Bürgerrechte & Polizei

Cilip 131
März 2023

Mit Technologien gegen Migration

Virtual Reality-Trainings bei der Polizei
Landesversammlungsgesetz Hessen
Der „Fall Maninger"

Impressum

Bürgerrechte & Polizei/CILIP

Herausgeber und Verlag: Institut für Bürgerrechte & öffentliche Sicherheit e.V. , c/o Juristische Fakultät, Humboldt-Universität zu Berlin, Unter den Linden 6, 10099 Berlin
Druck: trigger.medien.gmbh, Berlin
V.i.S.d.P.: Norbert Pütter

Redaktion, Gestaltung + Satz: Dirk Burczyk, Benjamin Derin, Tom Jennissen, Sonja John, Marius Kühne, Jenny Künkel, Christian Meyer, Matthias Monroy, Marie-Theres Piening, Norbert Pütter, Stephanie Schmidt, Christian Schröder, Eric Töpfer, Friederike Wegner, Louisa Zech
Übersetzungen: Benjamin Derin, Sonja John, Marie-Theres Piening, Eric Töpfer

Titelbild: Ferngesteuertes Videoüberwachungssystem in Nogales, Arizona (Electronic Frontier Foundation, CC BY 3.0)

Zitiervorschlag: Bürgerrechte & Polizei/CILIP 131 (März 2023)
ISSN 0932-5409

Redaktion & Vertrieb: CILIP c/o Juristische Fakultät · Humboldt-Universität zu Berlin · Unter den Linden 6 · 10099 Berlin · www.cilip.de
info@cilip.de (Redaktion) · vertrieb@cilip.de (Vertrieb)

Bankverbindung: Institut für Bürgerrechte & öffentliche Sicherheit e.V.
Bank für Sozialwirtschaft
bis 23. April 2023:
IBAN DE18 1002 0500 0003 0564 00 · SWIFT- / BIC-Code: BFSWDE33BER
ab 24. April 2023:
IBAN DE22 3702 0500 0003 0564 00 · SWIFT- / BIC-Code: BFSWDE33XXX

Preise:
Personen: Einzelpreis: 10,– Euro · Jahresabo (3 Hefte): 25,– Euro
Institutionen: Einzelpreis: 15,– Euro · Jahresabo: 45,– Euro
Jahresabo zum Soli-Preis: 30,– Euro · Großer Soli-Preis: 50,– Euro
Alle Preise inkl. Porto im Inland · Auslandsporto pro Heft: 3,70 Euro
Neu abgeschlossene Abonnements sind mit Frist von vier Wochen kündbar.

Inhalt

Schwerpunkt: Mit Technologien gegen Migration

3 **Sensoren und Daten der Festung Europa**
Dirk Burczyk, Christian Meyer, Matthias Monroy, Stephanie Schmidt

17 **Technologische Gewalt an den Grenzen der EU und USA**
Petra Molnar

27 **Migrationsabwehr als angewandte Wissenschaft**
Norbert Pütter

37 **KI-Technologien für die EU-Grenzkontrolle**
Lise Endregard Hemat

47 **Polizeiliche Detektion von Menschen in Fahrzeugen**
Clemens Arzt

56 **Warnungen aus Großbritannien**
Lucie Audibert

67 **Blick auf die Grenze mit Gegenforensik**
Giovanna Reder

Außerhalb des Schwerpunkts

76 **Virtual Reality-Trainings bei Polizeibehörden**
León von der Burg, Johannes Ebenau, Jasper Janssen

88 **Landesversammlungsgesetz Hessen**
Marius Kühne

96 **Der „Fall Maninger"**
Anna M. Fauda

104 **Inland aktuell**

108 **Meldungen aus Europa**

112 **Literatur**

123 **Mitarbeiter*innen dieser Ausgabe**

Redaktionsmitteilung

Um 1860 begann der britische Kolonialbeamte William James Herschel in Bengalen Fingerabdrücke zu nutzen, um Betrug bei der Auszahlung von Ruhegehältern an pensionierte Sepoys, die subalternen indischen Soldaten, zu verhindern. Damit legte er das Fundament für die Biometrie, die sich heute zur Schlüsseltechnologie entwickelt hat für die Kontrolle von grenzüberschreitender Mobilität und Migration, aber in wachsendem Maße auch der einheimischen Bevölkerung. Als „kolonialen Bumerang" beschrieb Michel Foucault das Phänomen, dass Praktiken und Technologien, die in den Kolonien zur Durchsetzung und Sicherung imperialer Herrschaft entwickelt wurden, früher oder später auch in ihrem Mutterland zum Einsatz kommen.

Bis heute sind die rassifizierten „Fremden" das primäre Testfeld für neue Kontrolltechnologien. Ihre Körper und – neuerdings auch – ihre digitalen Schatten werden erfasst, gezählt und vermessen, um staatlichen Zugriff zu ermöglich. Myriaden von Sensoren säumen inzwischen die Wege, die Menschen nehmen bei ihren mehr oder weniger erfolgreichen Versuchen, die Schleusen und Mauern dieser Welt zu überwinden. Immer neue, ausgefeiltere Technologien kommen dabei zum Einsatz, immer undurchschaubarer wird die Verarbeitung der Unmengen gesammelter Informationen. Die Rechte der überwachten Menschen werden dabei regelmäßig mit Füßen getreten – allzu häufig mit tödlichen Konsequenzen. Zugleich wird ein sicherheits-industrieller Apparat mit Milliarden gefüttert und die Flugbahn des Bumerangs kürzer. Das aktuelle Heft wirft einen Blick auf diese Technologien zur Migrationskontrolle, auf ihre Entwicklung, ihre Kosten und Folgen.

***

Anfangs erschien unsere Zeitschrift auch auf Englisch, später nur noch auf Deutsch. Trotzdem hatten wir stets auch englische Zusammenfassungen aller Artikel im Heft abgedruckt. Diese Summaries finden sich fortan nur noch online.

Unsere nächste Ausgabe widmet sich der Rolle der ach so unpolitischen Polizei als politischem Akteur.
(Eric Töpfer)

Mit Technologien gegen Migration

Die Sensoren und Daten der Festung Europa

von Dirk Burczyk, Christian Meyer, Matthias Monroy und Stephanie Schmidt

Um die unkontrollierte Migration aufzuspüren und zu verhindern, setzt die Europäische Union (EU) zunehmend Hochtechnologien ein. Diese lassen sich in sensor- und datenbasierte Anwendungen unterscheiden. Mit der Technologisierung der europäischen Außengrenzen gehen kommerzielle Interessen der Anbieter einher. Es gibt aber auch Ansätze von Nichtregierungsorganisationen, die verwendeten Beobachtungstechnologien im Sinne einer Sousveillance einzusetzen.

Weil man sich seit Jahren nicht auf Verteilungsquoten einigen kann, haben die 27 Regierungen beim EU-Migrationsgipfel Anfang Februar 2023 lieber andere Gemeinsamkeiten betont.[1] Ziele der Union seien demnach gestärkte Außengrenzen und Maßnahmen gegen irreguläre Migration. In den vergangenen Jahren setzt die EU dabei auch zunehmend auf Technologien zur Überwachung und Kontrolle flüchtender Menschen an ihren Außengrenzen. Konzentrierte sich dies bis zum Ende des Kalten Kriegs noch vor allem auf den Schutz des Territoriums, rückte seither der Umgang mit sowie die Verhinderung von Migration in den Fokus grenzpolitischer Interessen.[2] Aufgrund der Befürchtungen, dass sich nach dem Kalten Krieg vor allem Migrationsbewegungen als Auslöser für Krisen zeigen könnten, wurde ein Bedarf an umfassenden Regeln und Normen behauptet, die in dem 1993 (auf Bitte der UN-Kommission für Global Gover-

1 Ratsdok. EUCO 1/23 v. 9.2.2023

2 Schwertl, M.: Die Entmenschlichung der Grenze. Zur Bedeutung von Technisierung im EUropäischen Migrations- und Grenzregime. In: movements. Journal for Critical Migration and Border Regime Studies 2018, H. 2, S. 77-100

nance und der Regierung Schwedens) von Bimal Gosh entwickelten Konzept des „Migrationsmanagement" mündeten.[3] Neben den bekannten staatlichen Akteur*innen, wie die EU-Grenzagentur Frontex und ihren Entwicklungen von Grenztechnologien (wie bspw. das seit 2014 aktive Überwachungssystem EUROSUR), zeigen sich auch Industrie und zivile Forschungseinrichtungen im Bereich der Europäischen Migrations- und Grenzpolitik aktiv. So wurden etwa Drohnen, ursprünglich genutzt für die Schifffahrtskontrolle und im Kontext von Umweltüberwachung, letztlich auch im Bereich des Grenzschutzes und zur Überwachung von Migrationsbewegungen eingesetzt.[4]

Dass neue und auch zivile Technologien zur Überwachung schnell gegenüber Migrant*innen und Geflüchteten ihre Anwendung finden, ist im Kontext der „Festung Europa" wenig überraschend. Denn durch die Markierung von Migration als Bedrohung erscheinen die Technologien der Abwehr und Beobachtung als legitim. Gleichzeitig verstärkt ihr tatsächlicher Einsatz im Feld der Migrationskontrolle genau diese Markierung. Dieser Einsatz erfolgt so in der Regel ohne größeres Aufsehen oder wird meist erst dann zum Politikum, wenn auch Staatsangehörige des eigenen Landes betroffen sind.

Entlang des Berichts des Bundestagsausschusses für Bildung, Forschung und Technikfolgenabschätzung „Beobachtungstechnologien im Bereich der zivilen Sicherheit – Möglichkeiten und Herausforderungen" lassen sich die gegenwärtigen Entwicklungen ziviler Beobachtungstechnologien in ihrer Anwendung im Kontext des EUropäischen Grenzregimes systematisieren. Die Verfasser*innen unternehmen darin den Versuch eines Überblicks zu Technologien, die heute im Bereich der zivilen Sicherheit als Mittel für soziale Kontrolle genutzt werden können oder deren Anwendung in naher Zukunft wahrscheinlich ist. Der dort verwendete Begriff der „Beobachtungstechnologien" umfasst unterschiedliche Praktiken, die „das menschliche Wahrnehmungs- und Beurteilungsvermögen für Risiken, Gefahren oder Schäden in vielfältiger Weise" erweitern.[5]

3 Geiger, M; Pécoud, A.: The Politics of International Migration Management, in: Dies. (Hg.): The Politics of International Migration Management, New York 2010, S. 1-20

4 Schwertl a.a.O. (Fn. 2)

5 BT-Drs. 20/4200 v. 27.10.2022, S. 35

Die Studie unterteilt die technischen Lösungen und Einsatzformen in sensorbasierte und datenbasierte Anwendungen. Sensorbasierte Beobachtungstechnologien erfassen demnach „bestimmte physikalische oder chemische Eigenschaften der realen Welt und bereiten die Messgrößen in für den Menschen leicht interpretierbare Informationen auf". Datenbasierte Beobachtungstechnologien „erfassen und analysieren Informationen der digitalen Welt".[6] Sowohl durch ihre bereits erfolgte Verbreitung und Nutzung, als auch aufgrund des Entwicklungspotenzials für neue und erweiterte Anwendungen erfahren diese Technologien eine immer stärkere Bedeutung, heißt es im Vorwort. Davon profitierten etwa die Verkehrsüberwachung, der Brand- und Katastrophenschutz, der Rettungsdienst wie auch die Polizei im Kontext von Gefahrenabwehr und Strafverfolgung sowie die Geheimdienste. Zugleich werden viele der beschriebenen Beobachtungstechnologien auch zur Überwachung, Kontrolle und Verhinderung von Migration genutzt, etwa an regulären Grenzübergängen oder unkontrollierten Grenzabschnitten. Das Verständnis irregulärer Migration als „Gefahr" und das politische Ziel der Migrationsabwehr gehen dem Einsatz dieser Beobachtungstechnologien voraus und sind Gegenstand unserer Kritik.

Sensorbasierte Beobachtungstechnologien

Zu den am weitesten verbreiteten bodengestützten Sensortechnologien gehört die Videotechnik im öffentlich zugänglichen Raum. An internationalen Flughäfen und Bahnhöfen, wie auch an sogenannten Hotspots oder in Lagern für geflüchtete Menschen gehören sie beispielsweise in Griechenland zur Grundausstattung.[7] Die Kameras können mithilfe von Software und vernetzten Technologien über Echtzeit-Funktionen zur Muster- oder Gesichtserkennung verfügen, wenngleich der Einsatz dieser Funktionen in Deutschland bislang nur in zeitlich begrenzten Pilotprojekten erfolgt. Im Projekt SMILE hat Frontex jedoch bereits an Verfahren zur Objektklassifizierung in Foto- oder Videodaten geforscht. Nach Einführung des Einreise-/Ausreisesystems (EES) ab 2023 könnten damit die länger dauernden Kontrollprozeduren wieder verkürzt werden.[8] Im Projekt

6 ebd., S. 14
7 Panopticon für Geflüchtete, netzpolitik.org v. 30.9.2021
8 Frontex beendet Pilotprojekt zur Gesichtserkennung an EU-Außengrenzen, netzpolitik.org v. 9.11.2021

konnten die Reisenden über eine SMILE-App Reisepassdaten, Fingerabdrücke und ein Gesichtsfoto importieren. Das System glich die Daten dann mit nationalen und EU-Datenbanken zur Grenzkontrolle ab. Erfolgte der Übertritt mit dem Auto, konnte die Fahrer*innen im Fahrzeug bleiben und ihre Reisedokumente in ein Lesegerät einführen. Eine Kamera erfasste automatisiert das Nummernschild des Fahrzeugs, eine weitere Kamera erledigte die Gesichtserkennung. Stimmten die Angaben mit den vorregistrierten Daten überein, öffnete sich die Grenze. Das System soll auch bei Busreisenden funktionieren.

Retrograd, also nicht in Echtzeit, wird die Gesichtserkennung auf EU-Ebene bereits im Visa-Informationssystem zur Verifikation von Visaantragssteller*innen genutzt. Noch 2023 sollen diese und andere biometrische Datenbanken zusammen mit Gesichtsbildern aus dem neuen EES in einem „gemeinsamen Identitätsspeicher" mit einem „Abgleichsystem" zentralisiert gespeichert und durchsuchbar werden. Auch „Mehrfachidentitäten" sollen so automatisiert detektiert werden können. Allein das hierfür nötige System zur Gesichtserkennung kostet über 300 Mio. Euro.[9] Darüber hinaus forscht unter anderem Frontex bereits seit über zehn Jahren im Bereich der Emotionsanalyse zur Erkennung von Täuschungen, wenngleich sich diese Systeme noch nicht im Einsatz befinden. Das Forschungsprojekt iBorderCtrl hat beispielsweise untersucht, inwiefern eine solche Technik im Europäischen Reiseinformations- und -genehmigungssystems (ETIAS), das noch 2023 in Kraft treten soll, eingesetzt werden könnte. Bereits seit 2009 hat Frontex Forschungen der Universität Arizona finanziert, in denen die Treffergenauigkeit eines „Automatic Deception Detection Systems" (ADDS) ausgewertet wurde.[10] Die Funktionsweise der Technik beschreibt Lise Endregard Hemat in diesem Heft.

Zu den sensorbasierten Beobachtungstechnologien gehören auch Körperscanner für die Personenkontrolle, wie sie immer mehr an Flughäfen eingesetzt werden und dort die vorhandenen Metalldetektorschleusen ersetzen. Mit solchen Millimeterwellenscannern können auch Fahrzeuge in Gänze durchleuchtet werden. Wie Detektionstechnologien mithilfe von Infrarot-, Radar- und Röntgenstrahlung sowie dem Einsatz von CO_2-und Herzschlagdetektoren versteckte Personen aufspüren sollen, problematisiert der Beitrag von Clemens Arzt in dieser Ausgabe.

---

9 Milliarden für Europas Biometrie-Giganten, netzpolitik.org v. 11.9.2021

10 Antwort der EU-Kommission auf die Anfrage E-002653/2019, Europäisches Parlament v. 24.2.2020

Am Boden eingesetzte Tageslicht- und Wärmebildkameras können auch an Flugzeugen, Hubschraubern und Drohnen angebracht werden. Zur Lageaufklärung dienen sie dabei der Beobachtung von Grenzabschnitten oder zur Verfolgung von Personen, die mutmaßlich irregulär die Grenze überschreiten wollen. Frontex hat hierzu ab 2016 einen eigenen Flugdienst aufgebaut, der auf Anfrage einzelner Staaten an den Außengrenzen des Schengen-Raums patrouilliert. Die EU-Kommission finanziert zudem ein Forschungsprojekt zur Überwachung aus der Stratosphäre mithilfe zeppelinartiger Ballons oder Solarseglern, die ebenfalls mit bildgebenden Sensoren ausgestattet sind.[11]

Frontex greift – ebenso wie wohl die meisten nationalen Grenzbehörden – auf weltraumgestützte Beobachtungstechnologien zu und hat hierzu ab 2014 das bereits erwähnte Überwachungssystem EUROSUR in Betrieb genommen. Es basiert auf verschiedenen Satellitendiensten, darunter zur Erkennung auffälliger Muster etwa von kleinen Booten an Seeaußengrenzen der EU. Dabei kann es sich um optische Aufnahmen passiver Systeme ohne künstliche Beleuchtung der Erdoberfläche oder aktive Systeme mit elektromagnetischen Wellen handeln (Synthetic Aperture Radar). Sie stammen aus dem europäischen Erdbeobachtungsprogramm „Copernicus" oder von privaten Betreibern von Satellitendiensten.

Ebenfalls zu den sensorbasierten Beobachtungstechnologien zählt die akustische Beobachtung mithilfe von Mikrofonen. Im Bereich der Grenzüberwachung wurden derartige Systeme etwa im EU-Projekt FOLDOUT erprobt. Sie gehörten dort zu einer Kaskade verschiedener Überwachungstechnologien am Boden und in der Luft, die Norbert Pütter in diesem Heft darstellt. Zudem können offen oder verdeckt eingesetzte Ortungstechnologien wie GPS-Empfänger zur Bestimmung des Aufenthaltsorts von Personen genutzt werden. Wie elektronische Fußfesseln bzw. mit Apps zur Geolokalisierung ausgestattete Smartwatches in Großbritannien zur Aufenthaltsüberwachung von abzuschiebenden Personen eingesetzt werden, erklärt der Beitrag von Lucie Audibert in diesem Heft.

11 Frontex installiert Kameras in der Stratosphäre, golem.de v. 27.9.2022

Informationstechnische Beobachtung

Zur Aufdeckung irregulärer Migration beobachten die zuständigen Behörden auch das Internet, etwa um die Entwicklung von Grenzübertritten zu beobachten, aber auch die Unterstützung diese zu verhindern und zu verfolgen. Die EU-Polizeiagentur Europol hat hierfür – eigentlich zur Bekämpfung des islamistisch motivierten Terrorismus – 2014 eine Meldestelle für Internetinhalte eingerichtet, deren Aufgabenbereich ein Jahr später nach einer Ratserklärung um „Internetinhalte, mit denen Schlepper Migranten und Flüchtlinge anlocken", erweitert wurde.[12] Allein für Inhalte, die „für Schleuserdienste von Belarus nach Europa werben" hat die Meldestelle 2021 insgesamt 455 Accounts in Sozialen Medien ausgemacht und zur Entfernung an die Internetdienstleister gemeldet.[13] Noch weiter geht das britische Innenministerium, das Anbieter von Sozialen Medien auffordern will, Beiträge zu entfernen, wenn diese das Übersetzen über den Ärmelkanal in kleinen Booten „verherrlichen". Facebook, Instagram und Twitter sollen auf Geheiß des Ministeriums „völlig inakzeptable Clips" löschen, wenn diese „tödliche Überfahrten" fördern.[14]

Zur Bewältigung und Interpretation der großen Datenmengen kommen bei Europol auch Techniken der „Social Media Intelligence" (SOCMINT) zum Einsatz. Europol sucht dabei „nach gängigen, frei verfügbaren Informationen in sozialen Medien, z. B. Facebook, Twitter und Instagram hinsichtlich einer möglicher Ermittlungsrelevanz".[15] Auf diese Weise verfolgen einzelne Mitgliedstaaten und Europol unter anderem die Fluchthilfe über den Ärmelkanal nach Großbritannien. Dabei suchen die Behörden im Internet nach verdächtigen Angeboten für den Verkauf von Schlauchbooten oder Rettungswesten.[16]

Neben der Beobachtung offener Quellen sind Migrant*innen und Asylsuchende auch von Eingriffen in ihre digitale Privatsphäre betroffen. Der Bericht für Technikfolgenabschätzung spricht dabei von der Überwachung von Daten, „die eine Person in der berechtigten Erwartung, dass

12 Europäischer Rat: Außerordentliche Tagung des Europäischen Rates vom 23. April 2015 – Erklärung, Pressemitteilung v. 23. 4.2015

13 Europol coordinates referral action targeting migrant smuggling from Belarus, Europol Pressemitteilung v. 20.12.2021

14 A ban on „positive" videos won't stop the Channel crossings, but it may well cause more tragedies, www.theguardian.com v. 19.1.2023

15 BT-Drs. 19/16505 v. 15.1.2020

16 EU-Polizeien wollen versteckte Kameras an Stränden installieren, netzpolitik.org v. 26.11.2021

sie vertraulich bleiben, einem informationstechnischen System anvertraut hat".[17] So liest etwa das Bundesamt für Migration und Flüchtlinge (BAMF) die Mobiltelefone von vielen Asylsuchenden aus. Die Maßnahme soll die Feststellung von Identität und Staatsangehörigkeit ermöglichen, wenn die Antragsteller*innen keinen gültigen Pass oder Passersatz vorweisen können. Die Behörden prüfen die Plausibilität der Angaben, indem sie beispielsweise kontrollieren, ob im Adressbuch oder bei Anrufen und Nachrichten häufig Ländervorwahlen vorkommen, die dem genannten Heimatland entsprechen. Auch besuchte Webseiten werden nach derartigen Länderendungen durchsucht. Zudem extrahieren BAMF und Ausländerbehörden aus Fotos und Anwendung Daten, in denen der jeweilige Aufenthaltsort gespeichert ist. Wird die Mitwirkung bei der Maßnahme verweigert, können entweder Leistungen gekürzt oder sogar ein Asylantrag als „offensichtlich unbegründet" abgelehnt werden. In den ersten Monaten des Jahres 2022 hat das BAMF über 16.000 Datenträger auf diese Weise ausgelesen, davon hauptsächlich von Menschen aus Afghanistan, Syrien und dem Irak.[18] Weniger als ein Fünftel der Geräte wurde anschließend auch analysiert, bei rund 4 Prozent der Betroffenen wurde die Identität angeblich widerlegt. In rund zwei Dritteln der Fälle brachte die Handyauswertung keine verwertbaren Erkenntnisse. Unter anderem wegen der fehlenden Verhältnismäßigkeit hat das Bundesverwaltungsgericht die Praxis deshalb im Februar für rechtswidrig erklärt.[19] Auch Frontex und Europol geben in einem Bericht zur „Digitalisierung des Menschenschmuggels" Handreichungen über die von Geflüchteten am häufigsten genutzten Messenger sowie Informationen darüber, wie die Behörden Zugang zu den dort gespeicherten Inhalten erhalten.[20]

Auch die Ortung von Telefonen wird von Grenzbehörden bereits genutzt. Im EU-Forschungsprojekt FOLDOUT haben die Beteiligten etwa ermittelt, ob sich Handys in einer bestimmten Region in Funkmasten einbuchen und ob sich daraus Hinweise auf einen irregulären Grenzübertritt in der Nähe ergeben können. Das von den Menschen mitgeführte Telefon dient dabei als Ortungssender. Nach Angaben von Airbus ist auch die Drohne „Heron 1", die der Rüstungskonzern im Auftrag von Frontex

17 BT-Drs. 20/4200 v. 27.10.2022, S. 22
18 BT-Drs. 20/4019 v. 12.10.2022, 2. 28
19 vgl. die Meldung in diesem Heft auf S. 90
20 EU: Joint Europol-Frontex report on „digitalisation of migrant smuggling", Statewatch v. 25.10.2021

fliegt, mit Technik zur Ortung von Mobil- und Satellitentelefonen ausgerüstet – Frontex selbst hat dies in Anfragen bislang bestritten.[21] Laut Airbus trägt die Drohne im zentralen Mittelmeer aber sogenannte COMINT-Sensoren an Bord.[22] Die Abkürzung stammt aus dem Militär und steht für „Communication Intelligence", gemeint ist die Erfassung oder Auswertung von Telefonverbindungen zur Informationsgewinnung. Gegenüber den ebenfalls mitgeführten Tages- und Nachtsichtkameras und Radargeräten hat die Technik den Vorteil, dass eine Ortung auch nachts oder bei schlechtem Wetter möglich ist. Die Ergebnisse der Drohnenaufklärung werden per Satellit in Echtzeit ins Frontex- Hauptquartier in Warschau gestreamt.

Mobil- und Satellitentelefone können auch aus dem Weltraum geolokalisiert werden. Neue miniaturisierte Satelliten und Elon Musks Raumfahrtunternehmen SpaceX haben diese Spionagetechnologie auch für Grenzbehörden erschwinglich gemacht. Anbieter dieser Technik sind Firmen, die ansonsten Militär und Geheimdienste beliefern. Frontex vergibt Verträge über mehrere Millionen Euro für diese neue Technik.[23] Auch Boote mit Geflüchteten könnten auf diese Weise geortet werden, sofern die Menschen an Bord Satellitentelefone mitführen.

Predictive Border Policing

Wenn das Ziel Prävention ist,[24] man irregulärer Migration also zuvorkommen will, dann kann die Informationslage nicht gut genug sein. Unter digitalen Vorzeichen bedeutet das, dass der staatliche Hunger nach Daten nicht stillbar ist. Zur vorausschauenden Migrationskontrolle können Behörden außerdem anonymisierte Daten von Mobiltelefonen nutzen, die von den Netzbetreibern zur Verfügung gestellt werden. Die Geräte hin-

21 s. Demirel, O.: Tweet v. 30.4.2022, https://twitter.com/OezlemADemirel/status/1516731668689833987

22 European Maritime Safety Agency: RPAS for Maritime Surveillance, Lissabon 2022, https://fragdenstaat.de/files/foi/690128/ATDpart130.03.2022.pdf.pdf?download, S. 19

23 Spionagesatelliten im Frontex-Einsatz, netzpolitik.org v. 27.6.2022

24 Das BAMF spricht seit Jahren explizit von einer „Politik der Prävention illegaler Migration im Zusammenspiel mit anderen EU-Staaten", vgl. BAMF: Maßnahmen zur Verhinderung und Reduzierung irregulärer Migration. Studie der deutschen nationalen Kontaktstelle für das Europäische Migrationsnetzwerk (EMN), Working Paper 41, Nürnberg 2012.

terlassen digitale Spuren, die sich für die Handhabung von Naturkatastrophen, Konflikten, Krankheiten oder Volkszählungen nutzen lassen.[25] Wohl überall auf der Welt erfassen Anbieter routinemäßig, wenn ein Anruf über ihr Netz erfolgt oder eine SMS gesendet wird. Diese Verkehrsdaten enthalten den Ort des Funkmasts und einen Zeitstempel. Noch mehr Datensätze entstehen durch die Internetnutzung von Smartphones, die auch ohne aktives Zutun permanent im Hintergrund erfolgt. Behörden oder Forschende können keine Personen dahinter ermitteln, aber die Wege der Telefone nachvollziehen und daraus Prognosen erstellen. Werden Daten verschiedener Mobilfunknetzbetreiber verwendet, kann damit Migration auch über Nachbarländer hinweg verfolgt werden. Ähnliche Angaben erfasst Google mit seiner „Standort-Historie", wenn Nutzer*innen des Android-Betriebssystems in ihren Einstellungen die Aufzeichnung von geografischen GPS-Koordinaten oder WLAN-Netzen erlauben. Diese Informationen können durch weitere Datenquellen angereichert werden, darunter etwa Geldüberweisungen, die ebenfalls häufig über Mobiltelefone erfolgen. Das Gleiche gilt für Geodaten, die bei jeder Anmeldung beim eigenen E-Mail-Dienst oder Sozialen Medien gespeichert werden.

Mithilfe von Daten verschiedener Quellen will auch die EU-Kommission über ein sogenanntes EUMigraTool „Migrationsströme" in Europa vorhersagen und steuern.[26] Die Modellierung und Vorhersage soll unter Verwendung von „Deep Learning" erfolgen. Das Projekt ITFLOWS, in dem das Tool entwickelt wird, will in erster Linie eine Lösung erarbeiten, die eine „verlässliche Vorhersage von Migranten" in ganz Europa ermöglicht. Bislang gebe es diese Ansätze lediglich länderbezogen, etwa für das Vereinigte Königreich und Schweden. Dort würden unterschiedliche Datenquellen und Zeitrahmen für die Vorhersage genutzt. Einige der Frühwarnmodelle könnten zudem vorhersagen, „welche Länder das Potenzial haben, Flüchtlingsströme auszulösen". Hierzu können etwa politische Ereignisdatenbanken herangezogen werden, wie sie in Deutschland die Bundeswehr und das Auswärtigen Amt nutzen.[27] In seinem ersten Stadium soll das EUMigraTool offiziellen Angaben zufolge zwar nicht der Abwehr irregulärer Migration dienen, sondern deren Aufnahme, Um- und Ansiedlung unterstützen. Später plant ITFLOWS das Instrument zu nutzen, um

25 vgl. International Organization for Migration: Big data and migration, Data Bulletin. Informing a Global Compact for Migration - Nr. 5, Februar 2018

26 Mit „Künstlicher Intelligenz" gegen Migration, netzpolitik.org v. 5.10.2022

27 Blick in die Glaskugel: Bundeswehr will politische Ereignisse vorhersehen, netzpolitik.org v. 7.6.2018

„potenzielle Risiken für Spannungen zwischen Eingewanderten und EU-Bürgerinnen und -Bürgern zu erkennen“[28]. Schließlich will das Projekt Empfehlungen für politisch Verantwortliche, Regierungen und die Unionsorgane aussprechen.

Mit Sousveillance gegen die Überwacher?[29]

Zur Technologisierung von Migrationsbewegungen gehört auch ein Blick auf die technische Ermächtigung von flüchtenden Menschen, Aktivist*innen sowie zivilen Akteur*innen beispielsweise im Bereich der Seenotrettung. Die zunehmende freie Verfügbarkeit von Daten ermöglicht es beispielsweise, diese Daten zur Kontrolle von Behörden zu nutzen. Satellitenbilder und Positionsdaten von Schiffen können etwa zur nachträglichen Aufklärung von Menschenrechtsverletzungen im Mittelmeer und der Verfolgung von Verantwortlichen beitragen (siehe hierzu den Beitrag von Giovanna Reder in diesem Heft). Hochaufgelöste Bilder aus der Erdbeobachtung könnten außerdem bei der nichtstaatlichen Seenotrettung im Mittelmeer helfen. So experimentiert etwa der deutsche Verein Space-Eye mit der Nutzung von Satellitendaten.[30] Die rund ein Dutzend Wissenschaftler*innen und Studierenden nutzen dafür Bilder aus den Sentinel-Satelliten des EU-Erdbeobachtungsprogramms Copernicus der Europäischen Weltraumorganisation. Diese EU-Satellitendienste generieren Bilder mit geringer Auflösung und kurzer zeitlicher Abdeckung. Für eine effektive Beobachtung müsste der Verein daher weitere, teure Bilder von Satellitendiensten kaufen. Auch deshalb befindet sich das Projekt derzeit in einem wissenschaftlichen Stadium, dazu arbeitet Space-Eye mit verschiedenen Universitäten und Hochschulen zusammen.

Einen anderen Ansatz mit eigenem Überwachungsgerät verfolgt der Verein Searchwing, der mit der Hochschule Augsburg eine günstige, wasserdichte Drohne entwickelt hat.[31] Sie kann von einem Schiff aus der Hand gestartet werden, in einem bis zu zweistündigen Einsatz fliegt der Starrflügler bis zu 120 Kilometer weit. Die Technik wurde bereits mehrfach auf zivilen Rettungsschiffen im Mittelmeer getestet. Die Fähigkeiten sind jedoch durch die Nutzlast begrenzt, die bislang nur eine Zuladung von

28 https://cordis.europa.eu/project/id/882986/de

29 Sousveillance wird hier verstanden als „Überwachung von unten“, indem etwa staatliche Institutionen mit neuen Technologien beobachtet werden.

30 Satellitenüberwachung von unten, netzpolitik.org v. 11.1.2022

31 Drohnen für die nicht-staatliche Seenotrettung, netzpolitik.org v. 16.11.2021

Kameras mit einer Auflösung von 3280 x 2464 Pixel erlaubt. Eine Suche in der Nacht ist ebenfalls noch nicht möglich. Zudem muss die Drohne im Wasser landen und dort geborgen werden. Das größte Manko dürfte aber in der fehlenden Echtzeitübertragung bestehen.

Schließlich experimentieren Aktivist*innen auch mit der Nutzung von personenbezogenen Positionsdaten, um damit Menschenrechtsverletzungen zu verhindern oder zu dokumentieren. Die Unterstützungsplattform LeaveNoOneBehind programmiert dazu unter dem Namen „Claim Asylum EU" eine Web-App, die Menschen im Asylverfahren unterstützen soll.[32] Die Zielgruppe sind etwa Schutzsuchende in Griechenland oder Polen, die von den dortigen Grenzbehörden über die Grenze zurückgeschoben werden ohne dass sie einen Asylantrag stellen können. Mit der App sollen die Betroffenen sofort nach Erreichen eines EU-Mitgliedstaates auf elektronischem Weg einen Asylantrag stellen können und den Standort mit GPS-Daten protokollieren. Weil diese leicht zu verfälschen sind, können die Nutzer*innen Bilder von sich und der Umgebung aufnehmen, die mit Zeit- und Ortsstempel versehen in einer Cloud gespeichert werden können. Diese Bilder könnten im Nachhinein als Nachweis dienen, dass die Person tatsächlich europäischen Boden betreten hat. Mit der App verlören die Schutzsuchenden aber auch die Freiheit, undokumentiert in ein anderes Land weiterzureisen und erst dort ihren Asylantrag zu stellen. Denn gemäß der Dublin-Richtline ist jener Staat für die Bearbeitung des Antrags zuständig, über den die Einreise in das EU-Gebiet erfolgt ist.

Die Umkehr der neuen Beobachtungstechnologien, um diese gegen die europäische Migrationsabwehr in Stellung zu bringen, gelingt allenfalls in Ansätzen. Die neuen Formen der Sousveillance – oder besser: die neuen, hierfür verfügbaren Technologien – sind außerdem mit der Aufgabe von Datenschutz und Privatheit verbunden, wenn etwa bei der Nutzung einer App zum Stellen eines Asylantrags persönliche Fotos ins Internet geladen werden müssen. Diese Waffenungleichheit könnte sich allenfalls verändern, wenn die „Überwacher" ihre Daten teilen würden. Seenotrettungsorganisationen fordern seit Jahren von Frontex, die Aufnahmen ihrer Flugzeuge und Drohnen auch für deren Zwecke zur Verfügung zu stellen, das Gleiche könnte für Satellitendaten gelten, die Frontex von kommerziellen Anbietern kauft. Die Rettungsorganisationen beschreiben das Mittelmeer zu Recht als das wohl am besten überwachte Seegebiet

32 Eine App für das Recht auf Asyl, netzpolitik.org v. 17.10.2022

der Welt und fragen ebenfalls zu Recht, wieso dort also überhaupt noch Menschen ertrinken müssen.

Geschäftsfeld Migrationskontrolle

Anfang 2023 hat die Kommissionspräsidentin Ursula von der Leyen in einer Rede vor dem Europäischen Parlament die Bereitschaft zur technischen Migrationsabwehr bekräftigt. Die „dringendsten Probleme" gebe es demnach an der Landgrenze zwischen Bulgarien und der Türkei. Dort könne die EU weitere „Infrastruktur und Ausrüstung bereitstellen, wie Drohnen, Radar und andere Mittel zur Überwachung".[33] Die Kommissionspräsidentin bezeichnete dies als „nachhaltige Lösungen im Bereich Asyl und Migration". Damit liegt von der Leyen auf einer Linie mit den Regierungen von acht EU-Staaten, die in einem offenen Brief mehr Geld aus Brüssel für „operative und technische Maßnahmen für eine wirksame Grenzkontrolle" gefordert hatten. Zu den Unterzeichnenden gehören Griechenland, Österreich, Malta und Dänemark. Die Überwachungstechnologien sind an der griechisch-türkischen Grenze, der kroatisch-bosnischen Grenze, der serbisch-ungarischen Grenze und der bulgarisch-türkischen Grenze aber längst vorhanden. Dazu gehören Drohnen, Kameras, Wärmebildsensoren, Nachtsichtgeräte, Sensoren zur Detektion von Mobiltelefonen, Ortungsgeräte und Überwachungstürme.

Irreguläre Migration, insbesondere Fluchtbewegungen, wird also vor allem unter Sicherheitsaspekten diskutiert. Es ist jedoch nicht die Migration selbst, die krisenhaft ist, vielmehr ist es das EUropäische Grenzregime, das in die Krise gerät, wenn es sich auf Fluchtbewegungen nicht vorbereitet sieht. Kommen weitere Faktoren wie bspw. eine unvorbereitete Logistik in den Aufnahmegesellschaften hinzu, können dies mitunter ganze Gesellschaften als Krise erleben. Egal ob innenpolitisch oder wenn es um Migration auf EU-Ebene geht, reagiert der neoliberale Staat auf Krisen schnell mit autoritären Mitteln, die er nicht zuletzt technisch umgesetzt sieht. Dann bestimmt sich der Diskurs durch Diskussionen über technisch Machbares und nicht über politisch Umkämpftes. Der Einsatz solcher Technologien hat nach Angaben des Border Violence Monitoring

33 Speech by President von der Leyen at the European Parliament Plenary on the preparation of the Special European Council meeting of February, in particular the need to develop sustainable solutions in the area of asylum and migration v. 1.2.2023, https://ec.europa.eu/commission/presscorner/detail/en/speech_23_526

Netzwerks bereits jetzt für rechtswidrige Zurückweisungen gesorgt. Dabei wurden seit 2017 36 Zeugenaussagen aufgezeichnet, in denen der Einsatz von Drohnen zur Ortung, Festnahme und illegalen Zurückschiebung von Migrant*innen und Asylsuchenden beschrieben wird. Davon sollen mehr als 1.000 Personen betroffen gewesen sein.[34]

Ausgehend von der Idee des Krisenhaften, das mit Migrationsbewegungen einhergeht, verbindet sich vor allem mit vorausschauenden und vorhersagenden Technologien, samt ihrer mathematischen wie physikalischen Verfahren, das Versprechen einer berechenbaren Kontrolle über menschliche Verhaltensweisen. In der Technologisierung von Grenzen und technischen Bearbeitung von Migrationsbewegungen zeigen sich zugleich „entmenschlichende Tendenzen", und zwar in doppelter Weise: „einmal im Sinne der Abwesenheit und Unsichtbarkeit von Menschen als Grenzkontrolleure und -passant*innen und dann auch im Sinne eines anti-humanitären Blicks".[35] Denn die hier vorgestellten Technologien eint, dass sie den menschlichen Körper in den Fokus ihrer technischen Beobachtung stellen. Beobachtungstechnologien rücken mit ihrer Fortentwicklung so näher an das Subjekt. Dies beginnt bei der höheren Auflösung von Kamerabildern und geht über die Einbeziehung von sozialen Beziehungen, Bewegungsprofilen und Biometrie bis zur Beurteilung individueller Risikopotentiale (Stichwort Gefährder). Gleichzeitig ist es beim aktuellen Stand der Technologie möglich, bei der Beobachtung auf Distanz zu gehen und den Blick auf größere Strukturen zu lenken – sei es der Schiffsverkehr oder auffällige Ansammlungen von Mobiltelefonen.

Dabei haben wir es hier mit einer Form des technologischen Solutionismus[36] zur Bearbeitung eines eigentlich globalen gesellschaftlichen Problems zu tun: Anstatt über globale Ungerechtigkeit, fehlende Entwicklungsperspektiven für Individuen und Gesellschaften aufgrund von ökonomischen Interessen sowie den daraufhin folgenden politischen bis militärischen Intervention des globalen Nordens zu sprechen, wird hier die (illegalisierte) Migration als *problemhaft* in den Fokus gestellt – und dieses

34 Border Violence Monitoring Network: Member States' Use of New Technologies in Enforced Disappearances, Leipzig 2023, www.borderviolence.eu/eu-member-states-use-of-new-technologies-in-enforced-disappearances

35 Schwertl a.a.O. (Fn. 2), S. 93

36 Der Begriff meint die Vorstellung, dass alle Probleme der Welt letztendlich durch technische Entwicklungen gelöst werden können, s. Morozov, E.: Smarte neue Welt: digitale Technik und die Freiheit des Menschen, München 2013

„Problem" dann unter hohem Einsatz von Ressourcen einer technologischen Lösung zugeführt.

Die technologische Bearbeitung von Migrationsbewegungen zeigt sich so als ein Geschäftsfeld für diverse kommerzielle Anbieter die ihrerseits Produkte (Sensortechnologie, Software, Künstliche Intelligenz) initiativ als Lösungen anpreisen. Die betreffenden Technologien sind letztendlich Produkte eines kommerziell orientierten Sektors und werden als solche vermarktet. Dadurch werden nicht nur ökonomische Logiken in der Bearbeitung von Migration verstärkt, sondern Grenzkontrollen zu einem Geschäftsfeld. Gestärkt von einem staatlich propagandierten Narrativ der Bedrohung und Gefahr durch so genannte „unkontrollierte Migrationsbewegungen", erschließt sich der Grenzschutzindustrie ein profitables Geschäftsfeld. Die technische Basis des EUropäischen Grenzregimes wird unter den Prämissen von abzuwehrender Gefahr und technologischer Lösbarkeit stetig differenziert, ausgebaut und gefestigt. Dabei wird auch versucht, das ungleiche Kräfteverhältnis zwischen Globalem Süden und Norden mittels Technologie festzuschreiben und zu objektivieren.

