Teil III Sicherheit als Präemption, Autonomie als Infragestellung. Theoretische und normative Anregungen

> The story is sometimes told of the man who was lost somewhere in Scotland, and asked a farmer if he could tell him which was the way to Edinburgh. 'Oh sir,' the farmer replied, 'if I were you, I shouldn't start from here!'
>
> H. Bull, *The Anarchical Society*, 295

> Recognizing what we say, what we do, what we feel, who we are, can mean giving up some dreams of change as impossible; but it can also be a foundation – perhaps the only effective foundation – for genuine change.
>
> H. F. Pitkin, *Wittgenstein and Justice*, 338

Kapitel 8 Ein neuer sicherheitspolitischer Ansatz: Grundeigenschaften und Herausforderungen für die normative Ordnung

1 Die Logik der EU-Sicherheitspolitik im RFSR

In diesem Kapitel werde ich die Argumentationsfäden, die sich vom dritten bis zum siebten Kapitel des Buches erstrecken, zusammenziehen und dabei versuchen, die Haupttendenzen der EU-Sicherheitspolitik im RFSR zu fixieren. Die Analyse der Fallbeispiele hat gezeigt, dass sich das Sicherheitskonzept im Laufe des Aus- und Aufbaus des RFSR verändert hat.[762] Nicht nur hat Sicherheit Priorität vor den anderen beiden Konzepten der Trias und dabei auch vor Freiheit als logischem Kernelement gewonnen. Sicherheit droht am Ende auch diese ursprüngliche Idee der Freiheit als Freizügigkeit wieder einzuschränken. Dabei hat Sicherheit vor allem eine präemptive Komponente hinzugewonnen, die sie sowohl von präventiven als auch von reaktiven Modellen der Sicherheit unterscheidet.[763]

Daher können meines Erachtens die zwei bedeutendsten Eigenschaften der aktuellen EU-Sicherheitspolitik als Zirkularität und Präemption zusammengefasst werden. In welchem Sinn der sicherheitspolitische Ansatz der EU als zirkulär bezeichnet werden kann, wird im nächsten Abschnitt verdeutlicht. Dabei werde ich auf die Entwicklung des RFSR im Allgemeinen, die ich insbesondere in den Kapiteln 3 und 7 nachverfolgt habe,

762 Für eine Kontextualisierung des Wandels von Sicherheitskonzeptionen in der Moderne vgl. den zweiten Teil von Zoche; Kaufmann; Haverkamp (Hg.), *Zivile Sicherheit. Gesellschaftliche Dimensionen gegenwärtiger Sicherheitspolitiken* und insbesondere die Beiträge von Wolfgang Bonß, Hans-Jörg Albrecht, Rudolf Egg und Christopher Daase.

763 Eine unterschiedliche Kategorisierung wird von Ulrich Bröckling vorgeschlagen, wonach nicht scharf zwischen Prävention und Präemption unterschieden wird und präemptive Strategien zum allgemeinen Modell der Prävention gehören. Jedoch differenziert Bröckling *innerhalb* der Prävention zwischen drei „Vorbeugungsregimen": Hygiene als Verhütung von Infektionskrankheiten, Immunisierung und Vorsorgeprinzip. Dieses letzte Prinzip, insbesondere in der von Bröckling beschriebenen zweiten, post-9/11-Variante, stimmt meiner Meinung nach in groben Linien mit dem von mir im Folgenden skizzierten Modell der präemptiven Sicherheit überein. Vgl. Bröckling, Ulrich, *Gute Hirten führen sanft. Über Menschenregierungskünste*. Berlin: Suhrkamp 2017, 73–112.

Bezug nehmen. Im dritten Abschnitt dieses Kapitels arbeite ich die Rationalität der Sicherheitsmaßnahmen aus, die sich mehr und mehr als kennzeichnend für den sicherheitspolitischen Ansatz der EU erweist: das präemptive Sicherheitsmodell. Dabei werde ich mich zunächst auf die Analysen der drei Fallbeispiele, insbesondere der PNR-Richtlinie, stützen, die ich in den Kapiteln 4, 5 und 6 durchgeführt habe.

2 *Zirkuläre Sicherheit*

2.1 Von der Unterstützung des Marktes zum selbstständigen Zweck

Im siebten Kapitel dieses Buches habe ich die Analysen der speziellen Maßnahmen mit der allgemeinen Entwicklung der Sicherheitspolitik im RFSR in Verbindung gebracht.

Das ursprüngliche Phänomen, das die Maßnahmen im RFSR hervorgebracht hat, ist der europäische freie Markt mit seinen Grundfreiheiten. Diese Grundfreiheiten beziehen sich auf die freie Zirkulation der Waren, Personen, Dienstleistungen und des Kapitals. Es ist also ein sehr spezifisches Konzept von Freiheit, das hier realisiert werden soll, nämlich Freiheit als Freizügigkeit. Individuen sollen sich frei bewegen können, und die Hindernisse dazu müssen abgebaut werden. Staaten müssen also auf ihre Grenzkontrollen womöglich verzichten. Das bedeutet nur auf den ersten Blick eine Zurückhaltung der öffentlichen Gewalt, denn um zu garantieren, dass das Potenzial des freien Marktes sich voll entfalten kann und die Bedingungen der freien Zirkulation erhalten bleiben, bedarf es aktiver, öffentlicher Interventionen. Der Impuls für den Ausbau der Sicherheitsmaßnahmen ergibt sich aus dieser Logik: Es soll gesichert werden, dass die freie Zirkulation von Menschen, Waren, Dienstleistungen und Kapital reibungslos funktioniert. Der europäische freie Markt ist also das ursprüngliche Phänomen, das den Impuls für die Schaffung des RFSR gab. In diesem Raum ist Freiheit als Freizügigkeit der ursprüngliche Begriff und Wert: Die anderen beiden Begriffe, nämlich Sicherheit und Recht, sind gegenüber dem Freiheitsbegriff funktional.

In dem Prozess, im Rahmen dessen die Sicherheitsmaßnahmen im RFSR realisiert werden, findet jedoch ein Umbruch statt. Die ergriffenen Sicherheitsmaßnahmen sind keine Antwort auf ein konkretes *Sicherheits*problem und scheinen bald eine eigene, von den Herausforderungen des freien Marktes losgelöste Logik zu entfalten. Tatsächlich wurde durch die Implementierung des freien Marktes ein erwarteter Anstieg der Krimi-

nalität, etwa durch Studien des BKA, belegt. Dessen Ursachen wurden aber vor allem in der freien Zirkulation der Waren und des Kapitals ausgemacht und hätten eine gestiegene Kontrolle dieser erfordert. Der Ausbau der Kontrolle fokussiert sich aber im RFSR auf Personen und wird als eine Kompensation des Wegfalls der Grenzkontrollen gerechtfertigt. Die Verbindung zwischen Abbau der Personenkontrolle an den Grenzen und dem Anstieg der Kriminalität wurde dabei jedoch weder im Vorfeld plausibilisiert noch im Nachhinein überprüft. Nichtsdestotrotz findet eine doppelte Verschiebung statt: von der Grenzkontrolle zur Sicherheit durch grenzunabhängige Personenkontrolle und von Waren und Kapital auf Personen.

Die Sicherheitsmaßnahmen des RFSR sind also im Kern eine Form der Personenkontrolle, die sich von der ursprünglichen Logik der Kompensation als Pendant des freien Marktes losgelöst und sich über seine Grenzen hinaus verbreitet hat. Das Sicherheitsargument hat als Machtkatalysator funktioniert, der die für gültig gehaltene Legitimitätsschwelle absinken ließ. Denn je ernster das Sicherheitsproblem, auf das eine Antwort gegeben werden soll, desto niedriger sind die Standards, die eingehalten werden müssen, damit „die Lösung nicht Teil des Problems" wird. Folgerichtig ist nunmehr die Kraft, die den Machtausbau im RFSR vorantreibt, nicht mehr vom ursprünglichen Bereich des Marktes bestimmt, sondern entspringt aus einer Eigenlogik. Es ist die Logik der Lückenschließung, wonach durch die Abdeckung bestimmter Phänomene diejenigen sichtbar werden, die durch Kontrolle noch nicht abgedeckt werden und die damit neue Maßnahmen hervorrufen. Dabei ist Sicherheit durch grenzunabhängige Personenkontrolle ein Zweck an sich geworden, der sich unabhängig von den Herausforderungen des freien Marktes rechtfertigen lässt.

2.2 Die „Logik der Lückenschließung" des EU-Informationsaustauschs und seine Paradoxa

Im Zuge dieses Ausbaus, wie im siebten Kapitel dargestellt, haben die europäischen Datenbanken des RFSR im letzten Jahrzehnt eine signifikante Ausdehnung erlebt. Diese ist auf verschiedenen Ebenen erfolgt.

Erstens ist die Verflechtung zwischen Sicherheitsgewährleistung sowie Grenz- und Migrationspolitik verstärkt worden. Während das SIS und das VIS von Anfang an als Systeme mit dieser doppelten Funktion gedacht waren, ist der Einsatz von Eurodac für Strafverfolgungs- und Gefahrenabwehrzwecke erst nachträglich im Jahr 2013 eingeführt worden. Auch

die geplante zunehmende Vernetzung dieser Systeme untereinander läuft einer Trennung dieser Zwecke zuwider.

