Bürgerrechte & Polizei

Cilip 121
April 2020

Polizeiliche Datenkulturen

Der Berner Club – außer Kontrolle
IT-Sicherheitsgesetz 2.0

Impressum

Bürgerrechte & Polizei/CILIP

Herausgeber: Institut für Bürgerrechte & öffentliche Sicherheit e.V.
Verlag: Verlag CILIP GbR, c/o Juristische Fakultät, Humboldt-Universität zu Berlin, Unter den Linden 6, 10099 Berlin
Redaktion, Gestaltung + Satz: Heiner Busch (verantw.), Dirk Burczyk, Benjamin Derin, Tom Jennissen, Jenny Künkel, Christian Meyer, Matthias Monroy, Norbert Pütter, Stephanie Schmidt, Christian Schröder, Eric Töpfer, Friederike Wegner, Louisa Zech
Titelbild: Hard Disk Drive, https://pxhere.com
Übersetzungen: Benjamin Derin
Druck: trigger.medien.gmbh, Berlin
Berlin, April 2020

Inhaber- und Beteiligungsverhältnisse: Persönlich haftende GesellschafterInnen: Heiner Busch, freiberuflicher Journalist, Bern; Martina Kant, Wissenschaftliche Referentin, Berlin; Udo Kauß, Rechtsanwalt, Freiburg; Wolf-Dieter Narr (†), em. Professor, Berlin; Eric Töpfer, Wissenschaftlicher Angestellter, Berlin; Jan Wörlein, Promovend, Paris

Redaktion & Vertrieb: Verlag CILIP c/o Juristische Fakultät · Humboldt-Universität zu Berlin · Unter den Linden 6 · 10099 Berlin
E-Mail: vertrieb@cilip.de · www.cilip.de
Zuschriften an die Redaktion bitte an: info@cilip.de

Bankverbindung: Verlag CILIP · Bank für Sozialwirtschaft · BLZ: 100 205 00
Konto: 3076800 · IBAN: DE81 1002 0500 0003 0768 00
SWIFT-/BIC-Code: BFSWDE33BER

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
Das Abonnement verlängert sich automatisch um jeweils ein weiteres Jahr, wenn nicht bis 30.11. des Jahres gekündigt wird.

ISSN 0932-5409
Zitiervorschlag: Bürgerrechte & Polizei/CILIP 121 (April 2020)

Inhalt

Schwerpunkt: Polizeiliche Datenkulturen

Redaktionsmitteilung

*Mit ihrem Auftritt im Frankfurter Waldstadion im Juli 2018 hat die Schlagersängerin Helene Fischer nicht nur ihre 40.000 Zuschauer*innen begeistert. Auch Polizeikräfte wollten mehr über die Frau wissen und fragten deshalb an diesem Abend ganze 83 Mal ihre Daten im POLAS, dem Informationssystem der hessischen Polizei, ab. 2018 gab es in Hessen 180 Verdachtsfälle zu missbräuchlichen Suchläufen. Deren Zahl stieg nach der Einführung von Stichprobenkontrollen im Februar 2019 offenbar rapide an. Dabei ging es nicht nur um Voyeurismus wie am Beispiel von Frau Fischer, sondern in einigen Fällen auch um rechtsradikale Ausspähungsversuche.*

*Der Missbrauch verweist aber wie immer auf den normalen Gebrauch: Das hessische POLAS wird täglich über 40.000 Mal konsultiert, das Schengener Informationssystem verzeichnet sogar 220 Abfragen pro Sekunde. Der Zugang zur Informationstechnik ist längst nicht mehr nur für Spezialist*innen reserviert, wie das in den Anfängen der Polizeilichen EDV der Fall war. Jeder Arbeitsplatz der Polizei ist heute auch ein Computer-Arbeitsplatz. Die großen Fahndungsdatenbanken können heute von jeder Straßenecke auch von mobilen Systemen abgefragt werden. Der Abgleich von Fingerabdrücken, der früher Stunden in Anspruch nahm, verläuft heute automatisch. Die Videoüberwachung eines Straßenzuges in Heidelberg samt Übertragung der Bilder zur Polizei, die sich Anfang der 80er Jahre als skandalöser technischer Großaufwand darstellte, erscheint heute im Zeitalter der automatischen Gesichtserkennung als banal. Was also ist der Stand der polizeilichen Datenkultur? Einige Antworten dazu gibt es in diesem Heft.*

***

*Die Leser*innen, die uns im Netz folgen (https://twitter.com/cilip_de), werden unser Corona-Tagebuch der Inneren Sicherheit entdeckt haben. Die nächste Ausgabe von Bürgerrechte & Polizei/CILIP wird dazu Gedrucktes nachlegen.*
(Heiner Busch)

Der Blick nach vorn im Daten-Dschungel

Datafizierung und Prävention

von Benjamin Derin, Christian Meyer und Friederike Wegner

Staatliches Interesse an Daten ist keineswegs neu. Mit der fortschreitenden Digitalisierung gewinnt das Nutzungspotenzial von Informationen – und damit auch das polizeiliche Streben danach – jedoch eine neue Qualität. Der behördliche Datenhunger trifft zudem auf eine unter dem Primat der Prävention stehende Gesellschaft, die ihr Verständnis von Sicherheit und Risiko neu definiert.

Registrierungs- und Identifizierungstechniken haben eine lange historische Tradition. Das Interesse am (heimlichen) Beobachten anderer lässt sich bis in die Antike zurückverfolgen. In der Renaissance entwickelten sich kulturell geprägte Praktiken und Techniken (wie Geheimschriften, Kryptographie, verborgene Tunnel und Türen), die alsbald auch (sicherheits-)politisch genutzt wurden.

Selbst die scheinbar harmlose Einführung von Hausnummern diente nicht (nur) dazu, die Orientierung der Bevölkerung zu erleichtern. Hausnummern gibt es seit dem 18. Jahrhundert, dem Zeitalter von Rationalisierung und sich verdichtender Bürokratisierung; und sie waren stets eine von der Obrigkeit verordnete Maßnahme, die die staatliche Kontrolle in den Bereich der häuslichen Privatsphäre ausweitete. In Wien versuchte man 1753 im Zuge einer Polizeireform und unter dem Stichwort der Verbrechensbekämpfung eine Hausnummerierung einzuführen. Nutzen und Gebrauch der individuellen Häuserkennzeichnung wuchsen schnell über den ursprünglich angegeben Zweck hinaus. Die Nummerierung erleichterte die militärische Rekrutierung, die Bekämpfung von Bettelei, aber auch Steuer- und Versicherungsangelegenheiten.

Die Erhebung und statistische Auswertung von Daten und Informationen nahm Ende des 19. Jahrhunderts stark zu. Der Kriminalist Alphonse Bertillon entwickelte ein frühes biometrisches Verfahren zur Personenidentifikation, um Wiederholungtäter*innen zu erkennen. Ei-

nige Jahre später legte Francis Galton den Grundstein für die Daktyloskopie, die Nutzung des Fingerabdrucks. Heute begegnet uns die Biometrie in automatisierter Form als Fingerabdruck-Identifizierungssystem oder als „intelligente“ Videoüberwachung mit Gesichtserkennung.[1]

Ende der 1960er Jahre hatte die Polizei in Deutschland mit der EDV-Nutzung begonnen. 1972 gingen die ersten Komponenten des INPOL-Systems ans Netz. „Kommissar Computer“ trat auf den Plan, und sein Auftritt war verbunden mit neuen präventiven Konzepten, deren bedeutendster Vertreter Horst Herold wurde, der von 1971 bis 1981 Präsident des Bundeskriminalamts (BKA) war.[2]

Das technische Niveau der 1970er und frühen 1980er Jahre war zwar – von heute aus betrachtet – sehr niedrig. Dennoch zeigt sich bereits in diesen Jahren die Verschiebung des polizeilichen Selbstverständnisses von der Aufklärung und Verfolgung hin zur „vorbeugenden Bekämpfung“ von Straftaten. Die Polizei solle nicht nur reagieren, sondern frühzeitig agieren, „vor die Lage kommen“ … Derartige Parolen, mit denen heute das Predictive Policing beworben wird, fanden sich bereits in dieser frühen Phase der Computerisierung der Polizeiarbeit.

Als zusätzlicher Treibriemen für die Einführung neuer Techniken und für die Ausweitung darauf gestützter polizeilicher und geheimdienstlicher Befugnisse wirkte bereits in den 1970er Jahren die Terrorismusbekämpfung. Unter Herolds Präsidentschaft praktizierte das BKA Ende der 1970er Jahre die ersten Rasterfahndungen und bediente sich bei diesen „negativen Datenabgleichen“ unter anderem an den Datenbeständen anderer Behörden oder öffentlicher und privater Unternehmen.

Zwar stand die technische und rechtliche Entwicklung auch in den 1990er Jahren nicht still. Ideologisch getrieben wurde sie unter anderem durch die Debatte um „Organisierte Kriminalität“. Mit den Anschlägen des 11. September 2001 wurde die Terrorismusbekämpfung jedoch erneut zur zentralen Legitimationsfigur für den Ausbau von Überwachungsmöglichkeiten. Auf europäischer Ebene erfolgte ein enormer Ausbau großer Datenbanken, der mit dem Aufstieg der Biometrie als neuer Technik einherging. 2005 beschloss die Europäische Union (EU)

1 s. den Artikel von Roland Meyer in dieser Ausgabe

2 Ein ausführliches und noch heute lesenswertes Interview mit Herold Herold erschien in Bürgerrechte & Polizei/CILIP Nr. 16 (3/1983) und 18 (2/1984). Auf cilip.de ist es frei verfügbar.

ihre Richtlinie zur Vorratsspeicherung von Telekommunikationsdaten, 2016 folgte nach langem Hin und Her die Richtlinie zur Fluggastdatenspeicherung. Ähnliche Entwicklungen fanden auf nationaler Ebene (nicht nur) in Deutschland statt; das 2017 verabschiedete neue BKA-Gesetz sowie die neuen Länderpolizeigesetze sind aktuelle Beispiele.

Mit der Entwicklung der Informations- und Kommunikationstechnologien sind der Überwachung ungeahnte neue Möglichkeiten eröffnet worden. Heute haben Menschen eine Vielzahl von exakt zuordenbaren Adressen: Wohn- und Büroadressen, IP- und E-Mail-Adressen, (Mobil-) Telefonnummern und Smart-Homes. Entsprechend der wachsenden Datenvielfalt hat sich auch das Interesse an deren polizeilicher Erfassung und Analyse erweitert. Standortdatenabfrage, Chatverläufe, Staatstrojaner und Verschlüsselungsverbote sind Gegenstand populärer Debatten um Überwachung und Prävention.

Präventiver Hunger nach Daten

Präventionskonzepte waren weder in den 1970er Jahren, im „sozialdemokratischen Jahrzehnt“, noch sind sie heute im neoliberalen Zeitalter auf den Bereich der Inneren Sicherheit beschränkt.[3] In den 1970er Jahren waren sie Teil der allgemeinen Planungseuphorie, die die gesamte öffentliche Verwaltung erfasste. Für Horst Herold hatte die Polizei durch ihr in Akten und Karteien gebundenes Wissen über die Gesellschaft ein „Erkenntnisprivileg“. Die Mobilisierung dieses Wissens durch die EDV sowie eine daran ausgerichtete organisatorische Reform sollte die Polizei in die Lage versetzen, „Gesetzesnormen zur Aufhebung oder Änderung der gesellschaftlichen Bedingungen, unter denen Kriminalität entsteht“, zu formulieren. Die Polizei erschien dabei quasi als Motor einer „gesetzgeberischen Prävention“, einer Reformpolitik, die zu mehr Gleichheit und Gerechtigkeit führen sollte.

Die Hoffnungen auf eine „gesellschaftssanitäre Rolle“ der Polizei verschwand schon bald nach dem Ausscheiden des Intellektuellen Herold von der polizeilichen Tagesordnung. Ziel war nun nicht mehr die Abschaffung der Kriminalität, sondern nur noch deren Kontrolle. Doch auch unter dem neuen „abgespeckten“ Ziel bleibt Prävention abhängig

3 zur gesamtgesellschaftlichen Präventivorientierung: Castel, R.: Von der Gefährlichkeit zum Risiko: Auf dem Weg in eine post-disziplinäre Ordnung?, episteme. Online-Magazin für Philosophie und Praxis 2002, No. 2,www.episteme.de/htmls/Castel.html

von Information. „Jede Prävention steht vor einem grundlegenden Problem: Sie muss mit dem beschränkten Wissen der Gegenwart eine Prognose erstellen und auf dieser Basis ein präventives Handlungsprogramm entwerfen. Die Gewinnung und Verarbeitung von Informationen bildet deshalb die Basis jeder Präventionsstrategie“ und der „Bedarf an Informationen nimmt in dem Maße zu, indem Unklarheit über das Ausmaß und die Bedingungsfaktoren dessen besteht, was verhindert werden soll – ein Merkmal, das auf die komplexen Phänomene ‚Kriminalität‘ und ‚Sicherheit‘ eindeutig zutrifft. Wer erfolgreiche Kriminalprävention betreiben will, weiß deshalb nie genug.“[4]

Prävention als Risikomanagement

Dies gilt umso mehr, je größer die Schäden sind, denen präventiv entgegen getreten werden soll. Spätestens seit dem 11. September 2001 erscheinen auch Worst-Case-Sezenarien plausibel und bestimmen die Präventionskonzepte nicht nur in der Terrorismusbekämpfung.

Obwohl solche Worst-Case-Szenarien unwahrscheinlich erscheinen, sind die Maßnahmen, die ergriffen werden, um ihren Eintritt zu verhindern, real und haben Konsequenzen für die Grundrechte der davon Betroffenen. Auch wenn diese ansonsten „unbescholten“ sind, droht ihnen, wenn sie als Träger*innen gefährlicher Merkmale erkannt werden, der Ausschluss von bestimmten Rechten oder eine eingehende Kontrolle. Das ist die Logik, die beispielsweise der Fluggastdatenspeicherung und -auswertung oder den Einreisegenehmigungssystemen (wie dem System ETIAS der EU) unterliegt.

Mit der Prävention verändert sich grundlegend der gesellschaftliche Umgang mit der Zeit. Während traditionell Erfahrungen aus der Vergangenheit als Orientierung für ein Handeln in der Gegenwart dienten, wird heute zunehmend die Gegenwart unter der Imagination einer düsteren Zukunft umstrukturiert. Dass etwas schlimmes passieren wird, wird vorausgesetzt, die Bedrohung als gegeben angenommen. Einzig Wahrscheinlichkeit, Intensität und möglicher Zeitpunkt eines Terrorakts (oder eines schweren Verbrechens, einer Umweltkatastrophe oder ähnlichem) müssen noch ausgehandelt und dementsprechende Maßnahmen ergriffen werden.

4 siehe Pütter, N.: Prävention – eine populäre Überzeugung, in: Bürgerrechte & Polizei 86 (1/2007), S. 3-15 (9f.)

Diese Risikoprävention entspricht weitgehend jener Gouvernementalität, die Michel Foucault bereits ab Mitte des 18. Jahrhunderts als zunehmende staatliche Praxis erkannte. Ausgehend von der Ökonomie entstehe ein neuer Machttyp,[5] der auf die gesamte Bevölkerung und deren Sicherheit zielt – „zugleich aufgeklärt, durchdacht, analytisch, wohlberechnet, vorausschauend". Bürgerliche Wissenschaft und die Entstehung eines modernen Staatswesens stehen in engem Zusammenhang mit dem Glauben an eine Abbildbarkeit der Gesellschaft in Zahlen. Mittels Messungen und Statistik sollen Zusammenhänge aufgedeckt und Vorhersagen getroffen werden. Von nun an sind nicht mehr nur Verbote sowie Methoden des Überwachens und Strafens relevant, die sich an Einzelne richten, sondern zunehmend Fragen nach Kriminalitätsraten und Einflüssen auf deren Veränderung. Das Umfeld von Delikten (zum Beispiel Geographie, soziales Milieu) und Möglichkeiten, dieses zu beeinflussen, sind jetzt Gegenstand eines spezifisch staatlichen Wissens. Es geht, so Foucault, nicht länger um den einzelnen Regelübertritt, sondern um ein möglichst ökonomisches Verhältnis zwischen Delinquenz und Repression. Zugespitzt: Ab wie vielen Ladendiebstählen lohnt sich die Beschäftigung eines Ladendetektivs oder die Installation einer Kameraanlage? Oder etwas komplizierter: Welche Faktoren müssen zusammenkommen, damit der Algorithmus von Gotham den hessischen Polizist*innen empfiehlt, in eine bestimmte Straße zu fahren? Es geht mehr um akzeptable Grenzwerte und Relationen, weniger um Normen als vielmehr um Normalisierung.

Digitaler Präventionsstaat

Die Erfahrungen mit dem internationalen Terrorismus bieten den Anlass der neueren Präventionsstrategien, der technische Fortschritt – das, was gemeinhin als Digitalisierung bezeichnet wird – liefert die Möglichkeiten. Die Metainfrastruktur des Internets und die darüber stattfindende Kommunikation, Mobiltelefone, Digitalkameras und die Konvergenz dieser Technologien im Smartphone bringen eine zuvor unvorstellbare Menge und Qualität an Daten mit sich. Eine Unmenge an Bildern, Kontaktdaten und vor allem detaillierte Bewegungs-, Konsum- und Persön-

5 Foucault nennt diese Macht Gouvernementalität. Die Verweise beziehen sich auf: Foucault, M.: Sicherheit, Territorium, Bevölkerung. Geschichte der Gouvernementalität I, Frankfurt/M. 2006

lichkeitsprofile bieten nie dagewesene Erkenntnisse über Bevölkerung und Einzelpersonen. Diese zunächst privatwirtschaftlich gesammelten Daten wecken Begehrlichkeiten bei Polizeien und Geheimdiensten, die sie in ihrem präventiven Sinne nutzen. EU-Innenminister*innen freuten sich bereits 2007 über den anrollenden „Daten-Tsunami“ und bemühen sich seither, nicht vom sicherheitspolitischen Surfbrett zu fallen.[6] Die großen Plattformunternehmen mit ihren datenzentrierten Geschäftsmodellen (Google, Amazon, Facebook, Apple und deren angegliederte Firmen; kurz: GAFA) haben nicht nur faktische Datenmonopole, man kann auch davon ausgehen, dass sie über die avanciertesten Auswertungsmethoden verfügen. Doch ihr Interesse unterscheidet sich von dem der Polizeien. Statt um präventive Bevölkerungskontrolle geht es ihnen um kommerzielle Interessen. Die Subjekte sind für sie primär als Konsument*innen interessant, nicht als potenzielle Terrorist*innen. Daher ist es für GAFA und deren Werbekund*innen relativ gleichgültig, wenn einzelne kein Profil haben. Sie verkaufen zwar zielgerichtete (targeted) Werbung, doch dafür reichen Interessengruppen oder ein lokal eingegrenztes Publikum, um es für die Anzeigenkund*innen attraktiv zu machen. Staatliche Überwachung ist hingegen am Einzelnen interessiert. Sie darf – der Logik der Prävention folgend – keine Lücke dulden, weil das einzelne Subjekt, das durch das Raster fällt, reicht, um die Bombe in der U-Bahn zu legen.

Doch Plattformen und Sicherheitsbehörden inspirieren sich auch gegenseitig und sind nicht immer leicht zu trennen, wenn es um den Umgang mit Daten geht. Beispielsweise wurden die Potenziale rechnergestützten Marketings nach dem 11. September 2001 offensiv als Werkzeuge zur Terrorismusbekämpfung beworben und Google suchte schon vor dem Patriot Act in den eigenen Daten nach Hinweisen auf die 9/11-Attentäter. Suchanfragen sind in den vergangenen Jahren zu einem immer wichtigeren Teil polizeilicher Ermittlungen geworden. Google kooperiert seit 2004 verstärkt mit CIA und anderen Sicherheitsbehörden,

6 Die Rede vom Daten-Tsunami drückt auch eine – in der übrigen Digitalisierungsdiskussion wiederkehrende – Naturalisierung aus, die suggeriert, man sei den technologischen Veränderungen ausgeliefert und könne lediglich reagieren; siehe: EU-Innenpolitiker rüsten sich für den digitalen Tsunami, heise online v. 11.9.2018

macht mit ihnen Geschäfte und ist auch technologisch mit ihnen verstrickt, zumindest in den USA.[7]

Das Verhältnis zwischen GAFA und Staatsgewalt ist nichtsdestoweniger von Widersprüchen geprägt, die gelegentlich auch offen ausgetragen werden. Beispiele sind der Streit um die Verantwortlichkeiten bei gesetzwidrigen Postings (Uploadfilter), die wiederkehrenden Auseinandersetzungen um Backdoors zu staatlichen Überwachungszwecken in Apps oder den Zugriff auf verschlüsselte Daten in Mobiltelefonen.

Ebenso dient das Feld digitaler Kommunikation den Polizeien nicht nur als schier unendliche Ressource und Ermittlungsinstrument, sondern gilt ihnen ebenso als Gefahrengebiet, das genuine Bedrohungen wie Angriffe auf kritische Infrastrukturen oder Cybercrime hervorbringt.

Um die Sicherheit des Staats und seiner Interessen zu schützen, darf es keine unkontrollierten digitalen Schlupfwinkel (Darknet, verschlüsselte Kommunikation, anonymisierte Dienste) geben. Um diese auszuleuchten, soll kein Mittel ungenutzt bleiben. Was technisch möglich ist, soll auch gemacht werden – so der Imperativ innerer Sicherheit. Die Polizei muss mit dem Verbrechen gleichziehen, idealiter sogar besser ausgestattet sein. Das heißt im Klartext, es darf keine Verschlüsselung geben, die der Staat nicht knacken kann, keine Daten, auf die er keinen Zugriff hat.

Auch wenn die Präventionsorientierung nicht auf den Bereich innerer Sicherheit beschränkt ist, sondern ein gesamtgesellschaftliches Phänomen darstellt, hat die Polizei daran ihr ganz eigenes Interesse. Andererseits agiert sie nicht unabhängig von gesellschaftlichen Diskursen und Stimmungen, sondern steht mit ihnen in einer Wechselbeziehung.[8]

Der heutige Präventionsstaat fußt auf digitaler Technologie und wird diese Basis auch vorerst nicht verlassen. Eine kritische Perspektive muss sich dabei bewusst sein, dass auch ein noch so vorausschauendes Vorgehen gegen Kriminalität oder Terrorismus nur Symbolik oder bestenfalls Symptombekämpfung darstellen kann, da solche Phänomene letztlich auf Widersprüche in der (kapitalistischen) Gesellschaft zurückgehen und eine hundertprozentige Risikofreiheit unerreichbar ist.

---

7 Levin, Y.: Surveillance Valley. The Secret Military History of the Internet, New York 2018

8 zur subjektiven Sicherheit siehe Singelnstein, T.: Sicherheit, Prävention und Polizei, in: Bürgerrechte & Polizei/CILIP 118/119 (Juni 2019), S. 17-24

„Die Herrschaftsdienlichkeit der sich mehrfach überlagernden, vielfingrigen technologischen Sicherheitsnetze lässt sich kaum noch institutionell, noch viel weniger Personal zuordnen, so sehr Personen und Institutionen davon profitieren. Diese Netze dienen in einer nur technologisch erreichbaren Weite und Tiefe dem System kapitalistischer Herrschaft jenseits aller liberaldemokratischen Verfassungsgarnierungen."[9]

Techno Policing zwischen Glauben und Wissen

Prävention ist ein nicht abschließbarer Prozess. Dies gilt insbesondere auch, wenn sie leitende Strategie einer Technisierung, genauer einer Datafizierung der Polizei ist. Das Wissen über potenzielle Risiken könnte schließlich immer noch besser, noch umfassender sein. Hinter Maßnahmen wie der Vorratsdatenspeicherung steht der Gedanke, dass jede Person irgendwann zur Zielperson werden könnte.[10] Weil die Zukunft unbestimmt ist, müssen alle erfasst werden. Diese Rationalität entwickelt ihre eigene Dynamik. Das manische Datensammeln der Behörden dient aber nicht nur konkreten Ermittlungen. Die verfügbaren Daten werden auch zur algorithmischen Verdachtsschöpfung eingesetzt.

Programme wie hessenDATA[11] sollen der Polizei dazu verhelfen, „vor die Lage" zu kommen, also präventiv Alarm zu schlagen und proaktives Handeln auszulösen, beispielsweise durch die Bestreifung eines einbruchgefährdeten Gebiets oder die Hausdurchsuchung bei einem „Gefährder". Mit der Software werden keine neuen Daten erhoben, sondern bestehende Daten zusammengeführt und analysiert: Darunter fallen polizeiinterne Informationen über abgeschlossene Fälle und laufende Fahndungen, Daten aus Telefonüberwachungen oder ausgelesenen Handys und sonstige Kommunikationsdaten. Die Stärke ist die mögliche Verknüpfung von sogenannten strukturierten Daten (Tabellen etc.) mit unstrukturierten (etwa Fotos). Neue Zusammenhänge zwischen Objek-

9 Narr, W.-D: Die Technologisierung der Polizei, in: Bürgerrechte & Polizei/CILIP 76 (3/2003), S. 6-11

10 zum Begriff des Targeting: Chamayou, G.: Oceanic enemy. A brief philosophical history of the NSA, in: Radical Philosophy 2015, No. 191, pp. 2-12

11 HessenDATA basiert auf der Software Gotham und wurde von der US-amerikanischen Firma Palantir entwickelt. Seit 2017 ist es in Hessen im Einsatz, in NRW wird gerade ein vergleichbares Palantir-Produkt eingeführt. Zunächst war der Einsatz von hessenDATA auf Anti-Terror-Ermittlungen beschränkt, mittlerweile wird das System auch im Bereich der organisierten Kriminalität und rechtsmotivierter Straftaten genutzt. Eine Smartphone-Version für den mobilen Einsatz ist in Vorbereitung.

ten und Personen oder zwischen verschiedenen Ermittlungen sollen so zu Tage gefördert werden. Dazu kann hessenDATA auch Informationen aus sozialen Netzwerken einbeziehen. (Das hessische Innenministerium behauptet, dass die Software keinen Zugriff auf das Internet habe und nur Daten verwendet würden, welche die Polizei von Plattformen rechtmäßig erlangt hätte.)

Die Polizeibehörden sollen die öffentlich zugänglichen Daten auf Facebook, Twitter, Instagram und Co. zwar nicht anlasslos abgrasen, aber für konkrete Maßnahmen nutzen. Man bezeichnet dies als Social Media Intelligence oder allgemeiner als Open Source Intelligence (OSINT). Auch für den Verfassungsschutz sind die öffentlich zugänglichen Quellen durch Social Media erheblich gewachsen. Die Masse der Daten (nicht nur im Netz, sondern auch auf beschlagnahmten Geräten oder Bilder aus Videoüberwachung) ist nur noch maschinell zu bewältigen, so dass auch die Technisierung ihre eigene Dynamik entfaltet und für die Datenauswertung immer öfter auf sogenannte künstliche Intelligenz (KI) und maschinelles Lernen zurückgegriffen wird. Zugunsten des (Aber-)Glaubens an die Allmacht technikgestützter Prognostik wird allzu häufig übersehen, dass auch diese Algorithmen entwickelt, mit Daten gefüttert, anhand menschengemachter Theorien ausgerichtet und interpretiert werden müssen. Wie und nach welchen Anforderungen dies geschieht, bleibt weitgehend im Dunkeln. Und dass sich durch den Einsatz solcher Technologien ein höheres Sicherheitsniveau erreichen ließe, ist keineswegs nachgewiesen.

Ob die rechtsterroristische Anschlagswelle in Hessen diesen Glauben nachhaltig erschüttert hat, wird sich noch zeigen. Die Zeichen sehen nicht danach aus. Im Gegenteil laufen aktuell mehrere Forschungsprogramme, die sich der Verknüpfung von Social Media- und Polizeidaten widmen und technische Lösungen für gesellschaftliche Widersprüche nahelegen. Auch die Anbieter entsprechender Gadgets und Software verpassen ihrerseits keine Gelegenheit, den vermeintlichen technischen Vorsprung der Kriminellen zu betonen, damit ein möglichst großer Teil der Polizeibudgets später in den Konzernbilanzen auftaucht. Unter dem Titel SENTINEL experimentieren die Polizeien in Osnabrück, Dortmund und München mit OSINT und erhoffen sich Hinweise darauf, ob eine Zielperson Sportschütze, Kampfhundehalter oder kampfsporterfahren ist. Mit PANDORA, X-Sonar und RadigZ laufen aktuell zudem drei Forschungsprogramme zu Prävention gegen sogenannte Radikalisierung und Propaganda im Netz.

Neben dem Erkennen von Beziehungsmustern ist automatische Gesichtserkennung ein beliebtes Anwendungsfeld von KI. Das Problem der False Positives, also fälschlich gemeldeter Treffer, hat sich bei einem Test am Berliner Bahnhof Südkreuz erneut eindrücklich gezeigt. Gesichtserkennungssoftware lauert aber nicht nur hinter Kameras an öffentlichen Orten, sondern kann sich auch hinter lustigen Apps verbergen, deren Algorithmus durch die Nutzung trainiert wird.

Im Vergleich zu Kameras, die oft gut sichtbar sind, sind Datenbanken als maschinelle Infrastruktur, Software und gespeicherten Daten ihrem Wesen nach im Verborgenen. Einmal in den Datenbanken, wird der ursprüngliche Zweck der Speicherung von dem Datum getrennt und die Einträge können neu kombiniert werden. Was am Ende abgerufen wird, ist so mitunter hochgradig konstruiert und technisch geformt, erscheint auf dem Screen aber als nackte Wahrheit, die polizeiliches Handeln anleitet. Als Herrschaftswissen unterliegen polizeiliche Daten ebenso notwendig der Geheimhaltung[12] wie die Google Algorithmen als Herz des Geschäftsmodells.

Polizeiliche Praxis ändert sich unter dem Einfluss von Digitalisierungsprozessen. Doch es wäre unzulässig verkürzt zu behaupten, es sei „die Technik", die uns vor eine neue Situation stellt. Sicherheitstechnik ist wie alles andere auch von Menschen gemacht und daher nicht jenseits von sozialen Kräfteverhältnissen zu verstehen.

> „Zu keiner Zeit in der Menschheitsgeschichte hat es derart gute Bedingungen für eine totalitäre Diktatur gegeben wie heute … Natürlich kann man Bilder von Aufständen in Sekundenbruchteilen in alle Welt schicken, das kann kein Diktator mehr verhindern. Aber es ist schon die Frage, wer auf welche Informationen Zugriff hat. Da hat ein smarter totalitärer Herrscher ganz andere Möglichkeiten als ein x-beliebiger User."[13]

Die rechtliche Entwicklung

Die zunehmende präventive und sicherheitsobsessive Ausrichtung der Gesellschaft und die stets voranschreitenden technischen Möglichkeiten finden ihren Niederschlag auch in einer entsprechenden rechtlichen

12 Pütter, N.: Geheimisse im Informationszeitalter, in: Bürgerrechte & Polizei/CILIP 107 (Januar 2015), S. 3-9. Auch Foucault betont die Notwendigkeit der Geheimhaltung staatlichen Wissens.

13 Die Grenze ist überschritten. Interview mit Armin Grunwald, Süddeutsche Zeitung online v. 28.1.2018

Entwicklung. Einerseits füllen sich die Gesetzbücher mit neuen Eingriffsbefugnissen zur Datenerhebung, insbesondere im Vorfeld konkreter Gefahrenlagen und unter Einbeziehung der neuesten Überwachungstechnologien. Andererseits werden die Voraussetzungen für eine nahezu grenzenlose Nutzung, Auswertung, Speicherung und Weitergabe der verfügbaren Daten geschaffen.

Auf der Ebene der Datenerhebung sind neben klassische Ermittlungsbefugnisse wie die Telefonüberwachung etwa automatisierte Bestandsdatenauskünfte, Verkehrsdatenabfragen, E-Mail-Beschlagnahmen, Server-Überwachungen, stille SMS, IMSI-Catcher, Funkzellenabfragen, Quellen-TKÜ und Online-Durchsuchungen getreten. Dass noch um die Jahrtausendwende die Debatte um die Einführung eines vergleichsweise eingegrenzten Instruments wie des sogenannten Großen Lauschangriffs zum Rücktritt einer Justizministerin führen konnte, scheint in Zeiten, in denen Maßnahmen wie die Online-Durchsuchung per Änderungsantrag und ohne wesentlichen parteipolitischen Widerstand durch das Parlament geschleust werden, kaum noch vorstellbar. Bemerkenswert ist dabei, dass regelmäßig nicht das Gesetz die Praxis ändert, sondern umgekehrt: Technologien wie die stille SMS oder die Quellen-TKÜ werden von den Behörden zunächst ohne spezifische Ermächtigung eingesetzt, sobald die technischen Möglichkeiten entstehen, und im Zweifel auf bestehende Rechtsgrundlagen gestützt. Daraufhin entscheiden entweder die Gerichte, dass dies ausreicht – oder der Gesetzgeber erlässt schleunigst das erforderliche Gesetz.

Parallel zum Ausbau der originären Erhebungsermächtigungen findet eine zunehmende rechtliche Einbeziehung der Privaten unter Ausnutzung von deren mitunter massiven Datenbeständen und Ressourcen statt. Die Überwachung von Telefonen ist unter anderem deshalb so beliebt, weil die Betreibenden früh gesetzlich verpflichtet wurden, auf eigene Kosten die erforderlichen technischen Einrichtungen vorzuhalten. Und heute verblasst das Abfangen der Standortdaten einzelner Mobiltelefone durch die Polizei angesichts der gigantischen Datenlager, auf die Regelungen wie die Vorratsdatenspeicherung oder die Fluggastdatenspeicherung Zugriff versprechen. Hier wird sich insbesondere die Frage nach dem staatlichen Zugriff auf die Datenreservoirs von GAFA stellen (derzeit etwa anhand des Netzwerkdurchsetzungsgesetzes und seinen fortwährenden Ausweitungen).

Weil der staatliche Datenstaubsauger im Laufe der letzten Jahrzehnte in nahezu jeden Lebensbereich vorgedrungen ist, könnte der gesetzli-

che Datenhunger bald an eine Art natürliche Grenze stoßen: Irgendwann gibt es schlicht keine Felder mehr, die der Informationsgewinnung verschlossen sind und in die sich „Gesellschaftsfeinde“ noch flüchten könnten – das Gegenteil von „going dark“ ist nun mal die grenzenlose Helligkeit. Dies andeutend, hat sich die gesellschaftliche Auseinandersetzung bereits auf die nächste Ebene verlagert: Von wachsender Bedeutung ist der sich an die Erhebung anschließende Umgang mit den erlangten Daten. Das polizeiliche Interesse liegt häufig nicht so sehr in der Erlangung eines spezifischen Datums, sondern in Abgleich, Austausch und computergestützter Auswertung großer Mengen an Daten, die für sich genommen relativ harmlos sein können. Dieses Interesse ist wie dargelegt Konsequenz sowohl der technischen Entwicklung und der damit einhergehenden Analyse- und Verknüpfungsmöglichkeiten, als auch des gewandelten gesellschaftlichen Anspruchs dahingehend, Gefahren zu erkennen, bevor sie sich realisieren – also zu einem Zeitpunkt, zu dem die Relevanz der erhobenen Daten nicht ohne Weiteres ersichtlich ist. Nachdem sich mittlerweile die Erkenntnis durchgesetzt hat, dass auch die Weiterverwendung und der Abruf von Daten sowie schon die nur flüchtige Erfassung etwa im Rahmen massenhafter automatisierter Verfahren einen Eingriff in die informationelle Selbstbestimmung darstellen und es in dieser Hinsicht keine „belanglosen“ Daten gibt, entfaltet sich auf diesem Gebiet eine umso geschäftigere gesetzgeberische Aktivität. Dies umfasst etwa die Erleichterung der behördeninternen Weiterverwertung und Umwidmung von Daten (so unter dem erneuerten Bundeskriminalamtsgesetz), aber auch den Austausch unter Behörden (beispielsweise im Rahmen des Gemeinsamen Terrorismusabwehrzentrums oder den weitreichenden Übermittlungsbefugnissen der Landesverfassungsschutzgesetze), insbesondere auch auf internationaler Ebene und in auf den ersten Blick unscheinbaren Bereichen wie dem nunmehr direkten Zugriff aller Polizeibehörden auf die biometrischen Lichtbilddatenbanken der Meldebehörden ohne konkreten Anlass. Ebenso relevant ist die Ausweitung dessen, was mit verfügbaren Daten jeweils angestellt werden darf, also zum Beispiel die schrittweise in die Polizeigesetze implementierte Erlaubnis des Einsatzes von Analysesoftware wie hessenDATA, automatisierter Gesichtserkennungstechnologie und intelligenten Kamerasystemen, die selbstlernend erkennen sollen, ob jemand gerade in verdächtiger Weise einen Koffer abstellt. In dieselbe Kerbe schlagen auch Maßnahmen wie die erweiterte DNA-Analyse, mittels der das potenzielle Aussehen und teilweise auch die Herkunft eines Spuren-

gebers prognostiziert werden dürfen. Die Verlagerung von der Erhebungs- auf die Verwertungsebene wird bislang nur von einem unzureichenden Bewusstsein für die damit einhergehenden eigenständigen rechtlichen Problematiken begleitet. Das Dogma der Prävention und die schiere Wucht der technologischen Machbarkeit überlagern häufig noch jegliche Bedenken.