Der Diskurs um irreguläre Migrationsbewegungen als potenzielle Auslöser für Krisen und der damit verbundenen Sicht auf Migration als problemhaft prägt die Beobachtungstechnologien und deren Anwendung. Zugleich zeigt sich eine zunehmende Kommerzialisierung der sicherheitstechnologischen Bearbeitung von Grenzen, durch die sich auch die Ziele und Prioritäten der Programmierer und ihrer Auftraggeber in Hard- und Software stets präsent zeigen. Versuche, diese Technologien im Sinne von Sousveillance gerade zum Schutz von Menschen, ihres Lebens, ihrer Rechte und ihrer Würde zu nutzen, verweisen aber selbst auf dieser Ebene darauf, dass es sich letztlich um eine politische Auseinandersetzung handelt.

Digitale Festungen und Roboterhunde

Technologische Gewalt an den Grenzen der EU und USA

von Petra Molnar[1]

Legitimiert durch die Verbindung von Migration und Sicherheitsgefahren im Innern werden zur Abwehr unerwünschter Einwanderung weltweit fortgeschrittene Technologien eingesetzt. Am Beispiel der Vereinigten Staaten und der Europäischen Union (EU) zeigt sich, dass die technologische Aufrüstung der physischen Außengrenzen begleitet wird von der Vorverlagerung der Kontrollen in andere Länder. Dadurch werden autoritäre Regime unterstützt und Überwachungstechnologien exportiert, so dass die Ursachen für Flucht verschärft und zugleich Fluchtchancen und -bedingungen verschlechtert werden.

„Heute schlägt die EU ein neues Kapitel in der Migrationsfrage auf ... Diese Einrichtung spiegelt unsere Werte und unsere europäische Lebensweise wider", sagte Margaritis Schinas, Vizepräsident der EU-Kommission und Kommissar für die „Förderung der europäischen Lebensweise", bei der Eröffnung eines Hightech-Flüchtlingslagers auf Kos, seiner griechischen Heimatinsel. Meine Kolleg*innen und ich nahmen an der offiziellen Eröffnung teil und hörten diese Worte aus erster Hand. Die Prioritäten der EU sind klar, und ihre Sprache ist wohlüberlegt: „Die Flüchtlingsströme erheblich reduzieren", die Menschen „aus dem städtischen Leben fernhalten" und deutlich machen, dass „wir es uns selbst, unseren Kindern und den künftigen Generationen schuldig sind, unsere Inseln vor Überbelastung und bekannten Gefahren zu schützen".[2] Eingebettet in die sanften Hügel in der Nähe des Dorfes Pili, unweit eines Salzsees mit Fla-

1 Teile dieses Beitrags werden erscheinen in: Molnar, P.: Artificial Borders. New York 2024.
2 zit. n. Molnar, P.: Tweet v. 29.11.2021, online: https://twitter.com/_PMolnar/status/1465224748204498945

mingos, ist das neue Flüchtlingslager auf Kos umgeben von Stacheldrahtzäunen, Ein- und Ausgangsdrehkreuzen, Lautsprechern und Kameras. Ergänzt wird das Lager durch ein von der EU finanziertes Pilotprojekt namens ROBORDER, welches das Ziel verfolgt, ein „voll funktionsfähiges autonomes Grenzüberwachungssystem mit unbemannten mobilen Robotern" zur Kontrolle der Gewässer vor der türkischen Küste zu entwickeln.[3]

Vorbild für das Lager auf Kos ist der ausgedehnte Hightech-Komplex auf der Insel Samos, die ein beliebtes Ziel insbesondere für deutsche Tourist*innen ist und wo man im selben Meer schwimmen kann, in dem Flüchtende ertrinken. Samos war das erste von fünf neuen „Mehrzweck-Aufnahme- und Identifizierungszentren" (MPRICs), die es neben Kos noch auf den Inseln Lesbos, Chios und Leros gibt – alles sogenannte Hotspots, in denen seit Jahren Menschen aus Syrien, Afghanistan, der Demokratischen Republik Kongo und anderen Ländern ankommen. In all diesen Lagern werden Kameras mit Algorithmen zur Bewegungsanalyse eingesetzt, um das Verhalten der Insass*innen zu überwachen, was die EU rund 260 Millionen Euro kosten wird.[4]

Grenzen töten. Die ohnehin schon gewalttätige globale Grenzpolitik wird durch digitale Technologien, die zum Zweck der Grenzkontrolle und des Migrationsmanagements entwickelt wurden, noch verschärft. Diese Technologien trennen Familien, drängen Menschen in lebensbedrohliches Gelände und verschärfen die Diskriminierung, die für Menschen auf der Flucht und andere marginalisierte Gemeinschaften Alltag ist. Grenzgebiete dienen als Testlabor für neue Technologien, als Orte, an denen ihre Regulierung absichtlich beschränkt wird und an denen die Entwicklung und der Einsatz von Überwachungsmaßnahmen auf Kosten von Menschenleben von einer „anything goes"-Haltung geprägt sind. Heute sind Millionen von Menschen aufgrund von Kolonialismus und Imperialismus, Konflikten, Instabilität, Umweltfaktoren und wirtschaftlichen Ursachen auf der Flucht. An jedem Punkt ihrer Migrationsrouten sind sie Ziel von riskanten, unregulierten Technologien zur Kontrolle und Steuerung von Migration. Die Rhetorik des „Migrationsmanagements" impliziert, dass

3 s. die Homepage des Projekts: ROBORDER, online: https://roborder.eu/the-project/demonstrators

4 Refugees International: One Year Since Greece Opened New "Prison-Like" Refugee Camps, NGOs Call for a More Humane Approach v. 20.9.2022, www.refugeesinternational.org/reports/2022/9/20/one-year-since-greece-opened-new-prison-like-refugee-camps-ngos-call-for-a-more-humane-approach

Flüchtende und Migrant*innen kontrolliert werden müssen, da sie eine Bedrohung für die nationale Souveränität darstellten.

Die Regulierungslücken im Hinblick auf Grenztechnologien sind beabsichtigt, um technologische Experimente zu ermöglichen, die andernorts nicht erlaubt wären.[5] Technologien zur Migrationskontrolle operieren in einem globalen geopolitischen Kontext. Sie vergrößern die Kluft zwischen Nord und Süd sowie dem öffentlichen und privaten Sektor, wo die Macht, Innovationen zu entwickeln und zum Einsatz zu bringen, auf Kosten der Aufsicht und Rechenschaftspflicht geht. Die mächtigen Staaten des Globalen Nordens rechtfertigen diese Experimente mit der Notwendigkeit „permanenter Wachsamkeit, Aktivität und Intervention",[6] indem sie die Macht und die technologische Entwicklung in Nordamerika und Europa konzentrieren und gegen den sogenannten Globalen Süden einsetzen.

Aber wann und warum wurde beschlossen, dass dies die geeigneten Instrumente sind, insbesondere ohne angemessene Kontroll- oder Rechenschaftsmechanismen für den Fall, dass etwas schiefläuft? Einwanderungsentscheidungen sind schon jetzt undurchsichtig, ermessensabhängig und schwer zu verstehen, selbst wenn menschliche Beamte und nicht Technologien die Entscheidungen treffen. Viele von uns haben problematische Erfahrungen gemacht, wenn sie versuchten, eine Arbeitserlaubnis zu erhalten, mit ihrem Ehepartner zusammenzukommen oder ein Baby grenzüberschreitend zu adoptieren, ganz zu schweigen von der Suche nach Schutz auf der Flucht vor Konflikten und Kriegen. Die technologischen Experimente, menschliche Einwanderungsbeamt*innen zu unterstützen oder zu ersetzen, haben drastische Folgen: Im Vereinigten Königreich wurden 7.000 Student*innen zu Unrecht abgeschoben, weil ein fehlerhafter Algorithmus sie beschuldigte, bei einem Spracherwerbstest zu schummeln.[7] In den USA hat die Einwanderungs- und Zollbehörde (ICE)

5 s. z. B. die explizit auf Grenzschutz und Sicherheit ausgerichteten Mitteilungen der Zoll- und Grenzbehörde Kanadas (Canadian Border Services Agency) und das 2019 angekündigte Projekt (Titel: „Keeping Our Families Safe"), Daten zwischen Kanada und den Vereinigten Staaten auszutauschen: Strengthening Border Management, https://connect2canada.com v. 16.7.2019

6 Foucault, M.: The Birth of Biopolitics: Lectures at the Collège de France, 1978–1979, Basingstoke 2008, S. 131-134; ders.: Of Other Spaces, in: Diacritics 1986, H. 1, S. 22-27, https://monoskop.org/images/b/b0/Foucault_Michel_1984_1986_Of_Other_Spaces.pdf

7 Government deported 7,000 foreign students after falsely accusing them of cheating in English Language tests, Independent, www.independent.co.uk v. 14.6.2019

mit Palantir[8] und anderen Privatunternehmen zusammengearbeitet, um Familien aufzuspüren und zu trennen[9] sowie die Inhaftierungen und Abschiebungen von Menschen durchzusetzen, die vor Gewalt in Mittel- und Lateinamerika geflohen waren. Vor den Häfen der EU sind Zehntausende im Mittelmeer und in der Ägäis ertrunken, weil Überwachung als Waffe gegen sie eingesetzt wurde.

Doch was ist, wenn man diese automatisierten Entscheidungen anfechten will? Wer trägt die Verantwortung und haftet – der Technologieentwickler, die Programmierin, der Einwanderungsbeamte oder der Algorithmus selbst? Sollten Algorithmen vor Gericht eine Rechtspersönlichkeit haben, ähnlich wie ein Unternehmen? Es ist von zentraler Bedeutung, dass wir beginnen, Antworten auf diese Fragen zu suchen, da ein Großteil der bürokratischen Entscheidungen bezüglich Asyl und Einwanderung bereits heute in einer unguten rechtlichen Konstellation erfolgen: Ihre Auswirkungen auf individuelle Rechte sind erheblich und lebensverändernd, aber die Verfahrensgarantien schwach.

Zudem sind Grenzen im Wandel begriffen. Sie sind elastisch geworden und nicht mehr an einen physischen Ort gebunden. Wie Ayelet Schahar in ihrem Buch „The Shifting Border" schreibt, „stehen unsere Tore nicht länger unverrückbar an den territorialen Staatsgrenzen. Die Grenze selbst ist zu einer beweglichen Barriere geworden, zu einem losgelösten rechtlichen Konstrukt".[10] Der eigentliche physische Ort verliert an Bedeutung, da verschiedene politische Maßnahmen – und Technologien – die Grenze nach innen und außen verschieben und von der physischen Grenze entkoppeln. Mit der Externalisierung von Grenzen verlagern sich Grenzkontrollen ins Ausland. Dieses Phänomen ist in den letzten Jahren zum Hauptinstrument geworden, mit dem die USA[11] und die Länder der EU versuchen, irreguläre Migration in ihre Hoheitsgebiete zu stoppen.[12]

---

8 I'm a Mother of Four. Palantir's Tech Helped Put me in an ICE Detention Center, www.vice.com v. 20.12.2019

9 Palantir's Technology used in Mississippi raids were 680 were arrested, https://mijente.net v. 4.10.2019

10 Schachar, A: Shifting Border, Manchester 2020, S. 4, https://d2ujvcq4vw00sj.cloudfront.net/wp-content/uploads/2020/02/25102312/9781526145314_sample.pdf

11 Privacy International: Here's the Surveillance the US Exports to Central America as Aid – And it's Surviving Trump's Cuts v. 29.7.2019, Online unter: https://privacyinternational.org/news-analysis/3011/heres-surveillance-us-exports-central-america-aid-and-its-surviving-trumps-cuts

12 Akkerman, M.: Expanding the fortress, Amsterdam 2018, Online unter: www.tni.org/files/publication-downloads/expanding_the_fortress_-_1.6_may_11.pdf

Dazu nutzen sie moderne Technologien, Ausbildung und Ausrüstung von Behörden in Drittländern, um ihre Grenzen weit jenseits ihrer Territorien zu exportieren.[13]

Die Staaten mit den größten Rüstungs- und Sicherheitsbranchen transferieren auf diese Weise Technologien und Praktiken an Regierungen und Behörden auf der ganzen Welt, u. a. in einige der autoritärsten Länder. China, die europäischen Länder, Israel, die USA und Russland sowie Organisationen wie die EU sind allesamt wichtige Anbieter auf dem globalen Markt für Überwachung. Das Transnational Institute (TNI), eine Forschungsgruppe, die sich seit Jahrzehnten mit diesen Themen befasst und zahlreiche Berichte verfasst hat, sieht Externalisierung als „Ansatz, der mit Zuckerbrot und Peitsche arbeitet und finanzielle und politische Anreize für Drittstaaten, häufig ärmere Nationen, schafft, um etablierte Grenzen immer weiter von ihren Territorien weg zu verlagern". Die Externalisierung, oft als Kooperation dargestellt, reproduziert Machthierarchien, wobei verarmte Länder wie Niger die Drecksarbeit der EU erledigen, um die Migration einzudämmen. Laut TNI sind die meisten der 35 Länder, denen die EU für ihre Externalisierungspolitik Priorität einräumt, autoritär, bekannt für Menschenrechtsverletzungen und schlechte Indikatoren für die menschliche Entwicklung. Zudem verkaufen die europäischen Staaten Waffen an diese Länder, obwohl sie damit Konflikte, Gewalt und Unterdrückung anheizen und weitere Fluchtursachen schaffen.[14]

Die Externalisierung funktioniert auch deshalb, weil sie zur weltweiten Schwächung der internationalen Normen beiträgt, die das Recht auf Asyl schützen. In einer komplizierten geopolitischen Realität geraten Menschen, die unterwegs sind, um Sicherheit zu suchen, zwischen die Fronten – ohne Zugang zu Anwält*innen, humanitärer Hilfe oder sogar Ärzt*innen – und werden aktiv daran gehindert, ihr Recht auf Schutz zu suchen. Mächtige Länder verbünden sich mit unverhohlener Islamophobie und Rassismus gegen „muslimische Eindringlinge" und Migrant*innen aus Afrika. Geprägt werden die expandierenden Grenzen von transnationalen Rüstungs- und Sicherheitskonzernen und geopolitischen Interessen. Dabei lernen die Staaten begierig voneinander, und keines dieser

13 New Report Underlines the EU's Strategy in the War on Migration: Border Externalisation v. 18.9.2019, Online unter: https://privacyinternational.org/news-analysis/3224/new-report-underlines-eus-strategy-war-migration-border-externalisation

14 Akkerman a.a.O. (Fn. 12), S. 3

technologischen Experimente findet im luftleeren Raum statt. Zwei Regionen, die in dieser Hinsicht führend sind, sind die USA und die EU.

USA: Abschreckung durch vielschichtige Grenzen

Das eindringliche Bild von einem Auge, das eine einzige Träne vergießt, ziert den Betonwall der rostigen Mauer, die die Grenzstadt Nogales zwischen den USA und Mexiko teilt. Doch es gibt auch andere Arten von Augen, die die Sonora-Wüste, ein riesiges Gebiet im US-Bundesstaat Arizona und eine häufig genutzte Route für Flüchtende und Menschen auf dem Weg von Mittel- und Südamerika nach Norden, überwachen: Drohnen, Überwachungstürme mit künstlicher Intelligenz (KI)[15] und jetzt auch „Roboterhunde" in Militärqualität,[16] die laut dem US-Ministerium für Heimatschutz (DHS) seit Februar 2022 entlang dieser tödlichen Grenze eingesetzt werden. Die sogenannten „Robo Dogs" wurden ursprünglich für Kampfeinsätze und taktische Übungen entwickelt. Die vierbeinigen autonomen Maschinen sind sehr stark und schnell, manchmal bewaffnet[17] und in der Lage, Türen aufzubrechen und sich sogar selbst aufzurichten, wenn sie von einem Menschen mit voller Wucht getreten werden.[18]

Als humanere Alternative zum von Donald Trump forcierten Bau von Mauern und dem Einsperren von Kindern in Käfigen haben die US-Regierungen unter den demokratischen Präsidenten Obama und Biden diese „Smart Border"-Technologien bezeichnet. Allerdings haben Wissenschaftler*innen dokumentiert, dass die Zahl der Todesfälle unter Migrant*innen mit dem Einsatz dieser Technologien an der Grenze zwischen den USA und Mexiko gestiegen ist, weil die Migrationsrouten sich in gefährlicheres Terrain durch die Wüste von Arizona verschoben haben.[19] Im Aufbau befindet sich etwa „ein Netzwerk von fünfundfünfzig Türmen, die mit Kameras, Wärme- und Bewegungssensoren, Radarsystemen und

15 The U.S. Border Patrol and an Israeli Military Contractor Are Putting a Native American Reservation Under "Persistent Surveillance", https://theintercept.com v. 25.8.2019

16 US tests of robotic patrol dogs on Mexican border prompt outcry, www.theguardian.com v. 4.2.2022

17 They're putting guns on robot dogs now, www.theverge.com v. 14.10.2021

18 WATCH: A Robot That Just Won't Quit Even When It's Kicked, www.npr.org v. 9.2.2015

19 Robo Dogs and Refugees: The Future of the Global Border Industrial Complex, www.theborderchronicle.com v. 17.2.2022

einem GPS-System ausgestattet sind";[20] es nimmt dabei auch das etwa eine Meile von der Grenze entfernte Reservat der Tohono O'odham Nation ins Visier.[21]

Auch die USA sind sehr daran interessiert, ihre Grenze so weit wie möglich von der geographischen Grenzlinie vorzuverlagern. Der Journalist Todd Miller, der mehrere Bücher über Grenzen und Migration geschrieben hat, zieht die Idee des Grenzimperialismus heran, um die Politik der USA zu erklären, welche die Grenze zwischen den USA und Mexiko in mehreren Schichten ausdehnt bis hinunter zum Darién Gap zwischen Panama und Venezuela. Miller bezeichnet das gesamte Gebiet als eine Art „dritte Grenze", die Menschen davon abhalten soll, US-Territorium zu erreichen.[22] Es ist die Angst, überrannt zu werden, die erklärt, warum die USA so hart daran arbeiten, die Grenzen weit nach Lateinamerika zu verschieben. Aber es sind die Menschen, die am Grenzübertritt gehindert werden, die viel mehr zu befürchten haben. Im Mai 2021 standen mindestens 18.680 Asylbewerber*innen auf Wartelisten in mexikanischen Grenzstädten. Dort gestrandet, sind sie extremer Gewalt ausgesetzt. Menschen, die von den USA zurückgeschoben werden, sind in Mexiko Vergewaltigungen, Entführungen und Übergriffen ausgesetzt. Besonders betroffen sind LGBTQ+ und schwarze Asylbewerber*innen.[23]

Der Einsatz militärischer oder quasimilitärischer, autonomer Technologien wie Roboterhunde und KI-gestützte Überwachungstürme wird legitimiert durch die Stigmatisierung von Einwanderung als Gefahr für die nationale Sicherheit[24] und die wachsende Kriminalisierung von Migration.

---

20 Campaign to Stop Killer Robots: Submission from the Campaign to Stop Killer Robots, Washington DC 2021, www.ohchr.org/sites/default/files/Documents/Issues/Racism/SR/RaceBordersDigitalTechnologies/Campaign_to_Stop_Killer_Robots_.pdf

21 Robo Dogs and Refugees, a.a.O. (Fn. 19)

22 Border Militarization and Empire: An Interview with Todd Miller, Alliance for Global Justice v. 30.4.2018, https://afgj.org/border-militarization-and-empire-an-interview-with-todd-miller

23 Morley, S.P. et al.: 'There is a Target on Us' – The Impact of Anti-Black Racism on African Migrants at Mexico's Southern Border, New York 2021, https://imumi.org/attachments/2020/The-Impact-of-Anti-Black-Racism-on-African-Migrants-at-Mexico.pdf

24 s. z. B. International Organization for Migration: International Terrorism and Migration, Geneva 2010, www.iom.int/jahia/webdav/shared/shared/mainsite/activities/tcm/international_terrorism_and_migration.pdf; s. auch: Smart Borders, Immigration Enforcement & Border Security Markets in Europe 2017-2022, www.prnewswire.com v. 4.4.2017; s. auch die Darstellung der Europäischen Kommission, in der Migration und Terrorismusbekämpfung in einem Atemzug genannt werden: https://commission.europa.eu/about-european-commission/departments-and-executive-agencies/migration-and-home-affairs_en

Diese Verschiebung rechtfertigt zunehmend harte und invasive Technologien, um an den Grenzen „die Bedrohungslage zu entschärfen".[25] Die Folgen sind katastrophal. Doch die USA sind nicht der einzige Vorreiter in diesem Bereich. Sie nehmen Anleihen und lernen von der Europäischen Union und sind für diese zugleich Quelle der Inspiration.

Externalisierung und die Expansion der Festung Europa

Hightech-Flüchtlingslager, prädiktive Analysen von Personenbewegungen, umfassende Abkommen zum Datenaustausch. Dies sind nur einige der Technologien, die die immer größer werdende Festung Europa nachfragt. Auch diese Projekte greifen bewusst auf andere Länder über und erweitern die Reichweite der EU bei der Steuerung von Mobilität und Migration. TNI schätzt, dass der grenzindustrielle Komplex bis 2025 ein Volumen von 65 bis 68 Milliarden Dollar erreichen wird, mit den größten Zuwächsen in den Feldern Biometrie und KI.[26] Brüssel und die einflussreichen westeuropäischen Mitgliedstaaten üben Druck auf schwächere Mitglieder und Nachbarländer aus, um Pufferzonen auf dem Balkan zu schaffen und selbst Griechenland als „Schutzschild" zu benutzen. Frontex, die Grenzschutztruppe der EU, spielt eine zentrale Rolle bei der Auslagerung der Grenzen. Frontex verlässt sich nicht nur auf israelische Drohnen zur Detektion von Booten, die das Mittelmeer überqueren, sondern hat auch einen Vertrag mit dem israelischen Windward-Projekt erneuert, das ein Werkzeug zur maritimen Analyse anbietet, um mittels Tracking von Schiffen und dem Zusammenführen digitaler Daten „Bösewichte auf See zu fangen". Schon seit langem steht Frontex für eine Agenda der Versicherheitlichung.

Sowohl die EU als auch die USA treiben ihre Rüstungs- und Sicherheitsagenda voran, indem sie ihre eigenen Grenzen militarisieren und weiter nach außen verlagern. Nachdem der Syrien-Krieg Millionen von Menschen nach Europa gezwungen hatte, versuchte die EU-Kommission, ihre Migrationspolitik neu zu gestalten. Dies gipfelte im Neuen Pakt für Asyl und Migration, einem umfassenden Paket, das auf eine äußerst restriktive Grenzkontrollpolitik, eine verstärkte Militarisierung und Externalisierung, Inhaftierung, die Normalisierung von Überwachung und eine

25 Constructing the EU's High-Tech Borders: FRONTEX and Dual-Use Drones for Border Management, Taylor & Francis Online v. 2.7.2018.

26 Akkerman, M.: Financing Border Wars, 2021, S. 1, www.tni.org/files/publication-downloads/financingborderwars-report-tni_2.pdf

Ausweitung von Abschiebungen abzielt. Auch hierbei wird die Migrationskontrolle eindeutig mit äußerer und innerer Sicherheit verknüpft. Die EU finanziert und manchmal spendet sie auch Militär- und Sicherheitsausrüstung und übt politischen Druck auf Drittstaaten aus, damit diese ihre Kapazitäten zur Grenzkontrolle verstärken. Zugleich kurbelt sie damit den Markt für solche Systeme in Afrika und andernorts an.

Hightech-Experimente[27] finden nicht im luftleeren Raum statt. Mächtige staatliche Interessen bestimmen, welche Technologien entwickelt und eingesetzt werden. Politische Entscheidungsträger*innen entscheiden sich zunehmend für eine Eindämmungspolitik anstatt einen humanitären Ansatz zu verfolgen und räumen damit nationaler Sicherheit und Überwachung den Vorrang vor Menschenrechten ein. Im Jahr 2021 forderte die damalige UN-Menschenrechtskommissarin Michelle Bachelet ein Moratorium für Hochrisikotechnologien,[28] einschließlich Grenzüberwachung, doch die EU und die globale Migrationskontrollindustrie folgten diesem Aufruf nicht. Im Rahmen der Verhandlungen über das geplante KI-Gesetz wird derzeit in der EU darüber diskutiert, ob – wie von 200 zivilgesellschaftlichen und akademischen Organisationen gefordert – intelligente Technologien zur Migrationskontrolle als zu riskant verboten werden sollen.[29] Es bleibt abzuwarten, ob dies ein weiteres Beispiel für politische Entscheidungen in Brüssel sein wird, das die bittere Realität vor Ort ignoriert.

Die Auslagerung von Grenzkontrollen lockt mit Entwicklungsgeldern und Militärausgaben Global Player, die mitmachen, um ihr Stück vom Kuchen abzubekommen. Die Autorin und Aktivistin Harsha Walia erinnert daran, dass dies den Grenzimperialismus aufrechterhält, bei dem mächtige Akteure wie die USA und die EU enormen geopolitischen und finanziellen Einfluss auf Länder in Lateinamerika, Afrika und dem Nahen Osten ausüben. Dabei kommt die beschämende imperiale und koloniale Geschichte auf neue Art und Weise zum Tragen und verursacht massenhafte

27 Moria 2.0: The EU's sandbox for surveillance technologies, www.euractiv.com v. 31.3.2021

28 Artificial intelligence risks to privacy demand urgent action – Bachelet, www.ohchr.org v. 15.0.2021

29 EDRi: Civil society calls for the EU AI act to better protect people on the move v. 6.12.2022, https://edri.org/our-work/civil-society-calls-for-the-eu-ai-act-to-better-protect-people-on-the-move

Vertreibung, während zugleich aktiv daran gearbeitet wird, diese zurückzuhalten.[30]

Fazit

77 Grenzmauern durchziehen inzwischen die Landschaften dieser Welt und es werden noch mehr.[31] Sie sind sowohl physisch als auch digital, begründen eine umfassende Überwachung mit dem Vorwand, illegale Einwanderer und Terroristen aufzuspüren und schaffen so Feindbilder, die zur gesellschaftlichen Mobilisierung geeignet sind.[32] Der Einsatz (quasi)militärischer autonomer Technologien untermauert die Verknüpfung von Einwanderung und nationaler Sicherheit. Zudem geht der Export dieser Technologien mit der Ausweitung anderer Praktiken zur Kontrolle und Steuerung von Migration einher. Keine dieser Technologien, Projekte und Entscheidungen ist neutral. Alle technologischen Entscheidungen haben eine inhärente politische Dimension und reproduzieren Vorurteile. Damit erhöhen sie ausgerechnet für jene Menschen das Risiko, Schaden zu nehmen, die bereits heute marginalisiert, diskriminiert und durch die weltweite Verschärfung der Grenzen gefährdet sind.

30 Walia, H.: Undoing border imperialism, Oakland 2013

31 The World Is Witnessing a Rapid Proliferation of Border Walls, MPI v. 2.3.2022, www.migrationpolicy.org/article/rapid-proliferation-number-border-walls

32 Fekete, L.: A Suitable Enemy: Racism, Migration, and Islamophobia in Europe. London 2009

Den Fortschritt nutzen

Migrationsabwehr als angewandte Wissenschaft

von Norbert Pütter

In der Forschungsförderung unterstützen Europäische Union und deutsche Bundesregierung die Abwehr unerwünschter Einwanderung: Die Entdeckung von unerlaubt Einreisenden oder Eingereisten soll verbessert, Grenzen sollen effektiver überwacht und Netzwerke der Grenzsicherungsbehörden sollen gestärkt werden. Die Forschungen legitimieren sich mit Lücken im Grenzschutz, deren Existenz sie zugleich aufdecken und schließen wollen. Sie versprechen, soziale Probleme mit den Mitteln fortgeschrittener Informations- und Naturwissenschaft zu lösen – mit negativen Wirkungen weit jenseits der Migrationsabwehr.

Öffentlich wenig bekannt ist, woran die Unternehmen der Informations-, Kommunikations- und Überwachungstechnologien in ihren Laboratorien und Forschungsabteilungen gegenwärtig arbeiten. Erkennbar ist nur jener Ausschnitt an Forschungs- und Entwicklungstätigkeiten, die über staatliche Förderprogramme unterstützt werden. Der Blick auf diesen Ausschnitt erlaubt zwei Hinweise: Erstens kann er anzeigen, mit welchen Verfahren, welche Teilziele zur Umsetzung der politisch gewünschten Migrationsabwehr verfolgt werden sollen. Weil es hier um Forschungsvorhaben geht, handelt es sich regelmäßig um vollmundige Versprechen über die praktische Nützlichkeit des durch die Forschung Entwickelten; insofern ist deren tatsächliche Wirkung für die Zukunft ungewiss. Zweitens erlaubt die Forschungsförderung einen Blick auf den Zustand der Migrationsabwehr: Denn die Projekte verdanken ihre Förderung dem Umstand, dass sie in ihren Anträgen erfolgreich bestehende Überwachungs- und Kontrolldefizite behaupten, die sie zu schließen versprechen. Da die Abwehr unerwünschter Migration seit Jahrzehnten zum Kern europäischer Grenzpolitik gehört, wird in den Forschungsprojekten zugleich

deutlich, welchen Umfang und welche Eingriffstiefe das Grenzkontrollparadigma mittlerweile erreicht hat.

Auch wenn es zahlreiche nationale und europäische Förderlinien gibt und auch wenn in Rechnung gestellt wird, dass Auftragsforschungen von Regierungen und Behörden damit nicht erfasst werden können, so erlaubt der Blick auf die großen Forschungsförderprogramme Hinweise auf Zustand und Zukunft der Migrationskontrolle mit technisch-wissenschaftlichen Mitteln. Die entsprechenden Forschungen sind in Deutschland gebündelt im Rahmenprogramm „Forschung für die zivile Sicherheit"[1] (kurz: Sicherheitsforschung (SiFo)) der Bundesregierung;[2] auf Ebene der Europäischen Union (EU) finden sie unter dem Dach des Horizon-Rahmenprogramms statt.[3] Beide Programme funktionieren ähnlich: Für eine mehrjährige Zeitspanne werden allgemeine Förderschwerpunkte vorgegeben, die dann in spezifizierten Ausschreibungen bzw. Calls umgesetzt werden. SiFo besteht seit 2007 mit jeweils fünfjähriger Laufzeit, gegenwärtig läuft die dritte Förderperiode (2018-2023). Geförderte Projekte zur Migrationskontrolle finden sich nicht nur unter dem Aufruf „Fragen der Migration", der dem Querschnittsthema „Gesellschaft" zugeordnet ist, sondern auch in anderen Säulen des Programms. Horizon, mit siebenjähriger Laufzeit, setzt seit 2014 die „Forschungsrahmenprogramme" der EU fort. In der aktuellen Förderperiode (2021-2027) wird die „zivile Sicherheit für die Gesellschaft" als ein Feld der Forschung benannt. Unter den fast 130 Calls, die bislang unter diesem Titel veröffentlicht wurden, galten zehn dem „Effektiven Management an den Außengrenzen der EU". Daneben finden sich migrationsrelevante Forschungen in anderen Horizon-Förderlinien.

Bei der Durchsicht der von diesen Programmen geförderten Vorhaben wurden im Folgenden nur jene laufenden oder in den vergangenen Jahren abgeschlossene Projekte berücksichtigt, die einen eindeutig technischen Fokus aufweisen und die Bezüge zur illega(lisiert)en Migration aufweisen.

---

1 Die durch das Rahmenprogramm geförderten Projekte sind in der SiFo-Datenbank erfasst, s. www.sifo.de/SiteGlobals/Forms/sifo/projektsuche/projektsuche_formular.html. Alle Angaben zu den Projekten beziehen sich auf die hier hinterlegten Informationen.

2 s. Töpfer, E.: Entwicklungsauftrag „Zivile Sicherheit", in: Bürgerrechte & Polizei/CILIP 94 (H. 3/2009), S. 21-27. Ich danke Eric Töpfer für seine hilfreichen Hinweise zu diesem Beitrag.

3 Als Nachfolger von „Horizon 2020" läuft das Programm ggw. unter dem Titel „Horizon Europe". Die von der EU geförderten Projekte sind in der CORDIS-Datenbank verzeichnet: https://cordis.europa.eu/projects/de. Alle Angaben zu den Projekten beziehen sich auf die hier hinterlegten Informationen.

Das so entstehende Bild zeigt deshalb in zeitlicher und sachlicher Hinsicht nur einen Ausschnitt.[4] Es werden auch Vorhaben gefördert, die einen sozial- oder rechtswissenschaftlichen Fokus haben oder die Zusammenarbeit der beteiligten Behörden verbessern wollen. So finanziert die EU gegenwärtig das Projekt CRiTERIA[5] mit knapp 5 Mio. Euro. In dem bis 2024 laufenden Projekt soll „eine Methode zur Risikobewertung" entwickelt werden, die mit „umfassenden Risikofaktoren" arbeitet, indem „Erzählungen, Ereignissen und Einstellungen sowie der Anfälligkeit von Grenzen und Menschen" Rechnung getragen wird. Im Projekt MEDEA (Mediterranean practitioners' network capacity building for effecitive response to emerging securiy challenges, dt.: Netzwerk der Praktiker*innen aus dem Mittelmeerraum zur Bildung effektiver Antworten auf wachsende Sicherheitsherausforderungen, Fördersumme 3,5 Mio. Euro) soll ein stabiles Behördennetzwerk aufgebaut werden, das u. a. jährlich eine Forschungs- und Innovationsagenda entwickeln und die gemeinsame Herstellung von Sicherheitstechnologien und Fähigkeiten durch Praktiker*innen und „Anbietern von Innovationen" befördern soll. Hier sind die Grenzen zur repressiven migrationspolitischen Verwendung fließend.

Bezogen auf die auf Migrationsabwehr fokussierten Projekte lassen sich drei Zielrichtungen oder Kontrollorte feststellen: 1. Die Aufdeckung von illegal einreisenden Personen im Moment des versuchten Grenzübertritts. 2. Die großräumige Überwachung der Grenzlinie auf Land und See. 3. Die Kontrolle im Innern, um jene, die die Grenze unerlaubt überwunden haben, zurück- oder abschieben zu können.

Detektion

Wenn von der „Festung Europa" die Rede war bzw. ist, dann war schon immer die Abwehr unerwünschter Menschen aus der EU gemeint und

4 s. zur EU-Förderung: Hayes, B.: In den Fußstapfen von Uncle Sam, in: Bürgerrechte & Polizei/CILIP 94 (H. 3, 2009), S. 14-20; Die großen Brüder von INDECT, www.telepolis.de v. 28.11.2011; Jones, C.: Europäische Sicherheitsforschung, in: Bürgerrechte & Polizei/CILIP 115 (April 2018), S. 59-66; Andres, J.: Migration und Militarisierung, in: Bürgerrechte & Polizei/CILIP 128 (März 2022), S. 48-55

5 Üblich ist, die Projekte durch Akronyme zu kennzeichnen. Gerne wird versucht, das durch die Abkürzung ein bekanntes Wort entsteht, zumindest soll sie lesbar sein. CRiTERIA wurde gebildet aus dem offiziellen Projekttitel „Comprehensive data-driven Risk and Threat Assessment Methods for the Early and Reliable Identification, Validation and Analysis of migration-related risks", offizielle deutscher Titel „Grenzüberschreitende, verbesserte Risikobewertungen".

keineswegs die Verhinderung des Warenverkehrs. Denn der (auch Außen-)Grenzen überschreitende Handel gilt als Garant von Wohlstand und Fortschritt im Innern. Die Logik, Grenzen für Waren durchlässig und zugleich für unerwünschte Einwanderer*innen undurchdringlich zu machen, liegt allen Anstrengungen zugrunde, mit den Waren versteckt Einreisende aufzuspüren. Namentlich geht es bei diesem Aufdecken (Detektion) um die Verstecke in Containern, Kühltransportern oder anderen verschlossenen Behältnissen. Angesichts des Umfangs des internationalen Warenverkehrs ist es praktisch unmöglich und kontrollstrategisch illusorisch, alle infrage kommenden Lieferungen nach versteckten Personen zu durchsuchen. Den Ausweg aus diesem Dilemma bieten die Verfahren der „non-intrusive inspection" (nicht eindringende Untersuchung), deren Optimierung verschiedene Forschungsvorhaben dienten.

Im deutschen Förderkontext gehört das Projekt STRATUM in diese Rubrik. In der „Analyse über rechtliche, gesellschaftliche und technische Aspekte und Maßnahmen zur Aufdeckung illegaler Migration und Bekämpfung der Schleusungskriminalität", so der offizielle Titel, sollten „u. a. Wärmebild- sowie Terahertzkameras zum Einsatz kommen und auf ihre Eignung untersucht werden, im fließenden Straßenverkehr Fahrzeuge auf versteckte Personen zu detektieren". Das Projekt, Laufzeit von 2019 bis 2022, wurde mit 1,9 Mio. Euro gefördert; das Konsortium bestand aus vier Hochschulen und zwei Fraunhofer-Instituten, die Bundespolizei und das Polizeipräsidium Ludwigsburg waren als „assoziierte Partner" dabei.[6]

Auf EU-Ebene war das größte in diesem Bereich geförderte Projekt C-BORD. Mit einer Laufzeit von 2015 bis 2018 wurde das Vorhaben mit dem Titel „effective Container inspection at BORDer control points" mit über 11,8 Mio. Euro gefördert. Unter Leitung des französischen Forschungszentrums für Kernenergie waren weitere 17 Einrichtungen beteiligt. Obwohl auch illegale Einwanderung als ein relevantes Problem benannt wird, war das Programm auf die Detektion von Sprengstoffen, gefährlichen Substanzen und illegalen Drogen ausgerichtet. Durch die Kombination fünf unterschiedlicher Detektionsinstrumente sollte das Aufspüren effektiver und effizienter gestaltet werden: Röntgenaufnahmen, radi-

6 Zu den mit dieser Art von Detektion verbundenen rechtlichen Problemen s. den Beitrag von Clemens Arzt in diesem Heft.

ologische Untersuchungsmethoden, Geruchsspuren und Einsatz verschiedener Sensoren. Menschen werden durch diese Verfahren eher zufällig entdeckt.

Hier setzt das Projekt TRACK an. Einsatzfähig gemacht werden soll ein „Tragbares duales GC-IMS mit Multielement-Sensorsystem zur schnellen und zuverlässigen Detektion versteckter Personen und Waren" (so der offizielle Titel). Das deutsch-österreichische Kooperationsprojekt wurde in den Jahren 2020-2022 mit 620.000 Euro aus SiFo-Mitteln gefördert. Unter Koordination der Airsense Analytics GmbH waren zwei Universitäten (Hannover, Innsbruck), zwei weitere private Firmen, Johanniter aus beiden Ländern, das österreichische Innenministerium sowie als „assoziierte Partner" die Generalzolldirektion und die Bundespolizei beteiligt. Im Projekt sollte ein „tragbares Messsystem" erforscht werden, „das in der Luft kleinste Konzentrationen charakteristischer Merkmale von menschlichen Ausdünstungen wie Atemluft oder Schweiß detektieren" kann. Durch das Ansaugen der Luft über die Dichtungen von Lastwagen oder Containern soll deren Untersuchung im geschlossenen Zustand möglich sein.

Grenzüberwachung

Der Kern der Migrationsabwehr besteht in der Sicherung der Land- und Seegrenzen. Mit knapp 5 Mio. Euro fördert die EU das Projekt NESTOR (aN Enhanced pre-fontier intelligence picture to Safeguard The EurOpean boRders, offzieller deutscher Titel „Ganzheitliches Überwachungssystem der EU-Grenzen"). Koordiniert von der griechischen Polizei sind neben einigen Innenministerien vor allem private IT-Firmen unter den Projektbeteiligten vertreten. Das Projekt verspricht „ein voll funktionsfähiges, umfassendes Grenzüberwachungssystem der nächsten Generation", das „auch über See- und Landgrenzen hinaus eine Lageerkennung im Grenzvorbereich ermöglicht". Aufgedeckt werden sollen die „von kriminellen Netzwerken genutzten Routen", die wegen „geografische(r) Herausforderungen" gegenwärtig noch unerkannt bleiben.

Wie ein solches System aussehen kann, zeigt das bereits abgeschlossene Projekt FOLDOUT (Through-foliage detection, including in the outermost regions of the EU, dt.: Aufdeckung unter Laub(bäumen), auch in den äußersten Regionen der EU). Mit 8,2 Mio. Euro wurde das Projekt gefördert, in dem 21 privatwirtschaftliche Sicherheitsanbieter und -institute zusammenarbeiteten. FOLDOUT versprach nicht nur effektivere und

weniger aufwändige Kontrollen in schwer kontrollierbaren Grenzregionen, sondern auch „Leben zu retten". Entwickelt werden sollte ein System, das verschiedenen Daten erhebt und zu einer „Aufdeckungs-Plattform" zusammenfügt. Die über verschiedene Sensoren gewonnenen Informationen sollen mit Daten über die Verkehrsentwicklung oder Ereignisse jenseits des unmittelbaren Grenzbereichs zusammengeführt werden, um auf dieser Grundlage eine Bewertung drohender Gefahren und Szenarien für mögliche Reaktionen zu entwickeln.

