Schriften zur Kriminologie 32

Felix Butz

Polizei und Massendaten

Kriminologisch-rechtswissenschaftliche Perspektiven auf die Rekonfiguration polizeilicher Sozialkontrolle

Nomos

Schriften zur Kriminologie

herausgegeben von

Band 32

Felix Butz

Polizei und Massendaten

Kriminologisch-rechtswissenschaftliche Perspektiven auf die Rekonfiguration polizeilicher Sozialkontrolle

Nomos

Gefördert durch die Deutsche Forschungsgemeinschaft (DFG) - 549206645.

Gefördert durch den Open-Access-Publikationsfonds der Universität Leipzig.

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.d-nb.de abrufbar.

Zugl.: Leipzig, Univ., Diss., 2023

1. Auflage 2024

Publiziert von
Nomos Verlagsgesellschaft mbH & Co. KG
Waldseestraße 3–5 | 76530 Baden-Baden
www.nomos.de

Gesamtherstellung:
Nomos Verlagsgesellschaft mbH & Co. KG
Waldseestraße 3–5 | 76530 Baden-Baden

ISBN (Print): 978-3-7560-1713-3
ISBN (ePDF): 978-3-7489-4443-0

DOI: https://doi.org/10.5771/9783748944430

Onlineversion
Nomos eLibrary

Vorwort

Dissertationen zu schreiben ist voraussetzungsreich, wobei der erfolgreiche Ausgang eines solchen Projekts nicht selten zu einem Großteil mit den externen Bedingungen, dem Umfeld, der schreibenden Person steht und fällt. Insofern durfte und darf ich mich glücklich schätzen, die mir zu teil gewordene freundschaftliche und kollegiale Unterstützung erfahren zu haben.

Mein besonderer und ausdrücklicher Dank gilt hierbei allen voran Katrin Höffler, die mir nicht nur unerschütterliches Vertrauen entgegenbrachte und stets interessiert mit Rat und Tat zur Seite stand, sondern mir auch intellektuell und zeitlich die größtmöglichen Freiräume gewährte. Mit ihrer unkomplizierten, begeisterungsfähigen und überaus freundlichen Art hat sie eine für mich beispiellose Forschungsatmosphäre geschaffen – ohne sie hätte das Projekt in dieser Form nicht stattfinden können. Auch Johannes Eichenhofer möchte ich meinen herzlichen Dank aussprechen: Dafür, dass er sich unvermittelt als Zweitprüfer bereit erklärt und das Gutachten umgehend erstattet hat, sowie für die anregenden und ideengebenden Diskussionen während und nach der Verteidigung.

Stets eine Unterstützung, sowohl fachlich als auch – und wohl fast wichtiger – moralisch sowie emotional, war der Lehrstuhl, zunächst in Göttingen, später in Leipzig. Besonders bedanken möchte ich mich hier bei Hauke Bock, Tim Festerling. Katharina Reisch und Marius Riebel. Auch wenn pandemiebedingt die „analogen" Zusammenkünfte im Wesentlichen auf Tagungen beschränkt waren, haben mich ihr Zuspruch und der freundschaftliche Austausch mit ihnen stets beflügelt. Diese Würdigung gilt auch Lucia Sommerer, die zwar mittlerweile ihren eigenen Lehrstuhl hat, mich aber damals, wie heute durch ihr eigenes wissenschaftliches Wirken motiviert. Zu Dank verpflichtet bin ich zudem Jasper Laakmann und Anne Karzel für ihre zeitaufwendige, wie minutiöse Unterstützung bei der Korrektur.

Wie alle im Wissenschaftsbetrieb wissen, fußt die Forschung auch viel auf wissenschaftlichen Institutionen und den in ihnen wirkenden Personen: So möchte ich mich bedanken bei den Teilnehmenden der Tagungen, Workshops und sonstigen Diskussionsrunden, in denen ich meine Ideen testen durfte, sowie den Mitarbeitenden in den vielen Bibliothek, die mir

als Ort des Austauschs, Denkens und Arbeitens dienten. Daneben bin ich der Deutschen Forschungsgesellschaft sowie dem Open-Access-Fonds der Universitätsbibliothek Leipzig zu Dank verpflichtet für die großzügige Publikationsförderung, die sie mir zuteilwerden ließen und die maßgeblich zur (Open-Access-)Veröffentlichung dieses Werks beigetragen haben.

Zuletzt, so ist es guter Brauch, steht der persönlichste Dank. Haike, Henning und Philipp haben mir mitgegeben, was ich brauche, um diese und andere große Aufgaben zu meistern, haben mich mit Wort und Tat unterstützt und mir mit ihrem steten Glauben daran, dass ich schon wisse, was ich tue, Sicherheit gegeben. Olivia hat wie niemand sonst miterlebt, welche alltäglichen und außerordentlichen Entbehrungen mit einer solchen Arbeit einhergehen. Sie hat mich in und durch Tiefphasen er- und getragen; vor allem zeigt sie mir immer wieder, worauf es wirklich ankommt. Ihnen allen gebührt meine tief empfundene Dankbarkeit.

Berlin, d. 23.1.2024

Inhaltsverzeichnis

Prolegomenon: Spätmoderne Gesellschaft und polizeiliche Sozialkontrolle

> „Technology is neither good nor bad; nor is it neutral [...] technology's interaction with the social ecology is such that technical developments frequently have environmental, social, and human consequences that go far beyond the immediate purposes of the technical devices and practices themselves."[1]
> Melvin Kranzberg, 1986

Die Gesellschaft scheint in schlechter Verfassung. Obwohl diese Beobachtung aus soziologischer Perspektive kein Grund für überbordende Sorge sein sollte,[2] scheint die Intensität der Krisenhaftigkeit der uns umgebenden Sozialstruktur gegenwärtig doch ganz besonders anzuschwellen. Egal welchem System man sich zuzuwenden scheint – ökonomisches, ökologisches, politisches, gesundheitliches et cetera – überall begegnet man Widersprüchen, Konflikten, Krisenmomenten. Ohne Hoffnung auf Lösung etabliert sich der Begriff der Polykrise als bescheidener Versuch der Beschreibung für die unentwirrbaren Verflechtungen gegenwärtiger gesellschaftlicher Herausforderungen.[3] Wir müssen vor diesem Hintergrund lernen, wie es *Reckwitz* schreibt, „die Spätmoderne als eine widersprüchliche, konflikthafte Gesellschaftsformation zu begreifen".[4] Globalisierung und Digitalisierung haben hergebrachte Strukturen gelöst und in Bewegung gesetzt. Kultureller Wertewandel, politische Legitimationsverluste und Steuerungsschwierigkeiten, vielfältige Migrationsbewegungen, neue Kommunikationsformen, Postindustrialisierung der Ökonomien und ökologische Skaleneffekte führen in drängende gesellschaftliche Aushandlungsprozesse hinein, die neue soziale Arrangements hervorbringen. Die faccettenreichen Milieus der Spätmoderne befördern eine multipolare Sozialordnung, geprägt von kulturelle Heterogenität, von Polarisierung und Antagonismen.[5] In dieser

1 *Kranzberg* Technology and Culture 27 (1986), 544 (545).
2 *Nassehi,* Unbehagen.
3 *Tooze*, Defining polycrisis - from crisis pictures to the crisis matrix., https://adamtooze.substack.com/p/chartbook-130-defining-polycrisis (Stand: 01.10.2023).
4 *Reckwitz,* Das Ende der Illusionen, S. 18.
5 *Reckwitz,* Das Ende der Illusionen, S. 298.

Situation erlebt sich die Gesellschaft selbst als unübersichtlich und unsicher.[6] Die zunehmende Singularisierung[7] von Individuen und Kollektiven befördert zudem eine soziale Fragmentierung, welche die Frage nach der Integration oder sogar noch grundsätzlicher: der Integrationsfähigkeit spätmoderner Gesellschaft mit neuer Aktualität auf den Plan ruft.[8]

Menschen unterscheiden sich seit jeher in kulturellem und ethnischem Hintergrund, in religiösen Präferenzen oder wirtschaftlichem Status.[9] Die spätmoderne Auseinandersetzung um das richtige Kulturverständnis und den richtigen Umgang mit ihr befördert jedoch Kulturationstechniken[10], mit denen diese Unterschiede – im positiven wie im negativen Sinne – betont und damit verstärkt werden. Im Zuge dessen kommt es zu einer Pluralisierung der Sozialordnungen – derogativ ist mitunter auch von sogenannten Parallelgesellschaften die Rede – für die es einen geteilten Normenbestand immer weniger zu geben scheint. Nichtsdestotrotz existiert weiterhin eine Mehrheitsgesellschaft, die von ihren Vorstellungen abweichendes Verhalten registriert, markiert und regelmäßig abwertet. Vor dem Hintergrund zunehmender Fragmentierung erscheint die Organisation eines verträglichen Zusammenlebens als eine zentrale Herausforderung des 21. Jahrhundert.[11] Während pluralitätsbedingte Devianzformen häufig nicht aus sich selbst heraus stigmatisierungs- und sanktionswürdig sind, produziert die digitalisierte, globalisierte Gesellschaft der Spätmoderne auch neue Formen inhärent schädlicher Devianz: Terrorismus, Cyberkriminalität und bestimmte – nachgewiesenermaßen bestehende – Formen des organisierten Verbrechens sind Kriminalitätsphänomene, die sich spiegelbildlich zur Gesellschaft durch einen hohen Grad an Vernetztheit, Transnationalität und

6 So nahm in den letzten Jahren das Unsicherheitsempfinden der deutschen Wohnbevölkerung wieder zu, wobei abzuwarten bleibt, ob sich dieser Trend hinsichtlich der kriminalitätsbezogenen Empfindungen fortsetzen wird, siehe dazu *Birkel/Church/Hummelsheim-Doss* ua (Hrsg.), Der Deutsche Viktimisierungssurvey 2017, 46 ff; bezogen auf Straftaten etwas relativierend sind insoweit die Ergebnisse der R+V-Studie "Die Ängste der Deutschen". Auch hier gibt es allerdings Ergebnisse, die sich als relativ ausgeprägte Angst vor anomischen Gesellschaftszuständen interpretieren lassen, siehe *R+V Versicherung AG*, Die Ängste der Deutschen, https://www.ruv.de/newsroom/themenspezial-die-aengste-der-deutschen/langzeitvergleich (Stand: 01.10.2023).

7 *Reckwitz,* Die Gesellschaft der Singularitäten.

8 *Reckwitz,* Das Ende der Illusionen, S. 298.

9 *R. Meier* in Deflem (Hrsg.), The Handbook of Social Control, 23 (27).

10 *Reckwitz,* Das Ende der Illusionen, S. 29.

11 *Sennett,* Together.

Komplexität auszeichnen, was den gesellschaftlichen Umgang mit ihnen stark erschwert.

Die kollektive Suche nach Antworten auf diese neuen Devianzphänomene bedingt dabei einen Wandel der Sozialkontrolle, also derjenigen gesellschaftlichen Institutionen, Akteure und Dynamiken, die auf die Herstellung und den Erhalt der sozialen Ordnung und die Sicherung des Normbestandes gerichtet sind.[12] Eine zunehmend zentrale Rolle bei der Umsetzung des kollektiven Wunsches nach Produktion und Aufrechterhaltung einer robusten Ordnung nehmen – wie es für die technikgläubige Fortschrittsgesellschaft gar nicht anders sein kann – technologische Lösungsansätze ein. Im Sinne des von *Morozov* beschriebenen Solutionismus[13], eine Ideologie, die gesellschaftliche Probleme für vor allem mit technologischen Mitteln lösbar hält, wird die Identifizierung, Kategorisierung, Sanktionierung und Verhinderung von deviantem Verhalten vielerorts zu einer technischen Frage. Gleichzeitig hat sich – befeuert durch viele medial begleitete Skandale – eine teilweise etwas pauschale Technikkritik ausgebreitet, die unter anderem vor dem Risiko einer umfassenden (Sozial-)Kontrolle im Wege der Nutzung datenbasierter Informationstechnologie, wie sie im Zuge der Digitalisierung entwickelt wurde und wird, durch staatliche oder auch ökonomische Akteure warnt.[14]

Allerdings zeigen die jüngeren Entwicklungen etwa in China, dass eine merkliche Intensivierung von informationstechnologisch fundierten Überwachungs- und Kontrollpraktiken durch den Staat kein reines Gedankenspiel mehr ist. Zwar driftet der westliche Diskurs hierzu mitunter in etwas überzogene Darstellungen des chinesischen Kontrollapparats ab. Dass aber der technische Überwachungs- und Kontrollapparat, von dem das viel besprochene Sozialkreditsystem[15] ebenso nur eine Komponente ist wie die Unterdrückungsmaschinerie gegenüber der Uighurischen Bevölkerung in Xinjiang,[16] Ausdruck einer qualitativ neuen Sozialkontrolle ist, wird sich schwerlich bestreiten lassen. Dabei ist der Wandel hin zu einer datengetriebenen Regierungsführung mitnichten ein Phänomen alleine in autoritären Staaten, das man in wissenschaftlichen und gesellschaftlichen Diskursen im „Westen" distanziert und gefällig rezipieren könnte. Vielmehr zeigen

12 Näher dazu unten S. 84 ff.
13 *Morozov,* To save everything, click here.
14 *Reckwitz,* Das Ende der Illusionen, S. 14.
15 *Creemers* SSRN Journal 2018; *Dai* SSRN Journal 2018; *C. Lee* OIR 43 (2019), 952.
16 *Beydoun* Washington and Lee Law Review (Wash. & Lee L. Rev) 79 (2022), 769.

sich unter anderem in den technologie-affinen Vereinigten Staaten, Wiege und nach wie vor wichtiges Zentrum des modernen Liberalismus, starke Tendenzen zur Nutzung von Informationstechnologien zur Sozialkontrolle,[17] die sich aber aufgrund der unterschiedlichen Sozialstrukturen und politische Kulturen der beiden Gesellschaften unterschiedlich materialisieren. Gleichzeitig verdeutlichen diese Entwicklungen und die um sie herum geführten Debatten die fundamentale Bedeutung von sozialer Kontrolle für die gesellschaftlichen Entfaltungsbedingungen von Individuen wie auch Kollektiven im 21. Jahrhundert.

Vor diesem Hintergrund – und das ist das dieser Studie zugrundeliegende Erkenntnisinteresse – muss auch für den hiesigen Kontext ergründet werden, welche Auswirkungen das Zusammentreffen von informationstechnologischen Innovationen der Digitalisierung mit den Bedürfnissen der spätmodernen Gesellschaft Deutschlands nach (staatlicher) Sozialkontrolle mit sich bringt. Insofern geraten unweigerlich die deutschen Polizeibehörden in den Blick. Als staatliche Organisation mit breitem Maßnahmenspektrum und Inhaberin des Gewaltmonopols ist die Polizei eine der mächtigsten Institutionen der Gesellschaft. Daneben ist sie die zentrale Akteurin im Feld der formellen Sozialkontrolle. Sie registriert – sowohl eigeninitiativ als auch durch Hinweise aus der Bevölkerung – abweichendes Verhalten und macht es damit häufig überhaupt erst prozessierbar. Zudem ist die Polizei aufgrund ihres organisationalen Charakters – wie auch wirtschaftliche Unternehmen und sonstige staatliche Behörden – massiv von der Digitalisierung betroffen und muss sich anpassen. Gleichzeitig ist sie aufgrund ihrer Rolle und Position aufgerufen, die beschriebenen Um- und Unordnungsphänomene der Spätmoderne überwachend und kontrollierend zu adressieren. In der Polizei als Institution treffen mithin die beschriebenen Dynamiken in einer Weise zusammen, die sie zu Kristallisationspunkt für die Rekonfigurationsprozesse rund um den spätmodernen und informationstechnologisch fundierten Umgang mit Devianz bzw. Kriminalität machen.[18]

Um diese Prozesse näher zu beleuchten, nimmt die vorliegende Studie die Polizei als Organisation in ihrer Reaktion auf das Massendatenphänomen in den Blick, um daraus Schlüsse, bezogen auf den Wandel polizeilicher und damit auch – zumindest in Teilen – gesellschaftlicher Sozial-

17 Im Kontext der Polizei siehe etwa *Ferguson,* The rise of big data policing; im Kontext des strafjustiziellen Systems siehe etwa *Lageson,* Digital Punishment.

18 Ähnlich *Egbert/Leese,* Criminal futures.

kontrolle, ziehen zu können. Dabei wird das Massendatenphänomen als technologischer oder technologie-induzierter Anknüpfungspunkt genommen, da Massendaten – aus hier vertretener Perspektive – das basale Element und epistemische Fundament der gegenwärtigen Digital- oder Informationsgesellschaft sind. Denn es werden immer mehr technische Erkenntnisverfahren auf Grundlage dieses wissenschaftlich (*Nassehi* spricht insoweit auch von *szientoid*, also wissenschaftsähnlich[19]) und technologisch bedingten Wandels des menschlichen Mediensystems geschaffen, was einen tiefgehenden Einfluss auf unser Verhältnis zur Welt und gesellschaftliche Machtverteilung sowie -ausübung hat. So heißt es etwa bei *Jasanoff* im Kontext der Produktion sozialer Ordnung:

> „What we know about the world is intimately linked to our sense of what can we can do about it, as well as to the felt legitimacy of specific actors, instruments and courses of action. Whether power is conceived in classical terms, as the power of the hegemon to govern the subject, or in the terms most eloquently proposed by Michel Foucault, as a disciplining force dispersed throughout society and implemented by many kinds of institutions, science and technology are indispensable to the expression and exercise of power"[20]

Es ist nichts Neues, dass Wissen ein zentraler Faktor für Macht ist. Allerdings verändert die Verarbeitung von Massendaten den Modus der Wissensproduktion und ermöglicht so bisher nicht dagewesene informationelle Aufschlüsselungen von Personen, Strukturen und Ereignissen. Die dadurch möglichen Machtakkumulationen sind per se eine Gefahr für rechtsstaatlich und demokratisch verfasste Gesellschaften, weshalb die wissenschaftliche Erforschung dieser Dynamiken in gesellschaftlich mächtigen Institutionen wie der Polizei dringend geboten erscheint.

Das gilt umso mehr, als dass der gegenwärtige Kenntnisstand zu polizeilicher Daten- bzw. Informationsverarbeitung eher überschaubar ist. Einerseits hat dies seinen Grund in der Dynamik des Forschungsgegenstandes: Die technischen Kapazitäten zur Verarbeitung von Daten zu Überwachungs- und Kontrollzwecken durchlaufen gegenwärtig – und ohne dass ein Ende absehbar wäre – schnelle Innovationszyklen, mit denen eine wissenschaftliche Auseinandersetzung nur begrenzt mithalten kann. In der Folge verbleibt die Forschung zur massendatengestützten Polizeiarbeit

19 *Nassehi,* Muster, S. 68 et passim.
20 *Jasanoff* in Jasanoff (Hrsg.), States of knowledge, 13 (14).

mitunter im Spekulativen.[21] Hinzu kommt, dass die Polizei als sicherheitsbehördliche Institution nur ungern ihre Prozesse offenlegt. Zudem war das wissenschaftliche Interesse an der sich an die Datenerhebung anschließenden Datenverarbeitungsprozesse im polizeilichen Informationswesen bisher nicht in einer der hier dargelegten Bedeutung dieser Aspekte angemessenen Weise vorhanden. In der Folge ist nur wenig – vor allem empirisch – darüber bekannt, wie die Polizei (Massen-)Daten nutzt und welche Auswirkungen das auf sie als Organisation, ihr Verhältnis zur Gesellschaft und die Konfiguration polizeilicher Sozialkontrolle hat.

Trotz dieser Erkenntnisdefizite ist das Forschungsfeld zur polizeilichen Datenverarbeitung im Kontext des Massendatenphänomens keine weiße Landkarte. Im englischsprachigen Diskurs findet sich sprachbedingt der Großteil der bisherigen Arbeiten. Neben grundlegenden Arbeiten zum Verhältnis von Polizei und Informationstechnologie[22] ist dabei vor allem die Rolle von Algorithmen mitsamt ihrer Probleme für die polizeiliche Datenverarbeitung, insbesondere in Form des sogenannten Predictive Policing[23], Gegenstand etlicher Untersuchungen gewesen.[24] Zudem ist auch die Massendatenverarbeitung als ein die Polizei umfassender Wandlungsprozess wissenschaftlich bearbeitet worden.[25] Besonders hervorzuheben ist *Fergusons* „Rise of Big Data Policing", das als erste Arbeit eine Globalperspektive auf das Phänomen bei der US-amerikanischen Polizei entwirft und dabei auch den relevanten Aspekt der Diskriminierung explizit beleuchtet.[26] Ebenfalls wegweisend ist *Braynes* Studie „Predict and Surveil", in der die Soziologin – ebenfalls für die US-amerikanische Polizei – vor

21 *Brayne,* Predict and surveil, S. 4.

