SSOAR

Open Access Repository
www.ssoar.info

Intelligente Grenzen und interoperable Datenbanken für die innere Sicherheit der EU: Umsetzungsrisiken und rechtsstaatliche Anforderungen

Bossong, Raphael

Veröffentlichungsversion / Published Version
Forschungsbericht / research report

Zur Verfügung gestellt in Kooperation mit / provided in cooperation with:
Stiftung Wissenschaft und Politik (SWP)

Empfohlene Zitierung / Suggested Citation:
Bossong, R. (2018). *Intelligente Grenzen und interoperable Datenbanken für die innere Sicherheit der EU: Umsetzungsrisiken und rechtsstaatliche Anforderungen.* (SWP-Studie, 4/2018). Berlin: Stiftung Wissenschaft und Politik -SWP- Deutsches Institut für Internationale Politik und Sicherheit. https://nbn-resolving.org/urn:nbn:de:0168-ssoar-57452-7

Nutzungsbedingungen:
Dieser Text wird unter einer Deposit-Lizenz (Keine Weiterverbreitung - keine Bearbeitung) zur Verfügung gestellt. Gewährt wird ein nicht exklusives, nicht übertragbares, persönliches und beschränktes Recht auf Nutzung dieses Dokuments. Dieses Dokument ist ausschließlich für den persönlichen, nicht-kommerziellen Gebrauch bestimmt. Auf sämtlichen Kopien dieses Dokuments müssen alle Urheberrechtshinweise und sonstigen Hinweise auf gesetzlichen Schutz beibehalten werden. Sie dürfen dieses Dokument nicht in irgendeiner Weise abändern, noch dürfen Sie dieses Dokument für öffentliche oder kommerzielle Zwecke vervielfältigen, öffentlich ausstellen, aufführen, vertreiben oder anderweitig nutzen.
Mit der Verwendung dieses Dokuments erkennen Sie die Nutzungsbedingungen an.

Terms of use:
This document is made available under Deposit Licence (No Redistribution - no modifications). We grant a non-exclusive, non-transferable, individual and limited right to using this document. This document is solely intended for your personal, non-commercial use. All of the copies of this documents must retain all copyright information and other information regarding legal protection. You are not allowed to alter this document in any way, to copy it for public or commercial purposes, to exhibit the document in public, to perform, distribute or otherwise use the document in public.
By using this particular document, you accept the above-stated conditions of use.

gesis Leibniz-Institut für Sozialwissenschaften

Mitglied der Leibniz-Gemeinschaft

SWP

SWP-Studie

Raphael Bossong

Intelligente Grenzen und interoperable Datenbanken für die innere Sicherheit der EU

Umsetzungsrisiken und rechtsstaatliche Anforderungen

Stiftung Wissenschaft und Politik
Deutsches Institut für
Internationale Politik und Sicherheit

SWP-Studie 4
April 2018

Die Studie untersucht die Bestrebungen der EU, sogenannte intelligente Grenzen zu schaffen und Datenbanken auszubauen, die der Strafverfolgung und der Migrationskontrolle dienen. Intelligente Grenzkontrollen werden durch die USA schon seit den frühen 2000er Jahren global vorangetrieben. Auf Seiten der EU sorgt die langfristige Entwicklung des Raums der Freiheit, der Sicherheit und des Rechts dafür, dass die Ansprüche an das innereuropäische Informationsmanagement wachsen. Zudem folgt die EU seit 2017 dem übergeordneten Ziel, eine Interoperabilität von Datenbanken zur inneren Sicherheit herzustellen.

Die Bemühungen, die komplexen Reformvorhaben zu verwirklichen, haben sich zuletzt beschleunigt. Dieser Prozess ist mit drei Risiken verbunden. Erstens kann sich die Einführung intelligenter Grenzen über Jahre hinziehen; dabei gibt es in vielen EU-Mitgliedstaaten bereits heute erhebliche Umsetzungsdefizite beim polizeilichen Informationsmanagement. Zweitens drohen überzogene Erwartungen, was die Effektivität intelligenter Grenzen im Kampf gegen Terrorismus und irreguläre Migration betrifft. Drittens besteht kein klarer Zusammenhang zwischen neuer Sicherheitstechnik und den Chancen darauf, die Personenfreizügigkeit aufrechtzuerhalten oder das Vertrauen der Bürger in die EU zu bewahren.

Die Mitgliedstaaten sollten deshalb mit Umsicht agieren, wenn interoperable Datenbanken und digitale Grenzkontrollen geschaffen werden. Vorrang sollten verlässliche rechtsstaatliche Rahmenbedingungen haben. Drei Arbeitsfelder sind dabei vordringlich. Erstens vertiefen neuere Urteile des Europäischen Gerichtshofs die Zweifel, ob es verhältnismäßig ist, die Daten von Reisenden pauschal und anlasslos zu speichern. Zweitens muss das EU-Datenschutzrecht weiter konsolidiert werden. Drittens sind die Verfahren und Rechtswege zu stärken, mit denen sich Einreiseverweigerungen für die EU anfechten lassen.

SWP-Studie

Raphael Bossong

Intelligente Grenzen und interoperable Datenbanken für die innere Sicherheit der EU

Umsetzungsrisiken und rechtsstaatliche Anforderungen

Stiftung Wissenschaft und Politik
Deutsches Institut für
Internationale Politik und Sicherheit

SWP-Studie 4
April 2018

Alle Rechte vorbehalten.
Abdruck oder vergleichbare Verwendung von Arbeiten der Stiftung Wissenschaft und Politik ist auch in Auszügen nur mit vorheriger schriftlicher Genehmigung gestattet.

SWP-Studien unterliegen einem Begutachtungsverfahren durch Fachkolleginnen und -kollegen und durch die Institutsleitung *(peer review)*. Sie geben die Auffassung der Autoren und Autorinnen wieder.

© Stiftung Wissenschaft und Politik, Berlin, 2018

SWP
Stiftung Wissenschaft und Politik
Deutsches Institut für Internationale Politik und Sicherheit

Ludwigkirchplatz 34
10719 Berlin
Telefon +49 30 880 07-0
Fax +49 30 880 07-200
www.swp-berlin.org
swp@swp-berlin.org

ISSN 1611-6372

Inhalt

5 Problemstellung und Empfehlungen

7 Die Entwicklung intelligenter Grenzen und des polizeilichen Informationsmanagements in der EU
8 Grundsatzdebatte über intelligente Grenzen und EU-Sicherheitspolitik
10 Polizeiliches Informationsmanagement
11 Intelligente Grenzen
13 Interoperabilität von Datenbanken

17 Risiken der verdichteten EU-Sicherheitsagenda
17 Umsetzung in den Mitgliedstaaten
19 Effekte auf Terrorismusbekämpfung und irreguläre Migration
21 Sicherheitstechnik und öffentliches Vertrauen

25 Herausforderungen bei Datenschutz und rechtsstaatlicher Aufsicht
25 Die Verhältnismäßigkeit der anlasslosen Datenspeicherung
27 Konsolidierung des europäischen Datenschutzregimes
29 Gestärkte Aufsichts- und Korrekturmechanismen

32 Schlussfolgerungen und Ausblick

34 Abkürzungen

Dr. Raphael Bossong ist Wissenschaftler in der Forschungsgruppe EU/Europa

Intelligente Grenzen und interoperable Datenbanken für die innere Sicherheit der EU. Umsetzungsrisiken und rechtsstaatliche Anforderungen

Wie der Grenzschutz und die innere Sicherheit gestärkt werden können, ist eine der zentralen politischen Fragen der EU. Zwei bekannte Ansätze sind die Stärkung gemeinsamer Institutionen, wie der Europäischen Grenz- und Küstenwache, und die Verlagerung von Kontrollen in die europäische Nachbarschaft. Der dritte und weniger bekannte Ansatz zielt darauf, sogenannte intelligente Grenzen und Infrastrukturen für den grenzüberschreitenden Datenaustausch auszubauen.

Derzeit verfolgen die Europäische Kommission und die EU-Mitgliedstaaten gleich mehrere Maßnahmenstränge für diesen technischen Ansatz: 1. die Erweiterung der Funktionen bestehender EU-Datenbanken zur Migrationskontrolle und polizeilichen Zusammenarbeit, wie des Schengener Informationssystems; 2. die Schaffung neuer Grenzkontrollsysteme, wie einer elektronischen Einreiseerlaubnis und eines biometrischen Ein- und Ausreiseregisters; 3. die systematische Verbindung aller EU-Datenbanken unter dem Schlagwort der »Interoperabilität«, womit auch die EU-Agenturen zur inneren Sicherheit gestärkt werden.

Mit diesem Sicherheitspaket würde sich die EU den Kontrollpraktiken der USA annähern. So sollen alle einreisenden Drittstaatsangehörigen vorab einer Risikobewertung unterzogen und beim Grenzübertritt lückenlos mit biometrischen Daten erfasst werden. Eine integrierte Abfrage von interoperablen Datenbanken könnte Sicherheitsbehörden dabei helfen, gesuchte Personen an der Einreise zu hindern oder innerhalb der EU der Strafverfolgung zuzuführen. Schließlich sollen falsche Dateneinträge oder Fälle von Identitätsmissbrauch durch den stetigen Abgleich von biometrischen Informationen deutlich seltener werden.

Diese technischen Maßnahmen sollen zugleich eine Antwort auf die Vertrauenskrise sein, in welche die deutsche und europäische Politik seit 2015 durch den Anstieg irregulärer Migration und durch schwere Terroranschläge geraten ist. Der Europäische Rat von

Bratislava unterstrich im Herbst 2016, dass elektronisch vernetzte Personenkontrollen als Bestandteil eines größeren Maßnahmenpakets für die innere Sicherheit zu priorisieren seien. Darüber hinaus präsentiert die EU-Kommission interoperable Datenbanken und intelligente Grenzen als zentrale Bausteine für eine europäische »Sicherheitsunion«, die sich in einer wachsenden operativen Zusammenarbeit von Sicherheitsbehörden niederschlägt. Vor diesem Hintergrund beschloss die EU bereits Ende 2017, ein biometrisches Ein- und Ausreisesystem zu schaffen, während 2018 neun weitere Gesetzesvorschläge aus diesem Themenfeld verhandelt werden.

Die vorliegende Studie fragt danach, welche Risiken und Herausforderungen damit einhergehen, dass intelligente Grenzen sowie Datenbanken für Strafverfolgung und Migrationskontrolle beschleunigt ausgebaut werden. Wenn Außengrenzen und innere Sicherheit der EU nachhaltig gestärkt werden sollen, bedarf es einer differenzierten Betrachtung der stark verdichteten und technisch komplexen Reformagenda. So lassen sich die aktuellen EU-Gesetzesvorhaben nur zum Teil als Antwort auf die Migrationskrise und die Terroranschläge seit 2015 verstehen. Zum einen wurden intelligente Grenzen schon seit den frühen 2000er Jahren durch Anforderungen der USA vorangetrieben. Zum anderen erzeugte die innereuropäische Entwicklung des Raums der Freiheit, der Sicherheit und des Rechts wachsende Ansprüche, ein kohärentes Informationsmanagement der Strafverfolgungsbehörden zu verwirklichen. Erst 2016 verknüpfte die Kommission diese zwei Diskussionen und proklamierte das übergeordnete Ziel der Interoperabilität von Datenbanken für Grenzsicherheit und Strafverfolgung.

Aus der Komplexität und der krisengetriebenen Beschleunigung des Maßnahmenpakets ergeben sich drei Risiken. Erstens kann sich die Einführung intelligenter Grenzen über Jahre hinziehen, während in vielen EU-Mitgliedstaaten erhebliche Umsetzungsdefizite beim polizeilichen Informationsmanagement bestehen. Es droht die Glaubwürdigkeit der EU-Sicherheitspolitik zu belasten, wenn ohne klare Priorisierung eine Vielzahl von Reformvorhaben angehäuft wird. Zweitens gibt es das Risiko überzogener Erwartungen, was die Effektivität intelligenter Grenzen im Kampf gegen Terrorismus und irreguläre Migration betrifft. Angesichts der begrenzten Wirkung, die solche Kontrollsysteme in den USA hatten, sowie der gegenwärtigen Bedrohungslage für die EU kann nicht mit einem Wendepunkt gerechnet werden. Drittens besteht kein klarer Zusammenhang zwischen neuer Sicherheitstechnik und dem öffentlichen Bild oder der Legitimität der EU. Bürger nehmen die Lage der inneren Sicherheit Europas nur mittelbar wahr. Die globale Entwicklung der Biometrie und der automatisierten Datenanalyse kann aber gesellschaftliche Sorgen vor einer zunehmenden Überwachung verstärken.

Somit ist der Ausbau von intelligenten Grenzen und interoperablen Datenbanken ein langfristiger wie anspruchsvoller Prozess, der vor allem die reguläre grenzüberschreitende Polizeiarbeit und die Verwaltung legaler Migration betrifft. Die EU-Mitgliedstaaten sollten sich aus einer kurzfristigen Entscheidungsdynamik hin zu mehr Sicherheitstechnik lösen und drei spezifische Herausforderungen bearbeiten, um einen verlässlichen rechtsstaatlichen Rahmen für intensivierte Grenzkontrollen und Datenverarbeitungsprozesse der Sicherheitsbehörden zu gewährleisten.

Erstens verschärfen neuere Urteile des Europäischen Gerichtshofs die Frage, inwiefern eine anlasslose Datenspeicherung verhältnismäßig ist. Die bereits beschlossene EU-Richtlinie zur Auswertung von Fluggastdaten (PNR), die als Bestandteil intelligenter Grenzen gilt, sollte deshalb überdacht werden. Zweitens ist es eine dringende Aufgabe, das EU-Datenschutzrecht zu konsolidieren. Beachtet werden sollten dabei vor allem die Umsetzung der Datenschutzrichtlinie für Strafverfolgungsbehörden und die laufenden Verhandlungen über eine Neufassung der Datenschutzverordnung für EU-Organe. Technische Lösungen zur Datensparsamkeit sind im Rahmen der Interoperabilität nicht ausreichend. Drittens sollten die Verfahren und Rechtswege gestärkt werden, mit denen sich Einreiseverweigerungen für die EU anfechten lassen. Anlass dazu geben neue Mechanismen der Risikobewertung, die stärkere Nutzung der Biometrie sowie die steigende Zahl an betroffenen Drittstaatsangehörigen. Darüber hinaus werden künftig im Rahmen einer neuen elektronischen Einreiseerlaubnis für die Schengen-Zone (ETIAS) nachrichtendienstliche Informationen genutzt, um eine europäische Warnliste zu Terroristen und Schwerverbrechern zu erstellen. Deshalb sollte auch die politische Aufsicht über Europol, das die Warnliste mitgestalten soll, vertieft werden.

Die Entwicklung intelligenter Grenzen und des polizeilichen Informationsmanagements in der EU

Seit 2015 hat sich eine intensive Debatte entwickelt, wie die EU ihre Außengrenzen besser sichern kann. Grundsätzlich lassen sich dabei drei Ansätze erkennen. Erstens besteht die Option, den europäischen Grenzschutz zu vergemeinschaften. Eigenständige EU-Kräfte zur Sicherung der Grenzen wurden von führenden Politikern wiederholt als langfristig notwendiges Integrationsziel genannt.[1] Die im Sommer 2016 verabschiedete Reform der EU-Grenzschutzbehörde Frontex, die zur Europäischen Agentur für die Grenz- und Küstenwache umbenannt wurde, blieb noch ein deutliches Stück dahinter zurück.[2] Der zweite Ansatz ist die sogenannte Externalisierung der europäischen Grenzsicherung in Drittstaaten. Die Externalisierung kann bereits seit Mitte der 2000er Jahre als eine explizite Strategie der EU gelten;[3] sie schlug sich seither in zahlreichen Partnerschaftsabkommen und Finanzierungsinstrumenten nieder. Ins Zentrum der Debatte rückte sie aber erst ab 2016 durch das Flüchtlingsabkommen mit der Türkei und durch politische Anstrengungen für vergleichbare Regelungen mit Nordafrika.[4]

Diese Studie widmet sich dem dritten und öffentlich eher wenig diskutierten Ansatz, um Grenzsicherung und innere Sicherheit der EU zu stärken. Er besteht in der technischen Modernisierung und Vernetzung von Grenz- und Personenkontrollen sowie einem erleichterten Datenzugriff für Strafverfolgungsbehörden. Um die Freizügigkeit zu erhalten und eine verbesserte Terrorismusbekämpfung zu gewährleisten,[5] soll die EU — so die Bratislava-Erklärung — lückenlos alle Ein- und Ausreisen von Drittstaatsangehörigen biometrisch erfassen und eine elektronische Einreiseerlaubnis für visabefreite Reisende schaffen. Darüber hinaus sollen Polizei- und Grenzschutzbehörden besser auf Informationen aus unterschiedlichen EU-Datenbanken zugreifen kön-

1 Die vielbeachtete Grundsatzrede, die Frankreichs Präsident Emmanuel Macron im September 2017 zum Thema Europa hielt, nahm Bezug auf diese Vision. Siehe »Sorbonne Speech of Emmanuel Macron — Full text/English version«, 26.9.2017, <http://international.blogs.ouest-france.fr/archive/2017/09/29/macron-sorbonne-verbatim-europe-18583.html> (Zugriff am 4.12.2017). Auch im Zuge der Verhandlungen über den nächsten Finanzrahmen der EU wird eine solche Option debattiert. Siehe Europäische Kommission, *EU Budget for the Future*, 14.2.2018, <https://ec.europa.eu/commission/sites/beta-political/files/what-kind-of-europe-for-our-future_en.pdf> (Zugriff am 26.2.2018).

2 Die personellen wie materiellen Kapazitäten der Agentur wurden ausgeweitet. Zudem erhielt sie den Auftrag, nach »Schwachstellen« an den europäischen Außengrenzen zu suchen. Keine hinreichende Zustimmung fand indes der Vorschlag, dass es Frontex möglich sein solle, Grenzsicherungsmaßnahmen auch gegen den Willen eines betroffenen Mitgliedstaates durchzuführen.

3 Andrew Geddes, »Europe's Border Relationships and International Migration Relations«, in: *Journal of Common Market Studies*, 43 (2005) 4, S. 787–806.

4 Anne Koch/Annette Weber/Isabelle Werenfels (Hg.), *Migrationsprofiteure? Autoritäre Staaten in Afrika und das europäische Migrationsmanagement*, Berlin: Stiftung Wissenschaft und Politik, April 2018 (SWP-Studie 3/2018).

5 Europäischer Rat, *Erklärung von Bratislava*, 16.9.2016, S. 3f, <www.consilium.europa.eu/media/21232/160916-bratislava-declaration-and-roadmap-de.pdf> (Zugriff am 4.12.2017).

nen, um Identitätsmissbrauch zu verhindern und Ermittlungen zu beschleunigen.