In den Ergebnisdokumenten findet sich eine Abbildung, die die durch FOLDOUT angestrebte Überwachungsstruktur zeigt. Sie beginnt mit der Satelliten-Überwachung oberhalb der 20 km-Entfernung von der Erdoberfläche, die stundengenaue Angaben liefern, bis zu einer Höhe von 20 km soll eine Echtzeit-Überwachung durch Luftschiffe („Stratobus") ermöglicht werden. Die aus diesen Höhen erfolgende permanente Datensammlung soll ergänzt werden durch anlassbezogene Überwachungsflüge mit Drohnen oder Hubschraubern. Schließlich wird im Grenzgebiet eine Reihe von Sensoren installiert: thermische (Temperaturen), seismische (Erderschütterungen), hyperspektrale (elektromagnetische Wellen), elektrooptische (Vergrößerung des Sichtbaren), auch der Einsatz von Lasern und die Analyse von Radio-Frequenzen ist vorgesehen. Projektiert wird ein umfassendes Überwachungssystem, das vom Weltraum bis zur lokalen Identifizierung einzelner Lebensäußerungen reicht.

Seegrenzen

Besonderes Augenmerk gilt der Überwachung der Seegrenzen. Mit 5,1 Mio. Euro förderte Horizon in den Jahre 2016 bis 2018 das Projekt SafeShore (System for detection of Threat Agents in Maritime Border Environment, dt.: System zur Aufdeckung von Gefahren an den Seegrenzen). Koordiniert von der belgischen Militärschule waren Hersteller von Sicherheitstechnik aus Bulgarien, Rumänien, Tschechien und Israel beteiligt. Die neuen Gefahren werden in kleinen Wasserfahrzeugen und Drohnen gesehen, die von „Menschenhändlern ... Terroristen oder Drogenhändlern" genutzt würden. Weil diese Objekte für die herkömmliche Radarüberwachung zu klein seien, entwickelte SafeShore ein Detektionssystem, das die lichtgestützte Objekterkennung mit Abstandsmessung (LiDAR) mit akustischen Sensoren, Funkerfassung sowie visueller und thermischer Videoauswertung kombiniert. Durch die Koppelung von Stationen, die jeweils nur einen begrenzten Raum abdecken, soll die Überwachung

entlang größerer Küstenlinien möglich werden. Die Prototypen wurden in der Nordsee, im Schwarzen und im Mittelmeer erfolgreich getestet.

Von 2017 bis 2020 förderte Horizon das Projekt MARISA (Maritime Integrated Surveillance Awareness, dt.: Integrierte Meeres-Überwachung) mit knapp 8 Mio. Euro. Dass das Meer einen Raum vielfältiger Gefahren darstelle, ist der Ausgangspunkt des Projekts: illegale Migration, Menschenhandel, Terrorismus, Piraterie, Waffen- und Drogenschmuggel. Die vielen Daten und Erkenntnisse, die bei den zuständigen Behörden im Kampf gegen diese Gefahren anfallen, sollen durch MARISA verknüpft und zugänglich gemacht werden: All jene Behörden, die mit der Sicherheit auf See befasst sind, sollen mit einem Werkzeug („data fusion toolkit") ausgestattet werden, das „unterschiedliche Methoden, Techniken und Module in Beziehung setzt zu verschiedenen heterogenen und homogenen Daten und Informationen aus zahlreichen Quellen, einschließlich Internet und Sozialen Netzwerken, mit dem Ziel, den Informationsaustausch, die Aufmerksamkeit, Entscheidungsprozesse und Reaktionsfähigkeiten zu verbessern". Unter den 21 beteiligten Einrichtungen waren nicht nur private Unternehmen aus verschiedenen Mitgliedstaaten und Forschungseinrichtungen (aus Deutschland das Fraunhofer-Institut aus München), sondern auch die Verteidigungsministerien Spaniens, Italiens und Portugals. Beteiligt waren zudem die Forschungsorganisation der NATO sowie Rüstungsfirmen aus Spanien (GMV Aerospace and Defense) und Frankreich (Airbus Defense and Space). In fünf Regionen (Nordsee, Mittelmeer) wurde das System erprobt.

Die Ergebnisse von MARISA sind ausführlich dokumentiert – allein 47 begleitende Teil- und Zwischenberichte sowie 31 Veröffentlichungen. Das Projekt, so dessen Koordinator, werde „die Früherkennung von irregulärer Einwanderung und Menschenhandel verbessern und eine rasche Reaktion durch eine Zusammenarbeit zwischen Behörden, Ämtern und Frontex ... bei Such- und Rettungsmissionen möglich machen". Aufschlussreich sind auch die erhofften Perspektiven zur Weiterentwicklung des Systems. Demnach sollen künftig weitere Datenquellen eingebunden werden: Satellitenüberwachung, die Globale Ereignisdatenbank, Systeme der allgemeinen Schifffahrtsüberwachung etc.

Identitätsprüfungen an der Grenze und im Inland

Neben der versteckten Einreise kann illegale Einwanderung auch durch die Nutzung gefälschter Identitätsdokumente erfolgen. Es liegt deshalb

nahe, dass Anstrengungen unternommen werden, um gefälschte Dokumente bei der Einreise als solche zu erkennen. Zwischen 2018 und 2020 flossen knapp 2,1 Mio. Euro an Horizon-Mittel in das Projekt Smart-Trust (Secure Mobile ID for Trusted Smart Borders, dt.: Sichere mobile Identifizierung für vertrauenswürdige intelligente Grenzen). Die „Mobile ID"-Software ermöglicht die Prüfung digitaler Ausweisdokumente durch die Verbindung mit biometrischen Verfahren. „Unter Verwendung von Mobilgeräten" soll das System „Einzelpersonen, Unternehmen und Regierungen eine vollständige papier- und kontaktlose Identifizierung bei der Abfertigung" an Grenzen ermöglichen. Damit stellt das System einen Baustein für die vollständige Ein- und Ausreisekontrolle (auch) von EU-Bürger*innen dar; zugleich ist es ein Mittel unberechtigte Einreiseversuche aufzudecken.

Eine fast schon klassische Linie verfolgte das SiFo-Projekt SmartIdentification (Smartphone-basierte Analyse von Migrationstrends zur Identifikation von Schleuserrouten).[7] Von 2018 bis 2020 mit 950.000 Euro gefördert, koordiniert von der Technischen Universität in Aachen (als Projektpartner neben anderen das Bundespolizeipräsidium und als assoziierter Partner SAP Deutschland SE & Co. KG) zielte dieses deutsch-österreichische Kooperationsvorhaben auf verschiedene Zwecke: Anhand der Auswertung ihrer Smartphones und anderer mitgeführter Dokumente sollten die Angaben von Migrant*innen ohne Identitätsdokumente überprüft werden, auf dem Smartphone befindliche Bilder für die Altersbestimmung genutzt und zugleich mithilfe der Positionsdaten „Schleuserrouten" identifiziert und „alternative Kommunikationsplattformen zur Entdeckung der Schleuser analysiert werden".

Der leichteren Aufdeckung gefälschter Identitätsdokumente im Inland dient das SiFo-Projekt MEDIAN (Mobile berührungslose Identitätsprüfung im Anwendungsfeld Migration). Das Vorhaben wurde in den Jahren 2018 bis 2021 mit 2,7 Mio. Euro gefördert. Koordiniert von der Bundesdruckerei waren zwei Hochschulen und zwei private IT-Firmen direkt, die Landeskriminalämter Bayerns und Berlins als assoziierte Partner beteiligt. Im Rahmen von MEDIAN sollte eine technische Lösung entwickelt werden für die „schnelle und berührungslose Erfassung sowie einen automatisierten Abgleich von Fingerabdrücken und Gesichtsbildern". Die erhobenen Daten sollten „mit polizeilichen Hintergrundsystemen" abgeglichen werden.

7 S. a. den Beitrag von Lucie Audibert in diesem Heft.

Die Prüfung der Identität von Migrant*innen, die ohne Berechtigung nach Deutschland eingereist sind, ist für deren Rechtsstatus und den Umgang der Behörden mit ihnen von Bedeutung. Denn sie umfasst nicht allein die Echtheit mitgeführter Dokumente und ob diese die überprüfte Person ausweisen, sondern sie erstreckt sich auch auf die Bestimmung des Herkunftslandes und des Alters. Das SiFo-Projekt AUDEO (Audiobasierte Herkunftslanderkennung von Migranten) zielte darauf, die Herkunft von Menschen, die sich im Asylverfahren befinden, zu klären. Im Asylverfahren ist das Herkunftsland besonders wichtig: Von ihm hängt ab, ob das Asylverfahren überhaupt eröffnet wird, welche Chancen auf Anerkennung bestehen, welche Rechte während der Dauer des Verfahrens gewährt werden, ob subsidiärer Schutz möglich ist oder Abschiebehindernisse bestehen. AUDEO wollte die Herkunft durch eine „software-basierte Sprach- und Dialektanalyse" bestimmen, die mit einer „stimmlichen Emotionserkennung" gekoppelt wird. Anhand von „Mikrotremor, Verzögerungen und stimmlichen Anomalien" sollten Täuschungsversuche erkannt werden. Versprochen wurde eine über 90-prozentige und justiziable Erfolgsquote. An dem vom Bundespolizeipräsidium koordinierten, von 2019 bis 2021 mit 932.000 Euro geförderten Projekt, waren neben einer privaten Hochschule, Ausländerbehörden aus Bayern und Berlin sowie Sony Mobile Communication beteiligt.

Mit nur 173.000 Euro fördert Horizon das Projekt UMAFAE (Unaccompanied Minors Automatic Forensic Age Estimation, offizieller deutscher Titel: Bestimmung des biologischen Alters von Minderjährigen durch künstliche Intelligenz). Das Projekt läuft noch bis Februar 2024; es wird von einer spanischen IT-Firma betrieben. Die Altersfeststellung von Menschen ohne Ausweisdokumente ist aus verschiedenen Gründen von Bedeutung: In Art. 24 der Aufnahmerichtlinie der EU werden besondere Schutzbestimmungen für Minderjährige festgeschrieben, die Abschiebung Minderjähriger ist erschwert; für Deutschland bestimmt die Volljährigkeit darüber, ob das Asyl- oder das Kinder- und Jugendhilferecht angewendet werden. UMAFAE möchte die Praxis der Altersfeststellung in den Mitgliedstaaten vereinheitlichen, indem mit den Mitteln Künstlicher Intelligenz ein einheitliches Verfahren etabliert wird.

Schlussfolgerungen

Die vorgestellten Projekte im Feld der Forschungsförderung lassen sich durch vier Merkmale charakterisieren:

1. Weil sich mit Migrationsabwehr Geld verdienen lässt, entsteht ein kooperatives Geflecht aus privatwirtschaftlichen Anbietern, öffentlichen oder privaten Forschungseinrichtungen und den Behörden, die an technologischen Lösungen ihrer Aufgaben interessiert sind.
2. Migrationsabwehr wird als ein technisch zu lösendes Problem konzipiert. Dabei wird einerseits daran gearbeitet, stabile, vereinheitlichte oder zumindest kompatible Standards und Verfahren zu entwickeln. Andererseits werden technologische Verfahren so kombiniert, dass sie jederzeit und überall vorher definierte Auffälligkeiten entdecken können. Hightech wird eingesetzt, um die Unüberwindbarkeit der Grenzen zu erhöhen – sei es als Ersatz für Zäune und Mauern, sofern diese aus topografischen Gründen nicht möglich oder aus politischen Gründen nicht opportun erscheinen, oder sei es als technologische Verstärkung der physischen Barrieren.
3. Mit dem technischen Fokus ist quasi automatisch verbunden, dass die Forschungen die Abschottungslogik als unhinterfragte Basis ihres Tuns (und Geldverdienens) bekräftigen und die Migrant*innen als zu polizierende Objekte behandeln. Auch der Bezug auf „Schleuser" oder auf die Rettung von Menschenleben kann nicht darüber hinwegtäuschen, dass die rigide Abschottung erst zu jenen Fluchtrouten und -verhalten führt, die mit aufgerüsteter Technik verhindert werden sollen.
4. Schließlich wird in einigen Projekten (FOLDOUT, MARISA) deutlich, dass sie weit über die Migrationskontrolle ausstrahlen. Kurz: Sie bergen das Potenzial zu einer totalitären Überwachung der gesamten Gesellschaft. Was erfolgreich getestet wird, um Flüchtende in unzugänglichen Grenzregionen zu entdecken, das wird auch tauglich sein, Demonstrierende zu beobachten oder Einzelpersonen im städtischen Raum zu lokalisieren. Die Forschung(sförderung) verstärkt nicht nur die Ignoranz gegenüber dem Leiden der Flüchtenden, sondern sie schafft zugleich Instrumente, die die gesamte Gesellschaft technologisch gestützter Kontrolle unterwerfen.

Wirklich nur Forschung?

Die EU lässt dubiose KI für die Grenzkontrolle entwickeln

von Lise Endregard Hemat

Der Artikel untersucht neue technologische Trends in der Digitalisierung von Grenzen. Die EU fördert derartige Experimente zum Einsatz von Künstlicher Intelligenz (KI) in der Grenzkontrolle und rechtfertigt dies damit, es handele sich um bloße Forschung. Doch insbesondere dort, wo Migrant*innen ins Visier genommen werden, gilt es zu berücksichtigen, dass Forschung unsere Vorstellungen von der Welt widerspiegelt.[1]

In ihrer KI-Strategie hat die EU-Kommission das Ziel ausgegeben, eines der führenden Zentren für Technologien Künstlicher Intelligenz zu werden.[2] Dazu fördert sie KI-Forschungsprojekte, um technologische Kompetenz und Lösungen zur Bewältigung ihrer Herausforderungen zu entwickeln. Dieser Artikel greift auf die KI-Definition zurück, die die von der EU-Kommission eingesetzte „Hochrangige Expertengruppe für Künstliche Intelligenz" entworfen hat.[3] KI meint demnach Softwaresysteme (und möglicherweise auch Hardware), denen ein komplexes Ziel gesetzt wird, die ihre Umgebung durch das Sammeln und Interpretieren von Daten wahrnehmen, diese Informationen auswerten und davon ausgehend Entscheidungen darüber treffen, welches Vorgehen am besten geeignet ist, das Ziel zu erreichen. Darüber hinaus können KI-Systeme ihr Verhalten

1 Dieser Artikel verwendet „Migrant*innen" als allgemeinen Begriff, der Geflüchtete und andere Kategorien von Migrant*innen gemäß der Definition von Jørgen Carling umfasst, vgl. Carling, J.: Refugees Are Also Migrants. All Migrants Matter, in: University of Oxford, Faculty of Law Blogs v. 3.9. 2015, https://blogs.law.ox.ac.uk/research-subject-groups/centre-criminology/centreborder-criminologies/blog/2015/09/refugees-are-also.

2 EU-Kommission: Ein europäischer Ansatz für künstliche Intelligenz, online: https://digital-strategy.ec.europa.eu/de/policies/european-approach-artificial-intelligence

3 High-Level Expert Group on Artificial Intelligence: A definition of AI: Main capabilities and scientific disciplines, online: https://ec.europa.eu/futurium/en/system/files/ged/ai_hleg_definition_of_ai_18_december_1.pdf

anpassen, indem sie analysieren, wie sich ihre Umwelt durch ihr vorangegangenes eigenes Vorgehen verändert.

Bei der Entwicklung von KI können unterschiedlichste Herangehensweisen und Techniken zum Einsatz kommen. Eine von ihnen ist das maschinelle Lernen. Es ist typischerweise dort nützlich, wo es um Probleme geht, die nicht mit symbolischen Denkregeln beschrieben werden können, wie beispielsweise Fragen der Sprache. Einfach gesagt: Anstatt dem System eine Regel vorzugeben, die es zu befolgen gilt, geben ihm die Entwickler*innen eingehende und ausgehende Informationen und ermöglichen dadurch Generalisierungen. Ausgehend von diesen Generalisierungen, deren Funktionsweise Menschen möglicherweise noch nicht einmal verstehen, kann das System Aufgaben lösen und menschliches Denken simulieren.

KI ermöglicht in vielen Fällen Effizienz und Präzision. Eines der Gebiete, auf dem die EU dies erhöhen möchte, ist die Kontrolle der Grenzen. Experimente mit KI sind daher mit einer weiteren Entwicklung verwoben: der Digitalisierung der Grenzen. Das Bestreben der EU, die Effizienz und Sicherheit der Grenzen mit digitalen Mitteln zu steigern, begann bereits 2008 mit dem „Smart Borders Package".[4] Es sollte Grenzen „smarter" machen, um die Sicherheits- und Strafvollzugsbehörden mit den Werkzeugen auszustatten, Europa vor Terrorismus, Kriminalität und irregulärer Einwanderung zu schützen.

Derartige Sicherheitsbedrohungen sind komplex, transnational, entwickeln sich rasch und spornen so neuartige technologische Lösungen an – einschließlich der KI. Diese Bedürfnisse vereinigten sich in den EU-geförderten Forschungsprojekten. Das Förderprogramm der EU für Forschung und Innovation zwischen 2004 und 2010 lief unter dem Namen „Horizon 2020 (H2020)". Es enthielt ein Arbeitsprogramm namens „Sichere Gesellschaften" mit dem Unterthema „Border Security and External Security", in dem die EU dazu aufrief, neuartige Lösungen für das Schaffen effizienter und sicherer Landgrenzen zu finden.

Nicht alle Menschen teilen die Begeisterung für die mit EU-Förderung entwickelten KI-Sicherheitstechnologien. Ella Jakubowska von European Digital Rights (EDRi) zufolge zeichnet sich „ein breiterer Trend dahingehend ab, dass die EU öffentliche Gelder in dystopische und experimentelle

4 EU-Kommission: Stronger and Smarter Information Systems for Borders and Security, Kommissionsdokument COM (2016) 205 final v. 6.4.2016

Überwachungsprojekte steckt, in denen Menschen wie Laborratten behandelt werden".[5] Petra Molnar, Associate Director des Refugee Law Lab der York University, teilt diese Bedenken und steht technologischen Experimenten kritisch gegenüber, insbesondere auf dem Gebiet der Grenzkontrolle, da Migrant*innen häufig die Versuchssubjekte sind.[6] Ihr zufolge werden diese Versuche durch unterschiedliche Rechte von Migrant*innen und denen von EU-Bürger*innen ermöglicht. Migrant*innen werden von der EU und den Technologieentwickler*innen als Menschen mit geringeren individuellen Rechten wahrgenommen, was sie zum „perfekten Ziel" experimenteller Technologien macht. Der folgende Abschnitt beschreibt ein solches auf die Grenzkontrolle gerichtetes, EU-gefördertes KI-Technologieprojekt näher.[7]

iBorderCtrl

Das Forschungsprojekt „Intelligent Portable Border Control System (iBorderCtrl)" hat in dieser Hinsicht erhebliche Kritik erfahren. Kritiker*innen meinen, dass das Projekt eine pseudowissenschaftliche Technologie entwickelt habe, die die Rechte und Sicherheit von Migrant*innen gefährdet.[8] Übergeordnetes Ziel dieses Projekts war es, eine KI-Technologie zum besseren Schutz der europäischen Grenzen vor Terrorismus, Kriminalität und irregulärer Migration zu entwickeln. Hierfür entwarfen die Forscher*innen einen KI-gestützten „Lügendetektor" namens „automated deception detection system (ADDS)". Die Projektseite von iBorderCtrl hat diese Technologie als „Lügendetektor" bezeichnet, der Datenschutz-

5 With Drones and Thermal Cameras, Greek Officials Monitor Refugees, www.aljazeera.com v. 24.12.2020

6 Molnar, P.: Technology on the Margins: AI and Global Migration Management from a Human Rights Perspective, in: Cambridge International Law Journal 2019, Nr. 2, S. 305-330

7 Dieser Aufsatz basiert auf Arbeiten, die für die Masterarbeit der Autorin durchgeführt wurden: Hemat, L.E.: „Just" Research: A Case Study of EU-funded Research with Experimental Artificial Intelligence Technology for Border Control, MA thesis, University of Oslo The Faculty of Law, Norwegian Centre for Human Right, Oslo 2022, www.prio.org/publications/13182.

8 EU Border „Lie Detector" System Criticised as Pseudoscience, www.theguardian.com v. 2.11.2018; Kinchin, N.: Technology, Displaced? The Risks and Potential of Artifical Intelligence for Fair, Effective, and Efficient Refugee Status Determination", in: Law in Context 2021, Nr. 3, S. 45-73, https://journals.latrobe.edu.au/32ff498d-a8d1-4f58-9b6e-1146461e14c1

beauftragte Zoltán Székely jedoch darauf hingewiesen, dass ein „deception detector" (Täuschungsdetektor) sich davon grundsätzlich unterscheide. Im Rahmen dieses Artikels wird nicht auf die technischen Einzelheiten eingegangen und die Technologie daher als ADDS bezeichnet.

Der Zweck des beforschten ADDS sollte es sein, in die EU kommende Drittstaatsangehörige zu überprüfen.[9] Bevor sie an der Grenze ankämen, müssten sie Bilder ihres Reisepasses und Visums auf eine Website hochladen und sich einer Befragung durch einen als virtuellen Avatar auf dem Monitor dargestellten Grenzschützer von iBorderCtrl unterziehen. Während der Befragung müsste die Webcam angeschaltet bleiben, damit das System die Mikrogestik auf der Suche nach Täuschungsanzeichen analysieren kann. Mikrogesten sind winzige und rasche Gesichtsbewegungen, die angeblich mit Stress und Besorgnis einhergehen, wie etwa ein Augenlid halb zu schließen und wieder zu öffnen. Da das System auf maschinellem Lernen basiert, wäre es im Nachhinein unmöglich zu bestimmen, welche Geste für die Kennzeichnung als Täuschung maßgeblich gewesen wäre.[10]

Nach der Befragung würden die Einreisenden einen QR-Code erhalten, den sie an die Grenze mitbringen. Erst dort würden sie dann von Grenzbeamt*innen überprüft. Auf ihrem (im Rahmen des Projektes entwickelten) „iCross"-Gerät könnten die Beamt*innen den jeweiligen „Täuschungsscore" abrufen und entscheiden, ob weitere Befragungen durchgeführt werden, die Einreise abgelehnt oder gestattet wird. Die Reisenden würden ihren eigenen Score nie erfahren.[11]

Das ADDS wurde nie an Grenzen eingesetzt und auch nicht ausführlich erprobt. Aufgrund der Kritik wurden Tests, die an der ungarischen Grenze hätten erfolgen sollen, aufgeschoben.[12] Stattdessen wurde an einer Grenzübergangsstelle einer Landgrenze eine freiwillige Warteschlange eröffnet, an der Freiwillige das System ausprobieren konnten. Dort fanden

9 „Drittstaatsangehörige" meint hier alle Personen, die nicht Staatsangehörige eines Schengen-Mitgliedstaates sind.

10 O'Shea, J. et al.: "Intelligent Deception Detection through Machine Based Interviewing, in: International Joint Conference on Neural Networks, Rio de Janeiro 2018, S. 1-8, https://doi.org/10.1109/IJCNN.2018.8489392

11 Hemat, L.E.: Trends in the Digitalisation of EU Borders: How Experimentations with AI for Border Control Treat Migrants as Test Subjects, PRIO Policy Brief 2022, Nr. 15, www.prio.org/publications/13253; We Tested Europe's New Lie Detector for Travelers – and Immediately Triggered a False Positive, https://theintercept.com v. 26.7.2019

12 Zoltán Székely, Interview mit der Autorin, 2022

sich am Ende vor allem neugierige Journalist*innen und Aktivist*innen wieder.

Rationalisierungen für iBorderCtrl

Nach der Kritik, die iBorderCtrl erfahren hatte, musste die Kommission reagieren. 2020 erinnerte sie, dass es sich „bei iBorderCtrl um ein Forschungsprojekt handelte, das weder die Erprobung noch den Einsatz eines tatsächlich funktionsfähigen Systems ins Auge gefasst hat."[13] Diese Stellungnahme suggeriert, dass EU-geförderte Forschung unproblematisch ist, wenn sie nicht umgesetzt wird. Auf die Kritik an den potenziellen menschenrechtlichen Problematiken ist die Kommission nicht eingegangen. Ähnliche Überlegungen wurden durch Frontex vorgetragen – als mögliche Endnutzerin eine zentrale Stakeholderin bei der Erforschung von Grenztechnologien. Zwei Befragte aus der Abteilung für Forschung und Innovation bei Frontex haben behauptet, die Technologie sei „Lichtjahre" von einem Einsatz entfernt.[14] Meiner Meinung nach kann aber Forschung, wenngleich sie einen legitimen und wichtigen Zweck darstellt, nicht einfach deshalb als völlig unproblematisch abgetan werden, nur weil sie nicht eingesetzt wird.

Erstens gibt es immer bestimmte Gründe dafür, dass geforscht wird. Die ADDS-Technologie wurde unter anderem als nützlich beim Kampf gegen „irreguläre Migration" wahrgenommen. Das iBorderCtrl-Projekt geht daher von der immer weiter verbreiteten Vorstellung aus, dass Technologien dabei helfen können, „Migrationskrisen" zu lösen, und dass digitalisierte Grenzen die Sicherheit in Europa erhöhen werden. Einer solchen Vorstellung liegt die Annahme zugrunde, dass Migration kontrolliert werden kann, wenn wir Informationen über sie haben. Diese Rhetorik ist fragwürdig. Besters und Bronn beispielsweise haben argumentiert, dass die europäische Digitalisierung der Migrationssteuerung sich in „gieriger" Informationstechnologie verfangen hat. Informationstechnologie will stetig mehr. Wenn wir immer mehr Datensammelsysteme einführen, stehen wir am Ende mit enormen Datenmengen da, es fehlen aber nach wie vor

13 Europäisches Parlament: Antwort der EU-Kommission auf die Parlamentarische Anfrage – E-000152/2020 v. 30.3.2020

14 Befragte aus der Abteilung für Forschung und Innovation bei Frontex, Interview mit der Autorin, 2022

Systeme, um die strukturellen Probleme zu beheben, die Migration verursachen.[15] iBorderCtrl ist ein Beispiel für diesen Datenhunger, denn das Projekt sollte das „Ein-/Ausreisesystem" (EES) unterstützen, dessen Inbetriebnahme für Mai 2023 vorgesehen war. Das EES wird noch mehr Daten über Drittstaatsangehörige sammeln, wann immer sie den Schengen-Raum betreten, verlassen oder durchqueren. iBorderCtrl sollte die durch EES verursachten längeren Warteschlangen wieder verkürzen, indem es die Grenzkontrolle teilweise in die Wohnungen der Drittstaatsangehörigen auslagert.

Zweitens sind Grenztechnologien nicht neutral. Martins und Jumberts Aufsatz über die Co-Produktion von Sicherheits-„Problemen" und „-Lösungen" legt dar, wie aufgrund der Versicherheitlichung von Migrant*innen an modernsten Technologien geforscht wird. Theorien der Versicherheitlichung zeigen auf, dass das, was als Bedrohung wahrgenommen wird, und das, was als schutzbedürftig angesehen wird, sozial konstruiert ist. Die mächtige Position der EU ermöglicht ihr festzulegen, welche Themen in welcher Weise Aufmerksamkeit verdienen. Migration als Risiko zu framen, kann die Grenzen dessen, was als angemessen erachtet wird, verschieben, und so die Entwicklung außerordentlicher Technologien ermöglichen. Mit anderen Worten: Technologien, die ansonsten als völlig unangemessen und überflüssig erachtet würden, werden als nützlich bei der Bewältigung der von Migrant*innen angeblich ausgehenden Sicherheitsbedrohungen angesehen.[16]

Es darf davon ausgegangen werden, dass EU-Bürger*innen heftig protestieren würden, wenn die EU Millionen Euros für die Entwicklung eines Systems ausgeben würde, das ihre Glaubwürdigkeit bei einer Reise überprüfen soll.

Die europäischen Grenzen sind hoch technologisiert und es ist nicht unvorstellbar, dass ADDS in der Zukunft eingesetzt werden könnte. So hat Frontex ausdrücklich angegeben, dass KI-Projekte im Rahmen von H2020 Technologien für die Zukunft der Grenzkontrolle schaffen.[17] Trotz

15 Besters, M.; Brom F.W.A.: „Greedy" Information Technology: The Digitalization of the European Migration Policy, in: European Journal of Migration and Law 2010, H. 4, S. 455-470, https://doi.org/10.1163/157181610X535782

16 Martins, B.O.; Jumbert. M.G.: EU Border Technologies and the Co-Production of Security „Problems" and „Solutions", in: Journal of Ethnic and Migration Studies 2020, H. 6, S. 1430-1447, https://doi.org/10.1080/1369183X.2020.1851470

17 Frontex: EU Research, Stand 2021, archivierte Seite: https://web.archive.org/https://frontex.europa.eu/future-of-border-control/eu-research/horizon-projects/?p=1

der Statements der Europäischen Kommission und von Frontex, wonach iBorderCtrl weit davon entfernt sei, eingesetzt zu werden, will der EU-Abgeordnete Patrick Breyer aufgedeckt haben, dass iBorderCtrl Lobbyismus beinhalte, um die Gesetzgebung so zu ändern, dass das System tatsächlich eingesetzt werden könnte. Breyer erhob eine Transparenzklage gegen die EU-Forschungsagentur auf Offenlegung der klassifizierten i-BorderCtrl-Dokumente zu Legalität, Ethik und Ergebnissen. Er erhielt Recht und die Dokumente wurden herausgegeben, waren jedoch weitreichend geschwärzt. Es war ihm möglich, den Text wiederherzustellen und so aufzudecken, dass zu den Zielen des Projekts gehörte, die EU-Gesetzgebung zu beeinflussen.[18] Darüber hinaus wurde in einem späteren H2020-Projekt namens „TRESSPASS" eine ähnliche Technologie zur Überprüfung von Aufrichtigkeit entwickelt. Es strebte an, eine Echtzeit-Verhaltensanalyse zur Risikoeinschätzung an Flughäfen zu erstellen, um Reisende zu evaluieren.[19]

Migrant*innen als Versuchssubjekte

Beginnend mit dem Schengener-Informationssystem 1995 sind Migrant*innen kontinuierlich Betroffene neuer EU-Sicherheitsanwendungen – ein Gebiet, das seitdem hochgradig technologisiert ist. Indem die Freizügigkeit für EU-Bürger*innen innerhalb des Schengen-Raums etabliert wurde, wurde die Bewegungsfreiheit von Drittstaatsangehörigen dorthin eingeschränkt. Alyna Smith, Vizedirektorin der Nichtregierungsorganisation PICUM (Platform for International Cooperation on Undocumented Migrants), argumentiert, dass der Fokus auf den Schutz der EU vor Migrant*innen (insbesondere irregulären) „ein völlig überdimensioniertes Augenmerk legt, auf eine äußerst negative Weise".[20] Ihrer Ansicht nach stellen irreguläre Migrant*innen keine solch schwerwiegenden Sicherheitsbedrohungen dar, dass sie es rechtfertigen würden, Millionen von Euro für Experimente mit Technologien auszugeben, die darauf abzielen, diese fernzuhalten.

---

18 Breyer, P.: Big brother „video lie detector": EU research funds are misused to lobby for legislative changes, 27.4.2021, www.patrick-breyer.de/en/big-brother-video-lie-detector-eu-research-funds-are-misused-to-lobby-for-legislative-changes

19 Monroy, M.: EU Project iBorderCTRL: Is the Lie Detector Coming or Not?, 26.4.2021, https://digit.site36.net/2021/04/26/eu-project-iborderctrl-is-the-lie-detector-coming-or-not

20 Alyna Smith, Interview mit der Autorin, 2022

Wie bereits ausgeführt, verschiebt die Versicherheitlichung von Migrant*innen die Grenze dessen, was als angemessene und erforderliche Reaktion angesehen wird. In der Folge beobachten wir dubiose technologische Experimente, die für den Einsatz an EU-Bürger*innen wahrscheinlich niemals freigegeben würden. Matthias Monroy weist darauf hin, dass Drittstaatsangehörige womöglich zur Zielgruppe für iBorderCtrl wurden, weil „niemand protestieren würde, da keine EU-Bürger*innen betroffen sind."[21] Ein weiterer Grund dafür, dass Drittstaatsangehörige hierfür ausgewählt werden, mag mit der potenziellen negativen Stigmatisierung von Migrant*innen zusammenhängen. „Täuschungsdetektion" ist ein negativ aufgeladener Begriff, der voraussetzt, dass die Betroffenen absichtlich täuschen könnten – eine erniedrigende Idee. Es scheint, dass diese herabwürdigenden Vorstellungen von Migrant*innen in der Debatte darüber übersehen oder zumindest nicht aktiv hinterfragt werden.

Costica Dumbrava, Politikanalyst beim Wissenschaftliche Dienst des Europäischen Parlaments, betont, dass Technologien nie „gerecht" sind, weil sie bestehende Ideen repräsentieren und perpetuieren.[22] Dass auf Migrant*innen abgezielt wird, ist nicht neu. Asylsuchende waren die ersten, denen die EU durch EURODAC Fingerabdrücke abnehmen ließ. Monroy zufolge zeigt dies, dass Migrant*innen als geeignete Versuchspersonen für experimentelle Technologien erachtet wurden. Auch Molnar, Smith, Besters und Brom behaupten, dass die Migrationssteuerung der EU zum Versuchslabor für neuartige Technologien geworden ist.[23]

Migrant*innen ins Visier zu nehmen, ist zudem problematisch, weil ein System wie iBorderCtrl auf maschinelles Lernen angewiesen ist und das Sammeln enormer Datenmengen erfordern würde. Die EU erhebt bereits viele Daten von Reisenden und das System von iBorderCtrl würde noch mehr davon benötigen. Es ist wichtig, sich in Erinnerung zu rufen, dass Daten verloren werden können – so geschehen durch den Cyberangriff auf das Internationale Komitee vom Roten Kreuz (IKRK) im November 2021.[24] Ein gehackter Server enthielt Kontaktinformationen, Namen

21 Matthias Monroy, Interview mit der Autorin, 2022

22 Costica Dumbrava, Interview mit der Autorin, 2022

23 Molnar, P.: Technology on the margins: AI and global migration management from a human rights perspective, in: Cambridge International Law Journal 2019, Nr. 2, S. 305-330, https://doi.org/10.4337/cilj.2019.02.07

24 IKRK: Cyber attack on ICRC: What we know v. 16.2.2022, www.icrc.org/en/document/cyber-attack-icrc-what-we-know

und Ortsangaben von mehr als 500.000 Personen, darunter Gefangene, Vermisste und deren Familien sowie Menschen, die Unterstützung durch das IKRK aufgrund bewaffneter Konflikte oder Migration erhalten. Burkhard Schafer, Professor für Computational Legal Theory, zeigt sich „immer sehr skeptisch gegenüber einem Argument für die Ausweitung von Datennutzung", denn „sobald wir die Infrastrukturen aufbauen, sobald wir die Daten erheben, sind sie da".[25] Ist es zu rechtfertigen und angemessen, noch mehr Daten zu erheben, um Migration zu steuern und die selbstdefinierten Sicherheitsprobleme der EU zu lösen? Erschwerend tritt hinzu, dass für Migrant*innen das Finden von und der Zugang zu Abhilfe und Rechtswegen bei Datenmissbrauch herausfordernd ist oder sie Diskriminierung ausgesetzt sind.

Fehlende ethische Bewertung

Bei Forschungsprojekten von dieser Größenordnung und Bedeutung sind die ethische Bewertung und der vorsichtige Umgang mit Daten ersichtlich besonders wichtig. Vertreter*innen aus der Abteilung für Forschung und Innovation bei Frontex, mit denen ich gesprochen habe, waren der Meinung, dass iBorderCtrl einer ausführlichen ethischen Bewertung unterzogen worden sei. Meiner Untersuchung zufolge handelte es sich jedoch um einen kurzen, nahezu nicht vorhandenen Prozess. Der Datenschutzbeauftragte für iBorderCtrl, Zoltán Székely, ließ wissen, dass seine Ernennung überstürzt und nicht durchdacht gewesen sei. Sie sei in den letzten Tagen der Antragstellung erfolgt, weil man plötzlich bemerkt habe, dass eine*n Verantwortliche*n dafür benötigt würde. Er sei hauptsächlich aufgrund seines Abschlusses in Politikwissenschaft ausgewählt worden.

Zum Zeitpunkt der Antragstellung für die Förderung von iBorderCtrl wurde eine Datenschutz-Folgeabschätzung nicht vorausgesetzt. Die Forschenden wollten jedoch eine ordnungsgemäße ethische Bewertung durchführen und baten verschiedene Universitäten um Rat. Während sie dabei waren, sich um Beratung zu bemühen, wurden sie von der ungarischen Grenzpolizei darüber informiert, dass sie alle Versuche würden aufschieben müssen. Diese Nachricht kam, nachdem das ADDS auf einer Ausstellung zur Erprobung zur Verfügung stand und das Projekt daraufhin negative Reaktionen erhalten hatte. Das Team konnte die ethische

25 Burkhard Schafer, Interview mit der Autorin, 2022

Beratung durch Universitäten deshalb nicht wie geplant in Anspruch nehmen.[26] In späteren Jahren sind ethische Bewertungen im Rahmen von H2020-Forschungsprojekten vermutlich mehr in den Blick gerückt, werden aber noch nicht als adäquat angesehen. Sarah Perret, Research Associate am King's College London, hat selbst erlebt, dass ethische Erwägungen als Formalität behandelt werden und Projekte „Schlagworte" nennen, um die Ethik-Voraussetzungen zu erfüllen.[27]

Schlussbemerkungen

In den obigen Abschnitten habe ich versucht darzulegen, dass das EU-geförderte Experimentieren unabhängig von seiner Umsetzung Auswirkungen hat. Migration wird als eine Gefahr geframed, die mit zusätzlichen Informationen gelöst werden könne, wobei sich die Grenzen dessen, was als akzeptabel erachtet wird, verschieben. Solche Prozesse können die Entwicklung außergewöhnlicher Technologien befördern. Die Vorstellung, iBorderCtrl biete noch keinen Grund zur Sorge, habe ich mit Blick auf Erkenntnisse hinterfragt, wonach das Projekt vorhatte, Lobbyarbeit für Gesetzesänderungen zu betreiben, während künftige Projekte ähnliche Technologien fortentwickeln. Indem auf Drittstaatsangehörige abgezielt wird, ist iBorderCtrl eines von vielen Projekten, in denen die Migrationssteuerung der EU ein Versuchslabor für neuartige Technologien wird. Letztere erfordern große Datenmengen, die wiederum verloren gehen können. So entstehen Risiken, die angesichts der verletzlichen Position der Betroffenen zu hoch sein könnten. Das alles ist umso besorgniserregender angesichts der nicht hinreichenden ethischen Bewertung des Projektes. Dieser Artikel unternimmt den Versuch, eine Debatte über die solchen Forschungsprojekten zugrundeliegenden Wahrnehmungen anzustoßen. Während Technologien immer fortschrittlicher werden, erlangt auch die Gewährleistung der Menschenrechte derer, auf die sie abzielen, eine immer größere Bedeutung.

26 Zoltán Székely, Interview mit der Autorin, 2022
27 Sarah Perret, Interview mit der Autorin, 2022

Röntgentechnik für die Festung Europa

Über die Detektion von Flüchtenden in Fahrzeugen

von Clemens Arzt

Das politische Bestreben, mögliche Fluchtwege nach Deutschland für Menschen immer undurchlässiger zu machen, nimmt in zunehmendem Maße auch technische Möglichkeiten in den Blick, um unkontrollierte Reisebewegungen und Grenzübertritte zu verhindern. Der Beitrag nimmt dabei in jüngerer Zeit untersuchte Technologien in den Blick und versucht, diese rechtlich einzuordnen.

Die Verhinderung der „unkontrollierten" Einreise flüchtender Menschen ist spätestens seit dem Sommer 2015 ein Markenkern der „Festung Europa" und deutscher Politik. Menschen auf der Flucht verstecken sich nicht selten in Kraftfahrzeugen oder Containern. Dabei kommt es auch zu dramatischen Todesfällen. Unter dem Label der Gefahrenabwehr und einer „geregelten Flüchtlingspolitik" untersuchte ein vom Bundesforschungsministerium finanziertes Forschungsprojekt (STRATUM[1]), wie in Fahrzeugen versteckte Menschen schnell und unauffällig aufgespürt (detektiert) werden könnten. Der Beitrag stellt diese Techniken vor und fragt, wie deren Nutzung durch die Polizei rechtlich zu beurteilen ist.[2] Zunächst werden die technischen Methoden zum Aufspüren von Menschen vorgestellt. Gefragt wird sodann, ob sich aus dem europäischen oder Völkerrecht ein Recht auf „unkontrollierte Einreise" ableiten lässt, mit dem solche Detektionsmaßnahmen unvereinbar wären. Anschließend werden die grundrechtlichen und gesetzlichen Rahmenbedingungen solcher Maßnahmen in Deutschland vorgestellt und hinterfragt.

1 www.sifo.de/sifo/shareddocs/Downloads/files/projektumriss_stratum.pdf

2 Erheblich gekürzte und überarbeitete Fassung eines Beitrags von Arzt, C.; Vaudlet, M.; Hofrichter, D.: Technische Detektion von Flüchtlingen in Fahrzeugen durch die Polizei und rechtliche Begrenzungen, in: Die Öffentliche Verwaltung 2022, H. 15, S. 701-711. Dieser Beitrag wird alleine vom Autor verantwortet.

Grundsätzlich kommen für eine polizeiliche Detektion von Menschen in Fahrzeugen verschiedene Ansätze und Technologien in Betracht. Zu nennen sind anlasslose oder anlassbezogene, mobile oder stationäre polizeiliche Maßnahmen. Detektionstechnologien zum Auffinden versteckter Personen in Fahrzeugen können etwa Infrarot-, Radar- und Röntgenstrahlung sowie der Einsatz von CO_2- und Herzschlagdetektoren sein. Weitere sind denkbar. Diese Technologien können in aktive und passive Systeme unterteilt werden, was für die Einschätzung der Eingriffsintensität in die Grundrechte relevant sein kann.