Zweitens ist eine Ausdehnung hinsichtlich der Nutzung biometrischer Daten erfolgt. Wie erwähnt, ist es seit 2017 erlaubt, verschiedene Arten biometrischer Daten im SIS nicht nur wie bisher für die Identitätsfeststellung, sondern auch für die Suche im System zu benutzen.[764] Eine solche Funktion ist im VIS bereits eingebaut und wird entsprechend genutzt.[765] Zudem ist es nun im SIS möglich, Ausschreibungen von Unbekannten anhand von deren Fingerabdrücken einzugeben. DNA-Profile, eine Datenkategorie, die bisher nicht im SIS vertreten war, werden nun für die Identitätsbestätigung von Vermissten eingeführt. Schließlich ist die geplante Intensivierung der Vernetzung der Datenbanken auch hinsichtlich der Nutzung biometrischer Daten bedeutsam, da wie erwähnt derzeit die technischen Voraussetzungen geschaffen werden, um die verschiedenen Informationssysteme anhand von Gesichtsbildern, Fingerabdrücken und anderen daktyloskopischen Daten zentralisiert abzufragen.[766]

Drittens deuten verschiedene andere Maßnahmen, wie die beschlossene Erhöhung der Speicherzeit oder die Erweiterung des Kreises der Zugriffsberechtigten im SIS, ebenfalls auf eine Ausdehnung der Möglichkeiten der europäischen Datenbanken hin.

Schließlich scheinen die Entwicklungen auf EU-Ebene paradigmatisch für die Tendenzen zu sein, die Ralf Poscher als kennzeichnend für das gesamte Feld der zivilen Sicherheit identifiziert hat.[767] Dazu gehören die Internationalisierung der Sicherheitsmaßnahmen, deren Zentralisierung, die Verschmelzung von Repression und Prävention sowie von Polizei und Geheimdiensten einerseits und Polizei und Militär andererseits. Insbesondere scheint die Stärkung der Interoperabilität der europäischen Informationssysteme die Dynamiken der Internationalisierung und der Zentralisierung zu verschmelzen und auf eine neue Ebene zu heben. Denn Zentralisierung findet hier unmittelbar auf supranationaler Ebene statt und zeigt in Richtung eines gesamten und zentralisierten europäischen Meta-Informationssystems. Was die Verschmelzung von Repression und

764 Wie erwähnt (vgl. Kapitel 4 oben) war eine solche Nutzung von Fingerabdrücken bereits vor 2017 rechtlich erlaubt, aber technisch noch nicht möglich. Für andere Arten biometrischer Daten, wie Lichtbilder und DNA-Profile, ist die rechtliche Grundlage für die Recherchefunktion erst 2017 geschaffen worden.

765 Vgl. eu-LISA, Report on the technical functioning of the Visa Information System (VIS), August 2020, 4.

766 Vgl. oben, Kapitel 7, Abschnitt 4.3.

767 Vgl. Poscher, Tendencies in Public Civil Security Law.

Prävention angeht, scheint diese sich auf EU-Ebene durch eine Verschiebung zu einem dritten Ansatz zu manifestieren, wie ich im nächsten Abschnitt anhand des Paradigmas der präemptiven Sicherheit argumentieren werde. Die letzte Tendenz, die Poscher erwähnt, nämlich die in zwei Bereichen stattfindende Verschmelzung der Kompetenzen verschiedener Behörden (von Polizei und Geheimdiensten einerseits und von Polizei und Militär andererseits), scheint mir im Fall der EU-Informationssysteme vor allem durch die Zunahme der Verwendung der Informationssysteme für verdeckte Kontrollen und als Verschmelzung zwischen Sicherheits- und Grenzmanagementmaßnahmen stattzufinden.

Diese Verschiebungen und Ausweitungen bedeuten nicht nur einen *quantitativen* Sprung, sondern auch eine *qualitative* Veränderung. Wie schon in Bezug auf das SIS erwähnt, verändert allein die Möglichkeit, aufgrund von biometrischen Daten Suchen einzuleiten, die Natur des Systems. Waren bisher das SIS und das VIS Systeme, die spezifische Fragen für einen bestimmten Zweck beantworten sollten (etwa „Ist diese Person schon verurteilt worden?“ oder „Hat diese Person ein gültiges Visum?“), werden sie nun aufgrund der neuen Funktionen zu Systemen, die bisher unbekannte Verbindungen herstellen können (etwa zwischen zwei daktyloskopischen Spuren, die niemandem zugeordnet werden können). Die bereits existierenden und geplanten Verbindungen zwischen den Informationssystemen potenzieren diese Fähigkeit, neue Verbindungen herzustellen. Die parallele Abfrage verschiedener Systeme und die Vernetzung dieser miteinander erlauben es, umfangreiche Personenprofile zu erzeugen. Zum Beispiel kann eine Suche in mehreren Datenbanken gleichzeitig Auskunft darüber geben, ob eine Person etwa als Zeuge in einem gerichtlichen Verfahren gesucht wird (SIS), über Name und Adresse der Arbeitgeberin eines Ausländers während seines früheren visumspflichtigen Aufenthalts (VIS) und möglicherweise, durch eine zukünftige Verbindung mit dem PNR-System, über frühere Reiseziele der Arbeitgeberin. Damit entsteht ein umfassendes Bild der Person, inklusive der Kontakte zu Unbeteiligten, ohne dass im Vorfeld entschieden werden muss, welche Informationen relevant sein können.

Die Logik, die dieser Erweiterung unterliegt, ist eine der „Lückenschließung“. Die existierenden Informationssysteme werden von der EU-Kommission als Erfolgsmaßnahmen beschrieben; jedoch werden regelmäßig nach den Erfolgen die noch bevorstehenden Herausforderungen und die noch nicht durch die Datenerfassung abgedeckten Bereiche erwähnt.

Folgende Schlussfolgerungen zieht zum Beispiel die Kommission 2016 aus einem Evaluationsbericht über das SIS:

> Das SIS II wird vor dem Hintergrund größter Besorgnisse bezüglich der inneren Sicherheit, grenzüberschreitenden Kriminalität und irregulären Migration betrieben – einige der schwerwiegendsten Herausforderungen weltweit. Die Gesamtevaluierung bestätigt den herausragenden operativen und technischen Erfolg dieses Systems. Offenkundig können kein operatives System und keine diesbezügliche Rechtsgrundlage jemals vollkommen sein; deshalb hat die Kommission für die Zwecke der kontinuierlichen Verbesserung des SIS II […] Möglichkeiten zur weiteren Steigerung von Wirksamkeit, Effizienz, Bedeutung und Kohärenz sowie zur Förderung des EU-weiten Mehrwerts des SIS II identifiziert […].[768]

Analog führt die Kommission zur Begründung des Vorschlags zur Einführung neuer Datenbanken Folgendes aus:

> Die bestehenden Informationssysteme decken ein sehr breites Spektrum von Daten ab, die für das Grenzmanagement und die Strafverfolgung benötigt werden. Dennoch gibt es noch große Lücken. Die Kommission hat, um einige dieser Lücken zu beseitigen, Legislativvorschläge zur Schaffung eines Einreise-/Ausreisesystems sowie für eine EU-weite Erfassung von Fluggastdatensätzen vorgelegt. Bei anderen erkannten Lücken gilt es sorgfältig zu prüfen, ob zusätzliche EU-Instrumente erforderlich sind.[769]

Wie im sechsten Kapitel erwähnt, spielen gegenwärtig ähnliche Überlegungen bei der Definition der zukünftigen Gestaltung der PNR-Maßnahmen eine Rolle, die sich auf nicht kriminalistische Datenbanken erstrecken. Die Entscheidung, nicht kriminalistische Daten für Zwecke der Kriminalitätsbekämpfung zu verwenden, führt zu einer Art Spirale der Verifizierung. Da die PNR-Daten aktuell etwa nicht das Geburtsdatum erfassen, führt der Abgleich mit behördlichen Datenbanken zu Fehltreffern. Um die Genauigkeit der PNR-Maßnahmen zu erhöhen, wäre es daher

768 Bericht der Kommission an das Europäische Parlament und den Rat über die Evaluierung des Schengener Informationssystems der zweiten Generation (SIS II) nach den Art. 24 Abs. 5, Art. 43 Abs. 3 und Art. 50 Abs. 5 der Verordnung (EG) Nr. 1987/2006 in Verbindung mit den Art. 59 Abs. 3, Art. 66 Abs. 5 und Art. 66 Abs. 5 des Beschlusses 2007/533/JI vom 21.12.2016 COM(2016) 880 final, 18.

769 COM(2016) 205 final, 14.

nach Ansicht der Kommission sinnvoll, den Fluggesellschaften (und eventuell auch den Reisebüros) vorzuschreiben, bei der Buchung auch das Geburtsdatum zu erfassen und dieses den Behörden zu übermitteln. Je mehr nicht kriminalistische (d. h. nicht verifizierte) Daten für Behördenzwecke verwendet werden, desto stärker könnte diese Verifizierungs- oder Identifizierungsspirale auch in nicht behördlichen Kontexten werden.[770]

Durch diese Logik entsteht das Paradoxon, das unter dem Begriff der „Sicherheitsspirale" bekannt ist: Das Versprechen nach Sicherheit ruft Erwartungen hervor, an denen die Ergebnisse zwar gemessen werden, die aber nie vollständig erfüllt werden können. Stattdessen werden neue Sicherheitslücken identifiziert, wofür ein erhöhter Ressourceneinsatz benötigt wird, der aber wiederum nicht genügen wird, um dem Versprechen einer umfassenden Sicherheit gerecht zu werden.[771]

Zudem verweist das Sicherheitsparadoxon auf die Eigenlogik der Sicherheitsmaßnahmen: Einmal eingeleitet zielen sie auf Selbststeigerung aus eigenem Antrieb, statt auf erhöhte äußere Bedrohungen oder Gefahren zu reagieren. Und das, selbst wenn ihnen wie im Falle der analysierten EU-Maßnahmen eine Widersprüchlichkeit mit den grundlegenden Zielen der EU innewohnt, wie etwa die Auswertung der Mobilitätsdaten aller

770 Neuerdings wurde etwa vom deutschen Bundesinnenministerium gefordert, eine Ausweisepflicht für Nutzer_inenn von Online-Diensten wie E-Mails und Messenger einzuführen, damit diese Daten für Strafverfolgungen zur Verfügung gestellt werden können. Vgl. Reuter, Markus, TKG-Novelle. Seehofer will Personalausweis-Pflicht für E-Mail und Messenger einführen, in: Netzpolitik.org, 03.03.2021.