Ausblick

Es stellt sich einmal mehr die Frage, in was für einer Gesellschaft wir leben wollen. Passen die enorme Ausweitung des Erlaubten und deren Auswirkungen auf Bürgerrechte mit unseren Vorstellungen zusammen? Das perfide und ständig wiederholte Versprechen, dass die nächste schwere Straftat oder der nächste Anschlag zwar bevorstünden, sich aber mittels ausreichender Eingriffsbefugnisse und Datenverarbeitung verhindern ließen, kann nicht darüber hinwegtäuschen, dass hundertprozentige Sicherheit und automatisierte Prävention illusorisch bleiben müssen. Ohne die Risiken zu leugnen, die aus einer Gesellschaft voller Widersprüche notwendig erwachsen, müssen die Maßnahmen zu deren Bekämpfung immer kritisiert und manchmal auch selbst bekämpft werden.

Die durchaus verheerenden Ereignisse um die Corona-Pandemie der letzten Monate haben die Wucht solcher Hoffnungen eindrucksvoll bewiesen: Die Telekom übermittelte an das dem Bundesgesundheitsministerium unterstellte Robert-Koch-Institut unbürokratisch die Bewegungsdaten von 46 Millionen Kund*innen zur Abbildung von Mobilitätsverhalten, und Pläne für eine gesetzliche Ermächtigung zur personenbezogenen Ortung aller Kontaktpersonen von Infizierten lagen sofort auf dem Tisch. Dieses Beispiel außerhalb des Innere-Sicherheits-Diskurses zeigt, wie schmerzhaft die Auseinandersetzung über die Grenzen von Datenverarbeitung werden kann – aber auch, warum sie so dringend notwendig und besser früher als später zu führen ist.

Von der Kartei zum „Datenhaus“

Eine kleine Geschichte polizeilicher Datenhaltung

von Dirk Burczyk

Alle Jahre wieder ... überlegt sich die deutsche Polizei, ihre Informationssysteme zu modernisieren. Mit dem Programm „Polizei 2020“ startet der nächste Versuch, die bislang getrennten „Datensilos“ durch ein gemeinsame „Datenhaus der deutschen Polizei“ zu ersetzen.

Seit fast 50 Jahren versucht die Polizei in Deutschland, die in den Landeskriminalämtern und im Bundeskriminalamt (BKA) verfügbaren Informationen in einem Verbund zusammenzuführen. Und ebenfalls seit 50 Jahren stehen die Innenminister*innen von Bund und Ländern vor dem Problem, dass die Länder – in denen Fragen einer effizienten Polizeiarbeit immer eines der Topthemen in Wahlkämpfen sind – unabhängig voneinander mit dem Aufbau von Informationsverarbeitungssystemen beginnen. Als die Innenministerkonferenz 1972 den Aufbau des „Informationssystems der Polizei“ (INPOL) beschloss, musste sie eine Reihe nicht kompatibler Systeme miteinander verbinden. Statt eines vereinheitlichten polizeilichen Meldedienstes kam dabei aber nur ein Fahndungssystem heraus. An den Terminals der unteren Polizeibehörden konnten nun Fahndungsausschreibungen über das jeweilige Landesrechenzentrum an das Rechenzentrum des BKA übermittelt und damit automatisch bundesweit verteilt, aktualisiert, gelöscht und abgerufen werden. Damit änderte sich der polizeiliche Alltag rasant, Personenüberprüfungen konnten innerhalb von Sekunden per Funk mit dem Kolleg*innen am Terminal vorgenommen werden.

Neben der Fahndungsdatenbank wurden Datenbanken zu Personen, Institutionen, Objekten und Sachen (PIOS, später kamen „Ereignisse“ hinzu) eingerichtet, offiziell als „Aktenerschließungssysteme“ bezeichnet. Anders als im Kriminalaktennachweis KAN, in dem tatsächlich zunächst nur Fundstellen in Ermittlungsakten hinterlegt sind, ließen

sich mit den PIOS-Datenbanken einzelne Daten unabhängig von ihrem Aktenzusammenhang recherchieren.[1] Zugang hatten hier nur die fachlich zuständigen Referate oder Abteilungen. Ab 1976 wurden zu einzelnen Phänomen- oder Sachbereichen „PIOS-Verfahren“ eingeführt, das erste zum Bereich Terrorismus. Diese Verfahren wurden entweder als Verbund- oder Zentraldateien geführt. In den Verbunddateien konnten die örtlichen Sachbearbeiter*innen die Daten direkt und ohne weitere Bearbeitung durch das BKA eingeben. Anders die Zentraldateien, bei denen die Daten mündlich oder per Fernschreiber angeliefert und von einem Mitarbeiter des BKA eingegeben wurden; auch die Abfrage erfolgte auf diesem Weg. Ab 1986 sollte mit der Einrichtung von „Arbeitsdateien“ auf Basis der PIOS-Verfahren der Informationsaustausch in den Bereichen Innere Sicherheit/Staatsschutz, Drogen, „Organisierte“ Kriminalität u. a. weiter verbessert werden. Daneben wurden zur Bewältigung umfangreicher Ermittlungsverfahren „Spurendokumentationssysteme“ (SPUDOK) eingerichtet, in denen ebenfalls komplexe Suchen möglich waren.

Der PC kommt in die Polizei

Mit den 80er Jahren begann auch eine neue technologische Entwicklung. Elektronische Datenverarbeitung hieß nicht mehr nur Großrechner mit Eingabeterminals, sondern auch PC am Arbeitsplatz. Der hielt auch in den Büros der Kriminalpolizei Einzug. Die folgende Entwicklung ließ sich unter den Schlagworten Vernetzung und dezentrale Datenverarbeitung zusammenfassen.[2] Großrechner, Mehrplatzsysteme (Terminals) in Kriminalämtern und PC-Arbeitsplätze in örtlichen Polizeibehörden sollten in einem Netz zusammengebracht werden und die bis dahin betriebenen Sondernetze für Datenübertragungen per Telefon, Fernschreiber und zwischen Großrechnern ersetzen. Zugleich ermöglichte es der PC, Daten vor Ort zu erfassen und hierfür auch jeweils eigene Verfahren zu entwickeln. In den Polizeibehörden machten sich Kriminalbeamt*innen daran, eigene Datenbanken und Anwendungen zu entwickeln.

---

1 Schraut, L.: PIOS-Dateien, Meldedienste und Spurendokumentationen – die wichtigsten Systeme, in: Bürgerrechte & Polizei/CILIP 41 (1/1992), S. 29-34

2 Schallbruch, M.; Mörs, S.: Neue Wege in der polizeilichen Datenverarbeitung – Dezentralisierung des Technikeinsatzes und Erschließung neuer Arbeitsgebiete, in: Bürgerrechte & Polizei/CILIP 41 (1/1992), S. 12-18

Damit entstand ein kreativer Wildwuchs. 1992 beschlossen die Arbeitsgremien der Innenministerkonferenz zu seiner Neuordnung das fachliche Grobkonzept für INPOL-Neu, das das alte INPOL ersetzen sollte. Erst 1998 begann der Realisierungsprozess, der aber an der ungenügenden Vorbereitung der Länder scheiterte. 2002 gab es einen bescheideneren Neubeginn, der nicht mehr die volle Integration aller Dienststellen in einen Rechnerverbund vorsah, sondern eine Weiterentwicklung des alten INPOL aus Großrechnern und Eingabeterminals war.

Der eigentliche Makel dieses Systems, nämlich der Wildwuchs aus inzwischen 27 im Verbund genutzten Anwendungen, die nur zum Teil anhand personenbezogener Merkmale durchsucht werden konnten, blieb erhalten.[3] Wie in den alten Tagen der polizeilichen Meldedienste mussten Daten weiterhin mehrfach eingegeben werden – in den zentralen Datenbanken (Personenfahndung, Fingerabdruckdatenbank AFIS etc.) und gegebenenfalls zusätzlich in den Meldediensten. Das eigentliche Ziel, alle Daten nur noch einmal erfassen zu müssen und danach für die verschiedenen Anwendungen freizugeben, konnte nicht erreicht werden. Dafür hätten sich Bund und Länder auf gemeinsame Standards, Schnittstellen oder sogar einheitliche Systeme zur Erfassung der Daten einigen müssen.

INPOL-Neu sollte ursprünglich aber nicht nur ein „Datenpool" sein, sondern darüber hinaus auch für strategische Auswertungen und Analysen geeignet sein: für Ein- und Ausgangsstatistiken der Kriminalstatistik, für Lagebilder, für operative Führungsaufgaben. 2003 wurde dann nur noch eine Schmalspurvariante des ursprünglichen Plans aufs Gleis gesetzt: Aus der Fahndungsdatenbank wurde INPOL-Z, ein allgemeines Fahndungs- und Auskunftssystem, das die Bedürfnisse der einfachen Einsatzbeamt*innen befriedigte. Die PIOS-Verfahren (und weitere fachspezifische Anwendungen) und Falldateien wurden durch INPOL-Fall ersetzt, in erster Linie für die Kriminalämter. Hier konnten in Freitextfeldern zusätzliche Informationen gespeichert werden – sowohl Text als auch multimediale Inhalte. Alle Objekte in den Dateien ließen sich beliebig verknüpfen, für die Fallanalyse eine zentrale Fähigkeit. Immerhin konnten alle INPOL-Falldateien nun zugleich durchsucht werden, wobei den Sachbearbeiter*innen nur die Treffer angezeigt werden, für die sie

3 Busch, H.: INPOL-Neu – Informatisierung des polizeilichen Alltags, in: Bürgerrechte & Polizei/CILIP 76 (3/2003), S. 12-19

die Berechtigung haben (je nach fachlicher Zuständigkeit). Damit wurde auch dem alten hierarchischen Polizeikonzept Genüge getan, dass Informationen von unten nach oben zu liefern sind, aber vor allem die unteren Ränge nur jene Dinge erfahren, die für ihre Aufgabenerledigung notwendig sind. Derzeit betreibt das BKA 38 Verbunddateien, die zum größten Teil im INPOL-Verbund geführt werden, sowie 129 Zentraldateien. Hinzu kommen an die 400 Strafverfolgungsdateien zu einzelnen Fällen, die sog. Amtsdateien.[4]

PIAV – Aufbruch zu alten Ufern

Am Ziel, polizeilich erfasste Daten so vorzuhalten und aufbereiten zu können, dass sie sowohl den Recherchebedürfnissen im einzelnen Fall als auch einer strategischen Aufbereitung genügen – also dem Erkennen neuer krimineller „Trends" und der Ausrichtung darauf –, haben Politik und Polizeiführung festgehalten. 2006, drei Jahre nach Einführung von INPOL-Neu, beschloss die IMK deshalb den Aufbau des „Polizeilichen Informations- und Analyseverbunds" (PIAV). Im PIAV werden keine Datenbanken geschaffen, so wie in INPOL-Fall. Vielmehr können die ohnehin vorhandenen Daten in den Informationssystemen der Landeskriminalämter wie über eine Web-Oberfläche von allen durchsucht werden. Dafür müssen entsprechende Schnittstellen programmiert werden.

Als Lehre aus dem INPOL-Desaster beschloss man gleich einen stufenweisen Ausbau: zunächst „PIAV-operativ" mit Anwendungen für einzelne Deliktsbereiche und am Ende „PIAV-strategisch". Als Startpunkt entschied man sich für den Bereich Waffen- und Sprengstoffkriminalität. Die alte INPOL-Falldatei „Waffen- und Sprengstoffkriminalität" (WSK) mit dem alten Meldedienst wurde nun ersetzt.

Bis zur endgültigen Aufnahme des Wirkbetriebs des neuen PIAV-Moduls Mitte 2016 (!!) hatten die zuständigen Sachbearbeiter*innen eine E-Post (eine Art dienstliche E-Mail) an alle zuständigen Dienststellen zu richten, wenn bspw. eine Kalaschnikow irgendwo angeboten wurde. Das führte nur selten zu Trefferfällen, die auch nicht immer aktiv zurückgemeldet wurden (weil die Sachbearbeiter*innen mit eigenen Fällen ausgelastet waren). Nun können über den Anbieter der Waffe, über die Seriennummer, Herstellungsdatum oder Chargennummer

4 Stand der Umsetzung des Programms „Polizei 2020", Antwort auf die Kleine Anfrage der Fraktion DIE LINKE, BT-Drs. 19/15346 v. 21.11.2019

Suchabfragen im PIAV gestellt werden: Ist der Händler bekannt? Gibt es ähnliche Seriennummern? Gab es an definierten Orten oder Zeiten schon ähnliche Angebote? Das ersetzt nicht die Recherchearbeit der Sachbearbeiter*innen zu jedem einzelnen „Treffer“, erleichtert aber das Generieren neuer Ermittlungsansätze. Mittlerweile wurde das Modul WSK um „Gemeingefährliche Straftaten und Rauschgiftkriminalität“ erweitert, weitere Bereiche sollen folgen.

Neues Etikett: „Polizei 2020“

INPOL-Neu konnte das Problem der technischen Inkompatibilität der polizeilichen Datentöpfe nicht lösen, und auch PIAV stellte hierfür offenbar keinen überzeugenden Ersatz dar. 2016 wurde deshalb ein weiteres Projekt gestartet, das „einheitliche Fallbearbeitungssystem“ eFBS. Es folgt der Einsicht, dass ein gemeinsames polizeiliches Informationssystem nur dann effektiv ist, wenn die „Quellsysteme“ in allen Polizeibehörden einheitlich funktionieren.

Fallbearbeitungssysteme werden vor allem von der Kriminalpolizei genutzt, um in komplexen Ermittlungsverfahren Daten eingeben und durchsuchbar halten, Verknüpfungen zwischen Personen und Objekten erkennen und Ermittlungsmaßnahmen nachhalten zu können. Daher kommen hier in einem System nicht nur eine Datenbank, sondern noch weitere Anwendungen zum Einsatz, die aber alle über eine gemeinsame Benutzeroberfläche bedient werden können.

Da nicht jede*r Beamt*in in jede Ermittlung schauen darf – sowohl aus datenschutzrechtlichen Gründen als auch zum Schutz von (insbesondere verdeckten) Ermittlungen – wird die dahinterliegende Datenbank in mehrere „Töpfe“ geteilt. Aber nur, wenn alle angeschlossenen Fallbearbeitungssysteme nach demselben Informationsmodell funktionieren, also die Informationen in identischer Weise Daten- und Objektkategorien zuweisen, ist die Übermittlung in ein zentrales System möglich, in dem dann die Objekte (Namen, Fahrzeuge, Tatwaffen, Fingerabdrücke etc.) übergreifend abgefragt und verknüpft werden können, um neue Tatkomplexe zu bearbeiten. Bei der Programmierung neuer Anwendungen im Polizeiverbund ist daher nun auch ein „Informationsmodell Polizei“ (IMP) zu beachten. Allerdings ist Baden-Württemberg

bisher das einzige Bundesland, das es geschafft hat, ein auf dem IMP basierendes Asservatenmanagementsystem überhaupt *auszuschreiben*.[5]

Ebenfalls 2016 wurde eine Modernisierung von INPOL-Neu auf den Weg gebracht. Das alles kostet viel Geld. Bei der Legitimation dieser Ausgaben kamen den Innenministern einige rechtliche Neuerungen zupass, die dringend in der gesetzlichen Grundlage für die polizeiliche Datenverarbeitung umgesetzt werden mussten. Das war zum einen das Urteil des Bundesverfassungsgerichts zum BKA-Gesetz und damit zu den Anforderungen an die polizeiliche Datenverarbeitung,[6] und zum anderen das Inkrafttreten der Datenschutzrichtlinie der EU,[7] die ebenfalls Vorgaben zur polizeilichen Datenverarbeitung und zum Informationsaustausch macht.

Der weitere Aufbau von PIAV, die Einführung eines eFBS, die Modernisierung von INPOL-Neu wurden Ende 2016 unter dem Oberbegriff „Polizei 2020" präsentiert und 2017 erstmals im Haushalt des Bundesinnenministeriums untersetzt. Insgesamt plant der Bund für die Umsetzung des Programms 254 Millionen Euro, wie dem Gesetzentwurf zur Novellierung des BKA-Gesetzes 2017 zu entnehmen war. Hinzu kommen die Kosten bei Bundespolizei und Zollkriminalamt sowie in den Landespolizeien. Insgesamt ist die Rede von 500 Millionen Euro Gesamtkosten, die durch den Bund und die Länder im Rahmen eines „Police-IT-Fonds" erbracht werden sollen. Im „white paper Polizei 2020" wird außerdem die Einführung eines einheitlichen Vorgangsbearbeitungssystems eVBS als Ziel genannt.[8]

Zu tun gibt es einiges. Einige Länder sehen gar nicht ein, dass sie ihre zum Teil selbst entwickelten, zum Teil zumindest nach ihren fachlichen Vorgaben angepassten Fall- und Vorgangsbearbeitungssysteme zugunsten eines eFBS bzw. eines eVBS aufgeben sollen.

Beim 2018 in BKA und Bundespolizei eingeführten eFBS handelt es sich um eine Variante des Produkts b-case der Firma Rola security solu-

5 White paper „Polizei 2020" v. 18.1.2018, S. 27 (www.bmi.bund.de/SharedDocs/ downloads/ DE/ veroeffentlichungen/2018/polizei-2020-white-paper.pdf)

6 Bundesverfassungsgericht: Urteil v. 20.4.2016, Az.: 1 BvR 966/09 (www.bverfg.de)

7 Richtlinie (EU) 2016/680 v. 27.4.2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr

8 White paper a.a.O. (Fn. 5)

tions, einer Telekom-Tochter. Auch in zwei Dritteln der Länder ist eine Variante dieses Fallbearbeitungssystems etabliert, RSCase. Diese könnten auf das neue Produkt wechseln; wann und ob sie das tun, ist noch unklar. Notwendig wäre es, denn gleicher Anbieter und gleiches Programm bedeuten nicht, dass diese Systeme untereinander Informationen austauschen können. Bei länderübergreifenden Lagen und Ermittlungen geschieht dies vereinzelt weiter „händisch".[9] Hamburg, Hessen, Baden-Württemberg und Brandenburg nutzten lange Zeit eine Eigenentwicklung für die Fallbearbeitung, CRIME (Criminal Research Investigation Management Software), sind aber im Februar 2019 ebenfalls bereits auf das eFBS gewechselt.[10]

So lange unterschiedliche FBS genutzt werden, müssen jeweils eigene Anwendungen für die Anbindung an PIAV programmiert werden – nur so können aus dem FBS heraus Informationen direkt in PIAV abgefragt und umgekehrt an PIAV ausgeliefert werden, ohne sie erneut eingeben zu müssen. Gerade für die Kriminalbeamt*innen, die früher bei jedem Vorgang entscheiden mussten, ob sie Daten und Erkenntnisse über die Kriminalpolizeilichen Meldedienste in die Verbunddateien des BKA anliefern und damit ein weiteres Mal eingeben müssen, wäre das sicherlich eine Erleichterung.

Für das Gelingen des Gesamtprojekts wird jedoch die Einführung eines eVBS als deutlich kritischer angesehen. „Ohne dessen Einbindung dürfte das angestrebte Ziel der Einmalerfassung der Daten nicht erreichbar sein", kommentierte der „Behördenspiegel".[11] Schließlich werden in den Vorgangsbearbeitungssystemen alle polizeilich relevanten Vorgänge erfasst, von der nächtlichen Ruhestörung über den aufgenommenen Verkehrsunfall bis hin zu angezeigten Kapitalverbrechen. Mit ihnen arbeiten also vornehmlich die uniformierten Polizist*innen der Schutz- und der Verkehrspolizei. Sie enthalten Massen von personenbezogenen Daten von Geschädigten, Verdächtigen, Zeugen oder auch gänzlich unbeteiligten Personen, die im Rahmen der Sachverhaltsaufklärung in Kontakt mit der Polizei gekommen sind. Durch die Fokussierung auf die Bedürfnisse der Dienststellen in der Fläche geriet bei zahlreichen Eigen-

9 Polizeiliche IT-Landschaft gleicht einem Flickenteppich", Meldung des Bundes Deutscher Kriminalbeamter (BDK) v. 30.3.2016 (www.bdk.de)

10 Diese und viele weitere nützliche Informationen sind unter dem „Glossar" auf der Seite police-it.org zu finden

11 Der lange Weg zum gemeinsamen Datenhaus, Behördenspiegel v. 8.1.2020

entwicklungen in diesem Bereich aus dem Blick, dass die dort erhobenen Daten gegebenenfalls einmal außerhalb des eigenen Bundeslandes zur Verfügung stehen müssen.

Datenschutz im Nexus

Der Umgang mit Daten gerät bei der Polizei nicht nur durch Einzelfälle wie „Helene Fischer“ ins Zwielicht. Auch Prüfungen durch Datenschutzbeauftragte fördern regelmäßig einen rechtswidrigen Umgang mit Daten zutage. Die Rationalität des polizeilichen Umgangs mit einmal erhobenen Daten folgt dem Messie-Prinzip: „Man weiß ja nicht, wofür man es noch mal braucht“. Unter diesem Motto kann bereits eine Personalienfeststellung im Rahmen einer polizeilichen Maßnahme gegen andere Personen ausreichen, um weiter gespeichert zu werden. So stellte der bayerische Datenschutzbeauftragte bei einer Prüfung des Kriminalaktennachweises der Landespolizei, einem Vorgangsbearbeitungssystem, tausende unberechtigte Speicherungen fest.[12] Von 54.543 durch das Zollkriminalamt in der „Falldatei Rauschgift“ gespeicherten Personendatensätzen mussten nach einer gemeinsamen Prüfung durch die Datenschutzbeauftragten des Bundes und der Länder 43.452 gelöscht werden.[13] Im Bereich der erkennungsdienstlichen Daten beim BKA mussten 2,1 Millionen Datensätze gelöscht werden, die das BKA entweder ungeprüft in seinen eigenen Datenbestand übernommen hatte oder für die keine fristgerechte Prüfung vorgenommen wurde, ob die Daten tatsächlich noch benötigt wurden.[14] Und wie viele selbst erstellte excel-, access- oder word-Dateien auf Polizei-PC schlummern, in denen Beamt*innen wegen der fehlenden Interoperabilität der Datenbanken selbst Daten zusammengeführt haben, kann nur spekuliert werden. Häufige Beanstandungen von Datenschutzbeauftragten beziehen sich außerdem darauf, dass die Speichervoraussetzungen in den Errichtungsanordnungen nicht erfüllt sind oder dazu jedenfalls kein Aktenrückhalt vorliegt.

Die Errichtung der Zentral- und Verbunddateien beim Bundeskriminalamt setzte bislang zwingend immer eine solche Errichtungsanord-

12 Schulzki-Haddouti, C.: Außer Kontrolle. Fragwürdiger Datenschutz in Polizeisystemen, in: c´t 2016, H. 13, S. 154-157 (auch auf heise online)

13 Bundesbeauftragter für den Datenschutz und die Informationsfreiheit: 27. Tätigkeitsbericht für 2017 und 2018, BT-Drs. 19/9800 v. 8.5.2019, S. 78

14 ebd.

nung voraus. Darin sind detailliert Zweck der Datei, Speicheranlässe und zu speichernde Daten definiert. Diese Errichtungsanordnungen sind zentraler Maßstab für die Prüfungen durch die Datenschutzaufsicht. Mit dem 2018 in Kraft getretenen neuen Bundeskriminalamtsgesetz wurden diese Errichtungsanordnungen aber abgeschafft. Denn alle polizeilichen Daten sollen ja nun in einem einzigen Informationssystem gespeichert werden. Die Einhaltung datenschutzrechtlicher Standards – in erster Linie der Erforderlichkeit und Zweckbindung – sollen zukünftig vor allem technisch sichergestellt werden. Unter der Überschrift „Stärkung des Datenschutzes durch Technik" ist im white paper Polizei 2020 die Rede von „dynamischen und zielgerichteten Berechtigungskonzepten", die weitaus „differenzierter und zielgerichteter" seien als aktuelle Regelungen. Ein „zielgerichteter und passgenauer Datenschutz" (sprich: auf keinen Fall mehr als nötig) soll durch ein „modernes, differenziertes und dynamisches Zugriffsmanagement" gesichert werden.[15] Bei der Vorstellung des Programms sprach der Präsident des BKA immer wieder von einem „Rechte- und Rollenkonzept", mit dem zukünftig die Vorgaben des Bundesverfassungsgerichts gewahrt werden sollen. Das heißt, dass weiterhin nicht alle Polizist*innen auf alle Daten Zugriff haben, sondern einerseits nur auf diejenigen, die zu ihrer Aufgabenerfüllung erforderlich sind, also die Drogenfahnderin nur auf die Daten mit Bezug zur Rauschgiftkriminalität. Andererseits muss das Konzept der „hypothetischen Datenneuerhebung" umgesetzt werden, nach dem Informationen aus einer eingriffsintensiven Maßnahme (etwa einer Telefonüberwachung bei gewerbsmäßigem Drogenhandel) nur dann in einer anderen Ermittlung oder einem Gefahrenabwehrvorgang – also zu einem anderen Zweck – verwendet werden dürfen, wenn dabei erneut dieselbe Maßnahme durchgeführt werden dürfte (etwa eine Mordermittlung ohne Zusammenhang zur anderen Tat). Dieses Prinzip setzt zwingend eine entsprechende Kennzeichnung der Daten im Informationssystem voraus – also Angaben zum Erhebungszweck, zur Herkunft der Information, auch zu Aussonderungsprüffristen.

Ein zentrales Problem entsteht nun durch den Nexus, den Übergang vom alten Datenhaltungsregime zum neuen: schon technisch, denn alle Daten müssen zunächst dem Informationsmodell Polizei entsprechen, sonst können sie nicht migriert werden. Praktisch müssen bei der Migra-

15 White paper a.a.O. (Fn. 5), S. 10

tion alle personenbezogenen Daten daraufhin geprüft werden, ob sie tatsächlich weiter erforderlich sind. Auch dabei müssen alle speichernden Stellen mitmachen, denn die Daten stehen dann ja dem gesamten Verbund zur Verfügung. Zunächst einmal bleiben jedoch alle Zentral- und Verbunddateien sowie die BKA-eigenen Falldateien so bestehen, wie sie sind – dafür hat sich das BKA eine unbefristete Übergangsregelung in das neue BKA-Gesetz schreiben lassen. Und wie dann das neue Informationssystem beschaffen sein und wie das Rechte- und Rollenkonzept darin umgesetzt werden soll, dazu gibt es noch nicht einmal ein technisches Konzept. Der Bundesdatenschutzbeauftragte stellte für 2018 fest, „dass weder BMI noch BKA mir bislang detaillierte und aussagekräftige Unterlagen für die geplante neue IT-Struktur der deutschen Polizei vorgelegt haben."[16] An diesem Befund hat sich bis Anfang 2020 nichts geändert.

Von einem einheitlichen Datenhaus, in das alle Polizeibehörden in Deutschland auf dem gleichen Weg ihre Daten zuliefern und in dem alles für alle auch tatsächlich verfügbar ist, ist der aktuelle Zustand also noch weit entfernt. „Kommissar Computer" bleibt weiterhin science fiction aus den 70ern. Es mag einerseits possierlich sein, dass sich die hochtrabenden Pläne und Ankündigungen so deutlich in der Wirklichkeit blamieren. In dem dadurch weiterwachsenden Wildwuchs von Informationssystemen kommen aber vor allem die Rechte derjenigen unter die Räder, deren Daten dort gespeichert sind.

16 Bundesbeauftragter a.a.O. (Fn. 13), S. 70

Einsatzmittel Smartphone

Nutzung von Mobiltelefonen im polizeilichen Arbeitsalltag

von Stephanie Schmidt

Die Ausstattung der deutschen Polizeien mit Smartphones ist Teil des Projekts „Polizei 2020“ und soll den Arbeitsalltag der Beamt*innen erleichtern. Als soziales Objekt legt das Smartphone aber Kommunikations- und Handlungspraktiken nahe, die abseits dienstlicher Aufgaben liegen.

Unter dem Projekt „Polizei 2020“ wollen die Innenminister*innen von Bund und Ländern nicht nur das Informationswesen der Polizeien des Bundes und der Länder vereinheitlichen, sondern auch explizit (digitale) Technik zum Ausbau des Informationsmanagements in der Polizei entwickeln und/oder erweitern. Konkret sieht das Programm vor, die Polizei mit PCs, Tablets und Smartphones auszustatten.

Anfang 2020 wurde beispielsweise die Polizei in Nordrhein-Westfalen mit insgesamt 20.000 Smartphones (konkret mit dem IPhone 8) ausgerüstet. Auf diesen befinden sich Programme, die das polizeiliche Arbeiten aus Sicht des Innenministeriums verbessern und erleichtern sollen, wie ein speziell für die Polizei entwickelter Messenger sowie Apps, die den direkten Zugriff auf polizeilich erfasste Daten, Ausweis- und KfZ-Daten ermöglichen, entsprechende Informationen vor Ort auslesen und diese dann mit den gespeicherten Informationen abgleichen können. Auch die Warnapp NINA (Notfall-Informations- und Nachrichten-App des Bundesamts für Bevölkerungsschutz und Katastrophenhilfe) und Programme für den Zugriff auf die dienstlichen Emails sind auf den Telefonen installiert.[1] NRW ist jedoch nicht das einzige Bundesland, das dienstliche Smartphones in den Arbeitsalltag der Beamt*innen eingeführt hat. Auch Rheinland-Pfalz will seine Beamt*innen bis 2021 mit

1 NRW: 20.000 iPhones sollen Polizisten besser vernetzen, heise online v. 7.6.2019

Smartphones samt dem selbst entwickelten Messenger „poMMes“ (polizeilicher Multimedia-Messenger) ausrüsten.[2] Niedersachsen und Hessen arbeiten bereits mit dem Messenger Stashcat, der mit dem in der Polizei bereits bekannten Funkgeräte-Hersteller Hytera und dem Anbieter für Kommunikationsplattformen Frequentis zusammenarbeitet.[3]

Die Einführung von Smartphones zur dienstlichen Nutzung im Arbeitsalltag lehnt sich eng an verbreitete Gewohnheiten im Umgang mit Technik an. Es liegt nahe, ein Objekt wie das Smartphone, das für die meisten Beamt*innen ein Alltagsbegleiter ist, zu einem beruflich nutzbaren Gegenstand zu machen, der auch noch Arbeitserleichterung verspricht. Die Möglichkeiten erscheinen nahezu endlos: Nachschlagewerke, wie die App kapoPEDIA der Kantonspolizei St. Gallen, versprechen schnell abrufbares Wissen über polizeiliche Maßnahmen und rechtliches Hintergrundwissen, das besonders für Beamt*innen in den ersten Ausbildungsjahren attraktiv sein soll. Eingebaute Ortungssysteme informieren während einer polizeilichen Maßnahme die Dienststelle über den Aufenthaltsort ihrer Beamt*innen, ohne dass dies direkt mit den Mitarbeiter*innen rückgekoppelt wird, und implementierte Fingerabdruckscanner sollen die vor-Ort-Identitätsfeststellung von Personen erleichtern. Kurz: Das Smartphone soll zum taktischen Begleiter im polizeilichen Alltag werden und dabei Arbeitszeit und -aufwand reduzieren.

Daher reagierte das österreichische Innenministerium im Sommer 2019 mit großem Unverständnis auf den Befund, dass trotz dieser goldenen Versprechen ein großer Teil der Beamt*innen die angeschafften Smartphones und Tablets nicht benutzt.[4] Der Grund: die Polizist*innen haben Bedenken, weil sie sich durch die Dienstsmartphones überwacht fühlen. Allein die Möglichkeit, jederzeit den Aufenthaltsort zu bestimmen, erhöht die Kontrolle auf die Polizist*innen. Dass Polizist*innen ein Gerät zur Verfügung gestellt wird, heißt also noch lange nicht, dass es auch genutzt wird – und noch viel weniger ist darüber ausgesagt, wie es genutzt wird.

Medien erfüllen keinen Zweck an sich, sondern sind stets eingebunden in soziale und kulturelle Kontexte, Machtverhältnisse und normative

2 vgl. dpa: Smartphones und eigener Messenger bei der Polizei – positives Zwischenfazit, heise online v. 25.5.2019

3 BOS-Funk: Messenger Stashcat kooperiert mit Hytera und Frequentis, heise online v. 25.11.2019

4 Polizisten verweigern neue IPhones, ORF online v. 3.7.2019

Rahmungen. Dinge können daher nur innerhalb ihrer sozialen und kulturellen Einbindung und der daraus resultierenden Nutzungspraktiken und Umgangsweisen verstanden werden.[5] Im Folgenden soll also weder der Großartigkeit der Technik gehuldigt, noch ein Technikdeterminismus beschworen werden. Vielmehr geht es darum nachzuzeichnen, in welcher Weise Smartphones im Alltag der Beamt*innen bestimmte Handlungs- und Kommunikationsmuster ermöglichen oder befördern, während sie andere ver- oder behindern.[6] Oder kurz: Was machen Polizist*innen mit dem Smartphone und was macht das Smartphone mit den Polizist*innen?

Das Smartphone als Begleiter im Arbeitsalltag

Das Handy selbst ist wie selbstverständlich bereits seit Jahren Teil der polizeilichen Arbeitswelt. Zunächst wurde es nicht als Diensthandy, sondern als Ermittlungsgegenstand in der polizeilichen Praxis relevant: Besonders im kriminalpolizeilichen Bereich ist das Handy ein begehrtes Objekt, das Zugang zu der Sozial- und Kommunikationswelt der Besitzer*innen bieten kann und damit nicht selten im Zentrum polizeilicher Ermittlungen steht. Allein 2019 hat die Polizei Berlin 336.569 sogenannte „Stille SMS" versandt, um Standort oder Bewegungsprofile von Betroffenen zu erhalten und entsprechende Maßnahmen, z. B. Festnahmen, treffen zu können.[7] Auch das Abhören von Gesprächen oder das Mitschneiden von Messenger-Unterhaltungen sind polizeiliche Maßnahmen, die (fremde) Handys als Zielobjekte für Ermittlungen ausweisen.

Doch auch abseits kriminalpolizeilicher Ermittlungen sind Handys, und insbesondere Smartphones, Teil des polizeilichen Alltags. Peter Ullrich und Philipp Knopp haben analysiert, dass Smartphones auch im Rahmen von Großveranstaltungen und Protesten quantitativ und qualitativ an Relevanz gewinnen und „heute bei politischen Protesten allgegenwärtig" sind; auch weil sie Demonstrierende „zumindest partiell in die Lage (versetzen), eine ‚neue Sichtbarkeit' polizeilicher Handlungen

5 vgl. Bareither, C.: Medien der Alltäglichkeit, in: Zeitschrift für Volkskunde 2019, H. 1, S. 3-26

6 vgl. Hahn, H.P.: Die geringen Dinge des Alltags. Kritische Anmerkungen zu einigen aktuellen Trends der material culture studies, in: Braun, K.; Dieterich, C.-M.; Treiber, A.: (Hg.): Materialisierungen von Kultur. Diskurse, Dinge, Praktiken, Würzburg 2015, S. 30

7 vgl. Heimliche Ortungsimpulse. Viele „Stille SMS" bei Bund und Ländern, Netzpolitik.org v. 10.2.2020

zu erzeugen“.[8] Dabei meint Sichtbarkeit nicht in erster Linie das tatsächliche Abbild des Ereignisses, das auf Video festgehalten wird, sondern vielmehr die mögliche mediale und soziale Verbreitung des Videos, die Debatten um das polizeiliche Handeln erst ermöglicht. Gerade diese Sichtbarkeit führt dazu, dass Beamt*innen eher abwehrend auf das Filmen ihrer Einsätze reagieren und nicht selten gegen die Filmenden vorgehen.