Passiv erfasst etwa die Infrarotdetektion optische Wärmesignaturen, also einen für das menschliche Auge nicht sichtbaren Bereich des elektromagnetischen Spektrums. In der Regel werden hierbei Temperaturen an der Oberfläche von Objekten wie etwa Fahrzeugen gemessen. CO_2-Detektoren können mithilfe eines Sensors den CO_2-Gehalt ihrer Umgebung messen und beispielsweise an einer Sonde in ein Kraftfahrzeug eingeführt werden, um eine Luftprobe zu entnehmen. Damit kann die Anwesenheit von Menschen festgestellt werden. Herzschlagdetektoren nehmen durch den Gebrauch eines oder mehrerer Sensoren oder auch eines Mikrophons die Geräusche und Vibrationen ihrer Umgebung auf und können aus diesen Daten einen gegebenenfalls in einem Fahrzeug von Menschen ausgehenden Herzschlag identifizieren. Alle diese Systeme sind passive Systeme.

Radarsysteme wurden ursprünglich für die Erfassung von Objekten auf große Entfernungen konzipiert. Mittels moderner Siliziumtechnologie wurden komplexe Radarsysteme später in einen MMIC-Chip (Monolithic Microwave Integrated Circuit) integriert. Dies ermöglicht die Entwicklung kleiner und dennoch leistungsfähiger Systeme, welche auch für den mobilen Einsatz Verwendung finden, z. B. für fahrer*innenlose Fahrzeuge.

Bei der Nutzung von Röntgenstrahlung können sogenannte Backscatterverfahren (auch Rückstreuverfahren genannt) und Transmissionsverfahren herangezogen werden. Bei beiden Verfahrensarten wird das zu untersuchende Objekt bzw. die Person aktiv mittels Röntgenstrahlung erfasst. Im Unterschied zum Transmissionsröntgen-Scanner wird im Backscatter-Verfahren das Objekt bzw. die Person nicht „durchleuchtet", sondern es werden die rückgestreuten Photonen zur Bildgebung detektiert. Beide Verfahren stellen aktive Systeme dar.

Recht auf unkontrollierte Einreise?

Bevor über eine mögliche polizeiliche Kontrolle von Fahrzeugen mittels dieser Technologien zum Zwecke der Verhinderung „unkontrollierter" Einreise nachgedacht werden kann, ist zu klären, ob es nicht grundsätzlich ein Recht auf „unkontrollierte Einreise" nach Deutschland ohne staatliche Kontrolle geben könnte. Denn durch ein solches Recht wären Detektionsmaßnahmen zumindest im Grenzraum unzulässig.

Der Europäische Gerichtshof für Menschenrechte (EGMR) und der Gerichtshof der Europäischen Union (EuGH) haben in den vergangenen Jahren mehrfach Urteile hierzu gefällt. So stellte der EGMR im Urteil *N.D. und N.T. gegen Spanien* fest, dass kein Recht auf eine freie Einreise bestehe; im Gegenteil könne sogar ein gewaltsames Zurückdrängen an den Grenzen in Fällen legal sein, in denen Migrant*innen unter Anwendung von Gewalt und auf irreguläre Weise Grenzen passieren wollten, soweit der Staat einen legalen Zugangsweg tatsächlich und wirksam bereitgestellt habe.[3] Dabei betonte der EGMR, dass die Europäische Menschenrechtskonvention (EMRK) generell kein individuelles Asylrecht beinhalte, sondern auf ein menschenrechtliches *Refoulement-Verbot* begrenzt sei, also Menschen nicht in Länder abgeschoben werden dürfen, wo schwere Menschenrechtsverletzungen wie Folter drohen.[4]

Anders legte der Generalanwalt beim EuGH, Paolo Mengozzi, das *Non-Refoulement-Prinzip* aus: Das Zurückweisungsverbot wirke nicht erst an den eigenen Landesgrenzen bei der Einreise, sondern müsse bereits im Herkunftsland oder einem dritten Staat Anwendung finden, wenn im Einzelfall die Voraussetzungen der Gefahr einer unmenschlichen Behandlung vorlägen. Der EuGH hat sich indes dieser Sicht nicht angeschlossen und eine freie Einreise abgelehnt.[5] Der EGMR wiederum bestätigte diese Betrachtung und verwies auf den allgemeinen Grundsatz des Völkerrechts, wonach die Vertragsstaaten der EMRK gemäß ihren vertraglichen Verpflichtungen das Recht auf Kontrolle der Einreise, des Aufenthalts und der Ausweisung von ausländischen Personen haben.[6]

3 EGMR: Urteil v. 13.2.2020 (GK), Nr. 8675/17 und 8697/15, Rn. 155, 201
4 ebd., Rn. 188
5 EuGH: Urteil v. 7.3.2017 (GK), Rs. C-638/16 PPU, Rn. 43
6 EGMR: Beschluss vom 5.5.2020 (GK), Nr. 3599/18, Rn. 124

Die Uneinigkeit der Richter*innen der Großen Kammer könnte andeuten, dass dieses Ergebnis nicht in Stein gemeißelt sein muss.[7] Für die Ausgangsfrage eines „Rechts auf unkontrollierte Einreise" und damit eines möglichen Verbots der untersuchten Detektionsmaßnahmen muss indes zum jetzigen Zeitpunkt festgehalten werden, dass ein solches Recht sich aus der Rechtsprechung von EGMR und EuGH wohl nicht herleiten lässt.

Eine weitere Möglichkeit der Herleitung eines solches Rechts auf unkontrollierte Einreise könnte jedoch der so genannte Schengener Grenzkodex (SGK) bieten.[8] Ein Grundsatz dieses Regelwerks ist, dass das Überschreiten der Binnengrenzen der teilnehmenden EU-Mitgliedstaaten und einiger weiterer Staaten innerhalb des sogenannten Schengen-Raums an jeder Stelle von jeder Person unabhängig von deren Staatsangehörigkeit erfolgen kann. Grenzkontrollen finden dort mithin (im Regelfall) nicht statt, wobei dieser Grundsatz seit Jahren nicht zuletzt von Deutschland untergraben wird. Art. 23 Buchstabe a Satz 1 SGK gestattet jedoch

> „die Ausübung der polizeilichen Befugnisse durch die zuständigen Behörden der Mitgliedstaaten nach Maßgabe des nationalen Rechts, sofern die Ausübung solcher Befugnisse nicht die gleiche Wirkung wie Grenzübertrittskontrollen hat."

Nach Art. 2 Nr. 11 SGK wird eine Kontrolle dann als Grenzübertrittskontrolle angesehen, wenn sie an den Grenzübertrittsstellen mit dem Ziel erfolgt, festzustellen, ob die betroffenen Personen in das jeweilige Hoheitsgebiet der Mitgliedstaaten ein- oder ausreisen dürfen. Auch aus dem SGK kann dabei nach heute wohl vorherrschender Meinung kein absolutes „Recht auf unkontrollierte Einreise" abgeleitet werden. Die Voraussetzungen einer zulässigen polizeilichen Kontrolle sind jedoch klar vorgegeben und eng abgesteckt, was z. B. hinsichtlich *racial profiling* bei solchen Kontrollen in Deutschland intensiv diskutiert wird.

Technische Detektionsmaßnahmen und Grundrechte

Ein Einsatz der hier betrachteten Detektionstechnologien führt zu einem Eingriff in die Grundrechte der betroffenen Personen. Grundsätzlich verlangt ein Grundrechtseingriff, dass er auf einer verfassungsmäßig zulässigen (polizeilichen) „Eingriffsbefugnis" in Gesetzesform beruht. Im Zentrum der technischen Detektion steht der Eingriff in das Grundrecht auf

7 vgl. Czech, P.: Entscheidungsanmerkung, in: Newsletter Menschenrechte 2020, H. 3, S. 168-169

8 Verordnung (EU) 2016/399 des Europäischen Parlaments und des Rates vom 9.3.2016

informationelle Selbstbestimmung (RiS) aus Art. 2 Abs. 1 GG in Verbindung mit Art. 1 Abs. 1 GG. Eingriffe in die körperliche Unversehrtheit aus Art. 2 Abs. 2 Satz 1 GG kommen insbesondere bei Nutzung aktiver Detektionssysteme in Betracht. Im Einzelfall kann auch ein Eingriff in die Religionsfreiheit aus Art. 4 GG vorliegen.

Das Grundrecht auf informationelle Selbstbestimmung schützt gegen die unbegrenzte und unbegründete staatliche Erhebung, Speicherung, Nutzung oder Weitergabe persönlicher Daten. Jede Person soll demnach grundsätzlich selbst über die Preisgabe und Verwendung ihrer persönlichen Daten bestimmen können. Dies gilt insbesondere, wenn personenbezogene Informationen seitens der Polizei in einer Art und Weise genutzt und verknüpft werden können, die Betroffene weder überschauen noch beherrschen können.[9] Dies ist der Regelfall bei einer polizeilichen Datenverarbeitung.

Werden Daten über den Aufenthalt oder die Anwesenheit einer Person in einem Fahrzeug erhoben, stellt dies einen Eingriff in das RiS dar, soweit ein Bezug zwischen dieser Person, ihrem Aufenthaltsort zu einem bestimmten Zeitpunkt und ihrer Reise hergestellt werden kann, was über die nach einer „Entdeckung" stattfindende Identitätsfeststellung gegeben ist. Diese Feststellung gilt für alle oben vorgestellten Technologien. Auch eine CO_2- oder Herzschlagdetektion soll letztlich personenbezogene Daten über die Anwesenheit in einem Fahrzeug liefern. Informationen über den Gesundheitszustand der Betroffenen lassen sich hieraus indes im Regelfall wohl nicht generieren.

Als besonders problematischer Grundrechtseingriff kommt zudem ein Eingriff in das durch Art. 2 Abs. 2 Satz 1 GG geschützte Recht auf körperliche Unversehrtheit durch den Einsatz von Röntgenstrahlung in Betracht. Hiervon ist, wie im Folgenden noch ausgeführt wird, bei Verwendung des Transmissionsröntgens auszugehen. Aber auch der Einsatz eines Röntgen-Backscatters zur Detektion dürfte zu einem Eingriff in das Recht auf körperliche Unversehrtheit[10] führen und ist nach geltendem Strahlenschutzrecht unzulässig. Im Einzelfall könnte die Detektion auch

9 vgl. Bundesverfassungsgericht: Urteil v. 15.12.1983, Az.: 1 BvR 209/83; s.a. Fährmann, J.; Aden, H.; Arzt C.: Transparenz der polizeilichen Datenverarbeitung: Defizite und technische Lösungsansätze, in: Friedewald u.a. (Hg.): Selbstbestimmung, Privatheit und Datenschutz – Gestaltungsoptionen für einen europäischen Weg, Wiesbaden 2022, S. 303-325

10 vgl. Michel, R.: Nicht medizinische Bildgebung. Ein Überblick, in: Fachverband Strahlenschutz Praxis 2016, H. 1, S. 5-11, www.fs-ev.org/fileadmin/user_upload/05_SSP/Probeartikel/Probeartikel_2016_1.pdf

zu einem Eingriff in das Grundrecht der Religionsfreiheit aus Art. 4 Abs. 1 GG führen, soweit etwa religiöse Bekleidungsvorschriften bestehen, deren Ziel technisch „umgangen" werden kann.

Aus Gründen der Verhältnismäßigkeit wäre beim Einsatz jedweder Detektionstechnologie darauf zu achten, dass im Falle einer rechtlichen Zulassung nur solche Maßnahmen umgesetzt werden, die möglichst wenig in die Rechte der Betroffenen eingreifen.

Röntgentechnologie als Mittel polizeilicher Maßnahmen?

Das Strahlenschutzgesetz (StrlSchG) regelt die Anwendung ionisierender Strahlung oder radioaktiver Stoffe am Menschen. Auch wenn im hier untersuchten Szenario der Einsatz der Röntgenstrahlung an einem Fahrzeug erfolgt, liegt dahinter die Absicht, Menschen aufzuspüren. Nach § 83 Abs. 1 Nr. 2 StrlSchG kommt ein Einsatz von Röntgenstrahlung zur Detektion von Menschen jedoch nur in Betracht, wenn er zur „Untersuchung einer Person in durch Gesetz vorgesehenen oder zugelassenen Fällen" erfolgt. Damit ist der Einsatz von Transmissionsröntgen als auch von Backscattern zur polizeilichen Detektion von Personen strahlenschutzrechtlich (derzeit) in Deutschland nicht zulässig, unabhängig von einer Bewertung der möglichen Strahlendosis.

Die Richtlinie 2013/59/Euratom regelt in Art. 22 Anforderungen, wann Menschen zwecks nicht-medizinischer Bildgebung radioaktiver Strahlung ausgesetzt werden dürfen. Durch einen Verweis auf Anhang V ist der Einsatz ionisierender Strahlung zur Ermittlung verborgener Personen bei der Frachtkontrolle grundsätzlich gestattet. Es bestehen indes zwei wichtige Einschränkungen: Art. 22 Abs. 4 Buchstabe d der Richtlinie schreibt vor, dass, „bei Verfahren, bei denen keine medizinisch-radiologischen Ausrüstungen zum Einsatz kommen, die Dosisrichtwerte deutlich unter den Dosisgrenzwerten für Einzelpersonen der Bevölkerungen liegen" müssen. Zudem muss die betroffene Person nach Art. 22 Abs. 4 Buchstabe e der Richtlinie grundsätzlich „informiert ... und ihre Einwilligung eingeholt" werden. Bei der Einwilligung handelt es sich um eine Erklärung, die im Vorfeld der Maßnahme erteilt werden muss.

Eine Ausnahme vom Erfordernis der Einwilligung des Betroffenen in den Einsatz ist nach der letztgenannten Regelung jedoch möglich, wenn „Strafverfolgungsbehörden nach den nationalen Rechtsvorschriften auch ohne die Einwilligung der betreffenden Person tätig werden dürfen".

Doch diese Ausnahme beschränkt sich auf die Strafverfolgung, also repressiv-polizeiliche Einsätze und erfordert für Deutschland eine ausdrückliche Regelung in der Strafprozessordnung (StPO), die (bisher) nicht existiert. Im Falle eines präventiv-polizeilichen Einsatzes von Röntgentechnologien zur Gefahrenabwehr kann hingegen auf eine Einwilligung in keinem Falle nicht verzichtet werden.

Zu den hohen Anforderungen an eine Einwilligung bei Datenerhebungen lohnt auch ein Blick in § 51 Bundesdatenschutzgesetz. Er verlangt eine eigene Rechtsvorschrift, die gestattet, eine polizeiliche Datenerhebung auf eine freiwillige Einwilligung zu stützen, und diese ist nur wirksam, wenn sie auf der freien Entscheidung der betroffenen Person beruht.

Andere Technologien als Mittel polizeilicher Maßnahmen

Auch der Einsatz von Infrarot- und Radargeräten sowie von CO_2- und Herzschlagdetektoren bedürfte einer speziellen polizeilichen Eingriffsbefugnis. Denkbar wäre es, die technische Detektion als Durchsuchung einer Sache anzusehen, etwa nach § 35 Allgemeines Sicherheits- und Ordnungsgesetz (ASOG) Berlin und § 102 StPO. Dabei wird in einer Sache nach etwas gesucht mit dem Ziel, etwas nicht offenkundig Sichtbares bzw. Verborgenes aufzudecken.[11] Bei der Detektion findet jedoch keine aktive Suche in oder an einer Sache statt. Vielmehr soll mittels Technikeinsatz die räumliche Begrenzung eines Fahrzeugs „durchbrochen" werden. Im technischen Sinne handelt es sich also um eine „Durchleuchtung". Während sich semantisch der Begriff Durchleuchten als Mittel erklären lässt, um einen Körper zu durchdringen, um das Innere zum Zweck einer Prüfung, Untersuchung sichtbar zu machen,[12] kann der Begriff „Durchsuchung" umschrieben werden als „in etwas gründlich suchen, um etwas oder jemanden zu finden" bzw. als „in jemandes Kleidung nach etwas, was er verborgen halten könnte, suchen".[13] Auch ein Vergleich zu § 5 Abs. 1 Satz 2 Luftsicherheitsgesetz (LuftSiG) macht diesen Unterschied deutlich, da dieser die Begriffe der Durchsuchung und Durchleuchtung alternativ benutzt und somit eine (rechtliche) Unterscheidung der beiden Vorgänge trifft.[14]

---

11 vgl. etwa Bundesverwaltungsgericht: Urteil v. 6.9.1974, Az.: I C 17.73, S. 37

12 vgl. Duden: www.duden.de/rechtschreibung/durchleuchten_pruefen_untersuchen

13 vgl. Duden: www.duden.de/rechtschreibung/durchsuchen_kontrollieren_durchsehen

14 Buchberger, E.: LuftSiG § 5 Rn. 7, in: Schenke, W.-R. u.a. (Hg.): Sicherheitsrecht des Bundes, München 2019

Die Detektion kann auch klar von der polizeilichen Nutzung von Bild- und Tonaufzeichnungsgeräte unterschieden werden. Detektionstechnologien wie etwa Infrarot oder Radar nehmen nicht einfach die äußere Erscheinung eines Gegenstandes als Bild auf, sondern die äußere Hülle eines Fahrzeuges wird im Rahmen der Detektion je nach Technologie „durchdrungen", um das Innere eines Fahrzeuges sichtbar zu machen oder Lebenszeichen dort zu verorten.

Auch eine Anwendung der rechtlichen Regelungen zum Einsatz „technischer Mittel", wie beispielsweise in § 25 Abs. 1 Satz 1 Nr. 2 ASOG oder § 100h Abs. 1 Satz 1 Nr. 2 StPO, ist nicht möglich. Denn z. B. § 100h StPO stellt auf einen Observationszweck ab, das technische Mittel muss also zur Beobachtung einer Person und ihres Verhaltens oder eines Objekts eingesetzt werden, was hier nicht gegeben ist.

Insgesamt fehlt es damit bis dato an einer Eingriffsbefugnis für den Einsatz von Infrarot- und Radargeräten oder CO_2- und Herzschlagdetektoren zum Aufspüren von Menschen in Fahrzeugen im Straßenverkehr.

Ausblick und Anforderungen

Aus bürgerrechtlicher Sicht ist zu befürchten, dass die Polizeien der Länder und des Bundes ähnlich wie im Falle der polizeilichen Drohnendetektion und -abwehrversuchen werden, einen Einsatz von Detektionstechnologien möglichst lange einer spezialgesetzlichen Regelung mit dem Argument zu „entziehen", dass diese bereits auf vorhandene Eingriffsbefugnisse gestützt werden könne oder es sich nur um Tests handele.[15] Der vorliegende Artikel hat jedoch dargelegt, dass gegenwärtig eine polizeiliche Eingriffsbefugnis fehlt. Hielte man Maßnahmen zur Detektion geflüchteter Menschen für ethisch vertretbar, bedürfte es demnach neuer, hinreichend bestimmter und verhältnismäßiger polizeilicher Eingriffsbefugnisse zur Abwehr *konkreter Gefahren im Einzelfall.*

Eine Zulässigkeit allein zur *Verhütung* von mit der illegalen Einreise verbundenen *Straftaten* nach dem Ausländerrecht ist mit Blick auf die dafür notwendigen anlasslosen Kontrollen einer Vielzahl von Straßennutzer*innen (beispielsweise bei Einsatz auf Autobahn- oder Mautbrücken) und auch mit Blick auf die Maßgaben des Schengener Grenzkodex nicht vertretbar, zumal im Falle eines Anfangsverdachtes auf herkömmliche

15 vgl. Arzt, C.; Fährmann, J.; Schuster, S.: Polizeiliche Drohnenabwehr, Detektion, Verifikation, Intervention - Grundrechtseingriffe und Eingriffsbefugnisse, in: Die Öffentliche Verwaltung 2020, H. 19, S. 866-877

Kontrollen des Fahrzeugs nach dem Strafprozessrecht zurückgegriffen werden kann. Ein Einsatz von Röntgenstrahlung ist nach geltendem Recht aus Gründen des Strahlenschutzes in allen Fällen unzulässig.

Was wäre nun notwendig, um überhaupt in diesem Rahmen verfassungsmäßige Eingriffsgrundlagen zu schaffen? Erforderlich wäre insbesondere beim zeitgleichen Einsatz mehrerer unterschiedlicher Detektionstechnologien vorab zunächst eine Datenschutzfolgeabschätzung im Sinne des § 67 Bundesdatenschutzgesetz respektive der einschlägigen landesgesetzlichen Regelungen und des Art. 27 der so genannten JI-Datenschutzrichtlinie der EU. Eine solche „präventive Selbstkontrolle" soll dem Ziel der Datenminimierung[16] dienen und ist ein „zentrales Element der strukturellen Stärkung des Datenschutzes".[17] Dies geschieht bisher bei der Einführung neuer polizeilicher Einsatzmittel allenfalls im Ausnahmefall.

Darüber hinaus könnte zukünftig im Wege einer „Überwachungsgesamtrechnung"[18] jede neue polizeiliche Eingriffsmaßnahme in ein Gesamtbild der Überwachung von Menschen durch Polizeien und Nachrichtendienste eingefügt und kritisch hinterfragt werden. Dabei wird auf eine „grundsätzliche, objektive gesamtgesellschaftliche Überwachungsdichte"[19] abgestellt, d. h., dass die „Summe" bereits bestehenden Überwachungsbefugnisse bei der Bewertung neu zu schaffender Eingriffsbefugnisse begrenzend Berücksichtigung findet, so die Hoffnung der Anhänger*innen dieses Ansatzes. Ob dieses Kalkül aufgeht, bleibt abzuwarten.

Die lange Liste polizeilicher Befugniserweiterungen seit dem Angriff auf das New Yorker World Trade Center am 11. September 2001 und dem Anschlag auf dem Berliner Breitscheidplatz im Jahr 2016 lässt indes wenig Hoffnung auf eine Rückbesinnung auf das Konzept eines freiheitlichen, sich selbst begrenzenden Rechtsstaates aufkommen, in dem die *rule of law* statt *rule by law* auf der Agenda steht.

16 Nolte, N.; Werkmeister, C.: § 67 Rn. 1, in: Gola, P.; Heckmann, D. (Hg.): Bundesdatenschutzgesetz, München 2019

17 BT-Drs. 18/11325 v. 24.2.2017, S. 117

18 vgl. Roßnagel, A.: Die „Überwachungs-Gesamtrechnung" – Das BVerfG und die Vorratsdatenspeicherung, in: Neue Juristische Wochenzeitschrift 2010, H. 18, S. 1238-1242

19 Knierim, A.: Kumulation von Datensammlungen auf Vorrat, in: Zeitschrift für Datenschutz 2011, H. 1, S. 17-22

Warnungen aus Großbritannien

Zunehmende Überwachung von Migrant*innen

von Lucie Audibert

Seit 10 Jahren strebt die britische Regierung danach, Menschen, die nach Großbritannien einwandern, im Rahmen der Politik der „feindlichen Umgebung" das Leben so unangenehm wie möglich zu machen. Neben vielen anderen Instrumenten und Praktiken werden dazu neuen Technologien und die Daten der Menschen genutzt. Die Beschlagnahmung von Handys und die GPS-Ortung sind zwei eindrucksvolle Beispiele. Dieser Artikel diskutiert, wie die Instrumente unter menschenrechtlicher Perspektive infrage gestellt und angegangen werden können.

Vor zehn Jahren kündigte in Großbritannien die damalige Innenministerin Theresa May die Strategie einer „feindlichen Umgebung" an, um die sogenannte „illegale Einwanderung" zu bekämpfen.[1] Durch das Schaffen von Hindernissen für Migrant*innen beim Zugang zu grundlegenden Rechten und Gütern wie Arbeit, öffentlichen Dienstleistungen oder Bankkonten hoffte die Regierung, diese von der Einreise abzuhalten und zur freiwilligen Ausreise zu bewegen. Es wurden Strategien und Praktiken angewendet, die Familien auseinanderreißen,[2] Menschen davon abhalten, notwendige medizinische Versorgung in Anspruch zu nehmen,[3] Kindern den Zugang zu kostenlosem Schulessen oder sogar den Schulbesuch

1 Theresa May Interview: 'We're going to give illegal migrants a really hostile reception', www.telegraph.co.uk v. 25.5.2012

2 „Hostile environment": the hardline Home Office policy tearing families apart, www.theguardian.com v. 28.11.2017

3 Medact: Patients Not Passports: Challenging healthcare charging in the NHS – Updated, London 2020, www.medact.org/wp-content/uploads/2020/10/Patients-Not-Passports-Challenging-healthcare-charging-in-the-NHS-October-2020-Update.pdf

grundsätzlich verwehren oder Opfer von Straftaten davon abhalten, sich bei der Polizei zu melden, weil sie Abschiebung fürchten.[4]

Diese Maßnahmen basieren auf der Annahme, dass Migrant*innen nicht die gleichen Menschenrechte und den gleichen Schutz wie Staatsbürger*innen verdienen. Dies zeigt sich im unerbittlichen Einsatz invasiver Überwachungs- und Kontrollmaßnahmen, die gleichzeitig in rechtstaatliche Garantien eingreifen und Menschenrechtsgarantien vorenthalten. Die britische Regierung bereitete sich sogar darauf vor, durch die Verabschiedung einer sogenannten „Einwanderungsausnahme" im Datenschutzgesetz von 2018 von den regulären Datenschutzverpflichtungen gemäß der EU-Datenschutzgrundverordnung (EU-DSGVO) abzuweichen. Dadurch werden Migrant*innen einige Schutzrechte verweigert, wenn ihre Daten für den Aufenthaltsstatus verarbeitet werden. Obwohl eine gerichtliche Anfechtung der Ausnahmeregelung erfolgreich war,[5] bleibt diese für Migrant*innen grundsätzlich in Kraft und wurde lediglich durch zusätzliche Garantien ergänzt.

In diesem Artikel werden zwei Beispiele der in Großbritannien gegen Migrant*innen eingesetzten Überwachungsmaßnahmen untersucht: die Beschlagnahmung von Handys samt Datenauslesung und die GPS-Ortung. Wir werden die damit verbundenen Technologien und ihre Auswirkungen auf die Betroffenen untersuchen und beurteilen, wie diese unter menschenrechtlichen Gesichtspunkten angefochten werden können und angefochten werden.

Beschlagnahmung von Handys und Datenauslesung

Heutzutage beinhalten Handys (insbesondere die weit verbreiteten Smartphones) mehr gespeicherte Informationen über das Privatleben einer Person als es bisher für digitale Geräte möglich war. Im Zuge der technologischen Entwicklungen sammeln Mobiltelefone immer mehr unterschiedliche und intime Informationen, etwa private Gespräche, tägliche Gesundheitsdaten, Browserverläufe, Finanzdaten, intime Bilder, GPS-Standortdaten usw. Die britische Datenschutzbehörde (der Information Commissioner oder ICO) stellte in einem Bericht über die Erfassung von

4 Bradley, G.M.: Care Don't Share, London 2018, www.libertyhumanrights.org.uk/wp-content/uploads/2020/02/Liberty-Care-Dont-Share-Report-280119-RGB.pdf.

5 England and Wales Court of Appeal: Entscheidung v. 26.5.2021, Az.: [2021] EWCA Civ 800, www.bailii.org/ew/cases/EWCA/Civ/2021/800.html

Mobiltelefonen durch die Polizei in England und Wales fest: „Heutzutage betrachten Menschen Mobiltelefone als Erweiterungen ihrer selbst; sie sind zu einzigartigen Speichern unserer persönlichen Informationen geworden, generieren riesige Datenmengen und sind oft Träger intimster und privatester Details unseres Alltagslebens." [6]

Polizeibehörden verschiedener Länder machen sich daher in den letzten Jahren diesen beispiellosen Fundus an potentiellen Beweismitteln zu Nutze. Verschiedene Unternehmen haben Programme zur Datenauslesung entwickelt.[7] Wie so oft, wenn Behörden neue Technologien einsetzen, fehlen auch in Großbritannien der rechtliche Rahmen sowie Sicherheitsvorkehrungen, um Datenmissbrauch zu verhindern und die Einhaltung von Menschenrechten und Datenschutzgesetzen zu gewährleisten.[8]

Beschlagnahmung von Mobiltelefonen an der Grenze

Im Jahr 2020 stellten Anwält*innen von Asylsuchenden fest, dass bei der Ankunft britische Einwanderungsbeamt*innen von einigen ihrer Mandant*innen die Telefone beschlagnahmten und diese nie oder erst nach Monaten zurückgegeben wurden. Nachdem Gerichtsverfahren eingeleitet worden waren, um die Rechtmäßigkeit der Beschlagnahmungen zu prüfen und die Wiedererlangung der Handys zu erwirken, stellte sich heraus, dass das Innenministerium zwischen April und November 2020 pauschal die Handys aller Migrant*innen, die in kleinen Booten Großbritannien erreichten, beschlagnahmen ließ. Sie sollten zur Herausgabe ihrer PIN-Nummern gezwungen werden und erhielten nur sehr begrenzte Informationen darüber, was mit ihren Handys und den darin enthaltenen Daten geschehen würde.

Dieser Fall führte zu einer Anfechtung der zugrundeliegenden systematischen Politik und Praxis des Innenministeriums. In den erstrittenen Offenlegungen von Dokumenten zeigte auch, dass die aus den Handys extrahierten Daten mit anderen Behörden ausgetauscht und analysiert wurden. Die Einwanderungsbehörden und die National Crime Agency lu-

6 ICO: Mobile Phone Data Extraction by Police Forces in England and Wales, 2020, https://ico.org.uk/media/about-the-ico/documents/2617838/ico-report-on-mpe-in-england-and-wales-v1_1.pdf

7 Privacy International: Digital stop and search: how the UK police can secretly download everything from your mobile phone, London 2018, https://privacyinternational.org/sites/default/files/2018-03/Digital%20Stop%20and%20Search%20Report.pdf

8 ICO a.a.O. (Fn. 6)

den die Daten von allen beschlagnahmten Handys herunter. Sie „wuschen" diese in behördenübergreifenden Datenbanken, um ihre Spuren zu vertuschen und relevante Informationen zu identifizieren und zu analysieren.

Die Wegnahme ihrer Handys bringt Asylbewerber*innen in eine Notlage. Telefone sind oft die letzte Verbindung zu ihrem Herkunftsland und ihren Lebenserinnerungen sowie die einzige Möglichkeit, mit ihrer Familie, ihren Freund*innen und ihren Anwält*innen Kontakt aufzunehmen und ihre behördlichen Verfahren zu bearbeiten. Da die Asylbewerber*innen zudem kaum oder gar nicht über den Zweck der Beschlagnahmung informiert wurden, bestand zudem Unsicherheit darüber, was die Einwanderungsbehörde aus den Daten herauslesen würde und ob dies Auswirkungen auf ihre Einwanderungsanträge haben könnte.

Weitverbreitete Rechtswidrigkeit

Das Innenministerium räumte im Laufe des Verfahrens schließlich ein, dass die Beschlagnahmungen aufgrund ihres pauschalen Charakters rechtswidrig sind (d. h. die Durchsuchungen und Beschlagnahmungen erfolgten nicht auf der Grundlage einer individuellen Bewertung der Wahrscheinlichkeit, dass das Handy Beweise für Einwanderungsdelikte enthält) und dass die Einbehaltung von Telefonen, die Datenauslesepolitik und die Anweisung, PIN-Nummern anzugeben, nicht mit dem Recht auf Privat- und Familienleben gemäß Artikel 8 der Europäischen Menschenrechtskonvention (EMRK) oder dem Data Protection Act 2018 vereinbar sind. Eine Intervention von dritter Seite durch die Menschenrechtsorganisation Privacy International zeigte mittels technischer Beweise auf, dass die auf Handys gespeicherten Datenmengen und die dem Innenministerium zur Verfügung stehenden Analysetechnologien eine noch nie dagewesene Eingriffsmöglichkeit in das Privatleben der Kläger*innen schuf.[9]

Das britische Berufungsgericht (High Court) urteilte daher, dass „die Beschlagnahme und Einbehaltung der Mobiltelefone der Kläger*innen die Rechte der Kläger*innen nach Artikel 8 verletzte, da der Eingriff in diese Rechte nicht im Sinne von Artikel 8 Absatz 2 gerechtfertigt werden kann".

9 Privacy International: PI intervenes in judicial review to support asylum seekers against the UK Home Secretary's seizure and extraction of their mobile phones v. 31.1.2022, https://privacyinternational.org/news-analysis/4782/pi-intervenes-judicial-review-support-asylum-seekers-against-uk-home-secretarys

Das Gericht stellte ferner fest, dass „die Erlangung des Zugangs zu privatem Material durch die Forderung nach den PIN-Nummern der Telefone ohne jede rechtmäßige Befugnis und die Androhung von Strafverfolgung einer nicht existierenden Straftat zur Durchsetzung der Forderung ein weiterer eindeutiger Eingriff in die Rechte der Kläger*innen nach Artikel 8 war".[10]

In einem weiteren Urteil, welches sich einige Monate später[11] mit den verbleibenden Fragen des Falles befasste, erließ das Berufungsgericht die bedeutende und ungewöhnliche Anordnung, auch jene Tausende von Migrant*innen, die von der rechtswidrigen Politik betroffen, aber nicht direkt am Fall beteiligt waren, zu entschädigen.[12] Das Gericht verpflichtete das Innenministerium, „alle angemessenen Anstrengungen" zu unternehmen, um jede Person, die der Meinung der Behörde nach einer rechtswidrigen Durchsuchung und/oder Beschlagnahmung eines Handys ausgesetzt war, über die Existenz des Urteils und ihr Recht auf Rechtsmittel zu informieren.

Abhilfe oder Wiedergutmachung sind beim Rechtsschutz für Menschen, die von Menschenrechtsverletzungen betroffen sind, häufig übersehene Aspekte, da sich die Urteile i. d. R. auf die Feststellung von Verstößen konzentrieren, die Betroffenen aber ohne konkrete Abhilfe zurücklassen [13] Dieser Fall verdeutlicht, wie Gerichte versuchen können, Regierungen für die schädlichen Folgen ihrer Politik zur Rechenschaft zu ziehen, indem sie von ihnen – auch für Hunderte oder Tausende vergangene Menschenrechtsverletzungen – verlangen, Wiedergutmachung zu leisten. Der Fall ist auch ein Beispiel für die Schwierigkeiten, systematische Verfehlungen vor Gericht zu bringen, da das Innenministerium während des gesamten Verfahrens immer wieder argumentierte, dass die Anfechtungsgründe der Kläger theoretischer Natur seien, da die praktischen Fragen

10 England and Wales High Court: Entscheidung v. 25.2.2022, Az.: [2022] EWHC 695 (Admin), § 135, www.bailii.org/ew/cases/EWHC/Admin/2022/695.html

11 England and Wales High Court: Entscheidung v. 14.10.2022, Az.: [2022] EWHC 2729 Admin, www.bailii.org/ew/cases/EWHC/Admin/2022/2729.html

12 Privacy International: UK High Court orders groundbreaking redress for thousands of migrants affected by unlawful phone seizures and data extraction v. 18.11.2022, https://privacyinternational.org/news-analysis/4987/uk-high-court-orders-groundbreaking-redress-thousands-migrants-affected-unlawful

13 European Court of Human Rights: Guide on Article 13 of the European Convention on Human Rights – Right to an effective remedy, 2022, www.echr.coe.int/documents/guide_art_13_eng.pdf

bereits geklärt seien. Immer wieder verliert das Innenministerium aber auch derartige Klagen gegen seine Behandlung von Asylbewerber*innen.[14]

GPS-Überwachung

Die elektronische Überwachung ist in vielen Ländern der Welt seit langem fester Bestandteil des Strafrechtssystems, i. d. R. zur Überwachung von aus der Haft entlassenen Personen oder zur Überwachung der Einhaltung von Kautionsauflagen.[15] Im Rahmen der technologischen „Innovation" auf dem strafjustiziellen Technologiemarkt wurde die herkömmliche Funkfrequenz-Überwachung (wobei die Entfernung zwischen einem Sender und einer Basisstation gemessen wird, die sich meist in der Wohnung der zu überwachenden Person befindet) durch die Nutzung von GPS-Tracking oder tragbaren Geräten, die den genauen GPS-Standort der jeweiligen Person rund um die Uhr überwachen können, abgelöst.[16]

Die erfassten GPS-Standortdaten werden als „Spurdaten" bezeichnet. Untersuchungen der Menschenrechtsorganisation Privacy International zeigen, dass es sich aufgrund ihres Umfangs und ihrer Detailgenauigkeit um hoch sensible Daten handelt, die „tiefe Einblicke in intime Details des Lebens einer Person gewähren, die ein umfassendes Bild der alltäglichen Gewohnheiten und Bewegungen, des ständigen oder vorübergehenden Wohnorts, der Hobbys und anderer Aktivitäten, der sozialen Beziehungen, der politischen, religiösen oder weltanschaulichen Interessen, der gesundheitlichen Belange, des Konsumverhaltens usw. offenbaren".[17]

---

14 A reprehensible way to behave: Crises mount up at the Home Office', www.independent.co.uk v. 2.1.2023

15 Audibert, L.; Bhatia, M.: From GPS tagging to facial recognition watches: expanding the surveillance of migrants in the UK, Institute of Race Relations v. 26.2.2022, https://irr.org.uk/article/from-gps-tagging-to-facial-recognition-watches-expanding-the-surveillance-of-migrants-in-the-uk

16 Privacy International: Electronic monitoring using GPS tags: a tech primer v. 9.2.2022, https://privacyinternational.org/explainer/4796/electronic-monitoring-using-gps-tags-tech-primer

17 Privacy International: Submission to the Information Commissioner – Request for assessment of processing operations by the Secretary of State for the Home Department („Home Office") v. 17.8.2022, https://privacyinternational.org/sites/default/files/2022-08/2022.08.17%20-%20Privacy%20International%20complaint%20against%20Home%20Office%20use%20of%20GPS%20Ankle%20Tags%20%5Bpublic%20version%5D.pdf

Im Jahr 2021 begann das Innenministerium mit dem Einsatz von GPS-Tracking zur elektronischen Überwachung von Personen, die gegen Kaution aus dem Asylgewahrsam entlassen wurden[18] – eine der Bedingungen, die gemäß Schedule 10 des Immigration Act 2016 für die Entlassung aus dem Asylgewahrsam gestellt werden können. Beim GPS-Tracking können Standortdaten mit unterschiedlicher Häufigkeit oder in unterschiedlichen Intervallen erfasst werden, z. B. jede Minute, alle 15 Minuten, alle 30 Minuten oder einmal in der Stunde, was sehr unterschiedliche Auswirkungen auf die Menge und Detailgenauigkeit Spurdaten hat. Anwält*innen, die überwachte Personen vertreten, haben darauf hingewiesen, dass das vom Innenministerium verwendete GPS-Tracking so eingestellt ist, dass Standortdaten einmal pro Minute erfasst werden.

Pauschaler Einsatz ohne individuelle Bewertung

Die Gesetzgebung, die eine elektronische Überwachung von Migrant*innen durch das Innenministerium ermöglicht, beinhaltet die ungewöhnliche „obligatorische Pflicht" zur elektronischen Überwachung von Personen, die von einer Abschiebung oder einem Abschiebungsverfahren betroffen sind (Schedule 10 § 2(3)(a)). Damit wurde der richterliche Ermessensspielraum und die richterliche Aufsicht faktisch abgeschafft, sodass die Entscheidung einer Anordnung über eine elektronische Überwachung nicht auf einer Bewertung der Notwendigkeit beruht, eine bestimmte Person zu überwachen. Das Innenministerium unternimmt währenddessen keinen Versuch, die Notwendigkeit und Verhältnismäßigkeit des Einsatzes auf individueller Basis zu begründen, wie in einer Reihe von Klagen von Einzelpersonen gegen ihre GPS-Tracking vor Gericht festgestellt wurde.[19]

Das Innenministerium scheint auch wenig bis gar keine Rücksicht auf die persönlichen Umstände der Betroffenen zu nehmen; so versuchte es etwa, GPS-Tracking bei schutzbedürftigen Personen und/oder Überlebenden von Menschenhandel und Folter durchzusetzen.[20] Forschungen von

18 Bail for Immigration Detainees: BID's Briefing on Electronic Monitoring, 24 March 2021, www.biduk.org/articles/805-bid-s-briefing-on-electronic-monitoring

19 Dunan Lewis.: Duncan Lewis challenges the use of 24/7 GPS tracking by the Home Office v. 26.10.2022, www.duncanlewis.co.uk/immigration_news/Duncan_Lewis_challenges_the_use_of_247_GPS_tracking_by_the_Home_Office_(26_October_2022).html

20 Another blow to Home Office as Rwanda asylum seekers not tagged on release from detention, www.independent.co.uk v. 11.7.2022

Migrant*innenrechtsorganisationen und Ärzt*innen haben aufgezeigt, dass das GPS-Tracking „erhebliche psychologische und physische Leiden" verursacht, darunter Angst, Schmerzen, Re-Traumatisierung, das Gefühl der sozialen Stigmatisierung, Schlaf- oder Beziehungsprobleme.[21]

War die Methodik ursprünglich auf Gruppen von „sehr gefährlichen Straftäter*innen" beschränkt, hat das Innenministerium nun im Rahmen eines im Juni 2022 veröffentlichten Pilotprojekts das GPS-Tracking auf Personen ausgeweitet, die auf „unnötigen und gefährlichen Wegen" nach Großbritannien kommen.[22] Die einzige Begründung, die der damalige Premierminister Boris Johnson für die signifikante Ausweitung der Maßnahmen anführte, war, dass man sicherstellen wolle, dass Menschen, die ins Land kommen, nicht aus dem System „verschwinden".[23] Dass jedoch nur etwa ein Prozent der aus dem Asylgewahrsam entlassenen Personen untertauchen, stellt die Notwendigkeit und Verhältnismäßigkeit der Maßnahme erneut in Frage.