22 *Chan* Criminal Justice 1 (2001), 139; *Chan/Brereton/Legosz* ua, E-policing: The Impact of Information Technology on Police Practices; *Manning* Crime and Justice 15 (1992), 349; *Manning,* The technology of policing.

23 Näher dazu unten S. 279 ff.

24 Ohne Anspruch auf Vollständigkeit: *Amoore/Raley* Security Dialogue 48 (2017), 3; *D. Wilson* in Završnik (Hrsg.), Big data, crime and social control, 108; *Babuta/Oswald* in McDaniel/Pease (Hrsg.), Predictive policing and artificial intelligence, 214; *Završnik* European Journal of Criminology 18 (2021), 623; *Grace* in McDaniel/Pease (Hrsg.), Predictive policing and artificial intelligence, 237; *Selbst* Georgia Law Review 52 (2018), 109; *Bennett Moses/Chan* Policing and Society 28 (2018), 806.

25 Ebenfalls ohne Anspruch auf Vollständigkeit: *Row/Muir* in McDaniel/Pease (Hrsg.), Predictive policing and artificial intelligence, 254; *Brayne* Am Sociol Rev 82 (2017), 977; *Joh* Harvard Law & Policy Review Vol. 10 (2016), 15; *Ridgeway* Annu. Rev. Criminol. 1 (2018), 401; *Laude/Reinhardt/Bomert* in Wehe/Siller (Hrsg.), Handbuch Polizeimanagement, 1; *Sanders/Sheptycki* Crime Law Soc Change 68 (2017), 1.

26 *Ferguson,* The rise of big data policing.

allem durch ethnografische Feldforschung eine neue Annäherungsebene an polizeiliche Massendatenverarbeitung eröffnet, indem sie es schafft die Implementierungen der neuen Informationspraktiken in den polizeilichen Arbeitsalltag näher darzustellen und auf ihre gesellschaftlichen Implikationen hin zu untersuchen.[27] Auch wenn sich hieraus generelle Dynamiken, Prozesse und Entwicklungstrends für den deutschsprachigen Forschungsraum und den Forschungsgegenstand der deutschen Polizei(en) destillieren lassen, lassen sich viele Ergebnisse aus Untersuchungen zu US-amerikanischen oder anderen Polizeiorganisationen nur begrenzt übertragen. Insoweit instruktiv ist allen voran die Studie „Criminal Futures" von *Egbert und Leese*, die zwar ebenfalls englischsprachig ist, aber deutsche und schweizerische Polizeibehörden zum Forschungsgegenstand hat.[28] Inhaltlich untersuchen die Autoren zwar das abgegrenzte Feld des raumbezogenen Predictive Policing[29] mit den qualitativen Mitteln des Interviews, der ethnografische Feldforschung und der Dokumentenanalyse. Dabei ermöglicht ihre Arbeit aber einen Blick in die vielfältigen Wandlungsprozesse, die eine algorithmisierte oder auch datafizierte[30] Polizeiarbeit für die Polizei selbst, ihre Beamt:innen und das gesellschaftliche Wissen über Kriminalität bedeutet. Ihrer Bedeutung als erste umfassende empirische Untersuchung zu polizeiliche Massendatenverarbeitung (unter anderem) in Deutschland entsprechend wurde sie in der vorliegenden Studie umfassend rezipiert. Ansonsten erfolgte die Auseinandersetzung der deutschsprachigen Forschung mit polizeilicher Informationsverarbeitung eher punktuell. Ein wachsendes Feld ist die rechtswissenschaftliche Befassung mit dem polizeilichen Informationswesen und der in ihm stattfindenden Datenverarbeitungen. So hat etwa *Bäcker* sich kritisch mit den Strukturen der Informationsarchitektur,[31] aber auch den Verarbeitungsverfahren der Polizei[32] auseinandergesetzt. Auch *Golla* hat bereits einige wichtige rechtsdogmatische Beiträge zur Polizei im Kontext des Massendatenphänomens geleistet.[33] Hervorzuheben ist zudem *Arzt*, dessen bereits langjährige kritische Begleitung der polizeilichen Informationsverarbeitung zuletzt in einer ebenfalls instrukti-

27 *Brayne,* Predict and surveil.
28 *Egbert/Leese,* Criminal futures.
29 Siehe dazu näher unten S. 279 ff.
30 Zum Begriff siehe unten S. 46 ff.
31 *Bäcker,* Kriminalpräventionsrecht, S. 474 ff.
32 *Bäcker* in Hoffmann-Riem (Hrsg.), Big Data - Regulative Herausforderungen, 167.
33 *Golla* Neue Juristische Wochenschrift 74 (2021), 667; *Golla* Kriminologisches Journal 52 (2020), 149.

ven Darstellung ihrer Rechtswirklichkeit auf Grundlage der dazu öffentlich verfügbaren Informationen gemündet ist.[34] Relevant sind außerdem die Arbeiten von *Aden und Fährmann* mit der Transparenz der polizeilichen Informationsverarbeitung und ihrer besseren Regulierung.[35] Aus rechtswissenschaftlicher Richtung relevant sind zudem Auseinandersetzungen mit den neueren Verfahren der polizeilichen Informationsverarbeitung wie etwa dem Predictive Policing, das vor allem von *Sommerer* mit einer fundierten Untersuchung bearbeitet wurde.[36] Schließlich sind noch die Arbeiten von *Singelnstein* zu nennen, der sich neben der Beschäftigung mit neuen Technologien der Kriminalitätskontrolle[37] vor allem auch mit den zugrundeliegenden gesellschaftsstrukturellen Entwicklungen aus kriminologischer Sicht kritisch auseinandergesetzt hat.[38]

Aufbauend auf diesen Vorarbeiten und mit dem Bewusstsein für den Wert einer möglichst umfassenden Perspektive auf das polizeiliche Informationswesen im Zeitalter der Massendaten will die vorliegende Studie dieses Informationswesen und die in ihm stattfindende polizeiliche Informationsverarbeitung in ihren jeweiligen Teilaspekten untersuchen, um ein möglichst faccettenreiches Bild zu zeichnen, das trotzdem natürlich keinesfalls vollständig sein wird. In Ergänzung zur Studie von *Egbert und Leese*, die sich aber vor allem auf ein informationstechnisches Verfahren konzentrieren, soll damit der Versuch einer Globalperspektive auf die polizeiliche Informationsverarbeitung in Deutschland unternommen werden. Dabei soll zudem das Verhältnis dieses Themenkomplexes – informationstechnologisch fundierte (Massen-)Datenverarbeitung durch die Polizeien – zum Phänomen der Sozialkontrolle in den Blick genommen werden. Beides ist in diesem Zuschnitt noch nicht beforscht worden. Dabei ist – wie eben erwähnt – eine vollständige Abbildung des polizeilichen Informationswesens und der polizeilichen Informationspraktiken aufgrund der Massivität dieser Forschungsgegenstände nicht möglich. Insofern geht es auch darum,

---

34 *Arzt* in *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch des Polizeirechts, G. Rn. 1108 ff.

35 *Aden/Fährmann* vorgänge. Zeitschrift für Bürgerrechte und Gesellschaftspolitik 227 (2019), 95; *Aden/Fährmann* Zeitschrift für Rechtspolitik 2019, 175; *Aden/Fährmann* Zeitschrift für Technikfolgenabschätzung in Theorie und Praxis 29 (2020), 24.

36 *Sommerer,* Personenbezogenes Predictive Policing.

37 *Singelnstein* in Stein/Greco/Jäger ua (Hrsg.), Systematik in Strafrechtswissenschaft und Gesetzgebung, 725; *Hoffmann-Riem* (Hrsg.), Big Data - Regulative Herausforderungen.

38 *Singelnstein/Stolle,* Sicherheitsgesellschaft; zuletzt *Singelnstein* in T. Fischer/Hilgendorf (Hrsg.), Gefahr, 95.

bisherige blinde Flecken im wissenschaftlichen Zugriff auf die Polizei unter dem Eindruck des Massendatenphänomens aufzuzeigen.

Der Zugriff der folgenden Arbeit ist im Wesentlichen zweigeteilt: Zum einen wird eine rechtswissenschaftliche Perspektive eingenommen, mit der das Recht des polizeilichen Informationswesens und der polizeilichen Informationspraktiken einer kritischen Bestandsaufnahme unterzogen werden soll. Dabei steht nicht die Entwicklung neuer dogmatischer Konzepte für die polizeiliche Informationsordnung im Mittelpunkt. Vielmehr will die Studie im Wege ihrer rechtsdogmatischen Ausführungen rechtliche Defizite und damit rechtswissenschaftlichen Forschungs- sowie gesetzgeberischen Handlungsbedarfe aufzeigen. Zum anderen soll das empirische Wissensdefizit mit der vorliegenden Untersuchung adressiert werden. Dazu wurde eine Interviewstudie mit polizeilichen Datenschutzbeauftragten als zentrale Personen im Kontext polizeilicher Datenverarbeitung durchgeführt, anhand derer eine Rekonstruktion der Prozesse und Dynamiken des polizeilichen Informationswesens unternommen wird. Ergänzt und fundiert werden diese beiden Teile durch theoretische Überlegungen zu den Grundkategorien, Konzepten und Phänomenen des Forschungsfeldes sowie durch eine historische Betrachtung polizeilicher Informationsverarbeitung in Deutschland, die den gegenwärtigen Zustand und seine ein stückweit kontingenten Entwicklungstendenzen in den Kontext einer historisch gewachsenen Gesellschaft stellt. Auf Grundlage dieser vier Säulen soll eine Perspektive auf den makrostrukturellen und strategischen Umgang der Gesellschaft mit dem polizeilichen Informationswesen in Gegenwart und Zukunft eröffnet werden. Daraus ergibt sich die folgende Gliederung der Arbeit:

Kapitel I. legt die theoretische Basis für die Studie. Es werden informations- und datentheoretische Begriffe und Konzepte vorgestellt, die der weiteren Verwendung dieser im Verlauf der Arbeit (etwa: Daten, Information, Massendaten, et cetera) zugrunde liegen. Zudem wird die Bedeutung des Wandels menschlicher Mediennutzung für den gegenwärtigen Moment umrissen. Auch der Technologie-Begriff wird im Lichte des Forschungsgegenstandes näher beleuchtet. In diesem Zusammenhang erfolgt zudem eine Auseinandersetzung mit den speziellen Informationstechnologien der Datenbank, des Algorithmus und des Informationssystems sowie mit ihren Implikationen für die polizeiliche Datenverarbeitung. Theoretische Überlegungen zu Begriff, Wirkweisen und Wandlungspotenzialen der Sozialkontrolle schließen Kapitel I. ab.

Kapitel II. wendet den Blick zunächst in die Vergangenheit und zeichnet die Entwicklung von polizeilichem Informationswesen und polizeilicher Informationsverarbeitung in der Geschichte Deutschlands nach. Beginnend mit der Institutionalisierung der modernen Polizei werden informationstechnologische Innovationen in ihren Wirkungen auf die Polizei als Organisation und ihr Verhältnis zu Gesellschaft und Kriminalität untersucht. Neben technischen Neuerungen spielen dabei auch organisationale Anpassungsprozesse eine entscheidende Rolle. Ein Fokus liegt zudem darauf, Kontinuitäten und Brüche in den polizeilichen Arbeits- und Denkweisen freizulegen. Die historische Rückschau endet mit einigen kursorischen Ausführungen zur gegenwärtigen informationstechnologischen Entwicklungsstufe, der Datafizierung, deren wissenschaftliche Erkundung Ziel des weiteren Verlaufs der Studie ist.

Dazu wird in Kapitel III. zunächst die rechtswissenschaftliche Perspektive auf die informationstechnologische Infrastruktur und die Informationspraktiken der Polizei eingenommen. Neben den verfassungsrechtlichen Rahmenbedingungen und Entwicklungen rund um das polizeiliche Informationswesen wird der durch die europäische Datenschutzreform mittlerweile ebenfalls wichtige unionsrechtliche Rechtsrahmen dargestellt und kommentiert. Im Anschluss werden die für die Rechtsanwendungsebene, auf der Polizeibeamt:innen bei ihrer Datenverarbeitung operieren, relevanten Vorgaben abgebildet. Dabei folgen die Ausführungen der Teilung, die hier bereits sprachlich einige Male angeklungen ist: Zunächst werden die normativen Rahmenbedingungen der informationstechnologischen Infrastruktur des polizeilichen Informationswesens, also seiner Dateien und Informationssysteme, aufgeführt und einer kritischen Überprüfung unterzogen. Sodann erfolgt dasselbe für die Vorschriften bezüglich der polizeilichen Datenverarbeitung, also solcher Informationspraktiken, die sich an die Datenerhebungsmaßnahmen anschließen. Die rechtswissenschaftliche Auseinandersetzung mit dem Forschungsthema endet mit einer Darstellung des hier sogenannten internen Datenschutzkontrollregimes, zu dem (unter anderem) die für den empirischen Zugang zum Informationswesen so wichtigen behördlichen Datenschutzbeauftragten bei den Polizeien gehören.

Kapitel IV. präsentiert eine Rekonstruktion des polizeilichen Informationswesens und des in ihm stattfindenden Informationshandelns auf Grundlage der mittels Expert:inneninterviews ergründeten Deutungen der polizeilichen Datenschutzbeauftragten. Neben Darstellung der Methodik ist das Kapitel darauf bedacht, die verschiedenen Aspekte der polizeilichen

Informationsverarbeitung, wie sie in den Gesprächsdaten freigelegt wurden, in einer möglichst kohärenten und konsistenten Weise für ein möglichst stimmiges Bild des Informationswesens zusammenzustellen.

Kapitel V. richtet den Blick wiederum auf mögliche Zukünfte der deutschen Polizei, wie sie sich vor dem Hintergrund ihrer informationstechnologisch in Gang gesetzten Entwicklungstendenzen abzeichnen. Dafür wird mit dem Konzept der sozio-technischen Imaginationen gearbeitet, um Szenarien unerwünschter Zukünfte mit einer erstrebenswerten Zukunft polizeilicher Datenverarbeitung im 21. Jahrhundert zu kontrastieren, für deren Erreichung Steuerung- und Regulierungspfade sowie -instrumente aufzeigt werden. Das Kapitel ist gleichsam als Synthese zu lesen, in der die Erkenntnisse und Ergebnisse der Untersuchung miteinander in Beziehung gesetzt werden. Die Methode des Szenariendesigns wurde dabei gewählt, um die komplexen und variierenden Wechselwirkungen der hier untersuchten Einflussfaktoren auf die polizeiliche Sozialkontrolle anschaulich zu machen.

Zum Abschluss dieser einleitenden Worte, noch einige Anmerkungen zur generellen Terminologie. Schon aufgefallen sein dürfte der Begriff des polizeilichen Informationswesen. Er wird verwendet, um die größte Einheit dessen zu beschreiben, was durch die informationstechnologische Infrastruktur der Polizei sowie die in ihr und um sie herum stattfindenden Informationshandlungen der Polizeibeamt:innen ausgemacht wird. Informationstechnologische Infrastruktur meint dabei all die technischen Geräte, Apparaturen und Systeme, die materiell die polizeiliche Datenverarbeitung ermöglichen. Informationshandlungen oder -praktiken sind die menschlichen Interaktionsweisen mit dieser Infrastruktur. Zudem wurde bereits in der Einleitung sowohl mit dem Begriff der Informationsverarbeitung als auch mit dem der Datenverarbeitung gearbeitet. Dabei ist Datenverarbeitung die akkurate Bezeichnung aus rechtlicher Sicht – es ist der Begriff, mit dem die datenschutzrechtliche Regulierung operiert. Allerdings erfasst der Begriff der Daten nur unzureichend die im Rahmen der Studie beschriebenen Phänomene.[39] Darüber hinaus ist die terminologische Abgrenzung auch im Recht keineswegs strikt. So wird mit Blick auf den hohen Stellenwert der informationellen Praktiken der Polizeien etwa auch von polizeilichem „Informationsrecht“[40] gesprochen, was eine gewisse Austauschbarkeit der Bezeichnungen impliziert. Vor diesem Hintergrund werden die Begriffe der Daten- oder Informationsverarbeitung in der vorliegenden Arbeit als

39 Siehe zum Datenbegriff unten S. 29 ff.

40 *Pitschas* Zeitschrift für Rechtspolitik 26 (1993), 174.

austauschbar angesehen, sodass mit der Nutzung des einen oder anderen Begriffes keine spezifische Bedeutung verbunden ist.

Kapitel I. Theoretische Basis

Eine Arbeit über den Wandel des polizeilichen Informationswesens unter dem Eindruck des Massendatenphänomens und der davon ausgehenden Wirkung auf die polizeiliche Sozialkontrolle kann nicht umhin, einige theoretische Grundüberlegungen zu umreißen. Zentral ist zunächst der Begriff der Information und damit zusammenhängende Konzepte, insbesondere auch das der (Massen-)Daten. Trotz der im Titel der vorliegenden Arbeit auftauchenden (Massen-)Daten scheint es dabei sinnvoll, den Begriff der Information hier als ersten Anknüpfungspunkt zu wählen (A.). Wie im weiteren Verlauf der folgenden Ausführungen näher ausgeführt werden wird, ist ein solcher Zugang sinnvoll, da das intuitive Begriffsverständnis der Information regelmäßig eine menschliche Involvierung, etwa in Form der Zuschreibung oder Ableitung von Bedeutung, der Interpretation und so weiter nahelegt und daher das „menschlichere" Phänomen ist. Daten hingegen sind nach ihrem allgemeinen Wortgebrauch häufig zu unstrukturiert für die Kognition der Menschen, sodass auf ihrer Grundlage kein direkter Zugang zur Welt hergestellt werden kann. Diese Unterscheidung ist relevant, da es gegenwärtig zu Verschiebungen in der Art und Weise kommt, wie Gesellschaften informationell mit ihrer Umwelt umgehen. Phänomene – natürliche wie soziale – werden zunehmend verdatet und sind in dieser Form für die menschliche Wahrnehmung ohne technologische Apparaturen mitunter unlesbar und unverständlich. Auch diese evolutive Dynamik der medialen Sphäre und ihre Bedeutung für die Gesellschaft sind für ein besseres Verständnis der Wandlungsprozesse im polizeilichen Informationswesen in den Blick zu nehmen (B.). Mit Blick auf die Bedeutung des Datenbegriffs für die gegenwärtige Konfiguration der medialen Sphäre der Gesellschaft müssen die informationstheoretischen Grundlagen, die bereits auch Bezüge zu Daten herstellen, um tiefergehende datentheoretische Überlegungen ergänzt werden (C.). Zusätzlich ist die essenzielle Rolle der (Informations-)Technologie für diese Entwicklung und damit auch für den Wandel des polizeilichen Informationswesens zu beleuchten (D.). Abschließend soll auf Grundlage der bis dahin versammelten Gedanken theoriegeleitet grundsätzliche Überlegungen dazu angestellt werden, wie sich diese Prozesse auf die gesellschaftliche und spezieller auch: polizeiliche Ausübung von Sozialkontrolle auswirken könnten (E.).

A. Informationstheoretische Grundlagen: Daten – Information – Wissen – (Weisheit?)

Die Bewusstwerdung der modernen Gesellschaften, dass Information eine ihrer basalen Größen ist, liegt bald ein halbes Jahrhundert in der Vergangenheit[41] und doch sind wir, wie *Floridi* treffend feststellt, dem Wesen von Information nur eingeschränkt näher gekommen – ein paradoxer Befund im Angesicht der allgegenwärtigen Präsenz des Phänomens: „Of our mundane and technical concepts information is currently one of the most important, most widely used and least understood."[42] Ihre existenzielle Bedeutung hat sich in einer Vielzahl verschiedener Perspektiven auf Information niedergeschlagen, die von informationsphilosophischen Diskursen verklammert werden. In diesen werden konzeptuelle Fragen, Grundprinzipien und Dynamiken von Information erkundet,[43] ohne dass sich bis jetzt ein Konsens hinsichtlich des Begriffs der Information und seiner Bedeutung herausbilden konnte.[44] Trotz dieser Fragmentierung haben sich Inseln wirkmächtiger Modelle und Konzepte bilden können, wozu etwa die einflussreiche DIKW-Pyramide (nach oben, zur Spitze hin, aufsteigend: data, information, knowledge, wisdom) gehört.[45] Auch wenn das Modell mit seiner logisch-hierarchischen Form und der damit verbundenen Annahme geradliniger Transformationsprozesse von einer Stufe zur Nächsten wohl zu Recht kritisiert wurde,[46] ist die Idee von Verbindungslinien zwischen den Größen und sequenziellen Stufenverhältnissen zwischen ihnen ein

41 *Webster,* Theories of the information society, S. 2.