Im Folgenden werden die politischen Konflikte und Entwicklungslinien aufgeschlüsselt, die im Zusammenhang mit dieser vermeintlich technischen Agenda bestehen. Zum einen befinden sich staatliche Grenzen in einem strukturellen Veränderungsprozess, weil die internationale Mobilität beständig wächst. Zum anderen ergeben sich kritische Fragen, was Effektivität und normative Auswirkungen von sogenannten intelligenten Grenzen angeht. Die EU ist dabei nicht nur ein besonderes Anwendungsfeld für die transnationale Vernetzung von Sicherheitsbehörden und Infrastrukturen. Historisch betrachtet wurden über polizeiliches Informationsmanagement und intelligente Grenzen lange zwei verschiedene Diskussionen geführt. Erst ab 2016, unter dem Eindruck der Sicherheits- und Migrationskrise, wurde das Ziel von Interoperabilität als übergreifende Klammer für diese zwei Reformstränge postuliert.

Grundsatzdebatte über intelligente Grenzen und EU-Sicherheitspolitik

Während der vergangenen zwei Jahrzehnte hat sich die Bedeutung von Grenzen in allen Industriegesellschaften fundamental gewandelt. Kontrollen, die traditionell an physischen Grenzen durchgeführt wurden, virtualisieren sich und erfolgen zunehmend innerhalb und außerhalb des staatlichen Territoriums.[6] Hoheitliche Aufgaben zur Wahrung der öffentlichen Sicherheit verschwimmen in einem informationstechnischen Netzwerk von mehrfachen Vor- und Nachkontrollen, die neben Polizei und Grenzschutzbehörden auch private Firmen (Fluggesellschaften, Sicherheitsdienstleister etc.) und andere Verwaltungsstellen (etwa Ausländerämter) miteinbeziehen. Die intelligenten Grenzen, die daraus resultieren, sollen nicht als direkter Ersatz für physische Barrieren dienen und den Nationalstaat abschotten. Erreichen will man vielmehr, dass sich internationale Mobilität gezielt steuern und flexibel absichern lässt.[7] Als Ideal gilt eine möglichst weitgehende Reisefreiheit, die durch punktgenaue Risikoanalysen und globale Warnlisten zu Terroristen und Schwerverbrechern flankiert wird. Selbst für ärmere Staaten könnte somit der Weg für eine Visaliberalisierung bereitet werden. Anstelle der traditionellen Einstufung nach Risikoländern tritt zunehmend eine individuelle Bewertung von Reisenden auf Basis automatisierter Datenanalysen.[8]

Kritiker dagegen bemerken, dass der versprochene Mehrwert intelligenter Grenzen zweifelhaft sei. Dies gelte insbesondere für die Abwehr des internationalen Terrorismus. Abgesehen vom Ausnahmeereignis des 11. September 2001 seien Drittstaatsangehörige, die sich an Außengrenzen kontrollieren lassen, keine zentrale Gefahrenquelle.[9] Tatsächlich wurden die allermeisten Anschläge in Europa und den USA von langfristig ansässigen Personen oder eigenen Staatsbürgern verübt.[10] Darüber hinaus kosten intelligente Grenzsysteme oft weit mehr als veranschlagt,[11] während zusätzliche Nachteile oder nichtmonetäre Kosten für individuelle Reisende entstehen. So schafft die individuelle Risikobewertung neue Formen der Diskriminierung zwischen hochmobilen Eliten — sogenannten Trusted Travellers[12] — und allen ande-

6 Peter Shields, »Borders as Information Flows and Transnational Networks«, in: *Global Media and Communication*, 10 (2014) 1, S. 3–33.

7 Deloitte Report, *Smart Borders – Increasing Security without Sacrificing Mobility*, Deloitte Development LLC 2014, <https://www2.deloitte.com/content/dam/Deloitte/global/Documents/Public-Sector/dttl-ps-GMBM-Border-Point-Booklet.pdf> (Zugriff am 4.12.2017).

8 Paul De Hert/Rocco Bellanova, *Transatlantic Cooperation on Travelers' Data Processing: From Sorting Countries to Sorting Individuals*, Washington, D.C.: Migration Policy Institute, März 2011 (Migration Policy Institute Paper), <http://immigrationresearch-info.org/system/files/dataprocessing-2011.pdf> (Zugriff am 4.12.2017).

9 National Consortium for the Study of Terrorism and Responses to Terrorism, *Border Crossings and Terrorist Attacks in the United States: Lessons for Protecting against Dangerous Entrants*, College Park, MD: November 2012, <www.start.umd.edu/start/publications/START_BorderCrossingsTerroristAttacks.pdf> (Zugriff am 19.3.2018).

10 Manni Crone/Martin Harrow, »Homegrown Terrorism in the West«, in: *Terrorism and Political Violence*, 23 (2011) 4, S. 521–536; Peter Bergen/Albert Ford/Alyssa Sims/David Sterman, *Terrorism in America after 9/11. New America Project Report*, Washington, D.C. 2017, <https://www.newamerica.org/in-depth/terrorism-in-america/> (Zugriff am 5.2.2018).

11 United States Government Accountability Office, *Testimony Before the Subcommittee on Immigration and the National Interest, U.S. Senate*, Juli 2016, <http://trac.syr.edu/immigration/library/P11325.pdf> (Zugriff am 4.12.2017).

12 Siehe zu den praktischen Erleichterungen für diese »vertrauenswürdigen Reisenden« an US-Flughäfen: Depart-

ren Personen.[13] Vor allem leidet die Privatsphäre, wenn Daten im Vorfeld von Grenzen erhoben werden.[14] Schließlich steht die Frage im Raum, ob die automatisierten Analysen und Entscheidungsprozesse intelligenter Grenzen zur Erosion rechtsstaatlicher Verantwortlichkeit führen.[15]

Für Sicherheitsbehörden könnte die grenzüberschreitende Zusammenarbeit selbstverständlich werden.

Vor dem Hintergrund dieser Grundsatzdebatte stellt die EU ein besonderes Anwendungsfeld für intelligente Grenzen dar. Der gesamte europäische Integrationsprozess ist darauf ausgerichtet, die Mobilität von Waren, Gütern, Dienstleistungen und Personen zu befördern. Seit den 1990er Jahren besteht zusätzlich die Ambition, den Rückbau nationaler Grenzen im Schengen-Raum durch eine vernetzte Sicherheitszusammenarbeit zu kompensieren.[16] Für diesen Zweck sind technische Infrastrukturen und polizeiliche Datenbanken von zentraler Bedeutung. Noch vor Übernahme des Schengen-Kodex in EU-Recht legte das Schengener Informationssystem (SIS) den Grundstein für eine tägliche Zusammenarbeit von Polizei- und Grenzschutzbehörden. Anstelle einer zentralen europäischen Agentur entstand zunächst ein horizontaler Informations- und Verwaltungsverbund[17] zwischen nationalen Sicherheitsbehörden, was sich mit dem Konzept intelligenter Grenzen überschneidet.[18]

Vergleichbar könnte die von der Europäischen Kommission verfolgte Idee einer Sicherheitsunion[19] in Zukunft an Substanz gewinnen, wenn technische Infrastrukturen ausgebaut werden.[20] Bereits seit 2015 steigt die Nutzung europäischer Datenbanken für Migrationssteuerung und polizeiliche Zusammenarbeit deutlich an.[21] Neue intelligente Grenzen und stärker vernetzte Datenbanken sollen diese Entwicklung beschleunigen. Somit könnte auf Ebene der Sicherheitsbehörden — und jenseits politischer Souveränitätsfragen — die grenzüberschreitende Zusammenarbeit und europäische Informationsverarbeitung zur Selbstverständlichkeit werden.

Kritiker wiederum betrachten diese Art der technokratischen Integration als illegitim und undemokratisch. Steigende Investitionen in Sicherheitstechnik korrespondieren im Urteil einiger linksliberaler Beobachter mit einer einseitigen wirtschaftspolitischen Ausrichtung der EU. Seit dem 11. September ist ein globaler Markt der »Homeland Security« entstanden. Während diese Sicherheitsindustrie in den Vereinigten Staaten seither eine zentrale Rolle erlangt hat,[22] lässt sich auch eine wachsende Repräsentanz und Vernetzung entsprechender Akteure in EU-Gremien nachweisen.[23] Europäische Entscheidungsträger

ment of Homeland Security, »Trusted Traveler Programs«, <https://www.cbp.gov/travel/trusted-traveler-programs> (Zugriff am 13.4.2018).

13 Louise Amoore, »Biometric Borders. Governing Mobilities in the War on Terror«, in: *Political Geography*, 25 (2006) 3, S. 336—351.

14 Polly Pallister-Wilkins, »How Walls Do Work: Security Barriers as Devices of Interruption and Data Capture«, in: *Security Dialogue*, 47 (2016) 2, S. 151—164; Michiel Besters/Frans W.A. Brom, »›Greedy‹ Information Technology. The Digitalization of the European Migration Policy«, in: *European Journal of Migration and Law*, 12 (2010) 4, S. 455—470.

15 Holger Pötzsch, »The Emergence of iBorder. Bordering Bodies, Networks, and Machines«, in: *Environment and Planning D: Society and Space*, 33 (2015) 1, S. 101—118.

16 Morten J. Pedersen, »The Intimate Relationship between Security, Effectiveness, and Legitimacy. A New Look at the Schengen Compensatory Measures«, in: *European Security*, 24 (2015) 4, S. 541—559.

17 Bettina Schöndorf-Haubold, *Europäisches Sicherheitsverwaltungsrecht*, Baden-Baden 2010.

18 Magdalena König, »The Borders, They Are A-Changin'! The Emergence of Socio-digital Borders in the EU«, in: *Internet Policy Review*, 5 (2016) 1, S. 1—14.

19 Bei der Sicherheitsunion geht es im Kern darum, die vertragsrechtlichen Beschränkungen der EU für die innere Sicherheit — siehe u.a. Artikel 4(2) EUV — soweit wie möglich zu überwinden und eine gemeinschaftliche Verantwortlichkeit der EU-Mitgliedstaaten auf diesem Politikfeld zu befördern.

20 Der zuständige EU-Kommissar Julian King veröffentlicht seit Anfang 2017 monatliche Berichte zur Sicherheitsunion. Neben der Cybersicherheit gelten intelligente Grenzen und die Vernetzung von EU-Datenbanken als zentrale Vorhaben, vgl. Europäische Kommission, *Twelfth Progress Report towards an Effective and Genuine Security Union*, COM (2017) 779 final, 12.12.2017.

21 eu-LISA, *Consolidated Annual Activity Report 2016*, 21.3.2017, S. 15—18.

22 Dana Priest/William Arkin, *Top Secret America. The Rise of the New American Security State*, New York 2011.

23 Ruben Andersson, »Europe's Failed ›Fight‹ against Irregular Migration: Ethnographic Notes on a Counterproductive Industry«, in: *Journal of Ethnic and Migration Studies*, 42 (2016) 87, S. 1055—1075; Transnational Institute Report,

tauschen sich verstärkt mit Organisationen der Sicherheitsindustrie aus. Dies könnte dazu beitragen, dass der Nutzen neuer Kontrolltechnologien nicht hinreichend kritisch hinterfragt wird.[24]

Zusammengefasst bietet sich das Bild einer stark polarisierten Debatte. Befürworter intelligenter Grenzen unterstreichen, dass es notwendig sei, die internationale Mobilität in technisch moderner Weise zu verwalten. Die Vernetzung von Informationsinfrastrukturen, die den Abbau physischer Grenzen kompensieren soll, trifft sich dabei mit zentralen Zielen der europäischen Integration. Kritiker betonen hingegen, dass intelligente Grenzen mit hohen finanziellen und normativen Kosten verbunden seien, während die EU einseitig von wirtschaftlichen Interessen beeinflusst werden könnte.

Um die kommenden Herausforderungen für die EU-Innenpolitik differenziert bewerten zu können, muss man die Vorgeschichte der aktuellen Reformagenda genauer betrachten. Dabei zeigt sich, dass es in den vergangenen zwei Jahrzehnten unterschiedliche Entwicklungspfade für das polizeiliche Informationsmanagement und für intelligente Grenzen gab. Erst seit 2016 haben sich diese Debatten stark beschleunigt und verdichtet, was sich im übergeordneten Ziel der Interoperabilität niederschlägt.

Polizeiliches Informationsmanagement

Das Schengener Informationssystem entstand bereits im Jahr 1995, um den Wegfall der Binnengrenzkontrollen zu kompensieren. 1998 wurde der »Raum der Freiheit, der Sicherheit und des Rechts« (RFSR) zu einem expliziten Integrationsziel der EU. Auf dieser Grundlage schuf man Konzepte des »gegenseitigen Vertrauens« und der »Verfügbarkeit« von Informationen. Diese Konzepte bedeuten im Kern, dass Strafverfolgungsbehörden bei grenzüberschreitenden Verfahren dieselben Ermittlungsmöglichkeiten und Informationszugänge haben sollen, über die sie national verfügen.[25] Neben ersten rechtlichen Instrumenten für diesen Informationsaustausch[26] wurde ab Mitte der 2000er Jahre eine neue Generation des Schengener Informationssystems (SIS II) ins Auge gefasst. Das SIS II sollte insbesondere die automatisierte Speicherung und Abfrage von Fingerabdrücken ermöglichen.[27] Und schon damals trat die Europäische Kommission mit ersten Ideen zur »Interoperabilität« von Datenbanken im RFSR hervor.[28]

Doch diese Vorhaben stagnierten. Gründe waren technische Hürden bei der Umsetzung, die Unkenntnis vieler nationaler Behörden über den recht jungen EU-Rahmen sowie die Herausforderung der EU-Osterweiterung. Angeführt von Deutschland setzten einige Mitgliedstaaten stattdessen darauf, die polizeiliche Zusammenarbeit in flexiblen Koalitionen zu vertiefen, was sich vor allem im Prümer Vertrag von 2005 niederschlug.[29] Dadurch wurde unter anderem ein horizontaler Austausch von Kraftfahrzeug-, Fingerabdruck- und DNA-Daten zur Strafverfolgung eröffnet.[30] Auf EU-Ebene beschloss man derweil ein horizontales System für den erleichterten Austausch von Strafregistern unter EU-Mitgliedstaaten (ECRIS).[31]

Erst ab 2010 ließ sich auf Grundlage des Lissabonner Vertrags eine neue Kooperationsstufe angehen. Das bis dahin gesonderte Regime der strafrechtlichen Zusammenarbeit wurde von der »dritten Säule« — mit einigen Ausnahmen — in das allgemeine EU-Recht überführt. Dieser Integrationsschritt wurde von einer ersten EU-Strategie für die innere Sicherheit begleitet.[32] Eine flankierende Fachstrategie zum

Market Forces: The Delevopment of the EU Security-Industrial Complex, 2014, <https://www.tni.org/en/publication/market-forces-the-development-of-the-eu-security-industrial-complex> (Zugriff am 4.12.2017).

24 Kristrún Gunnarsdóttir/Kjetil Rommetveit, »The Biometric Imaginary: (Dis)trust in a Policy Vacuum«, in: *Public Understanding of Science*, 26 (2017) 2, S. 195–211.

25 Weitere Antriebe waren die terroristischen Anschläge am 11. September 2001 in den USA und am 11. März 2004 in Madrid. Als erstrebenswert galt fortan, sicherheitsrelevante Informationen weitreichend zu teilen, statt sie auf einen engen Kreis von Behörden zu beschränken.

26 Darunter der sogenannte Schwedische Rahmenbeschluss.

27 Europäische Kommission, COM (2005) 230, 31.5.2005.

28 Europäische Kommission, COM (2005) 597, 24.11.2005.

29 Die ursprünglichen Unterzeichner dieses Vertrags, der informell ebenfalls als Schengen II bezeichnet wurde, waren Deutschland, Frankreich, Belgien, Niederlande, Luxemburg, Spanien und Österreich.

30 Große Teile des Prümer Vertrags wurden 2007 unter Ägide der deutschen Ratspräsidentschaft in EU-Recht überführt, was aber nichts an der dezentralen Informationsinfrastruktur änderte.

31 European Criminal Records System.

32 Rat der Europäischen Union, 6870/10, 25.2.2010.

Die wichtigsten EU-Datenbanken für Grenzkontrolle und innere Sicherheit

EURODAC: Zentral geführte EU-Datenbank zur Erfassung der Fingerabdrücke von Asylbewerbern und irregulären Einwanderern an EU-Außengrenzen. Primärer Zweck ist die Feststellung der nationalen Zuständigkeit zur Bearbeitung des Asylverfahrens nach dem sogenannten Dublin-Verfahren.

VIS: Zentral geführte EU-Datenbank mit Visumsanträgen für die Schengen-Zone, einschließlich der Fingerabdrücke der Antragsteller. Wird in der Regel bei der Bearbeitung eines Visumsantrags und zur Verifikation des Visums bei Grenzübertritt konsultiert.

SIS II: Multifunktionales und weitgehend dezentral geführtes polizeiliches Informationssystem zur Personen- und Sachfahndung sowie zur erleichterten Durchsetzung von aufenthaltsrechtlichen Entscheidungen in der Schengen-Zone.

polizeilichen Informationsmanagement[33] sah zahlreiche Maßnahmen vor, die bis heute verfolgt werden, unter anderem eine Stärkung des SIS, die Verbesserung der Datenqualität sowie kohärente grenzüberschreitende Abfragemechanismen.

Parallel dazu wuchs die Rolle von Europol, Frontex und der 2011 geschaffenen »Europäischen Agentur für das Betriebsmanagement von IT-Großsystemen im Bereich Freiheit, Sicherheit und Recht« (eu-LISA). Diese Agentur sollte primär die — seit Mitte der 2000er Jahre aufgebauten — EU-Datenbanken für Asylbewerber (EURODAC) und kurzzeitige Besucher (VIS) unterstützen (siehe Kasten). Zusätzlich sollte eu-LISA die stark verzögerte Inbetriebnahme von SIS II voranbringen,[34] die ab 2013 schließlich gelang — jedoch noch ohne die Möglichkeit, Fingerabdrücke automatisiert abzufragen. Allerdings wurde zur Bekämpfung von schwerer Kriminalität und internationalem Terrorismus eine Ausnahmeregelung beschlossen; sie ermöglicht bei entsprechenden Fällen eine polizeiliche Abfrage von Fingerabdrücken in den Datenbanken EURODAC und VIS, die ansonsten der Migrationskontrolle dienen.[35]

Diese internen Entwicklungen der EU-Sicherheitspolitik fielen von Sommer 2014 an mit dem rasanten Eroberungsfeldzug des »Islamischen Staates« in Teilen Syriens und des Irak zusammen. Spätestens ab dieser Zeit arbeiteten mehrere EU-Mitgliedstaaten mit Hochdruck daran, sowohl eigenen Staatsbürgern als auch langjährig ansässigen Drittstaatsangehörigen eine Ausreise in das vom IS kontrollierte Gebiet zu verwehren. Im Frühjahr 2015 — unter dem Eindruck des Pariser Anschlags auf die Redaktion von Charlie Hebdo — präsentierte die neue EU-Kommission unter Präsident Jean-Claude Juncker schließlich eine »EU-Agenda für Sicherheit«.[36] Zentrale Ziele dieser Agenda waren der verbesserte polizeiliche Informationsaustausch unter Einbeziehung von Europol und die stärkere Nutzung des SIS zur Terrorismusbekämpfung.