771 Vgl. auch Münkler, Herfried, Strategien der Sicherung: Welten der Sicherheit und Kulturen des Risikos. Theoretische Perspektiven, in: Münkler, Herfried; Bohlender, Matthias; Meurer, Sabine (Hg.), *Sicherheit und Risiko. Über den Umgang mit Gefahr im 21. Jahrhundert*. Bielefeld: Transcript 2010, 11–34, hier 12–13 und Gander, Hans-Helmuth, Das Verlangen nach Sicherheit. Anthropologische Befunde, in: Heckmann, Dirk; Schenke, Ralf P.; Sydow, Gernot (Hg.), *Verfassungsstaatlichkeit im Wandel. Festschrift für Thomas Würtenberger zum 70. Geburtstag*. Berlin: Duncker & Humblot 2013, 983–993. Über das Verhältnis zwischen der individuellen und der gesellschaftlichen Dimension von Sicherheit vgl. Kaufmann, Franz-Xaver, *Sicherheit als soziologisches und sozialpolitisches Problem: Untersuchungen zu einer Wertidee hochdifferenzierter Gesellschaften*. Münster; Berlin: Ferdinand Enke Verlag 1973, 24–28 und über die Verflechtung zwischen Sicherheit und Unsicherheit Kaufmann, Stefan, Security Through Technology? Logic, Ambivalence and Paradoxes of Technologised Security, in: European Journal for Security Research, 1/1, 2016, 77–95.

Fluggäste (mit möglichen Mobilitätseinschränkungen als Folge) oder die Idee, Reisegenehmigungen für *visumsbefreite* Reisende einzuführen.[772]

In diesen Fällen überrollt die Eigendynamik der EU-Sicherheitsmaßnahmen ebenjene Ziele, für deren Unterstützung sie hätten dienen sollen. Wie in Kapitel 3 geschildert, wurden die Sicherheitsmaßnahmen im RFSR anfänglich als Ausgleich zur Realisierung des freien Personenverkehrs eingeführt. Im Nachhinein haben sie jedoch diesen unterstützenden Charakter verloren und sich zu einem eigenständigen Bereich entwickelt.

In diesem Zusammenhang hat der Sicherheitsaspekt zunehmend eine das ursprünglich primäre Element der Freiheit überragende Bedeutung gewonnen. Nun haben die Sicherheitsmaßnahmen ein Ausmaß erreicht, das nicht nur andere Grundrechte, wie das Recht auf Privatleben und auf Schutz der personenbezogenen Daten, sondern auch den Kern der EU-Freiheiten, nämlich die Bewegungsfreiheit, einschränkt. Das gilt außerdem nicht nur für diejenigen, die von Anfang an von ihrem Genuss ausgeschlossen waren, sondern auch für diejenigen, die als EU-Bürger_innen oder durch die Befreiung von der Visumspflicht eigentlich Adressat_innen der erweiterten Bewegungsfreiheit wären.

3 Sicherheit als Präemption

3.1 Die Durchsetzung der präemptiven Logik als richtungsweisend für die EU-Sicherheitspolitik

In diesem Abschnitt wird eine weitere Tendenz der EU-Sicherheitspolitik im RFSR herausgearbeitet: nämlich ihre präemptive Ausrichtung. Im RFSR, wie auch die drei Fallbeispiele zeigen, koexistieren reaktive und präemptive Modelle nebeneinander. Der präemptive Ansatz scheint aber sowohl der grundlegenden Logik der Entwicklung der Sicherheitsmaßnahmen im RFSR zu entsprechen als auch das Modell zu sein, das sich mehr und mehr durchsetzt. Im Fall des SIS und der Prümer Regelungen, die an sich eher ein reaktiv-repressives Sicherheitsmodell verkörpern, ist die präemptive Logik später hinzugekommen,[773] wobei sie bei der Fluggastda-

772 Das ist jeweils der Fall bei der PNR-Richtlinie und beim ETIAS.

773 Beim SIS ist die präemptive Logik vor allem in dem zunehmenden Einsatz des Systems zum Zwecke der gezielten oder verdeckten Kontrolle sichtbar. Vgl. Kapitel 4, Abschnitt 6.1. Im Fall der Prümer Regelungen ist diese Logik ansatzweise vorhanden, zum Beispiel im Hinblick auf den automatisierten Aus-

tensätze-Richtlinie, der neuesten unten den analysierten Maßnahmen, am ausgeprägtesten ist.[774]

Daher werde ich im Folgenden die Tendenz der EU-Sicherheitspolitik hin zu einem präemptiven Ansatz insbesondere mit Bezug auf die PNR-Richtlinie illustrieren. Die PNR-Maßnahmen stellen allerdings eine Entwicklung dar, die richtungsweisend für den zukünftigen Ausbau der EU-Sicherheitspolitik im Allgemeinen sein könnten, wie etwa die Übernahme des risikobasierten Ansatzes beim ETIAS verdeutlicht. Dementsprechend sind die folgenden Erwägungen für den RFSR generell von Bedeutung.

3.2 Der präemptive Ansatz unter besonderer Berücksichtigung der PNR-Maßnahmen

Die im sechsten Kapitel hervorgehobenen zentralen Merkmale der PNR-Richtlinie weisen auf einige Tendenzen des sicherheitspolitischen Ansatzes hin, die ich auf den folgenden Seiten beleuchten möchte.

3.2.1 Effektvermeidung statt Ursachenbekämpfung

Der risikobasierte Ansatz der Fluggastdatensätze-Richtlinie wird auch als „proaktiv" beschrieben.[775] Dabei wird „proaktiv" dem Begriff „reaktiv"

---

tausch der daktyloskopischen Daten zur Verhinderung von Straftaten oder auf den nicht automatisierten Informationsaustausch zur Straftatenverhinderung und zur Gefahrenabwehr. Vgl. Kapitel 5, Abschnitte 3.2 und 3.3. Dagegen wird im SIS und im Prümer System eine reaktive Logik von den Maßnahmen verkörpert, die auf die Identifizierung von bereits bekannten Personen, etwa Verurteilten oder Angeklagten, abzielen.

774 Stark geprägt durch ein präemptives Sicherheitsverständnis war ebenfalls die EU-Richtlinie zur Vorratsdatenspeicherung von 2006, die 2014 vom EuGH für nichtig erklärt wurde. Vgl. Richtlinie 2006/24/EG des Europäischen Parlaments und des Rates vom 15.03.2006 über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste oder öffentlicher Kommunikationsnetze erzeugt oder verarbeitet werden, und zur Änderung der Richtlinie 2002/58/EG, Amtsblatt der Europäischen Union L 105/54 vom 13.04.2006 und Urteil des Gerichtshofs (Große Kammer) vom 08.04.2014, Digital Rights Ireland Ltd, verbundenen Rechtssachen C-293/12 und C-594/12.

775 Vgl. zum Beispiel den Vorschlag der Kommission COM(2011) 32 final, 02.02.2011 und Vermeulen; Bellanova, European 'smart' surveillance.

entgegengesetzt. Reaktive Maßnahmen werden ergriffen, nachdem ein bestimmtes Ereignis geschehen ist. Dieser reaktive Ansatz ist ebenfalls in der PNR-Richtlinie vertreten, und zwar dort, wo sie den Abgleich der Fluggastdaten mit vorhandenen Datenbanken ermöglicht, nachdem eine Straftat begangen wurde. Dagegen werden die PNR-Daten proaktiv eingesetzt, wenn sie *vor* der Begehung einer Straftat verwendet werden, um diese zu verhindern.

Diese Art von Proaktivität adressiert das bekämpfte Phänomen (Terrorismus bzw. schwere Kriminalität) in einer besonderen Art und Weise. Sie zielt nicht darauf ab, dieses zu beseitigen, indem es seine Ursachen bekämpft, was typisch für eine präventive Vorgehensweise wäre. Vielmehr werden die Existenz und das Weiterbestehen dieses Phänomens angenommen. Was vermieden werden soll, sind einzelne Erscheinungen dieses Phänomens, nämlich die Begehung einer begrenzten Zahl von Straftaten, deren Täter_innen als „gefährlichste" eingestuft wurden. Dabei wird eingeräumt, dass die Behörden nicht alle möglichen Schäden vermeiden können. Genauer: Nach dem risikobasierten Ansatz der algorithmischen Regulierung *sollten* sie es auch nicht tun. Vielmehr sollen sich die Behörden auf die Kontrolle der Bedrohungen konzentrieren, die nach einer Ex-ante-Evaluierung als potenziell am gefährlichsten eingestuft wurden.[776]

Dieser effektzentrierte und risikobasierte Ansatz ist keine absolute Neuigkeit. Eine ähnliche Wendung im strafrechtlichen Bereich wurde etwa bereits in den 1990er Jahren beobachtet.[777] Der italienische Philosoph Giorgio Agamben sieht in der Fokussierung auf die Effekte sogar ein kennzeichnendes Merkmal der modernen Regierungskunst.[778] Anstatt die Ursachen zu regieren, würde diese darauf abzielen, die Effekte zu kontrollieren. Dabei hebt Agamben hervor, dass diese Verschiebung von den Ursachen auf die Effekte eine Zunahme an Kontrolle mit sich bringt: „Causes demand to be known, while effects can only be checked and con-

776 Vgl. Beaussier, Anne-Laure et al., Accounting for failure: risk-based regulation and the problems of ensuring healthcare quality in the NHS, in: Health, Risk & Society, 18/3–4, 2016, 205–224, hier 206; Yeung, Algorithmic regulation; Ulbricht, When Big Data Meet Securitization. Algorithmic Regulation with Passenger Name Records.

777 Vgl. Feely, Malcom M.; Simon, Jonathan, The new penology: notes on the emerging strategy of corrections and its implications, in: Criminology, 30/4, 1992, 449–474.