42 *Floridi* Minds and Machines 13 (2003), 459 (459).

43 *Floridi* Metaphilosophy 35 (2004), 554 (555).

44 *Rowley* Journal of Information Science 33 (2007), 163 (165).

45 Die DIKW-Pyramide wird in der informationswissenschaftlichen Literatur vor allem *Ackoff* , Journal of Applied Systems Analysis 16 (1989), 3 zugeschrieben. Sie enthielt in der von *Ackoff* formulierten Form noch die Stufe „understanding". Allerdings hat sich diese Stufe eher in die Transformationsschritte zwischen den einzelnen Phänomenen verschoben, wie es etwa bei *Bellinger/Castro/Mills*, Data, Information, Knowledge, and Wisdom, http://www.systems-thinking.org/dikw/dikw.htm (Stand: 01.10.2023) zum Ausdruck kommt. Bereits früher hat zudem die Sensibilität der Kunst für gesellschaftliche Verschiebungen bereits die Grundessenz des „Modells" eingefangen und festgehalten, denn tatsächlich stammt eine frühere Formulierung aus einem Gedicht von T.S. Eliot, in dem es heißt: „Where is the wisdom that we have lost in knowledge? / Where is the knowledge that we have lost in information?", *Eliot,* The rock.

46 *Frické* Journal of Information Science 35 (2009), 131; *Zins* J. Am. Soc. Inf. Sci. 58 (2007), 479; *Weinberger*, The Problem with the Data-Information-Knowledge-

sinnvoller Ausgangspunkt für eine weitere Analyse dieser Basiskonzepte gegenwärtiger Informationsgesellschaften. Die folgende theoretische Aufschlüsselung orientiert sich insofern im Wesentlichen an den Kategorien Daten, Information und Wissen. Auch das Konzept der Weisheit wird, soweit das aufgrund seiner begrifflichen Flüchtigkeit möglich ist, kurz mit Bezügen zum Untersuchungsgegenstand umrissen. Ziel der Ausführungen ist dabei keine präzise Begriffsformung, sondern die Beleuchtung der für die vorliegende Arbeit relevanten Aspekte der jeweiligen Phänomene.

I. Daten

Der nur begrenzt bestehende konzeptionelle Konsens in den Informationswissenschaften erstreckt sich auch auf das Phänomen der Daten, sodass bereits dieser basale Baustein der Informationsgesellschaft durch begriffliche Heterogenität gekennzeichnet ist.[47]

Ein recht verbreitetes Verständnis konzeptualisiert Daten als Signale, die aus der Umwelt über die Sinne bzw. deren technische Erweiterungen oder Ergänzungen aufgenommen werden können.[48] Daten sind insofern menschlich oder auch: empirisch wahrnehmbare Reize.[49] Dabei schwingt ein differenzialistisches Verständnis mit, das heißt, erst durch einen Unterschied wird ein Reiz wahrnehmbar[50]: Schaut man in den blauen Himmel, so nimmt man visuell nur einen Blauton wahr. Erst eine Differenz in diesem visuellen Kontext, eine Wolke oder ein Vogel, setzt einen neuen wahrnehmbaren Reiz. *Burkhardt* spricht in Bezugnahme auf *Floridi* von „Daten als Information *als* Realität“[51]. Gemeint ist, dass Daten in diesem Verständnis noch keine Informationen *über* Realität sind; sie sind eine Vorstufe zu Information. Der Himmel *ist* nur blau und kann als solcher wahrgenommen werden. Erst aber, wenn mit einer medialen Apparatur daran angeschlossen wird, entsteht Information über subjektiv empfundene Realität, etwa indem jemand Sprache nutzt und sagt: „Der Himmel ist blau“.

Wisdom Hierarchy, https://hbr.org/2010/02/data-is-to-info-as-info-is-not (Stand: 01.10.2023).

47 Siehe dazu nur die verschiedenen Ansätze bei *Zins* J. Am. Soc. Inf. Sci. 58 (2007), 479.

48 *Rowley* Journal of Information Science 33 (2007), 163 (171).

49 *Zins* J. Am. Soc. Inf. Sci. 58 (2007), 479 (487).

50 *Floridi*, Semantic Conceptions of Information, https://stanford.library.sydney.edu.au/archives/sum2010/entries/information-semantic/ (Stand: 01.10.2023).

51 *Burkhardt,* Digitale Datenbanken, S. 195.

Werden solche Reize festgehalten, indem man sie mittels Messung sichtbar macht, so lässt sich ein weiteres Verständnis von Daten ausmachen: Daten sind Bezugnahmen auf die Realität in faktischer Form.[52] Je mehr sich technisch messen lässt, desto mehr kann in solchen Daten, die faktische Feststellungen über die Wirklichkeit ermöglichen, festgehalten werden. Gerade diese zunehmende Möglichkeit ist die technisch-epistemologische Grundlage für das Massendatenphänomen, das letztlich auf dem Fundament einer stetigen Verfeinerung von Messapparaturen aufbaut. Diese formale Komponente der Daten betrifft indessen nicht nur die Erhebung, das Sammeln von Daten, sondern auch die Verarbeitungsmöglichkeiten von Informationen. Daten können daher auch als Repräsentation von Informationen aufgefasst werden. In diesem Verständnis sind Daten keine Vorstufe von Information mehr, sondern bilden letztere digital ab. Zweck dieser begrifflichen Teilung zwischen Daten und Information ist, wie *Burkhardt* es formuliert, „die Differenzierung unterschiedlicher Agenturen der Informationsverarbeitung: Während Menschen in der Lage sind, mit Informationen umzugehen, vermögen Computer lediglich, Daten zu verarbeiten."[53] Daran knüpft sich auch eine weitere Konzeption von Daten als Inbegriff der „binär codierten, maschinenlesbaren Inskriptionen [an, welche] […] damit als Sammelbegriff für all das, was auf digitalen Datenträgern gespeichert vorliegt[, dient.]"[54] Hieran anschließend lassen sich Daten noch im Kontext des Computers charakterisieren. Dabei wurden Daten in der Entstehungsgeschichte von Computern häufig als sekundär gegenüber Programmen und Software angesehen: „Daten sind eher mit den Objekten vergleichbar, die durch ein Werkzeug verändert werden, als mit dem Werkzeug selbst."[55] Insofern erscheinen Daten dann vorrangig als Inhalt computertechnischer Operationen.[56] Allerdings dürfte diese Zweitrangigkeit von Daten im computertechnischen Kontext abgenommen haben. Zwar sind Daten nach wie vor nicht das Werkzeug, sondern werden von informationstechnologischen Werkzeugen genutzt. Jedoch sind letztere in fundamentaler Weise von einer adäquaten Datenbasis abhängig, was sich nicht zuletzt im daten- und informationswissenschaftlichen Sinnspruch „garbage in, garbage out" manifestiert.

52 Siehe zu diesem Verständnis auch *Burkhardt,* Digitale Datenbanken, S. 197 f.
53 *Burkhardt,* Digitale Datenbanken, S. 196.
54 *Burkhardt,* Digitale Datenbanken, S. 200.
55 *Burkhardt,* Digitale Datenbanken, S. 90.
56 *Burkhardt,* Digitale Datenbanken, S. 199.

Daten lassen sich also durchaus als Grundlage der menschlichen Wahrnehmung konzeptualisieren. Viel eher sind sie aber für die technologischen Erweiterungen unserer Sinne[57] erfahrbar, indem sie durch Messungen aufgenommen werden und so die Grundbausteine für darauf aufbauenden epistemischen Konstruktionen bilden. Erst so kann auch eine realitätsbeeinflussende Wirkung von Daten erzeugt werden, denn Daten alleine, ganz gleich ob in ihrer Form als wahrnehmbare Reize oder digitale Repräsentationen von Informationen, bringen eine solche Wirkung nicht hervor. Daten liegen zunächst nur vor[58] und müssen durch mediale Techniken – Sprache, Schrift, visuelle Medien, digitale Medien – in Bezug genommen und eine epistemische Struktur gebracht werden.

II. Information

Im Gegensatz zum stärker syntaktisch geprägten Begriffsverständnis von Daten zeichnet sich Information in dem Verständnis vieler demgegenüber dadurch aus, dass sie neben syntaktischen Aspekten im Sinne der semiotischen Dreiteilung[59] auch Aspekte der Semantik[60] und Pragmatik[61] kennt.[62] Dies räumt vor allem Menschen, die flexibel mit Bedeutung umgehen und Informationen zweckgerichtet nutzen können, eine wichtige Rolle in

57 *McLuhan,* Understanding media.

58 Freilich kann bereits der Datenerhebungsprozess konstruierende und differenzierende Effekte haben, s. dazu sogleich.

59 Zurückgehend auf *Morris,* Grundlagen der Zeichentheorie, S. 24; erstmals angewendet auf Information von *Weaver* in Shannon/Weaver (Hrsg.), Mathematische Grundlagen der Informationstheorie, 11 (35).

60 Die Semantik ist die wissenschaftliche Beschäftigung mit Bedeutung und mit den verschiedenen Beziehungen zwischen einem Zeichen und dem Bezeichneten.

61 Die Pragmatik ist die wissenschaftliche Beschäftigung mit den kontextabhängigen und nicht-wörtlichen Aspekten sprachlicher Bedeutung, die erst bei der Verwendung sprachlicher Ausdrücke entstehen, also in der Situation der Äußerung; es geht also vorrangig um die Relation zwischen Zeichen und Zeichenbenutzer:in.

62 Das gilt natürlich nicht für das syntaktische Verständnis von Information, wie es bei *Shannon/Weaver,* The mathematical theory of communication zum Ausdruck kommt. Da dieses Konzept den Informationsbegriff jedoch auf ein technisch-physikalisches Ereignis reduziert, bei dem die Übertragung von einer Zeichenmenge von einem Sender an einen Empfänger ohne Interesse für die (soziale) Bedeutung der Information im Mittelpunkt steht, hat er gegenüber semiotischen Begriffsverständnissen nur einen sehr begrenzten Anwendungsbereich.

Bezug auf Information ein.[63] Trotz dieser häufig genannten Dimensionen von Information fehlt – wie erwähnt – zum Informationsbegriff eine konsensuale Definition. Während auch einige Informationsbegriffe mitunter eher vereinfachen und Information recht schlicht mit Bedeutung oder empirischem Wissen gleichsetzen,[64] erscheint auch hier vor allem in der Zusammensetzung des Mosaiks der verschiedenen Begriffsfragmente die beste Möglichkeit zur Annäherung an die Bedeutung von Information zu liegen.

Ein Konzept, das gedanklich in Nähe der DIKW-Pyramide zu verorten ist, geht davon aus, dass Information sich gegenüber Daten durch einen Grad höherer Strukturiertheit auszeichnet,[65] wobei allerdings anerkannt wird, dass auch Daten nie ganz unstrukturiert sind, da jeder Wahrnehmungs- oder Erfassungsvorgang Daten in die für den jeweiligen Vorgang erforderliche Form bringt („raw data is an oxymoron"[66]).[67] Informationen sind dann insoweit Daten „in Formationen"[68] oder „formatierte Daten"[69]. Teil dieses Verständnisses ist aber auch, dass sich Information um Daten herum strukturiert, also ohne Daten nicht entsteht.[70]

Daneben lässt sich dem Informationsbegriff eine gewisse Prozesshaftigkeit zuschreiben, die aus seiner Subjektbezogenheit herrührt und sich vor allem auch in der kommunikativen Interaktion zwischen Menschen äußert. Damit wird der Informationsbegriff einerseits von einem Verständnis der Information als statische Größe abgelöst und dynamisiert. Andererseits deuten subjektbezogene Kommunikationsprozesse auf einen – auch etymologisch angelegten[71] – Kernaspekt der Information hin, namentlich

63 Siehe etwa *Jashapara,* Knowledge management, 14, 16; für einen systematischen Überblick s. *Zins* J. Am. Soc. Inf. Sci. 58 (2007), 479 (487 f.); ähnlich auch *Aulehner,* Polizeiliche Gefahren- und Informationsvorsorge, S. 231.

64 *Zins* J. Am. Soc. Inf. Sci. 58 (2007), 479 (487).

65 *Rowley* Journal of Information Science 33 (2007), 163 (174).

66 *Bowker,* Memory practices in the sciences, S. 184; *Gitelman* (Hrsg.), "Raw data" is an oxymoron.

67 So auch *Rowley* Journal of Information Science 33 (2007), 163 (174) Siehe dazu auch S. 50 ff.

68 *Awad/Ghaziri,* Knowledge management zitiert nach *Rowley* Journal of Information Science 33 (2007), 163 (168).

69 *Jessup/Valacich,* Information systems today, S. 7.

70 Siehe dazu die verschiedenen Definitionen bei *Rowley* Journal of Information Science 33 (2007), 163 (171); dieses inkludierende Stufenverhältnis entspricht auch der wirkmächtigen Formulierung von *Ackoff* , Journal of Applied Systems Analysis 16 (1989), 3 (3).

71 *Capurro/Hjørland* Ann. Rev. Info. Sci. Tech. 37 (2003), 343 (351 ff.).

die Wirkung von Information in Form der Beeinflussung der Informationsrezipient:innen.[72] Dies lässt sich noch weiter mit dem kybernetischen Verständnis von Informationen aufschlüsseln, das mit dem Konzept des Feedbacks, der Rückkoppelung, arbeitet: Zur Stabilisierung von Systemzuständen wird Input durch systemeigene Prozesse in einen am Systemzweck orientierten Output verwandelt, der auf die Systemumwelt einwirkt, aus der wiederum – eventuell veränderte – Inputs ins System gelangen.[73] Auf Kommunikationsprozesse angewandt erscheint, wie *Aulehner* es zusammenfassend formuliert, „Information bei einem Kommunikationsteilnehmer als Input und veranlaßt diesen zu einer Handlung als Output. Diese erscheint wiederum als Information beim Kommunikationspartner und regt diesen ebenfalls zu einer Handlung an."[74] Neben seinem Kernaspekt, den man als (Bedeutungs-)Inhalt von Information bezeichnen könnte, verweist der Informationsbegriff also auch auf ein Potenzial der *Wirkung*.[75] Wie die kursorische kybernetische Beschreibung impliziert, wird die Verarbeitung von Umweltreizen in Form von wie auch immer geartetem informationellem Input nicht ausschließlich von Menschen, sondern auch von technischen Systemen geleistet. Information spielt also auch eine Rolle in der Interaktion von Menschen mit informationstechnischen Artefakten.

Eine dritte Dimension des Informationsbegriff verweist hingegen auf einen genuin menschlichen Teilaspekt der Information. Wie bereits zuvor angesprochen, ist neben der wirkenden, also pragmatischen, Dimension auch Semantik eine relevante Teildimension von Information. Im Rahmen des semantischen Begriffsverständnisses von Information wird in erster Linie die Sinn- bzw. Bedeutungsdimension betont, womit die konzeptuelle Greifbarkeit aber eher verkompliziert wird, da es von kontingenten Passungsverhältnissen zwischen einer vorhandenen Datenstruktur und den kognitiven Schemata eines Individuums oder eines Kollektivs abhängt,

72 *Aulehner,* Polizeiliche Gefahren- und Informationsvorsorge, S. 231 f.

73 Das ist eine einfache Beschreibung eines Regelkreises etwa in Form eines Thermostats. Dabei handelt es sich zugegebenermaßen um eine sehr basale Beschreibung der Kybernetik, siehe dazu *Schiepek* in Schiepek (Hrsg.), Systemtheorie der Klinischen Psychologie, 307 (308 ff.).

74 *Aulehner,* Polizeiliche Gefahren- und Informationsvorsorge, S. 234; mit diesem kybernetischen Modell operiert auch das grundlegende Gutachen von *W. Steinmüller/Lutterbeck/Mallmann* ua, Grundfragen des Datenschutzes, Gutachten im Auftrag des Bundesministeriums des Innern, BT-Drs. 6/3826, 1971, S. 86.

75 Siehe dazu etwa *Hildebrandt* SSRN Journal 2017 (16), die dies zwar im Kontext von Information bespricht, sich dabei an der konkreten Stelle auf Daten bezieht.

ob bzw. inwiefern einem Datenpunkt Sinn oder Bedeutung zugeschrieben werden kann.[76] Was vor diesem Hintergrund als Information gelten kann, lässt sich demnach nur relativ bestimmen. Erschwert wird die genaue Bestimmung des semantischen Aspekts von Information auch durch das Massendatenphänomen. Denn obwohl der semantische Gehalt des Informationsbegriff in erster Linie auf menschliche kognitive Fähigkeiten verweist, sind die Transformationsschritte, die von (Massen-)Daten zu Information führen – exemplarisch nennen lassen sich etwa Klassifizierung, Neuordnung bzw. Sortierung, Aggregation, Durchführung von Berechnungen, Selektion[77] und Analyse – zunehmend ohne maschinelle Beteiligung überhaupt nicht mehr durchführbar. Mit der Zuwendung der Informatik zur Prozessierung von Semantik und Pragmatik[78] sowie dem informationstechnologischen Versuch über die Verarbeitung von Informationen, Zugriff auf die Realität zu erlangen, um diese steuernd beeinflussen zu können,[79] scheint insofern der Konnex zwischen dem semantischen Aspekt von Information und menschlichen Akteur:innen schwächer zu werden. Nichtsdestotrotz erfordern die Kontextabhängigkeit und subjektive Interpretationsoffenheit, die Information nach wie vor zugeschrieben wird[80] – zumindest im Rahmen der gegenwärtig zur Verfügung stehenden Informationsverarbeitungstechnologien – eine menschliche Partizipation in der Konstituierung von Information, wodurch sich ein vielgestaltiges Interaktionsfeld zwischen Menschen und informationstechnologischen Apparaturen auftut. Insofern verschwimmt die grundlegende Kontur der Unterscheidung zwischen Daten (für Maschinen) und Informationen (für Menschen) wieder stärker und der Informationsbegriff verunklart.

76 Man denke etwa an die digitalen Daten, die im Rahmen daktyloskopischer Erkennungsdienste bei der Polizei anfallen und deren Bedeutungsinhalt nur von einem kleinen Kollektiv hochspezialisierter Fachleute erkannt werden kann oder sogar nur noch von nicht-menschlichen Akteuren, wobei hier dann sicherlich fraglich wäre, an welche Stelle Information entsteht – durch die maschinelle Analyse oder erst durch die Wahrnehmung und kontextspezifische Verarbeitung durch einen Menschen im Anschluss an die maschinelle Analyse, siehe bspw. *Brayne,* Predict and surveil, Figure 1.1.

77 So etwa gefunden im bereichsspezifischen Werk von *Curtis/Cobham,* Business information systems, S. 4, wobei diese Arbeitsschritte durchaus generalisierbar erscheinen.

78 *S. Ott,* Information, S. 184.

79 So *Burkhardt,* Digitale Datenbanken, S. 197 zum Anliegen der Computerwissenschaft seit dem 2. Weltkrieg.

80 Siehe *Rowley* Journal of Information Science 33 (2007), 163 (171 f.) mwN.

Wirkmächtig, vor allem in sozialen Gemeinschaften, die sich selbst als Informationsgesellschaft empfinden, ist auch die – naturwissenschaftliche – Überlegung, es handle sich bei Information um eine neben Materien und Energie dritte Grundgröße der erfahrbaren Welt.[81] Das würde jedoch einen ontologisch irreduziblen Kern des Konzepts voraussetzen, der sich, wie etwa auch unterschiedliche Formalisierungsmöglichkeiten des Informationsbegriffs in der Mathematik zeigen,[82] nicht finden lässt. Insoweit bleibt der Informationsbegriff fragmentarisch und bildet ein „network of logically interdependent, but mutually irreducible, concepts",[83] sodass sich in medialen Konstellationen verschiedene Aspekte des Informationsphänomens bzw. -begriffs offenbaren und überlagern können.[84] Das erschwert eine genaue Analyse von Phänomenen, die rund um den Umgang mit Informationen – etwa wie vorliegend im Kontext polizeilicher Organisationen – auftreten.