Es sind die technischen Möglichkeiten des Geräts, die in diesem Kontext relevant werden und neue Handlungsräume eröffnen: Im Smartphone sind sowohl Videokamera und Fotoapparat als auch Audioaufnahmegerät enthalten. Das Aufgenommene kann daraufhin sofort versendet und in Chatgruppen oder sozialen Netzwerken geteilt werden. Es ist diese dem Smartphone innewohnende Möglichkeit zur Sozialität, die das ‚fremde‘ Gerät für die Beamt*innen als Ermittlungsobjekt interessant und – wenn die Kontrolle darüber nicht möglich ist oder es gar „gegen“ die Beamt*innen verkehrt wird – zugleich unheimlich werden lässt.

Als Diensthandys ergänzen Mobiltelefone den Funk auch als Arbeitsmittel – nicht nur dann, wenn der Funk aus technischen Gründen nicht funktioniert, sondern vielmehr aus praktischen Notwendigkeiten heraus. So kann es gerade in Großstädten mit einem ausgebauten Straßen-, S- und U-Bahnnetz vorkommen, dass die örtliche Streifenpolizei während eines Einsatzes, z. B. bei der Suche nach einer suizidalen Person, auch mit der Bundespolizei, die in Deutschland für den Bahn- und Schienenverkehr verantwortlich ist, zusammenarbeitet, mit welcher sie sich jedoch keinen gemeinsamen Funkkanal teilt. Zur Verständigung während der Suche, die über einen größeren Distanzbereich erfolgt, wird dann häufig das Handy eingesetzt, um einen ständigen Kontakt zu den Kolleg*innen zu halten. Wenngleich sowohl über Funk als auch über das Mobiltelefon Informationen ausgetauscht werden können, unterscheidet sich die Kommunikation beider Geräte voneinander. Weil Funkgespräche grundsätzlich von allen in der Funkgruppe mitgehört werden (können), werden Absprachen über das weitere praktische Vorgehen, sensible Informationen oder rechtliche Rückversicherungen im Regelfall über das Handy mit der Dienststelle kommuniziert. Damit wird einerseits ein

8 Knopp, P.; Ullrich, P.: Kampf um die Bilder. Videoüberwachung und Gegenüberwachung von Demonstrationen in Österreich (Langfassung), 2016, S. 5, (online auf: www.juridikum.at/fileadmin/user_upload/artikel/knopp-ullrich_langfassung.pdf)

ständiges ‚Grundrauschen' auf dem Funkkanal reduziert und der Funk nicht blockiert und andererseits die Vertraulichkeit der kommunizierten Informationen gewährleistet. Während beim Funk also potenziell auch die Vorgesetzten und Kolleg*innen zuhören, kann Kommunikation mit dem Handy sehr viel gezielter stattfinden. In der direkten Ansprache ist ein informelleres Gespräch und damit auch der Austausch über diffizile und möglicherweise problematische Themen möglich. Dinge werden aber nicht nur anders sagbar, weil der Nutzer*innenkreis als überschaubar eingeschätzt wird, sondern auch weil der Funk, aufgrund seiner Struktur und seiner Funktionsweise, spezifische Umgangsweisen ermöglicht und andere begrenzt. Diese den Medien eingeschriebenen Praxisaufforderungen und -beschränkungen bezeichnet der Psychologe James Gibson als „affordances" (dt. Affordanzen).[9] Der Funk affordiert also einen spezifischen Umgang und auch eine spezifische Sprechweise. Er ist pragmatisch und gerade in Stresssituationen von kurzen und eindeutigen Aussagen geprägt, die notwendig sind, um Arbeitsanweisungen oder handlungsleitende Informationen an die Beamt*innen vor Ort zu vermitteln. Dies funktioniert auch deshalb, weil der Funk ein reines Arbeitsmittel ist und im privaten Bereich kaum eine Rolle spielt. Seine Funktion ist also im Wesentlichen auf den (arbeitsrelevanten) Informationsaustausch beschränkt. Im Unterschied dazu ist das Mobiltelefon und besonders das Smartphone ein Gegenstand, der Polizist*innen auch in ihrem privaten Alltag begleitet und damit Praktiken jenseits der Organisation der Polizei affordiert. Zentraler als das Telefonieren sind dabei die zahlreichen Messenger- oder Social-Media-Apps, die die Kommunikation und das Teilen von Inhalten mit (vielen) anderen (gleichzeitig) ermöglichen. Vor allem auch, weil die Gruppenfunktion von Messengerdiensten einen vergemeinschaftenden Austausch über erlebte Einsätze oder Kuriositäten aus dem Dienstalltag ermöglicht und so auch verbindende Narrative und statusrelevante Heldenerzählungen konstituiert.[10] Dazu kommt, dass die polizeiliche Mediennutzung starken Regeln

9 vgl. Gibson, J.: The Ecological Approach to Visual Perception. Hillsdale; New Jersey 1986, siehe auch Bareither a.a.O. (Fn. 5)

10 Immer wieder werden in diesen (unverschlüsselten) Gruppen auch sensible Daten über Verdächtige, Fotos aus Einsätzen und Auszüge aus Akten untereinander geteilt. In ihnen werden außerdem politische Meinungen ausgetauscht, wie z. B. bei internen WhatsApp Gruppen der Polizei, in denen rechtsextremistische und rassistische Nachrichten ver-

unterliegt und so z. B. auf den Dienstcomputern kein vollständiger Internetzugriff möglich ist. Dieser Umstand und die vergemeinschaftende Funktion des Smartphones führen dazu, dass die Polizist*innen das private, eigene Smartphone parallel zu dem Diensthandy nutzen – auch um der möglichen Überwachung durch Vorgesetzte vorzubeugen.

Das Smartphone ist ein Objekt, das nahelegt, Alltägliches in sich aufzunehmen und anderen zur Verfügung zu stellen: Die Aufnahme eines Fotos bedarf nur weniger Klicks und ist in Kürze auf Instagram hochgeladen, auf Twitter oder in WhatsApp-Gruppen geteilt. Diese dem Objekt inneliegende Möglichkeit der Sozialität ist auch für die Beamt*innen in ihrem Alltag zentral. Langeweile im Dienst wird mit der Kommunikation mit Freunden, dem Spielen von kleineren Games, dem Surfen im Internet oder dem Scrollen auf Facebook überbrückt. Besonders bei einsatzarmen Nachtdiensten hilft die Interaktion mit dem Smartphone den Beamt*innen, wach und aktiv zu bleiben.[11] Diese Medienpraktiken sind nicht nur Interaktion mit der Technik selbst, sondern „integraler Bestandteil der soziokulturellen Prozesse, die wir Alltag nennen".[12] Die technologischen Rahmenbedingungen dienen so zwar der Eröffnung neuer Handlungsräume, ihre Wirkmächtigkeit jedoch entfalten sie erst in den Umgangsweisen selbst. Damit entwickeln sie auch eine über ihren intendierten Sinn hinausgehende Wirkmacht in der Alltagspraxis.

Die Digitalisierung des Ereignisses

Eine spezifische und bislang weitestgehend undiskutierte Rolle kommt den (privaten) Smartphones der Beamt*innen auch während des Einsatzes bei Großereignissen wie Fußballspielen oder Demonstrationen zu. Während der polizeitaktische Einsatz von Twitter besonders hinsichtlich seiner Bedeutung für die Deutungshoheit über Geschehnisse bereits gut analysiert wurde,[13] spielt auch der veralltäglichte Gebrauch von Smart-

schickt wurden. Siehe: Hessische Polizeianwärter unter Extremismusverdacht, FAZ online v. 7.9.2019

11 Die hier aufgezählten Beobachtungen entstammen meiner ethnografischen Feldforschung bei der Polizei, die ich im Rahmen meiner Dissertation durchgeführt habe.

12 Bareither a.a.O. (Fn. 5), S. 6

13 Für den G20 wurde das von dem Forschungsteam im Projekt „Mapping #NoG20" ausführlich getan. Vgl. Eskalation. Dynamiken der Gewalt im Kontext der G20-Proteste in Hamburg 2017, Forschungsbericht, Berlin; Hamburg: Institut für Protest- und Bewe-

phones für die Informationsgewinnung über Ereignisse bei den Polizist*innen selbst eine zentrale Rolle. Während der Ereignisse um den G20-Gipfel 2017 in Hamburg informierten sich die eingesetzten Beamt*innen per Smartphone über gleichzeitig stattfindende Geschehnisse an anderen Orten. Hierbei nutzten sie das Handy, um die unklaren und über Funk nur bruchstückhaften Informationen über die Situation ihrer Kolleg*innen zu ergänzen:

> „Es war noch so ein bisschen surreal, weil du hast das nicht miterlebt. Ja okay, man sagt dir was über Funk, gibt Informationen ab, aber du hast die Bilder nicht. Aber das haben wir auch noch während des Einsatzes miterlebt über Facebook. Da gingen ja auch schon die ersten Videos rum … Und wirklich jeden Tag, egal jetzt ob Mittwoch, wo noch nicht so viel los war – Montag und Dienstag ja auch. Oder dann Donnerstag, Freitag – wenn wir dann mal die Zeit hatten, um uns aufs Auto zu setzen, gings eigentlich nur permanent: Facebook, Facebook, Facebook! Was gibt's Neues? Gibt's schon wieder irgendwelche Berichte von verletzten Kollegen?“[14]

Auch in den WhatsApp-Gruppen mit Kolleg*innen wurden Bilder und Geschichten über verletzte Beamt*innen und die gewalttätigen Auseinandersetzungen geteilt. Das Smartphone bietet einen erweiterten Zugang zum Einsatzgeschehen – und zwar über die Grenzen des konkreten Raums hinweg. Unterstützt von den sensorischen Reizen, die durch Vibration und/oder Signalton bei Nachrichten vom Smartphone ausgehen, haben die Beamt*innen damit den Eindruck die Ereignisse buchstäblich ‚hautnah' und in Echtzeit mitzubekommen. Es bietet so also nicht nur die Möglichkeit, Erlebtes weiterzugeben, sondern auch die Geschichten der anderen scheinbar mitzuerleben.

Dieses digitale Storytelling gibt dabei vor, Wahrheiten zu produzieren: Weil die Informationen vorwiegend von der eigenen peer group kommen, wird ihnen ein erhöhter Wahrheitsgehalt zugestanden. Das Teilen von Angst-, Wut- oder auch Lust-Momenten führt dadurch zu einer sensorischen und emotionalen Verflechtung, die den Ereignisraum entgrenzt und ein Erleben eines fernen Geschehnisses durch das Medium des Smartphones ermöglicht. Für die Polizeibeamt*innen, die an

---

gungsforschung (ipb); Zentrum Technik und Gesellschaft TU Berlin (ZTG); Hamburger Institut für Sozialforschung (HIS), 2018 (https://g20.protestinstitut.eu/wp-content/uploads/2018/09/Eskalation_Hamburg2017.pdf)

14 Ausschnitt aus einem Interview mit einer*m Beamt*in über seinen*ihren Einsatz während des G20, 32003-INT, geführt von Stephanie Schmidt im Rahmen des Forschungsprojekts Mapping #NoG20

einem festgelegten Ort ausharren müssen, entsteht damit selbst im Zustand der Inaktivität eine (auch emotionale) Interaktivität.

Unter diesem Blickwinkel affordieren Smartphones nicht nur Kommunikationspraktiken zum Austausch von Informationen, sondern auch die Inszenierung und Kommunikation emotionaler Erfahrungen. Damit haben sie auch Einfluss auf die Emotionalität und Positioniertheit der nicht unmittelbar involvierten Beamt*innen: „Die Stimmung wurde immer gereizter … du hast es halt auch gehört … wie deine Kollegen in der Bredouille waren. Du konntest nicht helfen, du warst halt gefangen. Das hat uns alle wirklich massiv aufgeregt. Weil du willst ja deine Kollegen nicht sterben lassen, du willst ja helfen."[15] Die Erzählungen knüpfen hier an die im Vorfeld kommunizierte Gefahrenprognose der Polizei an und evozieren auch Veränderungen der Wahrnehmungs- und Handlungsschemata der einzelnen Beamt*innen. Die komplexen (und emotionalen) Diskurse, die in den sozialen Medien über das Geschehen geführt werden, wirken so auch auf die Deutungen und Interpretationen von lokalen Ereignissen zurück:

> „Auf einmal hör ich nur noch über Funk eine panische Stimme: ‚Helm auf! Helm auf! Da kommen Demonstranten auf euch zu.' Und wir haben schon gedacht: Verdammt, die wollen das Gebäude stürmen … Und dann sehen wir eine Meute von 20 bis 30 Leuten um die Ecke kommen. Und relativ abgeschlagen hinter der Gruppe Kollegen, und die haben die eingekesselt und einfach mal drauf. Drauf mit Schlagstock ohne Ende … Wo ich so gedacht hab, okay krass. Jetzt ist auf alle Fälle ein neues Stadium erreicht … Das hat auf alle Fälle rege Diskussionen angeregt. Also wir haben uns dann auch darüber unterhalten, ob wir das genauso gemacht hätten … wir waren uns einig, dass wir es im Grunde auch so gelöst hätten … Weil am Ende zählt auch unser eigenes Leben"[16]

Damit werden die über Smartphone und Funk kommunizierten Gefahrenszenarios auch in der Deutung von Situationen wirksam. Sie sind damit auch Affektgeneratoren,[17] die gruppeninterne Solidarisierungen und Feinbildkonstruktionen begünstigen und den Effekt selektiver Wahrnehmung stärken. Im Zuge dessen verschiebt sich auch die normative Rahmung von Handlungen, durch welche die Anwendung von

15 ebd.

16 ebd.

17 Reckwitz, A.: Praktiken und ihre Affekte, in: Schäfer, H. (Hg.): Praxistheorie: Ein soziologisches Forschungsprogramm, Bielefeld 2016, S. 163-180

(übermäßiger) Gewalt durch die Kolleg*innen nun als richtig und geboten erscheint.

Schlussbetrachtungen

Als privates Gerät ist das Smartphone bereits seit langem Teil der polizeilichen Arbeitswelt – als Objekt des Zeitvertreibs oder auch des sozialen Austauschs. Es ergänzt dabei den Funk als Kommunikationsmedium in spezifischer Weise. So ist es möglich, mit dem Smartphone auch informelles Wissen persönlich und schnell weiterzugeben, ohne der dienstlichen Kontrolle von Vorgesetzten zu unterliegen. Unabhängig von konkreten funktionalen Veränderungen im Arbeitsalltag der Beamt*innen, bildet das Smartphone auch eine Infrastruktur für Kommunikations- und Handlungsmuster, die digitales und analoges Handeln ineinander verschränkt. Es ermöglicht die Inszenierung und Kommunikation emotionaler Erlebnisse untereinander und kann damit in Einsatzsituationen zu einer raumübergreifenden Emotionalisierung beitragen.

Es ist also nicht nur ein technisches Gerät, das – als dienstliches Gerät – durch spezielle Apps und Messenger Einfluss auf den konkreten Arbeitsalltag und das Policing von polizeilichen Anlässen hat. Vielmehr ist es ein im Kern soziales Gerät, das auch einen Kommunikationsraum bildet und so Medienpraktiken affordiert, in denen sich Krisen- und Gefahrenszenarien diskursiv verdoppeln und auf das konkrete Handeln von Polizist*innen wirken.

„Datenschutz bleibt leere Hülle“

Die neuen polizeilichen Big Data-Anwendungen sind kaum mehr kontrollierbar

Interview mit dem Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit

Erfolglos versuchte Johannes Caspar, der Polizei nach dem G20-Gipfel die Speicherung zehntausender Gesichtsbilder zu verbieten. Matthias Monroy sprach mit ihm über die Rolle des Datenschutzes bei der Automatisierung von Informationssystemen, über Polizei in Sozialen Medien, Verschlüsselung und die EU-Zusammenarbeit.

Herr Caspar, was ist der Datenschutz noch wert, wenn die Polizei mir nichts, dir nichts Gesichter speichern und abgleichen darf?
Die biometrische Gesichtserkennung gibt es in zwei unterschiedlichen Varianten. Die Polizei kann den Fahndungsbestand in Echtzeit abgleichen und nach Personen im öffentlichen Raum suchen. Gibt es keinen Treffer, werden die Bilder gelöscht. Anders beim retrograden Einsatz der Gesichtserkennung: Hier geht es um die Ermittlung begangener Straftaten. Im Anschluss an den G20-Gipfel in Hamburg wurde eine Datenbank mit tausenden von Gesichtsprofilen erstellt, aus jedem im Video-bzw. Bildmaterial durch die Software identifiziertem Gesicht ein mathematisches Modell erzeugt. Dieser Datenbestand wurde gespeichert, um dann bis heute darüber immer wieder neue Suchläufe durchzuführen. Von diesen beiden Systemen wird meist die Echtzeiterkennung, wie sie am Berliner Bahnhof Südkreuz getestet wurde, kritisiert. Nicht weniger eingriffsintensiv ist aber mitunter das Modell wie bei uns in Hamburg, wo man über Jahre hinweg Daten von Personen, die friedlich demonstrierten oder einfach nur auf dem Weg zu ihrer Arbeit waren, vorhält und für Datenabgleiche nutzt.

Sie haben sich nach dem G20-Gipfel mit der Polizei angelegt und verloren. Das Verwaltungsgericht urteilte, dass Sie Ihre Anordnungsbefugnis zur Löschung einer Datei mit Gesichtsbildern nicht hätten nutzen dürfen.

Das Gericht verengt meine Befugnisse auf eine reine technisch-organisatorische Prüfung. Ich darf gegebenenfalls Auflagen erteilen; für die Überprüfung, ob sich für eine polizeiliche Maßnahme überhaupt eine Erlaubnis im Gesetz findet, bleibt nach Ansicht des Gerichts dann kein Raum. Vom Datenschutz bleibt dann nur eine leere Hülle. Eine Überprüfung polizeilicher Maßnahmen darauf, ob sie von hinreichenden Rechtsgrundlagen gedeckt ist, könnte unter Zugrundelegung dieser Ansicht wohl nur dann erfolgen, wenn der Bürger aktiv gegen die jeweilige Maßnahme klagt. Dies ist jedoch im Falle verdeckter Maßnahmen, wohl aber auch im Falle von „Videmo" problematisch. Wissen Sie, ob Sie möglicherweise in der von der Polizei angelegten Datenbank sind? Wenn das so stehen bleibt, können wir den Laden hier eigentlich dicht machen, jedenfalls was die Kontrolle von Strafverfolgungsbehörden anbelangt.

Das Verwaltungsgericht ist in seinem Urteil zu dem für mich unverständlichen Schluss gekommen, dass dieser Entscheidung keine grundsätzliche Bedeutung zukommt. Dies führt dazu, dass uns nicht automatisch die Möglichkeit der Berufung gegen das Urteil zusteht. Wir haben daher zunächst einen Antrag auf Zulassung der Berufung gestellt.

Der Senat hat auch das Hamburger Polizeigesetz entsprechend geändert …
In diesem Bereich besteht keine Anordnungsbefugnis mehr, sondern lediglich eine Feststellungsbefugnis. Das bedeutet, dass wir im Falle von Verstößen nach erfolgter Beanstandung selbst ein feststellendes Urteil vor Gericht erstreiten müssen. Die Hürden sind insoweit höher, als wir uns dann in der Klägersituation befinden.

Auch die Feststellungsbefugnis hätten Sie beinahe verloren …
Ja, das wäre fatal gewesen. Denn eine rechtlich verbindliche Abhilfebefugnis ist in der einschlägigen europäischen Richtlinie für den Bereich von Justiz und Inneres, der sogenannten JI-Richtlinie, vorgesehen. Die nach dieser Richtlinie zu erlassenden nationalen Regelungen dürfen dabei nicht unter das Niveau des EU-Rechts sinken. Nach Einschätzung der angehörten Sachverständigen im Gesetzgebungsverfahren reicht die Feststellungsklage für eine unionsrechtskonforme Umsetzung der europäischen Vorgaben nicht aus.

Wie wollen Sie in der Berufung argumentieren?
Wir werden deutlich machen, dass das Urteil wesentlichen rechtsdogmatischen Grundsätzen und verfassungs- und unionsrechtrechtlichen Prinzipien des Datenschutzrechts widerspricht. Darüber hinaus ist derzeit überaus fraglich, ob die beim Landeskriminalamt genutzte Software

„Videmo“ überhaupt ermöglicht, Zugriffe automatisiert zu protokollieren, und damit den Anforderungen für eine revisionssichere Datenhaltung gerecht wird.

In welchen Bundesländern gibt es eigentlich eine Anordnungsbefugnis und wo lediglich eine Feststellungsbefugnis? Gibt es Landesdatenschutzbeauftragte, deren schärfstes Schwert die Beanstandung ist?

Die in den Ländern bestehenden Regelungen sind zu differenziert, um einen umfassenden Überblick über die bestehende Rechtslage geben zu können. Die europäischen Vorgaben wurden in den Ländern teilweise noch nicht umgesetzt. Dort besteht folglich keine Anordnungsbefugnis und existieren auch keine vergleichbaren Regelungen. Andere Landesgesetze normieren ein zweistufiges Verfahren, nach dem jedenfalls nach erfolgter Beanstandung eine Anordnung erlassen werden kann. Teilweise können die Landesdatenschutzbeauftragten lediglich spezielle Untersagungen aussprechen oder sind auf eine Zustimmung des zuständigen Ministeriums angewiesen.

Der Bundesinnenminister hatte angekündigt, die biometrische Überwachung im Bundespolizeigesetz eindeutig zu regeln. In § 27 sind „selbsttätige Bildaufnahme- und Bildaufzeichnungsgeräte“ aber bereits erlaubt …

Dass der Staat nach besonderen gesetzlichen Vorgaben Videoüberwachung betreiben darf, heißt noch lange nicht, dass er die biometrischen Merkmale von Gesichtern berechnen darf. Dafür fehlt eine Rechtsgrundlage. Das wird wohl auch vom Bundesinnenminister so gesehen, der trotz der vorgenannten Regelung offenbar weitergehende Regelungen für erforderlich hält.

Wie stehen Sie zu Forderungen, die automatisierte Gesichtserkennung bei Videoüberwachungsanlagen generell zu verbieten?

Ich bin Realist. Ich denke, dass wir den Einsatz der Technologie nicht verhindern können. Ein Verbot dieser Technologie, wie sie die Europäische Union zunächst erwogen, dann aber im jüngst veröffentlichten Weißbuch zur Künstlichen Intelligenz nicht mehr weiter verfolgt hat, dürfte politisch nicht durchsetzbar sein. Erst recht, wenn immer wieder neue terroristische Anschläge das Gemeinwesen erschüttern. Ein Moratorium würde dem Schutz der Privatsphäre helfen, ist daher aber sehr unwahrscheinlich, dass es dazu kommt.

Die Macher von „ClearView" haben offenbar drei Milliarden Gesichtsbilder aus Sozialen Medien kopiert und mit einer Software durchsuchbar gemacht. Ein Alptraum für Datenschützer?
Das haben wir erwartet, es war doch nur eine Frage der Zeit, bis ein Unternehmen massenhaft Daten auf den verschiedenen Plattformen zusammensucht. Die Erfahrung zeigt: Alles, was möglich ist, wird auch gemacht. Das könnte man damit abtun, dass es immer ein schwarzes Schaf gibt, das es mit den rechtlichen Vorgaben nicht so genau nimmt. So einfach ist die Sache aber nicht. Der Clearview-Fall zeigt, dass die Datensicherheit bei dem Unternehmen klein geschrieben wurde und die Liste von insgesamt ca. 600 Kund*innen offenbar gestohlen wurde. Wir stehen vor einer massiven Erosion der Privatsphäre. Dieser Prozess ist schleichend und erfolgt nicht in einem eruptiven GAU, sondern in kleinen unmerklichen einzelnen Schritten. Begleitet wird er von einem Gewöhnungseffekt und der vorgeblichen kriminalpolitischen Notwendigkeit von neuen Eingriffsbefugnissen der Sicherheitsbehörden. Die EU hat mit der DSGVO zwar eine beispiellose Regelung zur Sicherung der Rechte und Freiheiten im digitalen Zeitalter beschlossen, nur kommt sie nicht bei den marktbeherrschenden Unternehmen an, die mit den Daten ihre Geschäfte im globalen Maßstab machen, weil der Rechtsvollzug nicht funktioniert. Datenschutz ist im permanenten Rückwärtsgang.

Dürfte die Hamburger Polizei diese Gesichtsbilder nutzen?
Wenn die Daten bei einem privaten Unternehmen liegen und dieses eigenständig das Datenmaterial nutzen würde, wäre dies problematisch. Wenn aber die Polizei selbst Zugriff darauf nehmen wollte, um massive Straftaten zu verfolgen oder Anschläge zu verhindern, stellt sich dies anders dar. Der Schritt hin zu einer Massendatenbank, wie sie ClearView mit Milliarden von Gesichtern erstellt hat, ist vor diesem Hintergrund so unvorstellbar nicht. Im Übrigen darf nicht vergessen werden: Der Staat setzt datenschutzwidrig erlangtes Material auch in anderen Bereichen ein. Erinnert sei nur an die sogenannten Steuer-CDs. Hier zählt am Ende nur das Ergebnis, nicht die rechtmäßige Herkunft der Daten.

Das erinnert an Horst Herold, der als Chef des Bundeskriminalamtes in den 70er Jahren die Rasterfahndung erfand. Was bedeutete „Automatisierung" damals und was bedeutet sie heute?
Im Prinzip sind die Ansätze ähnlich, wobei die automatisierte Massendatenanalyse heute technisch auf einem ganz anderen Stand ist. Das In-

strument der Rasterfahndung ist sowohl im präventiven als auch im Bereich der Strafverfolgung detailliert geregelt. Das kann man von den aktuellen automatisierten Verfahren so nicht sagen. Insbesondere bei der biometrischen Videographie fehlen eingrenzende Vorgaben und Verfahrensausgestaltungen, obwohl das Instrument sehr eingriffsintensiv ist. Derzeit geht es leider weniger um die Frage, ob und inwieweit bestimmt technische Verfahren rechtsstaatlich nutzbar sind, sondern um eine Aufrüstung der Sicherheitsbehörden mit digitaler Technik und um die Leistungsfähigkeit von Kontrollinstrumenten.

Die hessische Polizei macht das ja mit „Gotham" bzw. „HessenData" der Firma Palantir, auch Nordrhein-Westfalen beschafft die US-Software zur Gefahrenabwehr. Gibt es solche Pläne auch in Hamburg?

Es gab zumindest Überlegungen im Bereich Predictive Policing. Letztlich wurden diese wohl nicht weiter umgesetzt. Der Druck auf die Landespolizeien steigt jedoch. Grundsätzlich gilt: soweit es erfolgreiche Systeme gibt, werden diese auch angeschafft. Eine Vorschrift zur automatisierten Datenanalyse im neuen Hamburger Polizeigesetz, die der hessischen Regelung nachempfunden war, könnte so ein Türöffner für sogenannte Big-Data-Vorhaben sein.

Aber das Verfassungsgericht hat doch mit Rasterfahndung damals etwas ganz anderes gemeint als heute Palantir? Wo ist der Unterschied?

Für die Rasterfahndung, die präventiv erfolgt, muss auch eine konkrete Gefahr vorliegen. Im Bereich der Strafverfolgung müssen zureichende tatsächliche Anhaltspunkte für die Begehung einer besonderen Straftat vorliegen. Das hat das Bundesverfassungsgericht gefordert. Die Möglichkeiten, mit Hilfe der Künstlichen Intelligenz Muster von deviantem Verhalten zu erkennen und Geschehensabläufe zu prognostizieren, lange bevor sie begonnen haben, ist eine kriminalpolitische Verheißung, die es lohnend erscheinen lässt, alle erdenklichen Gefährdungsszenarien weit im Vorfeld von Gefahren anhand von Big Data zu analysieren. Das steht jedoch im Gegensatz zur Unschuldsvermutung des Einzelnen und widerspricht rechtsstaatlichen Grundsätzen, wenn damit personenbezogene Daten verarbeitet werden.

Horst Herold nannte die Rasterfahndung 1983 im Interview mit CILIP[1] die „einzig mögliche Form einer polizeilichen Fahndung, die Unschuldige

1 Bürgerrechte & Polizei/CILIP 16 (3/1983), S. 63-71 und 18 (2/1984), S. 30-46

und Nichtbetroffene dem Fahndungsvorgang fernhält". Am Ende blieben nur die wirklich Verdächtigen übrig. So argumentiert heute auch das Bundesinnenministerium zur Analyse von Fluggastdaten – das sei diskriminierungsfreier als der Blick der Grenzbeamt*innen. Wobei dort in die Zukunft geschaut, die Software also zur Gefahrenabwehr genutzt wird.

Man durchleuchtet alle, damit man diejenigen, die unschuldig sind, nicht weiter zu verfolgen braucht. Man muss sehr vorsichtig sein, um mit dieser Argumentation nicht in totalitären Bezügen zu enden. Der Rechtsstaat gibt gerade subjektive Rechte vor, nicht beliebig anlasslos überwacht zu werden. In der Konsequenz der hier zitierten Aussage sind streng genommen zunächst einmal alle verdächtig. Menschen, gegen die kein Verdacht besteht, müssen dann eigentlich dankbar sein, dass massenhaft Kontrollen erfolgen. Wahrscheinlich haben sie in dieser Logik sogar ein Recht auf massenhafte Datenabgleiche. Das erinnert an 1984 von George Orwell und ist dann am Ende eine Argumentation, die zum Rechtsstaat in diametraler Antithese steht.

Sind die neuen, algorithmenbasierten Instrumente diskriminierend?

Es ist bekannt, dass der Einsatz von KI ein hohes Diskriminierungspotential hat. Es ist jedoch nicht möglich, ohne ein umfassendes Monitoring Diskriminierungen in der Praxisanwendung zu dokumentieren. KI ist erst einmal eine Black Box. Der Einsatz von algorithmenbasierten Eingriffsinstrumenten ist im Output nicht abzuschätzen. In Hamburg haben wir uns mit der Gesichtserkennung bei G20 beschäftigt. Da sitzen allerdings immer Beamt*innen davor, die über die weiteren Schritte entscheiden. Anhaltspunkte, dass die Software diskriminiert und die Verfolgung unschuldiger Personen nahelegt, sind uns nicht bekannt. Eine automatisierte Protokollierung von Prüfläufen wäre hier zur Klärung erforderlich. Diese hat es jedoch nicht gegeben.

Wenn allerdings diese Beamt*innen ausführen, was die Software vorschlug, kann es doch zu Diskriminierungen kommen. Ein Bericht der Tagesschau hatte vor ein paar Jahren dokumentiert, wie zwei Beamte dann loszogen in San Francisco und Menschen in zerlumpter Kleidung, mit Kapuzenpullovern oder dunkler Hautfarbe kontrollierten …

Selbst wenn es beim Einsatz der Software lediglich um Entscheidungsvorschläge geht, nicht um unmittelbare automatisierte Entscheidungen, ist das individuelle Vorverständnis der Auswerter eine weitere verzerrende Fehlerquelle. Ein weiteres Problem ist die Beweislastverteilung bei KI-gestützten Verfahren – im Gegensatz zum rechtsstaatlichen Grund-

satz „in dubio pro reo“ nenne ich sie „in dubio pro machina“. Dem Verfahren der Datenverarbeitung ist eine Maschinenlogik immanent. Sie erzeugt eine prima-facie-Evidenz der Richtigkeit, die dazu führt, dass der Entscheider ohne die Übernahme eigener Verantwortung und Argumentationslasten nur schwer von der maschinellen Entscheidung abweichen kann. In der Folge braucht der Entscheider eine Antwort auf Frage: „Wieso bist du nicht eingeschritten, obwohl die Software dir die Gefahr angezeigt hat?“ Bei Personen mit Entscheidungsdruck wächst dann naturgemäß die Bereitschaft, Dinge zu exekutieren, die die Software vorgibt, während umgekehrt ein „Overruling“, also ein Übergehen der Maschinenentscheidung, als individuelles Risiko wahrgenommen wird.

Auch das Projekt „Polizei 2020“ verfolgt eine Automatisierung. Der eingeschlagene Weg schafft nicht unbedingt neue Datenbanken, sondern legt die bestehenden „Daten-Silos“ zusammen.

Diese Vernetzung und damit verbesserte Auswertung von Datenbanken sehen wir auch im EU-Projekt der „Interoperabilität“. Derartige zentralisierte übergreifende Informationssysteme stehen mit den Grundsätzen des Datenschutzes, insbesondere dem Grundsatz der Zweckbindung, im Spannungsverhältnis. Hier gilt es, technische Sicherungen zur Stärkung des Datenschutzes einzubauen, die eine exzessive und missbräuchliche Nutzung, sei es für dienstliche, sei es für rein persönliche Zwecke des Beamten, verhindern. Wichtig sind deshalb Sicherungsmechanismen, wie Vollprotokollierung und das Bestehen von starken Zugriffsberechtigungssystemen.

Wie ist das in Hamburg geregelt, wird jede Abfrage einer Datenbank protokolliert?

Das ist hier grundsätzlich der Fall. Es stellt sich jedoch die Frage, wie das im Einzelnen umgesetzt wird. Wir haben im Rahmen unserer Prüfungen feststellen müssen, dass weder die Referenzdatenbank zu G20 Zugriffe automatisiert protokolliert, noch eine Datenbank mit höchst sensiblen Daten, die für eine bestimmten Zeit offen zugänglich war.

Hamburgs Polizei ist sehr aktiv auf Twitter, sehen Sie da ein Problem?

Wir haben deutlich gemacht, dass entscheidend ist, dass keine personenbezogenen Daten veröffentlicht werden. Das lässt sich nicht immer hundertprozentig umsetzen, das haben Beispiele in anderen Bundesländern gezeigt. Etwa wenn getwittert wird, es habe Auseinandersetzungen in einem Hundefriseursalon in einem Stadtteil gegeben, wo es nur einen solchen Salon gibt. Die Nutzung sozialer Medien und Tracking Tools in

der öffentlichen Verwaltung ist insgesamt kritisch zu hinterfragen. Das betrifft das Betreiben von Fanpages bei Facebook, den Einsatz von Google Analytics oder eben das Betreiben eines Twitter-Accounts. Stets werden hier Daten von Bürgerinnen und Bürgern dritten Unternehmen übermittelt, die diese zu eigenen kommerziellen Zwecken verwenden und zu Profilen verarbeiten. Wozu das führt, hat der Cambrigde Analytica/Facebook-Skandal gezeigt. Längst geht es nicht mehr nur um Werbung für das Duftwasser oder den Sportschuh, sondern um die Manipulation von demokratischen Wahlen. Es ist aus meiner Sicht rechtsstaatlich höchst problematisch, wenn die Behörden bzw. öffentliche Stellen, die nach der Rechtsprechung des EuGH eine gemeinsame Verantwortung mit den Plattform-Anbietern haben, da mit reingehen.

Haben Sie das der Hamburger Polizei mal kommuniziert?
Wir haben unsere Kritik den öffentlichen Stellen ganz allgemein immer wieder vorgetragen. Aber das Ziel der Reichweitenerhöhung lässt hier wenig Raum für Selbstkritik. Immerhin haben wir bei der Hamburger Polizei keine konkreten Datenverstöße festgestellt. Nach der neuen EuGH-Rechtsprechung besteht jedoch weitergehender Handlungsbedarf.

Aber Sie können das doch nicht gutheißen, wenn die Polizei auf Facebook ist. Unter den nationalen Datenschutzbeauftragten haben Sie die Zuständigkeit für Facebook erhalten. Sie streiten mit der Firma …
Wir haben zahlreiche Behörden, die auf Facebook sind. Rundfunkanstalten, Ministerien und Parlamente, um nur einige zu nennen. Die Polizei ist hier keine Ausnahme. Wir müssen irgendwo anfangen, wir haben derzeit ein Anordnungsverfahren gegenüber hamburg.de eingeleitet, ein stadteigenes Unternehmen, das zahlreiche Tracker ohne Einwilligung Betroffener einsetzt. Klar, wäre es am Ende sinnvoller und effektiver, direkt gegen Facebook vorzugehen. Aber für die europaweiten Aktivitäten dieses Unternehmens ist die Datenschutzbehörde in Irland zuständig. Der Vollzug des Datenschutzes im europäischen Kontext liegt am Boden. Ich habe derzeit nicht den Eindruck, dass sich dort viel bewegt.