778 Vgl. Agamben, Giorgio, For a Theory of Destituent Power. Lecture Transcript, Athens, 16.11.2013.

trolled."[779] Wenn auch die Fokussierung auf Effekte und die dazugehörige Ausweitung der Überwachung und der Kontrolle keine absolute Neuheit sind, haben zunächst die Digitalisierung und die rasch steigenden Rechenkapazitäten die idealen Rahmenbedingungen geschaffen, damit sich diese Tendenzen verstärkt entfalten konnten. Die Möglichkeiten, die der Einsatz von KI-Methoden eröffnet, stellen eine weitere Steigerungsmöglichkeit dieser Tendenzen dar.

Im Kontext der gegenwärtigen Sicherheitspolitik der EU steht das proaktive Modell der PNR-Richtlinie im Widerspruch zur „Logik der Lückenschließung", an der sich die Entwicklung der EU-Politik im Raum der Freiheit, der Sicherheit und des Rechts orientiert und die auch für die Einführung der PNR-Richtlinie eine Rolle gespielt hat.[780] Wie oben erläutert, besteht diese Logik darin, progressiv die Sicherheitslücken zu schließen, die durch die bestehenden Maßnahmen nicht abgedeckt werden. Das zugrunde liegende Ideal dabei ist der Zustand absoluter Sicherheit, der auf die Beseitigung aller möglichen Bedrohungen abzielt. Dies wird aber im Fall der PNR-Richtlinie durch Maßnahmen verwirklicht, die *prinzipiell* nicht die Vermeidung *aller* Schäden vorsehen, wie es etwa zumindest ansatzweise der Fall bei einem Modell wäre, das auf Ursachenbekämpfung basiert.

3.2.2 Profile und die Erstellung von Gefährlichkeitsprognosen

Die Identifizierung der möglichen Effekte, die in Zukunft eintreten könnten und vermieden werden sollen, erfolgt aufgrund von Prognosen, die sich auf die Gefährlichkeit der einzelnen Individuen bezieht. Um diese Prognosen zu erstellen, stützen sich die PNR-Maßnahmen auf Kategorisierungen der Reisenden in verschiedene Risikokategorien.

Automatisierte Verfahren werden häufig als objektiver und neutraler als menschliche angesehen. Wie oben erwähnt hat auch die Kommission die Einführung der PNR-Richtlinie als eine Alternative zu möglicherweise diskriminierenden Kontrollen durch Beamte gerechtfertigt.[781] Menschen wer-

779 Agamben, For a Theory of Destituent Power, vgl. auch Morozov, Why the internet of things could destroy the welfare state.
780 Vgl. oben Abschnitt 2.2 in diesem Kapitel.
781 Vgl. Kapitel 6, Abschnitt 4.1.

den nun aufgrund von „objektiven Prüfkriterien“[782] auseinandersortiert, und nicht aufgrund subjektiver Einschätzungen.

Bei näherer Betrachtung erweist sich aber die Neutralität und Objektivität algorithmischer Verfahren als illusorisch. Algorithmen und Datenbanken sind menschliche Produkte, die genauso wie alle anderen Artefakte von menschlichen Vorstellungen geprägt werden.

Das kann auf verschiedenen Ebenen der automatisierten Verarbeitung von Daten beobachtet werden. Erstens können die Ausgangsdaten an sich, die für die Erarbeitung der Gefährlichkeitskriterien benutzt werden, bereits durch diskriminierende Praktiken geprägt sein. Wenn zum Beispiel bestimmte Personengruppen häufiger in den Kriminalstatistiken auftauchen, weil sie aufgrund ihrer äußerlichen Erscheinung besonders häufig kontrolliert werden, wird diese Häufigkeit in die Datenbank aufgenommen und möglicherweise von den Algorithmen als „Muster“ identifiziert.[783] Der Mechanismus an sich ist nicht neu, jedoch wäre es irreführend, zu denken, dass solche Mechanismen durch die Automatisierung der Filterungsverfahren verschwinden würden.

Zweitens sind Systeme, die Personen durch automatisierte Analyseverfahren sortieren und klassifizieren, auch auf eine spezielle, für sie spezifische, Art und Weise diskriminierend. Profile, die durch solche Analysen erzeugt werden, beziehen sich *per definitionem* auf relationale oder vergleichende statt individuelle Identitäten.[784] Entscheidungen über Individuen (etwa ob sie aufgrund ihrer „Gefährlichkeit“ weiteren Überprüfungen unterzogen werden sollen) werden nicht nur aufgrund ihrer Charakteristika getroffen, sondern auch basierend auf Annahmen und Hypothesen über die Kategorie, der sie zugeordnet wurden. Wenn zum Beispiel ein Fluggast sein Flugticket von Berlin nach Istanbul mit nur geringem zeitlichen Vorlauf kauft, dieses in bar bezahlt und womöglich noch einen 30 kg schwe-

---

782 COM(2011) 32 final, 02.02.2011, 6.

783 Für weitere Beispiele, wie algorithmische Systeme in den verschiedenen Phasen der Programmierung und Anwendung diskriminierend geprägt sein oder wirken können, vgl. Barocas, Solon; Selbst, Andrew D., Big Data’s Disparate Impact, in: California Law Review, 104, 2016, 671–732; Orrù, Elisa, Minimum Harm by Design. Reworking Privacy by Design to mitigate the risks of surveillance, in: Leenes, Ronald *et al.* (Hg.), *Computers, Privacy and Data Protection: Invisibilities & Infrastructures*. Dordrecht: Springer 2017, 107–137.

784 Vgl. Gandy, Oscar H., Data Mining, Surveillance, and Discrimination in the Post-9/11 Environment, in: Haggerty, Kevin D.; Ericson, Richard V. (Hg.), *The new politics of surveillance and visibility*. Toronto: University of Toronto Press 2007, 363–384, hier 370.

ren Rucksack eincheckt, obwohl der Rückflug bereits drei Tage nach dem Hinflug stattfindet, wird er eventuell als „Hochrisiko-Passagier" eingestuft. Diese Gefährlichkeitsprognose wird aber aufgrund von Annahmen über die Kategorie von Menschen, die die erwähnten Kriterien mit ihm teilen, und womöglich von anderen Individuen, die mit ihrem vergangenen Verhalten diesen Kriterien entsprachen, getroffen, nicht aber aufgrund seines eigenen vergangenen Verhaltens. Anders gesagt: Der Fluggast wird als „gefährlich" eingestuft, nicht weil er selbst sich in der Vergangenheit in einem Camp für „foreign fighters" in Syrien aufhielt oder weil in seinem vergangenen Verhalten Anhaltspunkte dafür zu finden wären. Vielmehr erfolgt diese Einstufung, weil beobachtet wurde bzw. angenommen wird, dass eine Anzahl von anderen Menschen, die von Deutschland nach Syrien in solche Camps gereist sind, kurzfristig einen Flug in die Türkei gebucht, das Ticket in bar bezahlt und einen Scheinruckflug gebucht haben, wobei sie zudem Gepäck für einen längeren Aufenthalt mit sich geführt haben. In die Gefährlichkeitsprognose über den Fluggast fließen damit Bewertungen ein, die nicht ihn individuell betreffen, sondern Menschen, die in die gleiche Kategorie wie er eingeteilt wurden. Selbst wenn die Programmierer_innen sich dessen nicht bewusst sind oder dies nicht intendieren, kann die Art, wie die verschiedenen Kategorien definiert werden, bereits diskriminierende Muster reproduzieren.

Die Fluggastdatensätze-Richtlinie schließt explizit aus, dass Entscheidungen über die Gefährlichkeit von Individuen „aufgrund der rassischen oder ethnischen Herkunft, der politischen Meinungen, der religiösen oder weltanschaulichen Überzeugungen, der Mitgliedschaft in einer Gewerkschaft, des Gesundheitszustands, des Sexuallebens oder der sexuellen Orientierung einer Person getroffen" werden.[785] Werden solche Daten an die nationale Zentralstelle übermittelt, darf diese sie nicht verarbeiten und muss sie löschen.[786]

Gerade bei der automatisierten Analyse von großen Datenmengen können aber Rückschlüsse über solche sensiblen Merkmale aus scheinbar nicht sensiblen Daten hervorgehen.[787] Die Postleitzahl könnte zum Bei-

785 Richtlinie (EU) 2016/681, Art. 7 (6).

786 Vgl. ebd., Art. 13 (4).

787 Vgl. Orrù, Minimum Harm by Design. Reworking Privacy by Design to mitigate the risks of surveillance, 129; Kamiran, Faisal; Calders, Toon; Pechenizkiy, Mykola, Techniques for Discrimination-Free Predictive Models, in: Custers, Bart *et al.* (Hg.), *Discrimination and privacy in the information society: data mining and profiling in large databases*. Berlin; Heidelberg: Springer 2013, 223–241. Vgl. auch Hardt, Moritz, Occupy Algorithms: Will Algorithms Serve the 99 %?

spiel Hinweise auf Ethnizität, Herkunft oder Migrationshintergrund liefern, oder Angaben über Mitreisende können die Beziehung zu den Passagier_innen, mit dem sie reisen, und damit potenziell Informationen über deren Sexualleben, offenbaren. Wie oben dargelegt, können durch maschinelles Lernen sogar Korrelationen erstellt werden, die ohne maschinelle Unterstützung (also durch menschliche Beobachtung allein) nicht erkannt werden können. Da diese Verbindungen durch die Verarbeitung der Daten selbst erzeugt werden und nicht im Voraus fixiert sind, ist es auch unmöglich, auszuschließen, dass solche potenziell sensiblen Assoziationen zum Einsatz kommen. Außerdem deutet die bisher nur sparsam vorhandene öffentlich zugängliche Literatur über den Einsatz von maschinellem Lernen für Verhaltensprofilierung darauf hin, dass Informationen wie Geschlecht, Alter, Aussehen und vor allem die im Freitextfeld eingegebenen Informationen besonders wertvoll für Profilierungszwecke sein könnten.[788]

Im Widerspruch zu den Erklärungen der Kommission über die Objektivität der automatisierten Datenverarbeitung führt die Fluggastdatensätze-Richtlinie selbst eine menschliche Überprüfung der Ergebnisse der automatisierten Auswertung ein. In der Richtlinie heißt es:

> Die zuständigen Behörden treffen Entscheidungen, aus denen sich eine nachteilige Rechtsfolge oder ein sonstiger schwerwiegender Nachteil für die betroffene Person ergibt, unter keinen Umständen allein auf der Grundlage der automatisierten Verarbeitung der PNR-Daten.[789]

Menschliche Beurteilungen wurden also zunächst als vorurteilsbeladen ausgeschlossen und durch „objektive" und „neutrale" maschinelle Verfahren ersetzt, um dann aber am Ende des Prozesses wieder eingeführt zu werden, um dadurch wiederum mögliche maschinelle Fehler zu beseitigen und zu garantieren, dass die Entscheidungen gerecht sind.[790]

Response Paper presented at the Governing Algorithms Conferenz, New York, 17.03.2013, wonach das Ableiten von Merkmalen aus sogenannten *proxies* (in diesem Fall: der Ethnizität aus der Postleitzahl) genau das ist, was Algorithmen besonders gut können.

