeit der Erfassung von intra-EU Flügen durch die Mitgliedsstaaten (vgl. Rat 2012: 2).

EU-PNR wurden seit jeher kontrovers diskutiert. So wurde der erste Vorschlag von 2007 aufgrund des Vertrags von Lissabon und der damit verbundenen Aufhebung der Säulenstruktur der EU hinfällig, während der Kommissionsvorschlag von 2011 vom Komitee für bürgerliche Freiheiten, Justiz und Inneres (LIBE-Ausschuß) in einem knappen Votum abgelehnt wurde[5]. Die Kommission reagierte auf dieses Votum mit dem Kommentar, dass es sich ‚nur' um eine Komitee-Abstimmung gehandelt habe und die Beschließung des PNR-Instruments nichts desto trotz überaus wichtig sei.[6] Dieser Handlungsdruck geht auch aus einer aktuellen Mitteilung der Kommission hervor (vgl. Kommission 2015b: 1). Der Richtlinienvorschlag des Rates von 2012 wird daher derzeit noch weiter diskutiert. Das Europäische Parlament beschloss zudem, bis Ende des Jahres 2015 die Richtlinie zu PNR final bearbeitet zu haben (vgl. Europäisches Parlament 2015: §13).

[4] Data-Mining bezeichnet nach einer Empfehlung des Ministerrats des Europäischen Rates eine zweite Stufe des Profiling, in der Daten analysiert und ‚untersucht' werden, um auf Korrelationen zwischen verschiedenen Verhaltensweisen und Charakteristika zu schließen (vgl. Ministerrat 2010: 25).
[5] Vgl. Europäisches Parlament (2013): Press release. Civil Liberties Committee rejects EU Passenger Name Record Proposal [online] http://www.europarl.europa.eu/news/de/news-room/content/20130422IPR07523/html/Civil-Liberties-Committee-rejects-EU-Passenger-Name-Record-proposal [eingesehen am 01.07.2015], 24.4.2013.
[6] Vgl. Mahony, Honor (2013): MEPs vote down air passenger data scheme, *euobserver* [online] https://euobserver.com/justice/119926 [eingesehen am 01.07.2015], 24.4.2013.

3.2.1 Definierende Eigenschaften

Wie andere Instrumente (SIS, SIS II, VIS, Eurodac) werden durch die PNR personenbezogene Informationen gesammelt, gespeichert und getauscht. Als Funktionsüberschneidungen ergäbe sich, dass „dieselben personenbezogenen Daten […] im Rahmen unterschiedlicher Instrumente erhoben, jedoch im Rahmen eines einzelnen Instruments jeweils nur einem beschränkten Zweck zugeführt werden [können]“ (Hinzufügung d. Verf. ; Kommission 2010b: 26). Eine Ausnahme bilden hier das das SIS II, das VIS und Eurodac, deren Grenzschutzweck durch die Bekämpfung des Terrorismus und der schweren Kriminalität erweitert wurden (vgl. Kommission 2005: 2).[7]

Unterschiede ergeben sich demnach in der *geäußerten* Zielausrichtung (bzw. dem Zweck) – während andere Instrumente der Information insbesondere auf das Grenzmanagement ausgerichtet sind, soll mit PNR-Daten bereits von Anfang an der Kampf gegen den Terrorismus unterstützt werden. Durch PNR-Daten sollen vor allem „‘unbekannte‘ Verdächtige“ (Kommission 2011a: 5) identifiziert werden, wohingegen Instrumente wie das SIS (II) nur „‘bekannte‘ Personen und gesuchte Gegenstände“ (Kommission 2011a: 6) identifizieren könnten. Außerdem würden die PNR-Daten *vor* dem und nicht *beim* Grenzübertritt angefordert werden (vgl. Kommission 2011a: 9). Im Gegensatz zu API-Daten, welche nur „auf Anfrage der […] beauftragten Behörde“ (Rat 2004: 2) angefragt werden können, ist bei PNR-Daten geplant, diese permanent, also ohne speziellen Anlass, an die zuständige Behörde zu übermitteln.

3.2.2 Design-Eigenschaften (Einzigartigkeit und Dynamik)

ZWECK DER PNR-DATENSÄTZE

PNR-Daten sollen auf drei Weisen genutzt werden (vgl. Kommission 2011a: 4):

(1) *Reaktiv* bei Ermittlungen, (2) *In Echtzeit*, d.h. vor Ankunft oder Abreise der Fluggäste, durch einen Abgleich mit anderen Datenbanken und zuvor festgelegten Prüfkriterien (vgl. Datenverarbeitung) und (3) *Proaktiv* zur Analyse und Bestimmung von Prüfkriterien.

Die Daten werden also zur Identifikation von ‚bekannten‘ Terroristen und Kriminellen (insbesondere durch den Abgleich mit anderen Daten) sowie zur Identifikation von ‚unbekannten‘ Individuen, die eine Sicherheitsbedrohung darstellen (insbesondere durch die

[7] Balzacq (2008) untersuchte diese Instrumente eingehend und stellte durch den Tool-Ansatz Versicherheitlichungsprozesse heraus.

Auswertung der Daten und Erstellung von Risikoindikatoren) verwendet (vgl. Brouwer 2009: 4).

Der Zweck der Erhebung und Nutzung von PNR-Daten wurde durch den Kampf gegen den Terrorismus in zwei Hinsichten verändert. Erstens wurde der ursprüngliche Verwendungszweck des Instruments deutlich modifiziert und zweitens fand in den Vorschlägen zu EU-PNR eine Erweiterung der Nutzungsmöglichkeiten statt.

PNR-Daten wurden ursprünglich für kommerzielle Zwecke der Fluggesellschaften genutzt (vgl. ICAO 2010: 2-1). Wie oben dargestellt, wird das Instrument der PNR nun im Kampf gegen den Terrorismus und verschiedene Zwecke der Strafverfolgung verwendet, wodurch es zu einem investigativen Instrument wurde (vgl. Hobbing 2008: 8). Der ursprüngliche Verwendungszweck (und damit die Natur des Instruments) wurden also deutlich geändert, wodurch ein *Function-creep*-Effekt eingetreten ist.

Zweitens zeigt sich die Zweckerweiterung auch in den verschiedenen Vorschlägen zu EU-PNR. Während im Entwurf von 2007 noch von der „Verhütung und Bekämpfung terroristischer Straftaten und organisierter Kriminalität“ (Kommission 2007: Art.1) die Rede ist, wird letzteres 2011 und 2012 durch „schwere Kriminalität“ (Kommission 2011a: Art.4 IIa; Rat 2012: Art.4 IIa) ersetzt. Hierbei ist anzumerken, dass die Tatbestände schwerer Kriminalität weit über die der organisierten hinausgehen[8]. Die alleinige Tatsache, dass PNR-Daten nicht nur für die Verhütung, Aufdeckung, Aufklärung und strafrechtlichen Verfolgung von terroristischen, sondern auch von anderen Straftaten verwendet werden können, zeigt bereits seine vielseitige Zweckbestimmung (vgl. Bigo et al. 2012: 23).

Die Straftaten, die durch das PNR-Informationsmanagement bekämpft werden sollen, wurden also de facto erweitert und betreffen nicht ausschließlich die Bekämpfung des Terrorismus.

DATENERFASSUNG UND DATENELEMENTE

Die Datenerfassung betrifft den Grenzübertritt von Mitgliedstaaten in Drittstaaten sowie alle Zwischenlandungen in Mitgliedsstaaten (vgl. Kommission 2011a: Art.2b). Das heißt, dass PNR-Daten insbesondere an den EU-Außengrenzen erhoben werden sollen.

Im dritten Richtlinienvorschlag wird die Datenerfassung auf die den möglichen Einbezug von Intra-EU Flüge erweitert (vgl. Rat 2012: 3). Die Erhebung ist den Mitgliedstaaten freigestellt und beträfe alle Flüge die die nationalstaatlichen Grenzen jedes einzelnen Mitgliedsstaates

[8] Vergleiche hierzu die zwei Definitionen von organisierter Kriminalität (Rahmenbeschluss 2008/841/JI des Rates vom 24. Oktober 2008, Art. 2) und schwerer Kriminalität (Rahmenbeschluss 2002/584/JI des Rates vom 13. Juni 2002, Art.2).

überqueren. Es können auch nur einzelne Flüge ausgewählt werden, die in der Einschätzung der Staaten als „gefährdend“ gelten (Rat 2012: Art.1a).

Die Datenelemente sind in 19 Kategorien gegliedert (siehe Anhang I). Diese beinhalten u.a. den gesamten Reisverlauf, die Sitzplatznummer sowie sonstige Sitzplatzinformationen, soweit verfügbar API-Daten, eine Kategorie die als ‚Allgemeine Hinweise‘ bezeichnet wird und alle Änderungen der gesamten Kategorien.
Während 2007 die Datenerfassung von „Allgemeinen Hinweisen“ noch mit dem Zusatz des ausdrücklichen Verbots der Verarbeitung von sensiblen Daten versehen ist (vgl. Kommission 2007: 27), wird dieses in den Datenelementen von 2012 nicht mehr genannt (vgl. Anhang I). Sogenannte ‚sensible Daten‘ geben beispielsweise direkt oder indirekt Aufschluss über die ethnische Herkunft, die religiöse oder weltanschauliche Überzeugung, die politische Einstellung, den Gesundheitszustand oder das Sexualleben einer Person (vgl. Kommission 2011a: 10).
Ein von den Arbeitsgruppen kommentierter Entwurf des Rahmenbeschlusses von 2009 zeigt auf, dass sensible Daten zwar nicht verarbeitet werden sollen, dennoch aber aufbewahrt und gesammelt werden können (vgl. Rat 2009: Art. 11a). Diese Formulierung wurde allerdings in den aktuelleren Vorschlägen wieder entfernt (vgl. Rat 2011: Art. 11a; Rat 2012: Art.11 IV). Auf informeller Ebene ist zumindest teilweise von Intentionen der Mitgliedsstaaten auszugehen, sensible Daten in die Erfassung von PNR mitaufzunehmen (vgl. Brouwer 2009: 8). Da die Ausgestaltung der PNR-Systeme bei den Mitgliedsstaaten selbst liegt (vgl. Institutioneller Zugriff), kann also ein Einbezug von sensiblen Daten nicht ausgeschlossen werden.

DATENÜBERMITTLUNG

Fluggesellschaften sind Teil des Übermittlungssystems der PNR-Daten. Die EU bevorzugt die ‚Push‘-Methode für alle Fluggesellschaften innerhalb der EU (vgl. Rat 2012: Art. 6I). Die Übermittlung der Daten (Übermittlungsmechanismus) erfolgt in der Regel elektronisch (vgl. Rat 2012: Art. 13). Die Fluggesellschaften müssen die Daten zu zwei Zeitpunkten übermitteln: Einmal mindestens 48 Stunden vor dem Abflug und einmal kurz nach der Schließung des Flugs (vgl. Rat 2012: Art. 6 IIa,b). In Ausnahmefällen können die PNR-Daten auch auf Anfrage der PNR-Zentralstelle zu anderen Zeitpunkten übermittelt werden (vgl. Rat 2012: Art. 6 IV).

DATENSPEICHERUNG

Die Speicherdauer von PNR-Daten beträgt im ersten Vorschlag fünf Jahre. Nach Ablauf dieser Frist werden die Daten anonymisiert nochmals acht Jahre vorbehalten, vorbehaltlich laufender polizeilicher Ermittlungen (vgl. Kommission 2007: Art.9).