Nutzen Sie Facebook oder Twitter?
Nein, höchstens als Test-Account, anonym und ohne eigene Meldungen zu verbreiten.

Sind Sie da der Exot unter den Datenschutzbeauftragten?
Nein, überhaupt nicht. In Deutschland ist die Nichtnutzung die vorherrschende Praxis. Wir führen derzeit eine Diskussion, die der Landesbe-

auftragte für den Datenschutz und die Informationsfreiheit in Baden-Württemberg auslöste, der seinen Twitter-Account nun abschalten will. Wir haben das Thema mittlerweile auch im EU-Datenschutzausschuss. Es fällt schwer, etwas zu verbieten, wenn wir selbst in der Datenschutzcommunity der EU unterschiedliche Standards haben und solche Dienste mitunter von einzelnen Aufsichtsbehörden genutzt werden.

Der Bundesbeauftragte für den Datenschutz fordert Ende-zu-Ende-Verschlüsselungen per Design in neuen Telekommunikationstechnologien. Wie sehen Sie das?

Genauso, es gibt ja inzwischen einige Dienste wie Messenger, wo wir zumindest davon ausgehen, dass dort eine Ende-zu-Ende-Verschlüsselung erfolgt. Man könnte nun argumentieren, dass dies dann ein Freibrief ist, völlig unbehelligt von Sicherheitsbehörden Straftaten vorzubereiten. Gleichzeitig bestehen jedoch auch Eingriffsbefugnisse von Sicherheitsbehörden, hier tätig zu werden, etwa durch Keylogger die Nachrichten abzufangen. In der Diskussion um Hate-Speech wird vertreten, dass sogar Passwörter weitergegeben werden sollen.

Habe ich Sie richtig verstanden; gegen Verschlüsselung ist nichts einzuwenden, weil die Polizei ja Trojaner einsetzen kann?

Die Polizei argumentiert, man könne gegen die Verschlüsselung nichts unternehmen ...

… und die Politik senkt deshalb die Anforderungen für eine Quellen-Telekommunikationsüberwachung …

So ist es. Als Antwort werden die Quellen-TKÜ und die Onlinedurchsuchung vorangetrieben oder sogar ein Generalschlüssel für Sicherheitsbehörden gefordert. Im gleichen Moment wird beklagt, dass Dienste wie WhatsApp überhaupt verschlüsseln. Die Telekommunikation für Sicherheitsbehörden freizugeben, halte ich für absolut unverhältnismäßig. Auch insofern ist die Forderung nach einer Verschlüsselung im Rahmen von Privacy by Design völlig legitim und kann nicht mit sicherheitspolitischen Erwägungen weggewischt werden.

Wie soll das dann durchgesetzt werden, wenn Sie sagen, wir sind für Ende-zu-Ende-Verschlüsselung, und die Ministerien sind dagegen?

Wir sind nicht in der Position, gesetzliche Regelungen zu verhandeln. Datenschutzbehörden haben natürlich eine Meinung, die sie artikulieren. Das heißt nicht, dass wir mit am Tisch sitzen und die Rechtsregeln für die Sicherheitsbehörden mit festlegen. Man beteiligt uns am Gesetz-

gebungsprozess, aber am Ende wird gewöhnlich umgesetzt, was die Sicherheitsbehörden für erforderlich halten. Insoweit können wir dann nur die Einhaltung dieser Regelungen überwachen. Soweit Kritik gegen Sicherheitsgesetze artikuliert wird, die folgenlos bleibt, können wir am Ende nur hoffen, dass sich mal ein Verfassungsgericht damit beschäftigt.

Das Gemeinsame Überwachungszentrum Nord sollte 2020 an den Start gehen, wann kommt es? Das müssten Sie ja dann mit den Kolleg*innen aus Niedersachsen, Mecklenburg-Vorpommern, Bremen und Schleswig-Holstein kontrollieren. Wie bereiten Sie sich darauf vor? Ist bereits klar, welche TKÜ-Maßnahmen dort erledigt werden? Auch Stille SMS und der Einsatz von Trojanern?

Das Landeskriminalamt Niedersachsen ertüchtigt aktuell das Rechenzentrum in Hamburg-Alsterdorf (mit Twin-Data-Center Niendorf), um dort die TKÜ der Nordländer implementieren zu können. Die Ausschreibungen wurden abgeschlossen und die benötigte Technik wird aktuell beschafft, dennoch geht das Landeskriminalamt nicht von einer Inbetriebnahme 2020 aus, eher gegen Mitte/Ende 2021. Bezüglich des Rechendienstleistungszentrums gibt es seit Projektbeginn eine Zusammenarbeit des Landeskriminalamts Niedersachsen mit den Landesdatenschutzbeauftragten der betroffenen Länder, das letzte Treffen fand Anfang Februar statt. Welche Überwachungsmaßnahmen im „Gemeinsamen Kompetenz- und Dienstleistungszentrum“ (GKDZ) konkret für das Land Hamburg durchgeführt werden sollen, entzieht sich noch unserer Kenntnis. Eine Auflistung der geplanten Überwachungsmaßnahmen soll seitens des Landeskriminalamts Hamburg in den kommenden Wochen an uns versandt werden.

Datenschutz funktioniert nur mit Kontrolle und Aufsicht. Wir haben das Beispiel der Presseakkreditierungen beim G20-Gipfel in Hamburg. Da konnte die damalige Datenschutzbeauftragte des Bundes gucken, welche Datensätze sind vorhanden. Aber die Erforderlichkeit der Speicherung konnte sie nicht prüfen, weil der Rückgriff auf die Akten der Landespolizeien den Landesdatenschutzbeauftragten vorbehalten ist.

Es ist tatsächlich so, dass die Verbunddateien eine gewisse Zusammenarbeit erfordern, das funktioniert in der Praxis jedoch. Die Aufsichtsbehörden müssen hier ihre Erkenntnisse miteinander teilen, wo dies möglich ist, und in ihrem Zuständigkeitsbereich eigenständig Kontrollen durchführen. Ich sehe nicht, dass die Kontrolle über die jeweils für bestimmte Bereiche der Datenverarbeitung zuständigen Polizeibehörden

nicht möglich wäre. Kontrolle und Aufsicht werden immer auch von der zuständigen Aufsichtsbehörde bestimmt.

Viele Gesetzesinitiativen, mit denen sich der deutsche Datenschutz befassen muss, werden auf EU-Ebene gemacht. Wie funktioniert die europäische Zusammenarbeit, was haben die Landesdatenschutzbeauftragten dort zu sagen und wie landen die Vorschläge dann bei der EU-Kommission?

Im nationalen Bereich legt die Datenschutzkonferenz der unabhängigen Aufsichtsbehörden von Bund und Ländern die Richtlinien für die europäischen Angelegenheiten fest. Im europäischen Datenschutzausschuss sitzen der Bundesbeauftragte und ein Ländervertreter und vertreten dort die nationale Ebene mit Blick auf anstehende Entscheidungen, Stellungnahmen oder Leitlinien. Die Länder sind auch an der Kontrolle der Agenturen beteiligt, z. B. für Europol.

Medien hören doch eigentlich gern auf Datenschutzbeauftragte, einige von Ihnen sind ja recht bekannt, Thilo Weichert zum Beispiel, und Sie selbst wurden jüngst von Politico zu einem der 28 einflussreichsten Europäer*innen erklärt.

Unser Gewicht im Bereich der sicherheitspolitischen Debatten ist eher mahnend. Insofern ist politische Beratung ein zentraler Aspekt, das will ich nicht wegreden. Hier kann die Kritik dazu führen, dass Gesetzgebung anders, datenschutzfreundlicher umgesetzt wird. Aber tatsächlich etwas zu verändern ist schwierig. Selbst dort, wo wir der Meinung sind, dass gegen Gesetze verstoßen wurde und eine aufsichtsbehördliche Kompetenz besteht. Ich erinnere wieder an das Beispiel der G20-Gesichtsfahndung in Hamburg. Hier stellt das Verwaltungsgericht selbst eine klare Anordnungsbefugnis der Datenschutzaufsichtsbehörde in Frage. Das wird zu überprüfen sein. Darüber hinaus gibt es derzeit insgesamt viel Gegenwind: Es besteht ein Trend in der öffentlichen Meinung, den Datenschutz in die Nähe des Täterschutzes zu rücken. Dabei befinden wir uns in einer wichtigen Phase, in der es darum geht, die Koordinaten zu bestimmen, wie weit wir gehen dürfen: Technologien, die wir aus China kennen, klopfen bereits heute an unsere Tür. Es wird darauf ankommen, hier wachsam und hartnäckig zu sein. Am Ende entscheidet diese Debatte über die Zukunft des Rechtsstaats.

Vielen Dank für das Interview!

KI in der Polizeiarbeit

Der Mythos vom vorhersagbaren Verbrechen

von Nina Galla

Schon mindestens 75 Staaten nutzen Künstliche Intelligenz (KI) zu polizeilichen Zwecken. Mit dem sogenannten „Predictive Policing" arbeiten 52 Länder, 64 nutzen automatisierte Gesichtserkennung in der Videoüberwachung.[1] Pilotprojekte gibt es auch in Deutschland.

Wenn von KI die Rede ist, geht es meist um Verfahren eines mehr oder weniger ausgeprägten maschinellen Lernens. Alle diese Systeme sind komplex, es braucht zahlreiche menschliche Entscheidungen, um sie so zu gestalten, dass sie tatsächlich ihren Zweck erfüllen. Diese Entscheidungen wiederum erfordern Kenntnis und Verständnis sowohl der technischen Verfahren als auch des sozialen Kontexts ihres Einsatzes.

Die Datenethik-Kommission empfiehlt in ihrem im November 2019 veröffentlichten Gutachten, diese Systeme je nach Auswirkungen und Risikopotenzial in verschiedene Risikoklassen einzuordnen, aus denen sich Anforderungen an ihre Regulierung ergeben.[2] KI in der Polizeiarbeit kann Auswirkungen auf das Vertrauen der Gesellschaft in die Behörden haben. Predictive Policing gehört daher in eine der höchsten Risikoklassen des Modells der Datenethik-Kommission.

Anders als manchmal suggeriert wird, sind KI-Systeme keine Zauberei. Es sind Maschinen, die mit hoher Rechenleistung statistische Verfahren anwenden. Sie ermitteln Wahrscheinlichkeiten. Sie können nur Korrelationen entdecken, keine Kausalitäten. Und sie wenden keine wissenschaftlichen Verfahren an, um zu ihren Ergebnissen zu kommen. Menschen wählen aus, zu welchem Zweck und mit welchen Daten ein

1 Forscher: Weltweit immer mehr Massenüberwachung mit KI, heise online v. 18.9.2019

2 Datenethikkommission der Bundesregierung: Gutachten, Berlin Oktober 2019, S. 177 (www.bmjv.de/SharedDocs/Downloads/DE/Themen/Fokusthemen/Gutachten_DEK_DE.pdf)

System trainiert wird. Menschen bewerten den Lernfortschritt und entscheiden, wie sie mit den Ergebnissen umgehen wollen. Menschen tragen also eine hohe Verantwortung entlang der gesamten Kette von Entwicklung, Einsatz und Evaluierung eines solchen Systems.

Eine sogenannte „starke KI", bei der eine Maschine in ihrem Lernverhalten unabhängig vom Menschen wäre, ist bis auf Weiteres technisch ausgeschlossen. Maschinen scheitern an Unvorhergesehenem und komplexen Zusammenhängen. Faktisch geht es also immer um „schwache KI", also darum, dass Maschinen wenig komplexe Aufgaben ausführen, welche bestimmten Regeln folgen und deren Kriterien für Computer zu verstehen, also operationalisierbar, sind.

Beruhigen kann das allerdings nicht, denn auch „schwache KI" ist – insbesondere beim Einsatz im polizeilichen Bereich – nicht frei von Risiken. Grundsätzlich geht es hier um die Vorverlagerung von Ermittlungen aufgrund von maschinell entdeckten Korrelationen und damit um eine mögliche Umkehr der Unschuldsvermutung. Weitere Probleme zeigen sich, wenn man betrachtet, wie eine Maschine überhaupt lernt und zu Entscheidungen kommt und wie mit diesen Entscheidungen umgegangen wird.

Trainingsdaten: Auf Basis welcher Daten lernen die Systeme, Entscheidungen zu treffen?

Maschinen lernen zunächst auf Basis bereits vorhandener Daten. Damit die Maschine überhaupt mit etwas arbeiten kann, müssen diese Daten für Maschinen lesbar und verständlich, also „operationalisierbar" sein. Einfach zu operationalisierende Daten sind Alter, Geschlecht, Uhrzeit, Ort – also Daten, die einen eindeutigen Zustand beschreiben. Bezogen auf die Polizeiarbeit können dies personenbezogene Daten sein oder Fallzahlen von Straftaten, die wiederum klassifiziert werden können. Nicht oder nur sehr schwer operationalisierbar sind subjektive Umstände bei der Begehung von Straftaten – Motive, Affekte, Interaktion mit anderen. Verbrechen werden daher nie zuverlässig vorhersagbar sein.

Es ist hingegen möglich, bestimmte Wahrscheinlichkeiten zu errechnen: Wo in der Vergangenheit oft eingebrochen wurde, wird in Zukunft vielleicht auch oft eingebrochen. Da es in den letzten Jahren auf Weihnachtsmärkten viele Taschendiebstähle gab, wird es sie voraussichtlich auch wieder in diesem Jahr geben. Damit können Theorien wie zum Beispiel der Near-Repeat-Ansatz unterstützt werden.

In der Polizeiarbeit werden aber vielfach unnötig Daten gesammelt und vorgehalten, um solche Trainingsdaten zu gewinnen. Sie sind für polizeiliche Zwecke nicht erforderlich. Von diesen Inputdaten ist jedoch das Ergebnis der maschinellen Arbeit abhängig: Bilden die Daten polizeilich relevante Vorgänge zu einseitig ab? Manifestieren sie bereits bestehende Diskriminierungen? Sind sie zu alt? Bilden sie falsche Verhältnisse ab? Sind sie überhaupt kausal zum Output oder verleiten sie zu falschen Maßnahmen? Grundsätzlich muss sich die Polizei hier fragen: Was soll eine Maschine hier besser können als der Mensch? Sind die Daten, die wir dafür brauchen, überhaupt in ausreichender Qualität und Quantität vorhanden und dabei operationalisierbar und kausal?

Algorithmus: Welches Lernverfahren wird gewählt, um das gewünschte Ziel zu erreichen?

Eine Maschine braucht ein Ziel, für das sie lernen soll. Das kann sein, eine bestimmte Reihenfolge festzulegen, eine Route zu finden, ein Muster zu erkennen oder eine Wahrscheinlichkeit zu ermitteln. Für diese Lernziele gibt es verschiedene Algorithmen, die beim Training eines Systems eingesetzt werden können. Die Wahl des Algorithmus ist daher essenziell für die Qualität des Ergebnisses. Aus diesem Grund ist es auch sehr problematisch, ein trainiertes KI-System für einen anderen als den ursprünglichen Zweck einzusetzen. Es bedarf einer besonderen Expertise, um die richtigen technischen Anforderungen für den jeweiligen sozialen Kontext zu definieren. Systeme des maschinellen Lernens werden daher auch als sozio-technische Systeme bezeichnet, da sie je nach Umfeld unterschiedliche soziale Wirkungen entfalten. Es ist derzeit fraglich, ob diese Kompetenzen in Polizeibehörden überhaupt ausreichend vorhanden sind.

Was macht der Mensch mit den Ergebnissen?

Im kommerziellen Kontext – etwa bei der Werbung durch Empfehlung von Produkten – ist das Schadenspotenzial von KI-Ergebnissen gering. Wer diesen Ergebnissen ausgesetzt wird, kann dem Vorschlag folgen oder auch nicht. Im polizeilichen Kontext ist dies logischerweise hochsensibel, denn hier geht es unter Umständen darum, ob die Polizei von Ermittlungs- und Zwangsbefugnissen Gebrauch macht oder nicht. Daher sind die Fragestellungen, welcher Art das Ergebnis ist (Wahrscheinlich-

keit, Klassifizierung, Vorschlag) und wie viel Handlungsspielraum den polizeilichen Entscheider*innen gegeben wird, genauso zentral wie die Auswahl der Inputdaten und des Algorithmus. Ein Beispiel: Das Land Baden-Württemberg plant am Hauptbahnhof Mannheim ein Projekt, das Bewegungsabläufe von Passant*innen analysieren und bestimmte Verhaltensmuster melden soll. Als „kritisches" Verhalten soll dabei auch das Rennen gelten.[3]

Für ein KI-System ist es sehr schwierig, eine allgemeine Regel zu lernen, da es für das Verhalten von Menschen zu viele individuelle Motivationen gibt. Wie soll das System unterscheiden lernen, ob ein Mensch zu etwas oder jemandem hinläuft (einem geliebten Menschen) oder vor etwas wegläuft? Und wenn der Mensch wegläuft – läuft er*sie weg vor eine*r potenziellen Straftäter*in oder ist sie*er selbst eine*r? Um das System richtig trainieren zu können, müssen Grenzen festgelegt werden, ab wann das Laufen am Bahnhof als risikoreich gilt. Damit die Maschine operationalisierbaren Input bekommt, muss diese Grenze scharf gezogen werden: Es sind nur Entscheidungen „gefährlich" oder „nicht gefährlich" möglich. Dies führt zwangsläufig dazu, dass harmloses Laufen hin und wieder als risikoreich bewertet wird und umgekehrt. Wo diese Grenze zu ziehen ist, entscheiden Menschen. Und hier stellt sich eine Frage, die nur gesamtgesellschaftlich festgelegt werden kann: Wollen wir lieber einige harmlose Passant*innen in die Klasse der Risikopersonen stecken oder besser einige Risikopersonen unerkannt lassen? Derzeit wird diese Debatte jedoch nicht öffentlich geführt.

Und im letzten Schritt: Wie geht der Mensch mit dem Ergebnis um, wenn ein Mensch als „risikoreiche*r Läufer*in" erkannt wird: Ist der Verdacht der Maschine schon Anlass genug für eine Überprüfung? Sind die Entscheider*innen fähig, eine mögliche Diskriminierung zu erkennen und kennen sie Wege für Rückmeldungen, dass das System optimiert werden muss? Was blüht der* Entscheider*in, wenn sie trotz maschineller Treffermeldung auf eine Überprüfung verzichtet?

Bei kritischen Anwendungsbereichen von KI heißt es stets, dass die Letztentscheidung immer noch beim Menschen liege. Hier gibt es aber noch viel mehr Fragen zu stellen – vom Automatisierungsgrad bis hin zu arbeitsrechtlichen Konsequenzen bei Nicht-Befolgen der maschinellen Empfehlung. In der Mensch-Maschine-Interaktion können bis zu zehn

3 Mannheim testet verhaltensbasierte Videoüberwachung, heise online v. 3.12.2018

verschiedene Automatisierungsgrade differenziert werden.[4] Das menschliche Verhalten im Umgang mit maschinellen Entscheidungsvorschlägen wird derzeit noch erforscht. Erste Ergebnisse zeigen, dass Menschen dazu neigen, maschinelle Entscheidungen nicht mehr in Frage zu stellen. Wenn beruhigend davon gesprochen wird, dass der Mensch stets die letzte Entscheidung treffe, lohnt es sich daher nachzufragen, welche Vorarbeit die Maschine denn geleistet hat: Hat sie Korrelationen dargestellt und drei mögliche Handlungsempfehlungen gegeben? Oder nur eine, und die Entscheidung des Menschen besteht nur noch darin, zuzustimmen oder abzulehnen? Noch weniger Spielraum gibt es bei Automatisierungsgraden, die eine Entscheidung ausführen und der Mensch sie nur noch stoppen kann. Auch hier trifft der Mensch die letzte Entscheidung, sie besteht jedoch nur noch aus Unterlassen oder Intervenieren.

Videoüberwachung am Südkreuz

Das wohl bekannteste KI-Projekt bislang in Deutschland ist das Pilotprojekt zur Gesichtserkennung am Berliner Bahnhof Südkreuz von 2017. Das Ergebnis: mangelhaft. Während das Bundesinnenministerium (BMI) die Ergebnisse durch Auslassung von wichtigen Informationen geschönt hat, machte der Chaos Computer Club dieser PR-Taktik einen Strich durch die Rechnung und stellte heraus, wie hoch die Fehlerquote der einzelnen Systeme tatsächlich war: Es könnten täglich mehr als 600 Passant*innen fälschlich als „Treffer“ klassifiziert werden.[5] Auch wenn die Interpretation des BMI aus rein politischen Gründen erfolgte, hinterlässt sie den Beigeschmack fehlender technischer und statistischer Kompetenz, die Ergebnisse korrekt zu interpretieren.

Auch in London hat eine Untersuchung der Gesichtserkennung durch die Polizei eine miserable Trefferquote von 20 Prozent offengelegt. Sie zeigte zusätzlich, dass Polizist*innen zu leichtfertig mit den Ergebnissen umgehen, unter anderem weil sie nicht ausreichend überprüft

4 Save, L.; Feuerberg, B.: Designing Human-Automation Interaction: a new level of Automation Taxonomy, in: De Waard, D. et al.: Human Factors: a view from an integrative perspective, HFES Europe Chapter Conference, Toulouse 2012, S. 43-55 (44) (www.hfes-europe.org/wp-content/uploads/2014/06/Save.pdf)

5 Videoüberwachung: Seehofer hält flächendeckende Gesichtserkennung für möglich, zeit.de v. 12.10.2018; CCC: Bundespolizei hat Bericht zur Gesichtserkennung absichtlich geschönt, heise online v. 15.10.2018

wurden.[6] Diese katastrophalen Ergebnisse hindern das BMI jedoch nicht daran, die Videoüberwachung an Bahnhöfen in Zukunft auszubauen. Bis 2023 sollen insgesamt 132,5 Millionen Euro investiert werden.[7]

SKALA – schwache Aussagekraft von Prognosen

Auch andere Predictive Policing-Experimente fielen bisher mittelmäßig aus, so zum Beispiel das Projekt SKALA (kurz für „System zur Kriminalitätsauswertung und Lageantizipation"), das von 2015-2017 in Nordrhein-Westfalen lief. Das Ziel des Pilotversuchs war es, die „Möglichkeiten und Grenzen der Prognose von Kriminalitätsbrennpunkten" sowie die „Effizienz und Effektivität daraus resultierender polizeilicher Maßnahmen" zu prüfen.[8] Der Fokus lag dabei auf Einbrüchen in Wohnungen und Gewerbeobjekten sowie bei KFZ-Delikten. Während in anderen Datenanalysesystemen (z.B. „Hessendata") Daten aus unterschiedlichen Quellen lediglich zusammengeführt werden, zeichnete sich SKALA durch eine Prognosefunktion aus.

Im Idealfall sollte mit SKALA eine Senkung der Kriminalitätshäufigkeit erreicht werden. Hierzu entwickelte das Landeskriminalamt NRW ein eigenes System, das sowohl strukturierte als auch unstrukturierte Daten analysieren und Muster erkennen kann. Als Datenbasis dienten polizeiliche Vorgangsdaten sowie Daten zu Bevölkerungsstruktur, Einkommen, Gebäudestruktur, Reiseaffinitäten und KFZ-Zulassungen, aber auch Fluchtmöglichkeiten wie die Nähe zu Bundesstraßen oder Autobahnen. Auch die allgemeine Straßenkriminalität, Berechnung der Tage seit dem letzten Einbruch im Wohnquartier beziehungsweise Straßenabschnitt („Near-Repeat-Ansatz"), der Modus Operandi der Tat sowie Wert und Art der Beute flossen in das System ein. Personenbezogene Daten (Täter- oder Opferdaten) wurden nicht verwendet.

Zunächst wurden wissenschaftliche Hypothesen generiert und Vorhersagevariablen identifiziert. Dann erfolgte die Auswahl und Aufbereitung der Daten. Eine erste Einschränkung der Vorhersagequalität ergibt sich daraus, dass Täter*innen wie oben angeführt nicht durchgehend

6 Gesichtserkennung in London hat miserable Trefferquote und kann Menschenrechte verletzen, Netzpolitik.org v. 5.7.2019

7 Bahn: mehr Überwachung mit Gesichtserkennung an Bahnhöfen, heise.de v. 12.9.2019

8 Landeskriminalamt NRW: Abschlussbericht Projekt SKALA, Düsseldorf 2018 (https://lka.polizei.nrw/sites/default/files/2019-01/180821_Abschlussbericht_SKALA_0.PDF)

rational handeln, das heißt, dass sie nicht in jedem Fall allein eine Kosten-Nutzen-Abwägung ihrer Tat vornehmen. Daraus resultierende Prognosefehler lassen sich auch nicht operationalisieren. Eine weitere Fehlerquelle resultiert aus dem Umstand, dass manche Delikte erst mit Verzug angezeigt werden oder auch die tatsächliche Deliktschwere erst später ermittelt wird. Deshalb wurden bei SKALA regelmäßig neue aktualisierte Gesamtdaten bezogen.

Zur Analyse wurde mit Entscheidungsbäumen gearbeitet. Entscheidungsbaummodelle gelten als gut nachvollziehbar, da hierbei Datenlücken erkannt und geschlossen werden können, außerdem können zielgenau Variablen verändert werden. So zeigte sich beispielsweise, dass Wetterdaten nicht die angenommene Relevanz für die Prognose hatten.

Zur Prognoseberechnung wurden raum- und zeitbezogene Daten (Jahreszeiten) zusammengeführt und Wohnquartiere als räumliche Bezugsgröße ausgewählt. Hierbei war darauf zu achten, dass die Quartiere eine ausreichende Homogenität aufweisen und die Einheiten weder zu groß noch zu klein gewählt werden. Je größer die Einheit, desto mehr Detailinformationen gehen verloren, desto höher ist aber auch die Wahrscheinlichkeit, dass ein erwartetes Ereignis eintritt. Ist die Einheit jedoch zu klein, könnten zu viele Details zu Unüberschaubarkeit und schlechterer Vergleichbarkeit führen. Im Laufe des Projekts wurde beispielsweise der Zuschnitt der Quartiere noch einmal angepasst. Die Ergebnisse der Prognosen wurden dann den Polizeikräften als Karten übermittelt. Zu bedenken ist hierbei, dass auch die Gestaltung von Visualisierungen nicht neutral ist und Farbgebungen das menschliche Verhalten beeinflussen können.

Die Ergebnisse beschreiben zunächst lediglich die beobachteten Effekte. Bei der Auswertung musste sichergestellt sein, dass hier keine Verzerrung entsteht, indem Taten, die nicht zum Katalog der definierten beobachteten Delikte gehören, hinzugerechnet werden. Wie sich auf zahlreichen Veranstaltungen herausstellte, sind Definitionen einheitlicher Validierungsindizes allerdings noch keine gängige Praxis im Bereich von Predictive Policing; dies erschwert auch die Vergleichbarkeit mit anderen Systemen. Die Analyse ist auch abhängig vom beobachteten Zeitraum. Es können sich große Abweichungen ergeben – abhängig davon, ob Daten aus einem Zeitraum von einem Tag oder zwei Wochen betrachtet wurden. Auch das betrachtete Quartier ist differenziert zu bewerten: Wenn sich die Prognose auf einen „Hotspot“ bezieht, in dem die Wahrscheinlichkeit für Straftaten sowieso schon hoch ist, dann ist

zwar auch die Erfolgsquote hoch, hat aber keinen Mehrwert. Tatsächlich lag die vom System berechnete Einbruchswahrscheinlichkeit höher in Wohnquartieren, die insgesamt stark von Einbrüchen betroffen sind, als in Quartieren, in denen der Zeitabstand zum letzten Einbruch hoch war. Im Ergebnis konnte die KI also das nachbilden, was erfahrene Polizeibeamt*innen ohnehin prognostizierten. Ob dieses Ergebnis den Einsatz von insgesamt mehr als 500.000 Euro rechtfertigt, bleibt fraglich.

Das wichtigste Ziel des SKALA-Projekts war jedoch, in Prognosegebieten Taten durch gezielte präventive Maßnahmen wie Bestreifung zu verhindern. „Trefferraten" können dadurch also nicht verifiziert werden, denn die Zahl ausgebliebener Straftaten lässt sich nicht berechnen. Auch wenn die Polizei in den getesteten Gebieten während des SKALA-Projekts ihre Maßnahmen gar nicht verstärkt hat, wurden keine „Trefferraten" berechnet. Denn auch hier bedeutet Korrelation keine Kausalität.

Auch zeigte sich, dass mehr Daten nicht zu besseren Ergebnissen führen. Es blieben elf Variablen übrig, die für die Prognose als sinnvoll erachtet wurden. Ausschlaggebender war der Zuschnitt der bewerteten Wohnquartiere. Je nach Wohnquartier und Jahreszeit zeigten sich unterschiedliche Korrelationen der ausgewählten Variablen, so dass eine Übertragbarkeit der Ergebnisse auf andere Zeiträume, Quartiere oder gar von der Stadt auf das Land nicht möglich ist.

KI verhindert keine Straftaten, gefährdet aber Bürgerrechte

Mittlerweile ist die Zahl der Einbruchsstraftaten in Deutschland wieder zurückgegangen, ohne dass es dafür eine eindeutige Erklärung gibt. Eine ganze Reihe weiterer Straftaten mit vielen Opfern, insbesondere Beziehungstaten, lässt sich mit Predictive Policing ohnehin nicht prognostizieren. Es fehlt wie gesagt an operationalisierbaren Daten. Das Freiburger Max-Planck-Institut für ausländisches und internationales Strafrecht hat in einer Studie ebenfalls herausgestellt, dass Predictive Policing höchstens im homöopathischen Bereich Nutzen für die Polizeiarbeit bringt.[9]

Bislang dürfen aufgrund mangelnder Rechtsgrundlagen Systeme der automatisierten Entscheidungsfindung nur als Pilotprojekte eingesetzt werden. Wie die oben genannten Beispiele zeigen, ist das ein großes

9 Predictive Policing – die Kunst, Verbrechen vorherzusagen, heise online v. 19.5.2019

Glück, da die Maschinen nicht ansatzweise halten, was sich Behörden von ihnen erhoffen. Und selbst wenn, stellt sich die Frage nach der benötigten Rechtsgrundlage.

Predictive Policing kann darüber hinaus auch Profilbildung bedeuten. Im September 2019 startete das EU-finanzierte Forschungsprogramm „Roxanne", das Sprach-, Video-, Orts- und Netzwerkdaten (auch aus sozialen Medien) aus unterschiedlichen Quellen auswerten und verbinden soll, um damit Netzwerke aufzudecken. Daran beteiligt sind neben Interpol auch die Universitäten Hannover und Saarbrücken. Hierbei können Menschen aufgrund von persönlichen Netzwerken zu Risikoklassen gezählt werden,[10] in die sie überhaupt nicht gehören. In den USA werden solche Profilbildungen und Netzwerkanalysen bereits angewendet. Das System macht dabei auch nicht Halt vor Rentnern und über 100-Jährigen, die vor Jahrzehnten in Gangs aktiv waren.[11] Die Technologie entwickelt sich schnell weiter: An der Wuhan University of Technology in China konnten kürzlich anhand von Schallwellen Bewegungen in einem Raum erkannt werden.[12] Die maschinelle Überwachung – sie geht weiter.

Wie weiter?

Schaut man hinter den Zauber der KI, wird deutlich, dass es keine Anwendungsbereiche gibt, in denen Maschinen bessere Polizeiarbeit machen können als die Polizei selbst. Das Versprechen, mit maschinellem Lernen könne ein höheres Sicherheitsniveau erreicht werden, ist nicht haltbar und irreführend. Damit die Gesellschaft dieser Mär nicht auf den Leim geht – mit allen beschriebenen Konsequenzen –, braucht es eine breite Aufklärung und Sensibilisierung zu den Möglichkeiten und Grenzen von Maschinen – und nicht zuletzt eine Aufwertung des Menschen, der immer noch besser in der Lage ist, komplexe Situationen einzuschätzen als jede Maschine.

Gesichtserkennung und auch Videoüberwachung finden derzeit nur wenige Gegner*innen, da die Vorstellung, man habe selbst nichts zu verbergen, zum subjektiven Gefühl einer Nicht-Beobachtung führt und

10 Strafverfolgung: Geheimdienstmethoden für Ermittler, Golem v. 8.11.2019
11 Big Data: Predictive policing in Chicago, Wired v. 12.12.2018

die Erfassung der eigenen Daten keinen unmittelbar spürbaren Nachteil ergibt.

Es ist jedoch nicht unerheblich, wo und von wem wir gefilmt werden, was mit den Aufnahmen geschieht und wer wo wie lang die Aufnahmen speichert. Es ist nicht immer bloß eine Spielerei, wenn Apps aus aktuellen Gesichtsbildern Emojis machen oder berechnen, wie jemand in dreißig Jahren aussehen wird. Es kann immer ein Training für Gesichtserkennungssoftware dahinter stehen, dem die einzelnen Nutzer*innen durch Hinweggehen über die Allgemeinen Geschäftsbedingungen (AGB) zustimmen, ohne es bewusst wahrzunehmen. Wenn unzureichende oder fehlerhafte Systeme von nicht ausgebildeten oder autorisierten Polizist*innen verwendet werden, geraten möglicherweise Daten in die Polizeiarbeit, die dort nicht hingehören. Die Pläne, zahlreiche Datenbanken auf europäischer Ebene zusammenzuführen, erhöhen das Risiko der unberechtigten Zugriffe.

Wenn ein System des maschinellen Lernens schon unbedingt eingesetzt werden soll, dann sollte es doch zunächst zu internen Zwecken innerhalb von Behörden pilotiert werden. Es könnten dabei (selbstverständlich unter Achtung von Datenschutz-Rechten der Arbeitenden) missbräuchliche Datennutzungen entdeckt oder auch rechte Netzwerke aufgedeckt werden – ohne Bürgerrechte zu gefährden. Dabei können gleichzeitig behörden-internes Wissen und Erfahrungen aufgebaut werden, die derzeit noch nicht flächendeckend vorhanden sind.

Auch die Fragestellung, in welcher Gesellschaft wir leben wollen, muss regelmäßig breit diskutiert werden: Nur eine informierte Gesellschaft ist in der Lage, den Sicherheitswahn der Behörden kritisch zu hinterfragen und Bürgerrechte zu schützen. Die Zahlen des Pilotversuchs am Südkreuz sind ernst zu nehmen: Wenn täglich 600 Menschen fälschlicherweise als Terrorist*innen klassifiziert werden, ist es eine Frage der Zeit, bis es auch jene trifft, die bislang meinten, sie hätten nichts zu verbergen.

Von den Behörden müssen wir erwarten und einfordern, dass sie offenlegen, wie sie ihre Systeme auswählen und trainieren, wer an welcher Stelle was entscheidet und welche Qualifikationen diese Person mitbringt. Entsprechend den Risikoklassen der Datenethikkommission braucht es einen klaren Katalog von Anforderungen für Systeme in der Polizeiarbeit und auch eine klare rote Linie: Können relevante Kriterien nicht erfüllt werden, darf das System nicht eingesetzt werden. Es muss auch gestoppt werden, wenn es im laufenden Betrieb Diskriminierungen

zeigt oder Entscheidungen nicht nachvollziehbar und reproduzierbar sind. Hierzu braucht es eine qualifizierte öffentliche Kontrollinstanz. Der Einsatz kann sich durchaus lohnen: In San Francisco wurde die Gesichtserkennung mittlerweile wieder deutlich eingeschränkt.[13]

Die Pläne des BMI, 135 Bahnhöfe mit biometrischer Gesichtserkennung auszustatten, sind vorerst gestoppt.[14] Parallel arbeitet allerdings das BKA an einer polizeilichen KI-Strategie.[15] Noch ist wenig dazu bekannt und man darf gespannt sein, wann und wo die Gesichtserkennung wieder auftaucht und wie sorgfältig die aktuellen Fehlerquellen der Pilotversuche erkannt und geschlossen wurden. Die Zeit bis dahin sollten Bürgerrechtler*innen nutzen, um unbequeme Fragen vorzubereiten und mit gesellschaftlicher Unterstützung zur rechten Zeit das Salz in die richtige Wunde zu streuen.