788 Vgl. INDECT D9.9. Report on current state-of-the-art of machine learning methods for behavioural profiling, 2011, www.indect-project.eu (letzter Zugriff: 03.06.2019), das sogar die „ethnic appearance of the offender" als wertvolle Information erwähnt (S. 13).

789 Richtlinie (EU) 2016/681, Art. 7 (6).

790 Vgl. Vermeulen; Bellanova, European 'smart' surveillance.

Sobald maschinelles Lernen hinzukommt, wird aus diesem Widerspruch eine Unmöglichkeit, weil die Überprüfbarkeit der Entscheidungen nicht mehr möglich sein wird. Wie unten näher ausgeführt wird,[791] werden die maschinell erzeugten Entscheidungen für Menschen nicht mehr nachvollziehbar sein. Da die Strukturen und Funktionen, die zu der Entscheidung geführt haben, keine im Voraus fixierte Funktion durchführen, sondern vom System selbst erzeugt werden und für Menschen nicht nachvollziehbar sind, wird es für Menschen unmöglich sein, sie kritisch und gründlich zu überprüfen. Tatsächlich werden sich die Kontrolleur_innen in diesen Fällen auf die mitgelieferte Übersetzung des automatisierten Verfahrens in Risikokategorien verlassen müssen.[792]

Zudem ist fraglich, ob solche Ergebnisse, die auf Wahrscheinlichkeiten hinweisen, überhaupt überprüfbar sein können. Die Ergebnisse der PNR-Profilierung werden Prognosen darüber enthalten, wie wahrscheinlich es ist, dass ein Mensch eine Bedrohung darstellen *wird*. Eine Aussage wie „Mensch X weist eine 95-prozentige Wahrscheinlichkeit auf, in Zukunft eine terroristische Straftat zu begehen" kann durchaus korrekt sein und trotzdem zu ungerechten Folgen führen. Denn die Wahrscheinlichkeit kann (nach welchen Kriterien auch immer) „korrekt" ermittelt worden sein, und damit kann es korrekt sein, zu sagen, dass dieser Mensch mit hoher Wahrscheinlichkeit eine terroristische Straftat begehen könnte. Die Aussage würde weiterhin korrekt sein, auch wenn dieser Mensch nach den verbleibenden 5 % *nie* eine terroristische Straftat begehen wird. Jedoch wäre es *ungerecht*, etwa diesem Menschen aufgrund seines Gefährlichkeitsprofils ein Flugverbot zu erteilen. Anders als Entscheidungen, die sich auf in der Vergangenheit begangene Taten beziehen, wäre die Gerechtigkeit einer solchen Entscheidung nur in Zukunft überprüfbar, wenn von jeglichen Interventionen abgesehen werden würde.[793] Solche Interventionen als proaktive Maßnahmen sind aber genau das, worauf die Gefährlichkeitsprognosen abzielen. Dieses Phänomen, auch als „asym-

791 Vgl. unten, Abschnitt 3.2.3 in diesem Kapitel.

792 Vgl. Leese, Matthias, The new profiling: Algorithms, black boxes, and the failure of anti-discriminatory safeguards in the European Union, in: Security Dialogue, 45/5, 2014, 494–511.

793 Die Kontrastierung mit Urteilen, die auf vergangenen Taten basieren, bedeutet nicht, dass diese immer korrekt wären oder immer auf sicherer Basis gesprochen werden können. Vielmehr bedeutet sie, dass in diesen Urteilen wenigstens *im Prinzip* überprüfbar ist, ob die Voraussetzungen für die Entscheidung (die bereits erfolgte Begehung einer Straftat) erfüllt sind.

metrisches Feedback“[794] bekannt, ist nicht spezifisch für Prognosen, die durch maschinelles Lernen erzeugt werden. Doch hat es für diese Art der Prognose gravierende Konsequenzen, da maschinelle Lernsysteme auf Feedback angewiesen sind, um die gewünschten Funktionalitäten zu entwickeln und zu verbessern und um deren spezifisches Potenzial, wie etwa die Analyse großer Datenmengen und die Anpassung an neue Situationen, zu entfalten.

3.2.3 Opazität der Bewertungskriterien

Die automatisierte Analyse der Fluggastdaten zum Zweck der Profilierung wird nach der PNR-Richtlinie benutzt, um Entscheidungsempfehlungen zu formulieren. Entsprechend werden Verhaltensnormen („Fluggast X soll näher überprüft werden“) formuliert, an denen sich menschliches Handeln orientieren soll. Die Formulierung von diesen Entscheidungsempfehlungen ist durch verschiedene Varianten von Opazität gekennzeichnet. Diese Opazität ist besonders ausgeprägt, wenn die Profilierung der Passagier_innen durch den Einsatz maschinellen Lernens erfolgt bzw. erfolgen würde, gilt aber unter bestimmten Bedingungen auch dann, wenn die Muster von Personen vorgegeben werden.

Die erste Form von Opazität betrifft die mangelnde Begründbarkeit der Kriterien, wodurch bestimmte Individuen als gefährlich eingestuft werden. Diese Form von Opazität ist unvermeidbar, wenn die Kriterien durch maschinelles Lernen zustande kommen: Durch maschinelles Lernen werden in (unstrukturierten) großen Datenmengen Regelmäßigkeiten aufgespürt. Diese sind umso interessanter, als sie zuvor unbekannt waren und nicht durch menschliche Verstandesleistung allein erkannt werden konnten.[795] Aufgrund dieser Regelmäßigkeiten werden Verbindungen zwischen Merkmalen erstellt, etwa zwischen dem Vorhandensein einer bestimmten Eigenschaft A und dem errechneten Bedrohungspotenzial einer Person B. Ob nun A und B in einem kausalen Zusammenhang stehen, ob beide durch einen dritten Faktor C verursacht wurden oder ob es reiner Zufall ist, dass sie zusammen auftreten, ist für die Erstellung der Korrelation unbedeutend. Zum Beispiel: Wenn sich etwa aus der Datenanalyse ergibt,

794 Zweig; Wenzelburger; Krafft, On Chances and Risks of Security Related Algorithmic Decision Making Systems, 13, Übersetzung E.O.

795 Genau deswegen, um „neue“ Korrelationen herauszufinden, wird maschinelles Lernen eingesetzt. Vgl. Yeung, Algorithmic regulation.

dass eine bestimmte Bezahlungsart häufig genug gekoppelt mit einem „abweichenden" Verhalten auftritt (d. h., nach dem Check-in den Flug nicht anzutreten), wird daraus eine Assoziation erstellt, ohne dass es eine logische Erklärung dafür geben muss. Warum nun genau diese Korrelation aufgestellt wird und nicht eine andere, oder warum das System zu einem bestimmten Ergebnis kommt und nicht zu einem anderen, kann nicht erklärt werden. Anders formuliert: Die relevanten Assoziationen werden sozusagen unmittelbar aus „Beobachtungen" erstellt, nicht aus logischen (kausalen) Zusammenhängen, und im Nachhinein ist es nicht möglich, die Wege zu rekonstruieren, die das System zu dem jeweiligen Ergebnis geführt haben.[796] Diese Unerklärbarkeit der Muster, die – wenn sie durch maschinelles Lernen erzeugt werden – *prinzipiell* ist, kann auch die von den Behörden vorgegebenen Muster betreffen, wenn diese aufgrund von Häufigkeitsbeobachtungen erstellt wurden und nicht plausibel erklärt werden können.

Dass eine solche Situation ein Problem in Bezug auf das Kriterium der Rechtfertigung darstellt, kann auf verschiedenen Ebenen verdeutlicht werden. Im deutschen Polizeirecht wird bisher zum Beispiel verlangt, dass die Gründe für die vertiefte Kontrolle („Gefahrerforschungseingriff") *plausibilisierbar* sein müssen. Dafür reicht es nicht, dass das eingesetzte System erfahrungsgemäß funktioniert, sondern es muss auch erklärbar sein, warum es das tut.[797] Der Grund dafür liegt in der Idee, dass Beamte die Maßnahme verantworten können müssen und dass dies nur dann möglich ist, wenn sie auch verstehen können, wie es zu der Prognose, welche die Maßnahme veranlasst hat, gekommen ist.[798] Auch auf europäischer Ebene werden benachteiligende Maßnahmen aufgrund von automatisierter Profilierung nur dann zugelassen, wenn bestimmte Grundrechte garantiert sind. Dazu zählt zwingend das Recht, das Einschreiten einer Person zu erwirken, um den eigenen Standpunkt darlegen zu können, die Gründe der Entscheidung erläutert zu bekommen und die Entscheidung anfechten zu können.[799] Wenn maschinelles Lernen zum Einsatz kommt, sind aber diese Voraussetzungen, wie ich geschildert habe, nicht gegeben.