Schleichende Funktionsausweitung

In verschiedenen Iterationen seiner „Immigration Bail policy" hat das Innenministerium die Gründe dargelegt, aus denen es auf Spurdaten zugreifen und diese überprüfen kann. Einige dieser Gründe sind eindeutige Beispiele für eine „schleichende Funktionsausweitung", ein häufig zu beobachtendes Phänomen, bei dem eine Technologie über den ursprünglich vorgesehenen Zweck hinaus verwendet wird – und in diesem Fall über das hinausgehend, was die Gesetzgebung vor Augen hatte.[24]

Einer dieser Gründe ist die Verwendung der GPS-Standortdaten von Personen, um fundierte Entscheidungen über ihre Einwanderungsanträge zu treffen: „Im Falle des Erhalts von Anträgen nach Artikel 8 oder weiteren Eingaben von Einzelpersonen können befugte Mitarbeiter*innen des

21 Bail for Immigration Detainees: Research reveals „inhumane" effects of GPS tagging on migrants v. 31.10.2022), www.biduk.org/articles/research-reveals-inhumane-effects-of-gps-tagging-on-migrants

22 Home Office: Immigration bail conditions: Electronic monitoring (EM) expansion pilot, Version 1.0 v. 15.6.2022, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1082956/Immigration_bail_conditions_-_Electronic_Monitoring__EM__Expansion_pilot.pdf

23 Savage, M.: Outrage over scheme to electronically tag asylum seekers arriving in UK, , www.theguardian.com v. 19.6.2022

24 Home Office: Immigration Bail, 27.1.2023, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1122225/Immigration_bail.pdf

Innenministeriums, die diese Anträge bearbeiten, Zugang zu den vollständigen Standortdaten verlangen, um die Ansprüche zu untermauern oder zu entkräften."

Artikel 8-Anträge oder weitere Eingaben sind Ansprüche von Einzelpersonen auf ihr Recht auf ein Privat- und Familienleben in Großbritannien, das durch eine verpflichtende Ausreise oder Abschiebung verletzt würde. Die Verwendung von Spurdaten für solche Beurteilungen und Entscheidungen ist gesetzlich nicht genehmigt und kann das Recht auf Privatsphäre, aber auch auf Vereinigungs-, Versammlungs- und Meinungsfreiheit verletzen. Ein typischer „Abschreckungseffekt" : Das Wissen, dass das Innenministerium mögliche Informationen über politische, religiöse, weltanschauliche oder sonstigen Ansichten einer Person verwenden könnte, kann dazu führen, dass Menschen ihre täglichen Aktivitäten einschränken (wie bereits in verschiedenen Aussagen von Betroffenen deutlich wurde),[25] weil sie befürchten, dass diese Informationen bewusst oder unbewusst gegen sie verwendet werden, wenn über ihre Anträge entschieden wird.

Unzureichende Sicherheitsvorkehrungen

Verglichen mit dem Einsatz im strafrechtlichen Kontext ist die elektronische Überwachung im Zusammenhang mit der Durchsetzung von Einwanderungsgesetzen mit begrenzten Sicherheitsvorkehrungen verbunden, was wiederum Anlass zu der Besorgnis bietet, das Innenministerium sei der Ansicht, dass Migrant*innen nicht dieselben Menschenrechte und denselben Schutz verdienen wie britische Bürger*innen.

Zwar geht dieser Artikel nicht auf die Angemessenheit der Sicherheitsvorkehrungen im Strafrechtssystem ein und räumt ein, dass auch in diesem Zusammenhang Probleme bestehen, dennoch gibt es auffällige Unterschiede. „Her Majesties Prisons and Probation Code of Practice for Electronic Monitoring",[26] die Leitlinien für den Einsatz der elektronischen Überwachung in der Bewährungshilfe, sieht unter anderem vor, dass nur Strafgerichte befugt sind, elektronische Überwachung anzuordnen und dass dabei Fragen der Fairness und Verhältnismäßigkeit berücksichtigen

25 s. z. B. die Zeug*innenaussagen in der Beschwerde von Privacy International beim Information Commissioner (Fn. 17)

26 HM Prison & Probation Service: Code of Practice – Electronic Monitoring Data, October 2020, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/926813/em-revised-code-practice.pdf

müssen; die Bewährungshilfe kann dies nicht selbst tun. Außerdem werden strengere Auflagen für die Verwendung von GPS-Tracking festgelegt und dieses zeitlich begrenzt, während es im Einwanderungssystem keine zeitliche Begrenzung gibt.

Auch eine Reihe von „Grundprinzipien" für die elektronische Überwachung, die vom Ministerial-Committee des Europarats festgelegt wurden, hat das Innenministerium beim GPS-Tracking von Migrant*innen eindeutig ignoriert. Diese verlangen insbesondere, dass die Dauer der elektronischen Überwachung gesetzlich geregelt ist, dass Entscheidungen über die Überwachung von der Justiz getroffen werden oder eine gerichtliche Überprüfung möglich ist sowie, dass die Dauer und die Intensität der Überwachung in einem angemessenen Verhältnis zur Schwere der behaupteten oder begangenen Straftat stehen.[27]

Das Vorhandensein und die Qualität von Sicherungen sind von grundlegender Bedeutung für die Bewertung des Rechtseingriffs einer Maßnahme gemäß der EMRK. Im Verfahren Uzun vs. Deutschland des Europäischen Gerichtshofs für Menschenrechte (EGMR), in dem es um die Anbringung eines GPS-Trackers im Auto einer Person ging,[28] urteilte das Gericht über den Eingriff der GPS-Überwachung in das Recht auf Privatleben gemäß Artikel 8 EMRK. Bei der Beurteilung der Notwendigkeit und Verhältnismäßigkeit der Überwachung berücksichtigte der EGMR die folgenden Faktoren: Dauer, Zeitpunkt, Ort und Rechtfertigung der Überwachung sowie die Existenz von minderinvasiven Methoden, die weniger in die Privatsphäre eingreifen, um das gleiche Ziel zu erreichen. Das GPS-Tracking von Migrant*innen in Großbritannien weist eine hohe Eingriffsintensität auf und lässt daher eine vernichtende Bewertung erwarten, wenn diese Praxis vor Gericht angefochten wird. Das Innenministerium scheint zu versuchen eine gerichtliche Überprüfung um jeden Preis zu vermeiden: Viele Klagen auf gerichtliche Überprüfung sind gescheitert, weil das Innenministerium das Tracking von Klagenden zu Beginn des Verfahrens entfernte und ihnen so den Grund der Klage nahm.

27 Council of Europe: Recommendation CM/Rec(2014) 4 of the Committee of Ministers to member states on electronic monitoring v. 19.2.2014

28 EGMR: Entscheidung 35623/05 v. 2.9.2010

Schlussfolgerung

Es sieht düster aus für die Menschenrechte von Migrant*innen in Großbritannien, aber Anwält*innen und Menschenrechtsorganisationen wehren sich mittels rechtlicher Anfechtungen, Untersuchungen, Beschwerden bei den Behörden[29] und durch Kampagnen. Und das britische Innenministerium wird regelmäßig an seine völker- und menschenrechtlichen Verpflichtungen erinnert – so auch von der Hohen Kommissarin der Vereinten Nationen für Menschenrechte nach der Verabschiedung des Nationality and Borders Act 2022, der ein gestuftes Asylsystem einführte, Migration kriminalisierte und die räumliche Auslagerung von Asylbearbeitungszentren in Gebiete außerhalb Großbritanniens vorbereitete.[30]

Doch die vom Innenministerium eingesetzten Überwachungsinstrumente werden sich fast zwangsläufig auf andere EU-Länder ausbreiten, da sicherheitsbesessene Regierungen oft im Ausland nach Inspirationen suchen (in den USA gibt es bereits GPS-Tracking von Migrant*innen)[31]. Menschenrechtsverteidiger*innen und Anwält*innen werden wachsam bleiben müssen. Mit der Weiterentwicklung von Technologien und Instrumenten zum Aufbau eines Überwachungsapparats gegen Migrant*innen,[32] werden neue und bestehende Probleme auftreten, die ein wachsames Auge der Zivilgesellschaft erfordern.

29 Beschwerden wurden gegen das Innenministerium bei der britischen Datenschutzbehörde und der Aufsichtsbehörde für forensische Wissenschaft eingereicht, s. Privacy International: Privacy International files complaints against GPS tagging of migrants in the UK v. 17.8.2022, https://privacyinternational.org/news-analysis/4941/privacy-international-files-complaints-against-gps-tagging-migrants-uk

30 OHCHR: UN Rights Chief urges revisions to UK borders bill v. 17.3.2022, www.ohchr.org/en/press-releases/2022/03/un-rights-chief-urges-revisions-uk-borders-bill

31 A US surveillance program tracks nearly 200,000 immigrants. What happens to their data?, www.theguardian.com v. 14.3.2022

32 vor kurzem hat das Innenministerium „nicht integrierte" Fingerabdruckscanner eingeführt, s. UK plans GPS tracking of potential deportees by fingerprint scanners, theguardian.com v. 13.1.2023

Der Blick auf die Grenze

Gegenforensik macht Formen der Grenzgewalt sichtbar

von Giovanna Reder

Der folgende Text beschreibt die fortschreitende Technisierung und Überwachung der EU-Außengrenzen sowie forensische Methoden unter Verwendung von Open-Source-Materialien. Dazu werden Projekte der Organisationen Border Forensics und Forensic Oceanography vorgestellt, die mit räumlichen und visuellen Analysen Menschenrechtsverletzungen aufdecken. Damit wollen sie den systemischen Charakter von Überwachung und Grenzgewalt sichtbar machen, die Rechte von Migrant*innen stärken und eine Politik der Bewegungsfreiheit proklamieren.

Seit Jahren verstärkt die Europäische Union[1] die Kontrolle ihrer Außengrenzen mit dem vorgegebenen Ziel, „die Sicherheit in Europa zu gewährleisten".[2] Im Rahmen dieses fortschreitenden Prozesses werden Überwachungstechnologien ständig weiterentwickelt und modernisiert. Der Zugang zu diesen Technologien ist häufig auf den Staat und seine Exekutive beschränkt. An den Grenzen und darüber hinaus werden sie eingesetzt, um einerseits Kontrolle auszuüben, aber auch, um den Status quo zu erhalten. Wie kann die Öffentlichkeit angesichts dieser sich ständig weiterentwickelnden und verstärkenden Tendenz Rechenschaft einfordern?

Technoprekarität

Technologie ist ein grundlegender, integraler Bestandteil der Grenze und prägt nicht nur deren Kontrolle, sondern auch ihr Ausmaß. Durch den

1 Dieser Artikel bezieht sich räumlich auf die EU-Grenzen, aber ähnliche Entwicklungen können auch in anderen Grenzgebieten beobachtet werden.

2 Europäischer Rat: Strengthening the EU's external borders, Stand: 24.2.2023, www.consilium.europa.eu/en/policies/strengthening-external-borders

vielfältigen Einsatz von Technologien dehnt sich die Grenze von einer Linie auf der Landkarte aus und schafft um sie herum eine Grenzzone, ein feindliches Umfeld.[3] Diese Ausdehnung wird von Staaten durch verschiedene technologische und juristische Maßnahmen verstärkt und dadurch eine sich ständig verschiebende Grenze geschaffen. Ayelet Shachar argumentiert in „The shifting border", dass dies den Staaten ermöglicht, Bewegung von Menschen zu regulieren und zu kontrollieren.[4] Die Überwachung von Grenzen befindet sich demnach in einem ständigen Wandel, hinzu kommen die technologischen Hilfsmittel, die für diese fortschreitende Ausweitung und Externalisierung genutzt werden.

Auch die EU hat in den letzten Jahren Anstrengungen unternommen, die Kontrolle der Außengrenze über die eigentliche Grenzlinie hinaus auf das Umfeld zu verlagern. Um Migrationsbewegungen auf Distanz frühzeitig erkennen und kontrollieren zu können, setzt der Staat auf Abkommen mit Drittländern, aber auch auf Technologien zur Kontrolle wie Satelliten, hochauflösende Kameras, Offshore-Sensoren und Aufklärungsflugzeuge sowie verschiedene Formen der Datenerfassung.[5] In der Nähe der Grenzlinie kommen immer häufiger sogenannte Body-Sensing-Technologien zum Einsatz. Dabei handelt es sich um Technologien, die insbesondere darauf abzielen, die Körper von Migrant*innen sichtbar zu machen: Infrarotkameras zur Erkennung von Körperwärme oder Herzschlagdetektoren, Radartechnologie, optische Kameras und GPS-Ortung. Sie sollen diese Körper und deren Bewegungen, Handlungen und Verhaltensweisen beobachten, bewachen und dokumentieren.

Durch die konstante und wachsende Beobachtung verschlechtert sich die bereits prekäre Situation von vielen Migrant*innen, wenn sie versuchen die Grenze zu überqueren. Die Überwachung ist – wie die Prekarität – ungleich verteilt und wird durch rassifizierte,[6] geschlechtsspezifische und wirtschaftliche Privilegien beeinflusst. In dem gleichnamigen Buch

3 Hostile Environments, www.e-flux.com v. Mai 2020

4 Shachar, A.: The shifting border: legal cartographies of migration and mobility, Manchester 2021, S. 7

5 They can see us in the dark: migrants grapple with hi-tech fortress EU, www.theguardian.com v. 26.3.2021

6 Der Begriff „racial" ist schwer ins Deutsche zu übersetzen und wird hier mit „rassifiziert" ersetzt. S. von Rath, A.; Gasser, L.: Race ≠ Rasse: 10 schwierig zu übersetzende Begriffe in Bezug auf Race, www.goethe.de/ins/no/de/kul/sup/ac/race.html.

wird diese Verstärkung der Prekarität durch „Überwachung als Technoprecarity" (Technoprekarität) bezeichnet.[7] Die Vielzahl der Mittel, die von staatliche Stellen eingesetzt werden, um Grenzen zu sichern, Migration zu verhindern und jede Bewegungen derer zu überwachen, die dennoch versuchen, die Grenze zu überqueren, ist überwältigend.

Gegenforensik

Doch die Entwicklung dieser Technologien hat auch die Arbeitsweise von Aktivist*innen, Journalist*innen und humanitärer Organisationen verändert. Sie erwiesen sich als nützlich, um Menschenrechtsberichte zu begleiten und durch Visualisierung von Informationen zu unterstützen. So beschäftigt Amnesty International bereits seit 2007 Expert*innen zur Analyse von Satellitenbildern, um beispielsweise Menschenrechtsverletzungen und die Vertreibung der Rohingya in Myanmar im Jahr 2017 zu recherchieren und dokumentieren.[8]

Die Verwendung dieser verschiedenen Methoden, die Kombination relevanter Daten und deren Kartierung zur Gewinnung neuer Erkenntnisse ist Teil einer Praxis, die als „Counter Forensics" („Gegenforensik") bezeichnet wird. Diese Methode, die auch Border Forensics anwendet, baut auf der früheren Arbeit der Organisation Forensic Architecture auf. Sie beruht auf der Annahme, dass klassische forensische Techniken meist unter dem Monopol staatlicher Behörden stehen und dazu genutzt werden, die Zivilgesellschaft zu überwachen. Gegenforensik versucht, die Logik der Überwachung zu verstehen und abzubilden.[9] Sie setzt dieselben Methoden ein, um staatliche und nichtstaatliche Akteure für Verbrechen zur Verantwortung zu ziehen. Dies beinhaltet auch die Verwendung von Beweisen, die vom Staat selbst produziert werden, in manchen Fällen auch mit dessen Technologien.

Die Bilder von Überwachungstechnologien als Beweismittel zu verwenden, birgt das Risiko, die Gewalt, die von diesen ausgeht, zu reproduzieren, also die Technoprekarität zu bestärken. Sie können aber auch das Potenzial haben, den systematischen Charakter dieser Gewalt aufzudecken, ohne die Muster des illegalisierten Grenzübertritts preiszugeben.

---

7 Precarity Lab: Dispossession by Surveillance, in: Technoprecarious, London 2020, https://goldsmithspress.pubpub.org/pub/1lfs5mgj/release/1

8 Hochauflösend ohne Wolken, bitte! Amnesty Journal, 26.7.2018, www.amnesty.de/informieren/amnesty-journal/hochaufloesend-ohne-wolken-bitte

9 Weizmann, E.: Forensic Architecture, New York 2017, S. 68

Dies wird von Border Forensics als „disobedient gaze" („unfolgsamer Blick") bezeichnet. Dieser Blick zielt „darauf ab, nicht das zu enthüllen, was das Regime, zu enthüllen versucht – die klandestine Migration –, sondern das zu offenbaren, was es zu verbergen versucht, die politische Gewalt, auf der es beruht, und die Menschenrechtsverletzungen, die sein strukturelles Ergebnis sind."[10] Dieser unfolgsame Blick versucht also die Perspektive darauf zu verschieben, wie wir Grenzen und ihre Auswirkungen betrachten und was sichtbar gemacht wird.

Während die staatlichen Technologien versuchen, die Körper von Migrant*innen sichtbar und damit kontrollierbar zu machen, versuchen sie ebenfalls, die gewalttätigen Praktiken der militarisierten Grenzkontrolle zu verbergen. Die Gewalt an den Grenzen schwankt dabei zwischen direkter (physischer) Gewalt durch Grenzschutzbeamt*innen z. B. während der Durchführung illegaler Pushbacks,[11] aber sie beinhaltet oft auch indirekte oder kontaktlose Gewalt wie politische und juristische Maßnahmen, die das Recht auf Asyl einschränken, oder die beschriebenen Technologien zur Überwachung. Die visuelle Arbeit von Border Forensics reflektiert darüber, wie Grenzüberwachung Bedingungen der (Un-)Sichtbarkeit und (Un-)Hörbarkeit schafft.

Im Folgenden stelle ich zwei Fallstudien von Forensic Oceanography und Border Forensics in den Vordergrund, die die Idee des unfolgsamen Blicks illustrieren und erforschen sowie den Einsatz technologischer Erfassungsinstrumente in der Praxis veranschaulichen.

Fallstudie 1: Left-to-die boat[12]

Der erste von Forensic Oceanography bearbeitete Fall war das sogenannte Left-to-die boat. Im März 2011 brachen 72 Menschen mit einem kleinen Schlauchboot nach Italien auf. Während der Überfahrt ging der Treibstoff aus und sie drifteten 14 Tage lang zurück an die libysche Küste. Dabei wurden sie immer wieder von europäischen staatlichen Akteuren beobachtet. Das Boot landete am 10. April südöstlich von Tripolis, von den 72 Passagieren überlebten nur neun. Um die Ereignisse und die Ver-

10 Pezzani, L.; Heller, C.: A disobedient gaze: strategic interventions in the knowledge(s) of maritime borders, Postcolonial Studies 2013, H. 3, S. 289-298 (294)

11 Pushbacks sind das unrechtmäßige Zurückdrängen von Geflüchteten, ohne dass diese Möglichkeit für ein Asylerfahren erhalten.

12 The Left-to-die Boat, https://forensic-architecture.org/investigation/the-left-to-die-boat

nachlässigung durch die staatlichen Behörden zu rekonstruieren, kombinierte Forensic Oceanography Zeugenaussagen der Überlebenden mit Wind- und Strömungsdaten sowie Satellitenbildern.

Eine wichtige Aufnahme dieser Untersuchung stammt aus dem Jahr 2011 von dem Satelliten „Envisat-1" der Europäischen Weltraumorganisation. Er zeichnet die Reflexion von Mikrowellen auf und wandelt diese in ein SAR-Bild (Synthetic Aperture Radar) um. Ruhige Meeresoberflächen erscheinen dabei dunkel, während Schiffe den größten Teil der Radarenergie zum Sensor zurückwerfen und als helle Pixel vor einem gleichmäßigen Hintergrund erscheinen. Die detaillierte Analyse der „Envisat"-Bilder half, größere Schiffe in der Nähe des Left-to-die boat zu identifizieren indem festgestellt wurde, welche dieser Schiffe in anderen Datensätzen wie der Schiffsortung mit AIS (Automatic Identification System) nicht erfasst wurden. Darin wird ein Signal an Küsten- oder Satellitenempfänger gesendet, das Echtzeit-Informationen über die Position und den Kurs aller registrierten Schiffe liefert. Die Nutzung eines AIS ist für große Handelsschiffe vorgeschrieben, nicht aber für Kriegsschiffe und andere bestimmte Schiffskategorien, die diese Signale unter Umständen unterdrücken können. Mit dem „Envisat"-Satellitenbild konnten die Militärschiffe also identifiziert und dieses in ein Beweisstück verwandelt werden. Dieses zeigt, dass während das Boot an die Küste zurücktrieb, staatliche Akteure zwar anwesend waren, aber untätig blieben. Bei der Untersuchung wurden diese Daten und Informationen mit der AIS-Ortung, den Notsignalen sowie der berechneten Drift unter Einbeziehung von Wind- und Strömungsdaten korreliert.

Durch eine derartige Kombination verschiedener Informationsfragmente soll versucht werden, die Formen der kontaktlosen Gewalt zu erklären und zu hinterfragen. In diesem Fall zeigte die Verwendung von Bildern, die Überwachungstechnologie erzeugt haben, „wie eine Vielzahl von Akteuren und Technologien zusammenwirken, um diesen Raum zu gestalten, und wie EUropa das Meer und seine Kräfte aktiv zum Zweck der Abschreckung von Migranten einsetzt."[13] Der Bericht, den Forensic Oceanography über das Left-to-die boat veröffentlichte, wurde im Zusammen-

13 Heller, C.; Pezzani, L.; Stierl, M.: Disobedient Sensing and Border Struggles at the Maritime Frontier of Europe, in: spheres # 4 (2017), https://spheres-journal.org/contribution/disobedient-sensing-and-border-struggles-at-the-maritime-frontier-of-europe

hang mit der unterlassenen Hilfeleistung auf See in mehreren Rechtsfällen vorgelegt. Zusammen mit europäischen Nichtregierungsorganisationen wurden in Frankreich, Italien, Belgien und Spanien Klagen eingereicht. Diese Initiativen sowie eine Untersuchung durch den Europarat[14] und mehrere Journalist*innen haben Staaten und Militärs gezwungen, weitere Daten über den Vorfall herauszugeben. Die im Bericht dargestellten Fakten wurden nie angefochten. Noch immer gibt es keine rechtliche Verantwortung für die Todesfälle.

Fallstudie 2: Airborne Complicity[15]

Seit dem Left-to-die boat hat sich das Mittelmeer als Grenzgebiet grundlegend verändert. Nicht nur wegen zunehmender Fluchtbewegungen im sogenannten „langen Sommer der Migration",[16] sondern auch, weil EUropa in den vergangenen Jahren Drittstaaten wie Libyen aufgerüstet und vor allem die Überwachung aus der Luft kontinuierlich aufgebaut hat. Parallel dazu hat auch die Zivilgesellschaft Kapazitäten zur Aufklärung entwickelt. Im Mittelmeer sind dies beispielsweise zivile Rettungsorganisationen sowie das Alarmphone, eine Hotline für Menschen in Not, die Menschenleben rettet und Übergriffe und Menschenrechtsverletzungen sowie die Vernachlässigung von Staaten dokumentiert.[17] Ohne deren aktivistische Arbeit würden viele Fälle nicht größer bekannt, wie Border Forensics anhand der Rekonstruktion der Ereignisse vom 30. Juli 2021 zeigen konnte.

An diesem Tag hat die libysche Küstenwache mehrere Boote mit Migrant*innen in dem Gebiet abgefangen, in dem eine Frontex-Drohne patrouillierte. Die von Border Forensics gesammelten Beweise deuten darauf hin, dass diese eine Schlüsselrolle bei Pullbacks spielte (bei dieser Praxis werden Bootsinsassen von der libyschen Küstenwache abgefangen und zurückgeholt). Dazu nutzte Border Forensics Flugbewegungsdaten, mit denen sich unter anderem die Präsenz von Frontex nachweisen lässt. Sie lassen sich durch ADS-B (Automatic Dependance Surveillance

14 Europarat: Lives lost in the Mediterranean Sea: Who is responsible?, Resolution 1872 (2012) v. 27.4.2012, https://pace.coe.int/en/files/18095

15 Border Forensics: Airborne Complicity – Frontex Aerial Surveillance Enables Abuse v. 12.12.2022, www.borderforensics.org/investigations/airborne-complicity

16 Kasparek, B.: Routen, Korridore und Räume der Ausnahme, in: Hess, S. u.a.: Der lange Sommer der Migration, Berlin 2017, S. 38-51

17 https://alarmphone.org/de

Broadcast) verfolgen. Die Nutzung eines ADS-B-Transponders ist für alle Flugzeuge in Europa vorgeschrieben, allerdings nur mit einem maximalen Abfluggewicht von 5.700 Kilogramm.[18] Dies schließt die meisten Frontex-Flugzeuge wie das „Diamond Aircraft-62" aus, das nur 1.999 Kilogramm wiegt und speziell für den europäischen Markt entwickelt wurde.[19] Die von Frontex geleasten Flugzeuge und auch die seit 2021 über den Rüstungskonzern Airbus geleaste Drohne ermöglichen es der Agentur also, „unter dem Radar" zu bleiben. Um die Daten der ADS-B-Transponder nutzbar zu machen, werden sie von Satelliten oder bodengestützten Empfangsanlagen aufgefangen und öffentlich zugänglich gemacht. Anbieter wie Flightradar stellen diese dann auf ihren Webseiten dar. Mitunter fordern aber private oder militärische Betreiber von Flugzeugen die Betreiber auf, deren Positionsdaten nicht anzuzeigen.

In der Untersuchung Airborne Complicity nutzte Border Forensics unter anderem Daten von der Website ADS-B Exchange. Sie wurde als Open-Source-Initiative ins Leben gerufen und hatte das Ziel, keine Daten zu filtern. Die Flugzeugsignale werden durch freiwillige Helfer*innen gesammelt, die dazu günstige Selbstbauempfänger aufstellen und dadurch unabhängig von den staatlichen Empfangsstationen sind. Dies half, die Behauptungen von Frontex zum Einsatz ihrer Luftfahrzeuge zu widerlegen. Insbesondere hat Border Forensics die Korrelation zwischen den Flugstunden, die Frontex über dem libyschen Fluginformationsgebiet verbracht hat, und der Anzahl der Pullbacks untersucht. Die Analyse des räumlichen und zeitlichen Zusammenhangs ergab, dass die Luftüberwachung von Frontex nicht dazu beiträgt, Leben auf See zu retten, sondern vielmehr die Zahl der völkerrechtswidrigen Zurückweisungen erhöht.

Methodik

Der Zugang zu Informationen aller Art und damit auch zu neuen Formen der Beweiserbringung ist heutzutage immens. Handyvideos und auch Webcams liefern eine beträchtliche Menge an Bildmaterial, auch Satellitenbilder sind online abrufbar und eine Vielzahl von Sensoren liefern zusätzliche Informationen. Mehrere Archive dokumentieren außerdem Grenzgewalt, wie die Datenbank mit Zeug*innenaussagen des Border Vi-

18 ADS-B UPDATE 2023 v. 24.1.2023, www.universalweather.com/blog/ads-b-update-2023
19 Diamond readies first DA62 piston twins for delivery, www.flightglobal.com v. 22.9.2015

olence Monitoring Network, das Angaben zu Pushbacks auf der Balkanroute sammelt.[20] Die Plattform Watch the Med kartiert Todesfälle und Verletzungen der Rechte von Migrant*innen an den Außengrenzen der EU online.[21] Soziale Medien dienen oft als Informationsquelle und Archiv zugleich. Darüber hinaus bieten Webseiten wie Suncalc die Möglichkeit, anhand von Schatten die Tageszeit eines Bildes zu berechnen. Andere ermöglichen Nutzer*innen, den Ursprung eines Bildes zurückzuverfolgen oder Metadaten auszulesen, darunter etwa Exifdata und Yandex.

Die Auswertung dieser Vielzahl an öffentlich zugänglichen Materialien wird als Open Source Intelligence (OSINT) bezeichnet. Methodik und Begrifflichkeit haben ihren Ursprung im Bereich der Nachrichtendienste,[22] sie werden aber auch von Grenzbehörden eingesetzt. So schreibt auch Frontex, „ein unverzichtbares Element, um auf dem Laufenden zu bleiben, ist die ständige Beobachtung offener und medialer Quellen."[23] CEPOL, die Agentur der Europäischen Union für die Aus- und Fortbildung auf dem Gebiet der Strafverfolgung, bietet spezifische Schulungen an, die vermitteln, wie durch OSINT Ermittlungen im Zusammenhang mit der „Beihilfe zur illegalen Einwanderung" verbessert werden.[24]

Auch die Projekte von Forensic Oceanography und Border Forensics wollen mit OSINT die systemische Gewalt von Grenzen sichtbar machen. Dabei arbeiten sie gleichzeitig mit den Gemeinschaften, die davon betroffen sind, zusammen und unterstützen diese. Erfahrungen von Überlebenden sowie Aktivist*innen, die vor Ort arbeiten, sind eines der wichtigsten Mittel der Rekonstruktion und als Beweismittel unerlässlich. Von staatlicher Seite wird oft die angebliche Objektivität von Technologie und Wissenschaft gegen die Fehlbarkeit menschlicher Zeugen*innenaussagen ausgespielt. In den Projekten von Border Forensics werden sie vereint, um ein Bild zu zeichnen, das die Erfahrungsberichte in den Mittelpunkt rückt, aber auch die Entstehung der Gewalt rekonstruiert.

Der unfolgsame Blick, der sich dem Staat widersetzt, muss nicht nur dessen Maßnahmen genau analysieren. Er muss auch beurteilen, ob die gesammelten Daten und Informationen niemandem schaden. Besonders

20 www.borderviolence.eu

21 https://watchthemed.net/index.php/main

22 Becker, M.: Den Heuhaufen filtern, um die Nadel zu finden, www.rosalux.de/publikation/id/39367/den-heuhaufen-filtern-um-die-nadel-zu-finden

23 Frontex: Situational awareness and monitoring, https://frontex.europa.eu/we-know/situational-awareness-and-monitoring/information-management

24 CEPOL: OSINT in Facilitated Illegal Immigration, www.cepol.europa.eu/training-education/04-2022-ons-osint-facilitated-illegal-immigration

bei grundsätzlich prekären Situationen wie der Überquerung von Grenzen können veröffentlichte Informationen (etwa zu Migrationsrouten) Menschen Probleme bereiten. Rothe und Shim warnen beispielsweise, dass das Sammeln von Daten durch Nichtregierungsorganisationen und die Verwendung derselben (Überwachungs-)Technik dazu führen können, dass diese selbst Zusammenhänge auskundschaften. Das könne zu einer „Verstaatlichung der Zivilgesellschaft" führen, bei der die Aufgaben des Staates von nichtstaatlichen Akteuren übernommen werden.[25]

Verschiebung des Blicks

Das Precarity Lab erklärt, wie die gegenwärtige Angst vor Überwachung aus der weißen Mittelschicht oft die eigene Mitschuld an der (Re-)Produktion von Prekarität ignoriert, ebenso wie die Tatsache, dass die Wurzeln der heutigen Überwachungspraktiken im Kontext von Sklaverei und Kolonialismus entwickelt wurden.[26] Neue Untersuchungsmethoden wie die Gegenforensik und OSINT geben uns die Möglichkeit, die Art und Weise, wie staatliche Macht ausgeübt wird, näher zu betrachten und die Technoprekarität bis zu einem gewissen Grad zu analysieren. Immer mehr Gruppen und Aktivist*innen nutzen Technologien wie Flugzeug- oder Schiffsverfolgung und Kartierung, um für die Rechte von Migrant*innen zu kämpfen.

Die Verarbeitung dieser Materialien sowie die Forschung und die Generierung von Wissen und Analysen rund um das Thema Migration und Fluchtwege muss aber auch kritisch reflektiert werden. Dies würde bedeuten, wie Shachar meint, den Blick von der Migration selbst abzuwenden und unsere Aufmerksamkeit auf die Bewegung der Grenzen zu richten: „Die Verschiebung der Perspektive, die ich vorschlage – vom vertrauten Ort der Untersuchung der Bewegung von Menschen über Grenzen hinweg zur kritischen Untersuchung der Bewegung von Grenzen, um die Mobilität von Menschen zu regulieren."[27] Die wachsenden Technisierung verändert, bewegt und verschiebt die Grenze und gleichzeitig gilt es aber, den Blick auf die daraus resultierende Technoprekarität nicht zu verlieren.

---

[25] Rothe, D.; Shim, D.: Sensing the Ground: On the Global Politics of Satellite-Based Activism, in: Review of International Studies 2018, H. 3, S.414-37, https://doi.org/10.1017/S0260210517000602

[26] Precarity Lab a.a.O. (Fn. 7)

[27] Shachar a.a.O. (Fn. 4), S. 6

Training der Zukunft?

Virtual Reality-Trainings bei deutschen Polizeibehörden

von León von der Burg, Johannes Ebenau und Jasper Janssen

Immer mehr Polizeien in Deutschland beschäftigen sich mit Virtual Reality (VR). An die Implementierung werden verschiedene Hoffnungen und Erwartungen insbesondere zur Verbesserung von polizeilicher Aus- und Fortbildung geknüpft. Es steht zur Disposition, inwiefern VR-Technologien diesen Erwartungen gerecht werden können oder ob mit ihnen nur leere Modernisierungsversprechen einhergehen. Der Beitrag gibt einen Überblick über polizeiliche Erprobungen von VR-Trainingstechnologien sowie die damit verbundenen Hoffnungen und Kritikpunkte.

Die Euphorie angesichts neuer technologischer Entwicklungen macht auch vor deutschen Polizeien nicht halt. Smartphones, die einsatzrelevante Informationen in Echtzeit zur Verfügung stellen, einsatzunterstützende Software, die den nächsten Einbruch vorhersagen soll, oder Drohnen zur Überwachung von Versammlungen oder Tatortsicherung werden als Einsatzmittel der Zukunft von modernen, noch effizienteren Polizeien präsentiert. Eins der aktuellsten Trendtechnologiefelder ist das der Virtual und Mixed Reality. Insbesondere in der polizeilichen Aus- und Fortbildung sollen sie bei der Erzeugung einer immersiven Lernumgebung helfen. Ihr Versprechen: realitätsnähere, qualifiziertere und kostengünstigere Trainings als bisher vor allem für komplexe Einsätze wie Amokläufe oder Terroranschläge. Doch was ist dran an der Technologie, die von manchen Polizeien bereits als ein „Quantensprung" im Einsatztraining bezeichnet wird?[1] Im Folgenden geben wir einen Überblick über die Technologien, zeigen wer mit ihnen trainiert, was Polizeibehörden sich von deren Nutzung versprechen und welche Kritikpunkte und Limitationen vorliegen.

1 Zorn, T.: Virtual Reality im Einsatztraining. Wie die Polizei NRW Pionierarbeit als Teil eines EU-Projekts leistet, in: Die Streife 2022, H. 3, S. 6-11 (6)

Die intuitive Verknüpfung zwischen digitaler und physischer Welt ist seit jeher ein Teilprojekt fortschreitender Digitalisierung. Die derzeitigen Hoffnungstechnologien lassen sich im Technologiefeld der Extended Reality (XR) zusammenfassen. Dieser Oberbegriff beinhaltet die unterschiedlichen Systeme der Virtual Reality und Mixed Reality (MR). Diese Systeme vereint das Bestreben, die Grenzen zwischen digitaler und physischer Welt weiter zu verschieben und Interaktionen von physischen und digitalen Objekten oder Applikationen durch Visualisierungs- und Projektionstechnologien zu ermöglichen. Während sich VR-Technologien durch Projektionen von physischen Aspekten auf virtuelle Oberflächen auszeichnen, ist es bei Systemen der MR anders herum. MR-Systeme, die sich zwischen Augmented Reality (AR) und Augmented Virtuality (AV) differenzieren lassen, ist gemein, dass virtuelle Elemente mithilfe von Bildschirmen, etwa AR-Brillen oder dem Bildschirm eines Smartphones in das Sichtfeld der Nutzenden projiziert werden. Ein populäres Beispiel dieser Technologie ist das Smartphone-Spiel Pokémon Go.[2] Im Kontext von Polizeien dominieren derzeit VR-Systeme den Markt, weshalb wir unsere Aufmerksamkeit in diesem Artikel vornehmlich solchen Systemen widmen.

VR-Technologie und ihre polizeiliche Erforschung

Das Prinzip von VR ist simpel: Die physischen Bewegungen von Nutzenden werden durch Sensoren aufgezeichnet und auf ein digitales Abbild, den sogenannten Avatar, in eine virtuelle Umgebung übersetzt. So ist es möglich, Nutzer*innen das Gefühl zu vermitteln, in eine virtuell geschaffene Welt einzutauchen, zu einem gewissen Grad mit ihr zu interagieren[3] und gleichzeitig das Gefühl zu haben, physisch an einem anderen Ort zu sein.[4] Ein Head-Mounted-Display (HMD), das umgangssprachlich als VR-Brille bezeichnet wird, ermöglicht in der VR die visuelle Orientierung und die Steuerung des Sichtfeldes durch Bewegungen mit dem Kopf. Andere

2 Auch die Nutzung von Pokémon Go hatte unlängst für Schlagzeilen gesorgt, nachdem zwei Polizisten im US-Bundestaat California einem Notruf nicht nachgekommen waren, weil sie Pokémon Go gespielt haben. Vgl. Polizeibeamte spielen „Pokémon Go", statt Räuber zu verfolgen – entlassen, RedaktionsNetzwerk Deutschland online v. 11.1.2022

3 Wohlgenannt, I. u.a.: Virtual Reality. Business & Information Systems Engineering 2020, H. 5, S. 455-461

4 Sanchez-Vives, V.; Slater, M.: From presence to consciousness through virtual reality. Nature Reviews Neuroscience 2005, H. 4, S. 332-339

Sensoren, etwa an VR-Handschuhen oder Controllern in Form von modifizierten Waffenreplikationen, ermöglichen die Übersetzung von Bewegungen und Interaktionen aus der physischen Welt auf das digitale Abbild im virtuellen Raum. Die Arten und Möglichkeiten der Steuerung wie Interaktion variieren dabei zwischen Systemen und Anbietern und ermöglichen einen unterschiedlichen Grad der Immersion, also des sensitiven Eintauchens in die virtuelle Umgebung. Da die Veränderung der virtuellen Oberfläche lediglich die (Um)Programmierung von Pixeln und Code, also keine Veränderung von physischer Materie bedarf, sind der Fantasie in der VR wenig Grenzen gesetzt. Deshalb erscheinen VR-Technologien für jene Anwendungsbereiche besonders attraktiv, die sich durch eine hohe und regelmäßige Anpassungsnotwendigkeit auszeichnen und die unter normalen Umständen einen enormen Aufwand von Ressourcen und Arbeit erfordern würden.[5] Für Szenario-Trainings in der VR bedeutet das etwa, dass Repräsentationen von Menschen oder Tieren, sogenannte Non-Player-Characters (NPCs), oder Objekte einfach aus einer Datenbank in zuvor vorbereitete Szenarios eingefügt werden können. Da diese virtuellen Welten im Grunde nichts anderes als eine grafische Oberfläche eines im Hintergrund laufenden komplexen Codes sind, werden während der Nutzung eine enorme Menge an Daten aufgezeichnet. Jede Bewegung, jedes gesprochene Wort und jeder abgefeuerte Schuss hat seine Entsprechung im Datenfluss und kann theoretisch für eine spätere Evaluation des individuellen Verhaltens und Leistungsbildes rekonstruiert werden.

Die Anfänge von XR-Systemen lassen sich, wie bei vielen anderen „Zukunftstechnologien" auch, auf militärische Forschung zurückführen.[6] XR-Technologien bilden heute einen wichtigen (häufig übersehenen) Teil in der militärischen Ausbildung, im Training und in der Weiterbildung. Darüber hinaus entwickelt sich seit einigen Jahren in der Gaming- und

5 Kaplan, D. u.a.: The Effects of Virtual Reality, Augmented Reality, and Mixed Reality as Training Enhancement Methods: A Meta-Analysis. Human Factors 2021, H. 4, S. 706-726

6 Auch wenn die erste XR-Technologie bereits in den 1960er Jahren im US-Militär erforscht wurde, hat die Technologie einen wirklichen Impetus erst in den 1990er Jahren erfahren, s.: Sutherland, E.: The ultimate display, in: Kalenich, A. (Hg.): Proceedings of the international federation for information processing congress 1965, H. 1, S. 506-508; Baumann, J.: Military applications of virtual reality, in: The Encyclopedia of Virtual Environments, College Park (Maryland) 1993; Seidel, J.; Chatelier, R. (Hg.): Virtual reality, training's future? Perspectives on virtual reality and related emerging technologies, New York 1997.