13 San Francisco verbietet Gesichtserkennung durch Behörden, Zeit online v. 15.5.2019

14 Bundespolizei: Nutzung von Gesichtserkennung wird wohl nicht erlaubt, RBB24 v. 24.1.2020

15 BT-Drs. 19/13221 v. 16.9.2019, S. 6

Ein aufhaltsamer Aufstieg

Kurze Geschichte der automatisierten Gesichtserkennung

von Roland Meyer

In einer konzertierten Aktion zwischen staatlichen Sicherheitsbehörden und kommerziellen Unternehmen wurde seit den 1960er Jahren die Entwicklung der automatisierten Gesichtserkennung vorangetrieben. Die gescheiterten Versuche und die nach wie vor hohen Falscherkennungsraten haben diese Geschichte nicht aufgehalten. Höchste Zeit für eine politische Debatte.

Der Minister war zufrieden. Als Horst Seehofer im Oktober 2018 die Ergebnisse des Pilotprojekts zum Einsatz automatisierter Gesichtserkennung am Berliner Bahnhof Südkreuz vorstellte, zeigte er sich sogar zu Scherzen aufgelegt. „Wenn die Politik nur 0,1 Prozent Fehler machen würde, dann wären wir gut", kommentierte er die Falscherkennungsraten der getesteten Systeme launig.[1]

Nicht nur, dass, wie der Chaos Computer Club herausfand,[2] die Treffer- und Fehlerraten im Abschlussbericht der Bundespolizei wohl geschönt waren – auch ohne vertiefte Kenntnisse in Statistik und Informatik hätten die Zahlen stutzig machen können. Schon mit einfacher Mittelstufenprozentrechnung zeigt sich nämlich, dass bereits die angegebene Fehlerquote im flächendeckenden Einsatz verheerende Konsequenzen hätte. Bei rund 90.000 Passant*innen, die den Bahnhof Südkreuz täglich passieren, würde das System rund 90 Mal am Tag falschen Alarm geben. Ein Einsatz auf allen Bahnhöfen im Bundesgebiet hätte gar, wie das Max-Planck-Institut für Bildungsforschung ausgerechnet hat, rund 350.000 Fehlalarme monatlich zur Folge – 350.000 Menschen,

1 zit. nach Kontraste: Millionenfach unnötige Personenkontrollen durch Gesichtserkennung?, ZDF v. 23.11.2018 (https://www.youtube.com/watch?v=kpkTtkKpAwM)

2 Chaos Computer Club: Pressemitteilung v. 13.10.2018 (www.ccc.de/de/updates/2018/debakel-am-suedkreuz)

die im Zweifelsfall von der Polizei gestoppt und kontrolliert würden. Und da die Zahl der gesuchten „Gefährder“ im Verhältnis zur Gesamtbevölkerung verschwindend gering ausfällt, stellt sich fast jeder Treffer des Systems als falscher Alarm heraus – mutmaßlich mehr als 99 Prozent.[3] Anders als Ministerium und Bundespolizei die Öffentlichkeit glauben machen wollten, hatten sich die Systeme also keinesfalls „in beeindruckender Weise bewährt“.[4]

Das muss schließlich auch dem Minister gedämmert haben. Ursprünglich hatte Seehofer angekündigt, noch 2020 die gesetzlichen Voraussetzungen zu schaffen, um automatisierte Geschichtserkennung an 135 Bahnhöfen und 14 Flughäfen einsetzbar zu machen. Im aktuellen Entwurf für das Bundespolizeigesetz ist davon keine Rede mehr. Überraschend ließ Seehofer verkünden, es seien noch „einige Fragen“ in Bezug auf die Technologie und ihre gesellschaftliche Akzeptanz offengeblieben. Tatsächlich lässt sich beobachten, dass der Einsatz automatisierter Gesichtserkennung auch in Deutschland immer kritischer diskutiert wird – auch jenseits jener Kreise, die immer schon Datenschutzbedenken angemeldet hatten.

Meldungen wie die über die Firma *Clearview*, die in riesigen Größenordnungen private Bilder aus Social-Media-Netzwerken mittels Gesichtserkennung durchsuchbar macht – selbstverständlich ohne die Einwilligung der Nutzer*innen –, haben auch hierzulande für Aufsehen gesorgt. In den USA artikulieren sich inzwischen massive zivilgesellschaftliche Forderungen nach einer Regulierung, wenn nicht gar einem Verbot der Technologie, und erste Städte – darunter die Tech-Metropole San Francisco – haben bereits einen „ban on facial recognition“ ausgesprochen. Weit handfester äußerte sich der Widerstand im vergangenen Sommer in Hong Kong, wo es die Demonstrant*innen gezielt auf die Demontage der Überwachungskameras abgesehen hatten, um der allgegenwärtigen Gesichtserkennung zu entgehen.

Was jedoch in der gegenwärtigen Debatte seltsam unterbelichtet scheint, ist die Tatsache, dass automatisierte Gesichtserkennung keineswegs eine neue Technologie ist. Vielmehr hat sie eine bereits über

3 Max-Planck-Institut für Bildungsforschung: Unstatistik des Monats. „Erfolgreiche“ Gesichtserkennung mit Hunderttausenden Fehlalarmen, Meldung v. 30.10.2018, (www.mpib-berlin.mpg.de/unstatistik-gesichtserkennung-mit-fehlalarm)

4 Bundesministerium des Innern: Pressemitteilung v. 11.10.2018 (www.bmi.bund.de)

fünfzigjährige Geschichte – eine Geschichte, die weithin unbekannt ist, die aber Schlaglichter auf die Gegenwart wirft. Diese Geschichte soll im Folgenden knapp skizziert werden.[5]

Von der Bertillonage zur „Videodatenverarbeitung"

Die ersten Versuche mit automatisierter Gesichtserkennung datieren bereits aus den 1960er Jahren. Als Pionier des Feldes kann der amerikanische Mathematiker Woody Bledsoe gelten, der um 1963 im Auftrag der CIA damit begann, den Einsatz von Computern bei der Identifizierung menschlicher Gesichter zu erforschen. Als Vorbild diente ihm das anthropometrische Signalement des französischen Kriminalisten Alphonse Bertillon, ein Mess- und Beschreibungsverfahren, das in den 1880er Jahren zur Identifizierung von Wiederholungstätern entwickelt worden war. Die vollständige Automatisierung der Gesichtsvermessung gelang Bledsoe jedoch nicht – vielmehr schlug er seinen Auftraggebern ein „Mensch-Maschine-System" mit klarer Kompetenzverteilung vor: Menschliche *operators* sollten zunächst auf polizeilichen Fahndungsbildern vorgegebene Merkmalspunkte wie Augen- und Mundwinkel, Nasen- und Kinnspitze markieren. Deren digital erfasste Koordinaten konnten anschließend vom Computer mit den bereits zuvor erfassten Datenbeständen abgeglichen werden. Der Computer blieb also in dieser frühesten Versuchsanordnung noch blind und war für den Dateninput auf menschliche Augenpaare angewiesen.

Während Bledsoes Arbeit, den Interessen seines Auftraggebers geschuldet, im Geheimen stattfand, suchten andere Forscher die Öffentlichkeit. So bewarb die *Nippon Electric Company* ihre neuartige Technologie der „Videodatenverarbeitung" 1970 auf der Weltausstellung im japanischen Osaka mit einem ganz besonderen Spektakel namens „Computer Physiognomy". Wer wollte, konnte hier sein Gesicht elektronisch erfassen lassen und erhielt als Andenken nicht nur ein ausgedrucktes Computerporträt, sondern auch eine spezielle Form der automatisierten Charakterdeutung. Auf Basis messbarer Ähnlichkeiten sollte der Rechner nämlich jedes erfasste Gesicht einem „Typus" zuordnen, der von jeweils einem von insgesamt sieben Prominentengesichtern repräsen-

5 Die folgenden Ausführungen basieren auf meinem Buch: Operative Porträts. Eine Bildgeschichte der Identifizierbarkeit, Konstanz 2019. Dort finden sich auch alle weiteren Quellen und ausführliche Nachweise.

tiert wurde – von Winston Churchill über John F. Kennedy bis zu Marylin Monroe. Doch nach welchen Kriterien die Zuordnung erfolgte, erfuhr das Publikum nicht. Gesichtserkennung, das gilt bis heute, präsentiert sich in der Regel als *black box*, deren Funktionsweise strukturell im Verborgenen bleibt – der Öffentlichkeit gegenüber ebenso wie nicht selten sogar jenen, die sie einsetzen: In diesem Fall mussten die beteiligten Wissenschaftler erst in der nachträglichen Datenanalyse erfahren, dass die Ergebnisse ihres fehleranfälligen Programms häufig reine Zufallsprodukte waren.

Das Experiment von Osaka erwies sich dennoch als folgenreich. Denn auf Basis der hier erhobenen Gesichtsdaten entwickelte der junge japanische Informatiker Takeo Kanade in seiner Dissertation von 1973 das erste Verfahren, das ohne menschliche Eingabehilfen auskam. Auch Kanade setzte auf die digitale Vermessung des Gesichts, doch Brillen, Bärte und Falten im Gesicht verwirrten sein System und machten die Lokalisierung von Merkmalspunkten wie Augen- oder Mundwinkeln schwierig. Als Testbilder verwendete er daher ausschließlich solche junger, bart- wie brillenloser, zudem überwiegend männlicher japanischer Gesichter, doch selbst die wurden nur in rund dreiviertel aller Fälle erkannt. Gesichtserkennung, auch das gilt bis heute, etabliert stets Standards der Erkennbarkeit, die nicht von jedem Gesicht gleichermaßen erfüllt werden.

Im Laufe der 1970er Jahre begann man vielerorts, an Verfahren der automatisierten Gesichtserkennung zu arbeiten – unter anderem auch am Bundeskriminalamt in Wiesbaden. Als Ziel schwebte BKA-Chef Horst Herold ein „Personenerkennungssystem“ vor, das alles objektiv messbar und vergleichbar machen sollte, was bislang der menschlichen Wahrnehmung vorbehalten gewesen war. In Zukunft könnten dann mittels Videotechnik, Datenverarbeitung und anderer Medien „alle Merkmale der Individualität“, einschließlich Mimik, Gang- und Stimmmustern, automatisch erfasst und ausgewertet werden. Doch wie andere Technologien, deren Entwicklung das BKA im Kampf gegen den RAF-Terrorismus mit großem Aufwand betrieb, kam die elektronische Personenerkennung nie über den Stand der Grundlagenforschung hinaus.

Fiction & Science

Auch international stagnierte in den 1980er Jahren die Forschung – zu viele Probleme schienen ungelöst, als dass in absehbarer Zeit mit einem

praxistauglichen Verfahren zu rechnen gewesen wäre. Als einsatzfähig erwies sich die Technologie allein im Reich der Fiktion. Insbesondere die Filme der James-Bond-Reihe führten seit den 1980er Jahren regelmäßig immer elaboriertere Formen der elektronischen Identifizierung vor. In *A View to a Kill* (1986) ist es ausgerechnet der Schurke Zorkin, der eine in seinem Arbeitszimmer versteckte Kamera nutzt, um den inkognito auftretenden Bond zu identifizieren. Während Zorkin sich noch mit seinem verdächtigen Gast unterhält, lässt er heimlich dessen digitales Überwachungsbild von seinem PC auswerten, der ihm schließlich verrät, mit wem er es in Wahrheit zu tun hat.

Den Einfluss der filmischen Fiktion auf die Realität sollte man nicht unterschätzen. So ist überliefert, dass die CIA regelmäßig, wenn einer neuer Bond in die Kinos kam, die dort vorgeführten Gadgets durch ihre technische Abteilung auf ihre Realisierbarkeit hin prüfen ließ. Vor allem aber prägten die Hollywoodfantasien der perfekten technischen Überwachung, wie sie seit den 1990er Jahren entstanden, populäre Vorstellungen technischer Machbarkeit. Filme wie etwa *Enemy of the State* (1998) zeichneten zwar ein düsteres Bild der Gefahren totaler Überwachung, doch die konkreten Schwachstellen der Technik sparten sie aus. Im Reich der Fiktion funktionierte die automatisierte Gesichtserkennung stets fehlerfrei.

Doch nicht nur Hollywood-Drehbuchautoren hielten in den späten 1990er Jahren automatisierte Gesichtserkennung für unmittelbar einsatzfähig. Tatsächlich hatte die Technologie mittlerweile die Entwicklungslabore verlassen. Der technische Durchbruch war 1991 gelungen, mit dem sogenannten *Eigenface*-Algorithmus der MIT-Forscher Matthew Turk und Alex Pentland. Anders als frühere merkmalsbasierte Verfahren setzten Turk und Pentland nicht auf die Vermessung der Anatomie des einzelnen Gesichts, sondern auf die statistische Auswertung von Helligkeitsverteilungen in großen Bilderdatenmengen. Dieser „holistische" Ansatz, ursprünglich im Auftrag eines Unternehmens entwickelt, das zur Messung von Einschaltquoten elektronisch erfassen wollte, wer gerade vor dem Fernseher saß, erwies sich als so erfolgreich, dass er in den 1990er Jahren einen wahren Forschungsboom auslöste.

In rascher Folge erschienen nun immer neue Erfolgsmeldungen aus den Computerlaboren amerikanischer Spitzenuniversitäten. Das Interesse auf Seiten von Militär und Sicherheitsbehörden war entsprechend groß. Doch da jedes Entwicklungsteam seine eigene Bilddatenbank verwendete, ließen sich die Erkennungsraten nicht vergleichen. Auf diesen

Mangel reagierte ab 1993 das FERET-Programm des US-Verteidigungsministeriums. Mit dem Aufbau einer einheitlichen Bilddatenbank sollte nun erstmals ein standardisierter Leistungsvergleich möglich werden. Dieser fand zwischen 1994 und 1996 in drei Phasen statt, bei denen jeweils die vielversprechendsten Teams auf Basis gemeinsamer Testaufgaben und Erfolgskriterien miteinander konkurrierten. Zwar stellte sich heraus, dass wechselnde Lichtverhältnisse, zeitliche Abstände zwischen den Aufnahmen und anderes mehr die Systeme unverändert vor große Herausforderungen stellten, doch allein die im Jahresrhythmus messbaren Fortschritte bestätigten die Beteiligten im Glauben an die bevorstehende Marktreife. Und so begann mit den FERET-Tests die Kommerzialisierung der Technologie, nutzten doch manche der beteiligten Forscher*innen die staatlich beglaubigten Testergebnisse, um Risikokapital für ihre neugegründeten Start-up-Firmen einzuwerben, die fortan Casinos, Flughäfen, Führerscheinstellen und Polizeibehörden mit Gesichtserkennungssoftware ausstatten sollten.

Ein öffentlichkeitswirksamer Coup gelang im Januar 2001 der Firma *Viisage*, die sich die Rechte am *Eigenface*-Algorithmus gesichert hatte: Mit ihrer Software wurden die Gesichter von über 70.000 Besucher*innen des Super-Bowl-Finales in Tampa (Florida) automatisch erfasst und mit polizeilichen Fahndungslisten abgeglichen. Obwohl keine Verhaftung erfolgte und unklar blieb, ob die Software überhaupt einen einzigen korrekten Treffer gelandet hatte, verbuchten die Beteiligten den Einsatz als Erfolg. Der größte Konkurrent von *Viisage*, nämlich *Visionics*, bot nun ebenfalls den Behörden von Tampa seine Dienste an, um im Sommer 2001 eine bestehende Videoüberwachungsanlage in der Innenstadt zum „Smart CCTV" aufzurüsten. Doch erwies sich die Technik als wenig „smart": Es häuften sich Fehlalarme, und nach wenigen Wochen Laufzeit schaltete die Polizei das Programm ab – ohne die Öffentlichkeit darüber zu informieren.[6]

Nach dem 11. September 2001

Derweil hatte *Visionics* längst einen größeren Markt anvisiert. Nur 14 Tage nach den Anschlägen vom 11. September veröffentlichte die Firma ein *white paper* mit dem Titel: „Protecting Civilization from the Faces of

6 vgl. Gates, K. A.: Our Biometric Future. Facial Recognition Technology and the Culture of Surveillance, New York; London 2011, S. 63–96

Terror“, das für die landesweite Aufrüstung aller Flughäfen mit Gesichtserkennung plädierte. Ausgerechnet jene Technologie, die wenige Wochen zuvor in Florida ebenso spektakulär wie von der Öffentlichkeit unbemerkt versagt hatte, hätte, so wurde dort suggeriert, die Terroristen rechtzeitig stoppen können. Mit der Wirklichkeit hatten solche Argumente nur wenig zu tun – nicht zuletzt, weil Mohammed Atta und seine Mittäter gar nicht unter falschem Namen oder mit gefälschten Papieren reisten. Für die biometrische Industrie markierte 9/11 dennoch einen „Paradigmenwechsel“. Bislang, so formulierte es im Februar 2002 der CEO von Visionics, Joseph J. Atick, in seiner Eröffnungsansprache zur Jahreskonferenz des *Biometric Consortiums*, hätte man mit „Privatsphärebedenken, Mangel als politischem Willen, unzureichender Finanzierung, fehlender Infrastruktur“ zu kämpfen gehabt – all dies wäre nun wie weggewischt.

In den Fokus rückte nach 9/11, etwa mit dem Programm „US-VISIT“ (ab 2005), vor allem die massive biometrische Aufrüstung der Grenzen. Zunächst nur ausgewählte Reisende aus islamischen Ländern, später dann fast alle, die mit Visum in die USA einreisten, wurden nun bei Ein- und Ausreise digital fotografiert und per Scanner daktyloskopisch erfasst. Zugleich wurde der Grenzübergang zur Datensammelstelle: Allein bis 2012 wurden so über 130 Millionen Nicht-US-Bürger*innen in den Datenbanken des Heimatschutzministeriums erfasst, wo ihre Daten bis zu 75 Jahre lang gespeichert werden. Parallel zur Reform der Einreisebestimmungen drängten die USA jene Staaten, deren Bürger*innen bislang ohne Visum einreisen konnten – darunter die Länder der EU –, zur Einführung „maschinenlesbarer“ Reisepässe, die die Speicherung biometrischer Daten erlauben. Mit allzu großem Widerstand mussten sie nicht rechnen. Denn auch hierzulande verknüpfte man nicht allein Sicherheits-, sondern auch ökonomische Interessen mit dem neuen biometrischen Passregime: „Die Pässe“, so formulierte es Otto Schily, Bundesinnenminister und später in den Aufsichtsräten gleich zweier Biometrie-Unternehmen aktiv, „sind auch ein Wirtschaftsfaktor. Wir zeigen, dass Deutschland das Knowhow und die Innovationskraft hat, um im jungen Sektor Biometrie Standards zu setzen.“

Die Einführung der e-Pässe in den 2000er Jahren war mithin auch eine staatliche Fördermaßnahme für die „Zukunftsbranche“ Biometrie. Nicht zuletzt boten Grenzkontrollen ideale Einsatzbedingungen für deren immer noch fehleranfällige Technologie: Stabile Umweltbedingungen, überwiegend kooperative Individuen sowie auch technisch relativ

einfach zu lösende Aufgaben. Denn die Verifikation, also der 1:1-Vergleich der Merkmale bei der Passkontrolle, ist weit unkomplizierter als etwa der Abgleich eines unbekannten Gesichts in der Menge mit großen Mengen von Fahndungsbildern. Aus Sicht der Sicherheitsbehörden war jedoch letzteres nach wie vor die eigentliche Herausforderung. Insbesondere mit dem Ausbau der Videoüberwachung im öffentlichen Raum gewann die Idee, den kaum mehr von menschlichen Augen überschaubaren Bilderstrom elektronisch auszuwerten, an Fürsprecher*innen. Auch das BKA wurde wieder aktiv. Im Oktober 2006 startete man im Mainzer Hauptbahnhof einen viermonatigen Testlauf der automatisierten „Foto-Fahndung". Ähnlich wie jüngst am Südkreuz waren auch hier die Gesichter von Freiwilligen zuvor gescannt worden – und sollten nun von „smarten" Überwachungskameras im täglichen Pendlerstrom identifiziert werden. Das Ergebnis: Die Trefferraten im Feldversuch entsprachen nicht annähernd jenen, mit denen die Hersteller der Systeme warben, und waren für den praktischen Einsatz völlig ungenügend. In der öffentlichen Berichterstattung jedoch wurde der Testlauf als erfolgreiches Pilotprojekt dargestellt – der flächendeckende Einsatz der Technologie stand, wieder einmal, unmittelbar bevor.[7]

Die neuen Player

Bis weit in die Nullerjahre war automatisierte Gesichtserkennung vor allem eine Sache spezialisierter Firmen der Sicherheitsbranche. Seit rund zehn Jahren allerdings drängen ganz neue Player auf den Markt – nicht zuletzt die Internetgiganten Facebook, Google und Amazon. Auch aus Angst vor neuer Konkurrenz warnte schon 2011 der bereits zitierte Joseph J. Atick vor einem „perfekten Sturm", der sich durch die Konvergenz von Smartphones, Social Media und Künstlichen Neuronalen Netzen ankündigte und Bürgerrechte in nie gekanntem Ausmaß bedrohte. Die Milliarden bereits namentlich identifizierbarer Bilder von Gesichtern, die mittlerweile online verfügbar waren, boten ideale Trainings- und Testbedingungen für neuartige Gesichtserkennungsalgorithmen, die nicht mehr auf vorgegebene Regeln der Auswertung, sondern auf *machine learning* setzten. Nicht zufällig können sich soziale Netzwerke wie Facebook mittlerweile der leistungsfähigsten Algorithmen der Bilderkennung

7 vgl. Kammerer, D.: Bilder der Überwachung, Frankfurt a.M. 2008, S. 216–226

rühmen – denn jedes Mal, wenn jemand ein Bild von sich hochlädt oder eine*n Bekannte*n auf einem Foto erkennt und taggt, wirkt er oder sie am Aufbau von Facebooks Bilddatenbanken und damit indirekt auch am Training seiner Algorithmen mit. Bilder von Gesichtern sind damit zur wertvollen Datenressource geworden – und zum Anker, der es erlaubt, beliebige Aufnahmen ein und derselben Person, in ganz unterschiedlichen Kontexten und selbst ohne deren Wissen erstellt, miteinander zu verknüpfen. Das Beispiel *Clearview*, das seinen Kund*innen – darunter Polizeibehörden ebenso wie Unternehmen und sogar Privatleute – verspricht, jedes beliebige Gesicht innerhalb von Sekunden im Abgleich mit Milliarden von Bildern aus sozialen Netzwerken zu identifizieren, zeigt, dass der „perfekte Sturm" längst Realität ist.

Lehren aus der Geschichte

Was lässt sich angesichts dessen aus der Geschichte, die hier skizziert wurde, lernen? Automatisierte Gesichtserkennung ist nicht über Nacht zum Thema geworden – sie wurde über Jahrzehnte massiv gefördert, in einer konzertierten Anstrengung staatlicher Behörden und kommerzieller Unternehmen, begleitet von einem populären Diskurs, der selbst, wo er sich technikkritisch gab, viele konkrete Probleme der Technologie ausblendete. Die Geschichte der automatisierten Gesichtserkennung ist eine Geschichte der gescheiterten Feldversuche und Testläufe – die in immer größeren Maßstäben durchgeführt werden, aber praktisch nie die Versprechen erfüllen, die Politik und Medien an sie knüpfen. Und dennoch ist sie eine Geschichte der Erfolgsmeldungen – weil das Interesse, auch problematische Ergebnisse als Erfolge zu verkaufen, einfach zu stark war.

Und die Probleme lagen und liegen nicht allein in den Fehlerraten. Völlig ungelöst ist auch ein Problem, mit dem schon Takeo Kanade in den 1970er Jahren zu tun hatte: Selbst die neueste Software erkennt nicht jedes Gesicht mit der gleichen Zuverlässigkeit, vielmehr werden gerade Menschen mit dunklerer Hautfarbe schlechter erkannt als solche mit hellerer Haut. Der flächendeckende Einsatz von Gesichtserken-

nungssoftware, das zeichnet sich jetzt schon in den USA ab, führt mithin zur Verstärkung bestehender polizeilicher Diskriminierung.[8]

Und nicht zuletzt, das zeigt das Beispiel *Clearview*, scheint eine Kontrolle des Einsatzes der Technologie immer schwerer möglich – mit noch unabsehbaren Folgen. Was die Geschichte uns aber definitiv nicht lehren sollte, ist, dass die hier beschriebenen Entwicklungen zwangsläufig seien. Technik ist kein Schicksal, und es ist noch nicht zu spät, eine gesellschaftliche Diskussion zu beginnen, ob und unter welchen Bedingungen automatisierte Gesichtserkennung künftig unseren Alltag bestimmen soll.

8 Dieses Problem wird unter dem Stichwort *algorithmic bias* diskutiert, eine aktuelle Einführung in die Debatte liefert: Benjamin, R.: Race After Technology: Abolitionist Tools for the New Jim Code, Cambridge 2019

220 Abfragen pro Sekunde

Das Schengener Informationssystem wächst dynamisch

von Matthias Monroy

Die größte europäische Fahndungsdatenbank ist in den letzten Jahren ausgebaut worden. Die Zahl der Speicherungen und Abfragen steigt deutlich. Jetzt werden schrittweise weitere Funktionen eingeführt, und der Kreis der Zugriffsberechtigten wird erweitert.

Das Schengener Informationssystem (SIS) wird seit 25 Jahren von Grenz-, Polizei-, Zoll- oder Ausländerbehörden genutzt, auch Geheimdienste greifen lesend und schreibend zu. Am heutigen SIS II sind 26 EU-Mitgliedstaaten (alle außer Irland und Zypern) sowie Island, Norwegen, Liechtenstein und die Schweiz beteiligt. Obwohl Einträge in der größten europäischen Fahndungsdatenbank einer Speicherfrist unterliegen, nimmt ihre Zahl deutlich zu. Zum 1. Januar 2020 waren mehr als 90 Millionen Personen und Gegenstände im SIS II gespeichert.[1] 2018 waren es noch 82 Millionen, 2017 etwa 76 Millionen. Die meisten Einträge (rund 22 Millionen) kamen 2018 aus Italien, gefolgt von Frankreich (15 Millionen) und Deutschland (fast 12 Millionen).[2]

Die Zahl der Abfragen steigt ebenfalls: 2018 haben über sechs Milliarden Zugriffe rund 267.000 Ergebnisse erzielt (jede 22.000 Abfrage ein „Treffer"), im letzten Jahr soll es fast sieben Milliarden Suchläufe gegeben haben. Diese Angaben stammen aus Statistiken, die Anfang jedes Jahres von der Europäischen Agentur für das Betriebsmanagement von IT-Großsystemen (eu-LISA) veröffentlicht werden.[3] Die Agentur mit Sitz

1 jüngste Angaben: BT-Drs. 19/16723 v. 23.1.2020, frühere Zahlen: SIS II wächst kontinuierlich in: Bürgerrechte & Polizei/CILIP 116 (Juli 2018), S. 93f.
2 2017: Italien 20 Mio. Einträge, Frankreich 11 Mio., Deutschland über 10 Mio.
3 www.eulisa.europa.eu/Activities/Large-Scale-It-Systems/Sis-II

in Tallinn (Estland) ist seit 2013, seit dem Abschluss der sechs Jahre dauernden Migration des SIS zum SIS II, für das System verantwortlich.[4]

Fast 99 Prozent aller SIS-Ausschreibungen sind Sachfahndungen. Bei rund drei Viertel davon geht es um als gestohlen oder vermisst gemeldete Ausweispapiere. An zweiter Stelle folgen Daten über gestohlene, verlorene oder für ungültig erklärte Wertpapiere und Zahlungsmittel. Fünf Prozent beziehen sich auf gestohlene Fahrzeuge, darunter auch Boote und Flugzeuge.

Personenfahndungen bilden mit rund 983.000 den kleineren Teil der Einträge. Über die Hälfte sind Aufenthaltsverweigerungen oder Einreisesperren nach Artikel 24 des SIS-II-Ratsbeschlusses. An zweiter Stelle steht der Artikel 36, mit dem im Dezember 2019 rund 207.000 Personen zur „verdeckten" oder zur „gezielten Kontrolle" ausgeschrieben waren (2018: 156.534). An dritter Stelle stehen Aufenthaltsermittlungen nach Artikel 34 von Beschuldigten oder Zeug*innen, die in einem Strafverfahren vor Gericht aussagen oder denen Schriftstücke zugestellt werden sollen. Mit Artikel 32 wurde 2018 mithilfe des SIS II nach rund 77.500 vermissten Jugendlichen und 38.000 Erwachsenen gesucht. Schlusslicht sind die rund 39.000 Europäischen Haftbefehle.

Möglich sind auch Ausschreibungen aus Drittstaaten. Diese „Fremdspeicherungen" müssen von einem regulären SIS-Teilnehmer vorgenommen werden. Tschechien übernimmt beispielsweise geheimdienstliche Ausschreibungen zur verdeckten Kontrolle (Artikel 36 Absatz 3) von Nicht-EU-Staaten des Westbalkans.[5] Unklar ist, wie die tschechischen Behörden prüfen, ob die Voraussetzungen für eine Speicherung vorliegen oder ob die Daten womöglich wieder gelöscht werden müssen. Mittlerweile dürften im SIS auch Ausschreibungen zu finden sein, die aus „Gefechtsfeldinformationen" stammen, die US-Behörden in Syrien oder dem Irak einsammeln. Dies hatte die finnische Ratspräsidentschaft in einer gemeinsamen Sitzung der Ratsarbeitsgruppen „Terrorismus", „Schengen Angelegenheiten" und „SIS/SIRENE" im Sommer vergangenen Jahres für die Verfolgung „ausländischer terroristischer Kämpfer" angeregt.[6]

4 „Schengener Informationssystem (SIS II) geht in Betrieb", Pressemitteilung EU-Kommission v. 9.4.2013

5 EU-observer v. 12.2.2020 (https://euobserver.com/justice/147420)

6 BT-Drs. 19/14653 v. 31.10.2019, vgl. auch BT-Drs. 19/10080 v. 10.5.2019

Upgrade für biometrische Daten

Seit zwei Jahren können die SIS-Teilnehmer mit einem Automatisierten Fingerabdruck-Identifizierungssystem (AFIS) auch die im SIS gespeicherten Fingerabdrücke durchsuchen. Nach Angaben des Bundesinnenministeriums (BMI) machen derzeit Behörden aus zehn Ländern von dieser Möglichkeit Gebrauch.[7] Auf diese Weise können etwa Tatortspuren unbekannter Verdächtiger mit SIS II-Fingerabdruckdaten bekannter Personen abgeglichen werden. Nach einem Upgrade ist es außerdem möglich, sogenannte Slaps zu durchsuchen.[8] Dabei handelt es sich um „flache Fingerabdrücke", wie sie demnächst im Rahmen des neuen „Einreise-/Ausreisesystems" (EES) mit Selbstbedienungskiosken an allen EU-Außengrenzen abgenommen werden. Auch Gesichtsbilder oder DNA-Daten können zu „Identifizierungszwecken" im SIS II gespeichert werden, sie sind aber noch nicht durchsuchbar.[9]

Seit der Einrichtung des Fingerabdrucksystems im Jahre 2018 hat sich die Zahl der dort gespeicherten „Fingerabdruckblätter" auf rund 273.000 verdreifacht. Davon wurden rund 56.000 von deutschen Kriminalämtern eingegeben. Auch die biometrischen Suchläufe nehmen deutlich zu. Allein die deutschen Behörden haben 2019 über 9.000 „Treffer" erzielt, etwa viermal mehr als 2018. Der Präsident des Bundeskriminalamtes (BKA), Holger Münch, beschreibt die neue Ermittlungsmaßnahme deshalb als „sehr erfolgreich".[10]

Drei neue Verordnungen

Jetzt erhält das SIS II weitere neue Funktionen. Dafür hat die EU Ende 2018 drei neue Verordnungen beschlossen, die nun unter Aufsicht der Ratsarbeitsgruppe „Schengen-Angelegenheiten" in mehreren Phasen umgesetzt werden.[11] Nach einem Jahr sollen Europol und Frontex über

7 Deutschland, Italien, Lettland, Liechtenstein, Luxemburg, Malta, Niederlande, Portugal, Slowenien, Ungarn. Laut dem von Statewatch veröffentlichten Ratsdok. 5618/20 v. 18.2.2020 wird die AFIS-Suchfunktionalität nicht nur von zehn, sondern von 15 Ländern genutzt, deutsche Behörden verfügen demnach über eine „Schnellsuchfunktion".

8 „New SIS II Release Successfully Deployed", Pressemitteilung eu-LISA v. 10.1.2020

9 Derzeit befinden sich im SIS II Lichtbilder zu 63.447 Personen, zur Anzahl bereits gespeicherter DNA-Daten macht die Bundesregierung keine Angaben.

10 „BKA-Chef sieht Fortschritt beim EU-Datentausch", Hamburger Abendblatt v. 1.2.2020

11 Verordnungen über die Nutzung des SIS für die Rückführung von illegal aufhältigen Drittstaatsangehörigen (2018/1860), für den Bereich der Grenzkontrollen (2018/1861)

einen vollen Zugang zum SIS II verfügen. Nach weiteren zwei Jahren müssen alle SIS-Teilnehmer das AFIS obligatorisch eingeführt haben. Alle übrigen Bestimmungen der drei Verordnungen sollen dann innerhalb von drei Jahren erfüllt werden.

Europol darf künftig nicht nur Ergebnisse von Ausschreibungen im SIS II auswerten, sondern auch zusätzliche Informationen mit den Mitgliedstaaten austauschen. Die nationalen Behörden müssen Europol außerdem informieren, wenn zu einer Person im Zusammenhang mit einer terroristischen Straftat im eigenen Vorgangsbearbeitungssystem ein Treffer erzielt wurde. Das bei Europol angesiedelte Europäische Zentrum zur Terrorismusbekämpfung (ECTC) prüft dann, ob in den Europol-Dateien weitere Informationen zu der Person vorliegen.

Neu ist ferner, dass Entscheidungen zur „Rückführung" von „illegal aufhältigen Drittstaatsangehörigen" ins SIS II eingegeben werden können. Die Speicherung von Einreiseverboten nach einer vollzogenen Abschiebung wird jetzt verpflichtend. Kinder können „präventiv" ausgeschrieben werden, wenn sie von Entführung durch ein Elternteil bedroht sind. Weitere Kategorien gibt es zu Personen, die „zu ihrem eigenen Schutz" an einer Reise gehindert werden sollen – etwa Minderjährige, denen eine Zwangsheirat oder die Genitalverstümmelung droht, oder Erwachsene, die von Menschenhandel bedroht sind. Ausgeweitet wurde zudem die Liste der Sachen, nach denen per SIS II gesucht werden kann.

Neue Möglichkeiten gibt es auch für das AFIS. Dort kann im Falle schwerer Straftaten oder „terroristischer Zwischenfälle" künftig nach Finger- oder Handballenabdrücken unbekannter Tatverdächtiger gefahndet werden. Die ausschreibende Stelle erhält eine Nachricht, wenn eine andere Polizei oder ein anderer Geheimdienst die gleichen Abdrücke ins SIS II eingibt. Diese Funktion wird derzeit noch nicht genutzt; laut Artikel 79 der Verordnung 2018/1862 muss die EU-Kommission in den nächsten zwei Jahren über den Start entscheiden. Derzeit untersucht eu-LISA, ob in allen nationalen Kontaktstellen (den sogenannten SIRENE-Büros) die technischen Voraussetzungen vorliegen.

Neben dem technischen Upgrade des SIS II wird auch die Steuerung für das Informationssystem umgebaut. Die Ratsarbeitsgruppe „SIS/SIRENE", die derzeit SIS-Angelegenheiten behandelt, soll aufgelöst

---

und im Bereich der polizeilichen und justiziellen Zusammenarbeit in Strafsachen (2018/1862), alle im Amtsblatt der EU (Abl. EU) L 312 v. 7.12.2018

werden. Sie wird in die Arbeitsgruppe „Informationsaustausch und Datenschutz“ (DAPIX) eingegliedert, aus der jedoch der Datenschutz herausgelöst und ebenfalls einer eigenen, neuen Gruppe überantwortet wird. Das neue Gebilde firmiert dann als Arbeitsgruppe „Informationsaustausch“ (IXIM).