Zusammenfassend lässt sich sagen: Information ist – trotz der informationstechnologischen Maschinisierung von Datenverarbeitungsprozessen – nach wie vor das in erster Linie an menschliche Kognition geknüpfte Phänomen, das sich aus der Interaktion mit Daten ergibt. Wie allerdings genau konkrete Informationen aus konkreten Daten inferiert werden, ist schwer abstrakt zu bestimmen. Zusätzlich enthält Information eine Wirkdimension, etwa als Wirkung auf Kommunikationsteilnehmer:innen oder auch im Rahmen von genetischer Information, deren (Nicht-)Vorhandensein ganz verschiedene Effekte nach sich ziehen kann. Diese Dimension ist für die menschliche Beziehung zur Realität absolut zentral, da Information als phänomenologisch umrissenem Konzept insofern eine Scharnierfunktion zwischen der Wahrnehmung der Welt und der Interaktion mit ihr zukommt.

III. Wissen

Die begriffliche Fassung von Wissen gestaltet sich als noch schwieriger als von Daten und Information,[85] was nicht zuletzt daran liegen dürfte,

81 Siehe dazu sowie zur dagegen geäußerten Kritik *Lyre* in Pietsch/Wernecke/M. Ott (Hrsg.), Berechenbarkeit der Welt?, 477.
82 *Lyre* in Pietsch/Wernecke/M. Ott (Hrsg.), Berechenbarkeit der Welt?, 477 (482 ff.).
83 *Floridi,* The philosophy of information, S. 33.
84 *Burkhardt,* Digitale Datenbanken, S. 194.
85 *Rowley* Journal of Information Science 33 (2007), 163 (172).

dass die letzteren beiden Größen durch eine kürzere Definitionsgeschichte weniger Raum für stark abweichende Auffassungen geben[86] und Wissen als Phänomen letztlich durch seine untrennbare Verknüpfung mit dem menschlichen Bewusstsein ebenfalls (noch) immer mit von dessen Undurchdringlichkeit erfasst wird.

Trotz der Kritik an der DIKW-Pyramide scheint es sinnvoll zu sein, Wissen als eine Größe zu konzeptualisieren, die auf Information basiert. Wissen zeichnet sich zusätzlich durch solche Facetten aus, die durch die Idiosynkrasien der menschlichen Kognition hinzukommen. Dazu gehören etwa Reflexion, Synthese und Kontext. Wissen entsteht in einer Gemengelage von kontextualen Informationen, Erfahrungen, Regeln und Werten. Konzeptuell an die DIKW-Pyramide angelehnt ist auf dem Kontinuum von Daten über Information zu Wissen die zunehmende Beteiligung der kognitiven Kapazitäten des Menschen das ausschlaggebende Merkmal. Wissen ist vielfältiger und tiefgründiger als Informationen und dadurch ungleich komplexer, weil jemand über konkrete Informationen nachgedacht, diesen eigene Erfahrungen hinzugefügt und sich eigene Urteile darüber gebildet hat.[87]

Wissen ermöglicht Orientierung und Struktur in einer zunächst unbestimmten Welt. Dafür weist Wissen eine festhaltende und eine wandelbare Komponente auf. Einerseits muss bereits gewusst werden, um weiteres Wissen lernen zu können. Andererseits muss die bestehende Wissensgrundlage aufgegeben werden können. Wissen ist Bedingung und Regulativ für Lernvorgänge und ermöglicht so eine Anpassung an unterschiedliche Umweltbedingungen.[88] Anders gewendet ist Wissen die Summe der Wahrnehmungsprozesse, die uns hilft, sinnvolle Schlussfolgerungen zu ziehen[89] und auf dieser Basis passende Handlungen in einer Umwelt zu ergreifen.

86 So *Weinberger*, The Problem with the Data-Information-Knowledge-Wisdom Hierarchy, https://hbr.org/2010/02/data-is-to-info-as-info-is-not (Stand: 01.10.2023).
87 *Pearlson/Saunders/Galletta,* Managing and using information systems, S. 12.
88 *Luhmann,* Soziale Systeme, S. 447 f.
89 *Awad/Ghaziri,* Knowledge management, S. 37 zitiert nach *Rowley* Journal of Information Science 33 (2007), 163 (173).

IV. Weisheit

Der Begriff der Weisheit ist schließlich der am wenigsten greifbare Teil der DIKW-Pyramide. Weisheit lässt sich etwa als Wissen in Verbindung mit Intuition und Urteilsvermögen konzeptualisieren, das die Fähigkeit zur Entscheidungsfindung erleichtert oder auch verbessert. Weisheit ist die Ebene in der Informationshierarchie, die vor allem Personen mit einem hohen Maß an Erfahrung und Reflexion zugeschrieben wird, die scheinbar intuitiv *wissen*, was zu tun ist und wie sie das erworbene Wissen bestmöglich – im Sinne dessen, was bekannt, aber auch dessen, was in ethischem Sinne gut ist – anwenden können.[90] Sie ist eine informationelle Stufe, die die Menschheit schon lange zu begleiten scheint – die Rolle der oder des Ältesten in der Stammesgesellschaft als diejenige Person, die in der Gemeinschaft am Längsten informationelle Reize aus der Umwelt aufnehmen und sie durch Reflexion und Erfahrung in ein konsistentes und praktisches Weltwissen verwandeln konnte, ist der frühste uns bekannte personale Inbegriff der Weisheit.[91] Heute scheinen in Bezug auf Weisheit vor allem ihre im Kern anthropologischen Implikationen von neuem Interesse. Vor dem Hintergrund der Schaffung von Maschinenintelligenzen wird in der Weisheit aufgrund ihrer inhärenten ethischen Aspekte eine originär menschliche Qualität gesehen: „Wisdom is a uniquely human state, or as I see it, wisdom requires one to have a soul, for it resides as much in the heart as in the mind."[92] Aufgrund seiner starken bewusstseins- und biografiebezogenen Komponenten hat es allerdings nur wenig verwendbare Aufschlüsselungen des Weisheitsbegriffes gegeben. Noch viel weniger ist zudem bekannt wie – was im Kontext der Polizei interessant wäre – Weisheit sich in Organisationen herausbildet und stabilisiert lässt.[93] Scheint der so verstandene Begriff der Weisheit auch vor allem in Zeiten von zunehmender Maschinenintelligenz einen wichtigen Impuls zu setzen, ist er für die Zwecke der vorliegenden Arbeit – die sich nicht primär um künstliche Intelligenz dreht – und aufgrund seiner überhaupt nur schwachen Kontur und schweren Fassbarkeit nicht brauchbar und daher zu vernachlässigen.

90 Angelehnt an *Pearlson/Saunders/Galletta,* Managing and using information systems, S. 12; *Rowley* Journal of Documentation 62 (2006), 251 (257).

91 *A. Assmann/J. Assmann* in Merten/Schmidt/Weischenberg (Hrsg.), Die Wirklichkeit der Medien, 114 (134).

92 *Bellinger/Castro/Mills*, Data, Information, Knowledge, and Wisdom, http://www.systems-thinking.org/dikw/dikw.htm (Stand: 01.10.2023).

93 *Rowley* Journal of Information Science 33 (2007), 163 (164).

Gleichzeitig ist damit aber nicht das Plädoyer verbunden, sich nicht näher mit dem Konzept auseinanderzusetzen. Vielmehr erscheint vor den geschilderten Zusammenhängen eine systematische Auseinandersetzung mit menschlicher Weisheit gebotener denn je.

B. Medienwandel als gesellschaftlicher Strukturwandel

Trotz der nach wie vor bestehenden Bruchstückhaftigkeit des gegenwärtigen informationstheoretischen Verständnisses veranschaulichen die digitalzeitlichen Umbrüche der Gegenwart die Bedeutung von Daten, Information, Wissen und Weisheit für die grundlegenden Strukturen der Gesellschaft. Ganz besonders deutlich wird diese umwälzende Kraft der Evolution von Medien,[94] wenn man mit *Luhmann* Kommunikation als irreduzible Kleinstgröße des Sozialen ansieht und damit ihre unhintergehbare Bedeutung für Gesellschaft freilegt.[95]

Die Räume des kommunikativ Möglichen hängen in einer jeden Gesellschaft maßgeblich von den kulturellen und medialen Konfigurationen[96]

94 Zum Medienbegriff und den Schwierigkeiten seiner genaueren Fassung siehe *Burkhardt,* Digitale Datenbanken, S. 23 ff. Deshalb wird vorliegend der alltagsverständliche Medienbegriff ohne nähere Erläuterung verwendet.

95 *Luhmann,* Soziale Systeme, S. 191 ff.

96 Der Konfigurationsbegriff wird hier verwendet in Anlehnung an Burkhardt *Burkhardt,* Digitale Datenbanken, S. 70 ff.: "Gebräuchlich ist der Begriff der medialen Konfiguration bereits in der Intermedialitätsforschung. Als mediale Konfiguration werden hier die Inszenierungsformen bezeichnet, »bei denen bestimmte technische Verfahren und Darstellungs- weisen eines Mediums im Rahmen eines anderen Mediums imitiert werden« (Wirth 2006b: 29). Die Thematisierung medialer Konfigurationen lenkt den Blick auf die intermediale **Verschränkung technischer Dispositive, Verfahren, Zeichensysteme etc. in konkreten Kommunikationssituationen.** Implizit vorausgesetzt wird hierbei die Unterscheidbarkeit bzw. Verschiedenheit einzelner Medien. Wie bereits diskutiert wurde, erweist sich die Differenzierung von Medien auf der Grundlage einer Mediendefinition jedoch als problematisch, weshalb vorgeschlagen wird, den Begriff der medialen Konfiguration eine Ebene niedriger anzusetzen, **um Medien als gewordene und historisch wandelbare Konfigurationen zu beschreiben**, die sich in unterschiedlichen Hinsichten (Ausdrucksmittel, Technologie, Materialität, Institutionalisierung usw.) verändern und transformieren können. Medien sind diesem Verständnis zufolge nicht begrifflich-systematisch, sondern nur empirisch-genetisch als mehr oder minder gefestigte mediale Konfigurationen zu unterscheiden, die **allenfalls temporär eine Spezifik** ausbilden, auf die in intermedialen Imitationsspielen Bezug genommen werden kann. Intermedialität ist demzufolge nur im Horizont der fragilen Stabilität medialer Konfigurationen denk- und beobachtbar.

der jeweiligen Zeit ab, wobei sich Kultur prinzipiell auf der Medienstruktur entfaltet, letztere also noch grundlegender in ihrer Bedeutung ist. Der Begriff des Mediums wird hier in einem – recht simplen – kommunikationsbezogenen Verständnis verwendet: Es handelt sich dabei um ein Instrument, durch das und mit dem sich Kommunikation entfalten[#] lässt. Die Medienepochen der Menschheit werden häufig in die der Sprache, der Schrift, des Buchdrucks und die der elektronischen Medien eingeteilt.[97] Während diese Einteilung nach wie vor analytischen Wert mit sich bringt, erscheint die Bezeichnung der gegenwärtigen Medienepoche als *elektronisch* schon beinahe veraltet, sind auch die physikalischen Basisprozesse zweifelsohne damit treffend beschrieben. So ist beispielsweise das Radio ein elektronisches Medium, das interessanterweise eine Renaissance der Sprache mit sich bringt,[98] aber es scheint sich doch deutlich von computerbasierten Medien zu unterscheiden. So nutzt etwa auch *Vesting* schon treffender den Begriff der „Computernetzwerke" in seiner Auseinandersetzung mit den Medien des Rechts.[99] Damit ist gegenüber dem Konzept der elektronischen Medien durchaus einiges an neuer analytischer Kraft hinzugekommen, Computer sind trotz ihre elektronischen Fundierung etwa gegenüber Radio und Film ein qualitativer Schritt in eine andere Richtung.[100] Auch das Netzwerkartige ist zweifelsohne eine oder sogar die Grundstruk-

---

So *Merten* in Merten/Schmidt/Weischenberg (Hrsg.), Die Wirklichkeit der Medien, 141 (143).

[#] Wird das Andere medialer Konstellationen als mediale Konfiguration begriffen, dann ist die Frage nebensächlich, ob beispielsweise der Raum, die Sprache, der Computer oder die Datenbank Medien sind oder nicht. Vielmehr gilt es diese als Bestandteile einer medialen Konfiguration zu begreifen, die daraufhin zu befragen sind, wie sie die Hervorbringung von sowie den Umgang mit medialen Konstellationen bedingen. Das Ziel der Auseinandersetzung mit medialen Konfigurationen ist die Beschreibung des Möglichkeitsraums, den diese aufspannen. Hierbei geht es nicht nur darum zu beobachten, was gesagt werden kann bzw. welche Unterscheidungen getroffen werden können, sondern auch, wie mediale Konstellationen hervorgebracht werden, wie sie distribuiert werden und wie an verschiedenen Orten und Zeiten an diese angeschlossen werden kann. **Kurzum: Es stellt sich die Frage, wie sich mediale Konfigurationen in unsere kommunikative Welt einschreiben und wie sich diese auf verschiedenen Ebenen verändert**." (Herv. d. Verf.)

97 Siehe bspw. *A. Assmann/J. Assmann* in Merten/Schmidt/Weischenberg (Hrsg.), Die Wirklichkeit der Medien, 114.

98 *A. Assmann/J. Assmann* in Merten/Schmidt/Weischenberg (Hrsg.), Die Wirklichkeit der Medien, 114 (138).

99 *Vesting,* Die Medien des Rechts: Computernetzwerke.

100 *Kittler,* Grammophon, film, typewriter, S. 7 spricht bspw. von einem "Universalmedium".

tur des Medialen zurzeit.[101] Zu implizit scheinen dagegen die datafizierten und algorithmisierten Aspekte der medialen Umwelten der gegenwärtigen Gesellschaften in einem Begriff wie dem der „Computernetzwerke" enthalten zu sein. Nichtsdestotrotz soll vorliegend mit *Vestings* Begriff verfahren werden, nicht zuletzt, weil ein kohärenteres Konzept für die mediale Konfiguration unserer Gegenwart noch nicht gefunden scheint.[102]

[103]Das mediale Fundament menschlicher Kommunikation ist die Sprache, die sich essenziell durch die meta-kommunikative Möglichkeit zur Negation sowie die arbiträre Codierung von Zeichen auszeichnet. Sie ermöglicht nicht nur Konzepte durch die Formulierung von Begriffen aus der nahtlosen Umwelt herauszulösen, sondern erlaubt die Ausbildung von Normen – etwa bezüglich des sozialen Verhaltens einer Gemeinschaft und auch hinsichtlich des Umgangs mit Sprache selbst. Dabei zieht Sprache den kommunikativen und damit auch sozialen Interaktionsraum zusammen: In oralen Gesellschaften beschränkt sich das Soziale auf denjenigen Radius, der durch die Wahrnehmung ihrer Mitglieder an einem umgrenzten Ort beschränkt ist. Informationen können nur zwischen Anwesenden weitergegeben werden und sind, wenn sie etwas nicht gegenwärtig Geschehendes beschreiben, stets durch Unsicherheiten geprägt. „Konstruktionen von Wirklichkeit durch Kommunikation", so schreibt *Merten*, „waren ohne Verfügbarkeit von Schrift also relativ riskant und zufällig, personenabhängig und tendenziell kurzlebig."[104] Zeitliches Empfinden kann im Wesentlichen nur zwischen rezenter Vergangenheit in der Erinnerung der Lebenden und der absoluten Vergangenheit, dem mythischen Ursprung der Welt und ihrer Bewohner:innen, unterscheiden.[105] Speicherplatz für Informationen ist begrenzt, das, was nicht aktiv in einem sprachlichen Bedeutungsnetz erhalten werden kann, aus dem sozialen Gedächtnis verschwindet, wobei sich vor allem pragmatisches Wissen, also solches, das gebraucht wird, jeweils halten kann. Zwar sind solche Stammesgesellschaften nicht völlig statisch, aber

101 Dazu *Castells,* Der Aufstieg der Netzwerkgesellschaft sowie die weiteren Bände der Reihe.

102 Auch *Luhmann,* Die Gesellschaft der Gesellschaft, S. 304, stellt sich angesichts des Medienwandels die Frage, "wie es sich auf die gesellschafliche Kommunikation auswirkt, wenn sie durch computervermitteltes Wissen beeinflußt wird".

103

104 *Merten* in Merten/Schmidt/Weischenberg (Hrsg.), Die Wirklichkeit der Medien, 141 (145).

105 *A. Assmann/J. Assmann* in Merten/Schmidt/Weischenberg (Hrsg.), Die Wirklichkeit der Medien, 114 (119).

Unerwartetes wird stets schematisch aus der Perspektive des gegenwärtigen Wissenshorizonts in die bestehenden Strukturen eingewoben. Wandel ist möglich, Entwicklung nicht. So heißt es bei *Assmann*: „Sie [die Gesellschaften] verschließen sich den Möglichkeiten der Evolution, der progressiven Rationalisierung von Handlungen, der Optimierung von Werkzeugen, der Abstrahierung kognitiver Strukturen."[106]

Mit Erfindung der Schrift verschiebt sich die Informationsverarbeitung menschlicher Gesellschaften radikal. Die Materialisierung von Information erlaubt eine externalisierte Speicherung und entpersonalisiert die menschliche Kommunikation ein stückweit. Gesellschaften sind in ihren Existenzbedingungen nicht mehr ausschließlich auf einen Raum unter Anwesenden beschränkt, vielmehr kann der Radius des Sozialen stark ausgedehnt werden. Die Ausdehnung erfolgt in zeitlicher Hinsicht, indem Informationen dauerhaft oder zumindest erheblich viel länger fixiert werden, als das gesprochene Wort oder auch das Gedächtnis sie tragen können. In sozialer Hinsicht kommt es zur Ausdehnung, indem Schrift Informationen – theoretisch – für beliebig viele Personen zugänglich macht und in sachlicher Hinsicht, indem Schrift die Authentizität der fixierten Informationen garantiert.[107] Mit einem sich wandelnden Vergangenheitsbewusstsein wird gesellschaftlich Entwicklung sichtbar und kann bewusst reflektiert werden. Gleichzeitig fragmentiert sozialer Konsens, denn der kulturelle Kanon, wie er in Sprache und zunächst auch in Schrift repräsentiert ist, wird durch andere, abweichende Perspektiven anders herausgefordert, wenn diese mit der Autorität schriftlicher Fixierung ausgestattet sind, statt nur gesprochen zu sein. Auch die Abstraktionsfähigkeit der Gesellschaft steigt.[108] Schrift ist die Informationstechnologie, die komplexer werdende Gesellschaften benötigen. Nicht umsonst entsteht sie unabhängig voneinander an verschiedenen Orten und Zeiten der Welt.[109] Gleichzeitig ist sie die Informationstechnologie, die komplexer werdende Gesellschaften und neue Gesellschaftsformen überhaupt erst ermöglicht. Neben diesen eher makrostrukturellen Auswirkungen ist auch die menschliche Kognition fundamental vom Wan-

106 *A. Assmann/J. Assmann* in Merten/Schmidt/Weischenberg (Hrsg.), Die Wirklichkeit der Medien, 114 (131 f.).

107 *Merten* in Merten/Schmidt/Weischenberg (Hrsg.), Die Wirklichkeit der Medien, 141 (148).

108 *A. Assmann/J. Assmann* in Merten/Schmidt/Weischenberg (Hrsg.), Die Wirklichkeit der Medien, 114 (132 f.).