Unterhaltungsindustrie eine zweite zunehmende Triebkraft in der Weiterentwicklung von XR- und insbesondere VR-Technologien.[7] Nicht nur markiert VR-basiertes Gaming als wachsendes Segment in der Gaming-Branche ein attraktives Feld für Investitionen, die dabei (weiter) entwickelten Hard- und Softwaresysteme bilden außerdem die Grundlage für immer mehr ernsthafte Inhalte: So basieren viele der VR-Umgebungen, welche von deutschen Polizeien genutzt oder getestet werden, auf den HMDs und/oder Gaming Engines die ursprünglich für Gaming-Inhalte produziert wurden.[8] In vielen Fällen werden also fürs Gaming entwickelte Technologien für Lernen, Training und Simulation genutzt. Dies erklärt auch, warum sich viele der VR-Umgebungen äußerlich kaum von Spielen unterscheiden. Neben militärischer Forschung und der Gaming- und Unterhaltungsindustrie wird die Verbreitung von XR-Technologien durch zwei weitere Entwicklungen vorangetrieben: Zum einen ist der Medienkonzern Meta (ehemals Facebook) bestrebt, das Internet mit dem „Metaverse" um eine per VR erleb- und bedienbare Sphäre nach eigenen Vorstellungen zu ergänzen. Zum anderen ist gleichzeitig der gesellschaftliche Bedarf nach digitalen Interaktionsmöglichkeiten durch die Kontakteinschränkungen der Covid-19-Pandemie gewachsen. Beide Entwicklungen führen dazu, dass immer mehr Arbeits- und Gesellschaftsbereiche entsprechende Anwendungsmöglichkeiten prüfen. Neben Dienstleistungen in den Bereichen der Medizin oder Logistik, betrifft dies auch deutsche Behörden und Organisation mit Sicherheitsaufgaben (BOS). So lassen sich bei deutschen Polizeibehörden mit Beginn der 2010er Jahre zunehmend Ambitionen erkennen, VR-Technologien auf ihre Möglichkeiten im Trainingsbereichen zu testen. Diese Initiativen sind dabei entweder Bestandteil größerer, durch die Europäische Union (EU) und ihre Forschungsinitiativen Horizon 2020 oder Horizon Europe finanzierten Verbundprojekte oder es handelt sich um individuelle Kooperationen einzelner Polizeibehörden mit Anbietern aus der Privatwirtschaft, wie etwa bei den Polizeien aus Rheinland-Pfalz und Niedersachsen.

---

7 Greengard, S.: Virtual reality, Cambridge; London 2019, S. 28

8 Gaming Engines bilden das Software-Gerüst, welches die Funktionalitäten der virtuellen Welten weitgehend begrenzen. Sie definieren was in der XR (nicht) machbar ist, indem sie bspw. physikalische Grundprinzipien simulieren oder den Grad der Interaktionalität anlegen, s.: van Der Heijden, T. u.a.: Use of Game Engines and VR in Industry and Modern Education, in: Ntalianis, K. u.a. (Hg.): Applied Physics, System Science and Computers III, Cham 2019, S. 88-93.

Gefördert durch die EU startete das Projekt „Training Augmented Reality Generalised Environment Toolkit" (TARGET), das in der Horizon 2020-Förderperiode von 2015 bis 2018 bewilligt und mit beinahe 6 Millionen Euro gefördert wurde. Neben 14 weiteren europäischen Projektpartnern aus Forschung und BOS arbeiteten die Deutsche Hochschule der Polizei,[9] die Hochschule der Polizei Brandenburg[10] und das Fraunhofer Institut unter französischer Projektleitung an der Harmonisierung von XR-Systemen zum Training von Polizeikräften.[11] Die entworfenen Trainingsszenarien waren dabei so heterogen wie die getesteten XR-Systeme.[12] Zwar wurde hier bereits mit VR-Technologien experimentiert, der Fokus lag jedoch noch auf MR-Technologien und der Ermittlung möglicher Synergieeffekte mit anderen Technologien der Zukunft, wie Künstlicher Intelligenz. Wesentliche Probleme lagen in der unausgereiften MR-Technik: Ungenauigkeiten in der graphischen und räumlichen Darstellung, stark begrenzte Rechenleistung und eingeschränkte Sichtfelder der HMDs sowie klobige und wenig interaktionsfähige NPCs brachten die Projektgruppe, neben positiven Bilanzen, zum Fazit: „Erst wenn die Technologien ausgereift sind, wird Training von Sicherheitsbehörden mit solchen Systemen möglich sein."[13]

Ungehindert von einem solch ernüchternden Ergebnis übernahm das Projekt SHOTPROS im Jahr 2019 den Forschungsschwerpunkt XR-Trainings und wurde mit rund fünf Millionen Euro über die Horizon Europe Finanzierungsinitiative der EU gefördert.[14] Ziel war es, ein VR basiertes Trainingssystem und Curriculum zu entwickeln mit dem Polizist*innen ihre Handlungs- und Entscheidungskompetenz in Stress- und Hochrisikosituationen verbessern können. Unter Leitung einer österreichischen Consultingfirma waren das Landesamt für Ausbildung, Fortbildung und

9 www.dhpol.de/departements/departement_II/FG_II.4/target.php

10 https://hpolbb.de/sites/default/files/field/dokumente/forschungsbericht_2014_und_forschungsplan_2015-2016.pdf

11 https://cordis.europa.eu/project/id/653350

12 Vidal, R.: Design and Implementation of High Reliability Organizing Based Performance Metrics in the Context of the EU H2020 Research Project TARGET, Aiming at Developing VR/AR Training Environment for Security Critical Agents, In: Bagnara, S. u.a. (Hg.): Proceedings of the 20th Congress of the International Ergonomics Association (IEA 2018). IEA 2018. Advances in Intelligent Systems and Computing 2019, H. 824

13 TARGET: Final Report on TARGET Platform, o.O. 2018, S. 75, https://ec.europa.eu/research/participants/documents/downloadPublic?documentIds=080166e5bef86d4d&appId=PPGMS v.14.12.2022, eigene Übersetzung

14 https://cordis.europa.eu/project/id/833672

Personalangelegenheiten der Polizei Nordrhein-Westfalen (NRW)[15] und die Polizei Berlin[16] neben verschiedenen europäischen Innenbehörden, Polizeien und Universitäten Projektpartner.

Ebenfalls 2019 baute die Hochschule der Polizei Rheinland-Pfalz ihr eigenes VR-Projekt SAFER (Simulation in der Ausbildung für Einsatzkräfte in Rheinland-Pfalz) in Kooperation mit dem niederländischen Unternehmen XVR-Simulations weiter aus.[17] Das System ist sowohl über VR als auch über herkömmliche Monitore nutzbar und wird bereits seit 2004 durch die Feuerwehr- und Katastrophenschutzschule Rheinland-Pfalz[18] und seit 2011 auch durch die Feuerwehrschule Sachsen sowie weitere in Katastrophenschutz involvierte Organisationen in verschiedenen Teilen der Ausbildung angewandt.[19] In der Polizei Niedersachsen beschäftigt sich seit 2019 eine Projektgruppe mit den Implementierungsmöglichkeiten von XR-Techniken in die Aus- und Weiterbildung, wie z. B. einer XVR-Simulationsumgebung die u. a. für Szenario-Übungen getestet wird.[20] Die Polizeiakademie Niedersachsen erprobt zudem am „Campus 4.0" verschiedene andere Anwendungsbereiche für XR-Technologien in der Ausbildung.[21] Außerdem wurde 2022 der „Pixplorer", ein VR-System zur virtuellen Tatortbegehung, vorgestellt und an die 28 niedersächsischen Fachkommissariate Forensik ausgeliefert.[22] Auch die Polizeien aus Bremen und Bayern arbeiten an der Implementierung von XR-Technologien.[23]

Horizonte polizeilichen Einsatztrainings in VR

Trotz der unterschiedlichen Entwicklungsstände und Pfade zur Implementierung von VR-Systemen zum Training, vereinen die Behörden konkrete Hoffnungen und Erwartungen an den Einsatz von VR. Polizeiliche

15 https://lafp.polizei.nrw/artikel/virtual-reality-projekt-shotpros-lafp-nrw-entwickelt-die-zukunft-des-polizeitrainings-mit
16 Pressemitteilung der Polizei Berlin Nr. 1566 v. 28.6.2019
17 Pressemitteilung des Innenministeriums Rheinland-Pfalz v. 22.5.2019
18 https://lfks.rlp.de/de/ueber-die-lfka/projekte/safer
19 Pressemitteilung des Innenministeriums Rheinland-Pfalz v. 22.6.2011
20 Pülm, M.: Einführung XVR-Simulationsumgebung, in: proPolizei. Informationen für die Polizei Niedersachsen 2020, H. 6
21 https://digitalagentur-niedersachsen.de/digitaler-ort-polizeiakademie-niedersachsen
22 Pressemitteilung des Innenministeriums Niedersachsen v. 29.8.2022
23 Bremer Polizei will wegen Corona virtuell trainieren, Weser Kurier v. 06.5.2022; www.fuehrungskraefte-forum.de/detail.jsp?v_id=7565; www.dpolg-bayern.de/artikel/virtual-reality-vr-wird-ausgebaut-237.htm

Akteure erwarten konkrete Verbesserungen des Einsatztrainings in mindestens drei Bereichen: dem Ressourcenaufwand, der gestalterischen Freiheit in der Szenarioerstellung und der verbesserten Möglichkeiten zur Erhebung und Auswertung von Trainingsdaten.

In den vergangenen Jahren haben sich insbesondere im Bereich komplexer und lebensbedrohlicher Einsatzszenarien Ausbildungsdefizite und neue Trainingsbedarfe bei europäischen BOS manifestiert: Amoktaten an Schulen wie in Erfurt (2002) oder Winnenden (2009) sowie Terroranschläge wie in Paris, Nizza, Berlin oder München. Was diese Ereignisse aus Sicht von BOS vereint, ist die hohe Dynamik der Situation, das zu erwartende hohe Schadensausmaß und die daraus resultierende Komplexität der Lagebearbeitung. Den Ereignissen ist auch gemein, dass BOS aus ihnen die Notwendigkeit zur Übung vergleichbarer Szenarien ableiteten. Die Übung solch komplexer Lagen bedarf der Beteiligung diverser BOS, versammelt teils hunderte Übende, erfordert einen erheblichen Ressourcenaufwand und verlangt eine gute Koordination. Kurz: sie sind aufwendig und teuer. Das Problem, Trainingsbedarfe zu erkennen, aber gleichzeitig kaum adäquate Trainingsumgebungen herstellen zu können, ist ein Ausgangspunkt, an dem VR-Training als polizeiliche Hoffnungstechnologie andockt. Es geht mit dem Versprechen einher, komplexe Einsatzsituationen mit vergleichsweise geringem Ressourcenaufwand virtuell inszenieren zu können.[24]

Polizeien erhoffen sich zudem eine darüberhinausgehende Verbesserung des Einsatztrainings durch die neuen technologischen Möglichkeiten. In einem Promo-Video zum VR-unterstützten Simulationstraining der Hochschule der Polizei Rheinland-Pfalz resümiert ein Polizeitrainer: Trainieren in Simulationen bedeute, „selbst zu erleben … in der Situation zu sein". Es ermögliche Polizeibeamt*innen das Erleben von Einsatzsituationen in „Echtzeit" und eigne sich somit als Tool zur Vorbereitung „für die Wirklichkeit durch die Wirklichkeit".[25] Die virtuelle Lernumgebung wird zur Wirklichkeit erklärt und darin gemachte Erfahrungen mit Einsatzerfahrungen verglichen. Die Hoffnung, dass „reale" Polizeieinsätze

24 s. Akhgar, B.: Serious Games for Enhancing Law Enforcement Agencies. From Virtual Reality to Augmented Reality, Cham 2019; Giessing, L.: The Potential of Virtual Reality for Police Training Under Stress: A SWOT Analysis, in: Arble, P.; Arnetz, B. (Hg.): Interventions, Training, and Technologies for Improved Police Well-Being and Performance, Hershey 2021, S. 102-124

25 https://youtu.be/oKRHw8YXeck

durch den Einsatz von VR in Zukunft besser vorbereitet werden können, teilt etwa auch die Polizei NRW: Im Mitarbeitermagazin „Streife" wird die Implementierung der Technologie im Rahmen des Projekts SHOTPROS als „Quantensprung" für polizeiliche Fort- und Ausbildung bezeichnet. Das VR-Training sei „die Zukunft" des Polizeitrainings und könne dabei helfen, die Entscheidungsfindung von Polizist*innen in Hochrisikosituationen zu verbessern.[26]

Einen dritten Vorteil von VR-Training sieht eine Einsatztrainer*in, die an der Erprobung der Technik im polizeilichen Ausbildungszentrum der Polizei NRW beteiligt war, in der Möglichkeit, ein sogenanntes „After-Action-Review" durchzuführen.[27] Die beim Training in virtuellen Welten generierten Daten über die Übenden und den Übungsverlauf ermögliche eine detaillierte Auswertung von Trainingssequenzen anhand verschiedener Metadaten, wie den Bewegungsabläufen, individuellen Sichtfeldern oder körperlichen Stressindikatoren. Ein Ziel des Einsatzes von VR im Polizeitraining sei es demnach, mit Hilfe des direkten Feedbacks Trainings effektiver zu evaluieren und dadurch in der Durchführung von Strategien und Taktiken größere Sicherheit zu erlangen. Dies führe wiederrum zu einer erhöhten Stressresistenz von Polizeibeamt*innen in Hochrisikosituationen.[28]

Diesen konkreten Hoffnungen und Erwartungen stehen jedoch einige Limitationen und kritische Anmerkungen entgegen, weshalb etliche Polizeien mit der Implementierung der Technologie zögern. Dem Argument der geringeren Kosten stehen beispielsweise hohe Anschaffungskosten für die notwendige Infrastruktur gegenüber. Zur Realisierung von VR-Trainings benötigt man neben der teuren Technik z. B. auch ausreichend große Übungshallen, die sich bestenfalls – je nach virtueller Welt – umbauen lassen, damit virtuelle Architektur eine reale materielle Entsprechung erhält. Hinzu kommen neue Personalaufwände, die notwendig sind, um die Technologie zu verwalten und entsprechende Szenarien zu entwerfen. Einsatztrainer*innen, die mit VR arbeiten, bräuchten eine entsprechende Zusatzqualifikation, um die weitreichenden Möglichkeiten der virtuellen Welt überhaupt für ihre Zwecke nutzen zu können. Entsprechend warnen Kritiker*innen vor anfallenden Opportunitätskosten,

26 Zorn a.a.O. (Fn. 1), S. 6 u. 8
27 ebd.
28 Giessing a.a.O. (Fn. 24)

die Mittel binden, die anderweitig eingesetzt werden könnten.[29] Polizeiliches Einsatztraining mithilfe von VR könnte demzufolge vor allem eine Kostenverschiebung statt eine Ersparnis bedeuten. Zudem kommt mit der teuren Anschaffung von moderner Technik immer auch eine Pfadabhängigkeit ins Spiel. Denn ist die Technik erstmal angeschafft und implementiert, spielt die Frage nach dem tatsächlichen Nutzen eine nebensächliche Rolle. Erfahrungsgemäß weitet sich die Nutzung nach der Einführung häufig über den ursprünglichen Zweck hinaus auf andere Anwendungsbereiche aus.[30]

Darüber hinaus stellen sich Fragen nach der Repräsentativität von virtuellen Welten und den Transfermöglichkeiten des Erlernten in die „reale" Welt. VR-Trainings folgen eigenen Rationalitäten des Erfahrens, die sich von der „realer" Welten unterscheiden. Virtuelle Welten sind zunächst vor allem visuelle Projektionen, die sich dementsprechend in erster Linie visuell erfahren lassen. Technologien, die andere Sinne, etwa durch Vibrationen oder Geruchsstoffe, ansprechen sollen, befinden sich derzeit noch in einem experimentellen Stadium und können die Lücke zwischen dem Erfahren virtueller Welten und dem Erfahren der „realen" Welt nicht schließen. Während auch in traditionellen Trainings Komplexitätsreduktionen angelegt sind, kommen in der XR durch die virtuelle Darstellung eigene Reduktionen hinzu. Die Szenarien entstehen nicht organisch, dadurch wirken die Welten häufig aufgeräumt und künstlich, sodass zwischen der zu trainierenden „Realität" und dem trainierten Szenario eine gewisse Distanz angelegt ist.[31] Hinsichtlich dieser Lücken zwischen „Realität" und Simulation muss die Frage nach (nichtintendierten) Lerneffekten ins Zentrum der Aufmerksamkeit gestellt werden. Ansonsten läuft das Polizeitraining Gefahr, eine „Realität ohne Original" zu simulieren.[32]

Auch dem vermeintlichen Vorteil einer evidenz-orientierten Evaluationsmöglichkeit durch die im VR-Training generierten Daten lassen sich verschiedene Argumente entgegenhalten. So stehen die Polizeibehörden vor Datenschutz- und Speicherkapazitätsproblemen. Laut Aussagen von

29 s. Staller, M.; Koerner, S.: Einsatztraining und Digitalität, in: Rüdiger, T.; Bayerl, P. (Hg.): Handbuch Cyberkriminologie, Wiesbaden 2020, S. 1-23

30 s. Koops, B.: The Concept of function creep, in: Law, Innovation and Technology 2021, H. 1, S. 29-56

31 s. von der Burg, L. u.a.: Training beyond boundaries? Virtual reality scenario training as worldmaking for complex, life threatening situations, in: Wolff-Seidel, S.; Seidel, M. (Hg.): Gaming and Geography: A multi-perspective approach to understanding the impacts of gaming on geography (education), Wiesbaden 2023 (im Erscheinen)

32 Staller; Koerner a.a.O. (Fn. 29) S. 17

beteiligtem Personal haben deutsche Polizeibehörden derzeit zumeist keine ausreichende Serverinfrastruktur, um die Massen an Trainingsdaten, die potentiell erhoben werden können, temporär oder dauerhaft speichern und evaluieren zu können. Hinzu kommt, dass die persönlichen Daten, die potentiell über die trainierenden Beamt*innen erhoben werden sollen, neue persönlichkeitsrechtliche Fragen aufwerfen. Welche Daten sollen warum und in welcher Form gespeichert werden und welche Schlüsse werden warum daraus gezogen? Welche Konsequenzen können beispielsweise „schlechtere" Werte für Beamt*innen bei ihrer Berufsausübung haben? Hinzu kommen Fragen zur Operationalisierung entsprechender Evaluationen. Ohne wissenschaftliche Methodenbegleitung droht eine strukturelle Verankerung von Fehlschlüssen und Pseudoevidenzen ins polizeiliche Einsatztraining Einzug zu erhalten.

Beware the hype: VR als Modernisierungsversprechen

Abseits von dem Ziel der Verbesserung des Einsatztrainings erwarten sich Polizeibehörden durch die Erprobung und Implementierung von VR-Technologien auch ein Image als moderne, zukunftsorientierte Institutionen, die den Herausforderungen und Gefahren einer digitalen Gegenwart gewachsen sind. Die Polizeiakademie Niedersachsen möchte mit der Einführung von XR-Technologien etwa ein „veränderte(s) Lernverhalten der Generation Y" berücksichtigen. Einem Bericht zum „Campus 4.0" zufolge sollen die Technologien eine Ausbildung ermöglichen, die „nah an der Wirklichkeit" ausgerichtet ist.[33] So erscheinen XR-Technologien gleichermaßen als Bemühung um das Image als Arbeitgeber und Sicherheitsdienstleister. Polizeien wollen als digitale Vorreiter auftreten, um junge Menschen anzusprechen und sehen XR-Technologien als Teil einer notwendigen Modernisierung. Diese Modernisierung betrifft auch das crime-fighting selbst. Der Interessenverbund Interpol und die europäische Behörde Europol machten jüngst mit Veröffentlichungen zum Metaverse auf sich aufmerksam. Mithilfe des Launches eines „global police metaverse" verspricht man sich bei Interpol ein besseres Verständnis von digitalen Anwendungen, um diese in Zukunft besser polizieren zu können: „Um das Metaverse zu verstehen, müssen wir es erfahren."[34] In einem Bericht

33 https://digitalagentur-niedersachsen.de/digitaler-ort-polizeiakademie-niedersachsen

34 INTERPOL launches first global police Metaverse, Pressemitteilung Interpol v. 20.10.2022, eigene Übersetzung

von Europol zum Metaverse werden virtuelle Welten als nützlich für Polizeitrainings, aber auch als Mittel für Propaganda, Rekrutierung und Training von Terrorist*innen beschrieben. Dementsprechend sei es notwendig, dass sich Polizeibehörden mit virtuellen Welten vertraut machen.[35] Die Beispiele rahmen VR bzw. XR als Zukunftstechnologiefeld, welches das Potential hätte, konventionelle Formen von Policing und dessen Ausbildung zu revolutionieren oder gar zu ersetzen. VR erscheint hier als „hot shit", der auch deshalb nützlich und anschlussfähig für Polizeien ist, weil er gerade intensiv beforscht und gefördert wird.[36] Zudem wirken „Zukunftstechnologien" wie VR anziehend auf Polizeien, da sie als scheinbare Antworten auf wiederkehrende Fragen nach Innovation und Modernität wirken.[37] VR-Technologien unterstützen die folgende Erzählung: Polizeien sind attraktive, moderne Sicherheitsdienstleister, die mit der Zeit gehen, sich didaktisch und technologisch neu aufstellen und so in der Lage sind, komplexe Lagen in realen und virtuellen Welten zu lösen und Sicherheit herzustellen. Technologien aus Modernisierungsgründen einzuführen ohne den konkreten Nutzen vorher zu untersuchen und nachzuweisen droht allerdings eine zweite Pfadabhängigkeit zu erzeugen. Technologische Modernisierung wird zum Selbstzweck, während die Problemlösung des Einsatztrainings auf potentiell unausgereifte Technik ausgelagert wird.

Fazit

Die Anschaffung und Implementierung von VR-Technologien sollen als Lösung für verschiedene polizeiliche Probleme fungieren. Neben Verbesserungen für und Vergünstigung von Einsatztrainings soll es Polizeien dabei helfen Cybercrimefighting zu üben und das Image eines modernen, attraktiven Arbeitgebers und kompetenten Sicherheitsdienstleister anzustreben. Bisherige VR-Erprobungen bespielen vor allem den letzten Punkt, und es ist davon auszugehen, dass die Technologien das traditionelle Einsatztraining nicht komplett ablösen werden, da die Repräsentativität von virtuellen Welten dafür nicht ausreicht. Wohl aber wird sich

35 Europol report finds metaverse police presence key to public engagement, Pressemitteilung Europol v. 21.10.2022

36 Mohr, E.: Hot Shit: Über die semiotische Konkurrenz von Marken, in: Kursbuch 194 (2018), S. 135-149; Staller; Koerner a.a.O. (Fn. 29)

37 ebd.

das Einsatztraining durch ein vermehrtes Auftauchen der Technologien verändern. Dabei gilt es derzeit insbesondere die Aushandlungen zu datenschutzrechtlichen Fragen und Repräsentativitätsanforderungen im Blick zu behalten und die Inhalte des Einsatztrainings genauso kritisch zu begutachten wie deren äußere Form. Außerdem bleibt zu beobachten, welche Kompetenzen die Polizeien durch die neuen Technologien und die Anstellung/Ausbildung des zugehörigen technischen Personals hinzugewinnen. In jedem Fall verstärkt die derzeitige Erprobung von VR-Technologien den Trend der Verstrickung von Polizeien mit privatwirtschaftlichen Akteuren, wie hier den diversen VR-Soft- und Hardwareprovidern.

Umkämpftes Demonstrationsrecht

Zum Entwurf eines hessischen Versammlungsgesetzes

von Marius Kühne

Hessen plant, wie bereits andere Bundesländer, ein Landesversammlungsgesetz. Bezüglich vieler Fragen würde dies schlicht die bestehende Rechtsprechung fortschreiben und könnte daher mehr Rechtsklarheit schaffen. Allerdings soll die Polizei Versammlungen auch umfassend überwachen und unter geringen Voraussetzungen in das Geschehen eingreifen dürfen. Progressive Ansätze wie die Abschaffung versammlungsspezifischer Strafvorschriften fehlen hingegen. Der Gesetzesentwurf der schwarz-grünen Regierung wird der verfassungsrechtlichen Bedeutung des Grundrechts auf Versammlungsfreiheit daher nicht gerecht.

Das Versammlungsgesetz des Bundes ist hoffnungslos veraltet und gibt unkundigen Leser*innen teilweise einen verfälschten Eindruck der Rechtslage. So legt etwa § 14 Abs. 1 Bundesversammlungsgesetz (BVersG) fest, dass eine Demonstration, „spätestens 48 Stunden vor der Bekanntgabe der zuständigen Behörde ... anzumelden" sei. Dabei ist allgemein anerkannt, dass als Reaktion auf aktuelle Ereignisse auch kurzfristige Eil- oder Spontanversammlungen zulässig sind. Im Gesetzestext findet sich dazu jedoch nichts. Genauso nennt § 3 Abs. 1 BVersG das Verbot, „in einer Versammlung Uniformen, Uniformteile oder gleichartige Kleidungsstücke als Ausdruck einer gemeinsamen politischen Gesinnung zu tragen", verschweigt jedoch, dass Streikwesten, Arbeitskleidung, Fußballtrikots o. ä. hiervon nicht umfasst sind. Das sogenannte Uniformverbot gilt nach der Rechtsprechung nur, wenn die Kleidung eine „suggestiv-militante", einschüchternde Wirkung gegenüber Dritten erzielt. Dieser Zustand, dass das geschriebene Recht sich von der tatsächlichen Rechtslage erheblich unterscheidet, ist im besonders grundrechtssensiblen Bereich der Versammlungsfreiheit ein Ärgernis.

Dass das Bundesversammlungsgesetz nicht weiterentwickelt und an die Rechtsprechung angepasst wird, liegt daran, dass seit der Föderalismusreform 2006 die Gesetzgebungskompetenz für das Versammlungsrecht bei den Ländern liegt. Davon haben bisher Bayern (2008), Sachsen-Anhalt (2009), Niedersachsen (2010), Sachsen (2012), Schleswig-Holstein (2015) sowie Berlin und Nordrhein-Westfalen (beide 2021) Gebrauch gemacht und eigene Landesversammlungsgesetze beschlossen. Der Vergleich der zuletzt von einer rot-rot-grünen Koalition in Berlin und von einer schwarz-gelben Koalition in Düsseldorf verabschiedeten Gesetze zeigt dabei parteipolitische Unterschiede in der Versammlungsgesetzgebung auf: Während das Berliner Gesetz trotz einiger Defizite als das wohl liberalste Landesversammlungsgesetz gelten kann, scheint das Gesetzgebungsvorhaben in NRW von einer größtmöglichen Abneigung gegen den grundrechtlich geschützten Gebrauch der Versammlungsfreiheit getragen zu sein.[1]

Gesetzesentwurf in Hessen: nicht nur Klarstellungen

Im November 2021 legte nun auch die hessische Landesregierung einen Gesetzesentwurf zur Neuregelung des Versammlungsrechts (VersG-E HE) vor.[2] Dieser ist in seiner Struktur weitgehend an dem zuletzt in NRW beschlossenen Gesetz sowie einem von Wissenschaftlern erarbeiteten Mustergesetzentwurf für ein Versammlungsgesetz orientiert.[3] Für Rechtsanwender*innen ist ein solches modernes Landesversammlungsgesetz erst einmal vorteilhaft, da es eine Vielzahl von Detailfragen verbindlich und systematisch regelt. So sieht etwa § 12 VersG-E HE im Einklang mit der Rechtsprechung vor, dass die Anmeldefrist für Eilversammlungen verkürzt wird (Abs. 5) oder für Spontanversammlungen entfallen kann (Abs. 6). Derartige für die Praxis hilfreiche Klarstellungen dürfen jedoch nicht darüber hinwegtäuschen, dass der Gesetzesentwurf auch etliche versammlungserschwerende Setzungen enthält. Hinsichtlich der Anzeige (umgangssprachlich: Anmeldung) von Versammlungen, die im Regelfall weiterhin 48 Stunden vor der Durchführung der Versammlung erfolgen muss, schreibt § 12 Abs. 1 S. 2 VersG-E HE vor, dass „bei der Berechnung

1 vgl. Kühne, M.: Ein Stück gebändigte Demokratie, in: Bürgerrechte & Polizei/CILIP 125 (April 2021), S. 58-68

2 LT Hessen Drs. 20/9471 v. 4.11.2022

3 Arbeitskreis Versammlungsrecht: Musterentwurf eines Versammlungsgesetzes (ME VersG), München 2011

der Frist Sonn- und Feiertage außer Betracht" bleiben. Faktisch erhöht sich damit in bestimmten Konstellationen die Anmeldefrist, ohne dass es dafür einen schlüssigen Grund gäbe. Große Versammlungen mit hohen Teilnehmer*innenzahlen, die z. B. umfassende Verkehrsumleitungen erforderlich machen, werden ohnehin bereits lange im Vorfeld angekündigt und beworben, für kleine Versammlungen ist eine Anmeldung 48 Stunden vor Beginn in der Regel völlig ausreichend. Eine vergleichbare Regelung im nordrhein-westfälischen Entwurf für ein Landesversammlungsgesetz wurde deshalb auch nach kritischen Äußerungen im Laufe des Gesetzgebungsverfahrens gestrichen.

Auch eine andere Parallele zum nordrhein-westfälischen Versammlungsgesetz hat das Potential, Veranstalter*innen von Versammlungen von der Wahrnehmung ihres Grundrechts abzuhalten. Nahezu wortgleich zu § 12 Abs. 2 VersG NRW normiert § 12 Abs. 8 VersG-E HE die Pflicht der Versammlungsleitung, der Polizei auf Anforderung die persönlichen Daten der vorgesehenen Ordner*innen mitzuteilen. Voraussetzung dafür soll lediglich die polizeiliche Sorge sein, dass von der Versammlung (nicht von den jeweiligen Ordner*innen!) eine Gefahr für die öffentliche Sicherheit ausgeht – was mit Gefahren für den Straßenverkehr bei nahezu jeder Versammlung gegeben sein dürfte. Die Vorschrift ist rechtspraktisch und politisch hochproblematisch: Veranstalter*innen organisieren die Ordner*innen häufig spontan, verfügen also im Vorfeld der Versammlung in der Regel gar nicht über die von der Polizei verlangten Daten. Zudem rekrutieren sich Ordner*innen häufig aus dem Umfeld der Veranstalter*innen, insbesondere wenn Bündnisse verschiedener Gruppen gemeinsam eine Demonstration veranstalten. Gerade bei politisch kontroversen Anliegen, etwa aus dem Bereich des Antifaschismus oder der Klimagerechtigkeit, fürchten die Beteiligten aus nachvollziehbaren Gründen eine Erfassung und Ausforschung durch die Polizei. Die Vorschrift des § 12 Abs. 8 VersG-E HE könnte dazu führen, dass sich für solche gesellschaftlich wichtigen Anliegen zukünftig weniger Ordner*innen finden, was die Wahrnehmung des Versammlungsrechts erschweren würde. Es ist zudem damit zu rechnen, dass die derart erhobenen Daten regelmäßig an den polizeilichen Staatsschutz sowie Verfassungsschutzbehörden übermittelt werden. Dafür erforderliche Regelungen zur Datenverarbeitung und Datenübermittlung sieht der Gesetzesentwurf jedoch nicht vor. Auch fehlt es an den obligatorischen datenschutzrechtlichen Vorkehrungen für sensible personenbezogene Daten, u. a. zu politischen und weltanschauli-

chen Ansichten, wie sie mit dem Versammlungskontext regelmäßig verbunden sind. Damit bereitet die Norm Verstößen gegen das Grundrecht auf informationelle Selbstbestimmung den Weg.

Vorsicht: Überwachung!

Ebenfalls dem nordrhein-westfälischen Versammlungsgesetz nachgebildet sind die weitreichenden Befugnisse zur Videobeobachtung und -aufzeichnung. Wie schon nach § 12a Abs. 1 BVersG soll es in Hessen der Polizei auch zukünftig erlaubt sein, Bild- und Tonübertragungen in Echtzeit sowie entsprechende Aufzeichnungen anzufertigen, wenn „tatsächliche Anhaltspunkte die Annahme rechtfertigen", dass von einer Person innerhalb der Versammlung eine „erhebliche Gefahr" ausgeht (§ 17 Abs. 2 VersG-E HE). Rechtsstaatlich bedenklich sind jedoch vor allem die sogenannten „Übersichtsaufnahmen", die mit dem Gesetz neu eingeführt würden. Diese dürfen zur „Lenkung und Leitung des Polizeieinsatzes" angefertigt werden, wenn dies „wegen der Größe und Unübersichtlichkeit der Versammlung im Einzelfall erforderlich ist" (§ 17 Abs. 2 VersG-E HE). Problematisch ist daran vor allem die geringe Eingriffsschwelle für das polizeiliche Filmen. Nahezu jede Versammlung weist eine gewisse Unübersichtlichkeit auf; die Gesetzesbegründung geht selbst davon aus, dass diese auch bei kleinen Versammlungen mit unter 100 Teilnehmenden gegeben sein kann.[4] Filmaufnahmen haben jedoch immer eine potentiell einschüchternde Wirkung, die sich durch technische Entwicklungen wie automatisierte Gesichtserkennung noch verstärken kann. Versammlungsteilnehmer*innen müssen damit rechnen, durch den Staat in ihrer politischen Betätigung erfasst zu werden. Die Übersichtsaufnahmen dürfen beim Vorliegen einer erheblichen Gefahr auch dafür genutzt werden, einzelne Versammlungsteilnehmer*innen zu identifizieren. Zwar muss die Polizei die Versammlungsleitung über die Anfertigung von Übersichtsaufnahmen oder -aufzeichnungen informieren, für Teilnehmer*innen ist jedoch nicht ersichtlich, zu welchem Zweck gefilmt wird.

Immerhin unterscheidet sich der hessische Gesetzesvorschlag von seinem nordrhein-westfälischen Pendant, indem er vorschreibt, dass die Übersichtsaufnahmen nur offen angefertigt werden dürfen (§ 17 Abs. 2 S. 1 VersG-E HE). In NRW ist dies sogar heimlich zulässig (§ 16 Abs. 3 S. 3 VersG NRW). Grundrechtsschonender wäre es jedoch gewesen, auf das

4 LT Hessen a.a.O. (Fn. 2), S. 41

Instrument der Übersichtsaufnahmen vollständig zu verzichten oder wenigstens, wie es das Berlin Versammlungsgesetzt vorsieht (§ 18 Abs. 2 VersG BE), die Identifizierung von Einzelpersonen mittels Übersichtsaufnahmen zu untersagen.

Die Überwachung von Versammlungsteilnehmer*innen kann grundsätzlich auch durch eingesetzte Zivilpolizist*innen erfolgen. Wenngleich gegen diese Vorschrift vermutlich regelmäßig verstoßen wurde, galt bisher, dass sich Polizeibeamt*innen in Zivil der Versammlungsleitung zu erkennen geben müssen (§ 12 BVersG). In § 11 S. 2 VersG-E HE wird diese Pflicht nun dahingehend abgeschwächt, dass es ausreichen soll, dass die Einsatzleitung den Leiter*innen einer Versammlung allgemein mitteilt, das zivile Polizeikräfte eingesetzt werden. Dies trägt zwar der Versammlungsfreiheit eher Rechnung, als die Pflicht wie in Nordrhein-Westfalen und Sachsen-Anhalt vollständig abzuschaffen, ist aber dennoch aus bürgerrechtlicher Sicht ein Rückschritt gegenüber der bisher geltenden bundesgesetzlichen Regelung.

Die Anwesenheit uniformierter Polizeieinheiten birgt hingegen andere Probleme: Sie hat einerseits ein Abschreckungspotential für potentielle Teilnehmer*innen, indem sie suggeriert, von einer Versammlung gingen Gefahren aus. Andererseits erschwert eine starke Polizeipräsenz die kommunikative Außenwirkung einer Versammlung gegenüber der Öffentlichkeit. Vor diesem Hintergrund ist § 11 S. 1 Nr. 1 VersG-E HE kritisch zu sehen, der für ein Anwesenheitsrecht der Polizei bei öffentlichen Versammlungen lediglich voraussetzt, dass „dies zur polizeilichen Aufgabenerfüllung nach diesem Gesetz erforderlich ist". Damit gibt die Gesetzgebung keinerlei Eingriffsschwelle für die polizeiliche Präsenz bei Versammlungen vor bzw. stellt diese ausschließlich in das Ermessen der Einsatzkräfte.

Licht und Schatten bei der Bestimmtheit

Wie weit polizeiliche Befugnisse reichen, hängt auch davon ab, ob und wie klar gesetzlichen Hürden für das polizeiliche Eingreifen und Kriterien für straf- und bußgeldbewehrte Verhaltensweisen durch die Versammlungsteilnehmer*innen definiert sind. Versammlungsbeschränkende Maßnahmen durch die Polizei setzen in der Regel das Vorliegen einer Gefahr für die öffentliche Sicherheit voraus. Einige Landespolizeigesetze und auch das Bundesversammlungsgesetz sehen zudem vor, dass die Polizei bereits bei einer unmittelbaren Gefährdung der „öffentlichen Ordnung"

einschreiten darf. Der Begriff der öffentlichen Ordnung nimmt auf die „jeweils herrschende sozialen und ethischen Anschauungen" Bezug.[5] Er ist mangels klarer Abgrenzbarkeit ungeeignet, Freiheitseinschränkungen in besonders grundrechtssensiblen Bereichen zu rechtfertigen. Zudem hat die Versammlungsfreiheit als Minderheitengrundrecht gerade die Funktion, die sozial-ethischen Anschauungen der Mehrheit in Frage zu stellen, um zukünftig andere gesellschaftliche Mehrheiten zu erkämpfen.[6] Aus diesen Gründen haben bereits Sachsen-Anhalt, Schleswig-Holstein, Nordrhein-Westfalen und auch Berlin, das allerdings zugleich ähnlich vage eine irgendwie vermittelte „Gewaltbereitschaft" allein zum Eingriffskritierium macht,[7] den Begriff aus ihren Versammlungsgesetzen gestrichen. Der Entwurf in Hessen hält dennoch an dem überkommenen Schutzgut der „öffentlichen Ordnung" fest.

Demgegenüber scheint die Formulierung des sog. „Uniform-, Militanz- und Einschüchterungsverbots" (§ 9 Abs. 1 VersG-E HE) besser gelungen zu sein. Danach ist es „verboten, in einer Versammlung 1. Uniformen, Uniformteile oder uniformähnliche Kleidungsstücke zu tragen oder 2. paramilitärisch aufzutreten oder in vergleichbarer Art und Weise mit anderen Personen zusammenzuwirken, wenn dadurch der Eindruck von Gewaltbereitschaft vermittelt oder eine einschüchternde Wirkung erzeugt wird." Im Gegensatz zum Gewalt- und Einschüchterungsverbot in NRW knüpft § 9 Abs. 1 VersG-E HE am individuellen Verhalten an und nicht an der Leitung von oder Teilnahme an Versammlungen, in denen das Verhalten einiger Teilnehmer*innen „militant" wirkt. Zudem wird versucht, durch weitere Kriterien das paramilitärische Auftreten oder vergleichbare Zusammenwirken näher zu spezifizieren, indem etwa „das Marschieren in Marschordnung, das Erteilen militärischer Kommandos oder andere besondere Begleitumstände" (§ 9 Abs. 1 S. 2 VersG-E HE) als beispielhafte Verhaltensweisen genannt werden. Zwar wirkt positiv, dass anders als in § 27 Abs. 8 VersG NRW ein Zuwiderhandeln nur mit einem Bußgeld und nicht als Straftat geahndet wird. Wünschenswert wäre jedoch gewesen, das Verbot analog zum Berliner Versammlungsgesetz dahingehend zu beschränken, dass das Verhalten nicht nur Gewaltbereitschaft vermitteln und einschüchternd wirken kann, sondern auch dazu „bestimmt" ist, also

5 Depenheuer, O.: Art. 8 GG, in: Maunz, T.; Düring, G. u.a.: Grundgesetz, 92. Ergänzungslieferung, München 2020, Rn. 155

6 Barczak, T.: § 15, in: Ridder, H.; Breitbach, M.; Deiseroth, D. (Hg.): Versammlungsrecht, 2. Aufl., Baden-Baden 2020, Rn. 163 (mit weiteren Nachweisen)

7 zu den Besonderheiten Berlins: Kühne a.a.O. (Fn. 1), S. 65

angenommen werden kann, dass die Wirkung intendiert ist (§ 9 Abs. 2 VersG BE). Sorge bereitet hier zudem die Gesetzesbegründung, die bereits das Zusammenschließen zu thematischen Blöcken bei „linksextremistischen Versammlungen" als Ausdruck von „Gewalt- und Kampfbereitschaft" bezeichnet.[8] Dies verkennt die Gestaltungsfreiheit von Versammlungen.

Gefahrenperspektive statt Versammlungsfreiheit

Im Versammlungsrecht zeigt sich, wie ein Staat mit unbequemen Protesten gegen die von der parlamentarischen Mehrheit getragene Politik umgeht. Das Versammlungsrecht soll dabei vor allem gesellschaftliche Minderheiten darin schützen, ihre Position auf die Straße zu tragen und gegenüber der politisch repräsentierten Mehrheit der Wahlberechtigten zu artikulieren. Damit ist ein vielfältiges Versammlungsgeschehen Wesensmerkmal einer lebendigen Demokratie. Der hessische Gesetzesentwurf scheint Versammlungen jedoch primär als eine Gefahr zu betrachten, der durch umfassende Überwachungsmaßnahmen sowie Erschwernisse bei der Anmeldung begegnet werden soll. Sollte der Gesetzesentwurf so vom Landtag beschlossen werden, stellt sich überdies die Frage, wo die grüne Handschrift des kleineren Partners einer der schwarz-grünen Koalition zu erkennen sein soll. Der Gesetzestext liest sich weitgehend wie klassische CDU-Politik.