„Projekt SIS 3.0“

Beim BKA firmiert die Umsetzung der drei neuen SIS-Verordnungen als „Projekt SIS 3.0“, das Amt veranschlagt hierfür bis 2024 rund 68,5 Millionen Euro. Die Bundesregierung will zusätzliche zehn Millionen Euro aus dem EU-Fonds für die Innere Sicherheit (ISF) abrufen. Weitere Kosten entstehen im Rahmen des Projekts „Interoperabilität“, mit dem die Informationssysteme der Europäischen Union neu geordnet werden. Die im SIS II, dem Visa-Informationssystem (VIS) und der Fingerabdruckdatei Eurodac gespeicherten Fingerabdrücke und Gesichtsbilder werden mit den dazugehörigen Personendaten in einem „Gemeinsamen Identitätsspeicher“ abgelegt. Hinzu kommen biometrische Daten aus dem Strafregister ECRIS und dem noch zu errichtenden „Ein-/Ausreisesystem“. Ebenfalls geplant ist ein „gemeinsamer Dienst für den Abgleich biometrischer Daten“, der jeden neuen Eintrag mit bereits vorhandenen Daten überprüft.

Das BMI bewertet die Umsetzung der „Interoperabilitäts“-Verordnungen als „insgesamt hochkomplex“.[12] Allein auf EU-Ebene müssen hierfür bis zu 70 Rechtsakte beschlossen oder erneuert werden. Derzeit liegt die EU-Kommission weitgehend im Zeitplan, laut BMI seien aber „Interdependenzen nicht auszuschließen“. Der Grund sind neue Verordnungen für VIS und Eurodac, die derzeit vom Rat, der Kommission und dem Parlament beraten werden. Im Falle von Eurodac blockiert das EU-Parlament seit 2016 die Vorschläge des Rates und knüpft seine Zustimmung an Verhandlungen zur Reform des Gemeinsamen Europäischen Asylsystems.

Großbritannien und das SIS

Der „Brexit“ bringt auch Probleme für das SIS. Erst 2015 hat die EU-Kommission den britischen Behörden den Zugang zum SIS II gewährt.

12 BT-Drs. 19/15608 v. 29.11.2019

Das Land ist aber nicht Mitglied des Schengener Abkommens, das die Abschaffung der Grenzkontrollen innerhalb der EU regelt, und setzte auch die Freizügigkeit nicht um. Deshalb dürfen britische Behörden keine Daten eingeben oder abfragen, die etwa irreguläre Migration betreffen.

Der vor fünf Jahren vollzogene Anschluss an das SIS II war vorläufig, der endgültige Beitritt sollte erst erfolgen, nachdem die Kommission die Umsetzung der geltenden SIS-Verordnung überprüft hat. Bei einer ersten Evaluierung 2015 zeigten sich laut dem Bewertungsausschuss zahlreiche Mängel. Wenige Monate später hat der Rat der EU deshalb in seinen Schlussfolgerungen eine weitere Überprüfung gefordert. Ein solcher Besuch erfolgte jedoch erst zwei Jahre später. Der Grund für die Verzögerung war ein neuer EU-Beschluss zur Schengen-Bewertung.[13] Demnach muss jedes teilnehmende Land künftig alle fünf Jahre eine solche Prozedur über sich ergehen lassen. Zuständig sind die Kommission und (in einem rotierenden Verfahren) die Schengen-Mitgliedstaaten.[14]

Die zweite Schengen-Überprüfung in Großbritannien erfolgte gemäß dem neuen Mechanismus. Der daraus folgende Evaluierungsbericht[15] dokumentiert erneut zahlreiche Versäumnisse und Verstöße. Auch nach dem ersten Kontrollbesuch 2015 seien „größere Mängel" nicht abgestellt worden. Britische Behörden verfügen demnach über „eine beträchtliche Anzahl vollständiger oder teilweiser Kopien" des SIS II. Das ist nicht ungewöhnlich, denn die SIRENE-Büros dürfen Backups anlegen oder Spiegelungen der Daten aufbewahren. So argumentiert auch die Kommission in der Antwort auf eine parlamentarische Anfrage.[16] Einige der britischen Kopien liegen jedoch in den Räumen von privaten IT-Dienstleistern, die die britische Regierung mit dem Betrieb des SIS II und anderer, angeschlossener Datenbanken beauftragt hat.[17] Dies widerspricht den Schengen-Regeln. Die Daten werden außerdem in nationale Datenbanken kopiert, etwa in die britische Warndatei („Warning Index"). In einigen Fällen sollen sich sogar SIS-Daten auf Laptops befinden.

13 Verordnung (EU) Nr. 1053/2013, Abl. EU L 295 v. 6.11.2013
14 2020 wird dieser Bewertungs- und Überwachungsmechanismus selbst evaluiert – ein übliches Verfahren bei neuen EU-Gesetzesakten; vgl. BT-Drs. 19/13990 v. 14.10.2019
15 https://twitter.com/NikolajNielsen/status/1203944161961021440
16 www.europarl.europa.eu/doceo/document/E-9-2019-002611-ASW_DE.pdf
17 ATOS aus Frankreich, IBM aus den USA und CGI aus Kanada

Zu den Prinzipien des SIS II gehört die Gegenseitigkeit und die gegenseitige Anerkennung. Alle teilnehmenden Staaten sollen Einträge aus anderen Ländern wie eigene behandeln. Die EU-Prüfer*innen haben den britischen Behörden 2015 und 2017 allerdings eine „begrenzte Reziprozität" attestiert. So werden etwa von den assoziierten Schengen-Ländern herausgegebene Auslieferungsersuchen nicht umgesetzt. Auch Haftbefehle aus EU-Mitgliedstaaten werden erst nach einer teils langwierigen Validierung in britische Systeme übernommen, eine „hohe Zahl" werde erst gar nicht anerkannt. Ähnlich nachlässig sind britische Beamt*innen laut dem Prüfbericht mit der Sachfahndung. So würden beispielsweise Fahrzeuge, die in einem anderen Mitgliedstaat gestohlen wurden, in Großbritannien nicht beschlagnahmt.

Großbritannien hat zwar vergleichsweise wenige Ausschreibungen ins SIS eingegeben, liegt aber bei Abfragen auf den vorderen Plätzen. 2016 führten britische Behörden rund 500 Millionen Abfragen durch, die zweithöchste Zahl unter den Mitgliedstaaten. Die Abfragen von Behörden anderer Schengen-Staaten in den britischen Ausschreibungen ergaben im selben Jahr aber nicht einmal 10.000 Treffer. Der Prüfbericht bezeichnet dieses Verhältnis als „nicht angemessen". Von den fast eine Million Personenfahndungen im SIS II stammen nur rund 37.000 aus Großbritannien. Das ist zwar ein eher niedriger Wert. Bei über der Hälfte dieser Einträge handelt es sich jedoch um Ausschreibungen zur verdeckten Kontrolle nach Artikel 36. Bei diesen heimlichen Fahndungen liegt Großbritannien im SIS II auf Platz drei nach Frankreich und Italien.

Trotz der hohen Anzahl eigener Fahndungen gemäß Artikel 36 behalten britische Behörden die Treffer nach Ausschreibungen aus anderen Ländern offenbar zunächst für sich. Erst wenn eigene Geheimdienste eine Überprüfung vorgenommen und die Informationen freigegeben haben, wird die Behörde des anderen Landes benachrichtigt. Dies erfolgt laut der Schengen-Evaluierung sogar bei Ausschreibungen mit dem Zusatz „unverzügliche Meldung", der nach den terroristischen Anschlägen 2015 in Frankreich im SIS II eingerichtet wurde.

„Sicherheitspartnerschaft" mit Großbritannien?

Ein Schengen-Staat, der die Regeln des SIS II nicht umsetzt, müsste eigentlich von der Zusammenarbeit ausgeschlossen werden. Nach den Evaluierungen von 2015 und 2017 stand tatsächlich zur Debatte, Großbritannien abzukoppeln. Die Regierungen der EU-Mitgliedstaaten ent-

schieden jedoch im Sommer 2018, das Evaluierungsverfahren trotz der „sehr schweren Mängel“ weiterzuführen.[18] Mit dem Beginn der „Brexit“-Verhandlungen wurde die Evaluierung des SIS II jedoch wenige Monate nach dem Ratsbeschluss gestoppt.

Gemäß dem Austrittsabkommen zum „Brexit“ darf Großbritannien in der Übergangsphase bis zum 31. Dezember 2020 weiterhin an EU-Informationssystemen teilnehmen.[19] Das bedeutet jedoch, dass die Überprüfung der britischen Umsetzung des SIS II wieder aufgenommen werden muss. Die EU-Kommission hat deshalb Empfehlungen ausgesprochen, wie die Mängel behoben werden sollen. Am 5. März 2020 veröffentlichte der EU-Rat einen Durchführungsbeschluss mit 34 Forderungen an Großbritannien, den Missbrauch des SIS II zu beheben.[20] Das britische Innenministerium muss nun mitteilen, wie es die Probleme angehen will. Anderenfalls droht erneut die Abkopplung vom SIS II, womöglich sogar noch vor dem Brexit.

Vermutlich will die Regierung in London den Zugriff auf das wertvolle EU-Informationssystem behalten. Würde Großbritannien nach dem vollzogenen Austritt aber wieder Mitglied des SIS II, müsste sich das Land zur weiteren Evaluierung bereit erklären und unterläge auch EU-Datenschutzregeln. Alternativ könnte die EU für die Teilnahme als Drittstaat am SIS II einen neuen Rahmenbeschluss ähnlich der „Schwedischen Initiative“ erlassen. Zur Debatte steht auch, den SIS II-Informationsaustausch mit britischen Behörden über Europol abzuwickeln. Einzelheiten sollen nun in Verhandlungen über eine „Sicherheitspartnerschaft“ geklärt werden.[21]

18 Ratsdok. 11474/18 v. 1.8.2018 (www.statewatch.org/news/2018/aug/eu-council-uk-schengen-sis-11474-18.pdf)
19 https://eur-lex.europa.eu/content/news/Brexit-UK-withdrawal-from-the-eu.html
20 Ratsdokument 6554/20 v. 5.3.2020
21 s. die Empfehlungen der Kommission COM (2020) 35 final v. 3.2.2020, insb. Anhang, S. 21ff.

Geheimdienstgilde außer Kontrolle

Der Club de Berne

von Jan Jirát und Lorenz Naegeli

Offiziell gilt der Club de Berne als Zusammenschluss der europäischen Geheimdienste. Neue Dokumente zeigen, dass auch US-Dienste mitmischen und dass die Geheimdienstgilde mittlerweile eine eigene operative Plattform samt personenbezogener Datenbank führt – ohne demokratische Kontrolle.

Ein rotes Kreuz, 27 weiße Sterne und der Berner Bär: So sieht das Wappen des Club de Berne aus. Ein Wappen, das nie an die Öffentlichkeit hätte gelangen sollen. Doch im November 2019 publizierte „Österreich“[1] ein internes Dokument und bescherte dem ominösen Geheimdienstclub damit das größte Leck seiner Geschichte. Offizielle Informationen über den Club de Berne gibt es nur wenige. Und es sind stets dieselben: Ob in einem Budgetbericht des EU-Parlaments zu Antiterroraktivitäten von 2015[2] oder in einer Mitteilung des Schweizerischen Bundesamts für Polizei (Fedpol) vom April 2004:[3] Der Club de Berne ist stets als „informeller Club“ beschrieben, der die Geheimdienstchefs der EU-Staaten sowie der Schweiz und Norwegens zusammenbringe.

Doch kürzlich belegte die Schweizer Wochenzeitung WOZ, dass der Club de Berne weit mehr ist als ein harmloser Debattierclub der europäischen Geheimdienstchefs. Ein bisher unveröffentlichtes Dokument zeigt, dass zumindest noch 2011 unter anderen auch das FBI, die CIA sowie der israelische Auslandsgeheimdienst Mossad am Informations-

1 Alarm: Verfassungsschutz steht total blamiert da, oe24.at v. 11.11.2019

2 European Parliamentary Research Service: Counter-terrorism funding in the EU budget, Briefing, June 2015 (www.europarl.europa.eu/RegData/etudes/BRIE/2015/559490/EPRS_BRI(2015)559490_EN.pdf

3 Treffen des Club de Berne in der Schweiz, Fedpol-Medienmitteilung v. 28.4.2004 (www.fedpol.ch)

austausch im Club de Berne beteiligt waren.[4] Was aber sind Aufgabe und Zweck dieser Geheimdienstgilde? Was sind ihre Aktivitäten, und wie weit reicht ihr Einfluss? Vor allem aber: Wie ist es möglich, dass der Club de Berne auf europäischem Boden praktisch losgelöst von jeder demokratischen Kontrolle operieren kann?

Entdeckung im Schweizer Bundesarchiv

Die Schweizer Historikerin Aviva Guttmann hat sich im Rahmen ihrer Forschungsarbeit zur Schweizer Terrorabwehr intensiv mit der Gründungsphase des Club de Berne auseinandergesetzt.[5] Für ihre Forschung konnte Guttmann im Schweizer Bundesarchiv in Bern Akten einsehen und fand Erhellendes über den bis dahin öffentlich weitgehend unbekannten Club. Gegründet wurde er 1969 – mutmaßlich in Bern, einen genauen Hinweis darauf fand Guttmann nicht – als Forum, in dessen Rahmen sich fortan zweimal jährlich die Chefs der neun Geheimdienste aus Belgien, Dänemark, Frankreich, Großbritannien, Holland, Italien, Luxemburg, Schweiz und der BRD trafen.

Guttmanns Recherchen zeigen, dass sich die Kontakte des Club de Berne schon zwei Jahre nach der Gründung ausweiteten: Die neun westeuropäischen Dienste tauschten sich damals mit den israelischen Inlands- und Auslandsgeheimdiensten Shin Beth und Mossad sowie dem US-amerikanischen FBI über palästinensische Terroristen und deren Unterstützer*innen aus. Der Austausch lief über ein verschlüsseltes Telegrammsystem namens Kilowatt. Ab 1974 existierte ein zweites solches System namens Megaton für den nicht-palästinensischen Terrorismus.[6] „Bis heute wurden weder die Öffentlichkeit noch das Parlament oder andere Departemente über die Existenz, geschweige denn über das Ausmaß der Praktiken dieses Geheimdienstaustausches informiert“, hält Guttmann fest.[7]

4 Der geheime Club der geheimen Dienste, WOZ v. 5.3.2020 (www.woz.ch)

5 Guttmann, A.: The Origins of International Counterterrorism. Switzerland at the Forefront of Crisis Negotiations, Multilateral Diplomacy, and Intelligence Cooperation (1969-1977), Leiden/Boston 2017

6 Aldrich, R.J.: Transatlantic intelligence and security cooperation, in: International Affairs 2004, No. 4, pp. 733-755 (https://warwick.ac.uk/fac/soc/pais/people/aldrich/ publications/ inta80_4_08_aldrich.pdf)

7 So spionierte die Schweiz mit Israel Araber aus, Tagesanzeiger v. 7.2.2016

Guttmanns Forschungsarbeit im Schweizer Bundesarchiv geht allerdings nicht über die 1980er Jahre hinaus, neuere Akten unterliegen der üblichen dreißig- bis fünfzigjährigen Sperrfrist bei bundesbehördlichen Dokumenten. Seither ist der Club de Berne weitgehend eine Blackbox. „Ich weiß jedoch", sagt Guttmann, „dass er bis heute eine bevorzugte Plattform für den Austausch innerhalb der Geheimdienste ist."

Der Club steht über den nationalen Diensten

Weil die offiziellen Informationen der politischen Behörden zum Club de Berne spärlich und irreführend sind, ist das geheime Dokument, das im November 2019 über das Boulevardblatt „Österreich" an die Öffentlichkeit gelangte, umso aufschlussreicher.[8] Konkret geht es um eine Sicherheitsüberprüfung, die der Club de Berne im Februar 2019 beim österreichischen Bundesamt für Verfassungsschutz und Terrorismusbekämpfung Geheimdienst (BVT) durchgeführt hatte. Das BVT war ins Visier der anderen europäischen Dienste geraten, weil Ende 2017 die rechtsextreme FPÖ die Kontrolle über das BVT übernommen hatte – eine Partei, der gute Kontakte nach Russland nachgewiesen wurden. Es bestanden Bedenken, was die Sicherheit der Daten anging.[9]

Die Prüfung durch den Club de Berne stellte dem BVT ein miserables Zeugnis aus: Im Bereich der Gebäudesicherheit und bei der Sicherheitsüberprüfung des Personals bestünden erhebliche Mängel; vor allem aber sei die Cybersicherheit absolut fahrlässig. Über das interne BVT-Netzwerk könnten selbst mäßig begabte Hacker in „Poseidon", das IT-Netz des Club de Berne, eindringen, konstatierte man.

Der geleakte Bericht bietet einen einmaligen Einblick in das Innenleben des Clubs, angefangen beim offiziellen Wappen. Zuständig für das „security assessment", das am 13. Februar 2019 im Wiener BVT-Hauptquartier stattfand, ist „Soteria", eine interne Gruppe des Club de Berne. Zu dieser Gruppe gehört auch der Schweizer Nachrichtendienst des Bundes (NDB), der an jenem Februartag das Personal- und Einstellungsmanagement des BVT begutachtete. Die weiteren in die Untersuchung involvierten Geheimdienste stammen aus Großbritannien, Deutschland und Litauen. Der Vorgang in Wien bestätigt den großen Einfluss des

8 Alarm: Verfassungsschutz steht total blamiert da, OE 24 v. 11.11.2019

9 Insider: Rauswurf des BVT aus „Berner Club" war nicht geplant, Kurier online v. 2.11.2018

Clubs und zeigt, dass dieser in seinem Selbstverständnis über den nationalen Diensten steht, ja sich sogar für diese verantwortlich fühlt.

NDB: Codenummer 10

Im Laufe der Recherche erhielten die beiden Autoren dieses Artikels ein bisher unbekanntes Dokument aus dem Jahr 2011. Es zeigt, dass sich der Club de Berne seit den 1970er Jahren zu einem noch weit größeren Netzwerk ausgewachsen hat und dass die offiziellen Behauptungen, es handle sich aktuell um eine rein innereuropäische Kooperation, falsch sind: Vor knapp zehn Jahren waren im Verteiler des Kommunikationsnetzes für den Austausch über islamischen Extremismus – mit dem Namen „Capriccio" – neben 27 EU-Diensten sowie denen aus der Schweiz (aufgelistet als Codenummer 10) und Norwegen mehrere nichteuropäische Geheimdienste in folgender Codenummer-Reihenfolge aufgelistet: 06 Mossad (Tel Aviv), 12 CSIS (Ottawa), 19 FBI (Washington), 22 ASIO (Canberra), 25 NZSIS (Wellington), 28 CIA (Brüssel) und 94 ISA (Tel Aviv). Ein zweites Dokument, ebenfalls von 2011, belegt einen weiteren Verteiler: „Toccata" dient dem Informationsaustausch zum nichtislamischen Terrorismus. Im Unterschied zu „Capriccio" fehlen darin aber der Mossad, die Israeli Security Agency (ISA) und die CIA.

„Operative Plattform" in Den Haag

Der Club de Berne hat in den letzten zwei Jahrzehnten massiv an Infrastruktur zugelegt: Aus den einst halbjährlichen Zusammentreffen der Dienstchefs in den 1970er Jahren ist mittlerweile eine verfestigte Geheimdienstorganisation gewachsen. Das lässt sich exemplarisch an einer Untergruppe aufzeigen: der Counter Terrorist Group (CTG).

Eine wichtige Information über diese CTG liefert die bereits erwähnte Medienmitteilung der Schweizer Bundespolizei (Fedpol) über ein Treffen des Club de Berne in der Schweiz im Jahr 2004: Damals wurde die Weiterentwicklung der Counter Terrorist Group beschlossen, die 2001 als Untergruppe gegründet worden war – als Schnittstelle mit der EU im Bereich Terrorismusbekämpfung. „Die CTG wird eine tragende Rolle bei der Verfolgung der maßgeblichen Ziele aus der Erklärung des Europäischen Rats zum Kampf gegen den Terror spielen", steht in der Pressemitteilung. Und die CTG sei auch ein „Forum für Experten für die Entwicklung praktischer Zusammenarbeit und eines besseren Verständnisses terroristischer Bedrohungen".

Anders gesagt: Der Club de Berne, respektive seine Untergruppe CTG, ist seit 2004 eine zentrale Stelle für die terroristischen Bedrohungsanalysen der europäischen Sicherheitsbehörden. Die CTG erstellt „Bedrohungsanalysen für führende Politiker auf EU Ebene", basierend „auf Angaben von Mitgliedsdiensten, die Zugang zu allen relevanten nachrichtendienstlichen Erkenntnissen haben". Damit wird klar, dass die CTG durch ihre Analysen den Fokus der nationalen Sicherheits- und Repressionsorgane maßgeblich beeinflusst – und damit auch den politischen Sicherheitsdiskurs. Der Club de Berne institutionalisiert sich, ohne sich in ein institutionelles demokratisches Gefüge einzubetten.

Der österreichische Historiker und Geheimdienstexperte Thomas Riegler[10] findet das äußerst problematisch: „Da sie nicht offiziell in die institutionelle Architektur der EU eingebettet sind und auch nicht auf einer vertraglichen Abmachung beruhen, sind beide Institutionen – der Club de Berne und die Counter Terrorist Group – lediglich an die nationalen Gesetze der jeweiligen Staaten gebunden. Einheitliche Regelung dazu gibt es nicht", sagt er im Gespräch. Das mache die rechtliche Frage sehr schwierig. „Der Club und die CTG folgen keinen übergeordneten Regeln. Und da sich die nationalen Gesetze stark unterscheiden, wird Kontrolle unmöglich", so Riegler. „Für wen arbeiten die Dienste eigentlich? Es entsteht der Eindruck, dass sie sich selber zuarbeiten, statt im Dienst der Öffentlichkeit und der Regierung zu stehen." Es sei wichtig, zu verstehen, dass hochrangige Amtsträger innerhalb der Dienste oft massive Macht anhäuften und Eigeninteressen verfolgten. „Sie werden regelrechte Mandarine der Macht, sind aber völlig gesichtslos. Eine aufsichtsleere Plattform wie der Club de Berne verstärkt diesen Effekt."

Ungeklärter „Beobachterstatus" der US-Dienste

Zur CTG sind weitere Eckpunkte bekannt. Im November 2016 berichtete netzpolitik.org erstmals umfassend über eine „operative Plattform", die die CTG mittlerweile am Sitz des niederländischen Geheimdiensts AIVD in der Nähe von Den Haag unterhält.[11] Dort tauschen sich die beteiligten Dienste in Echtzeit zu Maßnahmen und Gefahren aus; zudem

10 Thomas Riegler verfasste u.a. das Buch: Österreichs geheime Dienste, Wien 2018 (Ausschnitt online unter http://thomas-riegler.net v. 8.10.2019)

11 Zusammenarbeit europäischer Geheimdienste: Erste „operative Ergebnisse" in Den Haag, Netzpolitik.org v. 16.11.2016

gebe es auch „gemeinsame Operationsteams in diversen Formaten und zu verschiedenen Themenfeldern“, wie der niederländische Geheimdienstdirektor Rob Bertholee in einer Rede im Januar 2016 vermerkte.[12]

Zwei Jahre später veröffentlichte die niederländische Aufsichtsbehörde CTIVD einen Prüfbericht über die CTG-Datenbank „Phoenix“, die personenbezogene Daten über Dschihadreisende erfasst.[13] Der Bericht stellte etwa fest, dass das Qualitätsmanagement der eingespeisten Daten mangelhaft sei. Und er legte offen, dass US-Geheimdienste innerhalb der CTG „Beobachterstatus“ genießen – was das genau heißt, bleibt allerdings ungeklärt. Die Autoren dieses Artikels reichten bei der CTIVD insgesamt sieben Anfragen zu ihrem Bericht ein, sie blieben unbeantwortet, telefonisches Nachhaken wurde abgeklemmt, zu den versprochenen Rückrufen kam es nicht.

Auskunftsverweigerung partout

Der Linken-Bundestagsabgeordnete Andrej Hunko hat in den letzten Jahren immer wieder versucht, über parlamentarische Anfragen an die Bundesregierung zum Club de Berne und zur Counter Terrorist Group Licht ins Dunkel zu bringen. Vergeblich. Die Bundesregierung verweigerte standhaft praktisch jegliche Auskunft mit dem Verweis auf die sogenannte „Third Party Rule“.[14] Mitte März 2020 wollte Hunko von der Bundesregierung Details zur Reichweite des Informationsaustauschs im Club de Berne erfahren.[15] Zudem wollte er wissen, ob die Bundesregierung „sich die Mühe gemacht hat, ein Freigabeersuchen an die Dienste“ zu erwirken, um „dem Informationsbedürfnis des Parlaments“ zu entsprechen. Erneut blieben die Fragen mit Verweis aufs Staatswohl unbeantwortet. Eine Begründung dafür brauche die Bundesregierung nicht, ließ Innenstaatssekretär Volkmar Vogel verlauten.

Hunko pocht weiter auf Aufklärung: „Mit der operativen Plattform CTG ist der deutsche Inlandsgeheimdienst, das Bundesamt für Verfassungsschutz, seit 2016 de facto ein Auslandsgeheimdienst geworden.

12 Rede am Global Counterterrorism Forum (https://english.aivd.nl/publications)
13 https://english.ctivd.nl/latest/news/2018/04/26/index
14 Monroy, M.: Mit Geheimhaltung gegen Geheimdienstkontrolle, in: Bürgerrechte & Polizei/CILIP 113 (September 2017), S. 96
15 BT-Plenarprot. 19/151 v. 11.3.2020, S. 18848f.

Dafür braucht es Öffentlichkeit, denn es ist ein gravierendes Demokratieproblem, wenn über diese Verschiebung nichts bekannt werden darf."

Überhaupt weitet sich das Tätigkeitsfeld der CTG laufend aus. Im Jahresbericht 2018 der EU-Polizeiagentur Europol sind zwei gemeinsame Anti-Terror-Übungen („two table top exercises") mit der CTG ausgewiesen, an der auch das Zentrum für Terrorismusbekämpfung (ECTC), das Zentrum für Migrantenschleusung (EMSC) und die Meldestelle für Internetinhalte bei Europol teilnahmen.[16] Diese Zusammenarbeit soll weiter „verbessert" werden.[17] Ungeachtet der Tatsache, dass die EU dazu kein Mandat hat, kooperieren EU-Organe mit der CTG.

Nur die Spitze des Eisberges

Aus all diesen Puzzlestücken ergibt sich letztlich ein klareres Bild vom Club de Berne: Aus den einst halbjährlichen Zusammentreffen der Dienstchefs in den 1970er Jahren ist über die Jahrzehnte eine verfestigte Geheimdienstorganisation gewachsen, mitsamt einer operativen Plattform in Den Haag, gemeinsamen Operationsteams und einem Informationsaustausch, der bis heute auch nichteuropäische Dienste umfasst. Wie der Schweizer Historiker Adrian Hänni in einem lesenswerten Aufsatz nachzeichnet, ist der Club de Berne übrigens nicht die einzige geheim operierende Plattform.[18] „Zu diesen Clubs, die fast ausschließlich im Geheimen operieren und kaum einmal in der Medienberichterstattung auftauchen, zählen die Counter Terrorist Group (CTG) des Club de Berne, die Pariser Gruppe, die SIGINT Seniors, die Police Working Group on Terrorism (PWGOT) und die G 13+", schreibt Hänni.

Das zentrale Problem dabei: Es gibt zwar nationale Gesetze, so auch das neue Schweizer Nachrichtendienstgesetz, die eine Zusammenarbeit mit ausländischen Diensten erlauben wie auch die Bekanntgabe von Personendaten an solche Dienste. Für die multilaterale Geheimdienstzusammenarbeit innerhalb des Club de Berne, die bewusst nicht an Institutionen wie die EU oder die Nato angebunden ist, existiert hingegen keine gesetzliche Grundlage. Konsequenterweise ist deshalb auch keine

16 Europol: Consolidated Annual Activity Report 2018, Bucharest May 2019 (siehe www.europol.europa.eu/publication-documents)

17 BT-Drs. 19/17002 v. 3.2.2020

18 Hänni, A.: Die Nachrichtendienste und ihre geheimen Clubs, VSN-Bulletin v. 29.10.2018 (www.swissint.ch)

Aufsicht vorgesehen. Der Club de Berne, das zeigt das Beispiel aus Wien, ist niemandem Rechenschaft schuldig. Gerade die Schweiz weiß aber seit der „Fichenaffäre“, dem großen Staatsschutzskandal von 1989, dass Geheimdienste ohne adäquate Aufsicht ein Eigenleben entwickeln und letztlich die demokratischen Grundwerte unterminieren, die sie eigentlich schützen sollen.

Thorsten Wetzling von der Berliner Stiftung Neue Verantwortung[19] hält diesen aufsichtsleeren Raum für demokratiepolitisch gefährlich. „Es ist deshalb an der Zeit – zumindest im europäischen Rahmen –, für eine Harmonisierung der Rechtsschutzstandards und eine Erweiterung der Kontrollbefugnisse zu streiten“, sagt Wetzling im Gespräch.[20] In den letzten Jahren habe es in einigen Ländern neue Nachrichtendienstgesetze gegeben, die wichtige Errungenschaften der demokratischen Kontrolle enthielten. „Leider bringen aber auch die besten Regelungen im nationalstaatlichen Kontext nichts, wenn man sie mittels der internationalen Kooperation umgehen oder aushebeln kann.“ Einen ersten Fortschritt sieht Wetzling in der Gründung der internationalen Austauschplattform European Intelligence Oversight Forum,[21] an der unter anderem auch die Schweizer Aufsichtsbehörde AB-ND mitmacht.

Sämtliche Fragen an die Behörden bleiben unbeantwortet

Die Rechercheergebnisse werfen zahlreiche Fragen auf. Die beiden Autoren haben sie mit einem Fokus auf den Schweizer Geheimdienst (NDB) und die entsprechenden Dienstaufsichtsorgane aufgeworfen: Werden von den halbjährlichen Treffen des Club de Berne einsehbare Protokolle erstellt? Wie viele Schweizer Bürger*innen sind in der „Phoenix“-Datenbank erfasst? Können Betroffene einen Missbrauch ihrer Daten in den Niederlanden rechtlich überhaupt anfechten? Weshalb wird die Beteiligung der US-Dienste verschwiegen? Kann ausgeschlossen werden, dass vom NDB gelieferte Daten und Informationen über Datenbanken und Verteiler wie „Capriccio“ als Grundlage für den US-Drohnenkrieg dienen?

Der Schweizer Nachrichtendienst antwortete äußerst knapp: „Der NDB arbeitet mit über 100 ausländischen Partnerdiensten zusammen.

19 www.stiftung-nv.de
20 Geheimdienstaufsicht: Völlig unzureichend kontrolliert, WOZ v. 5.3.2020
21 https://guardint.org/about

Diese Liste wird vom Bundesrat genehmigt und ist klassifiziert, weshalb sich der NDB grundsätzlich nicht zur Zusammenarbeit mit seinen Partnerdiensten äußert." Auch der holländische Geheimdienst AIVD, der für das operative Zentrum der CTG verantwortlich ist, mauert. „Wir kommentieren nie etwas zum Club de Berne." Ein Besuch vor Ort in Den Haag komme nicht infrage.

Einen umfangreichen Fragebogen schickten wir auch der „unabhängigen Aufsichtsbehörde über die nachrichtendienstlichen Tätigkeiten", AB-ND, dem parlamentarischen Aufsichtsgremium GPDel (Geschäftsprüfungsdelegation) sowie dem Eidgenössischen Datenschutzbeauftragten. Alle drei Aufsichtsbehörden bestätigen, dass sie Kenntnis vom Club de Berne und von der CTG hätten. Unisono verweisen sie darauf, dass mit dem neuen Nachrichtendienstgesetz die Grundlage für die Zusammenarbeit mit dem Ausland und die Bekanntgabe von Personendaten an das Ausland gegeben sei. Verstörend ist insbesondere die Rückmeldung der GPDel, die zu keinem einzigen Punkt konkret Stellung bezieht.

Der rechte Troll

Unbeantwortet ist auch die Frage, wie politisch der Club de Berne ist. In einer BBC-Dokumentation über Nato-Operationen in Italien aus dem Jahre 1992 sagt das hochrangige italienische Geheimdienstmitglied Federico D'Amato, dass der Club de Berne als Reaktion auf die „Revolution der 68er" in Frankreich gegründet worden sei.[22] Recherchen der deutschen Journalistin Regine Igel bestätigen das. Gemäß ihr vorliegenden Informationen aus dem Protokoll einer Versammlung des Club de Berne in Köln 1973 sei „ein neuer Typus von Vertrauensleuten (sprich: Spitzeln, Anm. d. Red.) in aufständischen Organisationen gefragt, der auch aktiv werde, zum Motor der Gewalt werden müsse, um dann in die Führung der Organisationen der extremen Linken zu gelangen."[23]

In der erwähnten BBC-Dokumentation tritt auch Vincenzo Vinciguerra auf, einstiges Mitglied der neofaschistischen Terrororganisation „Ordine Nuovo".[24] Gemäß Vinciguerra hat der Berner Club in Italien auf die Dienste neofaschistischer Gruppen zurückgegriffen. Er beschreibt in der Doku die „Operation Chinese Poster" als konkrete Aktion des Club

22 https://www.youtube.com/watch?v=1YhRBxxyRqs
23 Igel, R.: Terrorjahre. Die dunkle Seite der CIA in Italien, München 2006, S. 281
24 siehe die Wikipedia-Einträge zu Vinciguerra und Ordine Nuovo

de Berne. Dabei handelte es sich um die Infiltrierung einer linken Demonstration in Italien im Jahr 1972 durch vermeintlich maoistische Kräfte, die in Wirklichkeit der neofaschistischen „Avanguardia Nazionale“ angehörten. Der Club de Berne wollte damit antikommunistische Ressentiments fördern, indem er eine „ultralinke“, extremistische Kraft produzierte. Dass Vinciguerra darüber im Detail Bescheid weiß, erstaunt nicht: Auch er war Mitglied bei der Avanguardia Nazionale.

Der Club de Berne operiert mutmaßlich auch heute noch im Bereich „Linksextremismus“. Das interne Dokument des Club de Berne aus dem Jahr 2011 belegt, dass es damals auch einen Verteiler namens „Rile“ zum Links- und Rechtsextremismus gab. So ist die Frage, ob der Club de Berne etwa im Sommer 2017 im Vorfeld oder auch während des G20-Gipfels in Hamburg, gegen den es massive linke Proteste gab, aktiv war.

Der Blick gegen Links hat historische Kontinuität: Im November 2018 hielt Hans-Georg Maaßen in Warschau seine Abschiedsrede vor dem Club de Berne. Kurz davor hatte die Regierung seine Absetzung als Chef des deutschen Inlandsgeheimdiensts beschlossen. Maaßen hatte die rechtsextremistischen Hetzjagden in Chemnitz im August 2018 öffentlich als „gezielte Falschinformation“ bezeichnet. In seiner Rede wiederholte er diese – widerlegte – Äußerung. Mehr noch: Er monierte, dass „linksradikale Kräfte in der SPD“ seine Äußerungen instrumentalisiert hätten, um „einen Bruch dieser Regierungskoalition zu provozieren“.

Entfesselt statt kontrolliert

Am Ende bleiben zum Club de Berne viele – zu viele – Fragen von öffentlichem Interesse offen. Klar ist hingegen: Der Deal beim neuen Schweizer Geheimdienstgesetz, das seit Herbst 2017 in Kraft ist, war eine reine Illusion. Das Gesetz sollte dem NDB massiv mehr Kompetenzen verschaffen, aber auch eine stärkere Aufsicht enthalten, versprachen die Schweizer Behörden im Vorfeld der Volksabstimmung im September 2016. Die Realität ist eine andere: Der Schweizer Geheimdienst ist entfesselt und operiert über seine internationalen Verstrickungen wie den Club de Berne sowie die CTG in einem Raum ohne Aufsicht. Die Kontrollbehörden dulden das nicht nur, sie rechtfertigen es auch noch.