109 *Merten* in Merten/Schmidt/Weischenberg (Hrsg.), Die Wirklichkeit der Medien, 141 (147).

del der Medien betroffen, wie es etwa *McLuhan* herausgearbeitet hat.[110] Daran angelehnt schreiben *Assmann und Assmann*:

> „Der oralen Multimedialität steht in der Schrift die rigorose Vereinseitigung des sinnlichen Spektrums aufs Visuelle gegenüber. An die Stelle einer ganzheitlich synästhetischen Wahrnehmung tritt die Konzentration des Blicks, der nicht im Schauen schweift, sondern im Lesen sammelt. Das, worauf er sich richtet, ist eine abstrakte Notation, ein Zeichen-Kode, nicht mehr."[111]

Mit dem Übergang von der Hand- zur Druckschriftlichkeit, ermöglicht durch die Technik des Buchdrucks, ändert sich nicht Schrift als Medium per se, aber die in ihr steckenden Potenziale werden in einer neuen Weise freigesetzt, was die Charakterisierung dieses Verfahrens als einschneidenden Evolutionssprung der Medien rechtfertigt. Das liegt zum einen an den quantitativen Möglichkeiten des Buchdrucks: In den ersten 50 Jahren des Buchdrucks werden mit einem Veröffentlichungsvolumen von ca. 8 Millionen Büchern die Leistungen aller europäischen Schreibstuben der vorigen elf Jahrhunderte in den Schatten gestellt.[112] Diese Massenmedialität des gedruckten Buches revolutioniert menschliche Informationsverarbeitung, indem zum ersten Mal Zugang zu externalisierten Informationen und damit zu Wissen in nie gekanntem Ausmaße skalierbar wird. Öffentlichkeit entsteht. Kritik und Kontingenz werden für eine zunehmende Masse erfahrbar. Monopolisiertes Wissen wird angefochten und die traditionelle Ordnung der Gesellschaften des frühen Druckzeitalters wird mit der Reformation erschüttert.[113] Der Medienwandel zieht eine fundamentale gesellschaftliche Fragmentierung und Zustände sozialer Unordnung nach sich. Gleichzeitig kommt es auch zu einem qualitativen Wandel der Medienevolution. Wo in der Schrift des Skriptors noch der handliche Duktus einen Rest an individueller Körperlichkeit sichtbar macht, radiert die Drucktechnik menschliche Idiosynkrasien aus. Die Lettern der Druckerpressen sind standardisiert und ermöglichen beliebige Kombinationen. So kann die mediale Zeichenabstraktion intensiviert und die Abstraktion in der medialen

110 *McLuhan,* The Gutenberg galaxy, passim.
111 *A. Assmann/J. Assmann* in Merten/Schmidt/Weischenberg (Hrsg.), Die Wirklichkeit der Medien, 114 (134).
112 *A. Assmann/J. Assmann* in Merten/Schmidt/Weischenberg (Hrsg.), Die Wirklichkeit der Medien, 114 (135).
113 *A. Assmann/J. Assmann* in Merten/Schmidt/Weischenberg (Hrsg.), Die Wirklichkeit der Medien, 114 (136).

Materialisierung von Informationen gesteigert werden. In dieser Rationalisierung medialer Herstellungsprozesse wird unter anderem eine der wesentlichen Voraussetzungen für das Entstehen der exakten Wissenschaften gesehen.[114] Neben gesellschaftlichen Un- oder auch: Umordnungsphänomenen ermöglicht die Buchdrucktechnologie indes auch neue Pfade der Ordnung. Neben der wissenschaftlichen Ordnung der Dinge bereitet der mediale Wandel auch neuen Formen sozialer Ordnung den Weg. Die bis in die Gegenwart dominierende Form der nationalstaatlichen Ordnung kann als eine Folge des Buchdrucks gelesen werden.[115] Erst die Standardisierung der Sprache kann die versprengten Gemeinschaften der frühen Neuzeit in Staatengebilden mit nationaler Identität zusammenbinden. Dabei werden die Freiheitsgrade der Druckerpressen, die etwa die Möglichkeit zu massenhafter Kritik mit sich bringt, ambivalent durch neue Kontrollmöglichkeiten ergänzt. Die zentralisierte Massenproduktion des Mediums gibt den Produzierenden die Möglichkeit der Beeinflussung dessen, was informationell in einer Gesellschaft zirkuliert, und ermöglicht auf diese Weise bis dato nicht gekannte Möglichkeiten der Kontrolle durch die im Entstehen begriffenen Staaten. *McLuhan* führt insofern treffend aus: „The producer-oriented or ruler-oriented version of the message of Gutenberg is simply that it is the ruler's right to impose uniform patterns of behaviour on society."[116]

Die nächste große Zensur medialer Konfigurationen wird durch die Elektronisierung der Übertragung und Speicherung von Informationen begründet. Kommunikationsmöglichkeiten weiten sich global über die ganze Welt aus und schaffen eine „virtuelle Weltkommunikationsgemeinschaft".[117] Die technische Infrastruktur der elektronischen Medienumwelt ermöglicht eine (noch) stärkere Vernetzung von Information.[118] Wieder ändert sich dadurch die Organisation des Wissens. Der im Buchdruckzeitalter halbwegs stabilisierte Bildungskanon wird durch die kakophonischen Dissonanzen

114 *A. Assmann/J. Assmann* in Merten/Schmidt/Weischenberg (Hrsg.), Die Wirklichkeit der Medien, 114 (136).

115 *McLuhan*, S. 115 et passim.

116 *McLuhan,* The Gutenberg galaxy, S. 236.

117 *A. Assmann/J. Assmann* in Merten/Schmidt/Weischenberg (Hrsg.), Die Wirklichkeit der Medien, 114 (137).

118 Auch vorherige mediale Konfigurationen lassen sich als Netz denken: Auch Sprache reagiert und verweist oft auf Sprache und bildet so eine netzwerkartige Struktur aus. Diese wird dann materialisiert durch Schrift und potenziert durch den Druck. Allerdings bringt die technische Infrastruktur der elektronischen Medien eine Verstetigung dieser materialisierten Netzwerkstruktur.

elektronischer Kommunikation zersplittert.[119] Die darin liegenden Unordnungspotenziale werden durch Reflexivität vernetzter Kommunikation vergrößert. Wie allen voran *Luhmann* systemtheoretisch dargelegt hat,[120] ist die Reflexivität sozialer Prozesse in ihren evolutiven Wirkungen unvorhersehbar. So ist die gegenwärtige Medienepoche der Computernetzwerke – die auf dem Fundament der elektronischen Medien steht, aber mit dem Computer ein vernetztes und interaktives Medium von besonderer Qualität aufweist – nicht mit den vorherigen Medienevolutionen vergleichbar.[121] Die heterarchisch[122]-azentrische Struktur der Computernetzwerke[123] egalisiert informationelle Ströme, womit sich die Frage stellt, „wie es sich auf die gesellschaftliche Kommunikation auswirkt, wenn sie durch computervermitteltes Wissen beeinflusst wird."[124] Jedenfalls kommt es zu einer Explosion von Informationsproduktion und -verarbeitung, die sich in den „weltweit operierende[n], konnexionistische[n] Netzwerke[n] des Sammelns, Auswertens und Wiederzugänglichmachens von Daten [abspielen…], die themenspezifisch, aber nicht räumlich begrenzt operieren."[125] Die gleichzeitige Erfahrbarkeit von in Daten granular kondensierten Gesellschaftsprozessen, die dadurch zumindest potentiell möglich wird, schafft Unübersichtlichkeit und Unordnung, weist aber auch informationstechnische Kontrollpotenziale auf. Die effektive Selektion von Information zur Konstruktion konsistenter Wirklichkeitsentwürfe wird in der Folge zur zentralen Anforderung an Informationsverarbeitungen, die – aufgrund der empfundenen oder tatsächlichen Unübersichtlichkeit und Unordnung erforderliche – gesellschaftliche Steuerungswirkung entfalten möchten.[126] Gleichzeitig wird Informationsverarbeitung, nachdem die diesbezüglichen Möglichkeiten des allein durch menschliche Kognition Prozessierbaren längst erschöpft sind, immer stärker technologisiert. Das wiederum verkleinert den Kreis derjenigen zunehmend, die mittels „rechnergestütztem Denken" Sinn aus den

119 *A. Assmann/J. Assmann* in Merten/Schmidt/Weischenberg (Hrsg.), Die Wirklichkeit der Medien, 114 (137 f.).
120 *Luhmann,* Die Gesellschaft der Gesellschaft, S. 413 ff.
121 *Merten* in Merten/Schmidt/Weischenberg (Hrsg.), Die Wirklichkeit der Medien, 141 (154).
122 Heterarchisch meint ein – im Gegensatz zum hierarchischen – im Wesentlichen gleichberechtigtes Ordnungsmodell verschiedener Elemente.
123 *Vesting,* Die Medien des Rechts: Computernetzwerke, S. 56.
124 *Luhmann,* Die Gesellschaft der Gesellschaft, S. 304.
125 *Luhmann,* Die Gesellschaft der Gesellschaft, S. 302.
126 *Merten* in Merten/Schmidt/Weischenberg (Hrsg.), Die Wirklichkeit der Medien, 141 (193 f.).

informationellen Strömen schöpfen können.[127] Es wird also gleichzeitig wichtiger und schwieriger, Informationen zu ordnen, was sich gleichsam in der Sozialordnung bemerkbar macht. „Ordnung", so schreibt *Nassehi*, „wird nun [im Zeitalter des Digitalen, FB] selbst zum Problem, weil ihre Beobachtung nicht mehr trivial ist."[128] So werden hergebrachte Ordnungsstrukturen – Nation, Familie, Partei und so weiter – instabil, während sich gleichzeitig im Erkennen der Musterhaftigkeit des Sozialen neue Ordnungspotenziale ergeben.[129] In diesen medialen Evolutionsprozessen, die sich in ihren Konsequenzen nach wie vor nur begrenzt abschätzen lassen (wobei man jedoch versuchen kann, die Strukturen der Neuerungen zu beschreiben[130]), ist auch die Entwicklung polizeilicher Informationsverarbeitung zu situieren. Diese kämpft einerseits mit Problemen der Strukturierung und Verwaltung der eigenen Daten und Informationen und der Produktion des daraus zu generierenden, handlungsleitenden Wissens. Andererseits erwachsen gerade der Polizei als eine der vorrangigen gesellschaftlichen Institutionen der Sozialkontrolle, durch ihre informationstechnologischen Strategien zur Lösung dieser Probleme neue Ordnungspotenziale, indem durch die Optimierung informationstechnologischer Verfahren die in der digitalen Gesellschaft vorhandenen „Kontrollüberschüsse"[131] zunehmend nutzbar werden.

C. Datentheoretische Fragmente

Neben dem nach wie vor wichtigen Computer werden gegenwärtige medientheoretische – aber auch gesellschaftliche – Diskurse vor allem auch durch die Begriffe der (Massen-)Daten und Algorithmen sowie damit zusammenhängender Konzepte künstlicher Intelligenz beherrscht. Da es vorliegend vor allem um Phänomene geht, die aus der digitalen Verdatung der Welt und der darauf reagierenden Datafizierung der polizeilichen Arbeit emergieren, erscheint eine Betonung des Datenbegriffes vorliegend naheliegender; allerdings sind damit stets und so auch im Folgenden die damit eng verbundenen algorithmischen Verfahren angesprochen. Auch

127 *A. Assmann/J. Assmann* in Merten/Schmidt/Weischenberg (Hrsg.), Die Wirklichkeit der Medien, 114 (137).
128 *Nassehi,* Muster, S. 39.
129 *Nassehi,* Muster, S. 41 ff.
130 So schon *Luhmann,* Die Gesellschaft der Gesellschaft, S. 302.
131 *Baecker,* Studien zur nächsten Gesellschaft, S. 169; *Nassehi,* Muster, S. 43.

wenn die Wandlungsprozesse unserer medialen Umgebungen sich in ihren Auswirkungen bisher nur begrenzt abschätzen lassen, kann doch schon – mit einem Fokus auf den (Massen-)Datenbegriff – über strukturelle Aspekte dieser Phänomene nachgedacht werden.

I. Massendaten – Verdatung – Datafizierung

Dem englischsprachigen Diskurs entlehnt, kann man den Massendaten-Begriff in die drei Vs aufgliedern[132]: Volumen, Velozität (Geschwindigkeit) und Vielfalt. Charakterisierend sind mithin große Datenmengen, die durch granulare[133] Erfassungen mittels Sensoren produziert werden, schnelle Datenverarbeitungsprozesse und eine Bandbreite an Datenquellen unterschiedlichster Art.[134] Treffender, weil facettenreicher ist die Definition von *boyd und Crawford*. Sie definieren Massendaten

> „as a cultural, technological, and scholarly phenomenon that rests on the interplay of: (1) Technology: maximizing computation power and algorithmic accuracy to gather, analyze, link, and compare large data sets. (2) Analysis: drawing on large data sets to identify patterns in order to make economic, social, technical, and legal claims. (3) Mythology: the widespread belief that large data sets offer a higher form of intelligence and knowledge that can generate insights that were previously impossible, with the aura of truth, objectivity, and accuracy."[135]

Die folgenden Ausführungen nehmen diese Definition als Ausgangspunkt für nähere Ausführungen sowie die Darstellung zusätzlicher Aspekte.

Voraussetzung für Massendaten als technisches Phänomen ist zunächst die – im Rahmen des Trends zum sogenannten *ubiquitous computing*[136] aufgekommene – Möglichkeit zur massenhaften Erfassung von digitalen Datenpunkten, die bereichspezifisch stark angereichte Daten-Akkumulatio-

132 In der Literatur finden sich auch noch weitere "Vs" zur Charakterisierung des Massendatenphänomens, siehe dazu etwa die Nachweise bei *Završnik* in Završnik (Hrsg.), Big Data, Crime, and Social Control, 3 (6).

133 *Kucklick,* Die granulare Gesellschaft.

134 *Laney*, 3D Data Management: Controlling Data Volume, Velocity, and Variety, 2001; *Lazer/Radford* Annu. Rev. Sociol. 43 (2017), 19; grundlegend und viel zitiert auch *Mayer-Schönberger/Cukier,* Big Data.

135 *boyd/Crawford* Information, Communication & Society 15 (2012), 662 (663).

136 *Weiser* Sci Am 265 (1991), 94.

nen entstehen lässt. Während in Anlehnung an die viel zitierten Überlegungen von *Mayer und Schönberger*[137] häufig darin schon der von der Digitalisierung zu unterscheidende Prozess der Datafizierung gesehen wird, ist mit der massenhaften Verwandlung von lebensweltlichen Prozessen in digitale Daten letztlich noch nicht das allein Charakteristische am Massendatenphänomen beschrieben. Vielmehr ist dieser Vorgang, den *Egbert* präziser als „Verdatung"[138] bezeichnet, zwar substanziell, muss aber durch einen Aspekt der Prozesshaftigkeit ergänzt werden.

Denn bezüglich der massenhaft anfallenden Daten-Akkumulationen haben sich neue informationelle Praktiken herausgebildet, deren Ziel es ist, aus den Massendaten Sinn und Wissen zu extrahieren. Zentral für diese Praktiken ist der Begriff des Algorithmus, der technisch eine bestimmte Abfolge von logischen Operationen zur Erfüllung einer spezifischen Aufgabe meint. Durch einen Input wird der Algorithmus gestartet und verwandelt diesen dann in den (hoffentlich gewünschten) Output.[139] Im Bereich des Massendatendiskurses hat sich jedoch ein darüber hinausreichendes Verständnis etabliert: Algorithmen sind Prozesse, mit denen – zumeist unter Nutzung technischer Verfahren wie dem maschinellen Lernen oder anderer Formen künstlicher Intelligenz – Computer automatisierte Entscheidungen über mögliche Zukünfte mithilfe eines großen Datensatzes treffen.[140] Im Stufenverhältnis von Daten, Informationen und Wissen, wie es die DIKW-Pyramide veranschaulicht, lässt sich auch ein Kontinuum von nicht-algorithmisch zu algorithmisch konzeptualisieren: Daten und einige Elemente von Information sind dabei die Domäne des Algorithmischen, andere Elemente von Information und Wissen (und Weisheit) hingegen die des Nicht-Algorithmischen also Menschlichen.[141] Erst diese neue Form der Wissensgenerierung, gleichsam der prozesshafte Aspekt des Massendatenphänomens, ist aufgrund ihrer Bedeutung für die Produktion von handlungsleitendem Wissen als Kernaspekt des Massendatenphänomens anzusehen. Datafizierung ist also durch die Kombination zweier Prozesse geprägt: „the transformation of human life into data through processes of

137 *Mayer-Schönberger/Cukier,* Big Data, S. 78.

138 *Egbert* in Hunold/Ruch (Hrsg.), Polizeiarbeit zwischen Praxishandeln und Rechtsordnung, 77 (78).

139 *Barocas/Rosenblat/boyd* ua SSRN Journal 2014 (3); siehe näher zum Algorithmus unter S. 77 ff.

140 *Brayne,* Predict and surveil, S. 3.

141 *Awad/Ghaziri,* Knowledge management zitiert nach *Rowley* Journal of Information Science 33 (2007), 163 (168).

quantification, and the generation of different kinds of value from data."[142] Für den polizeilichen Kontext lässt sich der Begriff der Datafizierung mit *Egbert* dahingehend spezifizieren, dass damit ein Typus der Datenverarbeitung angesprochen ist, der sich auf die „zunehmende Nutzung korrelativ fundierte, statistische Datenanalyse" stützt, also eine „auf Entscheidungsfindung ausgerichtete und algorithmisch vermittelte (Massen-)Analyse von Daten" ist, „deren Resultate entsprechend umgesetzt werden und somit die polizeilichen Praktiken nachhaltig prägen."[143]

Damit gehen tiefgreifende Veränderungen in der menschlichen Relation zur Umwelt einher und damit auch zu Kriminalität und Sozialkontrolle, wobei eine datengestützte Überwachung und Lenkung von Bevölkerungsverhalten durch staatliche Akteure allerdings keine Innovation des Massendatenzeitalters ist.[144] Bereits seit Aufkommen des Konzepts der Bevölkerung im siebzehnten Jahrhundert im Rahmen der mathematischen Entwicklung der statistischen Analyse erschien der Rückgriff auf objektive Größen wie Zahlen als Möglichkeit, den „Zufall zu zähmen" und damit Stabilität in einer zunehmend als instabilen und sich verändernden Welt zu schaffen.[145] Diese Entwicklung brachte die Idee einer „Norm" und mathematische Vorstellungen von Abweichung mit sich und ermöglichte auch Berechnungen von Risiken und damit einhergehende Prognosen ein.[146]Allerdings erfahren die der Quantifizierung des Sozialen innewohnenden Potenziale für Überwachung und Kontrolle eine deutliche Potenzierung durch die nunmehr zu beobachtende Datafizierung. Es ist *Završnik* darin zuzustimmen, wenn dieser in Bezug auf *Wittgensteins* viel zitierten Satz – die Grenzen der Sprache sind die Grenzen unserer Welt[147] – schreibt, dass „the language of big data is tearing down the world of what counts as crimerelevant knowledge (now databases), what counts as proper reasoning (now algorithms) and how we should tackle – prevent and investigate – crime (now predictive policing) and prosecute cases (now automated justice)."[148] Das transformative Potenzial der „Sprache" der Massendaten

142 *Mejias/Couldry* Internet Policy Review 8 (2019) (3).
143 *Egbert* in Hunold/Ruch (Hrsg.), Polizeiarbeit zwischen Praxishandeln und Rechtsordnung, 77 (78).
144 Grundlegend *Foucault,* Sicherheit, Territorium, Bevölkerung; siehe auch *Desrosières,* The politics of large numbers.
145 *Hacking,* The Taming of Chance, S. 3.
146 *Pangrazio/Sefton-Green* Learning, Media and Technology 45 (2020), 208 (209).
147 *Wittgenstein,* Tractatus logico-philosophicus.
148 *Završnik* in Završnik (Hrsg.), Big Data, Crime, and Social Control, 3 (3).

beruht dabei nicht nur auf einer granularen Aufschlüsselung von Personen, Ereignissen, Objekten und sonstigen Phänomenen in digitale Daten, sondern auch auf der Vielzahl an Instrumenten und Verfahren, die letztlich auf einem mathematischen Fundament stehen und eine „Grammatik kombinatorischer Möglichkeiten"[149] bieten. Diese erlaubt es, zuvor datafizierte Dinge beliebig miteinander zu arrangieren, Verbindungen herzustellen und zeigt auf diese Weise mannigfaltige, bis dato unerschlossene Ansatzpunkte für Wissensproduktion und daran anknüpfenden Handlungsoptionen auf.[150]

Massendaten und die mit ihnen zusammenhängenden informationellen Praktiken werden als Paradigmenwechsel begriffen. Autor:innen wie *Mayer-Schönberger und Cukier* sehen darin mit Blick auf die vorstehenden informationstheoretischen Überlegungen wohl zu recht eine Revolution der Wissensordnung.[151] Am radikalsten formuliert hat diese Umgestaltung bereits 2007 *Andersons* Idee der „end of theory", nach der die Wissenschaft als Methode wegen der „Datensintflut" überflüssig sei. Keine Hypothesen, Modelle und Experimente mehr – stattdessen wird das notwendige handlungsleitende Wissen nur noch aus den Daten selbst kontextspezifisch und situationsabhängig generiert und angewandt.[152] Dieses erkenntnistheoretische Paradigma – kritischer könnte man es auch eine Massendaten-Ideologie nennen – beruht, wie *Kitchin* gezeigt hat, auf vier Grundvoraussetzungen[153]: Massendatenverarbeitung erfassen weltliche Teilbereiche total und in höchstmögliche Auflösung (1), es gibt in keiner Weise Bedarf für apriorische Theorieleistungen (2), Massendaten sind frei von menschlichen *Biases* (Verzerrungen) und sprechen aus sich selbst heraus mit inhärenter Bedeutung und Wahrheit (3) und Bedeutung transzendiert Kontext und bereichsspezifische Wissensgrenzen und kann daher von allen interpretiert werden, die eine Statistik oder Datenvisualisierung entschlüsseln können (4). All diese Prämissen sind so angreifbar,[154] dass sie nach gegenwärtigem Stand nicht durchhaltbar erscheinen. Im Rahmen von Polizeiarbeit, die nach umfassender Objektivität strebt, sind aber zunächst vor allem die erste und dritte Grundvoraussetzung problematisch. Auch Massendaten

149 *Amoore* Security Dialogue 45 (2014), 423 (431).
150 *Završnik* in Završnik (Hrsg.), Big Data, Crime, and Social Control, 3 (3).
151 *Mayer-Schönberger/Cukier,* Big Data.
152 *Anderson*, The end of theory: The data deluge makes the scientific method obsolete.
153 *Kitchin* Big Data & Society 1 (2014), 1-12 (4).
154 *Kitchin* Big Data & Society 1 (2014), 1-12 (4 f.).

bleiben nur ein Ausschnitt aus der unendlich extensiven Wirklichkeit, der durch verschiedene Selektionsfilter gebildet wurde.[155] Die Produktion von Massendaten hängt insofern ab von einer „complex assemblage of people, places, documents, and technologies"[156]; so ermöglicht das informationstechnologisch fundierte Phänomen der Massendaten zwar mitunter eine bessere Konstruktion der Welt[157] durch algorithmische Datenverarbeitung, gleichzeitig bleiben aber auch Massendaten von Menschen gemacht und damit fehlbar – was auch für Formen der darauf aufbauenden Wissensgenerierung gilt.