Im zweiten Vorschlag beträgt die Speicherdauer fünf Jahre, nach dessen Ablauf die Daten (vorbehaltlich polizeilicher Ermittlungen) gelöscht werden müssen. Die Anonymisierung[9] der Daten erfolgt bereits nach 30 Tagen (vgl. Kommission 2011a: Art.9 II).

Der dritte Vorschlag stellt eine Art Zwischenlösung zwischen den ersten beiden Texten dar. Die Daten sollen dabei fünf Jahre gespeichert werden, innerhalb dieser Zeit aber nach zwei Jahren bezüglich der Identität des Flugreisenden anonymisiert werden (vgl. Rat 2012: Art.9 II). Die dargestellte Uneinigkeit um die Speicherdauer der PNR bezieht sich vor allem auf den Schutz von personenbezogenen Informationen, welche nach einem bestimmten Zeitraum unkenntlich gemacht werden müssen. Da der Vorschlag der Anonymisierung nach 30 Tagen auf eine Unkenntlichmachung nach zwei Jahren erweitert wurde, stellt der letzte Vorschlag de facto eine Verlängerung der Speicherdauer dar.

Diese Diskussion ist relevant, da sich die Anonymisierung auch auf die Kategorie der ‚Allgemeinen Hinweise' bezieht. Aus der Tatsache, diese möglichst lange verwenden zu wollen, können Schlussfolgerungen für das Bedrohungsbild gezogen werden (vgl. 3.2.4).

INSTITUTIONELLER ZUGRIFF UND AUSTAUSCH

Die Verarbeitung der PNR auf europäischer Ebene soll dezentral erfolgen, d.h. jeder Mitgliedsstaat bestimmt eine sogenannte „PNR-Zentralstelle" oder Mitgliedsstaaten bestimmen eine gemeinsame Stelle (vgl. Rat 2012: Art.3). Im zweiten Richtlinien-Vorschlag heißt es weiterhin, dass die Mitgliedsstaaten selbst bestimmen können, „wie sie ihr PNR-System ausgestalten und welche technischen Merkmale es erhalten soll" (vgl. Kommission 2011a: 14).

Zugriff auf die PNR-Daten von der Zentralstelle erhalten alle ‚zuständigen Behörden', die durch eine Liste von den Mitgliedsstaaten bestimmt wurden. Dabei muss es sich um Strafverfolgungsbehörden handeln, die im Bereich der Terrorismusbekämpfung tätig sind (vgl. Rat 2012: Art. 5 II).

[9] Die Anonymisierung bzw. ‚Unkenntlichmachung' bezieht sich auf Elemente, die die Identität des Flugreisenden darlegen. Dies beinhaltet: Name(n), auch die Namen von im PNR-Datensatz verzeichneten mitreisenden Personen; Anschrift und Kontaktdaten; alle Arten von Zahlungsinformationen einschließlich Rechnungsanschrift, die zur unmittelbaren Feststellung der Identität des Fluggasts, zu dem die PNR-Daten erstellt wurden, oder anderer Personen beitragen könnten; Vielflieger-Eintrag; allgemeine Hinweise, die zur unmittelbaren Feststellung der Identität des Fluggastes beitragen könnten, zu dem die PNR-Daten erstellt wurden; jedwede erweiterten Fluggastdaten. (vgl. Kommission 2012: Art. 9 II)

Passagierdaten, oder die Ergebnisse deren Verarbeitung, können zwischen Mitgliedsstaaten (vgl. Rat 2012: Art. 7), sowie im Einzelfall auch zwischen der PNR-Zentralstelle und Drittstaaten (vgl. Rat 2012: Art. 8) ausgetauscht werden. PNR-Zentralstellen als eigene oder als Teil von nationalen Behörden können also auch als Übermittlungssystem eingeordnet werden.

Während der Zugriff auf PNR-Daten in den Vorschlägen von 2007 und 2011 den nationalen Behörden vorbehalten wird, geht aus einer Mitteilung der Kommission hervor, dass auch Europol Zugriff auf die Systeme haben sollte (vgl. Kommission 2015b: 2).
Außerdem werden institutionelle Befugnisse möglicherweise auch durch den Abgleich mit anderen Instrumenten, insbesondere solchen des Grenzschutzes, erweitert (vgl. Datenverarbeitung). Die Zugriffsmöglichkeiten erscheinen in den vorliegenden Dokumenten intransparent und lassen Raum für Interpretationsmöglichkeiten.
Auf nationalstaatlicher Ebene ergeben sich auch Unterschiede bezüglich der Vorschläge der zuständigen Institutionen der Mitgliedsstaaten. Sind es im Vorschlag von 2007 noch solche, die für die „Verhütung und Bekämpfung terroristischer Straftaten und der organisierten Kriminalität“ (vgl. Kommission 2007: Art.4 II) zuständig sind, werden in Art. 5 II des Vorschlags von 2012 Institutionen genannt, die für die „Verhütung, Aufdeckung, Aufklärung oder strafrechtliche Verfolgung von terroristischen Straftaten oder schwerer Kriminalität“ verantwortlich sind.
In Kombination mit der Erweiterung der Tatbestandsmerkmale durch die Definition von ‚schwerer Kriminalität‘ erfolgt auch hier eine institutionelle Zugriffserweiterung durch den Einbezug weiterer Handlungsoptionen.

DATENVERARBEITUNG

Die Einsatzmöglichkeiten des Instruments zeigten bereits, wie PNR-Daten unterschiedlichen Zwecken zugeordnet werden können. Auch die Verarbeitungsmechanismen unterscheiden sich je nach Zielrichtung, also zwischen der Erkennung von ‚unbekannten‘ und ‚bekannten‘ Bedrohungen.
Die Erkennung von ‚unvorhergesehenen‘ Bedrohungen erfolgt insbesondere durch die Erstellung von Risikoindikatoren: dafür sollen die Mitgliedsstaaten eine „Einschätzung der potentiellen Bedrohung durch terroristische Straftaten und schwere Kriminalität“ (Kommission 2011a: 18) vornehmen, aus denen dann „objektive Prüfkriterien“ (Kommission 2011a: 6) hervorgehen sollen. In einer Mitteilung der Kommission heißt es weiterhin, dass

„Europol und Frontex erneut eine zentrale Rolle“ in der „Entwicklung und Verteilung solcher Risikoindikatoren anhand der von den Mitgliedsstaaten erhaltenen Informationen“ zukommt (Kommission 2015b: 8). Anhand dieser darf die PNR-Zentralstelle die Daten verarbeiten, falls eine Person „möglicherweise“ an einer terroristischen Straftat oder schwerer Kriminalität beteiligt ist (Rat 2012: Art.4 II). Auf der Grundlage der Analysen entstehen durch die Datenverarbeitung daraufhin auch neue, aktualisierte Risikoindikatoren (vgl. Kommission 2007: Art.3 V), d.h. neue Kriterien, wer oder was eine Bedrohung darstellt. Diese werden dann in dem PNR-Computersystem vermerkt, woraufhin eine *automatisierte* Analyse der Daten erfolgt. Bei einem Treffer der automatisierten Analyse muss diese von der PNR-Zentralstelle individuell überprüft werden (vgl. Rat 2012: Art. 4 II).
Zur Erkennung von ‚bekannten‘ Terroristen und Straftätern wird die Interoperabilität zwischen den unterschiedlichen Instrumenten durch die PNR-Daten vorangetrieben. Für die Nutzung der Daten in Echtzeit dürfen diese mit anderen relevanten Datenbanken abgeglichen werden (vgl. Rat 2012: Art.4 IIi).

Der konkrete Algorithmus, der hinter der Verarbeitung der Daten steckt, sowie die Festlegung von Kriterien sind weitestgehend intransparent, sodass diese als eine „Black-Box“ bezeichnet werden können (Leese 2014: 507). Die automatisierte Analyse der Daten durch das Instrument selbst ist besonders problematisch, da diese reaktiv bzw. in Echtzeit funktionieren soll. Da das Instrument selbst auswertet, was eine Bedrohung darstellt, betreibe es letztendlich Profiling (vgl. Brouwer 2009: 6; Bigo et al. 2012: 24; Leese 2014) (vgl. 3.2.4). Gemäß einer Empfehlung des Ministerkomitees des Europäischen Rates kann dies wie folgt definiert werden:

> ‘Profiling‘ means an automatic data processing technique that consists of applying a “profile” to an individual, particularly in order to take decisions concerning her or him or for analysing or predicting her or his personal preferences, behaviours and attitudes. (Ministerkomitee 2010: 9)

3.2.3 EU-PNR als Institution

Die kollektive Handlung, die durch Passagierdaten strukturiert wird, ist die Nutzung eines Flugzeuges bzw. die Übertretung von europäischen Grenzen.
In erster Linie ist das betroffene Subjekt der/ die Flugreisende. Die breite Auslegung dessen, was eine Bedrohung darstellen kann und deren kontinuierliche Erweiterung, könnte zu einer Verhaltensänderung der Fluggäste führen, da diese nicht mehr einordnen können, welches Verhalten als ‚natürlich‘ oder als ‚verdächtig‘ gewertet werde (vgl. Boehm 2010: 256f.).

Durch das Instrument wird insbesondere die gouvernementale Ebene strukturiert. Durch die europäische PNR-Gesetzgebung sollen nationalstaatliche Regelungen harmonisiert werden (vgl. Kommission 2011a: 13), da sich Interessen gemeinsam besser durchsetzen ließen (vgl. Kommission 2007: 7). Dies erfordere den Austausch der Daten untereinander und dafür Garantien, dass dieser auch wirklich erfolge. Die Mitgliedsstaaten könnten sich ohne das europäische Instrument der Fluggastdaten über eine Bereitstellung der Daten aus anderen Staaten nicht sicher sein (vgl. Kommission 2007: 7).

Das Instrument definiert, wer in den Prozess miteinbezogen wird: auf europäischer Ebene betrifft dies nationalstaatliche Strafverfolgungsbehörden sowie europäische Agenturen.

Bereits durch die Diskussion um europäische PNR sowie die Beschlüsse von Abkommen mit Drittstaaten fordern auch andere Staaten, die Daten für ihre eigenen Behörden zu erhalten (vgl. beispielsweise Mexiko[10]). Die Verweigerung solcher Datenaustausche könnte sich negativ auf die Außen- bzw. Verhandlungsbeziehungen im Allgemeinen auswirken. Deutlich zeigt sich dieser Verhandlungsdruck am PNR-Abkommen zwischen den USA und der EU (vgl. 3.3).

Insgesamt zeigt sich also durch die Existenz und die Institutionalisierung der Passagierdaten, dass die Beziehungen zwischen Regierungen verändert, bzw. strukturiert wurden.

3.2.4 Reflektion von spezifischem Bedrohungsbild

DIREKT

Durch den Fokus auf den Flugverkehr ist das transnationale Element mitinbegriffen. Zudem wird auch geäußert, dass die „Terrorismusgefahr […] nicht auf bestimmte Räume begrenzt" ist (Kommission 2007: 2) oder „die meisten terroristischen Aktivitäten grenzüberschreitenden Charakter haben und mit Reisen in andere Länder […] verbunden sind" (Kommission 2011a: 2). Dies rechtfertigt wiederum die Kooperation mit anderen Staaten, sei dies innerhalb oder außerhalb der EU. Mit der Funktionserweiterung des Instruments um die Möglichkeit der Erfassung von Intra-EU Flügen zeigt sich außerdem, dass die Bedrohung nicht nur außerhalb der EU, sondern auch *in* der EU angesiedelt ist. Die kollektive Bedrohungswahrnehmung richtet sich also auf das grenzüberschreitende Element aus.