Intelligente Grenzen

Unmittelbar nach den Anschlägen vom 11. September 2001 verabschiedeten die USA ein umfassendes Programm zur Modernisierung ihrer Grenzkontrollen. Diese »Smart Borders Initiative« beinhaltete neue Sicherheitsstandards für Reisedokumente, die systematische Auswertung von erweiterten Fluggastdaten (PNR)[37] sowie die Einführung einer elektronischen Einreiseerlaubnis (ESTA)[38] für visabefreite Reisende. Zudem wurde ein gesondertes Registrierungsprogramm für Einreisende aus mutmaßlichen muslimischen Risikoländern geschaffen.[39] Dieses überführte man ab 2004 in ein weniger diskriminierendes, aber flächendeckendes biometrisches Ein- und Ausreiseregister (EES)[40] für alle Drittstaatsangehörige. Schließlich wurden biometrische Visa verlangt und ein

33 Rat der Europäischen Union, 16637/09, 25.11.2009.

34 Joanna Parkin, *The Difficult Road to the Schengen Information System II: The Legacy of ›Laboratories‹ and the Cost for Fundamental Rights and the Rule of Law*, Brüssel: Centre for European Policy Studies (CEPS), April 2011 (CEPS Paper), <http://aei.pitt.edu/31282/1/SIS_II_paper_liberty_security_formatted1%5B1%5D.pdf> (Zugriff am 4.2.2018).

35 Diese Art der Abfrage sollte allerdings nur möglich sein, wenn keine anderen Daten oder Spuren für die Aufklärung oder Gefahrenabwehr zur Verfügung stehen.

36 Europäische Kommission, COM (2015) 185, 28.4.2015.

37 Passenger Name Records.

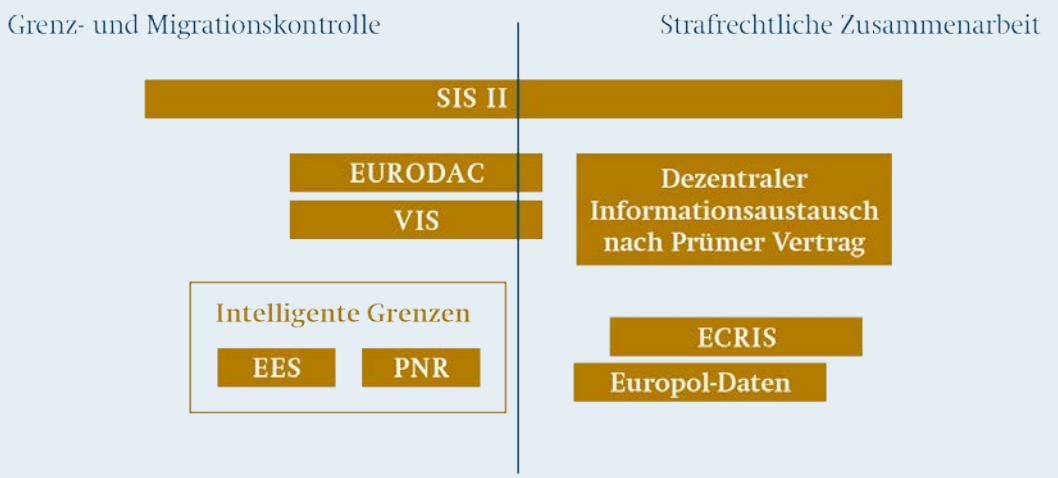
38 Electronic System for Travel Authorization.

39 United States Department of Justice, »Attorney General Prepared Remarks on the National Security Extry-Exit Registration System«, 6.6.2002, <https://www.justice.gov/archive/ag/speeches/2002/060502agpreparedremarks.htm> (Zugriff am 4.12.2017).

40 Entry-Exit System.

Graphik 1

EU-Datenbanken und Vorschläge für intelligente Grenzen 2013



Quelle: eigene Darstellung

umfassendes Screening-System für Terrorismusverdächtige mit Input aller US-Sicherheitsbehörden aufgebaut.[41]

Diese Agenda hatte umfassende internationale Auswirkungen. Biometrische Reisedokumente und die Übermittlung von PNR-Daten wurden zur Bedingung, um visafrei in die USA einreisen zu können.[42] Die EU beschloss recht zügig entsprechende Anpassungen bei der Dokumentensicherheit. Dagegen führte die Anforderung, Fluggastdaten zu übermitteln, zu schwierigen transatlantischen Verhandlungen und einer Serie von rechtlichen Anfechtungen über die gesamten 2000er Jahre.[43] Auch vor diesem Hintergrund versuchte die EU, sich aus einer passiven Reaktion zu lösen. Ab 2008 wurde das EU-Visainformationssystem aufgebaut, das nach amerikanischem Vorbild die biometrischen Daten und Fingerabdrücke von Antragstellern speichern sollte.[44] Parallel dazu präsentierte die Kommission erste Vorschläge für ein europäisches EES und ein eigenes PNR-System. Zu diesem Zeitpunkt gelang es jedoch nicht, dafür substantielle Unterstützung unter den Mitgliedstaaten zu mobilisieren. Befürchtet wurden massive Kostensteigerungen, nachdem es sich in den USA als sehr viel schwieriger denn geplant erwiesen hatte, das EES einzurichten.[45] Zugleich galt in Europa zwischen 2008 und 2012 die Bedrohung durch islamistischen Terrorismus internationaler Herkunft als vergleichs-

41 Homeland Security Directive Nr. 6 und 13 aus dem Jahr 2003, <https://www.pillsburylaw.com/images/content/2/6/v2/2605/5063B9DEFBD850B93561F589DC52D0F3.pdf> (Zugriff am 4.12.2017).

42 Als Vorreiter verschrieb sich Kanada noch 2001 der gesamten US-Programmatik. The Standing Senate Committee on Banking, Trade and Commerce, *Facilitating the Movement of Goods and People in a Security Environment*, 2002, <https://sencanada.ca/Content/SEN/Committee/371/bank/rep/rep17jun02-e.htm> (Zugriff am 4.12.2017).

43 Christian Kaunert/Sarah Léonard/Alex MacKenzie, »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*, 21 (2012) 4, S. 474–496.

44 Aus technischen Gründen dauerte die Umsetzung der biometrischen Datenerfassung in allen visapflichtigen Drittstaaten bis 2014.

45 C. Richard Neu, *Is It Time to Rethink U.S. Entry and Exit Processes?*, Santa Monica, CA: Rand Corporation, 2009 (Occasional Paper), <https://www.rand.org/content/dam/rand/pubs/occasional_papers/2009/RAND_OP235.pdf> (Zugriff am 4.12.2017); Ben Hayes/Mathias Vermeulen, *Borderline – Assessing the Costs and Fundamental Rights Implications of EUROSUR and the »Smart Borders« Proposals*, Berlin: Heinrich-Böll-Stiftung, Juni 2012, S. 41ff, <https://www.boell.de/sites/default/files/DRV_120523_BORDERLINE_-_Border_Surveillance.pdf> (Zugriff am 19.3.2018).

weise gering.[46] Die Kommission merkte an, die zentrale Herausforderung im Kampf gegen den Terrorismus bestehe darin, dass sich EU-Bürger oder langfristig ansässige Drittstaatsangehörige radikalisierten.[47] Alternative ökonomische Begründungen für die Einführung intelligenter Grenzen — wie etwa die Installation von automatisierten Grenzkontrollpunkten (ABC Gates)[48] zum schnelleren Passagierdurchsatz — entfalteten keine politische Dynamik, nicht zuletzt weil die Eurokrise zunehmend die Agenda beherrschte.

2013 legte die Kommission ein angepasstes Vorschlagspaket zu intelligenten Grenzen vor, wobei die finanziellen Kosten der Umsetzung niedriger als zuvor veranschlagt wurden.[49] Das Europäische Parlament verweigerte aber aus Gründen des Datenschutzes und der Verhältnismäßigkeit erneut seine Zustimmung.[50] Im Sommer 2015 unternahm die neue Juncker-Kommission einen weiteren Versuch, die anhaltende Kritik[51] an intelligenten Grenzen auszuräumen; sie stützte sich dabei auf erste EU-Pilotprojekte.[52] Trotz der sich zuspitzenden Flüchtlingskrise schien nach wie vor ein langwieriger Verhandlungsprozess bevorzustehen.

Interoperabilität von Datenbanken

Ende 2015 entwickelte sich eine neue politische Dynamik. Die schweren Anschläge von Paris im November des Jahres zeigten, dass die Kontrollen an EU-Außengrenzen nicht engmaschig genug waren, um terroristische Akteure aufzuhalten. Wie die Ermittlungen erwiesen, waren einige der Attentäter gezielt als Flüchtlinge über Griechenland eingeschleust worden.[53] Der führende Kopf der Zelle pendelte nicht nur zwischen Belgien und Frankreich, sondern konnte seit 2010 mehrfach unbehelligt nach Syrien reisen.[54] Deshalb wurde auf Betreiben Frankreichs ins Auge gefasst, systematische Ausreisekontrollen, bei denen das SIS zu etwaigen Einträgen abgefragt wird, auf alle EU-Bürger auszuweiten.[55] Derweil stellte sich im Zuge der Flüchtlingskrise heraus, dass viele Schutzsuchende und irreguläre Einwanderer nicht mehr registriert werden konnten. Das neue EU-Instrument der »Hotspots« half zwar an besonders belasteten Grenzabschnitten in Griechenland und Italien, zu einer systematischen Erfassung der anlandenden Personen zurückzukehren. Allerdings gab es auf dem Höhepunkt der Flüchtlingskrise auch in Deutschland große Lücken und zahlreiche Fehler bei der Registrierung.

Weiter erhöht wurde der Handlungsdruck durch die Terroranschläge von Brüssel im März 2016. Das Europäische Parlament gab seinen langjährigen Widerstand gegen das Vorhaben auf, ein eigenes PNR-System der EU im Gegenzug für eine Ausweitung des

46 Die jihadistisch inspirierten Anschläge von Mohammed Merah, der im März 2012 in Südfrankreich sieben Menschen ermordete, sind im Rückblick als Wendepunkt hin zu der hohen Gefahrenlage zu werten, die in Europa bis heute gilt.

47 Europäische Kommission, SEC (2008) 154, 13.2.2008.

48 Automated Border Control Gates.

49 Europäische Kommission, »›Intelligente Grenzen‹: Mehr Mobilität und Sicherheit«, Pressemitteilung, Brüssel, 28.2.2013, <http://europa.eu/rapid/press-release_IP-13-162_de.htm> (Zugriff am 27.3.2018).

50 Simon Sontowski, »Speed, Timing and Duration: Contested Temporalities, Techno-political Controversies and the Emergence of the EU's Smart Border«, in: *Journal of Ethnic and Migration Studies* (online first), 21.11.2017, <https://doi.org/10.1080/1369183X.2017.1401512> (Zugriff am 13.2.2018).

51 European Data Protection Supervisor, *Formal Comments of the EDPS on the European Commission Public Consultation on smart borders*, 3.11.2015, <https://edps.europa.eu/sites/edp/files/publication/15-11-03_comments_smart_borders_en.pdf> (Zugriff am 4.12.2017).

52 eu-LISA, *Smart Borders Pilot Project – Report on the Technical Conclusions of the Pilot*, November 2015, <www.eulisa.europa.eu/Publications/Reports/Smart%20Borders%20-%20Technical%20Report.pdf> (Zugriff am 4.12.2017).

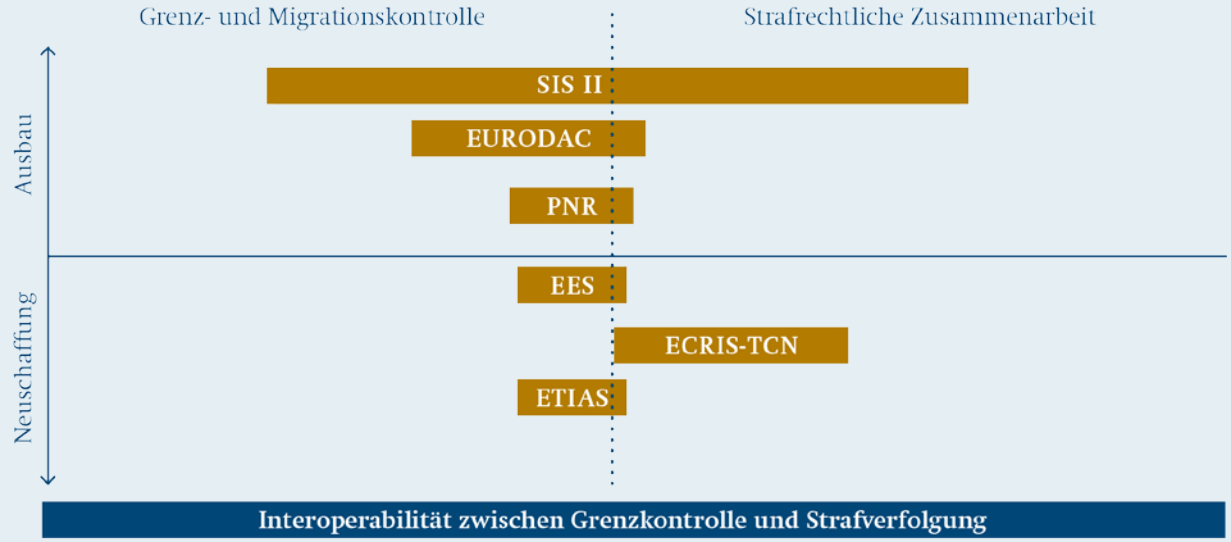
53 Die USA stellten offiziell fest, dass die Flüchtlingskrise genutzt wurde, um terroristische Akteure einzuschleusen. Dies führte zu neuen Diskussionen mit den meisten EU-Staaten, was eine anhaltende Visabefreiung betraf. Marco Stefan, *The Transatlantic Dispute over Visas: The Need for EU Action in the Face of US Non-reciprocity, Moving Targets and the Harvesting of EU Citizens' Data*, Brüssel: CEPS, Juli 2017 (CEPS Policy Insights, Nr. 2017-27), <https://www.ceps.eu/system/files/PI2017-27_MS_EU-US%20Visa%20Controversy.pdf> (Zugriff am 20.3.2018).

54 Jon Henley/Ian Traynor, »Movements of Isis Extremist Prior to Paris Attack Raise EU Security Questions«, in: *The Guardian*, 19.11.2015, <https://www.theguardian.com/world/2015/nov/19/movements-of-isis-extremist-prior-to-paris-attack-raises-eu-security-questions> (Zugriff am 4.2.2018).

55 Europäische Kommission, COM (2015) 670 final, 15.12.2015.

Graphik 2

Vorschläge für EU-Datenbanken und Interoperabilität 2016



Quelle: eigene Darstellung

EU-Datenschutzregimes zu schaffen.[56] Im April 2016 legte die Kommission eine umfassende Mitteilung zur Weiterentwicklung intelligenter Grenzen vor,[57] die seither als zentraler Bezugspunkt dient. Neben bestehenden Vorschlägen, wie der Schaffung eines biometrischen Ein- und Ausreisesystems,[58] wurde die Idee reaktiviert, eine elektronische Einreiseerlaubnis für visabefreite Reisende (ETIAS)[59] nach Vorbild des amerikanischen ESTA-Systems einzurichten. Zusätzlich sollte das schon existierende ECRIS[60]-System — zum Austausch von Strafakten — zumindest für Drittstaatsangehörige zu einer zentralen Datenbank weiterentwickelt werden. Die neue ECRIS-TCN[61]-Datenbank sollte mit der elektronischen Einreiseerlaubnis ETIAS verbunden werden.

Der eigentliche Kern der Kommissionsmitteilung bestand aber in der Forderung, alle EU-Datenbanken im Bereich von Strafverfolgung, Grenzsicherung und Migrationssteuerung eng miteinander zu verknüpfen. Dafür wurde das Konzept der Interoperabilität aus polizeilichen Expertendiskussionen aufgegriffen und mit den Vorschlägen zu intelligenten Grenzen verbunden. So sollen sich unterschiedliche personenbezogene wie biometrische Daten, die sowohl im polizeilichen als auch im migrationspolitischen Bereich erhoben werden, systematisch abgleichen lassen, um Identitätsmissbrauch zu verhindern und die allgemeine Gefahrenabwehr zu erleichtern.

Ergänzend zu diesen neuen Vorschlägen für intelligente Grenzen und Interoperabilität schlug die EU-Kommission vor, das EURODAC-System auszubauen.[62] Damit soll es möglich werden, mehr biometrische und persönliche Daten über Asylsuchende und irreguläre Zuwanderer zu speichern und Strafverfolgungsbehörden verbesserte Recherche-Instrumente zu bieten.

Insbesondere Deutschland unterstützte dieses Maßnahmenpaket. Die Idee, Personendaten einmalig zu

56 Shara Monteleone, *Completing the Adoption of an EU PNR Directive*, European Parliament Research Service, 7.4.2016, <www.europarl.europa.eu/RegData/etudes/ATAG/2016/580886/EPRS_ATA(2016)580886_EN.pdf> (Zugriff am 4.12.2017).

57 Europäische Kommission, COM (2016) 205, 6.4.2016.

58 Dieser Vorschlag klammerte besonders umstrittene wirtschaftliche Programme für registrierte Reisende aus. Europäische Kommission, COM (2016) 196, 6.4.2016.

59 European Travel Information and Authorisation System.

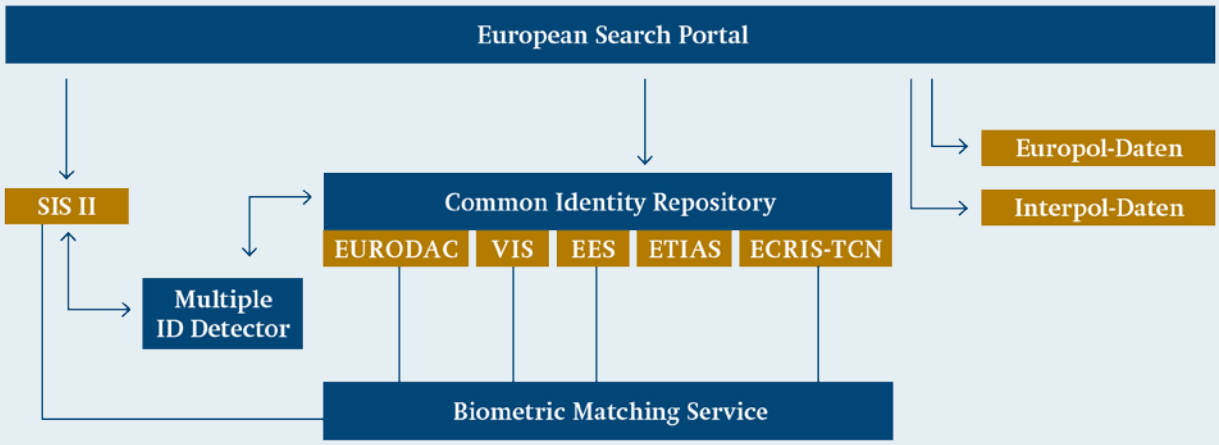
60 European Criminal Records Information System.