II. Konstruiertheit von Daten – Konstruktion durch Daten

Informationelle Handlungen wie das Erheben, Speichern, Auswerten und allgemeiner: Verarbeiten von Daten implizieren eine bereits vorfindliche Datenmaterie, die unverzerrt aufgenommen werden kann. All diese Datenverarbeitungsschritte setzen allerdings voraus, dass zunächst empirische Phänomene durch bestimmte Prozesse und Entscheidungen in Datenpunkte umgewandelt worden sind.[158] Bei einer solchen Herauslösung von Daten aus der „Nahtlosigkeit der Phänomene" sind vor allem die spezifischen Vorstellungen und interpretativen Strukturen der jeweiligen Professionskultur Faktoren, die den Daten eine bestimmte Form geben[159]. Da bereits auf Ebene der menschlichen Sprache Voreingenommenheit und kognitive Verzerrungen bestehen, setzen sich diese in allen anderen medialen Konfigurationen, die vom Menschen geschaffen und genutzt werden, fort.[160] Zudem sind die Entscheidungen darüber, welche Daten von wem zu welchem Zweck verarbeitet werden sollen, stets in einen sozialen Kontext eingebettet, der von vielfältigen relationalen Machtverhältnissen durchzogen ist.[161] Was mit Daten gemessen und quantifiziert werden kann, ist mithin keine

155 *Kitchin* Dialogues in Human Geography 3 (2013), 262 (265).
156 *Ribes/S. Jackson* in Gitelman (Hrsg.), "Raw data" is an oxymoron, 147.
157 *Amoore/Raley* Security Dialogue 48 (2017), 3 (5): "world-making capacities of algorithms".
158 *Egbert/Leese,* Criminal futures, S. 74.
159 *Gitelman/V. Jackson* in Gitelman (Hrsg.), "Raw data" is an oxymoron, 1 (3).
160 Siehe zu Biases in der menschlichen Sprache und den Implikationen für die gegenwärtigen informationstechnologischen Entwicklungen *Caliskan/Bryson/Narayanan* Science 356 (2017), 183.
161 *Brayne,* Predict and surveil, S. 5; siehe auch *Desrosières,* The politics of large numbers; *Buckel,* Subjektivierung und Kohäsion, S. 172

rein technische Frage, sondern vor allem auch eine normative, die mit institutionellen Prioritäten, organisatorischen Erfordernissen sowie gruppenspezifischen und individuellen Präferenzen zusammenhängt.[162] Die Massendatenproduktion ist insofern immer auf eine technische Infrastruktur angewiesen, welche die Datengenerierung beeinflusst, in ihrer konkreten Ausgestaltung aber kontingent ist.[163] Für polizeiliche Informationspraktiken lassen sich strukturellen Prädispositionen der Datengeneration beispielsweise an der BKADV[164] aufzeigen. Diese Verordnung regelt, welche Daten im polizeilichen Informationsverbund INPOL[165] gespeichert werden dürfen oder sollen und geben damit einen impliziten Einblick in die Fachkultur polizeilicher Datenverarbeitung. Dazu gehören – wenig verwunderlich – tat- und täterbezogene Datenarten, die zur Zuordnung von Personen zu bestimmten Kriminalitätsfeldern oder auch ganz generell zur Identifizierung von Personen dienen. Auffallend ist daneben eine Betonung kombinatorischer Datenpunkte, etwa zwischen Personen und Personen, Gruppen, Organisationen und Institutionen oder auch Ereignissen und Sachen (§ 2 Abs. 1 Nr. 12-14 BKADV). Daneben sind auch (noch) normativere Datenarten enthalten, etwa in Form der sog. personengebundenen Hinweise (§ 2 Abs. 1 Nr. 16 BKADV), die Beurteilungen wie „gewalttätig" oder „Psychische und Verhaltensstörung" enthalten.[166]

Die Idee der sozialen Konstruiertheit von Daten oder Information ist nicht neu, ebenso wenig wie die Verwendung von Daten durch den Staat zu gesellschaftsregulierenden Zwecken.[167] Allerdings hat sie im Rahmen des – insbesondere kritischen – Diskurses zu Massendaten neue Relevanz erlangt (auch hier: „raw data is an oxymoron"[168]). So wird der Konstruiertheit von Daten im Kontext der Polizei dann auch von *Egbert und Leese* eine besondere Bedeutung für den Bereich des Predictive Policing[169] zugemessen, da die Genauigkeit dieser algorithmisierten Form der Kriminalitätsanalyse sehr stark von der Qualität der polizeilichen Daten abhängt.[170] Das lässt sich indessen verallgemeinern: Da letztendlich die gesamte polizeiliche

162 *Brayne,* Predict and surveil, S. 5.
163 *Mejias/Couldry* Internet Policy Review 8 (2019) (3).
164 Näher zur BKADV unten S. 227 ff. et passim.
165 Näher zu INPOL unten S. 230 ff.; zum Hinweissystem siehe unten S. 247 ff.
166 Bremische Bürgerschaft, LT-Drs. 19/996, S. 4.
167 Grundlegend *Scott,* Seeing like a state
168 *Bowker,* Memory practices in the sciences, S. 184; *Gitelman* (Hrsg.), "Raw data" is an oxymoron.
169 Näher zum Predicitive Policing siehe unten S. 227 ff.
170 *Egbert/Leese,* Criminal futures, S. 75.

Tätigkeit auf der Produktion von Daten im Austausch mit empirischen Phänomenen und der weiteren Verarbeitungen dieser Daten beruht, muss durchweg ein hohes Daten-Qualitätsniveau gewährleistet werden, damit die Daten innerhalb der polizeilichen Organisationen den gewünschten Mehrfachnutzungen zugeführt werden können, um das polizeiliche Handeln wirksam anzuleiten. Vor allem ist auch mit Blick auf die *Biases* von Daten aus einer auf Qualität bedachten Perspektive zu fordern, dass die Daten möglichst objektiv konstruiert werden, damit sie die Welt nicht unnötig verzerrt wiedergeben.

Allerdings sind Daten und Informationen nicht nur konstruiert. Aufgrund ihrer Bedeutung für das menschliche Weltverhältnis sind sie auch entscheidend für die Konstruktion der Wirklichkeit.[171] Dabei sind informationelle (Daten-)Repräsentationen von Phänomenen wie Kriminalität jedoch nie ganz in der Lage, die bestehende Komplexität einzufangen und abzubilden.[172] Obwohl Daten in ihrer heutigen digitalen Form und ihrem Verarbeitungsmodus schon sehr fluide Abbilder der Realität erstellen können, sind sie, wenn auf ihrer Grundlage gehandelt wird, im Moment des Handelns doch nur wieder momentane Manifestationen von konkreten Wissenspraktiken in einem bestimmten Informationsmedium, das zusätzlich interpretationsbedürftig ist.[173] Allerdings vermögen gerade Transformationsschritte, die die Interpretationsfähigkeit steigern sollen (etwa Visualisierungen), dazu beizutragen, die dem lebensweltlichen Phänomen eigentlich innewohnenden Mehrdeutigkeiten zu verhüllen, indem sie stets bestimmte Aspekte eines Phänomens stärker betonen als andere.[174] Gleichzeitig werden dadurch aber erst die Abstraktheit und Vieldeutigkeit von Datenpunkte in eine greifbare Wirklichkeit transformiert, innerhalb derer konkrete Handlungen ergriffen werden können.[175] Die informationellen Repräsentationen der Wirklichkeit werden so zu einer eigenen, handlungsleitenden Wirklichkeit für sich, die, wenn sie nicht auf Daten von hinreichender Qualität und Repräsentativität basiert, gravierende Probleme für die handelnden Akteur:innen, aber vor allem auch die Betroffenen mit sich bringen kann, die von Entscheidungen auf Grundlage solcher

171 Grundlegend dazu *Berger/Luckmann,* The social construction of reality.
172 Siehe für die die Repräsentation von Wirklichkeit durch Massendaten generell *Kitchin* Big Data & Society 1 (2014), 1-12 (4).
173 Siehe dazu etwa das Beispiel der "crime maps" bei *Egbert/Leese,* Criminal futures, S. 119.
174 *Egbert/Leese,* Criminal futures, S. 120.
175 *Egbert/Leese,* Criminal futures, S. 128 f.

Repräsentationen tangiert werden. Durch informationelle Repräsentation wird der fluide Datenstrom in eine konkrete Realitätsinterpretation – etwa: gefährlicher Ort oder gefährliche Person – gegossen, die eine gewisse Stabilität aufweisen muss, um dann etwa polizeiliches Handeln auf ihr fußen lassen zu können. Gleichzeitig wird die Repräsentation nicht in einer Art gelingen, die subjektiver Interpretation von Seiten der Polizeibeamt:innen völlig die Grundlage entzieht und so bleibt im Rahmen der informationellen Repräsentation der Wirklichkeit Raum für Zuschreibungen und Deutungen. Insofern besteht ein Spannungsverhältnis zwischen Geschlossenheit und Offenheit datenbasierter Realitätskonstruktionen durch die Polizei: Das nachvollziehbare Anliegen, die informationellen Repräsentationen verständlich und praktikabel zu machen,[176] muss gleichzeitig so strukturiert sein, dass eine zu intuitive, vereinfachte Nutzung eine eventuell kritische Auseinandersetzung mit den Repräsentationen nicht völlig aufhebt. Dabei gibt es indessen auch wieder unterschiedliche Anforderungen an Reflexionserwartungen hinsichtlich der Repräsentationen. So sollen operative Kräfte wie der Streifendienst handlungsleitende Informationen offensichtlich auch nicht die ganze Zeit hinterfragen müssen. Denn oft kann und muss eine Repräsentation den Zugang zu einer informationsüberladenen Umgebung stark vereinfachen, wodurch überhaupt erst effektive Polizeiarbeit ermöglicht wird. Gleichzeitig ist aber beachtenswert, dass es informationelle Repräsentationen von Risiko sind, die vermittelt durch verschiedene technologische und auch kognitive Transformationsschritte, die sie durchlaufen, zu einem als real wahrgenommenen Kriminalitätsrisiko führen.[177] Ob dieses tatsächlich besteht ist – neben dem Umstand, dass es durch seine Zukunftsgerichtetheit immer einen Ungewissheitsgrad hat – insofern auch entscheidend von der Qualität der Daten und Transformationsschritte abhängig, die zur Risikoprognose geführt haben. Dabei ist das kein Problem, das spezifisch nur bei Spielarten des Predictive Policing oder sonstigen Massendatenverarbeitungen auftreten würden, sondern schon bei personenbezogene (Risiko-)Einschätzungen auftreten kann, die etwa im Rahmen der Nutzung von INPOL getroffen werden. Bekommen beispielsweise Polizeibeamt:innen bei einem Einsatz über bestimmte Personen Informationen aus ihrer Datenbank, werden sie ihr Handeln vermutlich zumindest teilweise an diese informationellen Repräsentationen, die in einem

176 *Egbert/Leese,* Criminal futures, S. 133.
177 *Egbert/Leese,* Criminal futures, S. 134.

rein deskriptiven Sinne Verzerrungen der Wirklichkeit sind, anpassen.[178] Vor dem Hintergrund der Fluidität[179] von datenbasierten Wirklichkeitsrepräsentationen – also der schnellen Wandelbarkeit durch hinzukommende oder wegfallende Datenpunkte – sind zusätzliche oder intensivierte (menschliche) Reflexionsmechanismen im Rahmen der Weiterverarbeitung erforderlich, die gegebenenfalls einen fehlerhaften informationellen Gehalt in den Datenaggregationen erkennen und korrigieren können.[180] *Biases*, also die nicht wirklichkeitsgetreue, verzerrte Darstellung bestimmter Eigenschaften, sind dabei in Datensätzen sehr verbreitet,[181] vor allem wenn sie auf selektiven Informationspraktiken beruhen, wie sie für Polizeien beschrieben worden sind.[182] Solche Verzerrungen in den Daten lassen sich auch für den deutschen Kontext bereits oberflächlich beobachten: Etwa die Überrepräsentierung von nicht-deutschen Tätern in der Polizeilichen Kriminalstatistik, und daran anknüpfend im Strafjustizsystem, ist Ausdruck selektiver Kontroll- bzw. Informationspraktiken.[183] Problematisch sind derartige *Biases* neben den offensichtlichen individuellen Diskriminierungsmöglichkeiten auch aufgrund struktureller Diskriminierungspotenziale: Handeln Polizeiorganisationen auf Grundlage ihrer selektiven Datenbasis, besteht immer die Gefahr eines sich selbstverstärkenden und perpetuierenden Kreislaufes, indem sich polizeiliche Aktivitäten auf das selektiv wahrgenommene abweichende Verhalten konzentrieren und dabei wiederum vor allem Daten über den selektierten Bereich produzieren, auf deren Grundlage wiederum weitere Handlungen primär im ausgewählten Bereich ergrif-

178 Siehe insbesondere zu dem in diesem Kontext relevanten Hinweissystem im polizeilichen Informationswesen unten S. 247 ff.

179 *Cheney-Lippold,* We are data, S. 147 et passim.

180 *Egbert/Leese,* Criminal futures, S. 99.

181 Für Verzerrungen bereits in unserer alltäglichen Sprache siehe etwa *Caliskan/Bryson/Narayanan* Science 356 (2017), 183; diese setzen sich etwa in "gesellschaftlichen" Daten fort, s. etwa *Olteanu/Castillo/Diaz* ua Front Big Data 2 (2019), 13; zudem ist auch naturwissenschaftliche Datenerhebung nicht frei von Biases, s. etwa *Dee* Q. J. R. Meteorol. Soc. 131 (2005), 3323.

182 *Dangelmaier/Brauer* in Hunold/Ruch (Hrsg.), Polizeiarbeit zwischen Praxishandeln und Rechtsordnung, 213; *Buil-Gil/Medina/Shlomo* The British Journal of Criminology 61 (2021), 364; generell zur Selektivität der Sozialkontrolle siehe etwa *Oberwittler/Lukas* in Hormel/Scherr (Hrsg.), Diskriminierung, 221; *Buil-Gil/Moretti/Langton* J Exp Criminol 2021.

183 Siehe dazu etwa *Hagemann* in Boers (Hrsg.), Kriminologische Perspektiven. Wissenschaftliches Symposium zum 70. Geburtstag von Klaus Sessar, 139 und *Walter* NK 19 (2007), 126.

fen werden.[184] Auf diese Weise wird auch die Welt aus polizeilicher Sicht in einer verzerrten Weise konstruiert: Bestimmte Gebiete oder Populationen erscheinen als besonders gefährlich und da die Polizei insofern eine große gesellschaftliche Deutungsmacht besitzt, diffundiert diese Einschätzung in die gesamtgesellschaftliche Konstruktion der Kriminalitätswirklichkeit.

III. Datensubjekte und Datendoubles

Auf Daten gestützte Wirklichkeitskonstruktionen betreffen nicht ausschließlich aber in einer Vielzahl der Fälle Menschen. Die dabei entstehenden datenbasierten Repräsentationen lassen sich durch den von *Lyon, Haggerty und Ericson* sowie andere geprägten Begriff[185] des Datendoubles[186] fassen und weiter beschreiben. Unter Datendoubles versteht man das aus persönlichen Datenfragmenten zusammengestellte, elektronische oder auch digitale Profil einer einzelnen Person, das in der Gesellschaft zunehmend an Bedeutung gewinnt, da auf seiner Grundlage Bewertungen und Urteile in verschiedenen Zusammenhängen getroffen werden. Das Datendouble wird zu einem Teil der Person, zu einer Komponente ihrer Identifizierung, auch wenn das Datensubjekt, also der Mensch, über den das Double angelegt wurde,[187] seine Richtigkeit in Frage stellen mag.[188] Die vor allem informationstechnologisch fundierte(n) „surveillant assemblage[s]" der spätmodernen Gesellschaft, wie etwa auch das polizeiliche Informationswesen, zerlegt den Körper und seine Verhaltensweisen in eine Reihe diskreter Bedeutungsströme und setzt diese zu einer neuen Entität zusammen, „which transcends human corporeality and reduces flesh to pure information."[189] So wird das Individuum vervielfältigt und ein zusätzliches Selbst im Digitalen geschaffen.[190] Neben, oder in vielen Fällen vielleicht sogar statt, der Beobachtung des Individuums werden in einer neuen Überwachungsform

184 *Završnik* (Hrsg.), Big data, crime and social control, S. 12; so auch *d'Alessandro/O'Neil/LaGatta* Big Data 5 (2017), 120 (132).
185 Darüber hinaus gibt es noch weitere Bezeichnung, wie etwa *Solove,* The digital person.
186 *Lyon,* Surveillance studies: an overview; *Haggerty/Ericson* Br J Sociol 51 (2000), 605.
187 *Lyon* International Sociology 19 (2004), 135; *Lyon* Ethics and Information Technology 3 (2001), 171.
188 *Lyon,* Surveillance studies: an overview, S. 199 f.
189 *Haggerty/Ericson* Br J Sociol 51 (2000), 605 (612 f.).
190 *Poster,* The mode of information, S. 97.