Die generelle Ausrichtung der EU auf Instrumente der Information, die insbesondere den Grenzübertritt betreffen (vgl. Kommission 2010b) und multi-funktional sein können (vgl. Bigo et al. 2012: 20-23), zeigt sich in dem Fluggastdaten-Instrument bestätigt.

[10] Vgl. Nielsen, Nikolaj (20.03.2015): Mexico-EU data dispute puts airlines at risk of sanctions, in: *euobserver* [online] https://euobserver.com/justice/128095 [eingesehen am 01.07.2015].

Die politischen Entscheidungen der Auswahl solcher Instrumente belegt, dass die EU als versicherheitlichender Akteur gerade diese Mittel als effektiv erachtet.

Des Weiteren verlangt die Verarbeitung und Auswertung von PNR-Daten nicht nur die Feststellung von Bedrohungen, sondern direkt auch das polizeiliche und strafrechtliche Vorgehen durch unbestimmte „Maßnahmen" gegen diese (Rat 2012: Art. 5 I). Die proaktive Auswertung der Daten zeigt den Trend auf, polizeiliche Maßnahmen auf geheimdienstlicher Basis zu ergreifen (*intelligence-led policing*, vgl. Balzacq 2008: 94f.; Bigo et al. 2012: 25). Diese Konvergenz zwischen strafrechtlichem und geheimdienstlichem Vorgehen entspricht gleichzeitig der generellen Handlungsausrichtung der EU (vgl. Bigo et al. 2012: 24f.).

INDIREKT

Die Bedrohung wird als ‚unbekannt' dargestellt. Durch die Erhebung von Informationen soll die Bedrohung ‚erkannt' werden, d.h. aus den Datenelementen, die PNR umfassen. Die Darstellung der triumphierenden, realen Macht über das Unvorhergesehene zeigt auf, dass die EU ontologisch die Annahme verfolgt, die Welt sei kalkulier- und messbar, insofern objektiv einschätzbar (vgl. Leese 2014: 498). Der Einbezug von Datenelementen, die Aufschluss über Verhaltensmuster und teilweise über Religion, Gesundheit und vieles mehr geben, kann diese ‚unbekannte' Bedrohung in der Wahrnehmung der EU entschlüsseln.

Durch die vorherige Erstellung von ‚Risikoindikatoren' werden auf der Grundlage von Expertenwissen Hypothesen erstellt, wer oder was eine Bedrohung darstellt, die direkt in das Instrument einfließen. Wie Leese (2014: 498) es ausdrückt, liegt dem die Annahme zu Grunde, „dass ein Passagier, der bestimmte Charakteristika aufweist, zu einer Bedrohung werden könnte, selbst wenn es keine objektivierbare Aussage über die Natur oder Wahrscheinlichkeit dieser Bedrohung gibt".

Dass die europäische Grenzschutzebehörde FRONTEX an der Erstellung von Risiko- bzw. Bedrohungsindikatoren mitwirken soll, bedeutet des Weiteren, dass illegale Immigration als sicherheitsrelevanter Aspekt der EU eingeordnet wird.

Wie im Abschnitt der Datenverarbeitung aufgezeigt, werden durch das automatisierte System Profile konstruiert. Diese legen also fest, wer oder was ‚abnormal' ist und in Kombination mit den direkten Effekten (zum Beispiel der polizeilichen Verfolgung) exkludiert wird (vgl. Bigo und Tsoukala 2008: 2). Durch den Abgleich mit unterschiedlichen Instrumenten wie dem SIS (I, II) erweitere das PNR-Instrument diese um das Element des Profiling und trage dadurch ausschlaggebend dazu bei, „Daten getriebene Handlungen" (Bigo et al. 2012: 25) zu manifestieren.

3.2.5 Versicherheitlichungsprozesse

Als versicherheitlichendes Instrument müssten PNR-Daten ein ‚aktives Tun' aufweisen können. Sie müssten die von Ihnen bestimmten Entitäten selbst in eine Sicherheitsbedrohung transformieren. Dies geschieht in zweierlei Hinsicht: erstens im Hinblick auf Migration und zweitens im Hinblick auf sensible Daten.

SENSIBLE DATEN UND MIGRATION

In den europäischen Vorschlägen zu PNR-Daten wird eindeutig postuliert, dass die Daten *weniger* für den Grenzschutz als für den Kampf gegen den Terrorismus eingesetzt werden würden (vgl. Kommission 2011a: 9). Gleichzeitig wird durch die Funktion der PNR-Daten, API-Daten mit in deren Analyse einzubeziehen, ein Instrument der Abwehr der illegalen Migration in ihre Erfassung aufgenommen. Dies geschieht auch durch die Beziehung der PNR mit anderen Instrumenten wie dem SIS, SIS II, VIS und des geplanten EES. All diese Instrumente haben gemeinsam, dass sie (teilweise ursprünglich) dem integrierten Grenzschutz dienen sollen.

Wie oben erläutert, sind die Zugriffsmöglichkeiten der Behörden bisher weitestgehend intransparent und es zeigt sich eher der Trend der Erweiterung von institutionellen Befugnissen (vgl. der Einbezug von Europol), was auch mit der Erweiterung der Straftatbestände, für die PNR-Daten genutzt werden dürfen, zusammenhängt. Die Verarbeitung von PNR-Daten durch FRONTEX kann dabei nicht ausgeschlossen werden, da die Agentur bereits an der Risikoerstellung mitwirkt. Bestärkend kommt hinzu, dass Europol und FRONTEX bereits viel mehr „als Verbindungs- und Geheimdienststellen, anstelle einer ‚EU-Polizei' oder ‚EU-Grenzschutzagentur'" arbeiten würden (Bigo et. al. 2012: 27). Diese geheimdienstliche Arbeit und die Interoperabilität der Instrumente könnten letztendlich dazu beitragen, dass auf der Grundlage von PNR-Daten auch illegale Immigration verfolgt wird.

Dies lässt Schlüsse auf eine Erweiterung der Policy-Zielsetzungen zu bzw. könnte zu einer Zweckerweiterung führen.

Die Europäische Agentur für Grundrechte (FRA) merkte in ihrem Gutachten zum Vorschlag zu PNR-Daten von 2011 an, dass unmittelbare sowie mittelbare Diskriminierung durch Passagierdaten möglich seien. Zum einen sei dies unmittelbar durch die Erfassung von Essenswünschen in der Kategorie ‚Allgemeine Hinweise', die Rückschlüsse auf die Religion zulassen, zum anderen mittelbar durch die Überprüfung von Personen aufgrund ihres Namens, der Rückschlüsse auf die Ethnie zulässt, möglich (vgl. FRA 2011: 8-11).

Bei Übermittlung von sensiblen Daten seien diese zwar von den PNR-Zentralstellen zu löschen (vgl. Rat 2012: Art.11 III), andererseits zeigt sich, dass in dieser Kategorie Daten erfasst werden sollen „die zur unmittelbaren Feststellung der Identität des Fluggastes beitragen könnten“ (Rat 2012: Art.9 II). Es ist davon auszugehen, dass es sich dabei um andere Merkmale handeln soll, als diejenigen, die bereits erfasst wurden. Somit könnten sich in der Kategorie nur noch auffällige Verhaltensweisen, äußerliche und sprachliche Merkmale (die Rückschlüsse auf die Ethnie zulassen) oder gesundheitliche Zustände (z.B. durch Mitnahme von Medikamenten) befinden. Hierzu merkt Evelin Brouwer (2006: 25) an, dass Profiling immer auf dem Mechanismus der Differenzierung zwischen bestimmten Personengruppen anhand spezifischer Kriterien basiere und die genannten Merkmale so dazu beitragen könnten. Profiling, das als geheimdienstliche Praktik zu direkten polizeilichen Maßnahmen führt (vgl. 3.2.4), zeigt auf, wie bereits durch das Instrument bestimmt wird, wer oder was eine Bedrohung darstellt.

Bigo et al (2015: 12) formulieren diesen Punkt zusammenfassend wie folgt:

> Datenbanken wie EU-PNR […] repräsentieren einen Schritt in Richtung eines personen-zentrierten Ansatzes der Mobilitätskontrolle und Überwachung, durch den Individuen auf der Grundlage von Profilen, die nicht notwendigerweise in Beziehung zur Nationalität oder dem Migrantenstatus stehen müssen, sondern vielmehr auf anderen Verhaltens-, physischen oder physiologischen Charakteristiken basieren, eine Sicherheitsbedrohung sein oder werden können.

Insgesamt können in der breit gefassten und subjektiv interpretierbaren Kategorie der ‚Allgemeinen Hinweise‘ sensible Daten enthalten sein. Das würde bedeuten, dass eine Versicherheitlichung von Religion, Gesundheit und Ethnie bzw. Verhaltensweisen, die auf diese schließen lassen, durch das PNR-Instrument möglich ist. Die Bedrohungswahrnehmung der Personen, die an einem PNR arbeiten, fließt unmittelbar in die Bewertung von ‚verdächtigen‘ Individuen in das Instrument mit ein, welches diese Informationen danach automatisiert weiterverarbeitet. Durch den Spielraum, den die Kategorie der ‚Allgemeinen Hinweise‘ gewährt, können so verschiedene Themen in einen Sicherheitskontext gerückt werden und Profile entstehen, wer oder was eine Gefahr darstellt.

Dadurch würde das Instrument die genannten Entitäten selbst, also durch sein aktives Zutun, versicherheitlichen. Es ersetzt dadurch die diskursive Logik, da die Verarbeitung der Faktoren nicht explizit geäußert wird, sondern erst in Verbindung mit dem Arbeitsmechanismus der PNR ersichtlich wird.

POLITIK AUßERHALB DES ‚REGELFALLS‘

Des Weiteren wird durch Aussagen der Kommission eine Politik gerechtfertigt, die sich außerhalb des ‚Normalfalls‘ bewegt und so zu Versicherheitlichungsprozessen durch das

PNR-Instrument beiträgt. So heißt es, dem Instrument sei Priorität einzuräumen und seine schnelle Verabschiedung sei erforderlich und überaus wichtig (vgl. 3.2). Die Diskreditierung des LIBE-Ausschusses sowie der Zeitdruck, der sich offenbar auch auf die schnelle Entscheidung des Europäischen Parlaments auswirkt, zeigen, wie Politik im Namen von Sicherheit besondere Praktiken legitimieren kann.

3.3 Externe Dimension von PNR- Daten

Im zweiten Abschnitt wird die externe Dimension von PNR-Daten anhand des Fallbeispiels von Abkommen zwischen der EU und den USA untersucht. Dafür werden die (finalen) Abkommen von 2004 (EG 2004 bzw. Kommission 2004), 2007 (EU 2007) und 2012 (EU 2012) herangezogen.

Die Existenz mehrerer, unterschiedlicher Abkommen erklärt sich insbesondere durch die Kritik des Europäischen Parlaments und des Europäischen Datenschutzbeauftragten hinsichtlich des Schutzes von personenbezogenen Daten. Nach erfolgreicher Klage bezüglich des ersten Abkommens vor dem Europäischen Gerichtshof (vgl. Guild und Brouwer 2006) wurde 2006 ein neues Interim-Abkommen mit den USA geschlossen, welches bis zum 31. Juli 2007 gültig war (vgl. Hailbronner et al 2008: 190). Im Lichte des Inkrafttretens des Vertrags von Lissabon und den dadurch veränderten Kompetenzen des Europäischen Parlaments wurden die letzten zwei finalen Abkommen von 2007 und 2012 geschlossen (vgl. Nino 2010: 69f).