61 Third Country Nationals.

62 Europäische Kommission, COM (2016) 272 final, 4.5.2016.

Graphik 3

Schematische Darstellung der Interoperabilität



Quelle: <www.statewatch.org/news/2018/jan/eu-com-interoperability-swd-473-PT-1-17.pdf>.

erfassen und mehrfach zu nutzen, entsprach den parallel stattfindenden Reformen in Deutschland zur Schaffung eines »Kerndatensystems« für Asylsuchende und irreguläre Migranten.[63] Um die EU-Reformagenda zu konsolidieren, erstellte die niederländische Ratspräsidentschaft einen detaillierten Fahrplan zum Informationsmanagement. Er umfasste in mehreren Kapiteln und rund 50 Einzelpunkten die gesamte Bandbreite der bis dahin erörterten Maßnahmen zur technischen Grenzsicherung und zum Datenaustausch zwischen Strafverfolgungsbehörden.[64] Als erster Schritt konnte bis Ende 2016 eine Einigung erreicht werden, wonach alle Reisenden an Schengen-Außengrenzen systematisch auf etwaige Einträge im SIS zu kontrollieren sind. Unmittelbar danach unterbreitete die Kommission drei weitere Gesetzesvorschläge, die darauf zielten, das SIS intensiver zur Terrorismusbekämpfung und im Umgang mit irregulärer Migration zu nutzen.[65]

Darüber hinaus berief die Kommission eine »Hochrangige Expertengruppe«, um das Ziel der Interoperabilität auszugestalten. In ihrem Abschlussbericht von Mai 2017 plädierte diese Expertengruppe für drei Mechanismen:[66] 1. Harmonisierung der personenbezogenen Kerndaten durch regelmäßige Abgleiche zwischen EU-Datenbanken (common identity repository); 2. technische Standardisierung der biometrischen Eingabe- und Abfragesysteme (common biometric matching service); 3. Einrichtung einer integrierten Suchoberfläche (single-search interface) für die Grenz- und Migrationskontrolle sowie die Strafverfolgung. Die letztgenannte Suchoberfläche soll das bisherige Verfahren ersetzen, das nur eine sequentielle Abfrage von unterschiedlichen EU-Datenbanken zulässt. Außerdem sollen erleichterte

63 Deutscher Bundestag, Drucksache 18/7203, 6.1.2016. Im Kerndatensystem sollen Schutzsuchende und irregulär Eingereiste nur einmal mit persönlichen Daten und relevanten biometrischen Merkmalen (Lichtbild, Fingerabdruck) erfasst werden. Dieser Kerndatensatz wird Verwaltungs- und Sicherheitsbehörden für die jeweils eigenen Zwecke zugänglich gemacht.

64 Rat der Europäischen Union, 9368/1/16, 6.6.2016.

65 Europäische Kommission, COM (2016) 881, 882, 883 final, 21.12.2016.

66 High-level Expert Group on Information Systems and Interoperability, *Final Report*, Mai 2017, <http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetailDoc&id=32600&no=1> (Zugriff am 4.12.2017).

Abfragemöglichkeiten für Datenbestände bei Europol und bei Interpol geschaffen werden.[67]

Nicht unterstützt von der Expertengruppe wurde die Maximaloption, alle EU-Datenbanken vollständig zusammenzuführen. Im Sinne eines technisch verankerten Datenschutzes[68] soll vielmehr auf das vom Prümer Vertrag bekannte »Hit/No Hit«-Verfahren zurückgegriffen werden. Dabei wird zunächst mit Hilfe anonymisierter Treffermeldungen angezeigt, ob und wo relevante Einträge in unterschiedlichen Mitgliedstaaten (oder Datenbanken) vorliegen. Erst auf Basis einer solchen Treffermeldung kann die Übermittlung weiterer Personen- oder Fahndungsdaten beantragt werden. Diese Verfahrensweise soll sicherstellen, dass Strafverfolgungsbehörden nur auf relevante Informationen zugreifen und dass sich im Einzelfall überprüfen lässt, ob die Datenabfrage berechtigt ist.[69] Flankierend soll die Datenqualität in EU-Informationssystemen zur Migrationskontrolle verbessert werden, indem bei eu-LISA eine übergreifende Verwaltung des »common identity repository« und des »common biometric matching service« erfolgt. Für das SIS soll ein gesonderter »Detektor für Mehrfachidentitäten« entstehen. Er würde einen Abgleich erlauben zwischen dem konsolidierten EU-Datenbestand des biometrischen »common identity repository« und den stärker fragmentierten, tendenziell fehlerhaften alphanumerischen Personenangaben, die von nationalen Strafverfolgungsbehörden erfasst werden können. Damit die skizzierten technischen Reformen sich verwirklichen lassen, sollen Ressourcen und Mandat der eu-LISA-Agentur deutlich erweitert werden.[70]

Der Rat der EU-Innenminister bekräftigte seine Unterstützung für das umfassende Vorgehen.[71] In diesem politischen Umfeld gelang es bis Ende 2017, die Schaffung des biometrischen Ein- und Ausreisesystems zu beschließen[72] und zwei detaillierte Gesetzesvorschläge für die Interoperabilität vorzulegen.[73] 2018 soll eine Reihe weiterer Schritte vorangebracht werden: der Ausbau des Schengen-Informationssystems und von EURODAC, die Stärkung der eu-LISA-Agentur sowie die Schaffung der elektronischen Einreiseerlaubnis ETIAS und eines zentralen Strafregisters für Drittstaatsangehörige (ECRIS-TCN).[74] Insgesamt betrachtet blieb die verschärfte Bedrohungswahrnehmung seit 2016 für diese politische Dynamik ausschlaggebend, während wirtschaftliche Interessen, die für intelligente Grenzen sprechen, in den Hintergrund rückten.

67 Dies betrifft insbesondere die »Lost and Stolen Travel Documents Database« bei Interpol.

68 Das »privacy by design«.

69 Als weitere »privacy by design«-Maßnahme sollen Strafverfolgungsbehörden nur Zugriff auf die zentralen Personenangaben des »common identity repository« erhalten. Beispielsweise würden die Behörden bei einem Personentreffer im VIS zunächst keine ergänzenden Angaben aus dem gespeicherten Visumsantrag bekommen (Visumsdauer, einladende Organisation etc.).

70 Europäische Kommission, COM (2017) 352 final.

71 Rat der Europäischen Union, 10151/17, 14.6.2017.

72 Verordnung (EU) 2017/2226.

73 Europäische Kommission, COM (2017) 793, 794 final, 12.12.2017.

74 Europäische Kommission, COM (2017) 779 final, 12.12.2017.

Risiken der verdichteten EU-Sicherheitsagenda

Auf Ebene der EU-Gesetzgebung brächte dieses Maßnahmenpaket für Ausbau und systematische Verbindung von Datenbanken einen großen Integrationsfortschritt. Die langjährigen Debatten zur verbesserten polizeilichen Zusammenarbeit im RFSR und zur Anpassung an die Kontrollpraktiken der USA könnten vorerst abgeschlossen werden. Ebenso würden die Mechanismen der Interoperabilität dazu beitragen, Identitätsmissbrauch einzudämmen und die Abfrage von EU-Datenbanken für verschiedene Zwecke der Grenzkontrolle und der allgemeinen Strafverfolgung zu erleichtern.

Allerdings ergeben sich auch drei zentrale Risiken für den operativen und politischen Mehrwert dieser gebündelten Vorhaben. Erstens drohen starke Verzögerungen, wenn neue Grenzkontrollsysteme und bereits beschlossene Reformen zum polizeilichen Informationsmanagement umgesetzt werden. Zweitens tragen ein biometrisches Ein- und Ausreisesystem und eine elektronische Einreiseerlaubnis für visabefreite Reisende nur wenig dazu bei, die terroristische Gefahrenabwehr zu stärken oder die irreguläre Migration zu reduzieren. Drittens kann man nicht davon ausgehen, dass die öffentliche Unterstützung für die EU durch das aktuelle Maßnahmenpaket signifikant gestärkt wird.[75] Unter ungünstigen politischen Umständen kann Sicherheitstechnik gesellschaftliche Ängste vielmehr verstärken.

Umsetzung in den Mitgliedstaaten

In optimistischen Szenarien der EU-Kommission wird damit gerechnet, dass ein biometrisches Ein- und Ausreisesystem 2020 in Betrieb geht. Blickt man dagegen auf die bisherige Entwicklung intelligenter Grenzen und der europäischen Polizei-Zusammenarbeit, so zeigt sich, dass bei vergleichbaren Reformen — etwa der Schaffung des SIS II — langjährige Verzögerungen auftraten. Auch in den Vereinigten Staaten dauerte es über ein Jahrzehnt, bis man von der politischen Entscheidung für ein EES zu einer weitgehend funktionierenden Kontrollpraxis gelangte. Doch bis heute lässt sich im Falle der USA nicht garantieren, dass lückenlos alle legalen Ein- und Ausreisen biometrisch erfasst werden.[76]

Die EU kann zwar im Vergleich zu den 2000er Jahren auf eine ausgereiftere Technik und eine Reihe von Pilotprojekten zurückgreifen, um die Einführung eines EES zu beschleunigen. Außerdem will man das Mandat der Agentur eu-LISA stärken; dieser Schritt soll den Mitgliedstaaten zusätzlich dabei helfen,[77] technische Fragen zu lösen, wie etwa die Standardisierung von Schnittstellen zwischen IT-Systemen oder von verwendeten Kontrollgeräten. Darüber hinaus wird es nach Einschätzung der Kommission möglich sein, dass die Einführungskosten des EES noch weitgehend über den laufenden EU-Finanzrahmen bis 2020 gedeckt werden.

Allerdings ergeben sich durch die Größe der Schengen-Zone und das erwartete Volumen der

75 Eine solche Verbindung postulierte insbesondere die Bratislava-Agenda des Europäischen Rates. Vgl. Europäischer Rat, *Erklärung von Bratislava* [wie Fn. 5], S. 4. Die Kommission sprach seit dieser Erklärung wiederholt von einem Zusammenhang zwischen Erwartungen der EU-Bürger und einer Reform der technischen Infrastruktur für Grenzkontrollen und innere Sicherheit. Vgl. Europäische Kommission, »Security Union: Commission Closes Information Gaps to Better Protect EU Citizens«, Press Release IP/17/5202, 21.12.2017.

76 United States Government Accountability Office, *Report to the Committee on the Judiciary, U.S. Senate*, Februar 2017, <www.gao.gov/assets/690/683036.pdf> (Zugriff am 4.12.2017).

77 Europäische Kommission, COM (2017) 352 final.

Datenerfassung besondere Herausforderungen.[78] Offizielle Schätzungen der Kommission gehen für 2025 von bis zu 300 Millionen Grenzübertritten pro Jahr aus, die von einem biometrischen Ein- und Ausreisesystem erfasst werden sollen.[79] Die elektronische Einreiseerlaubnis ETIAS soll weitere 40 Millionen Datenverarbeitungsvorgänge pro Jahr erzeugen.[80] Grundsätzlich bleibt die Verantwortung für die flächendeckende Umsetzung von Grenzkontrollen, einschließlich intelligenter Grenzen, bei den Schengen-Mitgliedstaaten, die über sehr unterschiedliche Ressourcen technischer und personeller Art verfügen. Das Europäische Parlament und externe Beobachter bezweifeln deshalb, dass die im EU-Budget veranschlagten 480 Millionen Euro bis 2020 ausreichen, um ein flächendeckendes EES zu schaffen. Stattdessen erscheinen ein Einführungsprozess bis Mitte der 2020er Jahre und Kosten von bis zu einer Milliarde Euro als deutlich wahrscheinlicher.[81]

Bereits die systematischen und lückenlosen Personenkontrollen unter Nutzung des SIS, die seit April 2017 an allen EU-Außengrenzen durchgeführt werden sollen, stellen einige der betroffenen Staaten vor große Schwierigkeiten. Zusätzlich zu Kapazitätsengpässen in Stoßzeiten[82] zeigt sich etwa, dass nationale Koordinationsstellen[83] für den erweiterten Informationsaustausch ausgebaut werden müssten.[84] Die seit Mitte der 2000er Jahre angestrebte technische Möglichkeit, Fingerabdrücke in standardisierter Weise im SIS zu speichern und abzufragen,[85] wurde erst im März 2018 durch eine Minderheit von zehn Schengen-Mitgliedstaaten aktiviert.[86] Darüber hinaus gibt es drei weitere Gesetzesvorschläge, nach denen das SIS in stärker verpflichtender Weise zur Terrorismusbekämpfung und Eindämmung irregulärer Migration zu nutzen wäre.[87]

Mit dem Maßnahmenpaket riskiert die europäische Sicherheitspolitik womöglich ihre Glaubwürdigkeit.

Eine aktualisierte Version des Fahrplans der niederländischen Ratspräsidentschaft[88] unterstreicht die anhaltenden Defizite im polizeilichen Informationsmanagement. Dies betrifft unter anderem die Einrichtung des Prümer Verfahrens zum horizontalen Informationsaustausch in allen Mitgliedstaaten oder die konsistente Nutzung von Europol-Informationssystemen. Viele kleinere EU-Mitgliedstaaten verfügen nur über einen begrenzten Pool an Finanzmitteln und technischen Experten für diese Reformen. Und auch in Deutschland zeigen sich regelmäßig große Hürden bei der Modernisierung und Integration von IT-Systemen der Sicherheitsbehörden.[89]

Der EU-Ministerrat widmet dem Thema eine anhaltend hohe politische Aufmerksamkeit. Dies kann dazu beitragen, dass nationale Reformprozesse mit mehr Nachdruck verfolgt und zusätzliche Ressourcen

78 Erschwerend kommt hinzu, dass die Anzahl kleiner Grenzübergänge und schwierig zu kontrollierender Küsten deutlich höher ist als in den USA.

79 Europäische Kommission, SWD (2016) 115 final, 6.4.2016.

80 European Parliamentary Research Service, *European Travel and Authorization System (ETIAS)*, Oktober 2017, <www.europarl.europa.eu/RegData/etudes/BRIE/2017/599298/EPRS_BRI(2017)599298_EN.pdf> (Zugriff am 4.12.2017).

81 European Parliamentary Research Service, *Smart Borders: Entry/Exit System*, Januar 2018, <www.europarl.europa.eu/RegData/etudes/BRIE/2016/586614/EPRS_BRI(2016)586614_EN.pdf> (Zugriff am 4.3.2018).

82 Alex Matthews u.a., »›This Is Getting Ridiculous‹: British Holidaymakers Faint and Miss Their Flights in Four Hour Queues at European Airports after Brussels Insists on Tough New EU Border Checks«, in: *Mail Online*, 1.8.2017, <www.dailymail.co.uk/news/article-4748182/EU-border-checks-leave-UK-tourists-queuingFOUR-hours.html> (Zugriff am 20.11.2017); Mark Thomas, »Border Controls between Croatia and Slovenia to Be Eased ahead of Tourist Season«, in: *Dubrovnik Times*, 20.6.2017, <www.thedubrovniktimes.com/news/croatia/item/2583-border-controls-between-croatia-and-slovenia-to-be-eased-ahead-of-tourist-season> (Zugriff am 20.11.2017).

83 Die sogenannten SIRENE-Büros (Supplementary Information Request at the National Entries).

84 Rat der Europäischen Union, 14527/17, 20.11.2017.

85 Europäische Kommission, COM (2005) 230, 31.5.2005.

86 eu-LISA, »eu-LISA Successfully Launches SIS II AFIS Phase One«, Press Release, 6.3.2018, <www.eulisa.europa.eu/Newsroom/News/Pages/eu-LISA-successfully-launches-SIS-II-AFIS-Phase-One.aspx> (Zugriff am 7.3.2018).

87 High-level Expert Group on Information Systems and Interoperability, *Final Report* [wie Fn. 66].

88 Rat der Europäischen Union, 14750/17, 27.11.2017.

89 So scheiterten in Deutschland mehrere Projekte für eine interoperable IT-Infrastruktur nationaler Polizeibehörden. Siehe »Trotz geplanter Modernisierung und Vereinheitlichung: Das BMI hält weiterhin am PIAV fest«, *Police-IT*, 9.12.2016, <https://police-it.org/piav-gescheitert-innen minister-neue-alte-visionen> (Zugriff am 20.11.2017).

mobilisiert werden. Es ist aber ebenso möglich, dass sich in den kommenden Jahren weitere Umsetzungsdefizite anhäufen. Seit der Integrationsprozess des RFSR begonnen hat, besteht eine strukturelle Lücke zwischen ambitionierten EU-Gesetzesvorhaben und der Praxis in den Mitgliedstaaten.[90] Gerade im Bereich der Terrorismusbekämpfung wird bis heute oftmals kritisiert, dass die EU ein sicherheitspolitischer »Papiertiger« sei.[91] Vor diesem Hintergrund lässt sich fragen, ob das verdichtete Maßnahmenpaket für intelligente Grenzen und interoperable Datenbanken zeitnah umgesetzt werden kann — oder ob es mittelfristig nicht eher ein Risiko für die Glaubwürdigkeit der europäischen Sicherheitspolitik darstellt. Wie skizziert, sollen im Laufe des Jahres 2018 neun weitere Gesetzesvorschläge[92] verhandelt werden. Darüber hinaus listet der Ratsfahrplan zum Informationsmanagement zahlreiche nichtlegislative Maßnahmen auf (Trainings, technische Pilotprojekte, Umsetzungsverfahren etc.), die ebenso von den Sicherheitsbehörden der Mitgliedstaaten in Angriff genommen werden sollen. Bisher ist keine klare Priorisierung oder Staffelung dieser vielfältigen Vorhaben zu erkennen.

Effekte auf Terrorismusbekämpfung und irreguläre Migration

Die krisengetriebene Darstellung, die EU müsse alle verfügbaren Instrumente zur Bekämpfung des internationalen Terrorismus und zur Eindämmung der irregulären Migration nutzen,[93] beinhaltet das Risiko, dass die Effektivität einzelner Gesetzesvorschläge nicht präzise genug untersucht wird. Dies gilt insbesondere für den möglichen Mehrwert intelligenter Grenzen für die innere Sicherheit der EU.[94]

Seit 2014 findet ein globaler Austausch von personenbezogenen Informationen zu sogenannten ausländischen Kämpfern statt.[95] Seit 2016 zielt dieser Informationsaustausch zusätzlich darauf ab, dass möglichst alle Personen, die aus Gebieten bzw. ehemaligen Gebieten des IS zurückkehren, bei Grenzübertritten erkannt und frühzeitig der Strafverfolgung zugeführt werden können. In diesem Zusammenhang sind erweiterte technische Grenzkontrollen und die Verwendung biometrischer Daten von beträchtlichem Nutzen.[96] Die USA spielen eine zentrale Rolle, wenn es darum geht, die Reisebewegungen ausländischer Kämpfer im weltweiten Maßstab zu kontrollieren. Amerikanische Streitkräfte sammeln und verwerten alle verfügbaren Daten in Konfliktgebieten,[97] während die US-Nachrichtendienste verdächtige Personen global überwachen. Deutschland und weitere 37 Staaten des US-Visa-Waiver-Programms unterhalten mit der amerikanischen Seite einen besonders intensiven Informationsaustausch über

90 Ludo Block, *From Politics to Policing: The Rationality Gap in EU Council Policy-Making*, Den Haag 2011.

91 Oldrich Bures, *EU Counterterrorism Policy: A Paper Tiger?*, Farnham 2011; Wim Wensink u.a., *The European Union's Policies on Counter-Terrorism. Relevance, Coherence and Effectiveness*, Brüssel: European Parliament, Januar 2017, <www.europarl.europa.eu/RegData/etudes/STUD/2017/583124/IPOL_STU(2017)583124_EN.pdf> (Zugriff am 4.12.2017).