Individuen zugeordnete Datenströme beobachtet, die *Clarke* als „dataveillance" beschrieben hat.[191]

Wie im Rahmen der historischen Darstellungen gezeigt werden wird,[192] ist die Polizei seit ihren Anfängen auf die Erstellungen von informationellen Profilen verdächtiger und sonst relevanter Personen fokussiert, sodass man hier bereits von Datendoubles *avant la lettre* sprechen kann. Mit den neuen Analysemöglichkeiten, die der informationstechnologische Wandel bereitstellt, können diese Ansätze allerdings quantitativ und qualitativ ausgebaut werden. So können einerseits die einzelnen Personen zugeordneten Individualprofile aussagekräftiger werden. Andererseits kann auch das abstrakte Profil eines bestimmten Delinquententypus – etwa des Wohnungseinbruchsdiebes – verfeinert werden. Die zunehmende Masse an Daten und Geschwindigkeit ihrer Verarbeitung lässt die dabei entstehenden Datendoubles allerdings instabil werden. Es gibt dann nicht mehr *das* Profil der kriminellen Person, vielmehr entsteht eine Art amorphes Musterkonzept von Abweichung bzw. devianten Personen, das abhängig ist vom Vorhandensein bestimmter Parameter,[193] wobei sich auch diese Parameter ständig aufgrund neuer datengenerierter Erkenntnisse wandeln können.[194]

Die Verwendung einer Reihe von Datenpunkten zur Rekonstruktion oder Vorhersage der Absichten und Verhaltensweisen einer Person (ob belastend oder entlastend) beruht dabei auf der Annahme, dass die Strafverfolgungsbehörden trotz dieser Fluidität von Datendoubles die korrekte Schlussfolgerung aus der Aggregation der – ebenfalls nur in Grenzen objektiven – Daten konstruieren.[195] Dabei kommt erschwerend hinzu, dass das Datendouble, wie *Cheney-Lippold* treffend feststellt, als eine durch Daten mess- und konstruierbare Größe konzeptuell *Webers* Idealtypus nahekommt.[196] Dieser, so heißt es bei ihm, „wird gewonnen durch einseitige *Steigerung eines* oder *einiger* Gesichtspunkte und durch Zusammenschluss einer Fülle von diffus und diskret, hier mehr, dort weniger, stellenweise gar nicht, vorhandenen *Einzel*erscheinungen, die sich jenen einseitig herausgehobenen Gesichtspunkten fügen, zu einem in sich einheitlichen Gedanken

191 *Clarke* Commun. ACM 31 (1988), 498.
192 Siehe dazu unten S. 101 ff.
193 Siehe etwa *Brayne,* Predict and surveil, S. 43.
194 *Cheney-Lippold,* We are data, S. 27.
195 *Brayne,* Predict and surveil, S. 54.
196 *Cheney-Lippold,* We are data, S. 23 f.

bilde."[197] Datendoubles entstehen insofern immer aus einer nur beschränkten Perspektive, die nicht alles erfassen kann. Es erscheint insofern wichtig, dass das Datendouble und das ihm Zugeschriebene als Konstruktion erkenn- und insofern anfechtbar bleiben, denn „in seiner begrifflichen Reinheit ist dieses Gedankenbild nirgends in der Wirklichkeit empirisch vorfindbar, es ist eine *Utopie*."[198] Die Gleichsetzung von Datendouble und real verdächtigem Subjekt ist demnach nicht ohne Schwierigkeiten, denn sie sind nicht identisch; ersteres ist nur die (unvollständige) informationelle Repräsentation von und Approximation an eine reale Person. Ergibt sich sogar erst im Wege datafizierter Polizeiarbeit aus aggregierten Daten ein möglicher Verdacht, ist ein so geformter Verdacht das Ergebnis einer mitunter schwer nachvollziehbaren Konstruktionen-Kette, deren Validität nur so stark sein kann wie ihr schwächstes Glied. Gleichzeitig hat dieser Prozess aber wieder performative, konstruierende Wirkung, worauf *Raley* verweist: „[T]he composition of flecks and bits of data into a profile of a terror suspect, the re-grounding of abstract data in the targeting of an actual life, will have the effect of producing that life, that body, as a terror suspect."[199]

IV. Datenwahrnehmung und Datenliterarität

Mediale Wandlungsprozesse haben, wie beschrieben, transformative Wirkungen auf die Gesellschaft als Ganzes. Spricht man von Strukturwandel, werden damit vor allem Veränderungen auf Makro- und Mesoebene assoziiert. Allerdings sind Medien auch für die individuelle Verbindung des Menschen zur Welt zentral, sie bedingen das „menschliche Selbst- und Weltverhältnis."[200] Deutlich wird das etwa im systemtheoretischen Verständnis des Menschen als psychisches System, das nur über mediale Konfigurationen an den gesellschaftlichen Systemen teilhaben kann: „Die Sprache überführt soziale in psychische Komplexität."[201] Auch auf Mikroebene, auf Ebene des einzelnen Individuums, der einzelnen Polizeibeamt:innen, sind daher

197 *Weber,* Gesammelte Aufsätze zur Wissenschaftslehre, S. 191, Hervorhebung im Original
198 *Weber,* Gesammelte Aufsätze zur Wissenschaftslehre, S. 191, Hervorhebung im Original.
199 *Raley* in Gitelman (Hrsg.), "Raw data" is an oxymoron, 121 (128).
200 *Burkhardt,* Digitale Datenbanken, S. 36.
201 *Luhmann,* Soziale Systeme, S. 368.

durch die informationstechnologische Evolution Auswirkungen zu erwarten.

Dabei ist der Diskurs um die Änderung der Wahrnehmung durch Veränderungen unserer Fähigkeiten zur Konzentration von Aufmerksamkeit jedenfalls nicht neu[202]; dass bereits seit Beginn der Moderne und sogar darüber hinaus[203] (informations)technologische Umwälzungen unsere Weltwahrnehmung verändern,[204] sagt dabei allerdings noch nichts darüber aus, in welchem Maße die individuellen und gesellschaftlichen Wahrnehmungsfähigkeiten sich gegenwärtig durch das Phänomen der Massendaten und neue, darauf fußende Modi der Wissensproduktion wandeln.[205] Hier lässt sich zwar Definitives noch nicht feststellen, jedoch sind durchaus Entwicklungstendenzen in ihren Grundzügen erkennbar.

In den fünf Jahrhunderten seit Erfindung und Verbreitung des Buchdrucks und auch der ersten elektronischen Medien war das menschliche Denken vor allem linear – es folgte der Struktur eines Druckerzeugnisses, später der eines Radio- oder Fernseherzeugnisses, die aber ebenfalls linear, anhand eines Sendeplans, geordnet waren. Dieses lineare Denken war, so schreibt *Carr*, die kognitive Grundstruktur für „the imaginative mind of the Renaissance, the rational mind of the Enlightenment, the inventive mind of the Industrial Revolution, even the subversive mind of Modernism."[206] Die medialen Konfigurationen der Gegenwart evozieren nun aber eine neue Strukturierung des menschlichen Geistes: Denken ist immer weniger linear, sondern zunehmend *vernetzt*.[207] Dabei handelt es sich keineswegs um eine rein epistemische Wirkung, die sich ausschließlich im Rahmen theoretischer Denkmodelle niederschlägt. Vielmehr materialisiert sich die Evolution der Kommunikationsmedien auch basal auf neurobiologischer Ebene der Gehirnstruktur. Die Nutzung (digitaler) Technologien, so legen

202 Siehe dazu bereits *Crary,* Suspensions of perception, der den Beginn des u.a. durch technologische Umwälzuungen induzierten Aufmerksamkeits- und Wahrnehmungsveränderungsdiskurses auf Mitte des 19. Jahrhunderts datiert.

203 *McLuhan,* The Gutenberg galaxy.

204 Die Idee, dass Medien die Welt völlig unverfälscht wiedergeben (sollen), ist Ausdruck eines normativen Medienbegriffs, siehe *Burkhardt,* Digitale Datenbanken, S. 39. Ein solcher kann für die Frage nach der tatsächlichen Wirkung von Medien auf die Wahrnehmung nur begrenzt eine Rolle spielen.

205 *Sacasas*, Attending to the World, https://theconvivialsociety.substack.com/p/attending-to-the-world?utm_source=url (Stand: 01.10.2023).

206 *Carr,* The shallows, S. 10.

207 Siehe etwa *Nyíri* Stud East Eur Thought 60 (2008), 149.

es neurowissenschaftliche Studien nahe,[208] hat signifikanten Einfluss auf die Gehirnfunktionen und das Verhalten, etwa auf visuelle Wahrnehmung, Sprache und Kognition. Die Einflüsse sind dabei sowohl positiv als auch negativ. Zu den bisher identifizierten schädlichen Auswirkungen einer extensiven Nutzung digitalen Technologien gehören etwa verstärkte Aufmerksamkeitsdefizitsymptome, Beeinträchtigung der emotionalen und sozialen Intelligenz, Technologie-Abhängigkeit, soziale Isolation, Beeinträchtigung der Gehirnentwicklung und Schlafstörungen. Dem stehen jedoch auch etliche förderliche Wirkungen gegenüber. So zeigten etwa Nutzer:innen, die bis dato nur wenig mit vernetzten Informationsmedien interagiert hatte, bei simulierten Internetrecherchen eine deutliche Zunahme der neuronalen Aktivität im Gehirn. Anwendungen digitaler Technologien zeigten zudem generell positive Wirkungen auf das Gedächtnis, die Multitasking-Fähigkeiten, die fluide Intelligenz[209] und andere kognitive Fähigkeiten. Neuronale Ursache dieser Wirkungen ist die Plastizität des Gehirns,[210] die eine Adaption an unterschiedliche Umweltbedingungen ermöglicht und sich dementsprechend auch an mit Daten saturierte, digital vermittelte Umgebungen anpassen kann. Die konzeptuelle Fassung des menschlichen Denkens als vernetzt setzt die Kognition mit Arbeitsprozessen computerbasierter Informationstechnologien gleich. Das Konzept von der Vernetzung des Denkens und des Gehirns geht dabei so weit, anzunehmen, dass Computer auch über entsprechende Apparaturen direkt mit dem Gehirn interagieren könnten. Das soll nicht zuletzt an der vergleichbaren Funktionsweise von Gehirn und Computer liegen: „Both involve the instantaneous transmission of electric signals to make linkages. Because our nervous system is plastic, it can take advantage of this compatibility and merge with the electronic media, making a single, larger system."[211] Verbindungen solcherart können die kognitiven Potenziale des Gehirns verstärken – allerdings nur in der ständigen Symbiose mit informationstechnologischen Apparaturen: Mit

208 Siehe überblicksweise dazu sowie zum Folgenden *Small/J. Lee/Kaufman* ua Dialogues Clin Neurosci 22 (2020), 179 sowie *Hoehe/Thibaut* Dialogues Clin Neurosci 22 (2020), 93.

209 Fluide Intelligenz meint die Fähigkeit, flexibel zu denken und zu argumentieren, und erfordert ein Arbeitsgedächtnis, d. h. die Fähigkeit, Informationen über einen kurzen Zeitraum hinweg zu behalten, *Small/J. Lee/Kaufman* ua Dialogues Clin Neurosci 22 (2020), 179 (185).

210 Grundlegend *Hebb,* The organization of behavior, erläuternd *Doidge,* The brain that changes itself.

211 *Doidge,* The brain that changes itself, S. 310 f.

einem Smartphone kann heutzutage jede:r durch fremde Orte navigieren und sich zurechtfinden. Ohne digitale Kartenanwendungen sind hingegen viele schon in der eigenen Heimatstadt orientierungslos.[212] So konnte auch experimentell gezeigt werden, dass technologische Assistenzsysteme bei der Lösung von Problemen, wenn sie „zu" hilfreich sind, dazu führen können, dass die menschliche Kognitionsfähigkeit, die zur Lösung des Problems erforderlich wäre, unentwickelt bleibt.[213]

Wie sich die verschiedenen informationstechnologischen Instrumente in den Händen der Polizist:innen auswirken und inwiefern es zu den beschriebenen Effekten kommen kann, ist bisher indessen kaum bekannt. Während die Stimulierung neuronaler Aktivitäten und damit die Verbesserung von Gedächtnis, Multitasking-Fähigkeiten und fluider Intelligenz begrüßenswert sind, gilt es, negative Auswirkungen des informationstechnologischen Wandels im Kontext der Polizei zu erkennen. So gibt es etwa Hinweise darauf, dass die Recherche in vernetzten Informationsspeichern – wie dem Internet – zur Überschätzung des eigenen Wissens, einem erhöhten kognitiven Selbstbewusstsein sowie zur Unterschätzung der Grenzen des eigenen Wissens führt.[214] Solch ein *Bias* könnte sich nachteilig etwa in kriminalpolizeilichen Ermittlungen auswirken, sowohl auf den Ermittlungserfolg als auch auf eventuell fälschlicherweise ins Visier der Ermittler:innen geratende Personen. Dieser zielkonflikthafte Aspekt des Einsatzes von datenverarbeitender Technologie im Polizeialltag wird auch von *Brayne* am Beispiel von komplexer Datenanalyse-Software beschrieben: „Of course, this situational awareness made possible by Palantir can, in addition to protecting officers, ratchet up their sense of danger and escalate an already tense situation. Such platforms provide an unprecedented number of data points supporting the „danger imperative"[215] Eine ähnliche Dynamik dürfte auch im deutschen Kontext eine Rolle gespielt haben, wo die Polizei immer wieder – in kritisierbarer Weise[216] – mit tödlichem Ausgang auf psychisch kranke Menschen, die in entsprechender Weise informationell in den polizeilichen Datenbanken repräsentiert sind,[217] schießt. Hier

212 Zur stimulierenden Wirkung von kognitiven Navigationsleistungen siehe die vielzitierte Studie von *Maguire/Gadian/Johnsrude* ua Proc Natl Acad Sci U S A 97 (2000), 4398.
213 *van Nimwegen,* The paradox of the guided user: assistance can be counter-effective.
214 *Fisher/Goddu/F. Keil* J Exp Psychol Gen 144 (2015), 674.
215 *Brayne,* Predict and surveil, S. 46 f.
216 *Finzen* Soziale Psychiatrie 2014, 40.
217 Siehe dazu unten S. 247 ff.

verengt sich die auf polizeiliche Daten gestützte Wahrnehmung in der Einsatzsituation auf den Gefährlichkeitsaspekte der Betroffenen. Vor diesem Hintergrund stellt sich auch die Frage, ob oder inwieweit sich durch die datenförmige Abbildung der Menschen eine Entpersonalisierung im Umgang von Polizist:innen mit Bürger:innen einstellt.

Dieser Aspekt weist auf die normative Dimension des Datenumgangs und der sich darauf gründenden Datenwahrnehmung hin. Es ist nichts Neues, dass polizeiliches Wissen keine rein technische, sondern auch eine normative Angelegenheit ist: Dass etwas gewusst werden kann, ist davon zu unterscheiden, ob oder wie etwas gewusst werden soll. Die normativen Rahmenbedingungen von Datenverarbeitung markieren Grenzen dessen, was gewusst werden soll und beeinflussen so, was gesucht, erhoben, verarbeitet, wahrgenommen und als wichtig erachtet wird.[218] Das ist umso wichtiger für soziale Phänomene wie Devianz bzw. Kriminalität, die zusätzlich noch von den normativen Gegebenheiten der jeweiligen Gesellschaft abhängen. Wissen über Kriminalität ist somit doppelt normativ. Vor dem Hintergrund der beschriebenen kognitiven Auswirkungen von Massendatenverarbeitung stellen sich die Fragen der Normativität polizeilicher Wahrnehmung indessen mit neuer Akzentuierung. Die Frage, welche Auswirkung eine bestimmte informationstechnologische Form der Wissensproduktion nach sich zieht, darf nicht unbeantwortet bleiben. Auch wenn die Weltkomplexität zunehmend die Notwendigkeit mit sich bringt, moderne Datenverarbeitungstechnologien zur Produktion handlungsermöglichenden Wissens zu nutzen, erscheint es verfehlt, daraus einen absoluten Imperativ der umfassenden Nutzung solcher Verfahren abzuleiten. Vielmehr bedarf es einer normativen Entscheidung über den Einsatz von Massendatenverarbeitungsverfahren, die sich, wie *Weizenbaum* schreibt, nicht auf „tasks that demand wisdom" erstrecken sollten.[219]

Wer über Daten wahrnimmt, nimmt die Welt also anders wahr. So durchläuft die von der Polizei betriebene Datafizierung von Kriminalität bestimmte, für Datenverarbeitungstechnologien spezifische, Simplifizierungen „to convert the messy realities of people's personal attributes and behaviours into the objective, tractable language of numbers."[220] Diese Daten haben dann aber für sich genommen zunächst wenig informationellen Gehalt. Dieser entsteht erst durch die Interpretation eines oder mehrerer

218 *Brayne,* Predict and surveil, S. 65.
219 *Weizenbaum,* Computer power and human reason, S. 227.
220 *Jasanoff* in Jasanoff (Hrsg.), States of knowledge, 13 (27).

Datensätze in einem Kontext, der bestimmt, auf welche Weise die gesammelten Daten verarbeitet und präsentiert werden müssen, um im jeweiligen Zusammenhang wirksam werden zu können.[221] Neben dem Kontext spielt indessen auch die „materielle Form" von Daten eine wesentliche Rolle für die Nutzungsmöglichkeiten der potentiell in den Daten repräsentierten Informationen. So ist es einerseits typisch für das gegenwärtige Massendatenparadigma, Daten in unverarbeiteten und unverschlüsselten Zuständen in großem Umfang zu sammeln, um nach Möglichkeit eine objektivere Datengrundlage zu schaffen, als dies bei selektiver kuratierten Datensätzen der Fall wäre. Diese Datengrundlagen sind allerdings für das menschliche Bewusstsein weitgehend unentzifferbar – erforderlich für die Entschlüsselung sind nunmehr komplizierte Technologien und spezielles Fachwissen.[222] So kann man es in diesem Zusammenhang – trotz der etwas unglücklichen Umkehrung von religiösen und wissenschaftlichen Erkenntnisverfahren – durchaus treffend finden, wenn *Gillespie* davon spricht, dass Algorithmen keine „barometers of the social" seien, vielmehr produzierten sie „hieroglyphs: shaped by the tool by which they are carved, requiring of priestly interpretation".[223] Zunehmend entscheiden also nicht mehr nur Polizeibeamt:innen aufgrund ihres hergebrachten professionellen Wissens und ihrer Erfahrungen, sondern es ist eine technische Interpretation der in Daten aufgelösten und algorithmisch verarbeiteten sozialen Beziehungsnetze, die polizeiliches Tätigwerden anleitet.[224] Dabei wäre es aber falsch, die Handlungsmacht ausschließlich im Bereich des Technisch-Maschinellen zu verorten. Die zur Entschlüsselung der Datensätze erforderliche Verarbeitung umfasst vielfältige Computerarbeiten (etwa: Archivierung, Kennzeichnung, Verknüpfung, Analyse und so weiter), die zwar häufig einen gewissen Automationsgrad aufweisen, aber immer auch von menschlichen Designentscheidungen abhängen und von Menschen – zumindest partiell – durchgeführt werden. Im Verlauf dieser Verarbeitungen nimmt die soziale Bedeutung der Datensätze zu, indem die Daten mit Blick auf die Wirklichkeit strukturiert werden, sodass sie immer stärker für die Datenarbeit durch Menschen verfügbar gemacht werden.[225] Dabei ist nur wenig

221 *A. Wolff/Gooch/Cavero Montaner* ua The Journal of Community Informatics 12 (2016) (16).
222 *Pangrazio/Sefton-Green* Learning, Media and Technology 45 (2020), 208 (212 f.).
223 *Gillespie* in Gillespie/Boczkowski/Foot (Hrsg.), Media Technologies, 167 (190).
224 *Cheney-Lippold,* We are data, S. 24.
225 *Selwyn* Learning, Media and Technology 40 (2015), 64 (65).

bekannt über die Wechselwirkungsprozesse zwischen Mensch und Maschine im Rahmen dieser Datenverarbeitungen, die immer mit bestimmten Motivationen, Interpretationen und Vorurteilen verwoben sind.[226] Denn während das wissenschaftliche Interesse an den neuen Technologien algorithmischer Wissensproduktion sehr groß ist, gibt es bisher vergleichsweise wenig Forschung zu der damit interagierenden menschlichen Komponente, insbesondere im Kontext komplexer Massendaten.[227]

Hier setzt das aus der Bildungsforschung stammende Konzept der Datenliteralität an, das im weitesten Sinne einen kompetenzvollen Umgang mit datenreichen Umgebungen zum Ziel hat. Als vergleichsweise neues Konzept sind die Definitionen von Datenliteralität[228] indessen noch im Fluss. Generell geht es darum Verständnis, Kontrolle und Handlungsfähigkeit in datengestützten Systemen zu entwickeln.[229] Der Begriff der Literalität umfasst dabei zunächst zwei miteinander verbundene mediale Praktiken: Lesen und Schreiben. In Bezug auf Daten lässt sich diese doppelte Dynamik in Analogie dazu als Fähigkeit konzeptualisieren, die Zeichen zu lesen, die in Daten eingeschrieben wurden, als auch die Fähigkeit, Dateneinschreibungen selbst vorzunehmen.[230] Datenliteralität beschreibt damit Fähigkeiten, die mit der Nutzung von Daten als Teil des alltäglichen Denkens und Argumentierens zur Lösung von Problemen verbunden sind. In einer zunehmend datenvermittelten Welt kann Datenliteralität somit als grundlegende Lebenskompetenz betrachtet werden, da ein mehr oder weniger intensiver Umgang mit Daten immer alltäglicher wird und der Einzelne zunehmend Urteile auf der Grundlage von Daten fällt und Entscheidungen über die Verwendung – auch der eigenen personenbezogenen – Daten trifft.[231] Mit Blick auf die zuvor erläuterte DIKW-Pyramide könnte man Datenliterarität weiter als Fähigkeit definieren, Daten in Informationen und schließlich in handlungspraktisches Wissen umzuwandeln. Das wiederum setzt die Fähigkeit voraus, Daten zu identifizieren, zu sammeln,