Die Dynamik bzw. die Veränderungen zwischen den Abkommen werden bereits in den Analysekategorien berücksichtigt.

3.3.1 Definierende Eigenschaften

Die Abkommen der externen Dimension, d.h. solche der EU mit Drittstaaten „gleichen sich hinsichtlich ihrer Zweckbestimmung, unterscheiden sich aber inhaltlich in Bezug auf Modalitäten der Übermittlung und die Art der vom Drittland eingegangenen Verpflichtungen“ (Kommission 2010a: 7).
Die Abkommen der USA und der EU gleichen nicht nur anderen externen Abkommen, sondern auch dem geplanten internen Instrument der EU-PNR (vgl. Pawlak 2009). In der externen sowie in der internen Dimension wird der Zweck verfolgt, Daten hinsichtlich möglicher Verbindungen zum Terrorismus sowie zu schwerer Kriminalität zu erheben, zu

speichern und auszuwerten (Kommission 2010b: 20). Die spezifischen Unterschiede der Modalitäten werden im nachfolgenden Teil näher beleuchtet.

Die Kooperation im Bereich Terrorismusbekämpfung zwischen den USA und der EU erstreckt sich des Weiteren auf mehrere Systeme, die den Austausch von Daten gewährleisten. Darunter befindet sich das EU-USA TFTP Abkommen, welches auf der Grundlage von Zahlungsverkehrsdaten der SWIFT (Society for Worldwide Interbank Financial Telecommunication) zur Verhinderung, Ermittlung, Aufdeckung und Verfolgung des Terrorismus und dessen Finanzierung beitragen soll (vgl. Kommission 2010a: 22). Hier wird also eine andere Art von Daten ausgetauscht, die geäußerte Zielrichtung bleibt aber dieselbe.

Außerdem legte die Kommission eine Mitteilung vor, in der Grundsätze und Verhandlungsleitlinien über PNR-Abkommen mit Drittstaaten beschrieben sind. Ähnlich wie in den Vorschlägen zu EU-PNR heißt es hier, dass PNR-Daten „hauptsächlich zur Erkenntnisgewinnung und weniger zur Identitätsüberprüfung verwendet“ (Kommission 2010a: 4) werden, da sie sich in ihrer Natur bereits stark von API-Daten unterscheiden würden. Auch hier steht die Risikoanalyse sowie die Identifizierung „‘unbekannter‘ Personen, d.h. Personen, die für Strafverfolgungszwecke von Interesse sein könnten und bisher nicht verdächtig waren“ (Kommission 2010a: 4) im Vordergrund. Dabei ist die Verwendung wiederum reaktiv, in Echtzeit und proaktiv gestaltet (vgl. Kommission 2010a: 5).

3.3.2 Design- Eigenschaften (Einzigartigkeit und Dynamik)

ZWECK DER PNR-DATENSÄTZE

In der Verpflichtungserklärung des Department of Homeland Security (DHS) von 2004 wird die Nutzung der PNR-Datenelemente auf die Verhütung und Bekämpfung von Terrorismus, anderer schwerer transnationaler Straftaten (einschließlich organisierter Kriminalität) bzw. Flucht vor Haftbefehlen oder Ingewahrsnahme bezüglich der genannten Straftaten beschränkt (vgl. Kommission 2004: §3).

Im Abkommen von 2007 werden diese Tatbestände bereits um den „Schutz lebenswichtiger Interessen der betroffenen Person oder anderer Personen oder im Zusammenhang mit Strafprozessen oder anderen gesetzlichen Erfordernissen“ erweitert. (vgl. EU 2007: §1).

Letztendlich werden diese Kategorien im Abkommen von 2012 in vier Paragraphen unterteilt und weiter definiert. So heißt es beispielsweise, dass PNR-Daten zur Ermittlung von Personen verwendet werden können, die bei Grenzübertritt in oder aus den USA einer ausführlichen

Befragung oder Kontrolle unterzogen werden (vgl. EU 2012: Art. 4 III). Dies kann sich insbesondere auf das Grenzmangement, also auf illegale Immigration, beziehen. In der Präambel wird dieser Punkt noch bestärkt, indem das Recht der Staaten, ihre Grenzen zu schützen, explizit Erwähnung findet. Außerdem scheint die Liste an Straftatbeständen nicht abschließend zu sein, da auch „jeglicher sonstige[r] Beitrag zu einer Handlung" (EU 2012: Art. 4 Ia vii) von terroristischen und damit verbundenen Straftaten durch PNR-Daten ermittelt werden darf.

Ähnlich dazu wird auch die grenzüberschreitende Natur von sonstigen Straftaten sehr weit gefasst. So wird Transnationalität beispielsweise durch „beträchtliche" Auswirkungen in einem anderen Land (EU 2012: Art. 4 Ib iv) definiert, wobei nicht klar ersichtlich ist, was dies beinhalten kann. So könnten die US- Behörden, die Zugriff auf die PNR-Daten haben, auch eine Straftat untersuchen, die zwei europäische Länder betrifft, da auch dies ‚grenzüberschreitender Natur' wäre (vgl. Hornung und Boehm 2012: 10).

Insgesamt ist also eine deutliche Zweckerweiterung der Nutzung von PNR-Daten in den Abkommen zu sehen. Die Nutzung wird dabei nicht auf terroristische Straftaten und schwere, transnationale Kriminalität beschränkt sondern beinhaltet beispielsweise das Mittel der Grenzkontrolle, das sich in erster Linie auf Migration bezieht.

DATENERFASSUNG

Die Datenerfassung betrifft Flüge zwischen der USA und der EU (2012: Art. 2 II). Der Übermittlung verpflichtet sind auch Fluggesellschaften, die sich in der EU befinden können (vgl. EU 2012: Art. 2 III).

Die Datenelemente umfassten im Abkommen von 2004 noch 34 Elemente und wurden in den nachfolgenden Abkommen von 2007 und 2012 auf 19 reduziert (vgl. Anhang II), welche fast deckungsgleich zu denen der EU-PNR sind. Diese Reduzierung sei jedoch „ im Wesentlichen kosmetischer Art ist, da es sich dabei um Zusammenlegung und Umbenennung von Datenfeldern statt um tatsächliche Streichungen handelt" (Europäisches Parlament 2007: P.18). So wurden beispielsweise die Datenelemente 26 (Spezielle Service-Anforderungen - OSI) und 27 (Spezielle Service-Anforderungen - SSI/SSR) des ersten Abkommens in einer Kategorie der ‚Allgemeinen Eintragungen' zusammengefasst. (vgl. Anhang II).

Des Weiteren wurden der Zugriff, die Verwendung und die Verarbeitung von sensiblen Daten in den Abkommen von 2007 und 2012 in ‚Ausnahmefällen' gestattet. Dies bezieht sich auf Umstände, in denen „eine Gefahr von Leib und Leben von Personen" besteht (EU 2012: Art. 6 III) Dies war 2004 noch untersagt (vgl. Kommission 2004: §9) und bedeutet so eine direkte Erweiterung der Datenelemente.

DATENÜBERMITTLUNG

Bei den Übermittlungssystemen handelt es sich um Fluggesellschaften, die sich in den USA oder in der EU befinden können (vgl. Datenerfassung). Der Übermittlungsmechanismus erfolgt auch hier elektronisch (vgl. EU 2012: Art. 15 II).

Während die ‚Pull'-Methode der Fluggesellschaften im ersten Abkommen noch bevorzugt wurde (vgl. Kommission 2004: §13), ist im zweiten Abkommen ein Wechsel zur ‚Push'-Methode zu beobachten (vgl. EU 2007: §VII), die auch im aktuellsten Abkommen Anwendung findet (vgl. EU 2012: Art. 15 I).

Die Übermittlung findet zu einem bestimmten Zeitpunkt (96 Stunden vor planmäßigem Abflug) und zu mehreren unbestimmten Zeitpunkten (bei Eingabe neuer PNR-Daten, in regelmäßigen Abständen, nach einem vom DHS festgelegten Zeitplan) statt. Diese „regulären Übermittlungen" können gemäß Art. 15 V (EU 2012) durch Ausnahmefälle erweitert werden, die Fluggesellschaften dazu verpflichten, zwischen den (un-)bestimmten Zeitpunkten erneute Lieferungen zu tätigen.

Im Verglich zum ‚Push'-System von 2007, wurden die Übermittlungszeitpunkte deutlich vermehrt. Im aktuellen Abkommen ist nicht ersichtlich, wann das DHS Zugriff auf PNR-Daten verlangen kann, da es die Zugangsregeln selbst zu bestimmen scheint (vgl. eigener Zeitplan).

DATENSPEICHERUNG

Im Abkommen von 2004 beträgt die Speicherdauer 3,5 Jahre und insgesamt 8 Jahre für Datensätze, auf die während der ersten Periode manuell zugegriffen wurde (vgl. Kommission 2004: §15). Das zweite Abkommen trifft eine Unterscheidung zwischen einer aktiven analytischen Datenbank, in der die PNR für 7 Jahre gespeichert werden, und einer ruhenden Datenbank, in der die PNR für weitere 8 Jahre gespeichert werden, bei denen besondere Zugriffsrechte gelten (vgl. EU 2007: §VII). Im neusten Abkommen von 2012 wurde die aktive Speicherdauer zwar auf 5 Jahre verkürzt, die ruhende Speicherdauer aber auf bis zu 10 zusätzliche Jahre verlängert. Nach den ersten 6 Monaten sind die gleichen Daten zu anonymisieren, wie es die EU-PNR verlangen. Die Unkenntlichmachung kann allerdings „zu Zwecken von Strafverfolgungsmaßnahmen […], einen konkreten Fall, eine konkrete Bedrohung oder ein konkretes Risiko" rückgängig gemacht, das heißt repersonalisiert werden. Nach den 15 Jahren Speicherdauer werden die Daten weder vernichtet (vgl. Kommission 2004: §15), noch gelöscht (2007), sondern „gänzlich anonymisiert" ohne die Möglichkeit der Rückgängigmachung (2012: Art.8 IV). Diese Unterscheidung ist relevant, da das Risiko der

Kenntlichmachung der Daten weiterhin bestehen würde, wenn die Daten nicht vollständig aus dem System gelöscht werden (vgl. Hornung und Boehm 2012: 12).
Zudem wurde die Speicherdauer von sensiblen Daten im Vergleich zwischen 2007 und 2012 erweitert. Die endgültige Löschung der Daten trat 2007 nach 30 Tagen ein (vgl. EU 2007: § III) während 2012 die Daten „30 Tage, *nachdem* das DHS die letzten PNR-Daten mit den sensiblen Daten erhalten hat" (eigene Hervorhebung; EU 2012: Art. 6 IV) gelöscht werden. Daten von Personen, die innerhalb der 30 Tagesfrist mehrere Male fliegen, werden also zusätzlich länger gespeichert (vgl. Hornung und Boehm 2012: 14).

Zusammenfassend ist eine deutliche Erweiterung der Speicherdauer zu erkennen. Die Anonymisierung der Datensätze beinhaltet die Möglichkeit der Rückgängigmachung und stellt damit keine Reduzierung der Speicherung dar, da solche Daten möglicherweise niemals vollständig aus dem System gelöscht werden. Vor allem die erweiterte Speicherdauer von sensiblen Daten lässt Rückschlüsse auf deren Relevanz für den Sicherheitsbereich zu (vgl. 3.3.4).