92 Europäische Kommission, COM (2016) 272, 731, 881, 882, 883; COM (2017) 344, 352, 793, 794.

93 Dimitri Avramopoulos, »Remarks by Commissioner Avramopoulos at the Special Committee on Terrorism (TERR)«, 23.1.2018, <https://ec.europa.eu/commission/commissioners/2014-2019/avramopoulos/announcements/remarks-commissioner-avramopoulos-special-committee-terrorism-terr_en> (Zugriff am 4.3.2018).

94 Siehe Kapitel 1 sowie European Parliament Study, *Smart Borders Revisited: An Assessment of the Commission's Revised Smart Borders Proposal*, Oktober 2016, <www.europarl.europa.eu/RegData/etudes/STUD/2016/571381/IPOL_STU(2016)571381_EN.pdf > (Zugriff am 4.12.2017).

95 United States Department of State, *Readout of the Meeting of the Small Group on the Global Coalition to Defeat ISIS in Jordan*, 15.11.2017, <https://www.state.gov/r/pa/prs/ps/2017/11/275610.htm> (Zugriff am 4.12.2017).

96 Homeland Security Task Force, *Final Report of the Task Force on Combating Terrorist and Foreign Fighter Travel*, September 2015, <https://homeland.house.gov/wp-content/uploads/2015/09/TaskForceFinalReport.pdf> (Zugriff am 4.3.2018). Es ist aber noch eine offene Frage, ob zurückkehrende ausländische Kämpfer des IS tatsächlich eine strategische Gefahr für westliche Staaten darstellen oder nicht. David Malet, »The European Experience with Foreign Fighters and Returnees«, in: Thomas Renard/Rik Coolsaet (Hg.), *Returnees: Who Are They, Why Are They (Not) Coming Back and How Should We Deal with Them*, Brüssel: Egmont — Royal Institute for International Relations, Februar 2018 (Egmont Occasional Paper 101), S. 6—18 <www.egmontinstitute.be/content/uploads/2018/02/egmont.papers.101_online_v1-3.pdf?type=pdf> (Zugriff am 4.3.2018).

97 Dies beinhaltet auch biometrische Informationen, wie etwa Fingerabdrücke von gefundenen Sprengsätzen. Siehe US Army, *Near Real Time Identity Operations (NRTIO)*, <www.dote.osd.mil/pub/reports/FY2016/pdf/army/2016nrtio.pdf> (Zugriff am 4.3.2018).

terroristische Gefährder.[98] Relevante Warnhinweise zu ausländischen Kämpfern werden zugleich über Nato-Kanäle und Interpol[99] sowie zunehmend mit Europol geteilt.[100] Europol unterstützt insbesondere die Sicherheitsüberprüfung von Personen, die sich in Griechenland und Italien im Rahmen der dort eingerichteten »Hotspots« als Schutzsuchende registrieren lassen.[101]

Fraglich ist, ob intelligente Grenzen dazu beitragen, die irreguläre Migration einzudämmen.

Bestehende EU-Datenbanken für Strafverfolgungsbehörden sollen in diesem Zusammenhang noch intensiver genutzt werden. Einer der drei neueren Gesetzesvorschläge zum Ausbau des SIS sieht vor, dass nationale Warnhinweise zu Terrorismusverdächtigen verpflichtend im europäischen SIS auszuschreiben sind.[102] Die neu geplante Möglichkeit, die Fingerabdrücke von bisher nicht identifizierten Strafverdächtigen im SIS zur Fahndung einzustellen, kann in Einzelfällen zur terroristischen Gefahrenabwehr beitragen. Einen Mehrwert verspricht insbesondere die systematische Sammlung von Daten zu ausländischen Kämpfern bei Europol, einschließlich Informationen aus Nordafrika.[103] Die von der EU vorgesehenen intelligenten Grenzsysteme können aber voraussichtlich keinen substantiellen Beitrag in dieser Hinsicht leisten. Während die USA ihr Ein- und Ausreisesystem mit einer stetig aktualisierten biometrischen Warnliste zu Terrorismusverdächtigen verknüpfen, sieht der verabschiedete Rechtsakt zum europäischen Ein- und Ausreisesystem lediglich einen begrenzten und nachträglichen Zugriff von Polizeibehörden vor. Bei regulären Grenzkontrollen soll im EES nur ein unmittelbarer Vergleich mit der EU-Visadatenbank stattfinden, um den legitimen Aufenthaltsstatus zu verifizieren. Somit bleibt der primäre operative Zweck des europäischen EES die Verwaltung der legalen Migration.[104]

Im Gegensatz dazu soll eine EU-Warnliste zu mutmaßlichen Terroristen sowie Kriegs- und Schwerverbrechern im Rahmen der elektronischen Einreiseerlaubnis ETIAS für visabefreite Drittstaatsangehörige geschaffen werden.[105] Bisher sind jedoch keine terroristischen Vorfälle in der EU bekannt geworden, bei der visabefreite und nur kurzfristig einreisende Drittstaatsangehörige eine besondere Rolle gespielt hätten. Zudem soll das ETIAS-System keine biometrischen Informationen beinhalten, was der Funktionsweise der multilateral verbreiteten Warnlisten zu ausländischen Kämpfern entgegensteht.[106]

Ebenso lässt sich in Frage stellen, ob intelligente Grenzen einen Mehrwert dazu leisten, die irreguläre Migration einzudämmen. Beantragt eine Person ein Schengen-Visum, soll künftig ein Abgleich mit dem

98 Ruth Ellen Wasem, *The US Visa Waiver Program. Facilitating Travel and Enhancing Security*, London: The Royal Institute of International Affairs — Chatham House, Oktober 2017 (Chatham House Research Paper), <https://www.chathamhouse.org/sites/files/chathamhouse/publications/research/2017-10-25-us-visa-waiver-wasem.pdf> (Zugriff am 4.12.2017).

99 United States Department of Justice, *Interpol Washington Spearheads Foreign Terrorist Fighter Program, Serves as Catalyst for Global Information Sharing Network*, 24.9.2014, <https://www.justice.gov/opa/pr/interpol-washington-spearheads-foreign-terrorist-fighter-program-serves-catalyst-global> (Zugriff am 4.12.2017).

100 Deutscher Bundestag, Drucksache 18/12451, 19.5.2017; Paul Cruickshank, »A View from the CT Foxhole: Peter Edge, ICE Acting Deputy Director, and Wil van Gemert, Europol Deputy Director«, in: *CTC Sentinel*, 10 (2017) 1, S. 11—16.

101 Europäisches Parlament, *Parliamentary Questions 12 June 2017. Answer Given by Mr King on Behalf of the Commission*, E-001454/2017.

102 COM(2016) 882 [wie Fn. 65]. Die Zahl der Ausschreibungen im SIS für »verdeckte Beobachtungen«, die insbesondere zur Überwachung von Terrorismusverdächtigen genutzt werden sollen, wächst seit 2016 deutlich an. Allerdings erscheint dabei die Beteiligung der Schengen-Mitgliedstaaten noch sehr uneinheitlich. Siehe Matthias Monroy, »Sharp Increase of Secret Alerts in the Schengen Information System«, 1.1.2018, <https://digit.site36.net/ 2018/03/01/sharp-increase-of-secret-alerts-in-the-schengen-information-system/> (Zugriff am 1.3.2018).

103 Die Mehrzahl der ausländischen Kämpfer des IS stammt aus dem Maghreb. Dies ist einer der Gründe, warum Europol derzeit mit Staaten der Region über den Austausch personenbezogener Daten verhandelt. Siehe beispielsweise Rat der Europäischen Union, 5037/18, 5039/18, 9.1.2018.

104 Dies entspricht der zwischen 2008 und 2013 durch die EU-Kommission ursprünglich vorgebrachten Begründung für ein EES und weitere intelligente Grenzsysteme.

105 Europäische Kommission, COM (2016) 731, 16.11.2016, Art. 29.

106 Eine Resolution des Sicherheitsrats der Vereinten Nationen vom 21.12.2017 empfiehlt explizit, solche biometrischen Warnlisten zu nutzen. Siehe United Nations Security Council, Resolution 2396 (2017), 21.12.2017, <http://unscr.com/en/resolutions/doc/2396> (Zugriff am 5.2.2018).

EES sicherstellen, dass sie in der Vergangenheit die gesetzlichen Aufenthaltsbestimmungen eingehalten hat. Dieses Verfahren kann dazu beitragen, dass Besucher der Schengen-Zone weniger häufig ein Visum überziehen oder dass Schengen-Visa in stärkerem Maße verweigert werden. Ob eine Ausreise erzwungen oder ein irregulärer Zuwanderer zurückgewiesen wird, lässt sich aber nicht allein von einem Datenbanktreffer im EES oder beim schon bestehenden VIS abhängig machen. Geltende Gesetze auf nationaler und EU-Ebene sowie internationale Verpflichtungen in der Migrations- und Flüchtlingspolitik geben vor, dass stets noch weitere Aspekte bei der Grenzkontrolle berücksichtigt werden, wie etwa die Vermeidung unmenschlicher Behandlung, die Wahrung von Grundrechten (faires Verfahren, Schutz der Familie etc.) oder die Möglichkeit zur Beantragung von Asyl.[107]

Insgesamt ist nicht zu erwarten, dass eine konsistentere Erfassung von Einreise- und Ausreisebewegungen die irreguläre Zuwanderung signifikant verringern wird. So hat sich über die vergangenen 15 Jahre die Zahl der illegalen Migranten in den USA weitgehend unabhängig von der Einführung eines biometrischen EES entwickelt.[108] In der Regel haben verstärkte Grenzkontrollen ambivalente Auswirkungen auf das Migrationsgeschehen.[109] Steigt für illegale Zuwanderer die Gefahr der Entdeckung, kann dies einen Abschreckungseffekt erzeugen, aber auch bewirken, dass sich die irreguläre Migration auf riskantere Reisewege verlagert. Anstelle regulärer Verkehrsmittel (mit anschließender Überziehung eines Besuchervisums) werden dann verstärkt die Dienste von Schleusern nachgefragt. Vor allem erhöht sich die Zahl der Personen, die langfristig in einen illegalen Aufenthaltsstatus abrutschen, statt zwischen Herkunfts- und Zielland hin- und herzupendeln.

Die europäische Migrationskrise unterstreicht, dass übergeordnete Triebkräfte — wie Gewaltkonflikte, Staatsversagen, demographische Entwicklung und wirtschaftliche Ungleichheit — entscheidend für den Umfang der Zuwanderung sind. Derzeit wird durch die biometrische Erfassung von Asylsuchenden und irregulären Zuwanderern in EURODAC nur dokumentiert, wie stark ungleichgewichtig diese Personen innerhalb der EU verteilt sind. Die primären Defizite des Dublin-Regimes für Asylverfahren liegen nicht — wie in einigen früheren Phasen — darin, dass potentielle Antragsteller an Schengen-Außengrenzen lückenhaft registriert würden. Problematisch sind vielmehr die sich anschließenden Verfahren zur Überstellung der Personen und die mangelnde Garantie gleichwertiger Abläufe und Aufnahmestandards in allen EU-Mitgliedstaaten.[110] Sofern nicht an allen Schengen-Binnengrenzen permanente und verschärfte Identitätskontrollen durchgeführt werden sollen, besteht deshalb kein signifikanter Zusammenhang zwischen intelligenten Grenzen und der sekundären Migration von Asylsuchenden innerhalb der EU.

Sicherheitstechnik und öffentliches Vertrauen

Aus einem anderem Blickwinkel steht jedoch bei allen aktuellen Maßnahmen zu Grenzsicherung und innerer Sicherheit die öffentliche Wahrnehmung der EU im Vordergrund. In den Eurobarometer-Umfragen zwischen 2014 bis 2017 stieg der Anteil der Bürger, die Angst vor Terrorismus äußern, von 6 Prozent auf 44 Prozent,[111] und seit 2015 gilt Terrorismus in der Bevölkerung als die zentrale Sicherheitsgefahr der EU.[112] Auf dem Höhepunkt der Flüchtlingskrise im

107 European Union Agency for Fundamental Rights, *Fundamental Rights and the Interoperability of EU Information Systems: Borders and Security*, Wien, Juli 2017, <http://fra.europa.eu/en/publication/2017/fundamental-rights-interoperability> (Zugriff am 4.2.2017).

108 Robert Warren, »DHS Overestimates Visa Overstays for 2016; Overstay Population Growth Near Zero during the Year«, in: *Journal on Migration and Human Security*, 5 (2017) 4, S. 768—779.

109 Douglas S. Massey/Jorge Durand/Karen A. Pren, »Why Border Enforcement Backfired«, in: *American Journal of Sociology*, 121 (2016) 5, S. 1557—1600; Amthias Czaika/Hein de Haas, »The Effect of Visas on Migration Processes«, in: *International Migration Review*, 51 (2016) 4, S. 893—926.

110 Bernd Parusel/Jan Schneider, *Reforming the Common European Asylum System: Responsibility-sharing and the Harmonisation of Asylum Outcomes*, Stockholm: Delegationen för migrationsstudier, 2017 (Delmi Report 2017:9), <http://delmi.se/upl/files/145454.pdf> (Zugriff am 5.2.2018).

111 Europäische Kommission, *Standard-Eurobarometer 87*, Mai 2017, S. 8, <ec.europa.eu/commfrontoffice/publicopinion/index.cfm/ResultDoc/download/DocumentKy/79566> (Zugriff am 4.12.2017).

112 Europäische Kommission, *Special Eurobarometer 432*, April 2015, <ec.europa.eu/commfrontoffice/publicopinion/

Herbst 2015 zeigten derweil 59 Prozent der befragten Bürger eine negative Einstellung gegenüber Einwanderung aus dem außereuropäischen Ausland.[113] Sowohl die Kommission als auch die EU-Mitgliedstaaten begründen deshalb den Ausbau von intelligenten Grenzen und von Datenbanken für Sicherheitsbehörden damit, dass das Vertrauen der Bürger zurückgewonnen werden müsse.[114]

Die Legitimität der EU lässt sich aber nicht in dieser unmittelbaren Weise mit neuen sicherheitspolitischen Entscheidungen verknüpfen. Zunächst ist die öffentliche Wahrnehmung der aktuellen Krise und der bestehenden Herausforderungen weniger eindeutig, als es die EU-Institutionen mit Verweis auf Eurobarometer-Umfragen oftmals suggerieren. So betrachten europäische Bürger die Personenfreizügigkeit — neben dem Frieden — nach wie vor als die wichtigste Errungenschaft der EU.[115] Die bestehenden Schwächen des Außengrenzschutzes können daher noch keine existentielle Krise des Schengen-Regimes begründen. Darüber hinaus ist die Problemwahrnehmung hinsichtlich Terrorismus und Migration sehr viel schwächer, wenn nach einem konkreten persönlichen Bezug gefragt wird. Unter dieser Maßgabe sind für die meisten europäischen Bürger noch immer sozial- und wirtschaftspolitische Themen vorrangig. Dementsprechend betrachten über 90 Prozent der im Eurobarometer befragten Personen ihr eigenes Lebensumfeld als sicher, während die innere Sicherheit der EU mit größerer Skepsis, aber auch nur sehr indirekt wahrgenommen wird.[116]

Insgesamt zeigt die Forschung, dass Wahrnehmungen terroristischer Gefahr in der westlichen Welt in keinem proportionalen Verhältnis zur Wahrscheinlichkeit von Anschlägen stehen, sondern primär medial vermittelt werden.[117] Auch der Zusammenhang zwischen dem Umfang an Einwanderung und einer Zunahme ausländerfeindlicher Einstellungen ist zu relativieren.[118] Politische Diskurse von Eliten und Parteien sind für krisenhafte Entwicklungen in der Einwanderungs- und Sicherheitspolitik mindestens ebenso von Bedeutung wie kritische Einstellungen in der Wählerschaft.[119]

Der Einsatz technischer Mittel birgt die Gefahr, dass ein Wettlauf um immer mehr Sicherheit entsteht.

Gerade deshalb könnte man argumentieren, dass ein technokratischer Politikansatz Vorteile bietet. Während es zu verzerrten Wahrnehmungen führen kann, wenn Fragen von Zuwanderung und Terrorismus zum Thema öffentlicher Debatten gemacht werden, lassen sich durch intensivierte Kontrollen im Hintergrund möglicherweise Krisen vermeiden. Zumindest im Fall der Zelle, die die Anschläge von Paris im November 2015 verübte, wäre es möglich gewesen, die Drahtzieher rechtzeitig zu verhaften, hätte man das SIS konsequent genutzt. Der Rückgriff auf technische Maßnahmen birgt jedoch auch das Risiko, dass ein Wettlauf um immer mehr Sicherheit entsteht. Beispielhaft zeigt sich diese Tendenz in den USA. Unmittelbar nach Amtsantritt von Präsident Trump wurde das »extreme vetting« eingeführt, das darauf zielt, die — zuvor schon sehr umfassenden — Personenkontrollen bei Einreisen noch restriktiver zu

index.cfm/ResultDoc/download/DocumentKy/64543> (Zugriff am 4.12.2017).

113 Europäische Kommission, *Standard-Eurobarometer 87* [wie Fn. 111], S. 31.

114 Vgl. Europäischer Rat, *Erklärung von Bratislava* [wie Fn. 5]; Europäische Kommission, SWD (2017) 47, 1.12.2017, S. 14.

115 Europäische Kommission, *Standard-Eurobarometer 84*, Dezember 2015, S. 56, <http://ec.europa.eu/commfrontoffice/publicopinion/index.cfm/Survey/getSurveyDetail/instruments/STANDARD/surveyKy/2098> (Zugriff am 4.12.2017); Europäische Kommission, *Standard-Eurobarometer 87* [wie Fn. 111].

116 Europäische Kommission, *Special Eurobarometer 464b*, Dezember 2017, S. 5, <http://ec.europa.eu/commfrontoffice/publicopinion/index.cfm/ResultDoc/download/DocumentKy/8698> (Zugriff am 14.2.2018).

117 Aaron M. Hoffman/William Shelby, »When the ›Laws of Fear‹ Do Not Apply: Effective Counterterrorism and the Sense of Security from Terrorism«, in: *Political Research Quarterly*, 70 (2017) 3, S. 618—631.

118 Unter günstigen Umständen kann gerade mehr Zuwanderung eine gemeinsame Lebenswelt und dadurch Vertrauen unter Bürgern schaffen. Yolande Pottie-Sherman/Rima Wilkes, »Does Size Really Matter? On the Relationship between Immigrant Group Size and Anti-Immigrant Prejudice«, in: *International Migration Review*, 51 (2017) 1, S. 218—250.