Achtung: Überkriminalisierung

Das geplante IT-Sicherheitsgesetz 2.0

von Louisa Zech

Einmal mehr soll sich der Bundestag mit dem Schutz von IT-Systemen und den darin gespeicherten Daten befassen. Der Reform des IT-Sicherheitsgesetzes von 2015 soll nun eine weitere folgen. Ein Entwurf des Bundesinnenministeriums (BMI) vom 27. März 2019 befindet sich derzeit in der Ressortabstimmung.[1]

Bereits vergangene Reformen im Bereich des Informationsstrafrechts wie die Einführung von § 202c Strafgesetzbuch (StGB) (Vorbereiten des Ausspähens und Abfangens von Daten) und § 202d StGB (Datenhehlerei) waren problematisch und sahen sich massiver Kritik ausgesetzt. Sie zeichneten sich durch eine weitgehende Vorfeldkriminalisierung und ausufernde Tatbestände aus, unter welche bisweilen sozialadäquate Handlungen subsumiert werden können. Das Strafrecht wird im IT-Bereich als Mittel der Gefahrenabwehr instrumentalisiert, mit der auf abstrakte und vermeintlich bestehende Bedrohungsszenarien reagiert werden soll. Die gesetzgeberischen Maßnahmen erscheinen dabei mehr als nur ungeeignet, um einen umfassenden Schutz der IT-Sicherheit zu gewährleisten. Damit reiht sich auch die Entwicklung des Informationsstrafrechts immer mehr in eine neoliberale Sicherheitslogik ein.

Für den Bereich des Strafrechts bedeutet diese Logik der absoluten Sicherheit eine Etablierung des sogenannten Risikostrafrechts. Die Bestrafung bestimmter Verhaltensweisen ist verfassungsrechtlich an das Ultima-Ratio-Prinzip und den Rechtsgüterschutz geknüpft. Das Strafrecht darf nur als letztes Mittel zur Verhaltensteuerung eingesetzt werden. Für den Gesetzgeber bedeutet dies, zunächst andere Maßnahmen,

1 Referentenentwurf des Bundesministerium des Innern, Bau und Heimat v. 27.3.2019, zuvor geleakt von Netzpolitik.org (https://netzpolitik.org/2019/it-sicherheitsgesetz-2-0-wir-veroeffentlichen-den-entwurf-der-das-bsi-zur-hackerbehoerde-machen-soll)

Alternativen zum Strafen, in Betracht zu ziehen. Seit den 1980er Jahren hat sich dies gewandelt. Ziel der Strafe ist mittlerweile nicht mehr die Wiederherstellung des Rechtsfriedens nach einer erfolgten Rechtsgutverletzung unter Anknüpfung an das Schuldprinzip. Vielmehr wird das Strafrecht als Instrument zur Eindämmung abstrakter Risiken zum Einsatz gebracht. Dies lässt sich insbesondere an der Kriminalisierung von Vorbereitungshandlungen, ausufernden Rechtsgütern (beispielsweise Kollektivrechtsgüter) und Gefährdungsdelikten erkennen.[2] Kriminalisiert werden Verhaltensweisen, die ein Rechtsgut weder verletzt noch in konkreter Weise gefährdet haben, die potenziellen Täter*innen brauchen mitunter nicht einmal zu einer Tat angesetzt zu haben.

Im Bereich der Computerkriminalität zeigt sich diese Logik beispielsweise am § 202c StGB, der 2007 mit dem 41. Strafrechtsänderungsgesetz eingeführt wurde. Dieser stellt die Entwicklung von sogenannten Hacker-Tools unter Strafe, also von Software, mit deren Hilfe man sich Zugang zu Daten verschaffen kann. Im nicht-virtuellen Raum entspräche dies der Herstellung eines Einbruchswerkzeugs, also einem Verhalten, das erst dann strafrechtlich geahndet wird, wenn damit auch tatsächlich versucht wird, eine Tür auszuhebeln. Der § 202c StGB knüpft also nicht an eine bestehende konkrete Gefahr des „Hackens“ an, sondern an die potenzielle Möglichkeit, dass diese Software zum „Hacken“ verwendet wird, ohne dass dabei etwa die konkrete Tatzeit und das konkrete Angriffsziel den potenziellen Täter*innen schon klar sein müssten. Für den Schutz informationstechnischer Systeme hat der Straftatbestand kaum etwas gebracht; IT-Sicherheitsunternehmen beklagten sogar eine negative Wirkung, da die Herstellung von „Hacker-Tools“ ein wichtiges Mittel darstellt, um informationstechnische Systeme auf ihre Sicherheit hin zu überprüfen und bestehende Sicherheitslücken zu erkennen.[3]

Der „digitale Hausfriedensbruch“

An diese Entwicklung knüpft nun auch die Reform des Kernstrafrechts durch das IT-Sicherheitsgesetz 2.0 an. Der Referentenentwurf sieht nicht nur die Erhöhung des Strafrahmens für gängige Computerdelikte (§§ 202a ff. und §§ 303a, 303b StGB) auf bis zu fünf Jahre vor, sondern

2 siehe hierzu auch: Derin, B.: Strafrechtliche Vorverlagerung: Der Wandel zum Präventionsstrafrecht, in: Bürgerrechte & Polizei/CILIP 117 (November 2018), S. 3-11

3 Kontraproduktiv für die IT-Sicherheit, Spiegel online, Netzwelt v. 25.9.2006

brächte auch neue Straftatbestände mit sich. Mit dem § 202e StGB-E soll unbefugtes Verschaffen des Zugangs zu einem informationstechnischen System, die Ingebrauchnahme eines solchen oder die Ingangsetzung bzw. Beeinflussung eines Datenverarbeitungsvorgangs oder informationstechnischen Ablaufs unter Strafe gestellt werden. Im Gegensatz zum bisherigen § 202a StGB kommt es auf eine tatsächliche Kenntnisnahme der im informationstechnischen System gespeicherten Daten nun nicht mehr an. § 202f StGB-E enthält zusätzlich entsprechende Qualifikationstatbestände (wie banden- oder gewerbsmäßige Begehung), insbesondere die Absicht des oder der Täter*in, mit der Begehung einer Tat nach den §§ 202a-E einen Ausfall oder eine wesentliche Beeinträchtigung der Funktionsfähigkeit kritischer Infrastrukturen zu bewirken.

Begründet wird die Neuregelung mit der Bekämpfung der „Botnetz-Kriminalität", die aufgrund vermeintlicher Strafbarkeitslücken nicht hinreichend strafrechtlich verfolgt werden könne.[4] Botnetze sind Netzwerke infizierter Systeme, die durch einen Command & Control-Server ferngesteuert werden können – unter anderem, um die Ressourcen der infizierten Geräte zu nutzen.

Wirklich neu ist dieser Vorschlag jedoch nicht. Bereits 2016 hat der Bundesrat auf Initiative des Landes Hessen einen Gesetzgebungsvorschlag in den Bundestag eingereicht, der ebenfalls die Implementierung des § 202e StGB-E („Digitaler Hausfriedensbruch") vorsah. Der Vorschlag wurde seinerzeit sowohl in der juristischen Literatur[5] als auch von Seiten der Bundesregierung[6] massiv kritisiert und schlussendlich vom Bundestag abgelehnt. Zentrale Kritikpunkte waren schon damals das unbestimmte Rechtsgut, der ausufernde Tatbestand, unter den sich auch sozialadäquate Handlungen subsumieren lassen, sowie die mangelnde Effektivität in der eigentlichen Zwecksetzung.

Ob in Bezug auf die „Botnetz-Kriminalität" tatsächlich Strafbarkeitslücken bestehen, ist jedoch auch heute sehr zu bezweifeln, da hier insbesondere eine Strafbarkeit gemäß §§ 202a ff. (Ausspähen und Abfangen von Daten, Vorbereitungshandlungen, Datenhehlerei) und §§ 303a,

4 Referentenentwurf BMI a.a.O (Fn. 1), S. 1

5 ausführliche und lesenswerte Kritik: Buermeyer, U.; Golla, S.: „Digitaler Hausfriedensbruch". Der Entwurf eines Gesetzes zur Strafbarkeit der unbefugten Benutzung informationstechnischer Systeme, in: Kommunikation & Recht (K&R) 2017, H. 1, S. 14-18 (17)

6 Stellungnahme der Bundesregierung, BT-Drs. 18/10182 v. 2.11.2016, S. 19, Anlage 2

303b StGB (Datenveränderung, Computersabotage) in Betracht kommt.[7] Zudem ist der Anwendungsbereich der Norm aufgrund seiner Weite dazu geeignet, an sich nicht strafwürdige Verhaltensweisen unter Strafe zu stellen. Unter dem Begriff IT-System werden alle Systeme verstanden, die der Verarbeitung elektronischer Daten dienen.[8] Vom Anwendungsbereich des „digitalen Hausfriedensbruchs" umfasst wäre damit jedwede unbefugte Ingebrauchnahme oder Verwendung datenverarbeitender Alltagsgegenstände wie Smart-TVs, Fitnessarmbänder oder Haushaltsgegenstände, „soweit sie geeignet ist, berechtigte Interessen eines anderen zu beeinträchtigen".[9] Diese einschränkende Klausel ist allerdings zu weit formuliert, als dass hierdurch sinnvoll Bagatellfälle vom Anwendungsbereich der Norm ausgeklammert werden könnten. Unter „berechtigten Interessen" versteht der Referentenentwurf „materielle oder ideelle, private oder öffentliche Interessen, sofern sie nur vom Recht als schutzwürdig anerkannt sind oder diesem jedenfalls nicht zuwiderlaufen."[10] Zu einer tatsächlichen Beeinträchtigung dieser Interessen muss es dabei aber gar nicht kommen. Es genüge schon – so die Begründung –, „dass die Tat dazu geeignet ist".

Entgegen der massiven Kritik am Entwurf des Bundesrates, startet das BMI mit seinem geplanten IT-Sicherheitsgesetz 2.0 einen weiteren Versuch der Kriminalisierung des „digitalen Hausfriedensbruchs" – in inhaltlich nur minimal abgeänderten Formulierung und ohne dass auf die wesentlichen kritischen Aspekte eingegangen worden wäre.

„Betreiben internetbasierter Leistungen"

Eine weitere zentrale Neuerung ist die Einführung des § 126a StGB-E. Danach soll sich strafbar machen, wer Dritten eine internetbasierte Leistung zugänglich macht, deren Zweck oder Tätigkeit darauf ausgerichtet ist, die Begehung von rechtswidrigen Taten zu ermöglichen, zu fördern oder zu erleichtern.[11] Unter einer internetbasierten Leistung wird dabei „jeder elektronische Kommunikationsdienst" verstanden, „der Daten

7 Buermeyer; Golla a.a.O. (Fn. 5), S. 15

8 siehe Bundeverfassungsgericht: Urteil des v. 27.2.2008 zur „Online-Durchsuchung" Az.: 1 BvR 370/07, 595/07, Rn. 173; s.a. Fragenkatalog des Bundesministeriums für Justiz v. 22.8.2007 (https://netzpolitik.org/wp-upload/fragen-onlinedurchsuchung-BMJ.pdf)

9 Mit eindrücklichen Fallbeispielen hierzu: Buermeyer; Golla a.a.O. (Fn. 4) S. 17

10 Referentenentwurf BMI a.a.O (Fn. 1), S. 84

11 ebd., S. 29

über das Internet überträgt und bestimmten Personen einen Nutzen stiftet."[12] Auch dieser Vorstoß ist nicht neu und wurde bereits am 17. April 2019 auf Initiative Nordrhein-Westfalens in einem entsprechenden Gesetzentwurf dem Bundestag vorgelegt.[13] Der Entwurf des BMI unterscheidet sich jedoch stark von dem des Bundesrates. Vor allem geht er sehr viel weiter. Der Anwendungsbereich ist hier nicht nur auf das Darknet beschränkt, sondern wird auf das allgemein zugängliche Internet ausgeweitet, in dem die Erreichbarkeit der internetbasierten Leistungen nicht eingeschränkt sein muss. Außerdem soll nicht mehr nur das „Anbieten" einer internetbasierten Plattform bestraft werden, sondern schon das bloße „Zugänglichmachen" einer solchen. Unter die neue Strafnorm könnte deshalb auch das zur Verfügung Stellen entsprechender Server fallen sowie das Betreiben von TOR-Servern, die ein anonymes Surfen im Internet ermöglichen. Kriminalisiert wird ferner nicht nur die „Ermöglichung", es reicht das „Erleichtern" einer Straftat. Im Gegensatz zum Entwurf des Bundesrates soll der Anwendungsbereich von § 126a StGB-E außerdem nicht auf einen bestimmten Straftatenkatalog beschränkt werden, sondern würde jegliche strafrechtlich relevanten Verhaltensweisen umfassen.[14]

Sowohl der Entwurf des Bundesrates als auch der Referentenentwurf des BMI argumentieren hier erneut mit Strafbarkeitslücken. Eine Strafbarkeit des Betreibens von Plattformen, mit Hilfe derer Straftaten erleichtert werden, könne nicht über die Beihilfe zu den dort verabredeten Taten konstruiert werden. Die einzelnen Straftaten seien noch nicht genügend konkretisiert, die Kommunikation der Beteiligten über verschlüsselte Kanäle und vollautomatisierte Verkaufsabwicklungssysteme erschwerten den Nachweis der Hilfeleistung zu einer konkreten strafbaren Handlung. Und außerdem sei das Schaffen der Grundlagen für eine „Underground Economy" nicht eine bloße Beihilfe zu einer Straftat, sondern durchaus eine aktive Tathandlung, die eigenständig einen strafwürdigen Charakter aufweise.[15]

12 Bäcker, M; Golla, S.: Strafrecht in der Finsternis. Zu dem Vorhaben eines „Darknet-Tatbestands", verfassungsblog.de v. 21.3.2019

13 BR-Drs. 33/19 v. 18.1.2019; BT-Drs. 19/9508 v. 17.4.2019

14 Zöller, M.: Strafbarkeit und Strafverfolgung internetbasierter Handelsplattformen für illegale Waren und Dienstleistungen, in: Kriminalpolitische Zeitschrift (KriPoz) 2019, Ausg. 5, S. 274-281 (278)

15 Referentenentwurf BMI a.a.O (Fn. 1), S. 77

Auch hier ist aber zu bezweifeln, ob überhaupt von „Strafbarkeitslücken“ gesprochen werden kann. Wenn nicht einmal eine Beihilfe zu Straftaten nachgewiesen werden kann, ist fraglich, ob es sich überhaupt um strafwürdiges Verhalten handelt. Die eigentliche Rechtsgutsgefährdung entsteht schließlich erst durch die Ausführung der verabredeten Straftaten beziehungsweise durch die tatsächliche Abwicklung der illegalen Geschäfte in der realen Welt. Die klassischen Darknet-Delikte wie der illegale Handel mit Waffen oder Betäubungsmitteln sowie die Verbreitung von Kinderpornografie sind darüber hinaus bereits durch andere Strafvorschriften umfassend strafbewehrt.[16]

Die Notwendigkeit der Kriminalisierung des Betreibens internetbasierter Leistungen ist bereits in Zweifel zu ziehen. Der § 126a StGB-E birgt darüber hinaus aber auch die Gefahr der Überkriminalisierung: Die Nutzung des Darknets und das Betreiben von Plattformen in diesem (zum Beispiel Diskussionsforen) sind nicht per se illegal und verfolgen auch nicht per se strafbare Zwecke. Vielmehr geht es um die gewährleistete Anonymität – frei von staatlicher Repression oder informeller Sozialkontrolle, ohne dass es bereits zu konkreten Rechtsgutsgefährdungen kommen muss. Eine Einschränkung durch das Tatbestandsmerkmal des Zwecks der Ermöglichung, Förderung oder Erleichterung einer Straftat reicht aber nicht aus, um nicht strafwürdige Verhaltensweisen vom Anwendungsbereich der Norm auszuklammern. So argumentieren Matthias Bäcker und Sebastian Golla: „Der Anbieter muss also gerade nicht bezwecken, dass mithilfe seiner Plattform tatsächlich Straftaten begangen werden. Er muss lediglich zweckgerichtet ein Umfeld schaffen, in dem solche Straftaten naheliegen.“[17] Auf die legale Nutzung des Darknets sind insbesondere Journalist*innen, Whistleblower*innen und Kritiker*innen in diktatorischen Regimen angewiesen. Organisationen wie etwa „Reporter ohne Grenzen“ oder „Zwiebelfreunde“ warnen vor „Kollateralschäden“, die die Neuregelung mit sich bringt, da gerade auch Betreiber*innen von TOR-Knoten oder anderer Dienste zur Anonymisierung einem Anfangsverdacht nach § 126a StGB-E unterliegen und somit Ziel von Ermittlungsmaßnahmen werden können. Insgesamt führe dies

16 Bartl, M.; Moßbrucker, D.; Rückert, C.: Angriff auf die Anonymität im Internet, o. O. 2019, S. 2 – www.reporter-ohne-grenzen.de, Meldung v. 5.7.2019

17 Bäcker; Golla a.a.O. (Fn. 12)

zu einer weitgehenden Abschreckung und Verunsicherung von Darknet-User*innen.[18]

Zwar erkennt auch das BMI an, dass es diese Art von Nutzung gibt: „Die Angebote im Darknet umfassen … Foren für Whistleblower oder Chatrooms für politisch Verfolgte aus autoritären Staaten …“[19] Dennoch werden in der öffentlichen Debatte immer wieder Äußerungen laut, die Nutzer*innen des Darknets unter Generalverdacht stellen. Der parlamentarische Staatssekretär – unter Bundesinnenminister Horst Seehofer – Günter Krings (CDU) erklärte: „Ich verstehe, warum das Darknet einen Nutzen in autokratischen Systemen haben kann … Aber in einer freien, offenen Demokratie gibt es meiner Meinung nach keinen legitimen Nutzen.“[20]

Fazit

Insgesamt bestehen sowohl im Falle des § 202e StGB-E („digitaler Hausfriedensbruch“) als auch des § 126a StGB-E (Betreiben internetbasierter Plattformen) erhebliche Zweifel an einem (straf-)gesetzgeberischen Handlungsbedarf. Der Referentenentwurf des BMI ist in beiden Fällen nicht in der Lage, tatsächlich bestehende Strafbarkeitslücken aufzuzeigen. Vielmehr wird das Strafrecht einmal mehr verfassungswidrig genutzt, um Aktionsfähigkeit und -bereitschaft seitens der Politik zu signalisieren. Auf abstrakte Gefahren und bestehende Risiken, die dem Bereich der Gefahrenabwehr zugeschrieben werden, soll mit strafrechtlichen Sanktionen und – damit unweigerlich verbunden – strafprozessualen Ermittlungen Abhilfe geleistet werden. Die Grenzen dessen, was als strafwürdig gelten soll und was nicht, verschwimmen dadurch zusehends. Das Ergebnis sind Tatbestände, die weit ins Vorfeld einer konkreten Gefährdung von Individualrechtsgütern wie Leben oder körperliche Unversehrtheit reichen,[21] die Kriminalisierung gesellschaftlich erwünschter bzw. sogar notwendiger Verhaltensweisen und eine Verunsicherung aufgrund eines weiten und schwammigen Anwendungsbereichs.

18 Bartl; Moßbrucker; Rückert a.a.O. (Fn. 16)
19 Referentenentwurf BMI a.a.O (Fn. 1), S. 76
20 zitiert n. Internet-Kriminalität: Wie die Länder Strafverfolgung im Darknet erleichtern wollen, Süddeutsche Zeitung online v. 11.3.2019
21 Zöller a.a.O. (Fn. 13)

Inland aktuell

Viele Ortungsimpulse in den Bundesländern

„Stille SMS“ sind Textnachrichten, deren Empfang das Mobiltelefon nicht anzeigt. Sie generieren aber einen Kommunikationsvorgang, den die Telefonanbieter protokollieren. Polizeien und Geheimdienste erhalten auf diese Weise den Standort und bei mehrmaliger Abfrage ein Bewegungsprofil der Betroffenen. Die Bundespolizei versendet um die 80.000 „Stille SMS“ pro Jahr, beim Bundeskriminalamt (BKA) pendelt dieser Wert um die 60.000. Die Zahlen unterliegen Schwankungen, die vermutlich auf besondere Ermittlungsverfahren zurückzuführen sind: 2015 hatte allein das BKA 140.000 Ortungsimpulse versandt, im Jahr darauf kam die Bundespolizei auf eine etwa gleiche Anzahl. Deutlich höher liegen hingegen die „Stillen SMS“ des Bundesamtes für Verfassungsschutz, das die Methode 2017 rund 320.000 mal genutzt hat. Seit 2018 können die Angaben zum Inlandsgeheimdienst nur noch in der Geheimschutzstelle im Bundestag eingesehen werden. Laut Bundesinnenministerium seien die Informationen fortan besonders schutzbedürftig, da sich „durch die regelmäßige halbjährliche Beantwortung … Einzelinformationen zu einem umfassenden Lagebild verdichten können“.[1] Auf diese Weise könnten Rückschlüsse auf die „technischen Fähigkeiten“ des Geheimdienstes gezogen werden.[2]

Bei den Landesämtern für Verfassungsschutz sind die Zahlen, sofern überhaupt Angaben gemacht werden, auffällig niedrig.[3] Der Verfassungsschutz Berlin versandte 2019 ganze 345 „Stille SMS“ (2018: 121, 2017: 49). Auffällig hohe Zahlen verzeichnen hingegen die Landespolizeien, das belegen Antworten auf Informationsfreiheitsanfragen. Demnach versenden allein die Polizeibehörden in Schleswig-Holstein so viele

1 Schreiben von Staatssekretär Günter Krings an MdB Andrej Hunko v. 11.3.2019, zit. n. BT-Drs.19/17055 v. 6.2.2020

2 vgl. Wissenschaftliche Dienste im Bundestag: Einstufung von Informationen als ‚GEHEIM‘ und parlamentarisches Informationsrecht, WD 3-3000-121/19 v. 13.5.2019

3 Viele „stille SMS“ bei Bund und Ländern, Netzpolitik.org v. 10.2.2020

Ortungsimpulse wie BKA und Bundespolizei zusammen (2019: 112.354, 2018: 111.628). Pro Ermittlung werden dort 400 „Stille SMS“ auf das Handy der Betroffenen geschickt.

In Metropolen wie Berlin und Hamburg, aber auch für das bevölkerungsreichste Bundesland Nordrhein-Westfalen sind diese Zahlen deutlich höher. 2019 hat die Polizei der Hauptstadt 336.569 „Stille SMS“ versandt (2018 sogar 447.972). Für Hamburg liegen die Werte zwar niedriger, aber auf ähnlichem Niveau. Aus Nordrhein-Westfalen sind sie nur bis zum Jahr 2016 bekannt; damals kamen rund 179.000 „Stille SMS“ zum Einsatz. Das war allerdings der mit Abstand niedrigste Wert seit 2007. Einige Bundesländer haben nicht auf die Informationsfreiheitsanfragen geantwortet. Aus Rheinland-Pfalz weiß man daher nur, dass die Landespolizei jährlich um die 100.000 „Stille SMS“ verschickt. Brandenburg mit rund 20.000 sowie Mecklenburg-Vorpommern mit 2.682 Fällen im Jahre 2018 sind die Schlusslichter. (Matthias Monroy)

Polizeihilfe für Chile: Spitzeln wie in BaWü

Das Landeskriminalamt (LKA) Baden-Württemberg hilft der chilenischen Polizei beim Aufbau einer Einheit für verdeckte Ermittlungen. Das ist der Antwort des Bundesinnenministeriums auf eine schriftliche Anfrage von Ulla Jelpke (Linke) zu entnehmen.[4] Mit welcher der beiden chilenischen Polizeiorganisationen das LKA kooperiert, gab das Ministerium zwar nicht bekannt. Es ist aber zu vermuten, dass die Einheit für verdeckte Ermittlungen in der Kriminalpolizei (Policía de Investigaciones) aufgebaut wird.

Für alle anderen polizeilichen Aufgaben ist die Gendarmerie (Carabineros) zuständig. Sie gehört zum Verteidigungsministerium, ihre Einheiten werden aber vom Innenminister befehligt. Die Truppe ging brutal gegen die Revolte vor, die Mitte Oktober zunächst in Santiago wegen Fahrpreiserhöhungen ausbrach und sich schnell auf das ganze Land ausbreitete. Mehr als 30 Menschen wurden bei Zusammenstößen mit der Polizei getötet, ebenso viele verloren ihr Augenlicht durch Tränengas oder Gummigeschosse.

Eine zentrale Forderung der Proteste war die bedingungslose Auflösung der Carabineros. Dessen ungeachtet stellte Chiles Präsident Sebas-

4 BT-Drs. 19/17884 v. 13.3.2020, Frage 25

tián Piñera Mitte März 2020 einen Plan zur Reform der Truppe vor. An einer Kommission zur Ausarbeitung von Vorschlägen war auch der deutsche Inspekteur der Bereitschaftspolizei der Länder, Andreas Backhoff, beteiligt.[5] Er empfahl, die Einsätze der Carabineros nachvollziehbar zu dokumentieren und mit „proaktiver Kommunikation" zu erklären. Einen Tag nach Veröffentlichung des Reformplans rief Piñera den Ausnahmezustand aus, den er mit dem Ausbruch der Corona-Epidemie begründete, und schickte zur Unterstützung der Carabineros das Militär auf die Straße. Bis zu diesem faktischen Ende der fünfmonatigen Proteste zählte das chilenische Menschenrechtsinstitut INDH fast 4.000 Verletzte, mehrere Tausend Demonstrant*innen sind in Haft.

Den „Arbeitsbesuch" des LKA Baden-Württemberg zu verdeckten Ermittlungen hat das Bundeskriminalamt (BKA) finanziert. Die Bundesbehörde ist selbst mit Ausbildungsmaßnahmen in Chile aktiv: Im Rahmen der deutschen „Polizeiaufbauhilfe" wurden dortige Polizeibehörden im vergangenen Jahr mit einem Stipendienprogramm unterstützt. Seit Ende 2019 hat das Bundesinnenministerium die Zusammenarbeit mit seinen chilenischen Partnern intensiviert. Auf Wunsch der chilenischen Regierung reisten im Dezember 2019 und im Februar 2020 Polizeidelegationen nach Santiago. Daran nahmen auch Angehörige der Berliner Polizei teil, die die chilenischen Polizeibehörden unter anderem zu „Kommunikation und Bürgerfreundlichkeit" berieten.[6]

Als Mitglied von Interpol hat das BKA Mitte Oktober 2019 auch an der Generalversammlung der internationalen Polizeiorganisation in Santiago teilgenommen. Zur Stunde des Ausbruchs der Aufstände wurde der ehemalige BKA-Vizepräsident Jürgen Stock für eine zweite Amtszeit als Interpol-Generalsekretär bestätigt. (Matthias Monroy)

Telekommunikationsüberwachung 2018

Nachdem die Zahl der Anordnungen von Telekommunikationsüberwachungen (TKÜ) 2017 gegenüber dem Vorjahr um 12,66 Prozent zurückgegangen war, haben sich die Zahlen nun wieder leicht „erholt". In der am 22. Januar 2020 vorlegten jährlichen Übersicht verzeichnet das Bun-

5 https://cdn.digital.gob.cl/filer_public/52/fe/52fe7434-e81b-48b9-b314-79cd56ce134f/consejo_carabineros_v2.pdf

6 Abgeordnetenhaus Berlin, Drs. 8/22545, eingegangen am 21.2.2020

desamt für Justiz für 2018 eine Zunahme um 4,4 Prozent.[7] Hatte es 2017 insgesamt 18.651 TKÜ-Maßnahmen gegeben, stieg diese Zahl 2018 auf 19.474. Davon wurde in 15.787 Fällen erstmals eine TKÜ angeordnet, 3.687 bestehende Anordnungen wurden verlängert.

In die Maßnahmen einbezogen waren 32.022 Telekommunikationsanschlüsse, davon 3.492 Festnetz-, 18.784 Mobilfunk- und 9.746 Internetanschlüsse. Unangefochtener Spitzenreiter der Anlassstraftaten aus dem umfassenden Katalog des § 100a Abs. 2 Strafprozessordnung (StPO) bleiben Straftaten nach dem Betäubungsmittelgesetz mit 7.846 Fällen, etwas weniger als im Vorjahr (8.108). Auf den Plätzen 2 und 3 folgen Betrug und Computerbetrug (2.874) sowie Bandendiebstahl und schwerer Bandendiebstahl (2.341). Staatsschutzdelikte im Sinne des § 100a Abs. 2 Nr. 1 StPO, darunter in erster Linie Vorfelddelikte im Bereich Terrorismus (§ 89 a, c StGB), haben mit 1.098 gegenüber 1.617 im Jahr 2017 deutlich abgenommen. Dies dürfte an der sinkenden Zahl ausreisender Djihadist*innen liegen.

Ebenfalls vorgelegt hat das Bundesamt die Statistik der Erhebung von Verkehrsdaten für 2018, in der aber die Angaben aus Bremen, Mecklenburg-Vorpommern, Rheinland-Pfalz, Saarland und Sachsen fehlen. Bemerkenswert ist dabei, dass in den elf Bundesländern, die Zahlen vorlegten, und seitens der Bundesanwaltschaft in 7.447 Verfahren 8.282 Erst- und 27 Verlängerungsanordnungen für Funkzellenabfragen (§ 100g Abs. 3 StPO) ergingen.

Bereits im November präsentierte das Bundeskriminalamt erstmals Zahlen zu seinem präventiven Einsatz von TKÜ-Maßnahmen zur „Abwehr von Gefahren des internationalen Terrorismus“.[8] Demnach hat das BKA im Berichtszeitraum vom 25. Mai 2018 bis 30. April 2019 in einem Gefahrenabwehrvorgang von seiner TKÜ-Befugnis Gebrauch gemacht. Es wurden sieben Kommunikationsanschlüsse überwacht, betroffen waren 32 Personen. Keine dieser Personen wurde im Anschluss über die Durchführung der Maßnahmen informiert. (Dirk Burczyk)

7 www.bundesjustizamt.de/DE/Themen/Buergerdienste/Justizstatistik/Telekommunikation/Telekommunikationsueberwachung_node.html

8 BT-Drs. 19/15570 v. 21.11.2019

Meldungen aus Europa

Schwieriger Start der Europäischen Staatsanwaltschaft

Am 16. Oktober haben der EU-Parlamentspräsident und die Fraktionsvorsitzenden die Rumänin Laura Codruta Kövesi als erste Generalstaatsanwältin der Europäischen Union förmlich bestätigt.[1] Sie leitet nun die neue Europäische Staatsanwaltschaft (EUStA), die ab November 2020 eigene Ermittlungen anstellen darf.[2] Diese sind zunächst auf Straftaten zulasten des EU-Haushaltes beschränkt, darunter Betrug, Korruption, grenzüberschreitender Mehrwertsteuerbetrug ab einer Schadenshöhe von 10 Mio. Euro. Die EUStA kann außerdem Strafverfolgungsmaßnahmen ergreifen und vor den zuständigen Gerichten der Mitgliedstaaten die Aufgaben der Staatsanwaltschaft wahrnehmen. Derzeit beteiligen sich 22 Mitgliedstaaten an der EUStA.

Kövesi rechnet mit zunächst 3.000 Fällen aus den Mitgliedstaaten, jedes Jahr könnten dann rund 2.000 weitere hinzukommen.[3] Weil derzeit nur 29 Mitarbeiter*innen eingestellt worden sind, befürchtet die Generalstaatsanwältin einen schleppenden Start der EUStA. Zudem muss das Kollegium der aus den beteiligten Mitgliedstaaten entsandten Europäischen Staatsanwält*innen noch gebildet werden. Erst wenn dieses vollständig ist, können Kooperationsverträge mit Agenturen wie Eurojust oder Europol geschlossen werden. In jedem Mitgliedstaat werden außerdem „Delegierte Europäische Staatsanwälte“ bestimmt. Deren Zahl stuft Kövesi als zu gering ein.

Kövesis Ernennung war lange umstritten. Die Abgeordneten hatten sie neben dem Franzosen Jean-François Bohnert und dem Deutschen Andrés Ritter als bevorzugte Kandidatin vorgeschlagen, der zuständige Ausschuss für bürgerliche Freiheiten (LIBE) nominierte sie schließlich.

1 „Laura Codruţa Kövesi wird erste Europäische Generalstaatsanwältin“, Pressemitteilung des Europäischen Parlaments v. 22.10.2019

2 vgl. Verordnung (EU) 2017/1939, in: Amtsblatt der EU L 283 v. 31.10.2017

3 https://multimedia.europarl.europa.eu/de/libe-committee-meeting-establishment-of-european-public-prosecutor-office-presentation-of-state-of-p_20200206_EP-099756A_BBO_370

Der Rat der EU-Justizminister favorisierte dagegen Bohnert. Erst im September sprach sich die Mehrheit der EU-Mitgliedsstaaten für Kövesi aus. Rumänien selbst lehnte ihre Ernennung bis zum Ende ab. Kövesi war Leiterin der rumänischen Korruptionsbekämpfungsbehörde und leitete dort mehr als 300 Ermittlungsverfahren gegen Minister, Abgeordnete und Kommunalpolitiker ein. Rumänische Behörden ermittelten gegen Kövesi, zwei Disziplinarverfahren wurden allerdings eingestellt. Weitere Ermittlungen erfolgten ab Frühjahr 2019 wegen des Vorwurfs der Korruption, diese wurden ebenfalls eingestellt. In einem neuen Sonderermittlungsausschuss wird nun abermals gegen Kövesi wegen Korruption, Amtsmissbrauch und Falschaussage ermittelt. Beobachter*innen bewerten dies als eine Kampagne, die durch den vorbestraften Chef der regierenden Sozialdemokraten (PSD), Liviu Dragnea, gesteuert werde.[4] Der Oberste Kassations- und Justizgerichtshof hatte Dragnea – wegen Korruption – zu drei Jahren und sechs Monaten Haft verurteilt.

(Matthias Monroy)

Polizeizugriffe auf Eurodac

Seit dem 20. Juli 2015 können Polizeibehörden zur „Verhütung, Aufdeckung oder Untersuchung terroristischer oder sonstiger schwerer Straftaten“ auf Eurodac, die europäische Datenbank mit Fingerabdrücken von Asylsuchenden, zugreifen, wenn zuvor ein Datenabgleich mit nationalen Datenbanken, dem Prüm-Netzwerk und dem Visa-Informationssystem erfolglos war. Europol nutzt die Möglichkeit seit 2017 über eine Schnittstelle der niederländischen Polizei.

Bis Ende 2019 wurde Eurodac 1.840-mal von Polizeien abgefragt.[5] Der Kreis der zugriffsberechtigten Länder ist zwar deutlich gewachsen, weil immer mehr Mitgliedstaaten die Prüm-Beschlüsse umsetzen und damit die Voraussetzung für den polizeilichen Zugriff auf die Eurodac-Daten erfüllen. Dennoch steigt die Zahl der Abfragen nicht kontinuierlich: 2017 hatte sie mit 664 Abfragen einen Höhepunkt, sank aber danach auf 306 in 2018 und 449 in 2019. Bis dahin hatten Behörden aus 14 Mitgliedstaaten die Möglichkeit genutzt, wobei die meisten Abfragen

4 „Die Gefürchtete“, Süddeutsche Zeitung v. 2.4.2019

5 Eigene Berechnungen auf Grundlage der Eurodac-Statistiken der EU-Agentur für das Betriebsmanagement der großen IT-System (eu-LISA) von 2015 bis 2019

aus Deutschland (59 Prozent) und Österreich (18 Prozent) kamen. Europol startete seinen Zugriff mit einem Massenabgleich von 105 Datensätzen, die es vom Terrorist Screening Centre des FBI erhalten hatte.[6] 2019 fragte das EU-Polizeiamt Eurodac kein einziges Mal ab.

Mehr als die Hälfte der Abfragen (N=989) erfolgte mit erkennungsdienstlichen Daten, diente also etwa zur Identitätsklärung von Personen, die der Polizei bekannt waren. Sie produzierten 1.013 Treffer (teilweise zu einer Person in mehreren Ländern). 851 Abfragen erfolgten mit Tatortspuren von unbekannten Personen. Hier gibt es keine Daten zum Ergebnis, da die Eurodac-Zentraleinheit keine eindeutigen „Treffer" an die abfragenden Behörden zurückmeldet, sondern nur Listen mit möglichen (sprich: ähnlichen) Kandidat*innen für einen Treffer, der dann von Daktyloskopen der Mitgliedstaaten manuell ermittelt werden muss.