INSTITUTIONELLER ZUGRIFF UND AUSTAUSCH

Innerstaatlich hat das Bureau of Customs and Border Protection (CBP) des DHS primären Zugriff auf die PNR-Daten, weshalb es sich um ein zentrales institutionelles System handelt (vgl. Kommission 2004: P.10). Dabei kann das CBP Daten auf Fall zu Fall Basis an andere amerikanische oder drittstaatliche Regierungsbehörden weitergeben (vgl. Kommission 2004: §29). Diese „designierten Behörden" müssen (intern wie extern) Terrorismusbekämpfungs- oder Strafverfolgungsaufgaben wahrnehmen und die Weitergabe darf nur zum Zwecke der Verhütung und Bekämpfung der in dem Abkommen aufgeführten Straftaten (vgl. 3.3.1) erfolgen (vgl. Kommission 2004: §29). Zusätzlich können Daten weitergeleitet werden, falls die „Offenlegung zum Schutz lebenswichtiger Interessen des Betroffenen oder anderer Personen, insbesondere im Fall erheblicher *Gesundheitsrisiken*" (Hervorhebung d. Verf.; Kommission 2004: §34) oder bezüglich „Strafprozessen oder anderen gesetzlichen Erfordernissen" notwendig sind (vgl. Kommission 2004: §35).
2007 können Daten vom DHS „in eigenem Ermessen" an US-Behörden weitergeleitet werden, die im „Bereich der Strafverfolgung, der öffentlichen Sicherheit oder der Terrorismusbekämpfung" (EU 2007: §II) tätig sind. Dies diene der Unterstützung der Untersuchung von Fällen, die mit der „Terrorismusbekämpfung, der grenzüberschreitenden Kriminalität und der öffentlichen Sicherheit […] (zu denen unter anderem Bedrohungen, Flüge, Einzelpersonen und problematische Strecken gehören)" zusammenhängen (EU 2007: §

II). Da die Weitergabe nun ‚in eigenem Ermessen', d.h. nicht mehr automatisch auf einer Fall-zu-Fall Basis erfolgt, kann bereits dieser Schritt als Erweiterung der Zugriffsmöglichkeiten von Behörden bewertet werden.
Letztendlich wird in Artikel 16 des Abkommens von 2012 auf die innerstaatliche Weitergabe nach Maßgabe des Artikel 4 verwiesen. Wie oben analysiert, wurden in Artikel 4 die Verwendungszwecke von PNR-Daten deutlich erweitert (vgl. 3.3.1), was nun einer institutionellen Zugriffserweiterung gleich kommt.
Die innerstaatlichen Zugriffs- und Austauschmöglichkeiten wurden also deutlich erweitert.

Während sich die Weitergabe von PNR-Daten an drittstaatliche Behörden 2004 an den internen Bestimmungen (vgl. oben) und im zweiten Abkommen an den rechtlich bestimmten Verwendungszwecken des Abkommens orientierte (vgl. EU 2007: §II), wurde dies im Abkommen von 2012 weiter gefasst.
Hier heißt es, dass Daten nur in konkreten Fällen (vgl. EU 2012: Art 17 III) und nur falls der Empfänger bei der Verwendung der Daten die Bedingungen des Abkommens erfüllt (vgl. EU 2012: Art. 17 I) weitergegeben werden dürfen. Dabei erfolgt kein direkter Verweis auf Bedingungen, die im Abkommen enthalten sind, sodass der für eine Datenweitergabe erforderliche Verwendungszweck unklar bleibt (vgl. Hornung und Boehm 2012: 13). Dies lässt die Schlussfolgerung zu, dass Daten auch für andere Verwendungszwecke als solche, die aus den Abkommen ersichtlich sind, weitergeben werden können, da das DHS selbst über die Zulässigkeit entscheidet (vgl. Hornung und Boehm 2012: 13). Die Weitergabe von „analytischen Informationen" ist außerdem auch an europäische Institutionen wie Europol, Eurojust und anderen Strafverfolgungs- und Justizbehörden möglich (vgl. EU 2012: Art.18).
Trotz der Aufnahme von „ausdrücklichen Vereinbarungen" (EU 2007: §II), die den Datenschutz von EU-PNR verbessern sollen, sowie einer Informationspflicht bei Weitergabe von Daten europäischer Bürgerinnen und Bürger gegenüber dem betroffenen Mitgliedsstaat (vgl. EU 2012: Art. 17 IV), bedeutet die unklare Formulierung und die Erweiterung der Verwendungszwecke von 2012 de facto eine Erweiterung des externen Datenaustauschs (vgl. Hornung und Boehm 2012: 14).

DATENVERARBEITUNG

Die Datenverarbeitung ist in den EU-USA Abkommen relativ intransparent (vgl. auch EU-PNR). Die Modalitäten beziehen sich auf die Handlungen, für die PNR-Daten verarbeitet werden dürfen (vgl. Zweckausweitung), den Austausch und Zugriff, jedoch nicht auf die *Art und Weise* der Verarbeitung. So ist beispielsweise unklar, woran genau eine Bedrohung

erkannt werden kann oder wie Risiken analysiert werden. Es wird nicht erwähnt, ob im Vorhinein Kategorien zur Erkennung von Gefahr festgelegt werden und ob es sich beim Erfassungssystem für PNR-Daten um eine evolutionäres System handelt, bei dem die ‚Fehlerquote' mit in das System aufgenommen wird.

Direkte Erwähnung findet nur die Tatsache, dass die automatisierte Verarbeitung und Verwendung von PNR-Daten, die sich rechtlich nachteilig auf die betroffene Person auswirkt, verboten ist (vgl. EU 2012: Art. 7). Folglich ist eine manuelle Verarbeitung zur Ergreifung von Maßnahmen erforderlich (vgl. EU-PNR).

Aus Sekundärquellen geht hervor, dass die Verarbeitungssysteme in erster Linie dazu beitragen sollen, potentielle Terroristen durch den Abgleich von PNR-Daten mit bestimmten Kontrolllisten zu erkennen. Dabei werden Verdächtige (sogenannte "Selectees") besonderen Kontrollen, beispielsweise bezüglich ihres Gepäcks, unterzogen. Die USA entwickelten vier Systeme dieser Art: das Computer-Assisted Passenger Prescreeing System (CAPPS), das CAPPS II, das Automated Targeting System (ATS) und das Secure-Flight-System. CAPPS, welches erstmals ab den späten 1990er Jahren verwendet wurde und CAPPS II (ab 2003) wurden unter anderem wegen Ineffizienz und hohen Fehlerquoten ausgesetzt. Ab 2006 wurde das ATS eingesetzt, welches aufgrund von Intransparenz und Geheimhaltung bei der Erstellung von ‚Terroristen-Profilen' stark kritisiert wurde. Gleichzeitig mit dem ATS wurde das Secure-Flight-Programm eingeleitet, welches eine einheitliches Screening- System und den Abgleich der PNR mit Beobachtungslisten der Regierung für internationale und nationale Flüge garantieren sollte. (vgl. Hobbing 2010: 87f.)

Trotz der andauernden Kritik (s.o.) ist immernoch unklar, welches Verarbeitungssystem derzeit genau verwendet wird und „ob ATS Vorläufer oder Teil des Secure Flight-Programms ist" (Rötzer 2007). Die generelle Verarbeitung von PNR-Daten wird weitestgehend geheimgehalten (vgl. Hobbing 2008: 51).

3.3.3 EU-USA PNR als Institution

Wie im Kapitel zu EU-PNR (vgl. 3.2) bereits diskutiert, werden durch das Instrument der PNR öffentliche, kollektive Handlungen des Flugverkehrs strukturiert. Dies bezieht sich hauptsächlich auf die Einreise von europäischen Staatsangehörigen in die USA.

Die Strukturierung der gouvernementalen Ebene zeigt sich in der externen Dimension von PNR-Daten deutlich. Balzacq (2008: 91) argumentiert, die PNR-Abkommen zwischen der EU und den USA seien keine gemeinsame Initiative, sondern vielmehr ein Produkt der

amerikanischen Politik nach dem 11. September 2001. Die EU sei durch die Machtunterschiede zwischen den beiden Akteuren (vgl. Kaunert et al. 2012: 485) stark unter Druck geraten und wäre somit auf Verhandlungen eingegangen.

Die Verweigerung des Datenaustauschs von Seiten der EU hätte möglicherweise auch negative Effekte auf andere (Policy-)Bereiche mit sich gezogen, was der EU als Verbündeten der USA hätte schaden können.

Zusätzlich wurde die Verhandlungsmacht der EU durch ‚Memorandums of Understandings' geschwächt. Diese Vereinbarungen betrafen insbesondere neue Mitgliedsstaaten der EU-Erweiterung von 2004[11], die noch nicht Teil der freien Visa-Bestimmungen zwischen den USA und anderen EU Staaten waren. Unter Zugeständnis von weiteren Erlaubnissen, die nicht im EU-USA Abkommen von 2007 enthalten waren, konnten diese Länder Teil des Visa-Waiver-Program (VWP) werden. Unter anderem beinhalteten diese neue zusätzliche Datenerhebung aus betroffenen Mitgliedsstaaten beispielsweise PNR von Personen, die über nicht aber *in* die USA geflogen seien. (vgl. Hobbing 2008: 48f.)

Diese Möglichkeit von bilateralen Vereinbarungen zwischen einzelnen Mitgliedsstaaten und den USA schwächt die Verhandlungsposition der EU in den PNR-Diskussionen, sowie in allen anderen verwandten Bereichen (vgl. Hobbing 2008: 50). Durch die unterschiedlichen Ausgestaltungen des Instruments der PNR wurden also innereuropäische sowie externe Handlungen der Regierungen maßgeblich strukturiert.

3.3.4 Reflektion von spezifischem Bedrohungsbild

DIREKT

In den untersuchten EU-USA Abkommen zeigen sich bestimmte Bedrohungswahrnehmungen direkt im Instrument. Abgesehen vom Fokus auf den Flugverkehr und damit die Transnationalität von Terrorismus (vgl. EU) zeigen die Erweiterungen der Natur und Funktionen des Instruments, dass immer mehr Strafbestände (vgl. 3.3.2) als Bedrohung für die innere Sicherheit eingeordnet werden. Durch das PNR-Instrument werden diese direkt mit der Bekämpfung des Terrorismus in Verbindung gesetzt, obwohl sie selbst keine terroristischen Straftaten darstellen.

[11] Vgl. beispielsweise das Memorandum of Understanding zwischen Tschechien und den USA (27.2.2008): *Memorandum of Understanding between the Ministry of the Interior of the Czech Republic and the Department of Homeland Security of the United States of America regarding the United States Visa Waiver Program and related enhanced Security Measures* [Online] http://www.vlada.cz/scripts/detail.php?id=31921 [eingesehen am 01.07.2015].

Des Weiteren werden durch die Auswertung von PNR direkte „Folgemaßnahmen“ (Kommission 2010a: 4) impliziert. Diese undefinierten Maßnahmen können auf der Grundlage von eingehenden Kontrollen und Befragungen von Individuen (vgl. 3.3.2. Zweck der PNR) beschlossen werden, was insbesondere die illegale Immigration betrifft. Indem PNR-Daten direkt zur Verhinderung von illegaler Immigration beitragen, reflektieren sie das bestimmte Bedrohungsbild, dass auch Migration ein Sicherheitsrisiko darstellt.

INDIREKT

Bedrohungswahrnehmungen zeigen sich auch indirekt im PNR-Instrument. Die konstante Erweiterung des Zwecks, der Datenerfassung, der Zugriffs- und Austauschmöglichkeiten sowie der Speicherdauer, kurz der Natur und Funktionen des Instruments, lassen darauf schließen, dass die Bedrohung als weit verbreitet bzw. schwer zu fassen eingeordnet wird. Sie ist nicht nur „unbekannt“ (vgl. EU-PNR) sondern variabel.