119 Daniel Stockemer, »Structural Data on Immigration or Immigration Perceptions? What Accounts for the Electoral Success of the Radical Right in Europe?«, in: *Journal of Common Market Studies*, 54 (2016) 4, S. 999—1016; Christoffer Green-Pedersen/Simon Otjes, »A Hot Topic? Immigration on the Agenda in Western Europe«, in: *Party Politics* (2017), online first (31.8.2017), <https://doi.org/10.1177/1354068817728211> (Zugriff am 14.02.2018).

gestalten.[120] Anstatt, wie propagiert, die traditionellen Grenzen durch weitgehend offene und intelligent vernetzte Grenzen zu ersetzen,[121] werden also immer mehr technische Kontrollen übereinander gelagert. Diese Entwicklung kann gesellschaftliche Ängste und Vorurteile gegenüber Drittstaatsangehörigen vertiefen.[122]

Vorgelagerte öffentliche Diskurse und politische Normen sind entscheidend dafür, ob Sicherheitstechnik zur Legitimierung der öffentlichen Ordnung beitragen kann oder nicht. Beispielsweise verfolgte Großbritannien spätestens seit 2007 im Rahmen des »e-Borders Programme« viele der Maßnahmen, die derzeit im Sinne intelligenter Grenzen der Schengen-Zone erwogen werden.[123] In derselben Zeit aber verschlechterten sich auf der Insel die mediale Darstellung der Grenzsicherheit und die öffentliche Meinung dazu.[124] Das Brexit-Referendum verdeutlichte besonders dramatisch, dass ein beträchtlicher Anteil der britischen Wähler die nationalen Grenzen als zu unsicher und zu durchlässig empfindet.[125] Im Gegensatz dazu bleibt in Kanada, das vergleichbare Investitionen in intelligente Grenzen tätigt, die gesellschaftliche Unterstützung für Einwanderung und internationale Mobilität relativ hoch.[126]

Vertiefte Befragungen aus unterschiedlichen EU-Ländern zeigen zudem, dass Bürger in der Regel keine Einzelfallabwägung zwischen neuer Überwachungstechnik und Freiheitsrechten vornehmen.[127] Sofern nicht grundsätzlich ein starker Staat Unterstützung findet, wird gleichermaßen ein Verlust von Sicherheit und von Freiheit befürchtet.[128] Experten aus Verwaltung und Sicherheitsbehörden haben eine vergleichbar gespaltene Meinung.[129] So werden automatisierte Grenzkontrollen entweder für dringend notwendig gehalten oder weitgehend abgelehnt. Die Weiterentwicklung dieser Technologien kann also nicht auf die Verwaltungsebene delegiert werden, sondern bleibt in jedem Fall an stark unterschiedliche Wertvorstellungen gekoppelt.

Drei globale technische Trends können zu einer weiteren Polarisierung bzw. zu Überwachungsängsten beitragen.[130] Erstens entwickelt sich die digitale Biometrie rapide fort. Während die Erfassung von Fingerabdrücken bis vor kurzem noch als sensibler Grundrechtseingriff galt, wird dieser Vorgang zunehmend alltäglich, etwa beim Gebrauch von Smartphones.[131] Technische Verbesserungen bei der Gesichtserkennung sorgen dafür, dass sich automatisierte Grenzkontrollschleusen an Flughäfen verbrei-

120 Beim »extreme vetting« sollen alle Lebensbereiche einer Person nach Hinweisen auf Sicherheitsgefahren durchleuchtet werden, was unter anderem Online-Aktivitäten und elektronische Identitäten der Einreisenden betreffen kann.

121 Siehe Kapitel 1.

122 Sami J. Karam, »Immigration and Trust«, in: *NewGeography* (online), 13.1.2018, <www.newgeography.com/content/005848-immigration-and-trust> (Zugriff am 5.2.2018).

123 House of Commons, Public Accounts Committee, »E-borders Inquiry« [2016], <https://www.parliament.uk/business/committees/committees-a-z/commons-select/public-accounts-committee/inquiries/parliament-2015/e-borders-15-16/> (Zugriff am 5.2.2018).

124 Bastian A. Vollmer, »Security or Insecurity? Representations of the UK Border in Public and Policy Discourses«, in: *Mobilities*, 12 (2017) 3, S. 295—310.

125 Matthew Goodwin/Caitlin Milazzo, »Taking Back Control? Investigating the Role of Immigration in the 2016 Vote for Brexit«, in: *The British Journal of Politics and International Relations*, 19 (2017) 3, S. 450—464.

126 Daniel Hiebert, *What's So Special about Canada? Understanding the Resilience of Immigration and Multiculturalism*, Washington, D.C.: Migration Policy Institute, Juni 2016 (Migration Policy Institute Report).

127 Vincenzo Pavone/Sara Degli Esposti, »Public Assessment of New Surveillance-oriented Security Technologies. Beyond the Trade-off between Privacy and Security«, in: *Public Understanding of Science*, 21 (2012) 5, S. 556—572; Michael Friedewald/Marc van Lieshout/Sven Rung/Merel Ooms, »The Context-Dependence of Citizens' Attitudes and Preferences Regarding Privacy and Security«, in: Serge Gutwirth/Ronald Leenes/Paul De Hert (Hg.), *Data Protection on the Move. Current Developments in ICT and Privacy/Data Protection*, Dordrecht u.a. 2016 (Law, Governance and Technology Series, Bd. 24), S. 51—74.

128 Sara Degli Esposti/Elvira Santiago Gómez, »Acceptable Surveillance-Orientated Security Technologies: Insights from the SurPRISE Project«, in: *Surveillance & Society*, 13 (2015) 3/4, S. 437—454.

129 Pinja Lehtonen/Pami Aalto, »Smart and Secure Borders through Automated Border Control Systems in the EU? The Views of Political Stakeholders in the Member States«, in: *European Security*, 26 (2017) 2, S. 207—225.

130 Kristoffer Lidén/Nina Boy/Elida Jacobsen, *Report on Societal Ethics and Biometric Technologies*, Societal Security Network, Dezember 2016, <https://www.prio.org/utility/DownloadFile.ashx?id=529&type=publicationfile> (Zugriff am 4.12.2017).

131 Anil K. Jain/Karthik Nandakumar/Arun Ross, »50 Years of Biometric Research: Accomplishments, Challenges, and Opportunities«, in: *Pattern Recognition Letters*, 79 (2016), S. 80—105.

ten.[132] Gleichzeitig wachsen die Möglichkeiten einer biometrischen Datensammlung auf Distanz. Als ethisch besonders problematisch kann dies unter dem Gesichtspunkt gelten, dass Betroffene möglicherweise nicht eingewilligt haben und den Vorgang nicht bewusst wahrnehmen.[133] Das Beispiel China verdeutlicht in drastischer Weise die neuen Möglichkeiten, eine flächendeckende Videoüberwachung durchzuführen und künstliche Intelligenz zur Bewertung individuellen Verhaltens einzusetzen.[134] Aber auch in westlichen Staaten entwickeln Sicherheitsbehörden ambitionierte Programme. So arbeitet etwa das FBI daran, eine vollautomatische Gesichtsbildfahndung zu ermöglichen.[135]

Biometrische Personen-Datenbanken sind ein attraktives Ziel für Hacker.

Zweitens beschleunigt sich die Sammlung und Integration von Daten aus allen Lebensbereichen. Vergleichbar zur Privatwirtschaft entwickelt sich unter Sicherheitsbehörden die Vision einer umfassenden mobilen Datenverarbeitung.[136] So können Einsatzkräfte mittels Smartphone oder Tablet deutlich mehr personenbezogene Informationen abfragen und einspeisen als bisher. Parallel sollen Einsatzkräfte durch die Auswertung großer Datenmengen gesteuert werden, wie es im Schlagwort des »predictive policing«[137] zum Ausdruck kommt. Diese Entwicklung erstreckt sich zunehmend auf die Grenz- und Migrationskontrolle. So nutzt die amerikanische Zoll- und Einwanderungsbehörde ICE[138] bei der Festnahme irregulärer Einwanderer zunehmend Daten, die aus sehr unterschiedlichen Kontexten (etwa sozialen Medien oder lokalen Personenregistern) zusammengetragen und automatisiert ausgewertet werden.[139]

Drittens wächst die Zahl von Cyberangriffen, die auf persönliche Informationen abzielen. Vermeintlich unverwechselbare biometrische Merkmale sind kopier- oder überlistbar, während als sicher ausgegebene Identitätskarten wiederholt geknackt wurden.[140] Darüber hinaus sind biometrische Personendatenbanken ein attraktives Ziel für Hacker. So wurden dem US Office of Personal Management schätzungsweise 5 Millionen persönliche Datensätze und Fingerabdrücke gestohlen.[141] Zudem gibt es Indizien dafür, dass Nachrichtendienste derartige Personendatenbanken in Drittstaaten infiltrieren.[142] Die Ausweitung biometrischer Datenbanken der EU erhöht die Anreize für vergleichbare Angriffe.[143]

132 Ruggero Donida Labati/Angelo Genovese/Enrique Muñoz/Vincenzo Piuri/Fabio Scotti/Gianluca Sforza, »Biometric Recognition in Automated Border Control: A Survey«, in: *ACM Computing Surveys (CSUR)*, 49 (2016) 2 (Artikel Nr. 24).

133 Emilio Mordini/Andrew P. Rebera, »No Identification without Representation. Constraints on the Use of Biometric Identification Systems«, in: *Review of Policy Research*, 29 (2012) 1, S. 5—20.

134 Simon Denyer, »Beijing Bets on Facial Recognition in a Big Drive for Total Surveillance«, in: *Washington Post*, 7.1.2018.

135 Jennifer Lynch, »FBI Wants to Remove Privacy Protections from Its Massive Biometrics Database«, *Electronic Frontier Foundation*, 31.5.2016.

136 Rat der Europäischen Union, 10127/17, 13.6.2017, <http://statewatch.org/news/2017/jun/eu-council-enlets-mobile-solutions-police-10127-17.pdf> (Zugriff am 4.12.2017).

137 Die jeweils genutzten Methoden reichen von statistischer Datenvisualisierung bis hin zu selbstlernenden Systemen. Erstere kann etwa die polizeiliche Bestreifung anleiten (predictive mapping), während Letztere auch zunehmend Einzeltäter betreffen (predictive identification).

138 United States Immigration and Customs Enforcement.

139 Dabei wird auch Analyse-Software genutzt, die zuvor für militärische und nachrichtendienstliche Zwecke entwickelt wurde. Spencer Woodman, »Palantir Provides the Engine for Donald Trump's Deportation Machine«, in: *The Intercept*, 2.3.2017.

140 Alex Hern, »Hacker Fakes German Minister's Fingerprints Using Photos of Her Hands«, in: *The Guardian*, 30.12.2014; Ben Schwan, »iPhone X: Vietnamesische Sicherheitsforscher umgehen Face ID mit Maske«, *Heise Online*, 13.11.2017; Richard Milne/Michael Peel, »Red Faces in Estonia over ID Card Security Flaw«, in: *Financial Times*, 6.9.2017.

141 Brendan I. Koerner, »Inside the Cyberattack that Shocked the US Government«, *Wired*, 23.10.2016.

142 Bob Egelko, »Suit Warns of Russian ›Back Door‹ into U.S. Fingerprint Systems«, *SFGate*, 14.8.2016; Rafay Baloch, »You Should Be Worried about #NADRAGate, Here's Why«, *commandeleven.com*, 8.6.2017.

143 Matthias Schulze/Raphael Bossong/Marcel Dickow, »Cyber-Sabotage der EU-Datenbanken zur inneren Sicherheit«, in: Lars Brozus (Hg.), *Während wir planten: Unerwartete Entwicklungen in der internationalen Politik. Foresight-Beiträge 2018*, Berlin: Stiftung Wissenschaft und Politik, April 2018 (SWP-Studie 5/2018), S. 16—20.

Herausforderungen bei Datenschutz und rechtsstaatlicher Aufsicht

Insgesamt betrachtet ist die Modernisierung der EU-Grenzkontrollen und des polizeilichen Datenmanagements ein anspruchsvoller Prozess, dessen Bedeutung nicht auf die Migrationskrise und den aktuellen Kampf gegen internationalen Terrorismus reduziert werden sollte. Ein Blick auf die historische Entwicklung dieser Agenda zeigt, dass damit sehr vielschichtige Vorhaben verfolgt werden, um die internationale Mobilität besser verwalten zu können und eine grenzüberschreitende Zusammenarbeit von Strafverfolgungsbehörden zu erleichtern. Dabei birgt die Beschleunigung der EU-Sicherheitsgesetzgebung seit 2016 beträchtliche Risiken. Die Umsetzungskapazitäten in den Mitgliedstaaten sollten ebenso wenig überschätzt werden wie der operative Mehrwert intelligenter Grenzen für die innere Sicherheit. Zugleich kann die wachsende Rolle von Sicherheitstechnik dazu beitragen, kritische Wahrnehmungen und Ängste der Bürger zu verschärfen, anstatt das Vertrauen in die innere Sicherheit zu fördern und die Personenfreizügigkeit im Schengen-Raum zu untermauern.

Deshalb sollten die EU-Mitgliedstaaten die aktuelle Entscheidungsdynamik hin zu intelligenten Grenzen und Interoperabilität überdenken. Wird die Perspektive über Migrationskrise und Terrorismusbekämpfung hinaus geweitet, zeigen sich drei alternative Handlungsprioritäten, um den mittelfristig zu erwartenden Ausbau intelligenter Grenzen und interoperabler Datenbanken auf eine nachhaltige rechtsstaatliche Grundlage zu stellen: 1. ein konstruktiver Umgang mit Urteilen des Europäischen Gerichtshofs zur Verhältnismäßigkeit der anlasslosen Datenspeicherung an intelligenten Grenzen; 2. die Konsolidierung des europäischen Datenschutzrechts; 3. Stärkung der Mechanismen, mit denen sich Einträge in EU-Datenbanken beaufsichtigen und damit verbundene Entscheidungen effektiv anfechten lassen.

Die Verhältnismäßigkeit der anlasslosen Datenspeicherung

Der Europäische Gerichtshof (EuGH) hat in den vergangenen drei Jahren ein streitbares Profil in Fragen des Grundrechts- und Datenschutzes gewonnen,[144] was sich zunehmend auf die Entwicklung intelligenter Grenzen auswirkt. Vergleichbar mit Standpunkten des Bundesverfassungsgerichts erklärte der EuGH, dass eine massenhafte und anlasslose Speicherung von Daten nur unter sehr engen Bedingungen als notwendig und verhältnismäßig gelten könne. Die EU-rechtliche Regelung zur anlasslosen Speicherung von Telekommunikationsdaten sei in dieser Hinsicht zu weitreichend. Es bedürfe der Eingrenzung auf Verdachtsgruppen, damit die verbürgten Grundrechte auf Privatsphäre und Datenschutz[145] gewahrt blieben. Ende 2016 wandte der EuGH diese kritische Argumentation auch auf nationale Regelungen zur Vorratsdatenspeicherung in Großbritannien und Schweden an.[146]

144 Der EuGH erlangte erst ab 2014 die Aufsicht für das gesamte Politikfeld des RFSR. Die Aufwertung der EU-Grundrechtecharta im Vertrag von Lissabon hatte zuvor die Basis für den EuGH gelegt, um sich im Spannungsfeld mit dem deutschen Verfassungsgericht und dem Europäischen Gerichtshof für Menschenrechte zu behaupten. Siehe Claudio Franzius, »Grundrechtsschutz in Europa: Zwischen Selbstbehauptungen und Selbstbeschränkungen der Rechtsordnungen und ihrer Gerichte«, in: *Zeitschrift für ausländisches öffentliches Recht und Völkerrecht*, 75 (2015) 1, S. 383–412.

145 Artikel 16 AEUV sowie Artikel 7 und 8 Grundrechtecharta.

146 Verbundene Rechtssache C-203/15 Tele2 Sverige AB und C-698/15 Watson, 21.12.2016.

Im Sommer 2017 kam der Gerichtshof zum Schluss, dass das EU-Abkommen mit Kanada zur Übermittlung von erweiterten Fluggastdaten (PNR) diesen Ansprüchen nicht genüge.[147] Zwar akzeptierte er, dass die flächendeckende Sammlung von PNR-Daten für Zwecke der unmittelbaren Gefahrenabwehr und Strafverfolgung als notwendig erachtet werden könne. Allerdings sollten, so der EuGH, nach Abreise aus Kanada die PNR-Daten europäischer Bürger nur dann längerfristig gespeichert werden können, wenn ein konkreter Anhaltspunkt für weitere Ermittlungen oder Gefahren bestehe.

Die geplanten Regeln für Fluggast-Daten widersprechen womöglich den Vorgaben des EuGH.

Für Sicherheitsbehörden ergibt sich die Aussagekraft von PNR-Daten aber gerade aus der querschnittsartigen Auswertung aller Reisebewegungen. So wird analysiert, welche längerfristigen Datenmuster (zuvor besuchte Reiseziele, Flugrouten, Begleitpersonen, Gepäck etc.) auf potentielle Gefährder und Straftäter hinweisen, die bisher nicht auffällig geworden sind. Würden die analysierbaren Datenbestände eingeschränkt, entgingen den Sicherheitsbehörden wichtige Ansatzpunkte für Ermittlungen. Dabei geht es nicht nur um die Abwehr terroristischer Gefahren; vor allem auch Zollbehörden greifen auf solche Auswertungen zurück.[148]

Somit sind die Anforderungen des EuGH nicht ohne weiteres durchsetzbar. Der Streit mit den Vereinigten Staaten zur Einführung der PNR-Datenübermittlung in den 2000er Jahren wurde vor dem Hintergrund der Drohung geführt, dass EU-Bürger ihre Visumsfreiheit verlieren könnten. Die derzeit geltenden PNR-Vereinbarungen mit den USA und auch Australien müssen in einigen Jahren erneuert werden. Darüber hinaus hält eine Resolution des Sicherheitsrats der Vereinten Nationen von Ende 2017 alle Staaten dazu an, die Auswertung von PNR-Daten zur Terrorismusbekämpfung einzuführen.[149] Die zwingende Neuverhandlung des PNR-Abkommens zwischen der EU und Kanada hat deshalb besondere Bedeutung. Es ist dringend notwendig, einen detaillierten und tragfähigen Kompromiss auszuarbeiten, der einer weiteren Prüfung vor dem EuGH standhalten kann.

Unklar ist, ob die eigene EU-Gesetzgebung zur PNR-Auswertung der neueren Argumentation des EuGH gerecht werden kann. Bei der Einigung im Frühjahr 2016 setzte das Europäische Parlament zahlreiche datenschutzrechtliche Mechanismen durch, etwa ein Verbot vollautomatisierter Risikobewertungen von Reisenden. Allerdings sollen die erhobenen PNR-Daten noch immer für bis zu fünf Jahre anlasslos gespeichert werden können. Folgt man dem Urteil des EuGH im Fall Kanada, wäre dieser Ansatz nicht mehr zu rechtfertigen. Die Mitgliedstaaten müssten vielmehr Sorge tragen, dass alle PNR-Daten gelöscht werden, sobald die erfasste Person aus der EU abgeflogen ist. Nur in begründeten Verdachtsfällen wäre erlaubt, die betreffenden Informationen längerfristig zu speichern. Um dieses Verfahren rein praktisch umsetzen zu können, wäre zumindest ein Ein- und Ausreisesystem an internationalen Flughäfen vonnöten, wie es in den USA und Kanada existiert. Diesen Teil des vorgesehenen europäischen EES umzusetzen wird auch unter günstigsten Annahmen mindestens drei Jahre dauern.[150] Schon deutlich früher könnte die EU-PNR-Richtlinie vor dem EuGH angefochten werden.