Ansätze, die unter dem Begriff „explainable artificial intelligence" („erklärbare künstliche Intelligenz") bekannt sind, versuchen dieses Problem

796 Vgl. Schubbach, Judging machines; Rademacher, Predictive Policing im deutschen Polizeirecht, 377.
797 Vgl. Rademacher, Predictive Policing im deutschen Polizeirecht, 386–391.
798 Vgl. ebd., 387.
799 Vgl. Richtlinie (EU) 2016/680 vom 04.05.2016, Art. 11 und Präambel, Ziff. 38.

zu umgehen. Was diese Ansätze leisten können, ist zwar, zu rechtfertigen, warum ein durch maschinelles Lernen erzeugtes Ergebnis richtig ist, nicht aber, wie es dazu gekommen ist. Diese Ansätze könnten also eine Rechtfertigung liefern, die nicht – wie die bisherigen gesetzlich verlangten Rechtfertigungen – auf Erklärung basiert.[800] Solche Ansätze können einen signifikanten Beitrag zur Akzeptanz von künstlicher Intelligenz leisten. Da sowohl das deutsche als auch das europäische Recht, wie oben ausgeführt, auf Erklärbarkeit bestehen, scheint jedoch eine solche Rechtfertigung nach dem jetzigen Stand unterhalb der rechtlichen Standards zu bleiben.

Zusammenfassend: Wenn Entscheidungen aufgrund nicht erklärbarer Bewertungen getroffen werden, fällt eine wichtige Voraussetzung dafür, dass sie gerechtfertigt und kritisiert werden können, fort: nämlich deren Begründbarkeit. Begründbarkeit als Lieferung plausibler Erklärungen scheint bisher eine nötige Voraussetzung für die Rechtfertigung behördlicher Maßnahmen, die benachteiligend für die Betroffenen sind.

3.2.4 Opazität der Überprüfungsmaßnahmen

Die zweite Variante der Opazität der Maßnahmen nach der Fluggastdatensätze-Richtlinie betrifft den weiteren Schritt der PNR-Maßnahmen. Die oben beschriebene erste Form der Opazität bezieht sich auf die Nicht-Erklärbarkeit der Gründe, die zu einer Gefährlichkeitsprognose geführt haben. Die zweite Variante der Opazität betrifft die genaueren Überprüfungen, welche den Bewertungen folgen, und ist unabhängig von der Art und Weise, wie diese Bewertungen generiert wurden. Sie betrifft somit sowohl Fälle, in denen die Muster vorgegeben sind, als auch Fälle, in denen sie automatisch produziert werden.

Die genaueren Überprüfungen, die der Profilierung folgen, sind durch Opazität gekennzeichnet, weil die Betroffenen zunächst nichts davon erfahren. Sie erfahren nämlich weder, dass sie vom System als „Hochrisiko-Passagier_innen“ eingestuft wurden, noch, dass sie weiteren menschlichen

800 Vgl. Schubbach, Judging machines. Für weitere Ansätze zur Überwachung von algorithmischen Entscheidungen, die keine Transparenz der Systeme voraussetzen vgl. Zweig, Katharina, Algorithmische Entscheidungen: Transparenz und Kontrolle, in: Analysen und Argumente aus der Konrad-Adenauer-Stiftung, 2019.

Überprüfungen unterzogen werden.[801] In beiden Fällen werden sie nicht benachrichtigt, die Richtlinie sieht lediglich vor,

> dass eine betroffene Person das Recht hat, den Datenschutzbeauftragten als zentrale Kontaktstelle im Zusammenhang mit allen Fragen bezüglich der Verarbeitung der PNR-Daten der betroffenen Person zu kontaktieren.[802]

Dabei wird aber nicht sichergestellt, dass alle Betroffenen informiert werden und damit tatsächlich von ihrem Auskunftsrecht Gebrauch machen können.[803] Erst wenn die genaueren Überprüfungen zu weiteren konkreten Folgen führen, wie etwa die Verweigerung des Flugantritts, können die Betroffenen davon erfahren.

Zwei Aspekte sind hier besonders relevant. Erstens: Wenn die genauere menschliche Überprüfung, die der automatisierten Risikoprofilierung folgt, bereits eine „nachteilige rechtliche Wirkung" darstellt, dann sind die oben erwähnten Garantien des Rechts auf Darstellung der eigenen Position, auf Erläuterung der Entscheidung und auf Anfechtbarkeit der Entscheidung nicht gegeben. Die offene Frage zu beantworten, ob dies der Fall ist, ist Aufgabe der gerichtlichen Kontrolle und geht über die Ziele vorliegender Untersuchung hinaus. Wenigstens im Sinne des deutschen Rechts auf informationelle Selbstbestimmung, wonach jeder behördliche Umgang mit personenbezogenen Daten eine erhebliche rechtliche Belastung und damit einen Eingriff darstellt,[804] scheint jedoch die Frage positiv beantwortbar zu sein.

---

801 Das bedeutet auch einen Unterschied zu anderen Formen der Passagierkontrolle, zum Beispiel einer Abtastung am Flughafen, nachdem der Metalldetektor Alarm geschlagen hat. Abgesehen von anderen möglichen Unterscheidungen in Bezug auf die Punktualität der Kontrolle, die Erhebung personenbezogener Daten etc., ist in diesem Zusammenhang relevant, dass im Fall der Passagierkontrollen an Flughäfen die Betroffenen jedoch ohne Weiteres sowohl den Alarm durch den Metalldetektor als auch die menschliche Kontrolle, die daraufhin folgt, erfahren. Damit ist auch die Gelegenheit gegeben, nach den Gründen der Abtastung zu fragen und die eigene Position zu klären („ich habe vergessen, meinen Schlüsselbund aus der Tasche zu nehmen") sowie auch die Maßnahme zu kritisieren.

802 Richtlinie (EU) 2016/681, Art. 5 (3).

803 Noch weniger wird in der Richtlinie spezifiziert, welche Informationen die betroffene Person erhalten muss oder dass die Datenschutzbeauftragten überhaupt verpflichtet sind, den Betroffenen irgendeine Auskunft zu geben.

804 Vgl. Rademacher, Predictive Policing im deutschen Polizeirecht, 391.

Zweitens: Die Nicht-Erfahrbarkeit der Überprüfungen, die im Hintergrund stattfinden, scheint eine schleichende Gefahr für die Demokratie darzustellen. Diese Gefahr kann in Anlehnung an die von der deutschen Juristin Indra Spiecker genannt Döhmann nachgewiesene Wechselbeziehung zwischen Demokratie und Fragmentierung verdeutlicht werden.[805]

Fragmentierung wird von Spiecker als Neugestaltung der Beziehungen zwischen Einzelheiten (den Individuen) und dem Gesamtsystem (dem demokratischen System) verstanden. Eine wichtige Stärke demokratischer Gesellschaften liegt darin, neu entstandene Fragmentierungen aufzugreifen und sie positiv zur Anpassung an den Wandel zu nutzen. Dafür sind aber „offene – physische, virtuelle und vor allem diskursive – Treffräume [eine zentrale Voraussetzung], in denen unterschiedliche Fragmentierungen aufeinandertreffen",[806] wodurch sie verhandelt, diskutiert und demokratisch verarbeitet werden können.

Obwohl Spiecker damit auf die Gefahren von Digitalisierungs- und Vernetzungsprozessen in anderen Bereichen als in der Sicherheitspolitik hinweisen will, können ihre Überlegungen auch für die Fluggastdatensätze-Richtlinie fruchtbar sein. Denn durch die Klassifizierung der Passagier_innen in Risikokategorien werden Fragmentierungen erzeugt, die nicht in eine öffentliche Diskussion überführt, kritisiert und infrage gestellt werden können, weil sie nicht wahrgenommen werden *können*. Die Risikokategorien als neue Fragmentierungen greifen auf eine flächendeckende Art und Weise zu: Sie teilen alle Passagier_innen in verschiedene Kategorien ein, die womöglich unterschiedlich behandelt werden. Die Passagier_innen bekommen damit eine auf sie zugeschnittene Behandlung, ohne zu erfahren, dass sich diese überhaupt von der Behandlung anderer Fluggäste unterscheidet, und folglich ohne diese hinterfragen zu können.

---

805 Vgl. Spiecker Döhmann, Indra, Kontexte der Demokratie: Partei, Medien und Sozialstrukturen, in: Spiecker Döhmann *et al.* (Hg.), *Fragmentierungen*, Bd. 77. Berlin: de Gruyter 2018, 9–66. Für eine Reflexion über algorithmische Regulierung und Demokratie vgl. Zweig; Wenzelburger; Krafft, On Chances and Risks of Security Related Algorithmic Decision Making Systems. Kritisch über die Auswirkungen des Einsatzes von *big-data*-Technologien und Demokratie im Allgemeinen vgl. O'Neil, Cathy, *Weapons of math destruction: how big data increases inequality and threatens democracy*. London: Penguin Books 2017; Pasquale, Frank, *The Black Box Society: the secret algorithms that control money and information*. Cambridge: Harvard University Press 2015.

806 Spiecker Döhmann, Kontexte der Demokratie, 35.

3.2.5 Opazität der Verhaltensnormen

Die dritte Variante der Opazität der Fluggastdatensätze-Richtlinie wird durch die Definition der Gefährlichkeitskriterien verwirklicht. Die Kriterien, die auf die Gefährlichkeit mancher Individuen hinweisen sollen, sind nicht in Bezug auf verbotene Handlungen definiert. Sie werden auch nicht aus kriminalistisch relevanten Daten abgeleitet, sondern aus Daten, die sich auf Tätigkeiten beziehen, die durchaus erlaubt und sogar für die Buchung und Durchführung der Reisen nötig sind.