Dieser ‚Unvorhersehbarkeit‘ kann in der Denkweise der versicherheitlichenden Akteure durch die Erfassung von Verhaltens- und Reisemustern entgegen gewirkt werden. Dabei werden auch sensible Daten und indirekte Rückschlüsse auf diese (z.B. Special Service Requests) durch das PNR-Instrument erfasst. Die verlängerte Speicherdauer von sensiblen Daten und damit die längere Einsehbarkeit zeigt zudem auf, dass solche Daten relevant für die innere Sicherheit sind (da sie sonst früher anonymisiert werden könnten). Das bedeutet, dass Dinge wie Ethnie, Gesundheit, Religion und besondere Verhaltensweisen als Quellen der Bedrohung der versicherheitlichenden Akteure (EU und USA) wahrgenommen werden.

Durch die institutionelle Kooperation und die Interoperabilität zwischen verschiedenen Instrumenten wird dieses Bedrohungsbild außerdem indirekt reproduziert. Durch die Verbreitung der ausgewerteten Daten, bestimmt das Instrument auch auf diesem Wege selbst, wer oder was eine Bedrohung darstellt.

3.3.5 Versicherheitlichungsprozesse

Als versicherheitlichendes Instrument würde das Instrument der Passagierdaten ein aktives Tun aufweisen. Durch seine Eigenlogik würde es bestimmte Entitäten durch sein aktives Zutun selbst versicherheitlichen.

SENSIBLE DATEN UND MIGRATION

Wie oben bereits gezeigt wurde, wird das spezifische Bedrohungsbild der Akteure im Instrument verarbeitet. Dadurch können Vermerke zur äußerlichem Erscheinungsbild

(Ethnie), zum Schutz ‚vitaler Interessen'(Gesundheitszustand), sowie zu Essenswünschen (Religion) aufgenommen und verarbeitet werden.
Auch die Wahrnehmung von Migration als Bedrohung wird durch das Instrument direkt in einen Sicherheitskontext transformiert: durch PNR-Daten ist es möglich, im Namen der inneren Sicherheit und Terrorismusbekämpfung gegen Migration vorzugehen bzw. unbestimmte Folgemaßnahmen zu ergreifen – letztendlich also, diese zu versicherheitlichen.

POLITIK AUßERHALB DES ‚REGELFALLS'

Des Weiteren sind die Abkommen zwischen der EU und den USA als eine Politik außerhalb des ‚Regelfalls' einzuordnen. Dabei konnten aufgrund der geäußerten Relevanz für die innere Sicherheit verschiedene Praktiken wie Geheimhaltung, der Ausschluss einer öffentlichen Debatte und starker Zeitdruck legitimiert werden. Unter diesem Mantel der ‚Außnahmepolitik' können sonst umstrittene Instrumente leichter gerechtfertigt und durchgesetzt werden, was zu Versicherheitlichungsprozessen beitragen kann (vgl. 2.2.2).

Wie oben erläutert, sind die Verarbeitung und die Zugriffsmöglichkeiten auf PNR-Daten der betrauten Behörden weitestgehend intransparent und geheim. Die Betonung von Geheimhaltung aus Gründen der inneren Sicherheit wurde von der Kommission selbst kritisiert, nachdem ein Beamter des DHS brieflich die Intention der USA äußerte, Entwurfsdokumente nicht zu veröffentlichen (vgl. Rat 2007). Geheimhaltung ist ein klarer Indikator für die Politik des Besonderen, die sich von den ‚normalen' Umständen abhebt.
Zudem wurde das europäische Parlament von der Verhandlung um das PNR-Abkommen von 2004 ausgeschlossen (vgl. Guild und Brouwer 2006: 2). Auch wäre durch die Verurteilung desselbigen Abkommens durch den Europäischen Gerichtshof (EuGH) der automatische Ausschluss des EP und des EuGH erfolgt, da dieser die falsche juristische Basis bemängelte (vgl. Balzacq 2008: 93f.). Die Verarbeitung von PNR-Daten (2004) wurde infolge dessen unter die dritte Säule statt unter die erste eingeordnet, wodurch sich das Abkommen nicht mehr auf den Transport-, sondern auf den Sicherheitssektor bezieht (vgl. Guild und Brouwer 2006: 3). Dieser Mangel an einer öffentlichen Debatte, kann als Abweichung von der ‚normalen' Politik eingeordnet werden.
Der Zeitdruck, dem die Europäische Union während der verschiedenen Abkommen unterlag, zeige die Ernsthaftigkeit der Situation und sei konträr gegenüber dem „normalen, ziemlich langsamen Ansatz der Kommission, […] ein Gesetz zu ändern" (vgl. Guild und Brouwer 2006: 1). Der Verhandlungsdruck, unter dem die EU stand (vgl. 3.3.3), ist zudem als

Zeitdruck zu bewerten, schnell ein gültiges Abkommen mit den USA zu beschließen, um nicht nachteilige Konsequenzen daraus zu ziehen.
Insgesamt zeigen sich also Praktiken, die von der ‚normalen Politik' abweichen und durch die die Versicherheitlichung der bestimmten Entitäten deutlich verstärkt werden konnte.

4 Zusammenfassung und Fazit

Wie Peters und van Nispen (1998: 2) es ausdrücken, besteht ein großes Recherchepotential in der „ungewissen Natur von Instrumenten". Diese Natur des Instruments der Fluggastdaten wurde in der vorliegenden Arbeit dargestellt. Dabei haben sich die Daten, die ein Passenger-Name-Record enthält, nicht geändert, wohl aber deren Verwendung und Einsatzgebiet. Das Mittel der Fluggesellschaften PNR für kommerzielle Zwecke zu nutzen, wurde durch die postulierte Relevanz für die Bekämpfung des Terrorismus regelrecht zweckentfremdet und konnte dadurch zu einem investigativen Instrument werden.
Im Gegensatz zu anderen Instrumenten der Information die Grenzübertritte betreffen, verfolgten die versicherheitlichenden Akteure mit der Nutzung der Passagierdaten von Anfang an das Ziel, transnationalen Terrorismus zu bekämpfen. Dennoch zeigen sich bereits innerhalb der Vorschläge zu EU-PNR, sowie in den EU-USA PNR, Veränderungen der Reichweite dieses Vorhabens: für beide Dimensionen ist schrittweise eine deutliche Erweiterung der Faktoren zu erkennen, die durch das Instrument der Passagierdaten bekämpft werden müssen (organisierte Kriminalität, schwere Kriminalität). Diese Wahrnehmung von Bedrohung zeigte sich auch hinsichtlich anderer Umstände. Insbesondere der Fokus auf die ‚Unbekanntheit' und ‚Unvorhersehbarkeit' der Bedrohung wird im Instrument reflektiert, was versicherheitlichende Praktiken zu rechtfertigen scheint. Neben dieser Reflektion des Bedrohungsbildes wird dieses zusätzlich durch den institutionellen und instrumentellen Austausch von ausgewerteten Daten reproduziert.
Auf der Grundlage dieser Eindrücke von Dingen, die für die Sicherheit eine Gefahr darstellen, werden letztendlich bestimmte Entitäten versicherheitlicht. Die Eigenlogik des Instruments, d.h. die Prozesse die es umfasst, ist dabei zentral. Erst im Zusammenhang mit dem Verarbeitungs- und Auswertungsmechanismus des Instruments wird deutlich, wie das Instrument aus sich selbst heraus Entitäten zu Bedrohungen transformiert. In den Vorschlägen der EU-PNR sowie den EU-USA PNR Abkommen betrifft dies Entitäten wie ethnische Zugehörigkeit, Religion, Gesundheitszustand und Migration in unterschiedlichen Ausmaßen. Neben diesen klar nennbaren Kategorien sind es auch unbestimmte Verhaltensweisen, die durch das Instrument verarbeitet werden können. Wie in der Arbeit gezeigt wurde, kann auf

der Grundlage dieser Faktoren ein Bedrohungsprofil erstellt werden, welches seinen Ursprung in der subjektiven Bewertung derjenigen findet, die an einem PNR arbeiten. Die automatisierte Auswertung dieser Bedrohungswahrnehmungen und die neue Erstellung von Risikoindikatoren sind es, die PNR zu einem versicherheitlichenden Instrument werden lassen. Der eigene Beitrag den das Instrument zu diesem Profiling leistet, entzieht sich so der diskursiven Logik und ist erst durch die genaue Betrachtung der Charakteristika von PNR zu verstehen.

Zusammenfassend kann eine Art Wirkungskette wie folgt dargestellt werden: im Instrument wird festgelegt, wer oder was eine Bedrohung ist, denn dies kann offensichtlich aus seinen Datenelementen (u.a. durch Erfassung von Verhaltensweisen und sensiblen Daten) erkannt werden. Durch Profiling-Mechanismen können so bestimmte Entitäten durch das Instrument selbst versicherheitlicht werden. Dabei hat es außerdem direkte und indirekte Effekte zur Folge: die polizeiliche und strafrechtliche Verfolgung als ‚Daten-getriebene Handlung' sowie die Verbreitung der impliziten Bedrohungswahrnehmung durch den Austausch zwischen Institutionen und anderen Instrumenten ist bereits im PNR-Instrument angelegt.
Versicherheitlichungsprozesse konnten ferner durch eine Politik außerhalb des ‚Regelfalls' erleichtert werden. Dies ist wenigstens für die bestehenden EU-USA PNR Abkommen der Fall. Obwohl sich Tendenzen dieser ‚Außnahmepolitik' auch in EU-PNR zeigen, ist hier das letzte Wort noch nicht gesprochen: Die formale Unterstützung des europäischen Parlaments ist nicht eindeutig, da dieses beständig Kritik an dem Vorhaben äußerte. Auch bei den Bürgerinnen und Bürgern, die direkt von den PNR betroffen wären, regt sich Widerstand[12]. Damit sind die formale und moralische Unterstützung des Instruments und damit die erfolgreiche Versicherheitlichung auf europäischer Ebene noch abzuwarten.

[12] Vgl. zum Beispiel [online] http://www.nopnr.org/ [eingesehen am 18.06.2015].

Anhang I EU-PNR Datenelemente (2012)

EU-PNR Datenelemente des Richtlinienvorschlags des Rats der EU von 2012

(vgl. Rat 2012: Anhang I, S.31f)

(1) PNR-Buchungscode (Record Locator)

(2) Datum der Buchung/Flugscheinausstellung

(3) Planmäßiges Abflugdatum bzw. planmäßige Abflugdaten

(4) Name(n)

(5) Anschrift und Kontaktangaben (Telefonnummer, E-Mail-Adresse)

(6) Alle Arten von Zahlungsinformationen einschließlich Rechnungsanschrift

(7) Gesamter Reiseverlauf für eine bestimmte Buchung

(8) Vielflieger-Eintrag

(9) Reisebüro/Sachbearbeiter

(10) Reisestatus des Fluggasts mit Angaben über Reisebestätigungen, Eincheckstatus, nicht angetretene Flüge (No show) und Fluggäste mit Flugschein, aber ohne Reservierung (Go show)

(11) Angaben über gesplittete/geteilte Buchungen

(12) Allgemeine Hinweise (einschließlich aller verfügbaren Angaben zu unbegleiteten Minderjährigenunter 18 Jahren, wie beispielsweise Name und Geschlecht des Minderjährigen, Alter, Sprache(n), Name und Kontaktdaten der Begleitperson beim Abflug und Angabe, in welcher Beziehung diese Person zu dem Minderjährigen steht, Name und Kontaktdaten der abholenden Person und Angabe, in welcher Beziehung diese Person zu dem Minderjährigen steht, begleitender Flughafenmitarbeiter bei Abflug und Ankunft)

(13) Flugscheindaten (Flugscheinnummer, Ausstellungsdatum, einfacher Flug (One-way), automatische Tarifanzeige (Automated Ticket Fare Quote fields)

(14) Sitzplatznummer und sonstige Sitzplatzinformationen

(15) Code-Sharing

(16) Vollständige Gepäckangaben

(17) Zahl und Namen von Mitreisenden im Rahmen einer Buchung

(18) Etwaige erweiterte Fluggastdaten (API-Daten) (unter anderem Art des Dokuments, Nummer des Dokuments, Staatsangehörigkeit, Ausstellungsland, Ablaufdatum des Dokuments, Familienname, Vorname, Geschlecht, Geburtsdatum, Fluggesellschaft, Flugnummer, Tag des Abflugs, Tag der Ankunft, Flughafen des Abflugs, Flughafen der Ankunft, Uhrzeit des Abflugs, Uhrzeit der Ankunft)

(19) Alle vormaligen Änderungen der unter den Nummern 1 bis 18 aufgeführten PNR-Daten.