Im Bereich der europäischen Asyl- und Flüchtlingspolitik war der EuGH zuletzt vorsichtiger damit, die Sicherheitsinteressen der Mitgliedstaaten zugunsten individueller Grundrechte zurückzuweisen.[151] Angesichts dieser Entwicklung ist möglich, dass er auch in anderen Fragen der Innenpolitik einen Interessenausgleich mit den nationalen Regierungen suchen wird. Problematisch ist aber, wenn einige Mitgliedstaaten kritische Urteile des EuGH, die in diesem Themenfeld ergangen sind, nicht vorausschauend auf ihre Sicherheitsgesetzgebung anwenden. Dies zeigt

147 Rat der Europäischen Union, 11931/17, 7.9.2017, <www.statewatch.org/news/2017/sep/eu-council-legal-service-eu-canada-pnr-cjeu-11931-17.pdf> (Zugriff am 4.12.2017).

148 Han Chang-Ryung/Rachel McGauran/Hans Nelen, »API and PNR Data in Use for Border Control Authorities«, in: *Security Journal*, 30 (2017) 4, S. 1045—1063.

149 United Nations Security Council, Resolution 2396 (2017) [wie Fn. 106], S. 7.

150 Siehe oben zu den längerfristigen Herausforderungen bei Umsetzung eines EES.

151 Thomas Spijkerboer, »The EU Court of Justice Refuses to Address Refugee Exclusion«, *Forced Migration Forum*, 19.1.2018, <https://forcedmigrationforum.com/2018/01/19/the-eu-court-of-justice-refuses-to-address-refugee-exclusion/> (Zugriff am 4.2.2018).

sich etwa mit Blick auf die anlasslose Vorratsdatenspeicherung.[152] Sie wird von zahlreichen europäischen Staaten unverändert aufrechterhalten; zugleich kommen Diskussionsprozesse nur schleppend voran, wie sich EU-weit die Maßgaben des Gerichtshofs anwenden ließen.[153] Im Gegensatz dazu könnte das noch laufende Umsetzungsverfahren zur PNR-Richtlinie genutzt werden, um einen neuen Zeitrahmen auszuarbeiten, der sich am gesamten Maßnahmenpaket für intelligente Grenzen orientiert. So ließen sich in den kommenden zwei bis drei Jahren zusätzliche Mechanismen für den Datenschutz ausarbeiten, wie etwa eine möglichst umfassende Anonymisierung und Begrenzung der Auswertungszwecke bei anlasslos gespeicherten PNR-Daten.

Konsolidierung des europäischen Datenschutzregimes

Das Jahr 2018 ist zentral für die Konsolidierung des EU-Datenschutzrechts. Ziel ist ein verlässliches Zusammenspiel von drei novellierten Rechtsakten der EU, nämlich der Datenschutz-Grundverordnung, der Datenschutzrichtlinie für nationale Strafverfolgungsbehörden und der Datenschutzverordnung für das Handeln von EU-Organen. Alle drei Datenschutzgesetze sind relevant für die Nutzung von EU-Datenbanken, während sich durch die angestrebte Interoperabilität neue Fragen ergeben, wie eine kohärente Anwendung möglich ist.

Bis Ende Mai 2018 sollte die Datenschutz-Grundverordnung der EU für alle zivilrechtlichen und wirtschaftlichen Belange umgesetzt werden. Im selben Zeitrahmen ist vorgesehen, die novellierte Datenschutzrichtlinie für die Tätigkeit von Strafverfolgungsbehörden in nationales Recht zu übertragen.[154] Die Richtlinie orientiert sich an der Grundverordnung, die zahlreiche Prinzipien für einen zeitgemäßen Datenschutz definiert. Dazu gehört etwa, dass biometrische Daten möglichst zurückhaltend genutzt werden, vollautomatisierte Profilbildungs- und Entscheidungsprozesse stark eingeschränkt sind oder betroffene Individuen direkte Auskunftsbefugnisse haben. Der Geltungsbereich der Datenschutzrichtlinie erstreckt sich dabei auch auf nationale Datenverarbeitungsprozesse, während in der Vergangenheit nur grenzüberschreitende Datenübermittlungen durch EU-Recht tangiert wurden.[155] Diese Ausweitung bedeutet, dass die EU-Grundrechtecharta und die damit verbundene Aufsichtsfunktion des EuGH potentiell auf alle Datenverarbeitungsprozesse nationaler Strafverfolgungsbehörden anwendbar sind.

Diesen weitreichenden Änderungen für mehr Datenschutz stehen Ausnahmeregelungen im Bereich der nationalen Sicherheit entgegen. Zudem sind in der Richtlinie die Befugnisse von Datenschutzbehörden und die damit verbundenen Sanktionsmöglichkeiten eher locker definiert. Somit stellt sich wie bei vielen EU-Richtlinien die Frage, ob nicht doch möglichst weitgehend am bestehenden nationalen Regelwerk festgehalten wird. Während Deutschland bereits im Sommer 2017 eine einheitliche Anpassung des nationalen Datenschutzgesetzes vorgenommen hat,[156] ist bei vielen anderen Mitgliedstaaten damit zu rechnen, dass sich Reformen im Kontext der Richtlinie verzögern werden.[157] Bislang liegt jedenfalls noch keine Bewertung vor, wie sich deren Vorgaben auf die Praxis der nationalen Sicherheitsbehörden auswirken.

Dass die Richtlinie in allen Mitgliedstaaten konsistent umgesetzt wird, ist aufgrund der vorgesehenen Interoperabilität von besonderer Bedeutung. Die europäische Migrationspolitik wurde schon vor dem Lissabonner Vertrag schrittweise in der ersten Säule der EU angesiedelt; das heißt, sie bildete schon ab den 2000er Jahren rechtlich ein zunehmend vergemeinschaftetes Politikfeld. Daraus resultiert eine Pfadabhängigkeit, die dazu führt, dass heute bei regulären Migrationskontrollen mit EU-Instrumenten die allge-

152 Privacy International, *National Data Retention Laws since the CJEU's Tele-2/Watson Judgment*, September 2017, <https://privacyinternational.org/sites/default/files/Data%20Retention_2017.pdf> (Zugriff am 14.2.2017).

153 Statewatch, *The »Reflection Process« on Data Retention: Working Documents Discussed by Council Published*, 28.2.2018, <http://statewatch.org/news/2018/feb/eu-drd-reflection-docs.htm> (Zugriff am 28.2.2017).

154 Richtlinie EU (2016/680), 27.4.2016.

155 Matthias Bäcker, »Die Datenschutzrichtlinie für Polizei und Strafjustiz und das deutsche Eingriffsrecht«, in: Hermann Hill/Dieter Kugelmann/Mario Martini (Hg.), *Perspektiven der digitalen Lebenswelt*, Baden-Baden 2017, S. 63–88.

156 Gesetz zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680, 30.6.2017.

157 Commission Expert Group on the Regulation (EU) 2016/679 and Directive (EU) 2016/680 (E03461), <http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetail&groupID=3461&NewSearch=1&NewSearch=> (Zugriff am 14.2.2018).

meine Datenschutz-Grundverordnung anzuwenden ist. Dies betrifft beispielsweise die Datenverarbeitung des künftigen Ein- und Ausreisesystems zur Überprüfung der legalen Aufenthaltsdauer. Davon zu unterscheiden ist die Zusammenarbeit von Polizei- und Strafverfolgungsbehörden, die historisch der dritten (nicht vergemeinschafteten) Säule der EU zugeordnet wurde. Wenn nun vorhandene Informationen in Migrations- und Grenzdatenbanken genutzt werden sollen, um die Arbeit von Strafverfolgungsbehörden zu unterstützen, ist die jeweilige nationale Gesetzgebung zur Umsetzung der gesonderten Datenschutzrichtlinie anzuwenden.

Grundsätzlich ist dieses differenzierte Vorgehen bekannt, da EURODAC und VIS seit 2013 in Ausnahmefällen zur Bekämpfung von schwerer Kriminalität oder Terrorismus abgefragt werden können. Im Rahmen der Interoperabilität soll es künftig jedoch der Regelfall sein, dass Daten flexibel für die Migrationskontrolle und für alltägliche Aufgaben der Strafverfolgungsbehörden genutzt werden.[158] Damit dürften die Fälle deutlich zunehmen, in denen schwierige Abgrenzungsentscheidungen zwischen verschiedenen datenschutzrechtlichen Bestimmungen der EU zu treffen sind.[159] Aus diesem Grund ist es so wichtig, dass die Datenschutzrichtlinie für Strafverfolgungsbehörden einheitlich umgesetzt wird und in allen Mitgliedstaaten vergleichbare Standards bei der Nutzung interoperabler EU-Datenbanken gelten. Die Zweckbindung von Daten, die in unterschiedlichen Systemen für die polizeiliche Zusammenarbeit und die Migrationskontrolle erfasst wurden, bleibt als rechtlicher Grundsatz erhalten; dieser verlangt nach einer möglichst präzisen Regelung, wann eine andersgeartete Datennutzung gerechtfertigt ist.[160] Technische Mittel zur Vermeidung datenschutzrechtlicher Konflikte — wie sie die Hochrangige Expertengruppe für die Interoperabilität mit Bezug auf das »Hit/No Hit«-Verfahren vorgeschlagen hat —, sind allein nicht ausreichend.

Die EU-Staaten könnten ihre Bemühungen um mehr Datenschutz überdenken.

Währenddessen laufen Verhandlungen zu einer Überarbeitung der Datenschutzverordnung für EU-Organe und EU-Handeln[161] — ein Prozess, der sich aus Gründen der Kohärenz in fast allen Belangen an der neuen Datenschutz-Grundverordnung orientiert.[162] Eine zentrale Differenz zwischen den Positionen des Ministerrats und jenen des Europäischen Parlaments besteht hier in der Frage, ob sich eine revidierte Datenschutzverordnung für EU-Institutionen auch auf den gesamten Politikbereich des RFSR erstrecken bzw. Agenturen wie Europol miteinbeziehen soll. Die Mitgliedstaaten lehnen eine flächendeckende Regelung ab; sie begründen dies mit den bereits bestehenden Datenschutzregeln für diese Agenturen und der besonderen Sensibilität des Themenfelds, das ansonsten in der Datenschutzrichtlinie für Strafverfolgungsbehörden geregelt wird. Die erst 2016 erneuerten rechtlichen Mandate von Europol und der Europäischen Agentur für Grenzschutz und Küstenwache zeugen in der Tat von Anstrengungen, die wachsenden Befugnisse zur Verarbeitung von personenbezogenen Daten einzuhegen und zu kontrollieren.[163]

Die vorgesehene Interoperabilität und der Ausbau intelligenter Grenzen könnten den Mitgliedstaaten jedoch Anlass für eine Neubewertung geben. So gelten beispielsweise biometrische Daten in der Europol-Verordnung — anders als bei allen anderen EU-Daten-

158 Dies soll durch alle drei Mechanismen des »common identity repository«, des »biometric matching service« und des »european search portal« ermöglicht werden. Deshalb handelt es sich um eine grundsätzlichere Reform der Zweckbindung von gespeicherten Informationen, als es die vereinzelte Abfrage von EURODAC und VIS durch Strafverfolgungsbehörden bedeutet.

159 European Data Protection Supervisor, *Reflection Paper on the Interoperability of Information Systems in the Area of Freedom, Security and Justice*, 17.11.2017, <www.statewatch.org/news/2017/nov/edps-interoperabilit-jha.pdf> (Zugriff am 14.2.2018).

160 Gerade in Deutschland wird diese rechtliche Debatte besonders intensiv geführt. Das Bundesverfassungsgericht hat 2016 den »Grundsatz der hypothetischen Datenneuerhebung« als Bewertungsmaßstab angelegt, um die Verhältnismäßigkeit einer weitergehenden Datenverarbeitung durch Strafverfolgungsbehörden zu beurteilen.

161 Verordnung (EG) Nr. 45/2001 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe und Einrichtungen der Gemeinschaft.

162 European Data Protection Supervisor, *Upgrading Data Protection Rules for EU Institutions and Bodies*, 15.5.2017 (Opinion 5/2017), <https://edps.europa.eu/sites/edp/files/publication/17-03-15_regulation_45-2001_en.pdf> (Zugriff am 4.12.2017).

163 Verordnung (EU) 2016/794, Kapitel IV; Verordnung (EU) 2016/1624, Art. 45—48.

schutzgesetzen — nicht als sensibel. Zugleich soll der »biometric matching service« im Rahmen der Interoperabilität auch Europol einen erweiterten Datenzugriff eröffnen. Für eu-LISA könnten ebenfalls neue Verantwortlichkeiten im Umgang mit personenbezogenen Daten entstehen,[164] sollte die Agentur etwa zum zentralen Dienstleister für die Datenqualität in allen Themenbereichen der Migrationskontrolle und der Strafverfolgung ausgebaut werden. Ein möglichst einheitlicher und verständlicher Rechtsrahmen für das Handeln von EU-Organen, einschließlich des gesamten Politikfelds des RFSR und seiner Agenturen, erscheint somit erstrebenswert. Wird die entsprechende Forderung des Europäischen Parlaments zurückgewiesen, könnte dies eine zügige Verhandlung anderer Sicherheitsgesetze und Vorhaben für intelligente Grenzen gefährden.

Gestärkte Aufsichts- und Korrekturmechanismen

Bisher räumt die EU-Gesetzgebung allgemeine Auskunfts-, Korrektur- und Löschungsrechte gegenüber jenen nationalen Behörden ein, die die europäischen Datenbanken für Zwecke der inneren Sicherheit und der Migrationskontrolle nutzen.[165] Dieses dezentrale System weist jedoch beträchtliche Schwächen auf.[166] Für Drittstaatsangehörige und Nichtexperten ist es schwierig, die Verantwortlichkeiten und Verfahren auf nationaler Ebene korrekt zuzuordnen. Nationale Datenschutzbehörden haben nur sehr begrenzte Ressourcen, um individuelle Antragsteller zu unterstützen oder regelmäßige Kontrollen bei Sicherheitsbehörden durchzuführen. Oftmals verzögert sich zudem die Änderung oder Löschung von Dateneinträgen, insbesondere wenn Behörden verschiedener Mitgliedstaaten involviert sind.

Zu empfehlen ist aber, dass das bestehende dezentrale System ausgebaut wird, vor allem mit Blick auf intelligente Grenzen und die Interoperabilität.[167] Die stärkere Nutzung biometrischer Daten kann helfen, Identitätsmissbrauch und alphanumerische Datenfehler zu vermeiden. Außerdem erhoffen Sicherheitsbehörden zu Recht, dass der automatische Datenabgleich im »common identity repository« und der »multiple identity detector« für einen einheitlicheren Personendatenbestand sorgen werden. Umso mehr muss sichergestellt sein, dass die betreffenden Dateneinträge im Zweifelsfall effektiv angefochten werden können.[168] Anwender ohne spezifische technische Ausbildung wissen in der Regel nicht, dass biometrische Daten keine vollständige Sicherheit dabei bieten, Personen zu identifizieren und zu authentifizieren. Das Problembewusstsein könnte noch weiter sinken, je häufiger biometrische Daten erhoben, automatisiert verarbeitet und über verschiedene Datenbanken abgeglichen werden. Interoperabilität darf also nicht dazu führen, dass fehlerhafte Personendaten nur mit besonderer Mühe korrigiert werden können.

Reguläre Polizei- und Grenzschutzkräfte werden zusätzlich über das einheitliche European Search Portal auf Fahndungsersuchen und Einträge bei Europol und Interpol zugreifen können. Selbst wenn das »Hit/No Hit«-Verfahren eine zweite Autorisierung der abfragenden Behörde verlangt, ist bei diesen Datenbeständen mit besonderer Umsicht zu agieren. Bereits die vorläufige Anzeige eines Datenbanktreffers bei Interpol oder Europol kann dazu führen, dass polizeiliche Maßnahmen ergriffen werden. Insbesondere bei Interpol ist dabei zu berücksichtigen, dass Fahndungsausschreibungen wiederholt von Drittstaaten

164 Siehe Europäische Kommission, COM (2017) 352, 9.6.2017, und European Data Protection Supervisor, *EDPS Opinion on the Proposal for a Regulation on the eu-LISA*, 9.10.2017.

165 Siehe beispielsweise SIS II Supervision Coordination Group, *The Schengen Information System. A Guide for Exercising the Right of Access*, Brüssel: European Data Protection Supervisor, Oktober 2015, <https://edps.europa.eu/sites/edp/files/publication/16-11-07_sis_ii_guide_of_access_en.pdf> (Zugriff am 4.12.2017).

166 SIS II Supervision Coordination Group, *Report on the Exercise of the Rights of the Data Subject in the Schengen Information System (SIS)*, Brüssel, Oktober 2014, <https://edps.europa.eu/sites/edp/files/publication/14-10-28_report_on_the_exercise_of_the_rights_of_the_data_subject_in_sis_ii_en.pdf> (Zugriff am 4.12.2017).

167 Meijers Committee, Standing Committee of Experts on International Immigration, Refugee and Criminal Law, *CM1802 Comments on the Proposal for a Regulation of the European Parliament and of the Council on Establishing a Framework for Interoperability between EU Information Systems*, 19.2.2018, <www.statewatch.org/news/2018/feb/eu-meijers-cttee-interoperability.pdf> (Zugriff am 24.2.2018).

168 European Union Agency for Fundamental Rights, *Fundamental Rights and the Interoperability of EU Information Systems* [wie Fn. 107].

missbräuchlich für Zwecke der politischen Verfolgung genutzt wurden.[169]

Grundsätzlich muss nach Artikel 47 der EU-Grundrechtecharta ein effektiver Rechtsweg gegenüber allen behördlichen Entscheidungen und Handlungen garantiert sein. Dies gilt nicht nur für die Arbeit von Strafverfolgungsbehörden, sondern auch für die allgemeine Grenz- und Migrationskontrolle. Selbst wenn Drittstaatsangehörige kein allgemeines Anrecht auf die Einreise haben, werden ihre Verfahrensrechte zunehmend inklusiv ausgelegt. In einem Urteil mit Bezug auf ein durch Polen verweigertes Schengen-Visum entschied der EuGH erst Ende 2017, dass eine Beschwerdeprüfung durch die Verwaltung nicht ausreiche.[170]

Nationale Grenzschutzbehörden werden in vielen Einzelfällen umstrittene Entscheidungen treffen.