Progressive Elemente sucht man hingegen vergeblich. Beispielsweise hätten drei Jahre Pandemie, in denen auf Demonstrationen regelmäßig FFP2-Masken getragen wurden, einen Anlass bieten können, das strafbewehrte Vermummungsverbot zu lockern. Dies gilt umso mehr, als die Rechtsprechung zuletzt sogar das Tragen einer Vermummung zum Schutz vor Bildaufnahmen durch Fotograf*innen der extremen Rechten als strafbar ansah (und nicht nur die Vermummung gegenüber der Polizei).[9] Auch hätte die Anzeige kleiner Versammlungen erleichtern werden können, anstatt das Verfahren insgesamt zu erschweren. Es gibt keinen sachlichen Grund dafür, dass für Kleinstversammlungen mit wenigen Personen die gleichen Pflichten gelten wie für Großdemonstrationen mit vielen Tausend Teilnehmer*innen. Wünschenswert im Sinne der Versammlungsfreiheit wäre zudem eine Verpflichtung der Versammlungsbehörde,

8 LT Hessen Drs. 20/9471 v. 4.11.2022, S. 27

9 Gauseweg, S.: Zum Abschuss freigegeben. Demonstrierende haben kein Recht auf Selbstschutz vor rechten Fotografen, in: Kritische Justiz 2022, H. 4, S. 494-502

den Anmelder*innen von Versammlungen Einsicht in alle Dokumente der Gefahrenprognose zu gewähren und etwaige Auflagen frühzeitig zu erteilen, um deren gerichtliche Überprüfung noch vor Beginn der Versammlung zu ermöglichen. Auch sollten progressive Versammlungsgesetze ausdrückliche Regeln zum Schutz von Pressevertreter*innen, zum Zugang für parlamentarischen Beobachter*innen sowie zur Befugnis aller Versammlungsteilnehmer*innen, den Polizeieinsatz zu filmen, enthalten.

Grundsätzlich schaffen die detaillierten Regelungen im geplanten Landesversammlungsgesetz, gegenüber dem nur durch die Rechtsprechung erneuerten Bundesgesetz, Rechtssicherheit. Dieser Vorteil darf jedoch nicht über die weitreichenden neuen Überwachungsbefugnisse der Polizei hinwegtäuschen, die der Gesetzentwurf vorsieht. Zudem enthalten bereits die Klarstellungen zur Bundesrechtsprechung bisweilen versteckte Einschränkungen des Versammlungsrechts. So legt etwa § 19 VersG-E HE zwar fest, dass Versammlungen auch auf den Privatgrundstücken von Unternehmen, die in öffentlicher Hand sind, durchgeführt werden dürfen und setzt damit das sog. Fraport-Urteil[10] des Bundesverfassungsgerichts um. Der deutlich weiterreichende „Bierdosenflashmob"-Beschluss[11] des Gerichts, der die Versammlungsfreiheit auf alle Flächen im Privatbesitz ausdehnt, die der Öffentlichkeit (etwa zu kommerziellen Zwecken) zugänglich gemacht wurden, findet sich jedoch nicht – wie in NRW im Gesetz (§ 21 S. 1 VersG NRW) – wieder. Hier drängt sich die Vermutung auf, dass der zunehmenden Nutzung privater Flächen im Eigentum von Konzernen durch die Klimagerechtigkeitsbewegung zu Protestzwecken entgegengewirkt werden soll.

Im Herbst 2023 wird der hessische Landtag neu gewählt. Die Regierungskoalition wird versuchen, das Landesversammlungsgesetz zuvor zu verabschieden. Zu hoffen bleibt, dass sich die Abgeordneten zur Entschärfung des Gesetzesentwurfes durchringen können. Dafür braucht es eine (hessische) Zivilgesellschaft, die sich gegen die Einhegung des Versammlungsrechts zur Wehr setzt – am besten auf der Straße.

10 Bundesverfassungsgericht: Urteil v. 22.2.2011, Az. 1 BvR 699/06,
11 Bundesverfassungsgericht: Beschluss v. 18.7.2015, Az. 1 BvQ 25/15

Mit rechten Dingen?

Der „Fall Maninger" und das Studium in der Bundespolizei

von Anna M. Fauda

Berichte über einen Professor mit neurechter Vergangenheit an der „Hochschule der Bundespolizei" für die Ausbildung von Führungskräften sorgen weiter für Schlagzeilen. Ein Blick hinter die Kulissen zeigt, dass es sich keineswegs um einen Einzelfall handelt. Dahinter stehen strukturelle Mängel bei der Auswahl des Lehrpersonals – während kritische Perspektiven intern unterdrückt werden.

Anfang August 2021 berichteten die Investigativ-Journalisten Marcus Engert und Aiko Kempen erstmals über den „Fall Stephan Maninger",[1] einen Professor für Sicherheitspolitik an der Hochschule des Bundes für öffentliche Verwaltung, Fachbereich Bundespolizei. Obwohl die Innenrevision der Bundespolizeiakademie den Fall schnell zu den Akten hatte legen wollen, ebbte die öffentliche Berichterstattung nicht ab. So wurde im Februar 2023 berichtet, die Spitze des Innenministeriums habe gegen die Bundespolizeiakademie durchgesetzt, dass Maninger nicht wieder unterrichten dürfe. Seine Professur behält er zunächst aber, ohne Lehrauftrag. Der Grund liege in seiner Vergangenheit, unter anderem seinen Beziehungen zum „Institut für Staatspolitik", einem think-tank der „Neuen Rechten". Mittlerweile prüft das Bundesamt für Verfassungsschutz (BfV) den Fall.[2] Fraglich ist, ob das BfV auch der drängenden Frage nachgeht, welche strukturellen Bedingungen die Berufung von Maninger zum Professor für Sicherheitspolitik überhaupt erst ermöglicht haben.

Doch was ist und macht eigentlich die Hochschule des Bundes für öffentliche Verwaltung (HS Bund) und der dort angesiedelte Fachbereich Bundespolizei? Wie alle Hochschulen verfolgt sie ausweislich ihrer

1 Verdacht auf rechte Vergangenheit: Bundespolizei prüft Biographie eines Professors für Sicherheitspolitik, www.buzzfeed.de v. 5.8.2021

2 Verfassungsschutz überprüft Professor, www.tagesschau.de v. 15.2.2023

Grundordnung das Ziel, „den Studierenden die wissenschaftlichen Erkenntnisse und Methoden sowie berufspraktische Fähigkeiten und Kenntnisse, die zur Erfüllung der Aufgaben in ihrer Laufbahn erforderlich sind", zu vermitteln. Darüber hinaus soll sie „die Studierenden zu wissenschaftlicher Arbeitsweise und zu verantwortlichem Handeln in einem freiheitlich-demokratischen und sozialen Rechtsstaat ... befähigen." [3]

Polizei und Hochschule: Ein Überblick

Ob dies so erreicht wird, ist davon abhängig, welche Personen (Wer) welche Inhalte (Was) mit welchen Methoden (Wie) lehren. Das „Wer" betrifft die Auswahl des Lehrpersonals (Auswahl- bzw. Berufungsverfahren), das „Was" und „Wie" die Konzeption und Durchführung von Lehre. Hinsichtlich aller drei „W" zeigen sich am Fachbereich Bundespolizei problematische Konfliktfelder, die sich aus der schwer durchschaubaren Anbindung der Hochschuleinrichtung an die Sicherheitsbehörde „Bundespolizei" ergeben.

Die Studierenden am Fachbereich Bundespolizei sind Menschen mit sehr unterschiedlicher Vorbildung und Praxiserfahrung: Bei den einen handelt es sich um junge Polizeikommissaranwärter*innen, die nach dem Abitur ihr Studium aufgenommen haben oder die schon einen Berufs- bzw. Hochschulabschluss besitzen (sog. Einsteiger*innen), bei den anderen um praxiserfahrene Bundespolizist*innen des mittleren Dienstes (Bereitschaftspolizei, Streifendienst, grenzpolizeilicher Einzeldienst etc.), die über das Hochschulstudium den Aufstieg in den gehobenen Dienst erreichen wollen. Am Ende steht der Abschluss als „Diplom-Verwaltungswirt*in".

Das Studium ist von eher prekären Bedingungen geprägt. Mit der „Einstellungsoffensive" der Bundespolizei sind die Studierendenzahlen erheblich angestiegen. Zum 1. Januar 2021 begannen 800 Studierende ihr Hauptstudium in Lübeck. Lehrsäle, Unterkünfte, Sportsäle sind auf einen Bedarf von ca. 300 Studierenden ausgerichtet, die Bibliothek kann die Standards einer Hochschulbibliothek nicht erfüllen, für eine moderne Ausstattung der Hörsäle fehlen die Mittel ebenso wie für ein flächendeckendes WLAN.

3 Grundordnung der Hochschule des Bundes für öffentliche Verwaltung (HS BundGrO), § 2 Abs. 2

Da für „Bildung" nicht der Bund, sondern die Länder zuständig sind, kann der Bund eine Hochschule nicht als solche anerkennen und ihre Abschlüsse damit verbindlich machen. Das müssen für die HS Bund mit Sitz in Brühl das Land Nordrhein-Westfalen, für den Fachbereich Bundespolizei in Lübeck das Land Schleswig-Holstein tun. Ebenfalls in Lübeck sitzt die Bundespolizeiakademie (BPOLAK). Sie ist für die Aus- und Fortbildungszentren der Bundespolizei zuständig und untersteht dem Bundespolizeipräsidium in Potsdam. Die oberste Dienstbehörde ist jeweils das Bundesministerium des Innern und für Heimat (BMI). Über den Präsidenten der Bundespolizeiakademie, der zugleich die Funktion der Leitung des Fachbereichs Bundespolizei der HS Bund innehat, ist die Hochschuleinrichtung nicht nur lokal, sondern auch institutionell mit der Bundespolizei verflochten. Für die zivilen Hochschullehrenden führt das zu einem Zwiespalt: Das Dienstverhältnis besteht zur Bundespolizei, vertreten durch das Bundespolizeipräsidium. Als Hochschullehrende, zumal als wissenschaftliches Lehrpersonal, genießen sie die Lehr- und Forschungsfreiheit nach Art. 5 Abs. 3 GG, was unvermeidlich konfliktbehaftet ist; etwa bei der Frage, ob und inwieweit Forschung überhaupt und noch dazu: zu welchen Themen sie möglich ist. Die Lübecker Hochschuleinrichtung ist also durch ihre Anbindung an die Sicherheitsbehörde Bundespolizei in besonderer Weise vom Spannungsverhältnis zwischen der „Staatsaufgabe Sicherheit" und der „freiheitlichen Verfassung des Grundgesetzes" geprägt. Die Personalunion auf der Leitungsebene und die Eingliederung in das Hierarchiegefüge des BMI bringen es zudem mit sich, politischen und institutionellen Interessen der vollziehenden Staatsgewalt unmittelbar ausgesetzt zu sein.[4] Um dem Anspruch an Wissenschaftlichkeit genügen zu können, braucht es daher in besonderem Maße klare Regeln und Strukturen.

Maninger – kein Einzelfall

Mit der Einstellungsoffensive für die Bundespolizei ab dem Jahr 2015[5] und dem daraus entstehenden Bedarf an Führungskräften im gehobenen Dienst waren ab dem Jahr 2018 auch Neueinstellungen beim wissenschaftlichen Lehrpersonal am Fachbereich Bundespolizei der HS Bund er-

4 vgl. BT-Drs. 20/5474 v. 31.1.2023, S. 2f.

5 vgl. Burczyk, D.: Aufrüstung im Anti-Terror-Kampf. Mehr Geld, mehr Personal und neue Waffen für die Polizei, in: Bürgerrechte & Polizei/CILIP 112 (März 2017), S. 13-20

forderlich. Die Anforderungen für diese Stellen sind im Bundesbeamtengesetz (§ 131 BBG) und in der HSBundGrO festgelegt. Zu den Anforderungskriterien gehören neben der pädagogischen Eignung vor allem wissenschaftliche Leistungen. Die Ausschreibung der Stellen und die Einstellung des wissenschaftlichen Lehrpersonals erfolgen durch die Personalverwaltung des Bundespolizeipräsidiums, also einer eher wissenschaftsfernen Einrichtung. Gerade bei Auswahl- und Berufungsverfahren haben sich dabei gravierende Mängel gezeigt.

Einerseits werden extern erlangte akademische Leistungen in der Hochschullehre und Forschung (Promotion, teilweise Habilitation) nicht berücksichtigt, selbst wenn sie in der Stellenausschreibung verlangt werden. Ihre Anerkennung in der Eingruppierung oder Einstufung muss erstritten werden. So erhielten zum 1. Januar 2018 neue Stelleninhaber*innen, die sich auf Stellen als verbeamtete Lehrende beworben hatten, lediglich auf ein Jahr befristete Arbeitsverträge. Andererseits gibt es Fälle, in denen Personen Professoren*innenstellen (in der Besoldung W2 und W3) oder mit ihnen vergleichbare wissenschaftliche Stellen (in der Besoldung A13-15) erhielten, ohne formal oder tatsächlich die Anforderungen zu erfüllen.

Dies betrifft schon die Person Stephan Maninger selbst. Im August 2021 berichteten die Journalisten Aiko Kempen und Marcus Engert erstmals über seine möglicherweise rechtsextreme Vergangenheit.[6] Stephan Maninger, so ihre Ausführungen, habe in der Vergangenheit der rechten Sammlungsbewegung „Afrikaaner Volksfront" in Südafrika angehört und sei als deren Pressesprecher aufgetreten. Nachdem er Ende der 1990er Jahre nach Deutschland übergesiedelt war, hielt er, so die Journalisten weiter, einen Vortrag vor dem NSU-Unterstützerumfeld. Zudem gründete er das „Institut für Staatspolitik (IfS)" mit und publizierte Ende der 1990er Jahre gut zwei Dutzend Artikel in der „Jungen Freiheit", und zwar zu einer Zeit, als die Zeitung durch verschiedene Landesämter für Verfassungsschutz beobachtet wurde.

Die Bundesregierung behauptet hinsichtlich seiner Eignung: „Die Berufung von S. M. erfolgte in enger Anlehnung an übliche Professorenberufungsverfahren deutscher Hochschulen."[7] Doch hier bestehen erhebliche Zweifel. Denn anders als für Professuren im Fachgebiet „Sicherheitspolitik" üblich, verfügt Maninger über keinen zureichenden Abschluss in

6 vgl. Verdacht auf rechte Vergangenheit a.a.O. (Fn. 1)
7 vgl. BT-Drs. 20/5474 v. 31.1.2023., S. 5

Politikwissenschaften. Seine Promotion, in der er seine Vorstellung eines ethnisch verfassten „Volksstaates" darlegt, ist nur in zwei Bibliotheken in Südafrika überhaupt erhältlich. Einschlägige politikwissenschaftliche Veröffentlichungen in Fachpublikationen fehlen. Bis heute veröffentlicht er regelmäßig in der Österreichischen Militärischen Zeitschrift, herausgegeben vom Bundesministerium der Landesverteidigung.

Dort veröffentlicht ebenfalls ein Kollege Maningers, der zuweilen auch in den Medien als „Sicherheitsexperte" gehandelte Stefan Goertz. Sie teilten sich lange ein Büro in Lübeck. Goertz ist seit 2019 nicht nur ebenfalls Professor für Sicherheitspolitik, sondern im Fachbereich Beauftragter für „Radikalisierungsprävention". In der Sicherheitsforschung ist er durch einen nacherzählenden Publikationsstil mit hohem Output bekannt, wird jedoch auch scharf kritisiert. In einer unlängst erschienenen Rezension wird ihm vorgeworfen, seine Datenauswahl und Darstellung so zu gestalten, dass sie sich seinem möglicherweise vorhandenen Ziel anpasse, nämlich Angst zu schüren und für eine umfassende Ausweitung polizeilicher Kompetenzen zu werben.[8]

Ebenfalls als Mitautor von Maninger ist Holger Alisch in jüngerer Zeit in Erscheinung getreten.[9] Maninger soll sich 2019 im Berufungsverfahren für Alisch eingesetzt haben, obwohl es wissenschaftlich geeignetere Bewerber*innen gegeben habe, so mit den Vorgängen betraute Personen an der HS Bund. Von Alisch wiederum führt eine Linie unmittelbar zu Martin Wagener, Professor für Nachrichtendienstrecht an der HS Bund, dessen Doktorand er war und mit dem er mindestens bis 2018 in enger Verbindung stand. Nach mittlerweile zwei einschlägigen Veröffentlichungen mit Anleihen im neurechten „Ethnopluralismus" wurde Wagener die Sicherheitsfreigabe entzogen, damit endete seine Tätigkeit am „Zentrum für Nachrichtendienstliche Aus- und Fortbildung" des Bundesnachrichtendienstes.[10] In diesem Zusammenhang gibt es noch einen weiteren bemerkenswerten Vorgang. Zur gleichen Zeit wie Alisch studierte bei Wagener die Inhaberin einer wissenschaftlichen Stelle am Fachbereich Bundespolizei der HS Bund. Dem Vernehmen nach wurde sie, obwohl sie lediglich über einen politikwissenschaftlichen Hochschulabschluss verfügt, bei ihrem Auswahlverfahren 2017 einem habilitierten Politikwissenschaftler

8 Staller, M.S.; Koerner; S.: Gewalt gegen Polizistinnen und Polizisten — Analyse einer „aktuellen Analyse", in: Polizei – Studium – Praxis 2022, H. 2, S. 18-21

9 zuletzt: Alisch, H.; Maninger, S.: Die Ukraine: Der Weg in den Krieg – eine realistische Perspektive, in: Österreichische Militärische Zeitschrift 2022, H. 3, S. 328-332

10 BND entzieht Professor Sicherheitsfreigabe, www.tagesschau.de v. 2.6.2022

mit reichhaltiger Lehr- und Forschungserfahrung vorgezogen. Auch in anderen Berufungsverfahren gibt es mindestens Auffälligkeiten – zu viele Einzelfälle jedenfalls, um zufällig zu sein. Zu den Auffälligkeiten gehört auch, dass es für insgesamt acht in 2019 zu vergebende Professuren jeweils nur wenige oder nur eine Bewerbung(en) gab.

Systematische Mängel in Berufungsverfahren

Wie kann so etwas gehen? Es geht mit den jeweiligen Protagonist*innen in den Auswahl- und Entscheidungsgremien; und es gedeiht hervorragend in einer hierarchisch geprägten (Polizeiführungs-)Kultur, in der eigene Regeln herrschen und die Abschottung nach außen, ggf. nach oben, das Gebot der Stunde ist.

Das „Professorenberufungsverfahren", durch das Maninger seine Professur erhielt, verlief nach den eigenen Regeln (Tradition) der „alten Kollegenschaft" in den Auswahl- und Entscheidungsgremien (Berufungskommission, Fachbereichsrat, Senat). Bereits die Ausschreibung der Professur wich von der für Berufungsverfahren in Deutschland geltenden Regel ab. Üblich und hier auch gesetzlich gefordert ist die öffentliche Ausschreibung. Die Professur war dagegen nur im Intranet der Bundespolizei, also lediglich intern ausgeschrieben. Die Berufungskommission bestand nur aus dem engsten Kollegenkreis; zwei Kommissionsmitglieder waren zugleich in weiteren internen Berufungsverfahren als Bewerber involviert. Im Unterschied zum Standard bei ausgeschriebenen Professuren wurden keine externen Fachgutachten eingeholt oder hochschulfremde Professor*innen als Gutachter*innen gehört. Bei internen Auswahlverfahren ist das in besonderen Maßen erforderlich. Aus dem engsten, langjährigen Kollegenkreis bestand auch der Fachbereichsrat, jenes Gremium, das die von der Berufungskommission erstellte Vorschlagsliste mit den für die Professur ausgewählten Kandidat*innen beschließt. Zum Teil gehörten sie auch dem in Brühl ansässigen Senat der HS Bund an, der nach der Grundordnung zur Vorschlagsliste des Fachbereichs eine Stellungnahme anzufertigen hat. Findet sich in der Stellungnahme Kritik?

Nicht nur Maningers Verfahren ist weit entfernt vom Standard „übliche(r) Professorenberufungsverfahren deutscher Hochschulen". Solche Auswahlverfahren entwürdigen das Institut der Professur, schädigen die Reputation einer Hochschule als Garant für die Qualität von Bildung, mindern die wissenschaftliche Qualität in Ausbildung und Forschung,

und sie hinterlassen Spuren im Kollegium des wissenschaftlichen Lehrpersonals.

Die Innenrevision: Worüber nicht geprüft werden darf

Auch die dafür eigentlich vorgesehenen internen Kontrollmechanismen haben nicht nur dabei versagt, einen neurechten Ideologen vom Fachbereich Bundespolizei der HS Bund zu entfernen, sondern sie verhinderten eine kritische Auseinandersetzung mit rechten, autoritativen Tendenzen in der Polizei. Die Innenrevision der Bundespolizeiakademie prüfte die in den Medien berichteten Sachverhalte zur Sache Maninger und kam zu dem Schluss, das habe lange vor seiner Zeit bei der Bundespolizei stattgefunden und sei disziplinar- oder strafrechtlich nicht relevant.[11] In anderen Polizeien wird aus guten Gründen, gerade bei diesen Vorwürfen, eine externe Innenrevision beauftragt. Naheliegend wäre auch gewesen, die Revision durch das BMI durchführen zu lassen, das die Professor*innen hochschulrechtlich bestellt.

Doch die Innenrevision hält nicht nur Kritik von außen fern. Aus einem Gespräch einer neu eingestellten hauptamtlich Lehrenden mit der damaligen Vizepräsidentin der Bundespolizei Ulrike Meuser im Sommer 2018 wird die Aussage kolportiert, in Diplomarbeiten am Fachbereich Bundespolizei seien „sensible Themen", wie Polizei und Rechtsextremismus oder Polizei und Racial Profiling, besser auszuklammern. Bei solchen Themen bestünde das Risiko, dass der politische Gegner das gegen die Bundespolizei verwenden könne. Die Bundesregierung behauptet hingegen, es gebe keinen Einfluss der Innenrevision auf Prüfungen oder die Formulierung von Diplomarbeitsthemen.[12]

Aiko Kempen beschreibt mindestens einen Fall, der ein anderes Bild zeichnet: „Wie insbesondere die Bundespolizei die Hoheit über mögliche brisante Forschungsergebnisse behalten will, zeigt sich noch heute: Interne Dokumente der Bundespolizeiakademie belegen, dass selbst Studienarbeiten von angehenden Polizisten, die sich mit sensiblen Themen wie Extremismus auseinandersetzen wollen, bereits bei der Prüfungsanmeldung als „Verschlusssache – nur für den Dienstgebrauch" deklariert

11 Wie unkritisch die Bundespolizei die rechte Vergangenheit eines Polizeiprofessors bewertet, https://fragdenstaat.de v. 21.6.

12 BT-Drucksache 20/5474 v. 31.1.2023, S. 8

werden."[13] Es gibt Belege dafür, dass die vollständige Themenliste der angemeldeten Diplomarbeiten an die Innenrevision des Bundespolizeipräsidiums weitergereicht wird. Lehrende berichten, dass aus dieser Innenrevision bis in die jüngste Gegenwart hinein wiederholt Diplomarbeitsthemen umformuliert und mit dem Vermerk VS-NfD (Verschlusssache) versehen wurden und sich ein Mitarbeiter dort selbst zum Zweitgutachter ernannt hat. Dieser Umgang mit Diplomarbeitsthemen ist ein „offenes Geheimnis" und führt immer wieder zu einer Vorzensur bei der Themenauswahl.

Was bleibt?

Wer den Fachbereich Bundespolizei der HS Bund genauer betrachtet, wird Anzeichen von Günstlingswirtschaft erkennen (müssen). Wer darüber hinaus die Dinge kritisch betrachtet, wird sich die Frage stellen, ob diese Verhältnisse nicht auch ein Symptom sind für das, was am Fachbereich Bundespolizei letztlich eine wissenschaftsbasierte anwendungsbezogene Ausbildung behindert: Das Fehlen eines klaren Rechtsrahmens, von klaren Zuständigkeits- und Verantwortungsstrukturen für eine Hochschule im Machtbereich der vollziehenden Staatsgewalt. Im diffusen Graubereich zwischen Sicherheitsbehörde und Hochschule bleibt zu viel Raum für Macht und Willkür.

Hochschule als Ort der Bildung lebt von Freiheit durch Recht. Erst auf dieser Basis gedeihen langfristig Vertrauen, Respekt und Dialog innerhalb der Gemeinschaft der Lehrenden und Lernenden. Die Studierenden am Fachbereich Bundespolizei haben es verdient, an ihrer Hochschule diejenige wissenschaftsbasierte, berufsfeldbezogene Ausbildung zu erhalten, die sie auf ihre anspruchsvolle Polizeiarbeit im gehobenen Dienst der Bundespolizei vorbereitet. Dazu gehört die kritische Auseinandersetzung mit dem Vorfindlichen. Erst sie befähigt zur Reflexion über das eigene Tun und zu einem verantwortlichen Handeln für den freiheitlich-demokratischen und sozialen Rechtsstaat.

13 Kempen, A.: Auf dem rechten Weg? Rassisten und Neonazis in der deutschen Polizei, Berlin u.a. 2021, S. 183

Inland aktuell

Razzia bei „Radio Dreyeckland"

Die Polizei hat am 17. Januar das „Radio Dreyeckland" in Freiburg durchsucht und dabei mehrere Durchsuchungsbeschlüsse der Staatsanwaltschaft Karlsruhe vollstreckt.[1] Zehn Beamt*innen durchsuchten dabei die Redaktionsräume des ältesten deutschen Freien Radios, außerdem die Wohnsitze von zwei Redakteuren. Dort wurden unter anderem USB-Sticks und Mobiltelefone beschlagnahmt. Hintergrund ist ein Ermittlungsverfahren wegen des „Verdachts eines Verstoßes gegen ein Vereinigungsverbot". Die Webseite des Rundfunkkollektivs hatte einen Artikel veröffentlicht, der auf „Linksunten Indymedia" verlinkt. Darin wurde über die Einstellung des Ermittlungsverfahrens wegen „Bildung einer kriminellen Vereinigung" gegen „Linksunten" berichtet. Die Internetplattform war 2017 vom damaligen Bundesinnenminister Thomas de Maizière (CDU) nach dem Vereinsgesetz verboten worden, da sich ihr Zweck und ihre Tätigkeiten „gegen die verfassungsmäßige Ordnung richteten".

Nachdem sich ein Redakteur als Autor des Artikels outete und den dafür genutzten Laptop übergab, zogen die Beamt*innen wieder ab. Der Betroffene wertet dies als Erpressung und einen „beispiellosen Eingriff in das Redaktionsgeheimnis". Zahlreiche Kontakte zu Quellen des langjährigen Journalisten befinden sich nun in den Händen der Polizei, allerdings auf einem verschlüsselten Gerät. Auch der Rechner eines Geschäftsführers wurde beschlagnahmt, die darauf befindlichen Daten waren nicht verschlüsselt. Ein anderer Geschäftsführer kritisiert die Durchsuchung als Angriff auf das Redaktionsgeheimnis und den Informant*innenschutz. Die Polizei habe nicht wie vorgeschrieben vor einer Durchsuchung mildere Mittel gewählt.

Außerdem habe die Staatsanwaltschaft eine Anfrage an den Hoster der Webseite des Radios gestellt und darin die Herausgabe von IP-Adressen aller Besucher*innen verlangt, erklärte ein Techniker. Das als Rechtfertigung angeführte Telemediengesetz erlaube eine solche Anfrage aber nur zu Bestandsdaten.

1 Pressemitteilung Polizeipräsidium Freiburg v. 17.1.2023

Handyauswertung durch BAMF war rechtswidrig

Das Bundesverwaltungsgericht in Leipzig sieht das regelmäßige Auslesen von Mobiltelefonen durch das Bundesamt für Migration und Flüchtlinge (BAMF) nicht vom Gesetz gedeckt. Die bei fehlenden Pässen oder Passersatzpapieren angeordnete Maßnahme müsse unter hinreichender Berücksichtigung sonstiger vorliegender Erkenntnisse und Dokumente erfolgen, argumentierte das Gericht in einem Urteil vom 16. Februar (Az. 1 C 19.21) und gab der Klage einer 44-Jährigen aus Afghanistan statt. Die Frau war mit der Gesellschaft für Freiheitsrechte (GFF) vor zwei Jahren gegen die Handyauswertung vor das Verwaltungsgericht (VG) in Berlin gezogen. Schon das VG hielt die Maßnahme für rechtswidrig. Weil die Praxis die Grundrechte Tausender Geflüchteter auch in anderen Bundesländern betrifft und die Rechtssache grundsätzliche Bedeutung hat, hatte das VG mit Einverständnis der GFF die Sprungrevision zugelassen.

Beim Auslesen der Mobiltelefone von Asylsuchenden erstellen Behörden eine Kopie der Inhalte und prüfen, ob im Adressbuch oder bei Anrufen und Nachrichten häufig Ländervorwahlen vorkommen, die dem in der Anhörung genannten Heimatland entsprechen. Auch besuchte Webseiten werden nach derartigen Länder-Endungen durchsucht. Aus Fotos und auf dem Telefon installierten Apps extrahiert das BAMF Geodaten, in denen der jeweilige Aufenthaltsort gespeichert ist. Außerdem werden die Login-Namen verschiedener Apps aufgelistet.

Die ausgelesenen Daten münden in einen Ergebnisreport, der von einem angestellten Volljuristen oder einer Volljurist*in begutachtet und freigegeben werden muss. Anschließend erfolgt unter anderem auf dieser Grundlage die Entscheidung über den Asylantrag. Im Falle der mit der GFF klagenden Frau war diese Entscheidung negativ.

Mit Stand August 2022[2] hatten nach Angaben des Bundesinnenministeriums im vergangenen Jahr 30,6 Prozent der Asylsuchenden bei der Antragstellung angegeben, über ein „Datenträger-Gerät" zu verfügen. 80 Prozent aller erlangten Geräte konnten demnach „technisch ausgelesen werden". Bis zum August hatte das BAMF im vergangenen Jahr über 16.000 Datenträger ausgelesen. Bei rund 4 Prozent der Betroffenen sei die Identität angeblich widerlegt worden. (beide: Matthias Monroy)

2 BT-Drs. 20/4019 v. 12.10.2022

Brandenburg bekommt Polizeibeauftragte

Nach zwei Jahren zäher Verhandlungen hat die rot-schwarz-grüne Koalition in Brandenburg am 16. Dezember 2022 ihr Versprechen aus dem Koalitionsvertrag umgesetzt und ein Gesetz zur Einrichtung einer Polizeibeauftragtenstelle verabschiedet.[3] Damit wird Brandenburg nun das siebente Bundesland mit einer solchen Ombudsperson. Anders als in den anderen Ländern, wo die Stellen zusätzlich als Bürger- oder Feuerwehrbeauftragte immer auch andere Aufgaben haben, wird sie in Brandenburg ausschließlich für Polizeithemen zuständig sein. So wie die bereits existierenden Beauftragten ist aber auch die Stelle in Brandenburg Hilfsorgan des Landtags bei der parlamentarischen Kontrolle, soll die Bevölkerung im „Dialog" mit der Polizei unterstützen und auf eine einvernehmliche Erledigung von Beschwerden hinwirken; zugleich ist sie zuständig für Eingaben aus der Polizei. Dafür verfügt die*der Beauftragte über umfassende Auskunfts-, Akteneinsichts-, Anhörungs- und Betretungsrechte. Außen vor bleibt sie*er jedoch, sobald straf- oder disziplinarrechtliche Verfahren laufen oder ein Vorgang Gegenstand eines parlamentarischen Untersuchungsausschusses ist. Allerdings hat die Stelle Zugriff auf sämtliche Beschwerdevorgänge der Polizei und muss – dies ein Novum in Deutschland – über alle gegen Polizeibeamt*innen gestellten Strafanzeigen und eingeleitete Disziplinarverfahren sowie über den Abschluss der Verfahren informiert werden. Ebenfalls neu im nationalen Vergleich ist das Recht, jederzeit an Sitzungen des Landtags und seines Innenausschusses teilzunehmen und sich dort mit Redebeiträgen zu allen Polizeiangelegenheiten äußern zu können. Der*die Beauftragte muss die „erforderliche Qualifikation und Erfahrung" für das Amt mitbringen und wird für sechs Jahre gewählt. Am 22. Februar 2023 stimmte der Landtag mit 49 zu 27 Stimmen bei drei Enthaltungen für die SPD-Politikerin Inka Gossmann-Reetz. Die gelernte Krankenschwester saß seit 2014 als Abgeordnete im Landtag, wo sie Vizechefin und innenpolitische Sprecherin der SPD-Fraktion und seit 2018 Vorsitzende der Parlamentarische Kommission zur Kontrolle des Verfassungsschutzes war. Die Vereidigung folgt Ende März.

(Eric Töpfer)

3 Gesetz über die Beauftragte oder den Beauftragten für Polizeiangelegenheiten des Landes Brandenburg (Brandenburgisches Polizeibeauftragtengesetz – BbgPBG), Gesetz- und Verordnungsblatt für das Land Brandenburg v. 19.12.2022, Jg. 33, Nr. 36, S. 1-7

Sicherheits- und Ordnungsgesetz MV verfassungswidrig

Nachdem in den Jahren ab 2017 in den meisten Bundesländern die Polizeigesetze verschärft wurden, erhoben einige Protestbündnisse Verfassungsbeschwerden gegen die Gesetze. Anfang Februar 2023 veröffentlichte das Bundesverfassungsgericht (BVerfG) eine Entscheidung zur Beschwerde des Bündnisses SOGenannte Sicherheit sowie der NGO Gesellschaft für Freiheitsrechte gegen das Sicherheits- und Ordnungsgesetz Mecklenburg-Vorpommern (SOG MV).[4] Das Gesetz enthielt eine Vielzahl von Regelungen zur verdeckten Datenerhebung, die das BVerfG nun beanstandete. Unter anderem ging es um die polizeilichen Befugnisse zur Observation von Personen, zur Anfertigung von Bild- und Tonaufnahmen, zum Einsatz von Vertrauenspersonen und verdeckten Ermittler*innen, zur Überwachung von Wohnräumen und Telekommunikation sowie zur Online-Durchsuchung. Das BVerfG hielt dazu fest, dass der Anlass für die Maßnahmen, die sog. Eingriffsschwelle, voraussetze, dass zumindest eine konkretisierte Gefahr für hinreichend gewichtige Rechtsgüter, etwa Leib, Leben und Freiheit einer Person, die Sicherheit von Bund und Ländern sowie den Schutz wichtiger Infrastruktureinrichtungen, bestehe. Überwachungsmaßnahmen seien hingegen nicht zulässig, wenn nur diffuse Anhaltspunkte für zukünftige Gefahren bestünden.

Weiterhin beanstandete das BVerfG, dass einige der polizeilichen Befugnisse nicht dem Schutz des Kernbereichs privater Lebensgestaltung genügen. Hierzu machte das Gericht detaillierte Vorgaben. Insbesondere müssen Regelungen gefunden werden, wie mit einmal erhobenen Daten, die kernbereichsrelevante Informationen enthalten, umgegangen wird. Die Maßstäbe des Bundesverfassungsgerichts wirken über Mecklenburg-Vorpommern hinaus. Ähnliche wie die für verfassungswidrig befundenden Regelungen des SOG MV finden sich auch in den Polizeigesetzen von Berlin, Bremen, Niedersachsen, Nordrhein-Westfalen, Sachsen-Anhalt, Schleswig-Holstein, Hessen und Rheinland-Pfalz[5] – und werden dort nun überarbeitet werden müssen. (Marius Kühne)

4 Bundesverfassungsgericht: Beschluss vom 9.12.2022, Az. 1 BvR 1345/21

5 Koch, T.: Handlungsbedarf im Gefahrenabwehrrecht: Das Bundesverfassungsgericht präzisiert die Maßstäbe für verdeckte Datenerhebungen, verfassungsblog.de v. 14.2.2023

Meldungen aus Europa

Neue deutsch-französische Polizeieinheit

Deutschland und Frankreich wollen ihre Zusammenarbeit gegen „Migrationsströme" verstärken. Eine 2021 gegründete „Gemeinsame deutsch-französische Diensteinheit" (GDFD) wird dazu in eine feste Organisationsform umgewandelt. Dies haben die deutsche Innenministerin Nancy Faeser und ihr Amtskollege Gérald Darmanin beim Ministerrat im Januar beschlossen.[1] Zur „Bekämpfung der irregulären Migration" soll die Einheit aus Bundespolizei und französischer Grenzpolizei gemeinsame Streifen durchführen. „Anlassbezogen" soll sie außerdem örtliche Dienststellen bei besonderen Einsatzlagen unterstützen. Genannt werden gemeinsame „Großkontrollen zur Feststellung von Behältnisschleusungen" und der Einsatz anlässlich des Weihnachtsmarkts in Straßburg.

Bereits 2019 hatten die beiden Regierungen im „Aachener Vertrag" eine deutsch-französischen Einsatzeinheit (DFEE) von Bundespolizei und Gendarmerie verabredet, die damaligen Innenminister Horst Seehofer und Christophe Castaner gründeten diese schließlich im Herbst 2019 unter der Bezeichnung „Daniel Nivel".[2] Namensgeber ist ein französischer Gendarm, der bei der Fußball-Weltmeisterschaft in Frankreich 1998 von deutschen Hooligans schwer verletzt wurde. Der Vorfall sorgte unter EU-Staaten für zahlreiche neue Kooperationen von Polizei und Justiz.

Anders als die GDFD handelt es sich bei der DFEE um eine „Gelegenheitseinheit", die etwa anlässlich politischer oder sportbezogener Großveranstaltungen zum Zuge kommen soll.[3] Die jeweils 15 Angehörigen von Bundespolizei und Gendarmerie stammen in Frankreich aus Motorradstaffeln, Fahndungsbrigaden oder Einsatzzügen. Auf deutscher Seite sollen ihr insbesondere Expert*innen „für die Bearbeitung von Migrations- und Dokumentenbetrugsdelikten" angehören. Die DFEE soll auch „Stabilisierungsoperationen" außerhalb der EU durchführen. Konkrete Planungen bestünden für derartige Einsätze aber derzeit nicht, so das Innenministerium auf Anfrage.

1 Pressemitteilung BMI v. 22.1.2023
2 Pressemitteilung BMI v. 16.10.2019
3 BT-Drs. 19/19059 v. 11.5.2020

Grimheden will mehr Frontex in Problemstaaten

Der Grundrechtsbeauftragte bei Frontex schlägt vor, den Artikel 46 der Frontex-Verordnung „umzukehren": Kommt es in einem Gaststaat zu Menschenrechtsverletzungen, soll Frontex demnach mehr und nicht weniger Personal dorthin entsenden, erklärt der aus Schweden stammende Jonas Grimheden auf Anfrage. Die Agentur komme mit Beamt*innen aus anderen Ländern als jenem, in dem die Verstöße passierten, erläutert er die Vorteile seiner Idee. Sie seien daher unabhängiger von dortigen nationalen Interessen. Würden Einsätze beendet, fehle es an einer „Hebelwirkung", so der Beauftragte, der das Amt vor 18 Monaten übernommen hat.

Der Artikel 46 ermöglicht den Rückzug aus Missionen in einem Gaststaat, „wenn die Voraussetzungen für ihre Durchführung nicht mehr gegeben sind". Die Entscheidung darüber obliegt allein dem Direktor der Agentur. Zu den möglichen Anlässen nennt die Verordnung die Zahl registrierter Beschwerden, interne Berichte über „schwerwiegende Vorfälle" oder Meldungen von „einschlägigen internationalen Organisationen".

Besonders der Frontex-Einsatz in Griechenland ist umstritten. Im vergangenen Sommer forderten sieben auf Samos tätige Nichtregierungsorganisationen den Abzug.[4] Sogar Grimheden selbst soll im vergangenen Jahr in Vierteljahresberichten angeregt haben, die Tätigkeit in dem Land einzustellen, weil griechische Grenzschutzbeamt*innen immer wieder Übergriffe begangen hätten. Das gehe aus vertraulichen Dokumenten hervor, berichtet die New York Times.[5] Demnach habe Grimheden „glaubwürdige Berichte" gesammelt, wonach griechische Behörden Geflüchtete systematisch sowohl an den See- als auch an den Landgrenzen abweisen, ihnen den Zugang zu internationalem Schutz verweigern, Kinder von ihren Eltern trennen und die Betroffenen „erniedrigend" behandeln.