Anhang II Vergleichende Tabelle der PNR-Datenelemente aus den PNR- Abkommen zwischen der EU und den USA

Tabelle 1: Vergleich der Datenelemente der EU-USA PNR I, II, III

EU-USA Abkommen 2004	EU-USA Abkommen 2007	EU-USA Abkommen 2012
1. PNR-Buchungscode (Record Locator)	1. PNR-Buchungscode (Record Locator)	1. PNR-Buchungscode (Record Locator Code)
2. Datum der Reservierung	2. Datum der Reservierung / der Ausstellung des Flugscheins	2. Datum der Buchung bzw. der Ausstellung des Flugscheins
3. Geplante Abflugdaten	3. Geplante Abflugdaten	3. Datum bzw. Daten des geplanten Flugs
4. Name	4. Name(n)	4. Name(n)
5. Andere Namen im PNR	5. Verfügbare Vielflieger- und Bonus-Daten (d. h. Gratisflugscheine, Upgrades usw.)	5. Verfügbare Vielflieger- und Bonus-Daten (d.h. Gratisflugscheine, Upgrades usw.)
6. Anschrift	6. Andere Namen im PNR, einschließlich Zahl der Reisenden im PNR	6. Andere Namen in dem PNR-Datensatz, einschließlich der Anzahl der in dem Datensatz erfassten Reisenden
7. Zahlungsart	7. Alle verfügbaren Kontaktinformationen (einschließlich Auftraggeberinformationen)	7. Sämtliche verfügbaren Kontaktinformationen, einschließlich Informationen zum Dateneingeber
8. Rechnungsanschrift	8. Alle verfügbaren Zahlungs-/Abrechnungsinformationen (ohne weitere Transaktionsdetails für eine Kreditkarte oder ein Konto, die nicht mit der die Reise betreffenden Transaktion verknüpft sind)	8. Sämtliche verfügbaren Zahlungs-/Abrechnungs-informationen (ohne weitere Transaktionsdetails für eine Kreditkarte oder ein Konto, die nicht mit der die Reise betreffenden Transaktion verknüpft sind)
9. Telefonnummern	9. Reiseverlauf für den jeweiligen PNR	9. Von dem jeweiligen PNR-Datensatz erfasste Reiseroute
10. Gesamter Reiseverlauf für den jeweiligen PNR	10. Reisebüro/Sachbearbeiter des Reisebüros	10. Reisebüro
11. Vielflieger-Eintrag (beschränkt auf abgeflogene Meilen und Anschrift(en))	11. Code-Sharing-Informationen	11. Code-Sharing-Informationen
12. Reisebüro	12. Informationen über Aufspaltung/Teilung einer Buchung	12. Informationen über Buchungssplitting bzw. –teilung
13. Bearbeiter	13. Reisestatus des Fluggastes (einschließlich Bestätigungen und Eincheckstatus)	13. Reisestatus des Fluggastes (einschließlich Bestätigungen und Eincheckstatus)
14. Codeshare-Information im PNR	14. Informationen über Flugscheinausstellung (Ticketing), einschließlich Flugscheinnummer, Angabe, ob Flugschein für einfachen Flug (One Way), sowie Automatic Ticket Fare Quote (automatische Tarifabfrage)	14. Flugscheininformationen (Ticketing Information), einschließlich Flugschein-nummer, Hinweis auf einen etwaigen einfachen Flug (One Way Ticket) und automatische Tarifanzeige (Automatic Ticket Fare Quote)
15. Reisestatus des Passagiers	15. Sämtliche Informationen zum Gepäck	15. Sämtliche Informationen zum Gepäck

Tabelle 1. Inhalt

16. Informationen über die Splittung/Teilung einer Buchung	16. Sitzplatzinformationen, einschließlich Sitzplatznummer	16. Sitzplatznummer und sonstige Sitzplatzinformationen
17. E-Mail-Adresse	17. Allgemeine Bemerkungen einschließlich OSI, SSI und SSR	17. Allgemeine Eintragungen einschließlich OSI-, SSI- und SSR-Informationen
18. Informationen über Flugscheinausstellung (Ticketing)	18. Etwaig erfasste APIS-Daten	18. Etwaige APIS-Informationen
19. Allgemeine Bemerkungen	19. Historie aller Änderungen der unter den Nummern 1 bis 18 aufgeführten PNR	19. Historie aller Änderungen in Bezug auf die unter den Nummern 1 bis 18 aufgeführten PNR-Daten
20 Flugscheinnummer		
21. Sitzplatznummer		
22. Datum der Flugscheinausstellung		
23. Historie über nicht angetretene Flüge (no show)		
24. Nummern der Gepäckanhänger		
25. Fluggäste mit Flugschein aber ohne Reservierung (Go show)		
26. Spezielle Service-Anforderungen (OSI — Special Service Requests)		
27. Spezielle Service-Anforderungen (SSI/SSR — Special Service Requests)		
28. Information über den Auftraggeber (received from)		
29. Alle Änderungen der PNR (PNR-History)		
30. Zahl der Reisenden im PNR		
31. Sitzplatzstatus		
32. Flugschein für einfache Strecken (one-way)		
33. Etwaige APIS-Informationen		
34. ATFQ-Felder (automatische Tarifabfrage)		

Quelle: eigene Zusammenstellung der Autorin basierend auf den Dokumenten EU (2004), EU (2007) und EU (2012

Balzacq, Thierry (2005): The Three Faces of Securitization. Political Agency, Audience and Context, in: *European Journal of International Relations*, Vol.11, Nr.2, S.171-201.

Balzacq, Thierry (2008): The Policy Tools of Securitization. Information Exchange, EU Foreign and Interior Policies, *Journal of Common Market Studies*, Vol. 46, Nr.1, S. 75-100.

Balzacq, Thierry (2010a): Constructivism and securitization studies, in: Myriam Dunn Cavelty, Victor Mauer (Hg.), *The Routledge Handbook of Security Studies*, Oxon: Routledge, S.56-72.

Balzacq, Thierry, Tugba Basara, Didier Bigo, Emmanuel-Pierre Guittet und Christian Olsson (2010b): Security Practices, in: Robert A. Denemark (Hg), *International Studies Encyclopedia Online*. Blackwell, S.1 - 30.

Balzacq, Thierry (Hg.) (2011): *Securitization Theory. How security problems emerge and dissolve*, Oxon: Routledge.

Bigo, Didier und Anastassia Tsoukala (2008): *Terror, Insecurity and Liberty. Illiberal practices of liberal regimes after 9/11*, Oxon: Routledge.

Bigo, Didier (2008): International Political Sociology, in: Paul D. Williams (Hg.), *Security Studies. An Introduction*, 2. Aufl., Oxon: Routledge, S.120-133.

Bigo, Didier, Sergio Carrera, Ben Hayes, Nicolas Hernanz, Julien Jeandesboz (2012): Evaluating current and forthcoming proposals on JHA databases and a smart borders system at EU external borders, in: Europäisches Parlament (Hg.), *Study for the LIBE committee, Directorate General for internal Policies, Policy Department C, Citizens' Rights and Constitutional Affairs*, , PE 462.513, Brüssel, S.1-91.

Bigo, Didier (2014): The (in)securitization practices of the three universes od EU border control. Military/Navy – border guards/police – database analysts, in: *Security Dialogue*, Vol. 45, Nr. 3, S.209-225.

Bigo, Didier, Evelien Brouwer, Sergio Carrera, Elsbeth Guild, Emmanuel-Pierre Guittet, Julien Jeandesboz, Francesco Ragazzi, Amandine Scherrer (2015): The EU Counter-Terrorism Policy Responses to the Attacks in Paris. Towards an EU Security and Liberty Agenda, in: *CEPS Papers in Liberty and Security in Europe*, Nr. 81, S.1-18.

Boehm, Franziska (2010): Tit for Tat. Europe's revenge for the Canadian and US-American PNR systems? The envisaged European model of analyzing flight passenger data, in: *Europäische Rechtsakademie Forum*, Nr.11, S.251-261.

Brouwer, Evelin (2006): Data Surveillance and Border Control in the EU. Balancing Efficiency and Legal Protection, in: Thierry Balzacq, Sergio Carrera (Hg), *Security versus Freedom? A Challenge for Europe's Future*, Hampshire: Ashgate Publishing Limited, S.137- 154.

Brouwer, Evelin (2009): The EU Passenger Name Record (PNR) System and Human Rights-Transferring Passenger Data or Passenger Freedom? In: *CEPS Working Document*, Nr. 320, S. 1-30.

Bures, Oldrich (2006): EU Counterterrorism Poliy. A Paper Tiger? In: Terrorism and Political Violence, Nr.18, S.57-78.

Buzan, Barry, Ole Waever und Jaap de Wilde (1998): *Security. A new Framework for Analysis*, Boulder: Lynne Rienner Publishers.

Chistyakova, Yulia (2015): Democratic legitimacy, effectiveness and impact of EU counter-terrorism measures, in: Fiona de Londras und Josephine Doody (Hg.): *The Imapact, Legitimacy and Effectiveness of EU Counter Terrorism*, Oxon: Routledge, S. 114-135.

De Bruijn, Hans und Hans A.M. Hufen (1998): The Traditional Approach to Policy Instruments, in: Guy B. Peters und Frans K.M. van Nispen (Hg.), *Public Policy Instruments. Evaluating the Tools of Public Administration*, Cheltenham: Edward Elgar, S.1-32

Europäische Agentur für Grundrechte (2011): *Gutachten der Agentur der Europäischen Union für Grundrechte betreffend den Vorschlag für eine Richtlinie über die Verwendung von Fluggastdatensätzen zu Zwecken der Verhütung, Aufdeckung, Aufklärung und strafrechtlichen Verfolgung von terroristischen Straftaten und schwerer Kriminalität (KOM(2011) 32 endgültig). FRA-Gutachten – 1/2011 Fluggastdatensätze*, Wien, 14. Juni 2011.

Europäische Gemeinschaft (2004): *Agreement between the European Community and the United States of America on the Processing and Transfer of PNR Data by Air Carriers to the United States Department of Homeland Security, Bureau of Customs and Border Protection. CE/USA/en*, (o.O.),(o.D.).