An diesen Standards müssen sich neue intelligente Grenzkontrollen messen lassen, die dazu führen können, dass die Einreise in die Schengen-Zone verweigert wird. Insbesondere für die vorgesehene elektronische Einreiseerlaubnis ETIAS werden alle Mitgliedstaaten einen effektiven Rechtsweg anbieten müssen.[171] Selbst wenn ein sehr hoher Prozentsatz aller ETIAS-Anträge positiv beschieden werden sollte, muss das Gesamtvolumen von voraussichtlich mindestens 40 Millionen Entscheidungen pro Jahr berücksichtigt werden. Nach Abschluss des Brexit werden zusätzlich alle britischen Staatsbürger eine ETIAS-Einreiseerlaubnis benötigen.

Die Bürger visabefreiter Drittstaaten verfügen in der Regel über die notwendigen Ressourcen, um ein juristisches Verfahren anstrengen zu können. Besonderheiten des ETIAS-Systems könnten verstärkt Anlass zu Auseinandersetzungen geben. Zwar soll die elektronische Einreiseerlaubnis auf Grundlage einer einheitlichen europäischen Risikobewertung erteilt werden. Dennoch werden nationale Grenzschutzbehörden umstrittene Einzelfallentscheidungen treffen müssen.[172] Beispielsweise gelten Vorstrafen bisher nur selten als Grund dafür, die Einreise in die Schengen-Zone zu verweigern.[173] Künftig aber sollen Strafeinträge, die möglicherweise in einem oder mehreren EU-Mitgliedstaaten erfolgt sind,[174] für das ETIAS-Verfahren systematisch abgefragt werden.[175] Ohne eine stärkere Konvergenz des europäischen Strafrechts wird zu klären sein, wie sich diese Einträge auf verhältnismäßige und rechtssichere Weise bewerten lassen. So könnte beispielsweise Portugal einem Drittstaatsangehörigen die Einreiseerlaubnis verweigern, wenn dieser in der Vergangenheit in einem anderen EU-Mitgliedstaat für ein Drogenvergehen verurteilt wurde — selbst wenn ein vergleichbarer Drogenbesitz in Portugal nicht strafbar wäre.

Schließlich stellt die ETIAS-Warnliste zu Terrorismusverdächtigen sowie Kriegs- und Schwerverbrechern[176] eine politische Herausforderung dar. Inspiriert wurde der Vorschlag für eine solche EU-Warnliste durch die »Terrorism Watchlist« bzw. die untergeordnete »No Fly List« der USA. Auch wenn die ETIAS-Warnliste sich auf visabefreite Drittstaatsange-

169 Andrew Rettman, »EU in Talks with Interpol on Political Abuse«, *euobserver*, 5.10.2017, <https://euobserver.com/justice/139292> (Zugriff am 4.12.2017). Der Fall des deutsch-türkischen Schriftstellers Dogan Akhanli, der aufgrund einer missbräuchlichen Interpol-Fahndung für einige Zeit in Spanien festgehalten wurde, beschäftigte im Herbst 2017 die Bundesregierung.

170 Urteil des Gerichtshofs in der Rechtssache C-403/16, <http://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:62016CJ0403> (Zugriff am 4.12.2017). In Deutschland besteht dieser Rechtsweg für Schengen-Visa, allerdings mit kleineren Einschränkungen im Vergleich zum Anspruch auf einen Rechtsbehelf nach Artikel 19(4) Grundgesetz. Siehe Kay Hailbronner, *Asyl- und Ausländerrecht*, Stuttgart [4]2017, Abs. 316.

171 Dies gilt auch dann, wenn — wie im amerikanischen ESTA-Verfahren — ein Ausnahmevisum anstelle einer verweigerten elektronischen Einreiseerlaubnis beantragt werden kann.

172 Nationale ETIAS-Stellen bearbeiten individuelle Anträge, während die Bewertungskriterien durch eine ETIAS-Zentralstelle bei Frontex überwacht werden sollen. Siehe Europäische Kommission, COM (2016) 731, 16.11.2016, insb. Artikel 28.

173 Dimitra Blitsa/Lauryn Gouldin/James B. Jacobs/Elena Larrauri, *Criminal Records and Immigration: Comparing the United States and the European Union*, New York: New York University School of Law, 2015 (New York University Public Law and Legal Theory Working Papers 539/2015), <http://lsr.nellco.org/nyu_plltwp/539> (Zugriff am 4.12.2017).

174 Im Rahmen des sogenannten ECRIS-TCN-Systems, siehe Kapitel 2.

175 Europäische Kommission, COM (2016) 731/3, 16.11.2016, Artikel 18; Europäische Kommission, COM (2017) 344, 29.6.2017.

176 Europäische Kommission, COM (2016) 731, 16.11.2016.

hörige beschränken soll, ist die EU bislang nicht auf die damit verbundene Verantwortung eingestellt. Zur Erteilung eines Schengen-Visums findet eine horizontale Konsultation zwischen nationalen Sicherheitsbehörden statt.[177] Bei diesem Verfahren bleibt es in der Verantwortung nationaler Behörden, eine Einreise zu verweigern, eine verdächtige Person zu kontrollieren oder sie festzunehmen. Formal soll dies auch für das kommende ETIAS-Verfahren gelten. Nationale ETIAS-Stellen werden jedoch kaum Ermessensspielraum haben, wenn ein Eintrag auf der europäischen Warnliste vorliegt. Umgekehrt wird die EU als Ganzes in die Verantwortung genommen, einen möglichst umfassenden Schutz zu garantieren. Ein terroristischer Anschlag, der aufgrund einer lückenhaften Warnliste nicht vereitelt werden konnte, wäre eine besondere Belastung für die EU-Sicherheitspolitik. Für die »Terrorism Watchlist« der USA gibt es aus vergleichbaren Gründen eine möglichst sorgfältige Datenauswertung, an der sich unterschiedliche Sicherheitsbehörden und Nachrichtendienste beteiligen.[178] Dennoch wird seit vielen Jahren kritisiert, dass diese Liste zu umfassend ausfalle.[179]

Die EU kann die Verfahren der Vereinigten Staaten nicht direkt nachbilden, da die EU-Verträge keine Kompetenz für die Arbeit von Nachrichtendiensten einräumen. Allerdings befindet sich das Anti-Terrorismus-Zentrum bei Europol im Wachstum, und es kann über nationale Staatsschutzstellen indirekt Zugriff auf nachrichtendienstliche Informationen erhalten.[180] Auf dieser Basis ist Europol in der Lage, für die gesamte EU die künftige ETIAS-Warnliste mitzugestalten. Zu diesem besonders sensiblen Aspekt intelligenter Grenzen sollte jedoch auch auf EU-Ebene eine begleitende politische Aufsicht erfolgen. Die 2017 eingerichtete interparlamentarische Kontrollversammlung von Europol, die europäische und nationale Abgeordnete zusammenbringt, bietet sich hierfür an.[181] Nationale Parlamentarier könnten ihre Fachkenntnisse und Auskunftsrechte zu nachrichtendienstlichen Themen einbringen, während das Europäische Parlament über die Entwicklung aller Agenturen im RFSR mitentscheiden würde.

177 Verordnung (EC) Nr. 767/2008, Artikel 50(3).

178 Walter Haydock, »Consolidating the Terrorist Watchlisting Bureaucracy«, *lawfareblog.com*, 14.6.2017.

179 Peter J. Phillips/Gabriela Pohl, »Terrorism Watch Lists, Suspect Ranking and Decision-Making Biases«, in: *Studies in Conflict & Terrorism* (online first article), 18.1.2018, <https://doi.org/10.1080/1057610X.2018.1432046/> (Zugriff am 8.2.2018).

180 Erreichen lässt sich dies über die Doppelfunktion einiger nationaler Behörden (als polizeiliche Staatsschutzstellen und als Binnennachrichtendienste) sowie durch die gemischte Nutzung von Europol-Informationssystemen. Zugleich besteht die Möglichkeit einer verstärkten informellen Kooperation mit der sogenannten Counter Terrorism Group (CTG). Siehe Deutscher Bundestag, Drucksache 18/11261, 21.2.2017.

181 FREE Group, *The Mejiers Committee on the Interparliamentary Scrutiny of Europol*, 16.2.2017, <https://free-group.eu/2017/02/16/the-mejiers-committee-on-the-interparliamentary-scrutny-of-europol/> (Zugriff am 4.12.2017).

Schlussfolgerungen und Ausblick

Die Einrichtung intelligenter Grenzen und der Ausbau von Datenbanken zur Migrationskontrolle und Strafverfolgung werden auf Ebene der europäischen Gesetzgebung mit Hochdruck vorangetrieben. Anders als in der europäischen Migrations- und Asylpolitik, wo es an Solidarität mangelt, wollen die EU-Mitgliedstaaten hier gemeinsamen Handlungswillen demonstrieren. Diese Dynamik führt nicht zwangsläufig zu einer »Festung Europa« mit biometrischen Toren. Idealerweise kann es die Offenheit europäischer Grenzen gerade unterstützen, wenn die Verwaltung der legalen Migration einfacher wird. Die systematische Verbindung von Datenbeständen und deren Interoperabilität können dazu beitragen, Identitätsmissbrauch zu erschweren und polizeiliche Fahndungen zu erleichtern. Grundsätzlich können sich die EU-Mitgliedstaaten nicht vor den langfristigen Entwicklungen in diesen Themenfeldern verschließen. Seit den frühen 2000er Jahren fordern die USA, intelligente Grenzen einzuführen; ebenso lange besteht innereuropäischer Reformdruck, ein kohärentes Informationsmanagement der Strafverfolgungsbehörden zu schaffen. Beide Faktoren werden noch weit in der Zukunft wirken.

Allerdings birgt die Verdichtung der EU-Sicherheitspolitik seit 2016 das Risiko, dass falsche Erwartungen entstehen und unausgewogene Prioritäten verfolgt werden. Der verstärkte Einsatz von Sicherheitstechnik ist nur bedingt dazu geeignet, das öffentliche Vertrauen in die EU zu stärken. Die gesamteuropäische Lage der inneren Sicherheit wird von Bürgern tendenziell verzerrt und zu kritisch wahrgenommen. Dennoch ist die Unterstützung für die Personenfreizügigkeit nach wie vor sehr hoch. Deshalb kann keine Rede sein von einer existentiellen Krise des Schengen-Regimes, die neue Grenztechnik zwingend erforderlich machte. Umgekehrt hat das Brexit-Referendum verdeutlicht, dass auch bereits vorhandene intelligente Grenzkontrollen keinen signifikanten Einfluss auf die öffentliche Meinung haben müssen. Es bleibt deshalb Aufgabe politischer Führung, die Gefahren für die innere Sicherheit einzuordnen und zu verantworten, die mit internationaler Mobilität und weitgehend durchlässigen Grenzen einhergehen. Andernfalls droht ein Wettlauf um immer mehr Sicherheitstechnik und Datenverarbeitung, die eine lückenlose Kontrolle versprechen, aber ebenso zu Überwachungsängsten und gesellschaftlicher Polarisierung beitragen können.

Auch aus funktionaler Sicht können neue intelligente Grenzsysteme nur wenig dabei helfen, die dringendsten Sicherheitsherausforderungen der EU zu bewältigen. Die flächendeckende Einführung eines Ein- und Ausreisesystems und einer elektronischen Einreiseerlaubnis wird mindestens vier bis fünf Jahre in Anspruch nehmen. Dabei werden es diese Systeme — so wie sie derzeit geplant sind — nicht erlauben, einen direkten Abgleich von biometrischen Daten ausländischer Kämpfer vorzunehmen. Zu diesem Zweck findet schon jetzt ein intensiver Informationsaustausch auf bi- und multilateraler Ebene statt, der auch Europol zunehmend einbindet. Die EU und ihre Mitgliedstaaten sind also in diesem Bereich der Terrorismusbekämpfung durchaus handlungsfähig. Derweil zeigen langfristige Erfahrungen der Vereinigten Staaten und der EU, dass irreguläre Zuwanderung nur unwesentlich durch Verfahren zur biometrischen Registrierung beeinflusst wird. Eine automatisierte Kontrolle der Aufenthaltsberechtigung (wie im EES) oder die möglichst lückenlose Erfassung von Asylsuchenden (wie in der EURODAC-Datenbank) können die Verwaltung der Migration unterstützen, schaffen aber ebenso Anreize für verdeckte Einreisen und langfristig illegale Aufenthalte.

Wenn nun also EU-Gesetzesvorhaben für intelligente Grenzen und für interoperable Datenbanken aneinander gekoppelt werden, sollte man kritische Fragen zur Effektivität einzelner Systeme nicht ausblenden. Vielmehr besteht das Risiko, dass die Umsetzungskapazitäten der nationalen Sicherheitsbehörden überlastet werden, weil sich immer mehr

EU-Initiativen anhäufen. In den vergangenen 15 Jahren haben sich fast alle Maßnahmen für das Informationsmanagement im RFSR und für intelligente Grenzen nur mit beträchtlichen Verzögerungen realisieren lassen. Um die innere Sicherheit der EU möglichst schnell zu stärken, sollte der Rat der Innenminister den Ausbau bestehender Instrumente zur polizeilichen Zusammenarbeit priorisieren. Dies betrifft insbesondere das Schengen-Informationssystem, das gleichermaßen für Migrationskontrolle und Terrorismusbekämpfung eingesetzt werden kann. Im Gegensatz dazu sollten neue intelligente Grenzen und die Interoperabilität als weniger dringliche Projekte behandelt werden; sie können selbst unter günstigen Umständen erst im kommenden Jahrzehnt ihre Wirkung entfalten.

Das Abkommen mit Kanada über Fluggast-Daten muss dringend neu verhandelt werden.

Zwar laden die aktuelle Sicherheitskrise und die Komplexität der EU-Datenbankarchitektur dazu ein, einheitliche Strukturen und damit einen historischen Bruch zu fordern. Die Zusammenführung von Daten und technischen Infrastrukturen stellt für sich genommen aber noch keinen Mehrwert dar — weder für eine zukünftige EU-Sicherheitsunion noch für die bestehende Schengen-Zone. Aus rechtsstaatlicher Sicht ist darauf zu achten, dass alle Sicherheitsbehörden eine möglichst verhältnismäßige und zielgerichtete Datenverarbeitung betreiben. Der Grundsatz der Zweckbindung von erhobenen Informationen muss trotz der angespannten Sicherheitslage erhalten bleiben. Die aktuellen Gesetzesvorschläge zur Interoperabilität orientieren sich in einigen zentralen Belangen an diesen normativen Ansprüchen. Ein einziger Datenpool für die europäische Migrationskontrolle und die Strafverfolgung wird nicht entstehen. Vielmehr sollen unterschiedliche Instrumente dabei helfen, getrennte Datenbanken besser zu verwalten und leichter abzufragen.

Die vorliegende Studie hat jedoch gezeigt, dass diese Art von technischem Datenschutz nicht ausreicht. Vielmehr sollten drei größere Handlungsfelder vorangestellt werden, damit sich ein Ausgleich zwischen Sicherheitsinteressen und Grundrechten erreichen lässt. Erstens hat der Europäische Gerichtshof in einer Reihe von Grundsatzurteilen die anlasslose Datenspeicherung für Zwecke der inneren Sicherheit zurückgewiesen. Das zuletzt betroffene Abkommen zur Übermittlung von Fluggastdaten (PNR) an Kanada ist dringend neu zu verhandeln, auch mit Blick auf bereits bestehende PNR-Abkommen mit den Vereinigten Staaten und Australien. Währenddessen sollten die EU-Mitgliedstaaten die Schaffung eines europäischen PNR-Systems zurückstellen, bis eine präzisere Regelung zur Verhältnismäßigkeit dieser Art von Datenverarbeitung ausgearbeitet werden kann.

Eine weitere unmittelbare Herausforderung für die Mitgliedstaaten besteht darin, das gesamte EU-Datenschutzrecht zu novellieren. Gerade weil die wegweisende Datenschutz-Grundverordnung schon bis Mai 2018 umzusetzen ist, darf die parallel verabschiedete Datenschutzrichtlinie für Strafverfolgungsbehörden nicht aus den Augen verloren werden. Beide Rechtsakte müssen Hand in Hand greifen, weil die allgemeine Grenz- und Migrationskontrolle der Datenschutz-Grundverordnung zugerechnet wird, während alle anderen polizeilichen Aufgaben unter die Datenschutzrichtlinie fallen. In Zukunft soll die Interoperabilität eine flexiblere und grenzüberschreitende Abfrage aller EU-Datenbanken für die Migrationskontrolle und die Strafverfolgung ermöglichen. Deshalb sollten die nationalen Bestimmungen zur Anwendung der Datenschutzrichtlinie möglichst einheitlich ausfallen. Zugleich könnte die Neufassung der Datenschutzverordnung für EU-Organe mehr Kohärenz bringen und den gesamten Politikbereich des RFSR mit seinen Agenturen einbeziehen.

Schließlich ist darauf zu achten, dass alle rechtlichen und politischen Aufsichtsmechanismen mit der Entwicklung von intelligenten Grenzen und Interoperabilität Schritt halten. Wenn Biometrie stärker genutzt wird und internationale Fahndungsersuchen sich leichter abfragen lassen, kann dies für Einzelpersonen mit dem Risiko verbunden sein, dass fehlerhafte Dateneinträge schwerer zu entkräften sind oder unverhältnismäßige polizeiliche Maßnahmen erfolgen. Auch für die elektronische Einreiseerlaubnis ETIAS sollte ein effektiver Rechtsweg garantiert werden, da eine hohe Zahl an Reisenden von neuartigen europäischen Verfahren zur Risikobewertung betroffen sein wird. Zu beachten ist überdies, dass die einheitliche ETIAS-Warnliste für mutmaßliche Terroristen sowie Kriegs- und Schwerverbrecher auf nachrichtendienstlichen Informationen basieren wird. Nationale Abgeordnete sollten die interparlamentarische Versammlung zur Kontrolle von Europol nutzen, um diesen besonders sensiblen Aspekt künftiger intelligenter Grenzen der EU im Blick zu behalten.

Abkürzungen

ABC Gates	Automated Border Control Gates
AEUV	Vertrag über die Arbeitsweise der Europäischen Union
CEPS	Centre for European Policy Studies (Brüssel)
CTG	Counter Terrorism Group
ECRIS	European Criminal Records Information System
ECRIS-TCN	European Criminal Records Information System — Third Country Nationals
EES	Entry-Exit System
ESTA	Electronic System for Travel Authorization (USA)
ETIAS	European Travel Information and Authorisation System
EU	Europäische Union
EuGH	Europäischer Gerichtshof
eu-LISA	European Agency for the operational management of large-scale IT systems in the Area of Freedom, Security and Justice
EURODAC	European Dactyloscopy (Datenbank)
Europol	European Police Office
EUV	Vertrag über die Europäische Union
FBI	Federal Bureau of Investigation
Frontex	Europäische Agentur für die Grenz- und Küstenwache
ICE	United States Immigration and Customs Enforcement
Interpol	International Criminal Police Organization
IS	Islamischer Staat
PNR	Passenger Name Record (erweiterte Fluggastdaten)
RFSR	Raum der Freiheit, der Sicherheit und des Rechts
SIRENE	Supplementary Information Request at the National Entries
SIS	Schengener Informationssystem
VIS	Visa-Informationssystem