Nehmen wir zum Beispiel die Daten zur Art der Bezahlung. Die relevante Frage hierbei ist nicht, ob das Flugticket etwa mit gefälschten Scheinen bezahlt wurde – was eine illegale Tätigkeit wäre. Denn die gesammelten Fluggastdaten enthalten in der Regel solche Informationen nicht.[807] Was die gesammelten Daten jedoch liefern, ist die Information über das Medium der Bezahlung, wobei eine Barbezahlung (an sich eine vollständig legale Form der Bezahlung) möglicherweise als „gefährlicher" als die Bezahlung mit Kreditkarte eingestuft wird. Wie dann dieses Kriterium (in Verbindung mit anderen) in einer bestimmten Situation gewichtet wird, hängt nicht von seinem Bezug zu einer externen Norm, die eine klare, binäre Unterscheidung zwischen verbotenem und erlaubtem Verhalten bietet, ab. Ob die Barzahlung nun in Verbindung mit anderen Kriterien dazu führt, dass eine Person herausgefiltert wird, verdankt sich vielmehr der statistischen Verteilung der Kriterien zwischen allen anderen Passagier_innen.[808] Denn was durch die Analyse der Daten gesucht wird, sind Anomalien oder Spitzenwerte. Die Analyse ist nur dann sinnvoll, wenn eine zahlenmäßig kleinere Gruppe von Fluggäste herausgefiltert werden kann. Wenn etwa an einem besonderen Tag oder auf einer bestimmten Route die Mehrheit der Passagier_innen bar bezahlt, dann hat das Kriterium der Barzahlung keine Aussagekraft. Wenn aber in einer anderen Situation 99 % der Passagier_innen mit Kreditkarte bezahlen, dann kann es durchaus attraktiv sein, die Barzahler genauer zu überprüfen. Es wäre, als ob die Geschwindigkeit, die auf einer Bundesstraße als verboten bzw. gefährlich gilt, nicht rechtlich festgelegt wurde, sondern aus der Analyse der Verkehrsdaten entstehen würde, etwa als die Geschwindigkeitsgrenze, die von 95 % der Fahrer nicht überschritten wird. Wer diese Grenze über-

807 Denn die Daten werden von Fluggesellschaften übermittelt und stammen nicht aus behördlichen Datenbanken.

808 Vgl. auch Leese, The new profiling: Algorithms, black boxes, and the failure of anti-discriminatory safeguards in the European Union.

schreitet, wird behördlichen Maßnahmen unterzogen, nicht weil sein bzw. ihr Verhalten verboten ist, sondern weil sein bzw. ihr Verhalten von dem der anderen Fahrer_innen erheblich abweicht.[809]

Das hat interessante Konsequenzen für die Art der Normativität, die durch solche Verfahren erzeugt wird. Denn Werturteile (was als „gefährlich" gilt) werden dabei nicht in Bezug auf ein normatives System definiert, das relativ stabil und relativ unabhängig von den empirischen Informationen über die Gegebenheiten, die es „normieren" soll, ist.[810] Werturteile werden vielmehr aus einem Pool empirischer Daten abgeleitet, die dasselbe empirische Verhalten beschreiben, das bewertet werden soll. Diese Form von Normativität kann als „empirische Normativität" bezeichnet werden: Gefährlichkeit wird nicht unter Bezug auf eine übergeordnete rechtliche Norm definiert, die gegenüber den vorhandenen Daten „extern" ist. Die Norm wird vielmehr aus den Daten selbst erarbeitet, ist sozusagen *den empirischen Daten immanent*. Nun wurde im ersten Kapitel argumentiert, dass eine externe, objektive, aus unserer Erfahrung losgelöste Normativität nicht erreichbar ist. Konsequenterweise könnte nun schlussfolgert werden, dass die empirische Ableitung der Kriterien im Fall der PNR-Richtlinie nur das übliche Vorgehen darstellt. Jedoch: Das Versprechen und die Funktion der rechtsstaatlichen Mechanismen, wie sie im zweiten Kapitel dieses Buches dargestellt wurden, liegt darin, dieser Befangenheit entgegenzuwirken und durch die rechtliche Fixierung der Normen (des verbotenen und erlaubten Verhaltens) Stabilität und Transparenz zu bieten. Die durch die PNR-Richtlinie eingeschlagene Richtung scheint diesen rechtsstaatlichen Anspruch infrage zu stellen. Die Konsequenz ist, dass niemand im Voraus mit Gewissheit vorhersehen kann, welche Tätigkeiten die Aufmerksamkeit der Behörden auf ihn oder sie lenken werden.

---

809 Um das Beispiel noch weiter zu verdeutlichen: Das Kriterium „schnell fahren" ist in beiden Fällen als ein entscheidendes Merkmal vorgegeben. Nur im ersten Fall ist klar definiert, was als „zu schnell" (und deswegen verboten) gilt – im zweiten Fall hingegen nicht, denn hier wird die Schwelle relational zum Verhalten anderer definiert und verschiebt sich ständig.

810 Natürlich spielen die empirischen Gegebenheiten auch für die Festlegung rechtlicher Normen eine Rolle, wie etwa, dass es Straßen und Kraftfahrzeuge gibt, die bestimmte technische Eigenschaften haben und eine bestimmte Geschwindigkeit erreichen können. Aber die Norm, etwa dass auf Bundesstraßen die maximal erlaubte Geschwindigkeit 100 km/h beträgt, gilt unabhängig vom allgemeinen Fahrverhalten an einem bestimmten Tag, etwa wie viele Fahrzeuge tatsächlich die Geschwindigkeitsgrenze überschreiten oder ob die durchschnittliche Geschwindigkeit der Fahrzeuge an dem Tag 80 oder 90 km/h ist.

Diese Mobilität der Gefährlichkeitsschwelle ist charakteristisch für die Logik der PNR-Richtlinie, unabhängig davon, ob die Kriterien von den Behörden vorgegeben werden oder durch maschinelles Lernen hergestellt werden. Die Instabilität spitzt sich aber zu, wenn maschinelles Lernen, insbesondere in den nicht durch Menschen überwachten Formen, zum Einsatz kommt. Denn dann entscheidet die statistische Verteilung der Merkmale nicht nur über die Gewichtung der vorgegebenen Kriterien, sondern Anomalien an sich werden zu Hauptkriterien der Klassifizierung. Die Mobilität der Kriterien wird ferner dadurch forciert, dass die Verarbeitung der Fluggastdaten dazu dienen soll, die Kriterien selbst kontinuierlich zu adaptieren.[811]

Schließlich wird diese Form der Opazität der PNR-Normen dadurch erschwert, dass die Gefährlichkeitskriterien und die Kalkulationsregeln nicht offengelegt werden. Dies wird von den Behörden dadurch gerechtfertigt, dass, wenn die Kriterien öffentlich wären, potenzielle Kriminelle oder Terrorist_innen ihr Verhalten anpassen könnten, um Kontrollen auszuweichen.[812] Jedoch scheint dieses Argument nicht vollständig zu überzeugen, da die aktuelle Forschung auf die Möglichkeit hinweist, die Kriterien offenzulegen, ohne diese der Manipulationsgefahr auszusetzen und ohne die Effektivität der Maßnahmen zu mindern.[813]

3.3 Das Modell der präemptiven Sicherheit

In diesem Abschnitt werde ich die Grundcharakteristika des präemptiven Sicherheitsmodells auf allgemeine Art und Weise darstellen. Die im vorigen Abschnitt hervorgehobenen Züge werden zu einem gemeinsamen Bild zusammengefügt und durch die Kontrastierung mit reaktiven und präventiven Ansätzen verdeutlicht.

Grundsätzlich kann ein risikobasierter, proaktiver Ansatz als ein *effektzentriertes* Modell verstanden werden, in dem es um die Vermeidung von den (schlimmsten) Effekten eines Phänomens anstatt um die Bekämpfung

811 Vgl. Kapitel 6, Abschnitt 6.3 und Yeung, Algorithmic regulation.

812 Vgl. Ulbricht, When Big Data Meet Securitization. Algorithmic Regulation with Passenger Name Records und Entwurf eines Gesetzes über die Verarbeitung von Fluggastdaten zur Umsetzung der Richtlinie (EU) 2016/681 (Fluggastdatengesetz – FlugDaG), 30.

813 Vgl. aus technischer Perspektive Hardt, Occupy Algorithms: Will Algorithms Serve the 99 %? und aus rechtlicher Perspektive Poscher, Tendencies in Public Civil Security Law, 70.

seiner Ursachen geht.[814] Präemptive Sicherheitsmodelle zielen darauf ab, die schwerwiegendsten negativen Effekte eines Phänomens vorauszusagen und sie dadurch zu verhindern.

Präemptive Modelle stehen daher in einem besonderen Verhältnis zum zeitlichen Geschehen, das sich von der zeitlichen Ausrichtung von sowohl reaktiven als auch präventiven Modellen unterscheidet. Reaktive Sicherheitsmodelle etwa basieren auf Ereignissen in der Vergangenheit und stellen eine Reaktion auf diese dar. Dagegen sind präemptive Modelle, wie präventive auch, zukunftsorientiert, weil sie darauf abzielen, bestimmte zukünftige Ereignisse zu vermeiden.[815] Dafür agieren beide Modelle in der Gegenwart.