Keine Informationen liegen vor über die Art und Schwere der aufzuklärenden Straftaten bzw. abzuwehrenden Gefahren oder den tatsächlichen polizeilichen Nutzen. Bis heute steht die nach Art. 40 der Eurodac-Verordnung vorgeschriebene Evaluierung durch die Kommission aus. Die sollte eigentlich Auswirkungen auf die Grundrechte überprüfen und u. a. prüfen, ob und inwiefern die polizeiliche Nutzung der Datenbank zur Diskriminierung von Asylsuchenden geführt hat. Anfang 2019 hatte der damalige Innenkommissar Dimitris Avramopoulos dazu gegenüber dem Europaparlament erklärt, dass man „das Gefühl" hatte, eine Evaluierung wäre angesichts der Verhandlungen um das Gemeinsame Europäische Asylsystem im Zeichen der „Flüchtlingskrise" nur „verwirrend und ablenkend" gewesen.[7] (Eric Töpfer)

Neue deutsch-französische Polizeieinheit

Die Bundespolizei und die Gendarmerie Nationale aus Frankreich haben eine „deutsch-französische Einsatzeinheit" (DFEE) gebildet.[8] Im Januar 2019 hatten die Regierungen der beiden Länder im Aachener Vertrag die Einrichtung der Truppe für „Stabilisierungsoperationen in Drittstaaten" verabredet, Einzelheiten regelt eine Verwaltungsvereinbarung. Vorgese-

6 Europol: 2017 Consolidated Annual Activity Report, Den Haag 2018, S. 36

7 Brief von Avramopolous an Claude Moraes, den Vorsitzenden des LIBE-Ausschusses, v. 22.1.2019

8 „Deutsch-Französische Einsatzeinheit unterstützt Bundespolizei im Wiesn-Einsatz", Meldung der Bundespolizeidirektion München v. 5.10.2019

hen sind Einsätze in „frankophonen Drittstaaten“, bei Großveranstaltungen und „im gemeinsamen Grenzgebiet“.

Die DFEE besteht derzeit aus jeweils zehn Angehörigen von Bundespolizei und Gendarmerie, in diesem Jahr soll sie auf jeweils 15 Beamt*innen anwachsen. Von deutscher Seite stammen die Polizist*innen aus der Kaserne im rheinland-pfälzischen Bad Bergzabern. Laut dem Bundesinnenministerium (BMI) handelt es sich bei der DFEE trotz des Namens „nicht um eine feste eigenständige Organisationseinheit“, sie werde vielmehr „anlassbezogen aufgerufen“.[9] Einsätze erfolgten bereits vor Unterzeichnung der Verwaltungsvereinbarung auf dem Münchner Oktoberfest und dem Cannstatter Wasen, anschließend war die Truppe zur Vorbereitung der Tour de France und zu einem Champions League-Spiel in Dortmund sowie – erstmals in voller Stärke - beim G-7-Gipfel in Frankreich eingesetzt. Im Grenzgebiet wird die DFEE außerdem im Rahmen sogenannter „Hubschraubersprungfahndungen“ angefordert. Rechtsgrundlage der gemeinsamen Einsätze sind laut BMI das bilaterale Mondorfer Abkommen „über die Zusammenarbeit der Polizei- und Zollbehörden in den Grenzgebieten“ von 1997, den Prümer Vertrag von 2005 sowie die Prüm-Beschlüsse der EU von 2008.

Die Beamt*innen der DFEE treffen sich auch regelmäßig zu „Fortbildungsveranstaltungen“. Neben Sprachtrainings geht es dabei unter anderem um Grundlagen der „polizeilichen Auslandsverwendung“ sowie die unterschiedliche „Polizeitaktik“ in beiden Ländern. Trainings erfolgten am Nationalen Ausbildungszentrum der Gendarmerie in St. Astier und einem Gendarmerie-Standort im ostfranzösischen Baccarat sowie bei der Bundespolizei in Bad Bergzabern. Alle weiteren geplanten Veranstaltungen sind derzeit wegen der Corona-Pandemie ausgesetzt.

Die Gendarmerie Nationale gehört nach wie vor zum Verteidigungsministerium und wurde erst 2009 gleichzeitig dem Innenministerium unterstellt.[10] Die Bundespolizei arbeitet nunmehr also eng mit einer Polizeibehörde zusammen, deren Angehörige eine militärische Grundausbildung durchlaufen und Kombattantenstatus haben. Die französische Gendarmerie gehört mit den italienischen Carabinieri zu den Gründern der „Europäischen Gendarmerietruppe“ (EUROGENDFOR).

(Matthias Monroy)

9 BT-Drs. 19/18092 v. 8.4.2020

10 www.senat.fr/dossier-legislatif/pjl07-499.html

Literatur

Zum Schwerpunkt

Die Digitalisierung der Polizeiarbeit war und ist ein bürgerrechtliches Dauerthema. Denn was die Apparate sich von ihrer technischen Modernisierung versprechen, das stellt sich für deren Kritiker*innen als Bedrohung dar: Wirksamkeitshoffnungen stehen Wirksamkeitsbefürchtungen gegenüber. Für Bürgerrechte & Polizei/Cilip steht im Zentrum, wie durch „Technik" die Definitionsmacht, die Ressourcen und Handlungsoptionen von Polizei und Geheimdiensten gegenüber Bürger*innen wachsen, wie technik- bzw. edv-gestützt Grundrechte ausgehöhlt werden. Mit dem Schwerpunkt dieses Heftes gehen wir gewissermaßen einen Schritt zurück, indem wir zunächst nur beleuchten, wie die Digitalisierung polizeiliches Handeln verändert oder verändern wird. Für die Modernisierungsbefürworter*innen in den Apparaten steht hingegen eine andere Perspektive im Zentrum: Sie sehen die Behörden im ständigen Wettlauf mit Gefährder*innen und Straftäter*innen, die in jeder technologischen Weiterentwicklung neue und perfidere Straftaten (oder schädigendes Verhalten) entdecken. Digitalisierung der Polizei muss der Digitalisierung der Kriminellen folgen, so der Tenor. Und damit sie dies tun kann, müssen Ressourcen, Personal und rechtliche Befugnisse geschaffen werden. Was die Digitalisierung im polizeilichen Alltag bedeutet, kommt auch in diesen Diskussionen nur am Rande vor.

Rüdiger, Thomas-Gabriel; Bayerl, Petra Saskia (Hg.): *Digitale Polizeiarbeit. Herausforderungen und Chancen, Wiesbaden (Springer VS) 2018, 301 S.*
Dieser Sammelband kann exemplarisch für die Diskussion in Deutschland genannt werden. Es überwiegen zwei Perspektiven: Erstens, dass die Polizei nicht gerüstet sei und dringend gerüstet werden müsse, um den neuen Gefahren („Cybercrime" etc.) entgegentreten zu können: technische Ausstattung, Kooperationen mit der IT-Industrie, Qualifikation und Rekrutierung des Personals. Und zweitens, dass in der Digitalisierung auch Chancen für die Arbeit der Polizei lägen, etwa indem sie Soziale Medien nutzt oder Bürgernähe digital gewährleiste.

Hering, Andreas; Vera, Antonio: *Polizei 4.0 und digitale Arbeitswelt: Eine qualitativ-empirische Untersuchung am Beispiel der Polizei NRW, in: Ritsert, Rolf; Vera, Antonio (Hg.): Management und Organisation in der Polizei. Studien zu Digitalisierung, Change Management, Motivation und Arbeitsgestaltung, Wiesbaden (Springer Gabler) 2020, S. 199-260*
Der Beitrag untersucht beispielhaft die Auswirkungen der polizeilichen Digitalisierung auf den „Arbeitsplatz Polizei". Im Kern geht es dabei um die Auswertung von acht qualitativen Interviews, die mit (leitenden) Polizeibeamt*innen geführt wurden. Die Herausforderungen, vor denen die Polizeien stehen, reichen von der Gestaltung der flexibilisierten Arbeitszeiten, über das Gesundheitsmanagement bis zu den Kriterien der Personalauswahl oder dem „war for talents" mit der Industrie. Wie ein solcher Innovationsschub die Polizeiarbeit qualitativ – in ihrer Ausrichtung, ihren Handlungslogiken, ihren Entscheidungsabläufen – verändern wird, das wird nicht betrachtet.

Hauber, Judith: *Postfaktizität und Predictive Policing, in: Lange, Hans-Jürgen; Wendekamm, Michaela (Hg.): Postfaktische Sicherheitspolitik. Gewährleistung von Sicherheit in unübersichtlichen Zeiten, Wiesbaden (Springer VS) 2019, S. 191-209*
Hauber ist Mitarbeiterin der Kriminologischen Zentralstelle der Polizei Hamburg. Sie fasst die Ergebnisse ihres Forschungsprojekts zur „vorhersagebasierten Polizeiarbeit" zusammen. Im ersten Teil werden die verschiedenen Versuche, Kriminalitätsbekämpfung mittels Predictive Policing zu betreiben in den Bereich des Postfaktischen verwiesen, weil sie mit ungeprüften theoretischen Versatzstücken und unzureichenden Operationalisierungen auf der Basis unklaren empirischen Wissens arbeiten und deshalb Wirksamkeit behaupten statt erzielen. Auf der Basis dieser Kritik entwickelt Hauber das Modell einer „problemorientierten Kriminalpolitik", in der „Technik lediglich als Hilfsmittel der polizeilichen Informationsverarbeitung zum Einsatz kommen" soll. Damit werden die Visionen der Digitalisierer*innen auf ein klassisches Maß gestutzt: Die EDV schafft kein Wissen neuer Qualität, sondern sie soll helfen, dass die Polizei ihre Arbeit (besser, effektiver etc.) tut. Eingebunden werden sollen die EDV-Anwendungen in das Konzept der „problemorientierten Polizeiarbeit", das seit Anfang der 1990er Jahre von Herman Goldstein entwickelt wurde. Die aufgrund theoretischer Annahmen programmierte Software führt zu einer „Identifikation und Analyse des Kriminalitätsproblems", so dass die ihm zugrundeliegenden

Probleme offenbart und dann gelöst werden können. Offen bleibt, wie die polizeiliche Praxis dazu bewegt und befähigt werden soll, kriminologischen Erkenntnissen zu folgen. Und fast noch wichtiger: Welche Kriminalitätsprobleme sind denn kausal (bei Goldstein „problem solving") durch die Polizei lösbar?

Houy, Constantin; Gutermuth, Oliver; Dadashnia, Sharam; Loos, Peter: *Digitale Polizeiarbeit, in: Klenk, Tanja; Nullmeier, Frank; Wewer, Göttrik (Hg.): Handbuch Digitalisierung in Staat und Verwaltung, Wiesbaden (Springer VS) 2019 (eBook)*
Der Aufsatz gibt auf zehn Seiten einen knappen Überblick über die Felder „digitaler Polizeiarbeit". Einerseits werden die Notwendigkeiten und Chancen „elektronischer Hilfsmittel" gesehen, andererseits dürften deren Risiken (etwa die „Diskriminierung von Personen") nicht vernachlässigt werden. Zwei Anwendungsfelder („Predictive Policing" und „Mobile digitale Polizeiarbeit" werden ebenso kurz vorgestellt wie die Pilotprojekte in den Bundesländern. „Big Data" werde an Bedeutung für Kriminalitätsbekämpfung und -prävention zunehmen; die Digitalisierung biete „organisationale Effizienzpotenziale", die die Arbeit „beschleunigen" und „das Informationsmanagement verbessern können".

Bergien, Rüdiger: *„Big Data" als Vision. Computereinführung und Organisationswandel in BKA und Staatssicherheit (1967-1989), in: Zeithistorische Forschungen 2017, S. 258-285*
Dieser lesenswerte Aufsatz beleuchtet die Frühphase der Digitalisierung in den staatlichen Sicherheitsapparaten – origineller- und erhellenderweise im Vergleich von Bundeskriminalamt und dem Ministerium für Staatssicherheit. Erstaunlich sind nicht nur die Parallelität der Entwicklung, sondern auch die jeweiligen Widerstände in den Apparaten, die den Visionen der Computerenthusiast*innen erfolgreich entgegengebracht wurden. Unterhalb des „großen Wurfs" von Zentralisierung und Vereinheitlichung findet aber ein institutioneller Wandel statt, der die Polizei langfristig verändert, etwa indem die Bedeutung von EDV-Spezialist*innen gegenüber den Cop Culture-Sozialisierten wächst. Wie weit dieser Einfluss geht und was er für die Ausrichtung von Polizeiarbeit bedeutet, bleibt allerdings offen.

Aus dem Netz

https://police-it.org

Wer sich über den Stand der Digitalisierung der deutschen Polizeiarbeit informieren möchte und sich nicht auf die spärlichen Informationen der Behörden und Ministerien verlassen möchte, muss diese Seite besuchen. Annette Brückner, von 1993 bis 2013 mit der Konzeption und Entwicklung polizeilicher Informationssysteme im In- und Ausland befasst, beschreibt sich selbst als „Kopf hinter POLICE-IT". Als Ziel ihres Portals benennt sie: „Bürger – von denen jeder mehr oder minder freiwillig Lieferant für polizeiliche Informationssysteme sein kann – aber auch Polizisten, Anwälte, Juristen, Journalisten und Politikern fachliches und technisches Know-How zur Verfügung zu stellen, damit sie besser verstehen, was sich hier vor ihrer aller Augen entwickelt."

Jenseits von „Tipps und Tricks", die sich an die Anwender*innen in den Behörden wenden, sind die Informationen in drei Bereiche gegliedert: Unter „Home" befindet sich der POLICE-IT Blog, in dem laufend Beträge zu aktuellen Themen veröffentlicht werden. Über den RSS Feed sind diese Meldungen abonnierbar. Der Blog ist über Kategorien erschließbar, die über die Sitemap zugänglich sind. In der Rubrik „Glossar" werden wichtige Begriffe, Institutionen und Akteur*innen erklärt. Hier erfährt man, was CRIME oder wer Rola Security Solutions ist. Im dritten Informationsbereich befinden sich – gegenwärtig sechs – Dossiers. Dabei handelt es sich um die thematische Zusammenstellung der verschiedenen Berichte die auf POLICE-IT erschienen sind, wie beim „INPOL-Dossier", oder um fortlaufende Berichte, etwa zum Komplex „Hessendata/Palantir": Dort finden sich nicht nur Informationen, z.B. zum Untersuchungsausschuss des hessischen Landtags, die man auch der Tagespresse entnehmen könnte. Vielmehr wird man in diesem Dossier auch über die Funktionsweise des Systems „Hessendata" so informiert (etwa in Teil 5 vom November 2018), dass auch Lai*innen verständlich wird, wie es funktionieren soll. Regelmäßig werden Quellen und Bezugsdokumente in den Dossiers und Meldungen genannt.

Die Suchfunktion von POLICE-IT erlaubt eine Freitextsuche über das gesamte Informationsangebot und eine Einschränkung über den Erscheinungszeitraum (Monatsarchiv). Wer spezifische Informationen sucht, wird schnell fündig werden.

Sonstige Neuerscheinungen

Eick, Volker; Arnold, Jörg (Hg.): *40 Jahre RAV. Im Kampf um die freie Advokatur und um ein demokratisches Recht, Münster (Westfälisches Dampfboot) 2019, 423 S., 35,– EUR*

Es gibt Institutionen, die müsste man erfinden, wenn es sie nicht schon gäbe. Der „Republikanische Anwältinnen- und Anwälteverein" gehört zweifellos in diese Kategorie. Denn dass Jurist*innen sich ihrer politischen Funktion und ihres professionellen Auftrags bewusst sind und dass sie daraus Motivation und Engagement zum kollektiven Handeln entwickeln, das ist der demokratisch gebotene Ausweg aus der Ambivalenz des Rechts: Einerseits im Rahmen der geltenden Rechtsordnung das anwaltschaftliche Mandat „in freier Advokatur" wahrzunehmen, d.h. das Recht für alle und frei von staatlichen Eingriffen zur Geltung zu bringen und darin die Chance zu sehen, „Recht" gerade auch für „sozial schwache" Gruppen durchzusetzen. Und anderseits die Rechtsordnung als Ausdruck von Herrschaftsverhältnissen wahrzunehmen, die verändert werden muss, wenn ihr „Klassencharakter" – um diesen altmodischen Begriff zu nutzen – nicht überhand nehmen soll.

Nun hat der RAV zu seinem 40ten sich und der Öffentlichkeit ein Geschenk gemacht, indem er einen Band vorgelegt hat, der Einblicke in seine Entstehungsgeschichte und sein Selbstverständnis, in die Breite seiner thematischen und strategischen Ausrichtung und in die Optionen zukünftiger Entwicklung gibt. Der Band versammelt insgesamt 37 Beiträge aus den Reihen des RAV (und befreundeter Organisationen), die in acht Kapiteln präsentiert werden: Dabei gelten die Kapitel 6-8 den eher institutionellen Aspekten: Rück- und Ausblick (Kap. 6), Berichte aus der „Gründergeneration" (Kap. 8) und der Blick der „Partner" auf den RAV (Grundrechtekomitee, Humanistische Union …, Kap. 7). Die ersten sechs Kapitel gelten der im engeren Sinne inhaltlichen Seite der RAV-Arbeit: Rechtstheorie und -kritik, Rechtspolitik und Rechtsruck, Kriminalpolitik, Anwaltspraxis und die Gefährdung des Rechtsstaats sowie „Sicherheitsrecht und Rechtsstaat". Unter diesen Überschriften sind ganz unterschiedliche Beiträge versammelt: von der Missachtung des Europäischen Gerichtshofs für Menschenrechte durch den Bundesgerichtshof, über die Rolle der Nebenklagevertretung in Verfahren wegen rechtsextremistisch motivierter Straftaten, bis zur Prozessbeobachtung in der Türkei oder zur Reform des Sexualstrafrechts. Was in diesen

Teilen präsentiert wird, sind nicht die Positionen des RAV, sondern das Spektrum der fachlichen Auseinandersetzungen, die sich aus dem in der Präambel der Satzung formulierten Ziel ergeben, das „Recht … zugunsten des oder der Schwächeren zu nutzen und zu entwickeln".

Zwei exemplarische Blicke, warum die Lektüre des Bandes lohnend ist. Zunächst zur rechtspolitischen Diagnose aus Sicht des RAV. Der gegenwärtige Vorsitzende Peer Stolle schreibt, es stehe „die Möglichkeit im Raum, dass sich in Europa eine neue Form des Faschismus entwickeln kann" (S. 342). „Autoritärer Sicherheitsstaat" oder „Sicherheitsgesellschaft" – beide vorher von Stolle zitierten Charakterisierungen treffen die antidemokratischen Gefahren vermutlich treffender als die Bilder, die mit „Faschismus" hervorgerufen werden. Am anderen Ende der Einschätzungen liegt der Beitrag von Wolfgang Wieland, wie dem informativen Anhang zu entnehmen ist, RAV-Vorsitzender von 1989-1996. Er ruft dazu auf, die Erfolge der eigenen Arbeit in Rechnung und sich den Realitäten zu stellen, statt „unterkomplex" immer dieselben Antworten zu geben. „Wem vierzig Jahre", so Wieland, nichts anderes einfalle als die „Warnung ‚Es ist Fünf vor Zwölf', für den muss ansonsten die Zeit stehen geblieben sein." (S. 397) Hier werden wohl Sensibilität und Alarmismus verwechselt. Und um bei der Metapher zu bleiben: Bei der Uhr, die den Abbau von demokratischen Standards zählt, gibt es immer wieder eine zwölfte Stunde, die besser nicht anbrechen sollte.

Der zweite Blick fällt auf jene Beiträge, die sich direkt mit den Apparaten beschäftigen – vornehmlich mit der Polizei, bei Udo Kauß und Rolf Gössner explizit mit dem „Verfassungsschutz". Auf die Polizei blicken die RAV-Autor*innen vor allem unter der Perspektive der Entgrenzungen. Das beginnt im 1. Kapitel mit Volker Eicks Aufsatz zum Aufstieg der privaten Sicherheitsdienstleister als Ausdruck der Kommerzialisierung von öffentlicher Sicherheit. Im 2. Kapitel widmet sich Klaus Bartl der „Sächsischen Demokratie", indem er den Zusammenhang zwischen strammer CDU-Dominanz, gezieltem Jurist*innen-Import aus den alten Bundesländern, einer Rechtspraxis, die gegen demokratische Kritik in Stellung gebracht wird und gleichzeitig Polizeieingriffe absegnet, sowie dem Sparkurs der Landesregierungen nachzeichnet, die der Justizkritik von rechts den Boden bereitet. Im 3. Kapitel zeichnet Roland Hefendehl am Beispiel von Freiburg im Breisgau die fragwürdige Konstruktion „gefährlicher Räume" nach. Offenkundig wird hier, wie sachlich oberflächlich und wenig überzeugend die Deklaration derartiger Räume ist.

Nicht die Räume sind gefährlich, sondern die Sonderrechte, die der Polizei mit dieser Rechtsfigur eingeräumt werden.

Aus den Beiträgen im 4. Kapitel wird deutlich, was „Anwaltspraxis" im RAV-Verständnis bedeutet. Zwei Beispiele: Gabriele Heinecke stellt die „politische Justiz" im Kontext des G20-Gipfels 2017 am Beispiel des 18-Jährigen Fabio V. dar, dem ein besonders schwerer Fall des Landfriedensbruchs vorgeworfen wird (Indiz: schwarze Jacke, dunkle Turnschuhe). Anna Luczak (S. 207 ff.) schildert die Vorgänge rund um den „Anwaltlichen Notdienst G8 Heiligendamm" im Sommer 2007. Sie beginnt mit den bundesweiten Hausdurchsuchungen und verdeckten Überwachungen im Vorfeld des Gipfels (erst im Herbst stellt der Bundesgerichtshof fest, dass die Rechtsgrundlage für diese Maßnahmen nicht erfüllt war). Im nahen Vorfeld und während des Gipfels wehrten sich die Anwält*innen gegen die polizeilichen Allgemeinverfügungen und die Einschränkungen des Versammlungsrechts. Dies gelang nur eingeschränkt, u. a. auch deshalb, weil die Gerichte mit gezielten polizeilichen Falschinformationen versorgt wurden. Als Schwerpunkt der Arbeit wird der anwaltschaftliche Kampf gegen die über 1.000 polizeilichen Freiheitsentziehungen geschildert: beginnend bei den praktischen Schikanen, überhaupt Kontakt zu den in den „Gefangenensammelstellen" Einsitzenden zu erhalten, über die teils unwürdige Käfighaltung bis zu dem Umstand, dass es der Polizei in der Mehrzahl der Fälle darum ging, die Betroffenen auf polizeirechtlicher Basis für einige Zeit aus dem Verkehr zu ziehen. Der „Ausnahmezustand" ist offenkundig eine Frage des politisch-polizeilichen Willens. Und anwaltschaftlich muss man sich mit kleinen – mitunter erst nachträglich eintretenden – Erfolgen zufrieden geben. (alle: Norbert Pütter)

Wächtler, Hartmut: *Widerspruch. Als Strafverteidiger in politischen Prozessen, Berlin (TRANSIT-Verlag) 2018, 173 S., 20,00 EUR*

Hartmut Wächtler, Jahrgang 1944, gehört zu den renommiertesten politischen Strafverteidiger*innen in Deutschland. Dabei war das ursprünglich gar nicht so klar, denn zunächst hatte er sich für das Jurastudium nur entschieden, „weil man dort ein weites berufliches Spektrum hatte und sich nicht so schnell würde entscheiden müssen" (S. 164). An der erzkonzervativen Münchner Ludwig-Maximilians-Universität, die wie andere Unis auch, noch munter von Ex-Nazis durchsetzt war, geriet er dann in den Strudel der aufbegehrenden Studentenschaft der 1968er Jahre. So erlebte er die seinerzeitigen politischen und juristischen Re-

pressalien aus erster Hand, engagierte sich in der „Rechtshilfe der APO“ und wurde 1973 schließlich Rechtsanwalt und Strafverteidiger. In diesem Buch schildert er einige seiner zahlreichen Fälle – wie die Verfahren gegen Rolf Pohle (S. 69) und Ulrike Meinhof (S. 85), den Berliner Tenno-Prozess (S. 109) oder die zahlreichen Verhandlungen im Zusammenhang mit dem Widerstand gegen die atomare Wiederaufbereitungsanlage in Wackersdorf (S. 130) – ebenso wie damit verbundene juristische Schikanen gegen sich selbst. Das alles präsentiert er recht detailgetreu, mit sarkastischem Humor und auch nicht ohne Selbstironie. Eine seiner Erkenntnisse dabei etwa lautet: „Die Justiz damals wie heute schätzt eine zu genaue Protokollierung der Verhandlung nicht“ (S. 75).

Für die Älteren (auch außerhalb Bayerns) ist sein Buch grausig amüsant und es kommen dabei auch immer wieder eigene, längst vergraben geglaubte Erinnerungen hoch. Für Jüngere dürfte vieles als kaum nachvollziehbare Vergangenheit erscheinen. Lesenswert ist es auch für sie. Denn was alles so passieren kann, zeigt der Fall um „Ricarda“ (S. 169ff.) – aus dem Jahre 2017, und das ist schließlich noch nicht so lange her.

(Otto Diederichs)

Theune, Lukas: *Polizeibeamte als Berufszeugen im Strafverfahren. Baden-Baden (Nomos) 2020, 281 S., 74,– EUR*

Die Praxisrelevanz der Berufszeug*innen im Strafverfahren ist unbestritten. Sie sind in einer Vielzahl von Hauptverhandlungen als Ermittlungsbeamt*innen, aber auch als unmittelbare Tatzeug*innen von zentraler Bedeutung und besitzen dort mit den Worten des Kriminologen Fritz Sack die „Herrschaft über die Wirklichkeit“. Umso mehr überrascht es, dass dieses Thema in der juristischen Wissenschaft, abgesehen von wenigen Fachaufsätzen und Anmerkungen in Lehrbüchern, bislang kaum einen größeren Niederschlag gefunden hat. Diese Forschungslücke schließt nun Rechtsanwalt Lukas Theune mit seiner Promotionsarbeit.

Die von Prof. Tobias Singelnstein (Ruhr-Universität Bochum) betreute Arbeit stellt eine systematische Untersuchung der rechtlichen und tatsächlichen Besonderheiten dieser Zeug*innengruppe dar und analysiert den Umgang der Strafjustiz mit diesem Beweismittel. Beschrieben wird etwa die Tatsache, dass Polizeizeug*innen von der Justiz eine ganze Reihe von nicht-kodifizierten Sonderrechten eingeräumt wird, welche im deutlichen Widerspruch zu den Regelungen der Strafprozessordnung stehen. Hierzu gehören etwa das von der Rechtsprechung nicht hinterfragte vermeintliche Recht dieser Zeug*innengruppe, sich durch das

Lesen der eigenen schriftlichen Aussage (und vielfach auch der Aussagen der Kolleg*innen) auf die Gerichtsverhandlung vorbereiten zu dürfen, und sich keiner Vernehmung unterziehen zu müssen, sondern die Aussage in Form eines schriftlichen Vermerks zu den Akten zu reichen.

Ein Schwerpunkt stellt dabei die Darstellung der Forschungsergebnisse zu den aussage- und wahrnehmungspsychologischen Eigenarten der Polizeizeug*innen dar. Also etwa die Frage nach den Umständen, unter denen eine Aussage entstanden ist, welche Motivation dem Aussageverhalten zugrunde liegt oder welche Bedeutung die berufsbedingte Routine sowie Gruppenvorurteile und Feindbilder haben. Aber auch die Untersuchung der Bedeutung des polizeilichen Korpsgeistes, der „Cop Culture" und des Konformitätsdrucks für die Glaubhaftigkeit der Zeug*innenaussage.

Die gewonnenen aussagepsychologischen Erkenntnisse wurden von Theune in einem zweiten Schritt in Form von qualitativen Expert*inneninterviews überprüft. Dabei wurden Richter*innen, Staatsanwält*innen und Verteidiger*innen als Spezialist*innen mit dem notwendigen forensischen Praxiswissen befragt. Untersucht wurde dabei die Frage, ob die Aussagen von Berufszeug*innen vor Gericht eine gegenüber sonstigen Zeug*innen besondere Würdigung erfahren. Als Ergebnis ist festzustellen, dass Richter*innen und Staatsanwält*innen ein besonderes Vertrauen in die Richtigkeit der Angaben von Polizeizeug*innen besitzen. Es bestätigt sich damit die allgemeine Erfahrung von Strafverteidiger*innen, wonach diese Zeug*innen beim Gericht ein besonderes Ansehen besitzen und eine Art „Zeug*innen 1. Klasse" darstellen. Die Richter*innen haben regelmäßig weder das erforderliche Fachwissen noch ein Interesse daran, die Glaubhaftigkeit dieser Aussagen intensiv zu überprüfen. Ihnen dienen die Aussagen der Polizeibeamt*innen pragmatisch dazu, den Akteninhalt aus dem Ermittlungsverfahren ohne kritische Überprüfung vollständig in die Hauptverhandlung einzuführen.

Resümierend schreibt der Autor: „Die klassische Funktion der Judikative als die Exekutive kontrollierende und überprüfende Gewalt wird von den Gerichten vernachlässigt; vielmehr herrscht ein Gefühl des gemeinsamen Auftrags der Strafverfolger von Polizei über Staatsanwaltschaft bis hin zum Gericht vor, das ein besonderes Näheverhältnis und Vertrauen mit sich bringt." Es wäre wünschenswert, wenn das Buch von Lukas Theune den Weg auf jeden Strafrichtertisch finden würde.

(Ulrich von Klinggräff)

Summaries

Thematic Focus: Data Culture

Looking Ahead Through the Data Jungle. Datafication and Prevention – An Introduction

by Benjamin Derin, Christian Meyer and Friederike Wegner

That governments are interested in data is by no means a new insight. But with advancing digitalization, potential uses for information are reaching new levels – and so is their pursuit by the police. The already large administrative appetite for data is now falling upon a more susceptible society that is increasingly adhering to the dogma of prevention and is redefining its understanding of security and risk.

From Card Files to Data Warehouses

by Dirk Burzcyk

The history of automated data processing by the German police began with the INPOL system in the 70s. Since the 90s, the police have regularly presented new plans to modernize their information systems. INPOL-neu was followed by PIAV, and with the current "Polizei 2020" project, the next attempt is being made at replacing the separate "data silos" with a joint data warehouse for all of German police.

Tactical Resource: Smartphone

by Stephanie Schmidt

Equipping German police with smartphones is part of the "Polizei 2020" project and aims at facilitating police officers' daily work routines. But smartphones are not merely technical devices influencing official day-to-day routine through apps and messengers. As social objects, they suggest actions and communicative practices which discursively duplicate crisis and hazard scenarios.

Data Protection is Turning into an Empty Vessel

Interview with the data protection commissioner of Hamburg

Johannes Caspar unsuccessfully tried to bar the police from storing tens of thousands of facial images after the G20 summit. Matthias Monroy talked to him about the role of data protection in the automation of information systems, police in social media, encryption, and EU cooperation.

Artificial Intelligence in Police Work

by Nina Galla

At least 75 countries are employing artificial intelligence (AI) for police purposes. Pilot projects exist in Germany, as well. In general, AI causes investigations to shift to an earlier point in time due to machine-detected correlations. The problems become apparent when considering how machines learn, how they reach decisions, and how these decisions are dealt with.

A Short History of Automated Facial Recognition

by Roland Meyer

In a concerted action by police and security authorities on the one hand and commercial enterprises on the other, the development of automated facial recognition has been pressed ahead since the 1960s. Failed attempts and persistently high false-positive quotas have not stopped this storyline. It's high time for a political discussion.

The SIS – 220 Queries per Second

by Matthias Monroy

Europe's largest wanted-persons database has been expanded in recent years. The amount of alerts and queries is rising significantly. Currently, additional functions are being gradually implemented, and the group of users whom access is granted is being broadened. Furthermore, the EU "Interoperability" project connects the SIS with other EU databases. Now, "Brexit" is sowing confusion.

Non-Thematic Contributions

The Club de Berne – Out of Control

by Jan Jirát and Lorenz Naegeli

Founded in 1969, the Club de Berne is today considered an official network of the domestic intelligence services of the EU countries plus Norway and Switzerland. New documents show that US agencies are involved, too. In the meantime, this guild of secret intelligence agencies disposes of its own operative platform that comes with a database of personal data. Although the latter may have been granted a legal foundation in national laws, there is still no democratic control.

The IT Security Act 2.0

by Louisa Zech

Once more, the German parliament is to address the protection of IT systems and the data they store. The 2015 reform of the IT Security Act is now to be followed by another. A draft by the Federal Ministry of the Interior from 27 March 2019 is currently undergoing interdepartmental coordination. The plan is characterized by extensive criminalization of activities in early or preparatory stages, as well as a worryingly broad wording of criminal offences.

Mitarbeiter*innen dieser Ausgabe

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

Heiner Busch, Bern, Redakteur von Bürgerrechte & Polizei/CILIP, Vorstandsmitglied des Komitees für Grundrechte und Demokratie

Benjamin Derin, Berlin, Rechtsanwalt, wissenschaftlicher Mitarbeiter am Lehrstuhl für Kriminologie an der Juristischen Fakultät der Ruhr-Universität Bochum, Redakteur von Bürgerrechte & Polizei/CILIP

Otto Diederichs, Berlin, freier Journalist

Nina Galla, Berlin, Referentin Enquete-Kommission „Künstliche Intelligenz" der Linksfraktion im Bundestag

Tom Jennissen, Berlin, Redakteur von Bürgerrechte & Polizei/CILIP, Rechtsanwalt, Mitglied des Republikanischen Anwältinnen- und Anwältevereins (RAV)

Jan Jirát, Zürich, Journalist bei der WOZ - Die Wochenzeitung

Ulrich von Klinggräff, Berlin, Rechtsanwalt, Mitglied im RAV

Jenny Künkel, Bordeaux, wissenschaftliche Mitarbeiterin am Centre National de la Recherche Scientifique (UMR 5319 Passages), Redakteurin von Bürgerrechte & Polizei/CILIP

Christian Meyer, Berlin, Soziologe und freier Journalist, promoviert an der FSU Jena, Redakteur von Bürgerrechte & Polizei/CILIP

Roland Meyer, Berlin, Kunst- und Medienwissenschaftler, Akademischer Mitarbeiter für Kunstgeschichte an der BTU Cottbus-Senftenberg

Matthias Monroy, Berlin, Redakteur von Bürgerrechte & Polizei/CILIP, Wissensarbeiter, Blogger, in Teilzeit bei der Linksfraktion im Bundestag

Lorenz Naegeli, Zürich, freier Journalist, meistens bei der WOZ

Norbert Pütter, Berlin, Redakteur von Bürgerrechte & Polizei/CILIP und Professor für Politikwissenschaft an der BTU Cottbus-Senftenberg

Stephanie Schmidt, Innsbruck, Kulturanthropologin, Universitätsassistentin für Europäische Ethnologie, Redakteurin von Bürgerrechte & Polizei/CILIP

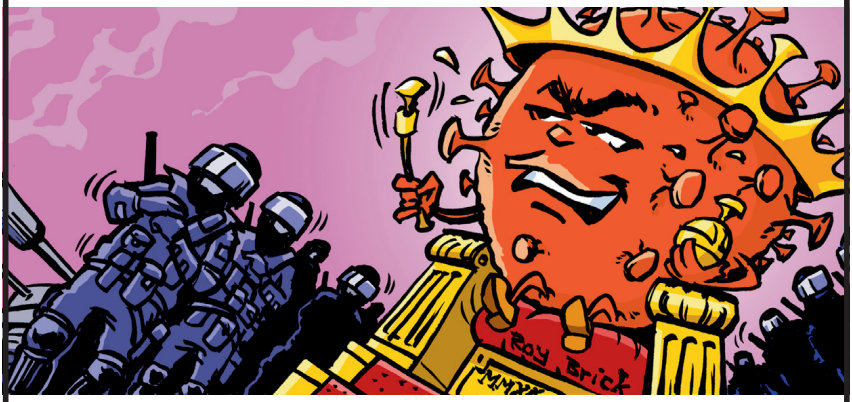
Christian Schröder, Berlin, Politologe, Redakteur von Bürgerrechte &Polizei/CILIP

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

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

Louisa Zech, Berlin, wissenschaftliche Mitarbeiterin am Lehrstuhl für Kriminologie an der Juristischen Fakultät der Ruhr-Universität Bochum, Redakteurin von Bürgerrechte & Polizei/CILIP

graswurzel revolution



GWR 448, April 2020
Probeexemplar kostenlos: www.graswurzel.net