Europäische Kommission (2004): Entscheidung der Kommission vom 14. Mai 2004 über die Angemessenheit des Schutzes der personenbezogenen Daten, die in den Passenger Name Records enthalten sind, welche dem United States Bureau of Customs and Border Protection übermittelt werden. (Bekannt gegeben unter Aktenzeichen K(2004) 1914), L 235/11, in: *Amtsblatt der Europäischen Union*, 14.5.2004.

Euopäische Kommission (2010a): *Mitteilung der Kommission über das sektorübergreifende Konzept für die Übermittlung von Fluggastdatensätzen (PNR) an Drittländer. KOM(2010) 492 endgültig*, Brüssel, 21.9.2010.

Europäische Kommission (2010b): *Mitteilung der Kommission an das Europäische Parlament und den Rat. Überblick über das Informationsmanagement im Bereich Freiheit, Sicherheit und Recht. KOM(2010) 385 endgültig*, Brüssel, 20.7.2010.

Europäische Kommission (2011a): *Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über die Verwendung von Fluggastdatensätzen zu Zwecken der Verhütung, Aufdeckung, Aufklärung und strafrechtlichen Verfolgung von terroristischen Straftaten und schwerer Kriminalität. KOM(2011) 32 endgültig*, Brüssel, 2.2.2011.

Europäische Kommission (2011b): *Arbeitsdokument der Kommissionsdienstellen. Zusammenfassung der Folgenabschätzung. Begleitdokument zum Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über ein gemeinsames Konzept für die Verwendung von Fluggastdaten. SEK(2011) 133 endgültig*, Brüssel, 02.02.2011.

Europäische Kommission (2015a): *Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen. Die europäische Sicherheitsagenda. COM(2015) 185 final*, Straßbourg, 28.4.2014.

Europäische Kommission (2015b): *EU PNR – the way forward. Following the Orientation Debate of 21 January 2015 on the European Agenda on Security*, (keine Dokumentennr.), (o.O.), [online] http://www.statewatch.org/news/2015/jan/eu-com-2015-01-26-pnr-compromise-note.pdf [eingesehen am 01.7.2015].

Europäisches Parlament (2007): *Abkommen über Fluggastdatensätze (PNR) mit den USA. Entschließung des Europäischen Parlaments vom 12. Juli 2007 zum Abkommen mit den Vereinigten Staaten von Amerika über Fluggastdatensätze. P6_TA(2007)0347*, (o.O.), (o.D.).

Europäisches Parlament (2015): *Entschließung des Europäischen Parlaments vom 11. Februar 2015 zu Maßnahmen zur Terrorismusbekämpfung. 2015/2530(RSP)*, (o.O.), 11.2.2015.

Europäische Union (2007): Abkommen zwischen der Europäischen Union und den Vereinigten Staaten von Amerika über die Verarbeitung von Fluggastdatensätzen (Passenger Name Records — PNR) und deren Übermittlung durch die Fluggesellschaften an das United States Department of Homeland Security (DHS) (PNR-Abkommen von 2007). L 2014/18, in: *Amtsblatt der Europäischen Union*, 4.8.2007.

Europäische Union (2012): Abkommen zwischen den Vereinigten Staaten von Amerika und der Europäischen Union über die Verwendung von Fluggastdatensätzen und deren

Übermittlung an das United States Department of Homeland Security. L 215/5, in: *Amtsblatt der Europäischen Union*, 11.8.2012.

Foucault, Michel (1978): *Dispositive der Macht. Über Sexualität, Wissen und Wahrheit*, Berlin: Merve Verlag.

Guild, Elspeth und Evelin Brouwer (2006): The Political Life of Data. The ECJ Decision on the PNR Agreement between the EU and the US, in: *CEPS Policy brief*, Nr. 109, S.1-6.

Hailbronner, Kay, Vagelis Papakonstantinou und Marcel Kau (2008): The Agreement on Passenger-Data Transfer (PNR) and the EU-US Cooperation in Data Communication, in: *International Migration*, Vol. 46, Nr.2, S.187-197.

Hayes, Ben und Chris Jones (2015): Taking stock. The evolution, adoption, implementation and evaluation of EU counter-terrorism policy, in: Fiona de Londras und Josephine Doody (Hg.): *The Imapact, Legitimacy and Effectiveness of EU Counter Terrorism*, Oxon: Routledge, S.13-39.

Hobbing, Peter (2008): Tracing Terrorists. The EU-Canada Agreement in PNR Matters, in: *CEPS Special Report*, (o. V.), (o. Nr.), S.1-71.

Hobbing, Peter (2010): Tracing terrorists. The European Union-Canada Agreement on Passenger Name Record (PNR) matters, in: Mark B. Salter (Hg.), *Mapping Transatlantic Security Relations. The EU, Canada, and the war on terror. Routledge Studies in liberty and security*, Oxon: Routledge, S. 73-97.

Hornung, Gerrit und Franziska Boehm (2012): Comparative Study on the 2011 draft Agreement between the United States of America and the European Union on the use and transfer of Passenger Name Records (PNR) to the United States Department of Homeland Security, (*keine Journalveröffentlichung*), Passau/Luxembourg.

International Civil Aviation Organization (ICAO) (2010): *Guidelines on Passenger Name Record (PNR) Data. Doc. 9944*, Montréal.

Jackson, Richard (2007): An analysis of EU counterterrorism discourse post-September 11, in: *Cambridge Review of International Affairs*, Vol. 20, Nr. 2, S.233-247.

Kaunert, Christian, Sarah Léonard und Alex MacKenzie (2012): The social construction of an EU interest in counter-terrorism. US influence and internal struggles in the cases of PNR and SWIFT, in: *European Security*, Vol. 21, Nr. 4, S.474-496.

Kommission der Europäischen Gemeinschaften (2005): *Mitteilung der Kommission an den Rat und das europäische Parlament über die Verbesserung der Effizienz der europäischen Datenbanken im Bereich Justiz und Inneres und die Steigerung ihrer Interoperabilität sowie der Synergien zwischen ihnen, KOM(2005)597 endgültig*, Brüssel, 24.11.2005.

Kommission der Europäischen Gemeinschaften (2007): *Vorschlag für einen Rahmenbeschluss des Rates über die Verwendung von Fluggastdatensätzen (PNR-Daten) zu Strafverfolgungszwecken, KOM(2007) 654 endgültig*, Brüssel, 6.11.2007.

Leese, Matthias (2014): The new profiling. Algorithms, black boxes, and failure of anti-discriminatory safeguards in the European Union, in: *Security Dialogue*, Vol. 45, Nr. 5, S. 494-51.

Lum, Cynthia, Leslie W. Kennedy und Alison Sherley (2006): Are counter-terrorism strategies effective? The results of the Campbell systematic review on counter-terrorism evaluation research, in: *Journal of Experimental Criminology*, Nr.2, S.489-516.

Ministerkomitee des Europäischen Rates (2010): *The protection of individuals with regard to automatic processing of personal data in the context of profiling. Recommendation CM/Rec(2010)13 and explanatory memorandum*, Strasbourg: Council of Europe Publishing, S.1-55.

Monar, Jörg (2007): Common Threat and Common Response? The European Union's Counter Terrorism Strategy and it's Problems, in: *Government and Opposition*, Vol. 42, Nr. 3, S. 292-313.

Nino, Michele (2010): The protection of personal data in the fight against terrorism. New perspectives of PNR European Union Instruments in the light of the Treaty of Lisbon, in: *Utrecht Law Review*, Vol. 6, Issue 1, S.62-85.

Pawlak, Patryk (2009): Made in the USA? The Influence of the US on the EU's Data Protection Regime, in: *CEPS Liberty and Security in Europe*, (o. V.), (o. Nr.), S.1-24.

Peters, Guy B. und Frans K.M. van Nispen (Hg.) (1998): *Public Policy Instruments. Evaluating the Tools of Public Administration*, Cheltenham: Edward Elgar.

Peters, Guy B. (2002): The Politics of Tool Choice, in: Lester M. Salamon (Hg.), *The Tools of Government. A Guide to the New Governance*, New York: Oxford University Press, S. 552-584.

Rat der Europäischen Union (2004): Richtlinie 2004/82/EG des Rates vom 29. April 2004 über die Verpflichtung von Beförderungsunternehmen, Angaben über die beförderten Personen zu übermitteln. L 261/24, in: *Amtsblatt der Europäischen Union*, 29.4.2004.

Rat der Europäischen Union (2005): *Strategie der Europäischen Union zur Terrorismusbekämpfung. 14469/4/05 REV 4*, Brüssel, 30.11.2005.

Rat der Europäischen Union (2007): *Agreement between the European Union and the United States of America on the processing and transfer of passenger name record (PNR) data by air carriers to the United States Department of Homeland Security (DHS) - Letter on confidentiality of negotiation documents. 12307/07 LIMITE*, Brussels, 31.8.2007.

Rat der Europäischen Union (2008): Rahmenbeschluss 2008/841/JI des Rates vom 24. Oktober 2008 zur Bekämpfung der organisierten Kriminalität. L 300/42, in: *Amtsblatt der Europäischen Union*, 11.11.2008.

Rat der Europäischen Union (2002): Rahmenbeschluus 2002/584/JI des Rates vom 13. Juni 2002 über den Europäischen Haftbefehl und die Übergabeverfahren zwischen den Mitgliedstaaten. L 190/1, in: *Amtsblatt der Europäischen Union*, 18.7.2002.

Rat der Europäischen Union (2009): *Note. Proposal for a Council Framework Decision on the use of Passenger Name Record (PNR) for law enforcement purposes. 5618/2/09 REV 2*, Brussels, 29.6.2009.

Rat der Europäischen Union (2011): *Note. Proposal for a directive of the European Parliament and of the Council on the use of Passenger Name Record data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime. 6361/11*, Brussels, 11.2.2011.

Rat der Europäischen Union (2012): *Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über die Verwendung von Fluggastdatensätzen zu Zwecken der Verhütung, Aufdeckung, Aufklärung und strafrechtlichen Verfolgung von terroristischen Straftaten und schwerer Kriminalität. 8916/12*, Brüssel, 23.4.2012.

Rat der Europäischen Union (2015): *Grundzüge der Terrorismusbekämpfungsstrategie für Syrien und Irak, mit besonderer Schwerpunktsetzung auf ausländische Kämpfer. 5369/15*, Brüssel, 16.1.2015.

Rötzer, Florian (2007): Von der Verlässlichkeit von Antiterrorlisten, *Heise-Online*, Telepolis, [online] http://www.heise.de/tp/artikel/25/25058/1.html [eingesehen am 01.07.2015], 12.4.2007.

Salamon, Lester M. (2002): The New Governance and the Tools of Public Action. An Introduction, in: Lester M. Salamon (Hg.), *The Tools of Government. A Guide to the New Governance*, New York: Oxford University Press, S.1-47.

Schneider, Anne und Helen Ingram (1990): Behavioral Assumptions of Policy Tools, in: *The Journal of Politics*, Vol. 52, Nr. 2, S.510-529.

Vedung, Evert (1998): Policy Instruments. Typologies and Theories, in: Marie-Louise Bemelmans-Videc, Ray C. Rist und Evert Vedung (Hg.): *Carrots, Sticks & Sermons. Policy Instruments & Their Evaluation*, New Brunswick: Transaction Publishers, S.21-58.

Ich versichere, dass ich die vorgelegte Bachelorarbeit eigenständig und ohne fremde Hilfe verfasst, keine anderen als die angegebenen Quellen verwendet und die den benutzten Quellen entnommenen Passagen als solche kenntlich gemacht habe. Die eingereichte Arbeit wurde bisher keiner anderen Prüfungsbehörde vorgelegt.

Unterschrift München, den 12. Juli 2015