Präemptive und präventive Sicherheitsmodelle teilen somit miteinander eine Art Projektion der zu erreichenden Ziele in die Zukunft, die aber durch eine Intervention in der Gegenwart erreicht werden sollen. Die epistemischen Strategien, um mit dieser Projektion in die Zukunft umzugehen, sind aber unterschiedlich. Während präventive Modelle auf *Ursachen* fokussieren und im Hinblick auf diese agieren wollen, suchen präemptive Modelle nach *Anzeichen*. Präventive Modelle wollen Ursachen erkennen, präemptive Modellen wollen Anzeichen interpretieren.[816] Dementsprechend gründen präemptive Modelle auf Korrelationen, während präventive Modelle auf *Kausalität* setzen. Letztere brauchen *Theorien*, die den Zusammenhang zwischen Ursachen und Effekten herstellen und verdeutlichen. Dagegen brauchen präemptive Modelle *Beobachtungen*, in denen verschiedene Elemente zueinander in Korrelation gebracht werden können. Erstere wollen das *Dass* erfassen, letztere fragen nach dem *Warum* eines bestimmten Phänomens.[817]

Ferner: In Bezug auf den Zustand, auf den sie einwirken wollen, stellen präventive Modelle eine *Diagnose*. Die Diagnose fokussiert auf ein bereits

814 Vgl. dazu auch Yeung, Algorithmic regulation und Morozov, Evgeny, *Smarte neue Welt: digitale Technik und die Freiheit des Menschen*. München: Blessing 2013.

815 Über das Verhältnis zwischen Sicherheit und Unwissen vgl. Burgess, J. Peter, Sicherheit als Ethik, in: Zoche, Peter; Kaufmann, Stefan; Arnold, Harald (Hg.), *Sichere Zeiten? Gesellschaftliche Dimensionen der Sicherheitsforschung*. Berlin Münster: LIT Verlag 2015, 33–42.

816 Am deutlichsten im Kontext der in den vorigen Kapiteln analysierten Maßnahmen zeigt sich das bei der PNR-Richtlinie, wonach Daten über Mobilität Hinweise auf die Gefährlichkeit der Flugpassagiere liefern sollen.

817 Auch in Bezug auf diese Aspekte stellt die PNR-Richtlinie die eindeutigste Illustration dar, vgl. oben Abschnitt 3.2 dieses Kapitels.

existierendes Problem, will dieses durch die Darstellung des Erscheinungsbildes und die Nennung der Ursachen verdeutlichen und womöglich eine Therapie aufzeigen, die zur Bewältigung des Problems führen soll. Präemptive Ansätze stellen dagegen eine *Prognose*. Die Frage ist nicht, ob ein Problem hier und jetzt besteht, sondern ob es in Zukunft bestehen wird. Die Prognose wird aufgrund von Indikatoren gestellt: Zeichen, die hier und jetzt präsent sind und an sich nicht problematisch sein müssen, sondern auf eine zukünftige problematische Situation hinweisen sollen.[818]

In beiden Fällen sollen Maßnahmen unternommen werden. Doch während sie im ersten Fall auf die Beseitigung der Ursachen und dabei idealerweise auf die Ausrottung des Problems zielen, wollen präemptive Maßnahmen punktuell und auf die noch nicht eingetretenen Effekte reagieren. Sicherheitsmaßnahmen, die von einer präventiven Logik gesteuert werden, adressieren die Ursachen eines bestimmten Kriminalitätsphänomens und sollen, wenigstens *idealiter*, das *Phänomen beseitigen*. Präemptive Sicherheitsmaßnahmen dagegen wollen punktuellen, besonders schwerwiegenden *Ereignissen zuvorkommen*. Für präemptive Modelle ist es irrelevant, wodurch bestimmte Ereignisse verursacht werden und warum es dazu kommt. Das adressierte (Kriminalitäts-)Phänomen wird nicht im Ganzen bekämpft: Ziel präemptiver Maßnahmen ist vielmehr, wie erwähnt, eine Realisierung der schwerwiegendsten Effekte zu vermeiden.[819]

3.4 Die normativen Implikationen des präemptiven Sicherheitsmodells

Die normativen Implikationen des präemptiven Sicherheitsmodells sind vielfach. Erstens ist diesem Modell eine allumfassende Tendenz immanent. Denn es wird nicht nach etwas gesucht, das im Vorfeld, etwa durch eine Theorie oder – wie im Fall eines repressiven Sicherheitsmodells – vergangene Ereignisse identifiziert wurde. Vielmehr sollen die Ergebnisse der Informationsanalyse selbst die Richtung vorgeben, in der es gesucht werden muss. Das bedeutet, dass die Selektion der relevanten und zu beobachtenden Gegenstände nicht im Vorfeld stattfinden kann. Deswegen neigen präemptive Modelle dazu, möglichst viele Informationen über möglichst

818 Vgl. in dieser Hinsicht die Maßnahmen der verdeckten Kontrolle im SIS (Kapitel 4, Abschnitte 4.6 und 6.1) und den gesamten Ansatz der PNR-Richtlinie (Kapitel 6, Abschnitt 6).

819 Vgl. am deutlichsten den risikobasierten Ansatz der Fluggastdatensätze-Richtlinie (Kapitel 6, Abschnitt 6.2).

viele Individuen oder Ereignisse zu sammeln und zu analysieren. Hier wird die Affinität zur Digitalisierung besonders sichtbar. Obwohl präemptive Systeme auch in einer analogen Welt denkbar sind, bieten Big Data und künstliche Intelligenz ideale Entfaltungsmöglichkeiten für präemptive Modelle. Sie ermöglichen es, die Quantität der erfassten Daten exponentiell zu steigern. Die Antiselektivität der präemptiven Ansätze stößt durch den Einsatz analoger Mittel an faktische Grenzen. In einer digitalen Welt entfallen diese Grenzen.[820]

Zweitens, da im Vorfeld nicht bekannt ist, was genau herausgefunden werden soll, müssen die Systeme offen und flexibel bleiben. Um effektiv zu sein, dürfen sie nicht im Vorfeld übermäßig eingeschränkt werden – sie müssen auf neue Erkenntnisse adaptierbar bleiben. Dieses Merkmal kann als Offenheit des präemptiven Sicherheitsmodells aufgefasst werden.[821]

Drittens ist schließlich ein präemptives Sicherheitsmodell durch Opazität gekennzeichnet: Die Korrelationen, auf denen die Prognosen basieren, müssen nicht erklärbar sein. Anders als kausale Zusammenhänge brauchen sie keine rationale Erklärung, warum sie bestehen. Sie können nur dadurch gerechtfertigt werden, indem ex post gezeigt wird, dass sie funktionieren, d. h., dass sie zu den richtigen Prognosen führen. Diese nicht erklärbaren Korrelationen können im besten Fall offengelegt werden, worauf aber häufig aus strategischen Gründen verzichtet wird, da ihre Offenlegung die Korrelationen zur Manipulierbarkeit exponieren könnte.

Hiermit wird ein weiterer Aspekt der Opazität präemptiver Sicherheitsmodelle deutlich. Denn es wird behauptet, dass Transparenz die Effektivität der Prognose schwächen könnte. Es soll nicht im Vorfeld bekannt gemacht werden, welches Verhalten zu welcher Prognose führt. Verhaltensoptionen werden nicht durch die binäre Trennung zwischen Erlaubtem und Verbotenem unterschieden. Potenziell alles, nicht nur verbotene Handlungen, könnte als Indiz für eine gewisse Prognose interpretiert

820 Besonders illustrativ für diese Tendenz ist die Sammlung nicht sicherheitsbezogener Daten aller Passagiere aufgrund der Fluggastdatensätze-Richtlinie, vgl. Kapitel 6.

821 Besonders deutlich wird dieser Aspekt durch die Bezeichnung des SIS als „flexibles Instrument“ (Kapitel 4, Abschnitt 6.1), die Adaptierbarkeit der Kriterien nach der PNR-Richtlinie (Kapitel 6, Abschnitt 6.3) und, obwohl weniger spezifisch, durch die flexible Verwendung der Prümer Instrumente für die im Vorfeld nicht als prioritär angesehenen Kategorien von Straftaten (Kapitel 5, Abschnitt 4). Offenheit und Flexibilität sind auch die grundlegenden Merkmale der Pläne für die Steigerung der Interoperabilität der europäischen Datenbanken, vgl. Kapitel 7, Abschnitt 4.3.

werden. Damit die Anzeichen richtig interpretiert werden können, soll zudem alles möglichst ungestört und ungesteuert weiterlaufen. In Bezug auf menschliches Handeln, das leicht beinflussbar und steuerbar ist, bedeutet das, dass sich Menschen weiter so verhalten müssen, als ob es keine Kontrollen gäbe. Dafür müssen diese Kontrollen und die zugrunde liegenden Kriterien möglichst verborgen bleiben.[822]

Dies alles ist normativ relevant, weil es grundlegende Mechanismen, die zum Schutz der individuellen Rechte dienen, infrage stellt. Kontrolle wird inhärent anlasslos und tendenziell allumfassend, im Vorfeld kann ihre Logik nicht von den Adressate_innen erkannt und ihre Effektivität nicht demonstriert werden. Die rechtsstaatlichen Grundmechanismen, die im zweiten Kapitel dieses Buches rekonstruiert wurden, sind nach wie vor wichtig, um diese neue Ausrichtung der Sicherheitspolitik kritisch zu überprüfen. Wie ich geschildert habe, reichen sie aber nicht, um die ausufernde Tendenz der präemptiven Sicherheitsmaßnahmen effektiv einzugrenzen. Wie Ralf Poscher gezeigt hat, können fundamentale rechtsstaatliche Prinzipien wie das Verhältnismäßigkeitsprinzip gegen die Logik der präemptiven Sicherheitsmaßnahmen kaum Widerstand leisten. Denn wenn es darum geht, schwere terroristische Angriffe zu vermeiden, können alle Maßnahmen verhältnismäßig scheinen.[823]

Die These, die ich im folgenden Kapitel aufstellen möchte, ist, dass es dafür ein Verständnis von Autonomie braucht, dessen philosophische Prämissen eher auf einem kontroversialistischen als auf einem konsensualistischen Ideal fußen.

822 Vgl. am prominentesten die PNR-Richtlinie (Abschnitt 3.2.3 in diesem Kapitel), aber auch die wachsende Bedeutung der verdeckten Kontrolle im SIS (Kapitel 4, Abschnitte 4.6 und 6.1).

823 Vgl. Poscher, Tendencies in Public Civil Security Law, 71.