Der neue Frontex-Chef Hans Leijtens hält jedoch an der Präsenz in Griechenland fest. Bei seiner Vorstellung im Europaparlament Ende November hatte der niederländische Gendarm noch erklärt, den Artikel 46 auszulösen, wenn dies „nötig" sei. Welche Umstände dafür gegeben sein müssten, führte er aber nicht aus. (beide: Matthias Monroy)

4 https://ihaverights.eu/wp-content/uploads/2022/07/Article-46-Samos-Human-Rights-Defenders-Letter-of-Concern.pdf

5 Greece Border Abuses Highlight Europe's Clashing Priorities on Migration, New York Times v. 14.2.2023

API-Daten für mehr Fluggastdatenspeicherung

Am 13.12.2022 hat die EU-Kommission einen Vorschlag für eine „Verordnung über die Erhebung und Übermittlung von API-Daten zur Verhütung, Aufdeckung, Untersuchung und Verfolgung von terroristischen Straftaten und zur Änderung der Verordnung (EU)2019/818" (API-VO) vorgelegt.[6] Die Advanced Passenger Information (API) wird von den Fluggesellschaften bei der Einreise in den Schengenraum während der Abfertigung der Fluggäste erhoben und bereits seit 2004 als Liste an die Grenzpolizeibehörde des Zielstaates übermittelt. Die API-Daten enthalten die Angaben aus den Reisepässen der Flugreisenden. Sie gelten laut Kommission als „verifizierte" Daten über die tatsächlich an Bord befindlichen Fluggäste, während die Passenger Name Record (PNR)-Daten, die vorab von Fluggesellschaften und Reiseunternehmen an die Behörden übermittelt werden, „unverifizierte" Daten enthalten – ob diese Fluggäste tatsächlich an Bord sind oder kurzfristig noch weitere Fluggäste zugestiegen sind, geht aus den PNR-Daten nicht hervor. Deshalb macht die EU-Kommission hier eine „Lücke" für die Überwachung der Fluggäste und die Fähigkeit der Passenger Information Units (PIU) aus, die PNR-Daten nach „Risikoreisenden" zu durchsuchen. Diese Lücke gilt dann selbstverständlich auch für Flugreisen innerhalb der EU, für die bislang keine API-Übermittlung erforderlich war. Daher sieht der VO-Entwurf die Ausweitung der API-Übermittlungen an die PIUs vor. Zugleich muss die Kommission allerdings berücksichtigen, dass der Europäische Gerichtshof (EuGH) mit seiner Entscheidung in der Rechtssache C-817/19 in Bezug auf PNR-Daten eingefordert hatte, dass Speicherung und Zugriff „wirksam begrenzt" werden müssten, insbesondere bei innereuropäischen Flügen. Ansonsten handelte es sich um eine unzulässige Vorratsdatenspeicherung. Daher sollen nach dem VO-Vorschlag bei innereuropäischen Flügen die API-Daten nur für die ausgewählten Flüge übermittelt werden, bei denen die Mitgliedstaaten auch zukünftig die Übermittlung von PNR-Daten verlangen. Während also einerseits die Zahl der von den PIUs durchleuchteten Fluggäste sinken soll, soll der über sie erhobene Datenkranz erweitert werden. Der Vorschlag steht im Kontext der Bemühungen von Kommission und Mitgliedstaaten, die EuGH-Rechtsprechung zur PNR-VO zu umgehen (vgl. Meldung in CLIP 130). (Dirk Burczyk)

6 COM (2022) 731 final v. 13.12.2022

Einigung zu „elektronischen Beweismitteln"

Das Europäische Parlament und der Rat haben sich im Januar 2023 auf zwei Gesetzesvorhaben zur Sicherung und Herausgabe elektronischer Beweismittel in Strafsachen geeinigt.[7] Das „E-Evidence"-Paket besteht aus einer Verordnung sowie einer ergänzenden Richtlinie. Hintergrund des Gesetzgebungsverfahrens ist, dass Strafverfolgungsbehörden zunehmend auf im Ausland gespeicherte Daten zugreifen wollen. Deren Herausgabe richtet sich traditionell nach den Vorschriften der internationalen Rechtshilfe. Allerdings werden entsprechende Verfahren von den Behörden als zu langsam und ineffizient wahrgenommen. Daher haben die USA bereits 2018 den sog. CLOUD ACT erlassen, der US-amerikanische Technologiefirmen verpflichtet, auch Daten, die auf ihren Servern im Ausland gespeichert werden, an US-Strafverfolgungsbehörden herauszugeben. Ein ähnliches Verfahren sieht die E-Evidence-Verordnung vor, auf die sich die europäischen Rechtssetzungsorgane nun geeinigt haben.

Demnach sollen die Strafverfolgungsbehörden des sog. Anordnungsstaates private Anbieter*innen von Kommunikationsdiensten o. ä., die in einem anderen EU-Mitgliedstaat, dem sog. Vollstreckungsstaat, ihren Sitz haben, zur Herausgabe der Daten (oder zur Sicherung für eine spätere Herausgabe) verpflichten können. Die Herausgabe oder Sicherung muss innerhalb von zehn Tagen, in Ausnahmefällen sogar innerhalb von acht Stunden erfolgen. Kommen die Diensteanbieter*innen der Anordnung nicht nach, drohen ihnen Bußgelder von bis zu 2 % ihres weltweiten Jahresumsatzes. Auch Unternehmen, die über keinen Sitz in der EU verfügen, aber dort Dienstleistungen anbieten, müssen gemäß der ergänzenden Richtlinie Vertreter*innen benennen, an die Herausgabe- und Sicherungsanordnungen gerichtet werden können.

Die Behörden im Vollstreckungsstaat können nur wenige in der Verordnung vorgesehene Ablehnungsgründe gegen die Herausgabe- oder Sicherungsanordnung geltend machen. Der Regelfall soll hingegen sein, dass die jeweiligen Unternehmen die angeforderten Daten an den Anordnungsstaat innerhalb der Frist herausgeben und so die Effizienz der Strafverfolgung steigern. Eine „Kompensation" dieses staatlichen Machtzuwachses durch die Stärkung von Beschuldigtenrechten im Strafverfahren findet dagegen nicht statt. (Marius Kühne)

7 Rat der EU: Pressemitteilung v. 25.1.2023 (Texte der beiden Vorhaben im Anhang)

Literatur

Zum Schwerpunkt

Die fortgeschrittenen Technologien der Grenzkontrollen scheinen in mehrfacher Hinsicht entfernt. Das klassische Bild einer physisch gesicherten und nur an Kontrollstellen durchlässigen Grenze ist für Europäer*innen erst an den Schengen-Außengrenzen erfahrbar. Werden diese in ihrem teilweise und zunehmend befestigten Formen in den Blick genommen, so sehen wir regelmäßig nur die durch Zäune, Mauern, Gräben, Wachtürmen errichteten Grenzen. Kaum bis gar nicht wahrnehmbar sind hingegen die mit den Potenzialen der Digitalisierung aufgerüsteten Formen der Überwachung des Grenzraums, der Kontrolle von Einreisewilligen sowie der präventiven Durchleuchtung der Grenzgeschehens. Der Wandel staatlicher Grenzen seit dem ausgehenden 20. Jahrhundert ist verbunden mit der Etablierung neuer Grenzkontrolltechnologien. Wer letztere verstehen will, muss zugleich in Rechnung stellen, dass Funktionen, Formen und Orte von (staatlichen) Grenzen sich verändert haben.

Mit der Europäisierung des Außengrenzgeschehens hängt vermutlich zusammen, dass zu diesem Thema nur wenige Text in Deutsch vorliegen. Wir geben im Folgenden eher Hinweise auf wenige leicht oder kostenlos zugängliche Veröffentlichungen, die einen exemplarischen Zugang zum Thema ermöglichen. Damit werden wir weder der umfänglichen Diskussion über den Form- und Bedeutungswandel von Grenzen gerecht, noch den vielfältigen zivilgesellschaftlichen Initiativen, die kritische Öffentlichkeit herstellen, Protest und Solidarität mit durch Grenzen Ausgeschlossenen praktizieren. In den Beiträgen des Schwerpunktes finden sich entsprechende Hinweise.

Mau, Steffen: *Sortiermaschinen. Die Neuerfindung der Grenzen im 21. Jahrhundert, München 2021*
Das Buch ist eine Pflichtlektüre für diejenigen, die den Kontext der neuen (staatlichen) Grenzen und deren technologische Basis verstehen wollen. Es ist eine der wenigen einschlägigen Veröffentlichungen in deutscher Sprache. Mau beginnt mit der Klarstellung eines Missverständnisses: Wer

glaubte, Globalisierung sei gleichbedeutend mit der Abschaffung von Grenz(kontroll)en, der/die irrte von Anfang an. Umgekehrt, so Mau, macht die Globalisierung andere, aber intensivierte Grenzen erforderlich. Denn nur so kann gewährleistet werden, dass in den globalisierten Strömen nur die ins Land kommen, die erwünscht sind. Dass darin die Funktion der neuen Grenzen liegt, das sagt bereits der Titel: Als „Sortiermaschinen" gewährleisten sie unaufwändige Grenzüberschreitungen der Privilegierten, die Kontrolle der legal Einreisenden und das Fernhalten der Unerwünschten. Fußend auf seinen Forschungen zu den nationalen Grenzen im globalen Kontext unterscheidet Mau verschiedene Grenztypen. Die modernen Detektions- und Überwachungstechnologien ersetzen oder erweitern das Arsenal „fortifizierter" (also mit physischen Barrieren geschützte) Grenzen, indem sie gleichzeitig deren permanente Überwachung mit wenig Personaleinsatz und die zielgenaue Identifikation von Personen erlauben. Für die neuen Grenzen sind laut Mau vier Merkmale kennzeichnend: Menschliche Mobilität wird als Sicherheitsproblem wahrgenommen, der Kontrollraum verschiebt sich von der Grenzlinie nach innen wie nach außen, die Grenzarrangements realisieren ein System gestufter Mobilitäts- und Freiheitsrechte, und sie sind schließlich Ausdruck einer globalen hierarchischen Ordnung.

Huber, Georg Johannes: *Power, policies, and algorithms – technologies of surveillance in the European border surveillance regime, Karlsruhe 2022, www.ksp.kit.edu/site/books/10.5445/KSP/1000129465/download/8720*
In der zuvor vorgestellten informativen und überzeugenden Analyse Mais erscheinen die Grenzen des 21. Jahrhunderts als ein quasi zwangsläufiges Produkt von ebenso zwangsläufigen Globalisierungsprozessen. In Hubers Untersuchung, seine politikwissenschaftliche Dissertation von 2020, ist der Gegenstand einerseits begrenzter (auf das EU-Grenzregime), andererseits aber weiter, indem er auch darauf schaut, welche Akteur*innen, Gruppen und Institutionen den Aus- und Umbau der Grenzen betreiben. Im Anschluss an die Darstellung der zeitgeschichtlichen Entwicklung der Europäischen Grenzpolitik und einem theoretischen Zwischenkapitel werden auf 40 Seiten die „digitalen Wände" und die mit Algorithmen programmierten Grenzübergänge vorgestellt. Dabei liegt der Schwerpunkt auf dem Ausbau der diversen (grenz-)polizeilichen Datenbanken – vom Schengener Informationssystem bis zum Reiseinformationssystem ETIAS – und der Darstellung von Eurosur. Auch wenn die technischen Details

nicht erläutert werden, das Zwischenfazit ist eindeutig: die Grenzüberwachung sei „teilweise automatisiert, teilweise biometrisch ausgerichtet, ein auf Big Data beruhendes System der Massenüberwachung, mit einer zunehmenden Tendenz, präventiv intendierte Prognosen anhand mathematischer Verfahren zu erstellen". Im Anschluss an die Arbeiten von Statewatch und Ben Hayes wird auf die Existenz eines Netzwerks aus EU-Agenturen, Regierungen der Mitgliedstaaten, Sicherheitsbehörden und Rüstungsindustrie, hingewiesen, das im Gleichklang ihrer Interessen die Einführung der modernen Grenzüberwachungstechnologien betreibt.

Akghar, Babak; Kavellieros, Dimitrios; Sdongos, Evangelos (Hg.): *Technology Developement for Security Praktioners, Cham 2022, https://link.springer.com/content/pdf/10.1007/978-3-030-69460-9.pdf*
Einen Einblick in die Werkstätten den Sicherheits-Technokraten gewährt dieses Werk. Neben den anderen Anwendungsfeldern (Cybercrime, Organisierte Kriminalität, Kritische Infrastrukturen und Krisenbewältigung) wird die Grenzsicherheit in sechs Beiträgen auf 100 Seiten abgehandelt. Vorgestellt werden verschiedene Projekte: TRESSPASS verspricht ein „innovatives Konzept" hin zu einem risikobasierten Ansatz des Grenzmanagements. Dazu werden Daten unterschiedlichster Quellen – Gepäckverfolgung, Bewegungsüberwachung, Web-Analysen, Kontrollpraktiken – mit Dritt- und Nachbarstaaten ausgetauscht, schließlich re-personalisiert und einem Sicherheitslevel zugeordnet. EWISA, ein Projekt der Grenzschutzbehörden Griechenlands, Finnlands, Spaniens und Rumäniens, hatte zum Ziel, Aufmerksamkeit und Reaktionsfähigkeit der Grenzbehörden angesichts von Bedrohungen zu steigern. Das System basiert auf einer Überwachung per Video, Radar und Sensoren, die schließlich zusammengeführt und ausgewertet werden. Die Ergebnisse in den vier Studienregionen fassen die Autoren folgendermaßen zusammen: Die entwickelten Technologien erzeugten einen außergewöhnlichen zusätzlichen Wert für die Überwachung der Grenzen." In den weiteren Beiträgen wird der Einsatz von Drohen in Schwarmformation, das Projekt FOLDOUT – ein gestuftes System der Grenzüberwachung von Satelliten bis zu verschiedenen Sensoren an Land –, das Netzwerk von Sicherheitsagenturen aus Mittelmeer- und Schwarzmeerstaaten MEDEA sowie das Projekt ANDROMEDA vorgestellt. Kennzeichnend für die Lage ist, dass die zuerst genannten Beiträge ihren technischen Horizont an keiner Stelle überschreiten, während es einem gesonderten Vorhaben überlassen bleibt, die recht-

lichen und ethischen Aspekte der Grenzüberwachungstechnologien zu erörtern. ANDROMEDA tut dies am Beispiel der Überwachung der Seegrenzen. Das Fazit ist eindeutig: Sichtbar wurden mehrere Konflikte mit den rechtlichen Grundlagen, mit den international verbürgten Menschenrechten, mit anerkannten ethischen Prinzipien und dem internationalen Flüchtlingsrecht, „insbesondere im Hinblick auf das Recht auf Privatheit, auf den personenbezogenen Datenschutz und den non-refoulement-Grundsatz". Derartige Konflikte könnten nur vermieden werden, wenn diese Aspekte bereits in der Entwicklung der Technologien und des Einsatz-Designs berücksichtigt würden.

Border Violence Monitoring Network: *EU Member States' use of new technologies in enforced disappearances, 2023, https://borderviolence.eu/app/uploads/Input-for-the-thematic-study-on-new-technologies-and-enforced-disappearances_version-2.pdf*
Exemplarisch für die realen Auswirkungen technisierter Außengrenzen steht diese Publikation des Border Violence Monitoring Network, eines Zusammenschlusses verschiedener NGOs, das Menschenrechtsverletzungen an den Grenzen dokumentieren und Gewalt gegen Migrant*innen stoppen will. Der aktuelle Bericht stellt eine Stellungnahme für die UN-Arbeitsgruppe zum „erzwungenen Verschwindenlassen" dar. Das Netzwerk hat Belege für Verhaftung, Festsetzung oder Zurückschiebung von fast 25.000 Personen seit 2017 gesammelt. Drohnen waren demnach an den Pushbacks von über 1.000 Personen beteiligt. Im Anhang werden 48 derartiger Einsätze mit genauen Daten aufgelistet.

Aizeki, Mizue; Bingham, Laura; Narváez, Santiago: *The Everywehere Border. Digital Migration Control Infrastructure in the Americas, tni v. 14.2.2023, www.tni.org/en/article/the-everywhere-border*
Dieser Beitrag beleuchtet beispielhaft, dass die technologiegestützte Abschottung keine europäische Spezialität ist. Er zeigt, wie die Südgrenze der USA weit in die Nachbarstaaten vorverlegt wird. Ermöglicht werde dies durch eine „digitale Infrastruktur, die auf den Erzeugnissen der Rüstungsindustrie und den Innovationen aus dem Silicon Valley beruht": interoperable Datenbestände tauschen Fingerabdrücke zwischen den nationalen Polizeibehörden aus, biometrische Daten werden von mexikanischen Behörden an die der USA weitergegeben, Soziale Medien und Apps werden ebenso zu Überwachungstools für die Polizei wie Identifizierungssysteme, die eigentlich den Zugang zu Hilfen gewährleisten sollen.

Aus dem Netz

https://migration-control.info

Der Fokus dieses Portals ist weniger die technische Aufrüstung der europäischen Außengrenzen, sondern deren Vorverlagerung (Externalisierung). In Fortsetzung eines ehemals von der taz betriebenen Projekts liegt der Schwerpunkt in der Dokumentation des Ausmaßes der Externalisierungspolitik und der Folgen in den Herkunfts- und Transitländern des afrikanischen Kontinents.

Migration-control beschreibt sich selbst als „ein transnationales Netzwerk aus antirassistischen Aktivist*innen, Journalist*innen, Übersetzer*innen und Forscher*innen". Dreizehn selbst wieder international aufgestellte Initiativen aus europäischen Ländern werden als Kooperationspartner aufgeführt. Durch die Links zu deren Homepages eröffnet die Seite einen Zugang zur zivilgesellschaftlichen Kritik an der Festung Europa und deren Ausbau.

Die (teilweise in vier Sprachen angebotenen) Informationen der Seite sind über die drei Kategorien „Wiki", „Blog" und „Archiv" gegliedert. Das „MigWiki" – systematisch und alphabetisch aufrufbar – enthält einerseits ausführliche Darstellung zentraler Begriffe und Institutionen, andererseits bietet es den Zugang zu länderbezogenen Veröffentlichungen. Im „Blog" werden aktuelle Nachrichten, Kommentare etc. eingestellt; seit gut zwei Jahren gibt es dort eine monatliche Zusammenfassung aktueller Artikel und Berichte. Im Blog kann anhand von acht Kategorien die Suche thematisch eingegrenzt werden. Das englischsprachige „Archiv" enthält die Sammlung weitergehender Analysen und Berichte, die nach inhaltlichen Schwerpunkten (von „Criminalization of Borderwork" bis „Sea Rescue Operations") geordnet sind.

Die Archiv-Suche unter „Border Surveillance Technology & Industry" ergibt 76 Treffer (März 2023). Zwar sind viele der angebotenen Links nicht mehr aktuell, die Kurz-Infos zu den Berichten führen dann aber doch zu interessanten Dokumenten: etwa der Bericht von migreurop vom Dezember 2020 („Data and New Technologies, the Hidden Face of Mobility Control") oder Petra Molnars Abhandlung zu den Technologien der Migrationskontrolle („Technological Testing Grounds", 2020) oder das (als vertraulich eingestufte) gemeinsame Lagebild von Frontex und Europol zur Bedeutung von Apps und digitalen Medien für das „migrant smuggling". (alle: Norbert Pütter)

Neuerscheinungen

Thüne, Martin; Klaas, Kathrin; Feltes, Thomas (Hg.): *Digitale Polizei. Einsatzfelder, Potentiale, Grenzen und Missstände, Frankfurt (Verlag für Polizeiwissenschaft) 2022, 353 S., 32,90 Euro*

Der Band gibt einen guten Einstieg in das Thema „Digitale Polizei" und einen gelungenen Überblick über die aktuell zentralen Themen im Feld: das erste Kapitel behandelt „Grundüberlegungen" zur Annäherung, eröffnet von einem eher launig-anekdotischen Beitrag von Thomas Feltes aus über 40 Jahren Feldforschung in der Polizei. Vor allem der Beitrag von Jo Reichertz und Sylvia Marlene Wilz beleuchtet die Änderungen, die die Digitalisierung für die Arbeit in der Polizei hat – von der Mail-Kommunikation über das vermehrt in Datenbanken und zugehörigen Anwendungen zu findende polizeiliche Wissen bis hin zur notwendigen Entwicklung dieser polizeilichen Arbeitswerkzeuge durch private Firmen. Ein zentrales Thema ist dabei die Zurückdrängung von informeller Arbeitskooperation innerhalb der Polizei, die mit traditionellen Werten wie Zusammengehörigkeit und Loyalität zur Organisation in Konflikt geraten kann. Eine Beobachtung, die für die gesamte Arbeitswelt der Büroangestellten gilt, findet sich auch hier wieder. Weitergabe von Wissen, Austausch mit erfahrenen Kolleg*innen, gemeinsame Reflexion von Erfahrungen und Arbeitsergebnissen hatten ihren Ort in der „Teeküche". Doch die Arbeit in einem Kommissariat heute, so berichten Reichertz und Wilz aus einer empirischen Studie, die sie 2018 bis 2020 durchgeführt haben, findet ihren Takt vor allem durch die Mail-Kommunikation: alle leben in dem Gefühl, Mails innerhalb weniger Minuten bearbeiten zu müssen, bei Problemen werden Verteiler möglichst groß gezogen, um Verantwortung abgeben zu können („Melden macht frei"). Informationen werden nur noch in kleiner Runde, „zwischen Tür und Angel", weitergegeben und damit aber wird zugleich – hier in gegenläufiger Tendenz zur festgestellten Zurückdrängung des Informellen – ein neuer, verkleinerter Raum geschaffen, in dem Praxiswissen erarbeitet und weitergegeben werden kann.

Hierzu findet sich im zweiten Kapitel zum Thema „Algorithmenbasierte Arbeit Konzepte polizeilicher Arbeit" weitere Vertiefungen unter anderem in dem lesenswerten Beitrag von Kai Seidensticker und Felix Bode „Predictive Policing und die Gefahr der Abstraktion von Polizeiarbeit". Sie führen dort den Begriff der „Abstraktion und Dekontextualisierung" von Polizeiarbeit ein: durch „predictive policing" und „intelligence-

led policing" werde Polizeiarbeit durch eine Form der Informationsverarbeitung und der Generierung neuer Ermittlungsansätze gesteuert, die schon aufgrund mangelnder Kompetenzen in der Polizei nicht verstanden und nachvollzogen werden könnten – obwohl die Anwendung des so generierten „Wissens" „auf der Straße" mit polizeilichen Grundrechtseingriffen einhergehen könne. Zugleich sehen sie hierin auch ein Potential, Polizeiarbeit transparenter und objektiver zu machen, etwa weil der vorurteilsbelasteten Konstruktion polizeilichen „Wissens" in einzelnen Räumen der Stadt mithilfe von umfassender Datenaufbereitung entgegengewirkt werden könne – unter der Voraussetzung, dass es ausreichend digitale Expertise und Reflexionsfähigkeit gibt. Deutlich wird, dass Seidensticker und Bode unter dem Schlagwort der „holistischen Polizeiarbeit" („holistic policing") eine stärker informations- und raumbasierte Polizeiarbeit befürworten, die gleichzeitig einer „weiteren Distanzierung" der Bevölkerung von der Polizei entgegenwirken solle. Hier ist der Beitrag von Simon Egbert zur „Digitalisierung als Präpressionstreiber" im selben Kapital schon deutlich kritischer und vermutlich realitätsnäher. Martin Thüne schließt das Kapitel mit einem Rundumblick zum Einsatz „Künstlicher Intelligenz" in der Polizei ab.

Die beiden weiteren Kapitel des Bandes widmen sich der „Polizei in sozialen Netzwerken" und der „Digitalisierung der polizeilichen Einsatz- und Ermittlungsarbeit". Im Eröffnungsbeitrag zu ersterem gehen Caren Stegelmann und Tabea Louis unter dem Titel „Teilen und Herrschen: zur Polizierung des Sicherheitsgefühls und der ‚guten Ordnung' in der Timeline" unter anderem der These nach, dass die sozialen Medien eine Rückkehr zur Vorstellungen der *Polizey* im 18. Jahrhundert befördern, als „einer produktiven Ordnungsinstanz, die sich für gesellschaftliche Vorgänge ganz allgemein zuständig fühlt und stimulierend, nicht nur repressiv, ... Einfluss nehmen möchte." (S. 164). Die Mechanismen zur Herstellung einer emotional-affirmativen Haltung in der Bevölkerung hierzu stellt unter anderem Ben Hundertmark vor (vgl. auch seinen Beitrag in CILIP 128). Das letzte Kapitel widmet sich in der Betrachtung des Einsatzes von Kameras und Body-Cams sowie der polizeilichen Datenverarbeitung eher „klassischen" Themen der bürgerrechtlichen Kritik an der Polizei, die allerdings in einem solchen Band nicht fehlen dürfen. (Dirk Burczyk)

Richart, Laurent; Rigaud, Sandrine: *Die Akte Pegasus. Wie die Spionagesoftware Privatsphäre, Pressefreiheit und Demokratie attackiert, München (Droemer) 2023, 415 S., 22,00 Euro*

Am 18. Juli 2021 veröffentlichten siebzehn Medien aus zehn Ländern auf drei Kontinenten nahezu zeitgleich und inhaltlich abgestimmt Berichte, in denen aufgedeckt wurde, dass mit der Software „Pegasus" in vielen Ländern der Welt Journalist*innen, politische Aktivist*innen und Oppositionelle ausgeforscht wurden. Das von der israelischen Firma NSO entwickelte und weltweit vertriebene Werkzeug zum Ausspionieren von und mithilfe von Mobiltelefonen war öffentlich bereits seit 2011 bekannt. Die Herstellerfirma preist Pegasus als wirksames Instrument zur Aufdeckung von Terrorismus und schwerer Kriminalität. Es werde nur an Regierung demokratischer Staaten verkauft; sein Export sei zudem an eine Lizensierung durch das israelische Verteidigungsministerium verbunden.

Bereits vor 2021 gab es Vermutungen, dass die Software auch in eher diktatorisch als demokratisch regierten Staaten genutzt und gegen Regimekritiker*innen eingesetzt wird. Aber erst als ein Whistleblower eine Liste mit über 50.000 Handynummern an Journalist*innen weitergab, konnte die Vermutung bestätigt werden. Laurent Richard und Sandrine Rigaud schildern in ihrem Buch den langen und aufwändigen Weg, der vom Erhalt der Liste bis zur Publikation im Juli 2021 führte. Es handelt sich um den Bericht der zentralen Personen eines internationalen Geflechts aus investigativen Journalist*innen und den IT-Spezialisten des Security Labs von Amnesty International („Pegasus Project"). Den journalistischen Kern stellte dabei der Zusammenschluss „Forbidden Storys" dar, der 2016 bereits die „Panama Papers" veröffentlicht und 2020 mit dem „Cartel Project" die Drogenkartelle in Mexiko unter die Lupe genommen hatte. Beeindruckend an dem vorliegenden Buch ist der personelle, technische und logistische Aufwand, der betrieben werden musste, um Pegasus als ein mächtiges Instrument zur Verfolgung Oppositioneller (besonders Journalist*innen) zu entlarven. Interessant an der Darstellung sind auch die vielen nationalen Kontexte, die in die Darstellung eingebunden werden: Ob in Mexiko oder Aserbeidschan, ob in Marokko oder in den Golfstaaten, bei der Suche nach Überwachungsspuren wird immer der politischen Kontext erläutert, warum eine bestimmte Person hätte ausgeforscht werden können. Quasi nebenbei liefert das Buch Kurzbiografien vieler aufrechter Journalist*innen, die ihre Arbeit mit staatlicher Überwachung, mit Gefängnis oder mit dem Tod bezahlen mussten.

Die 50.000er-Liste aus dem Hause NSO bildete den Ausgangspunkt der Recherchen. In einem ersten Schritt mussten den Handy-Nummern Namen zu geordnet werden. Gelang das, hatte man potentielle Pegasus-Zielpersonen. Im zweiten Schritt mussten dann deren Handys untersucht werden: Ließen sich Angriffsversuche nachweisen, ließen sich erfolgreiche Angriffe oder der Abfluss von Informationen nachweisen. Dabei kämpfte das Team mit einer ständig verbesserten Software, die schließlich in der Lage war, Spuren ihres eigenen Eindringens in das Gerät zu verwischen. Gelingt der Eingriff in das Gerät, dann haben die Überwachenden nicht nur Zugriff auf alle Daten (Chats, SMS, Fotos, Kontakte etc.), sondern Kamera und Mikrofon können unbemerkt aus der Ferne eingeschaltet werden. Das Buch schildert minutiös, welche Vorkehrungen getroffen werden mussten, um nicht selbst von Pegasus überwacht und durch Gegenmaßnahmen von PSO behindert zu werden.

Wer hingegen in der „Akte Pegasus" erhofft, was eine „Akte" verspricht, wird enttäuscht werden. Das Buch handelt von der interessanten Arbeit des „Pegasus Projekts", aber viel zu wenig und zu unsystematisch von der Überwachungspraxis durch Pegasus. Es fehlt eine konkretisierte Übersicht über die Zahl der Personen zugeordneten Telefonnummern, der nachgewiesenen Angriffsversuche und Überwachungen. Derartige Angaben finden sich an verstreuten Stellen des Buches oder sie müssen in den Veröffentlichungen der beteiligten Medien nachgesucht werden. Aber selbst eine Übersicht über die wichtigsten Pegasus-Publikationen der beteiligten Journalist*innen fehlt. Zwar wird aus vielen Quellen zitiert, aber keine einzige wird so konkret benannt, dass sie für Leser*innen nachprüfbar wäre. So bleibt es eine interessante Geschichte über die Arbeitsweise investigativen Journalismus' in Zeiten maximaler Überwachung.

Bedauerlich an der „Akte Pegasus" ist zudem, dass an keiner Stelle die regierungsamtlich-legale Überwachung infrage gestellt wird. Pegasus wurde immerhin in 45 Länder geliefert (auch nach Deutschland an das Bundeskriminalamt und den Bundesnachrichtendienst). Angeblich im Kampf gegen Terror und schwere Kriminalität. Auch hier – und nicht nur gegen Journalist*innen und Oppositionelle in diktatorischen Regimen – attackiert Pegasus „Privatsphäre ... und Demokratie" (Untertitel). Erst wenn in Rechnung gestellt wird, das Terror und schwere Kriminalität unscharfe, bedeutungsoffene Begriffe sind, dass es regelmäßig um das präventive Eindringen in verdächtigte Szenen geht, erst dann würde das volle Ausmaß der Pegasus-Bedrohung deutlich werden. Das fehlt im vorliegenden Band – leider. (Norbert Pütter)

Richter, Frank-Arno (Hg.): *Phänomen Clankriminalität. Grundlagen – Bekämpfungsstrategien – Perspektiven. Stuttgart u.a. (Richard Boorberg Verlag) 2022, 310 S., 38,00 Euro*

Erst nach Herausgabe des CILIP-Schwerpunktes zur Clankriminalität erschien der von dem Essener Polizeipräsident Frank Richter herausgegebene Sammelband über das „Phänomen Clankriminalität". Recht offensiv bewirbt der Boorberg-Verlag seine als Pflichtlektüre und praxisorientierter Leitfaden deklarierte Neuerscheinung; im Verlagsflyer ist von einem kompetenten Autorenteam die Rede, das „neue Wege zur Bekämpfung der Clankriminalität" vermittelt. Hinsichtlich der Stoßrichtung der Publikation gibt der Flyer eine klare Richtung vor, wenn mehrmals von der „Bekämpfung der Clankriminalität" und der Ankündigung eines strafrechtlichen Verfolgungskonzeptes die Rede ist. Der Band beinhaltet neben dem Vorwort des Herausgebers und einem Geleitwort seines Dienstherrn, des NRW-Innenministers Herbert Reul, elf Beiträge. Ein Autoren- und ein Stichwortverzeichnis runden das Werk ab.

In der Gesamtbetrachtung kann der Sammelband in mehrfacher Hinsicht nicht überzeugen. Auf der einen Seite scheitert er an seinem eigenen Anspruch, denn das Buch eignet sich weder als Pflichtlektüre noch als Leitfaden. Wer die angekündigten neuen Wege zur Bekämpfung der Clankriminalität sucht, wird nicht fündig werden. Die Aufsatzsammlung weist zudem eine geringe kriminologische Reflexionstiefe auf. Aus einer vornehmlich polizeilichen Perspektive werden die üblichen Stichwörter bedient, die bislang bereits zur kriminalpolitischen Skandalisierung herangezogen wurden. Dazu zählt beispielsweise der vornehmliche Rekurs auf die Organisierte Kriminalität (OK), der sich in diesem Umfang in den polizeilichen Lagebildern nicht wiederfindet. Die anzutreffende Einbeziehung der italienischen OK in den Clan-Diskurs lässt zudem vermuten, dass die OK-Bekämpfung der Polizei neue kriminalpolitische Impulse benötigt. Bemerkenswert ist des Weiteren die geringe kultur-, politik- und verwaltungswissenschaftliche Perspektive. Beispiele: Die als weltweite Einmaligkeit bezeichnete Endogamie ist bereits im europäischen Adel anzutreffen – und damit direkt vor unserer Haustür. Literatur, die das Vorhandensein der wiederkehrend behaupteten Parallelgesellschaft kritisch reflektiert, fehlt. Die skandalisierte Verweigerung von Aussagen gegenüber der Polizei durch Familienmitglieder beschreibt schlichtweg das strafprozessuale Recht zur Zeugnisverweigerung. In vielen Clanfamilien soll häusliche Gewalt intern geregelt werden und nicht – wie „nach deut-

scher Rechtslage" – mit Erstattung einer Strafanzeige. Dass in bio-deutschen Familien eine Strafanzeige auch nicht üblich ist, zeigt der Blick in vorliegende Dunkelfeldstudien. Ebenso wenig überzeugen die oberflächlichen migrationsrechtlichen Ausführungen, die bei Wendt und Kromberg anzutreffen sind, wobei Kromberg, Beigeordneter der Stadt Essen, auf rund 10 von 24 Seiten zum Teil mehrseitige Zitate aneinanderreiht.

Die Ankündigung eines kompetenten Autorenteams erweist sich fast durchgängig als zu hoch gegriffen, denn es fällt schwer, hier „ausgewiesene Kenner der kriminellen Clanszene" auszumachen. Am ehesten überzeugt der Beitrag von Arndt Sinn, der sich lehrbuchhaft mit der Anwendbarkeit des § 129 StGB auf Aspekte der Clankriminalität befasst. Redaktionell ist die mangelnde Abstimmung innerhalb der Beiträge zu beanstanden. So beschreibt die Mehrzahl der Autorenschaft das Definitionsproblem bzw. nimmt zum Teil umfangreich Bezug auf vorliegende Definitionen zur Clankriminalität. Die nach Redaktionsschluss getroffene Verständigung auf eine bundeseinheitliche Definition hat es nur noch in zwei Beiträge geschafft. Verlagsseitig ist die uneinheitliche Zitierweise sowie das mäßige Stichwortverzeichnis zu kritisieren. Dass etwa der Begriff „Clankriminalität" mit den Einträgen „Begriff der Clankriminalität" und „Clan-Begriff" doppelt genannt ist, hätte im Lektorat auffallen sollen. Ein einheitliches Literaturverzeichnis hätte sich schon deshalb angeboten, da es etliche Redundanzen bei den verwendeten Quellen gibt. Analog zu vergleichbaren Publikationen zur Clankriminalität werden auch hier umfangreich Zeitungsartikel zitiert bzw. Aufsätze der üblichen Verdächtigen.

Der Sammelband kann nur in geringem Maß Fundiertes zu „Grundlagen – Bekämpfungsstrategien – Perspektiven" beitragen. Der Anspruch des Herausgebers, Wissenschaft und Praxis zusammenzuführen, scheitert durch die geringe wissenschaftliche Beschäftigung mit dem Untersuchungsgegenstand. Wer zudem Argumente gegen die proklamierte Akademisierung der Polizei sucht, wird bei den Aufsätzen der Polizeipraktiker*innen fündig werden. Die teils problematischen kriminologischen Kompetenzen von Polizeischüler*innen bzw. -studierenden werden durch die Mängel in diesem „Leitfaden" eher verstärkt, statt sie im Rahmen der Ausbildung fundiert zu verringern. Der polizeilich geprägte Sammelband ist vor diesem Hintergrund nicht zu empfehlen. In Fortschreibung der 2020 erschienenen Broschüre der Essener Polizei über „Arabische Familienclans" lässt sich das Buch am ehesten noch als Werbung für die Politik der 1.000 Nadelstiche betrachten. (Karsten Lauber)

Mitarbeiter*innen dieser Ausgabe

Clemens Arzt, Berlin, Gründungsdirektor des FÖPS Berlin und bis März 2023 Professor für Polizei- und Versammlungsrecht an der HWR Berlin

Lucie Audibert, London, Anwältin bei Privacy International

Dirk Burczyk, Berlin, Referent für Innenpolitik der Linksfraktion im Bundestag und Redakteur von Bürgerrechte & Polizei/CILIP

León von der Burg, Hamburg, wissenschaftlicher Mitarbeiter im Forschungsprojekt „Situational Awareness: Sensing Security in the City" an der Universität Hamburg

Benjamin Derin, Berlin, Rechtsanwalt, wissenschaftlicher Mitarbeiter an der Professur für Kriminologie und Strafrecht an der Goethe-Universität in Frankfurt am Main, Redakteur von Bürgerrechte & Polizei/CILIP

Johannes Ebenau, Hamburg, wissenschaftlicher Mitarbeiter im Forschungsprojekt „Situational Awareness: Sensing Security in the City" an der Universität Hamburg

Lise Endregard Hemat, Oslo, Wissenschaftlerin am Friedensforschungsinstitut Oslo und Jurastudentin an der Universität Oslo

Jasper Janssen, Hamburg, wissenschaftliche Hilfskraft im Forschungsprojekt „Situational Awareness: Sensing Security in the City" an der Universität Hamburg

Tom Jennissen, Berlin, arbeitet als Rechtsanwalt und für die Digitale Gesellschaft, Redakteur von Bürgerrechte & Polizei/CILIP

Sonja John, Politologin, wissenschaftliche Mitarbeiterin im Forschungsprojekt „Police Accountability – Towards International Standards" an der Hochschule für Wirtschaft und Recht Berlin

Marius Kühne, Bochum, Politik- und Rechtswissenschaftler, wissenschaftlicher Mitarbeiter an der Ruhr-Universität Bochum, Redakteur von Bürgerrechte & Polizei/CILIP

Jenny Künkel, Bordeaux, wissenschaftliche Mitarbeiterin an der Universität Duisburg-Essen, Redakteurin von Bürgerrechte & Polizei/CILIP

Karsten Lauber, Leipzig, Kriminologe, Polizei- und Verwaltungswissenschaftler

Anna M. Fauda, Berlin, langjährige Tätigkeit in der Aus- und Fortbildung der Bundespolizei

Petra Molnar, Athen/ Boston, stellvertretende Direktorin Refugee Law Lab an der Universität York und Fellow am Berkman Klein Center in Harvard

Matthias Monroy, Berlin, Redakteur von Bürgerrechte & Polizei/CILIP

Marie-Theres Piening, Jena, wissenschaftliche Mitarbeiterin an der Professur für Kriminologie und Strafrecht an der Goethe-Universität in Frankfurt am Main

Norbert Pütter, Berlin, Politikwissenschaftler, Redakteur von Bürgerrechte & Polizei/CILIP

Giovanna Reder, Berlin, Researcherin bei Border Forensics

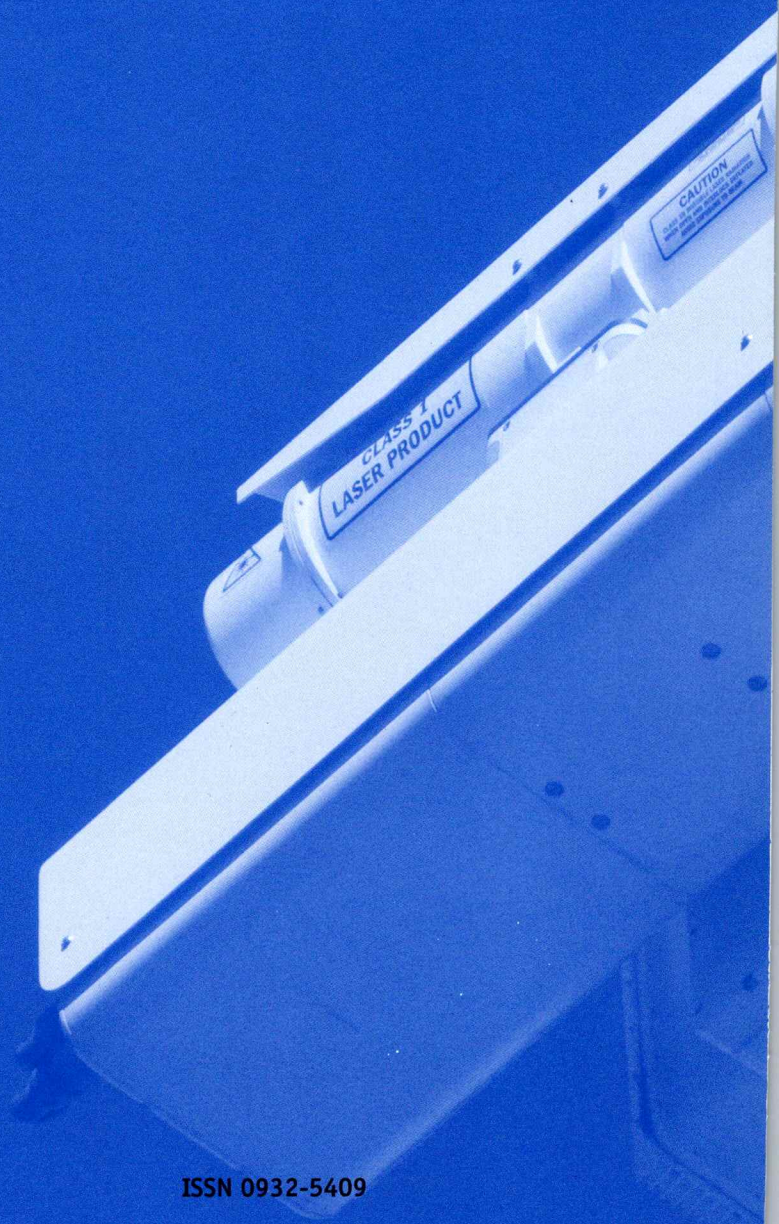
Stephanie Schmidt, Hamburg, Kulturanthropologin in der Kriminologischen Sozialforschung, Redakteurin von Bürgerrechte & Polizei/CILIP

Christian Schröder, Berlin, Redakteur von Bürgerrechte & Polizei/CILIP

Eric Töpfer, Berlin, Politikwissenschaftler, Redakteur von Bürgerrechte & Polizei/CILIP

Friederike Wegner, Berlin, Kulturwissenschaftlerin, Redakteurin von Bürgerrechte & Polizei/CILIP

Louisa Zech, Bochum, wissenschaftliche Mitarbeiterin an der Professur für Kriminologie und Strafrecht an der Goethe-Universität in Frankfurt am Main, Redakteurin von Bürgerrechte & Polizei/CILIP



ISSN 0932-5409