226 *Pangrazio/Sefton-Green* Learning, Media and Technology 45 (2020), 208 (213).
227 *A. Wolff/Gooch/Cavero Montaner* ua The Journal of Community Informatics 12 (2016) (10).
228 Zu anderen ebenfalls wichtigen und neuen Formen von Literarität im Zeitalter der Massendaten siehe etwa *Shields* IQ 28 (2005), 6 sowie *Pangrazio/Sefton-Green* Learning, Media and Technology 45 (2020), 208 (214 f.).
229 *Pangrazio/Sefton-Green* Learning, Media and Technology 45 (2020), 208 (212).
230 *Pangrazio/Sefton-Green* Learning, Media and Technology 45 (2020), 208 (212).
231 *A. Wolff/Gooch/Cavero Montaner* ua The Journal of Community Informatics 12 (2016) (10).

zu organisieren, zu analysieren, zusammenzufassen und zu priorisieren. Dazu gehört auch, Hypothesen zu entwickeln, Probleme zu identifizieren, Daten zu interpretieren und Handlungsoptionen zu bestimmen, zu planen, umzusetzen und die Umsetzung zu beobachten.[232] Spezieller, aber vor allem im zunehmend informationstechnisierten Polizeialltag relevant, ist das eher technische Konzept der „Dateninfrastrukturliteralität", das sich auf sich verschiebenden Beziehungen von Datenbanken, Software, Standards, Klassifikationssystemen, Prozessen, Benutzeroberflächen und anderen Elementen bezieht, welche an der Erstellung und Nutzung von Daten beteiligt sind.[233] In diesem Verständnis ist Datenliteralität mehr als nur das „Lesen" und „Schreiben" von Dateninschriften. Wesentlich ist vielmehr, eine Sensibilität für die Organisation von Dateninfrastrukturen zu entwickeln und die Fähigkeit auszubilden, die soziotechnischen Infrastrukturen, die an der Erstellung, Gewinnung und Analyse von Daten beteiligt sind, zu verstehen, innovativ darauf zu reagieren und – wenn nötig – in sie einzugreifen.[234]

Trotz der kontextabhängigen Diskrepanzen in den Definitionen von Datenliteralität, weisen die Versuche der begrifflichen Konturierung auch vereinende Gemeinsamkeiten auf. So sind erstens zumeist prozessbezogene Kompetenzen angesprochen, die die anwendungsbezogene Komponente der Datenliteralität berühren. Darunter fallen etwa das Durchführen von Datenerhebungsprozessen und das Planen, Umsetzen und Beobachten von auf Daten aufbauenden Handlungsabläufen.[235] In einer zweiten Kategorie lassen sich demgegenüber Kompetenzen zusammenfassen, die man als datenliterarisches Grundlagenwissen bezeichnen könnte, wie etwa ein Verständnis dafür, wie Daten erzeugt oder wie Informationen interpretativ aus Datensätzen gewonnen werden können.[236] Neben diesen allgemeineren Komponenten lässt sich aufgrund der teilweise komplexen Anforderungen in der Interaktion mit Daten noch die Komponente spezialisierten Wissens und spezialisierter Fähigkeiten als Teil des Konzepts der Datenliteralität ausmachen. Darunter fällt etwa die aufwändige Visualisierung von Daten, aber auch komplexe Datenkonvertierungen oder -verknüpfungen zu Ana-

232 *Mandinach/Gummer* Educational Researcher 42 (2013), 30 (30).
233 *Gray/Gerlitz/Bounegru* Big Data & Society 5 (2018), 1-13 (3).
234 *Gray/Gerlitz/Bounegru* Big Data & Society 5 (2018), 1-13 (8).
235 *A. Wolff/Gooch/Cavero Montaner* ua The Journal of Community Informatics 12 (2016) (12).
236 *A. Wolff/Gooch/Cavero Montaner* ua The Journal of Community Informatics 12 (2016) (12).

lysezwecken.[237] Neben diesen operativen Komponenten von Datenliteralität zeichnet sich der konzeptuelle Bedeutungsgehalt zusätzlich aber noch durch den Aspekt einer kritischen Kompetenz aus. Diese verlangt die Fähigkeit, Datenrepräsentationen anzuzweifeln, (die richtigen) Fragen zu stellen und zu reflektieren, anstatt schlicht Symbole zu entschlüsseln, wie es die maschinelle Intelligenz tut.[238]

Zusammengenommen ergibt sich daraus die folgende, an *Wolff et al.* angelehnte, Definition. Demnach ist Datenliteralität die Fähigkeit, auf der Grundlage verschieden großer Datensätze durch einen Untersuchungsprozess Fragen zu stellen und zu beantworten, wobei ethische Aspekte der Datennutzung zu berücksichtigen sind. Datenliteralität basiert auf grundlegenden praktischen und kreativen Fertigkeiten und beinhaltet auch die Fähigkeit, das Wissen über spezielle Formen des Datenumgangs und der Dateninfrastrukturen je nach Zielsetzung zu erweitern. Bezogen auf Datenverarbeitungsschritte umfasst Datenliteralität somit die Befähigung dazu, Daten zu erheben, auszuwählen, zu bereinigen, zu analysieren, zu visualisieren, zu kritisieren und zu interpretieren sowie die adäquate Kommunikation anhand von Daten und durch Daten schlussendlich als Teil eines weltbezogenen Gestaltungsprozesses zu nutzen.[239]

Erst eine in diesem Sinne datenliterale Person kann datenvermittelte Sachverhalte richtig bewerten, die konkret präsentierten Informationen kritisch bewerten und besser verstehen, wie die nunmehr von ihr beigesteuerten Daten genutzt werden können. Ohne die beschriebenen Fähigkeiten besteht die Gefahr, dass Wissen produziert wird, das als Fundament für Handlungen unzureichend ist.[240] Für Polizeiorganisationen, in denen Wissen und daran anknüpfende Entscheidungen zunehmend durch Datenverarbeitungsprozesse vermittelt werden, wird Datenliteralität zur Schlüsselkompetenz. Dabei wird zumeist ihre operative Komponente im Vordergrund stehen: Polizist:innen müssen mit vielfältigen Datenquellen und den daraus fließenden Datenarten zweckgerichtet umgehen können, also – in der Sprache der gesetzlichen Zweckbestimmungen – zur Abwehr von Gefahren und Aufklärung von Straftaten. Dabei ist es zwar unnötig von

237 *A. Wolff/Gooch/Cavero Montaner* ua The Journal of Community Informatics 12 (2016) (14).

238 *Pangrazio/Sefton-Green* Learning, Media and Technology 45 (2020), 208 (213).

239 *A. Wolff/Gooch/Cavero Montaner* ua The Journal of Community Informatics 12 (2016) (23).

240 *A. Wolff/Gooch/Cavero Montaner* ua The Journal of Community Informatics 12 (2016) (16).

jeder Person im Polizeidienst ein stark erhöhtes oder sogar Höchstmaß an Datenliteralität zu fordern. Zu unterschiedlich sind die verschiedenen Spezialisierungen innerhalb der Polizei, die etwa auf – auch hinsichtlich der anfallenden Daten – unterschiedliche Deliktsfelder wie beispielsweise das der Cyberkriminalität reagieren. Jedoch erscheint ein Verzicht auf allgemeine Datenliteralität vor dem Hintergrund steigender Mensch-Maschine-Interaktionen im polizeilichen Tätigkeitsfeld nicht durchhaltbar. Das gilt umso mehr für die kritischen Aspekte der Datenliteralität, deren Sicherstellung vor allem für technische Schlüsselpositionen im polizeilichen Informationswesen geboten scheint.

D. Technologie

Information und Daten sind für die vorliegende Untersuchung nicht nur als Phänomene per se von Interesse, sondern vor allem auch in ihrem Zusammenhang mit Technologie. Ähnlich wie schon bei Informationen und Daten ist auch der Begriff der Technologie nicht ganz einfach zu fassen. Das liegt wohl nicht zuletzt auch daran, dass Technologien, ähnlich wie auch Information und zunehmend auch Daten, so alltäglich (geworden) sind, dass die genaue Beschreibung aufgrund der Nähe zum zu Beschreibenden schwerfällt.[241] Technologie lässt sich zunächst als Phänomen fassen, dass untrennbar mit dem speziesistischen Selbstverständnis des Menschen verbunden ist: Es macht die Menschheit als solche aus, Technologien entwickeln und beherrschen gelernt zu haben. Über diese grundlegende Feststellung hinaus ist einem Großteil von Technologiedefinitionen gemein, dass sie Prozesse des Herstellens von Dingen, Wissenstypen zur Herstellung von Dingen oder die tatsächlich hergestellten Dinge umfassen. Zumeist wird Technologie jedoch mit einer praxisbezogenen Technik in Verbindung gebracht, die sich durch drei zentrale Elemente auszeichnet: Sie ist auf die Manipulation von Materie bezogen, hat eine Basis in der Ausnutzung naturwissenschaftlicher Erkenntnisse und ist auf die Erreichung praktischer Zwecke gerichtet.[242] Allerdings bleibt der von solchen Begriffsversuchen

241 Siehe dazu und zum Folgenden – freilich in anderem Kontext – bereits *Butz/Höffler* in Rüdiger/Bayerl (Hrsg.), Handbuch Cyberkriminologie 2, 427.

242 Siehe dazu ebenfalls in kriminalwissenschaftlichem Kontext *Brey* in Michael McGuire/Holt (Hrsg.), The Routledge handbook of technology, crime and justice, 17 (19).

erfasste Wirklichkeitsbereich sehr weit. Denn auch wenn es sich bei den Produkten der technologischen Entwicklung zwar nur um zwei grundlegende Typen handelt – einerseits Objekte (Werkzeuge, Geräte, Systeme) und andererseits Instruktionen für die Durchführung von Prozessen (Verfahren, Methoden) – erfassen diese beinahe alles Menschengemachte.[243]

Aufschlussreicher erscheint vor dem Hintergrund des Untersuchungszwecks die unter anderem von *McLuhan* propagierte Extensionstheorie[244], die davon ausgeht, dass technologische Artefakte als Mittel verstanden werden können, die auf den Fähigkeiten des menschlichen Körpers und Geistes aufbauen und diese erweitern und damit als Erweiterungen, als technologische Extensionen, des menschlichen Organismus fungieren.[245] Allerdings erscheint eine strikte Fokussierung auf den Menschen als Entität zu verengt, da Mensch-Objekt-Umwelt-Interaktionen so nur begrenzt miteinbezogen werden können. Denn jedes technologische Artefakt oder jede technologische Extension erweitert nicht nur die Möglichkeiten, die einem Individuum aufgrund seiner Fähigkeiten zur Verfügung stehen, sondern kann vielmehr als Erweiterung der Interaktionsmöglichkeiten zwischen den menschlichen Fähigkeiten und den Umweltelementen gesehen werden. Damit hängen die Möglichkeitsräume, die von einer Technologie für eine Person eröffnet werden, von ihrer zusätzlichen Funktionalität im Verhältnis zu den bereits verfügbaren Mitteln, zu Fähigkeiten und den Intentionen einer Person ab. Insofern entsteht ein multipolares Netzwerk zwischen einem technologischen Artefakt und verschiedenen interaktionsfähigen Knoten wie etwa Menschen und Tieren, natürlichen Objekten und Strukturen, sozialen Konventionen und Verfahren, sozialen und organisatorischen Strukturen sowie erworbenem Wissen und Fähigkeiten. Bei jeder Betrachtung der Funktion eines technologischen Artefakts für eine Person kann also berücksichtigt werden, wie es zu all diesen Mitteln und Verhältnissen beiträgt.[246] Diese amorphe Netzwerkstruktur mit zahllosen Knotenpunkten lässt sich grundsätzlich nur theoretisch umfassend beschreiben. Bereits der Versuch die technologischen Artefakte, von denen Polizeibeamt:innen während ihrer Tätigkeit umgeben sind, wie beispielsweise das Auto, eini-

243 *Brey* in Michael McGuire/Holt (Hrsg.), The Routledge handbook of technology, crime and justice, 17 (20).

244 *McLuhan,* Understanding media.

245 *Brey* in Michael McGuire/Holt (Hrsg.), The Routledge handbook of technology, crime and justice, 17 (22).

246 *Brey* in Michael McGuire/Holt (Hrsg.), The Routledge handbook of technology, crime and justice, 17 (24).

germaßen erschöpfend in ihren Beziehungsgeflechten und Wirkungen darzulegen, ist ein anspruchsvolles Unterfangen.[247] Hieran werden die enorme Komplexität sowie die Kontingenz menschlicher Technologie-Entwicklung und -nutzung deutlich. Wie Technologien zustande kommen und wirksam werden ist vor diesem Hintergrund keinesfalls vorherbestimmt, sondern hängt von einer Vielzahl zusätzlicher, ebenfalls nicht determinierten Faktoren, wie sozialen Konventionen und Strukturen, ab.[248]

Dieses Kontingenzpotenzial von Technologie einzufangen und aufzuschlüsseln, ist unter anderem ein Anliegen des Konzepts der Sozio-Technizität aus den *Science and Technology Studies*. Das Konzept geht von der Sozialgebundenheit aller technischen Artefakte aus, lehnt mithin eine strikte Trennung zwischen Technik und Sozialität ab, sodass aus soziologischer Perspektive stets genau zu untersuchen ist, welche Effekte eine Technologie nach Einbindung in das soziale Gewebe zeigt.[249] Aus dieser Perspektive ist das Interaktionsfeld zwischen Technologie und Gesellschaft vor allem ein Raum gleichzeitiger, einander beeinflussender Evolution.[250] Insofern materialisieren Technologien sich innerhalb der Gesellschaft durch vielfältige Verbindungen und Interaktionen mit der Umwelt. Das bedeutet einerseits eine gewisse Komplexität und Unübersichtlichkeit des sozio-technologischen Feldes, lehnt aber andererseits unterkomplexe Vorstellungen und Aussagen, etwa über die Fähigkeiten von Technologien im Sinne eines Solutionismus[251] sowie die Idee des technologischen Determinismus, kategorisch ab. Zwar gibt es technologische Pfadabhängigkeiten, aber die weiteren Entwicklungsverläufe sind offen und hängen von einer Fülle nicht-technologischer Faktoren – etwa rechtlicher, politischer, wirtschaftlicher, et cetera – ab.[252]

---

247 Ein Beispiel wäre *Seo,* Policing the open road, die polizeipraktische und (verfassungs-)rechtliche Implikationen der zunehmenden gesellschaftlichen Automobilisierung in den Vereinigten Staaten nachzeichnet.

248 Dazu auch *Nelson,* Geeks bearing gifts, S. 196, der davon spricht, dass der deterministische Nimbus des Technologie-Begriffes, die "fights and alternatives" verhüllt.

249 *Law* The Sociological Review 38 (1990), 1; siehe dazu auch Jasanoff in *Jasanoff/Kim* (Hrsg.), Dreamscapes of modernity, S. 2: "Bringing social thickness and complexity back into the appreciation of technological systems has been a central aim of the feld of science and technology studies".

250 *Latour* The Sociological Review 38 (1990), 103 (117).

251 Solutionismus meint die Idee, soziale Probleme schlicht mit (rein) technologischen Lösungskonzepten angehen zu können, siehe dazu *Morozov,* To save everything, click here.

252 *Egbert/Leese,* Criminal futures, S. 53 f.

Die Perspektive, die das Konzept der Sozio-Technizität ermöglicht, ist auch für das Verhältnis von Polizei und (Informations-)Technologie zentral. Im Kontext der Polizei sind vor allem die kriminogenen und kriminalpräventiven Potenziale technologischer Extensionen von Interesse. Wendet man sich den kriminogenen Potenzialen des Technologie-Einsatzes zu, so tut sich aufgrund der multipolaren Wechselwirkungen zwischen Technologie und Sozialsphäre ein weites Feld auf. Das gilt umso mehr, als in den technologisierten Gesellschaften der Spätmoderne technische Artefakte in alle Bereiche der Lebenswelt vorgedrungen sind. Dabei ist nicht nur die Saturierung der Umwelt mit Technologie, sondern auch ihre Wandlungsfähigkeit enorm und wenn auch Technologie selbst nicht determiniert ist, so scheint doch ihr Wandel eine der immerwährenden Konstanten zu sein, die geradezu notwendig für das Fortbestehen der Gesellschaft ist.[253] Insofern existieren zahllose Möglichkeiten für Delinquenz auf der Grundlage von Technologie-Interaktionen. Zudem evolvieren diese Kriminalitätsrisiken fortwährend durch die ständige technologische Innovation. Zusätzlich zu den Veränderungen in der Technologie selbst, treiben technikinduzierte Wandlungsprozesse auf der Makroebene, gegenwärtig insbesondere die Digitalisierung, auch soziale Umwälzungen an, die wiederum in Wechselwirkung miteinander ständig neue Risikoräume öffnen, in denen sich kriminelles Verhalten materialisieren kann.[254]

Auf diese kriminogenen Potenziale muss die Polizei reagieren – das ist einerseits Teil ihres Selbstverständnisses,[255] andererseits aber auch ein kriminalpolitisch prinzipiell sinnvolles Anliegen, denn

> „[w]hat one sees in countries in which crime is rampant is that criminals have won the arms race between criminals and law enforcement: they have the best technologies, modes of organization, information, training for skills, and other extensions. This, however, is not to say that systemic corruption, social deprivation, or high levels of inequality might not also contribute to high crime societies."[256]

253 Siehe zu diesem systemtheoretischen Grundgedanken etwa *August,* Technologisches Regieren, S. 150 ff.

254 *Ekblom* in Michael McGuire/Holt (Hrsg.), The Routledge handbook of technology, crime and justice, 353 (363 f.).

255 Siehe dazu unten S. 470 ff.

256 *Brey* in Michael McGuire/Holt (Hrsg.), The Routledge handbook of technology, crime and justice, 17 (30).

Allerdings wird diese polizeiliche Reaktion zumeist verzögert erfolgen. Ähnlich wie beim sog. *cultural lag*[257] gerät die Kriminalitätskontrolle aufgrund von technischen Anpassungsverzögerungen ins Hintertreffen, wenn kriminalpräventive Technologien nicht oder nicht schnell genug für sich auftuende Lücken in der Kriminalitätskontrolle entwickelt werden können. In der Sprache der Extensionstheorie geht es polizeilichen Akteur:innen insofern darum, die kriminogenen technologischen Extensionen einzuschränken oder ihre Wirkung durch eine Vergrößerung der kriminalpräventiven technologischen Extensionen zu neutralisieren. Freilich sind die Ausweitungen von kriminalpräventiven Extensionen keineswegs nur Antworten auf ein technologisches Aufrüsten von Delinquent:innen, etwa wenn spezielle technische Reaktionen auf Cyberkriminalität entwickelt werden. Vielmehr verläuft die Expansionslinie kriminalpräventiver Extensionen häufig in Bereichen, in denen abweichendes Verhalten nicht untrennbar mit Technologie verwoben ist. Beispielsweise ist die videokameragestützte Überwachung öffentlicher Räume kein Teil einer technologischen Aufholstrategie der Polizei. Vielmehr wird hier der Ausbau kriminalpräventiver Technologien betrieben, um herkömmliche Kriminalitätsformen besser adressieren zu können. Ähnliches lässt sich auch für die Nutzbarmachung von Massendaten durch die polizeiliche Informationsarchitektur feststellen. Zwar gibt es auch hier stellenweise externen Innovationsdruck in Form von Verfahren mit händisch nicht mehr zu verarbeitenden Daten. Generell betrachtet ist Massendatenverarbeitungstechnologie allerdings eine Extension von Wahrnehmung und Wissensproduktion, also der polizeilichen Kognition, die erhebliche kriminalpräventive Potenziale für die Reaktion auf Kriminalität im Allgemeinen mit sich bringen kann.

Für eine Systematisierung kriminalpräventiver technologischer Extensionen, lässt sich eine Einteilung *Breys* heranziehen, der zunächst in zwei Zweige teilt: Es existieren Technologien der Kriminalitätsverhütung und der Strafdurchsetzung. Für die Kriminalitätsverhütung kann man weiter unterteilen: So gibt es etwa informationstechnologische Artefakte, wie Datenbanken[258], die den Akteur:innen der Kriminalitätskontrolle aufzeigen, welche Deliktsziele, welche (potenziellen) Delinquenten und welche (illegalen) Mittel zur Deliktsbegehung in welchen Konstellationen potenziell relevant sind und dadurch eine bessere Ressourcenallokation ermöglichen.

257 *Ogburn,* Social change with respect to culture an original nature.
258 Zur Technologie der Datenbank siehe sogleich.

Daneben bestehen Überwachungstechnologien sowie technologische Artefakte, die Kriminalität durch Sicherung von Deliktszielen erschweren. Den Technologien der Strafdurchsetzung unterfallen hingegen Instrumente, die dem Aufspüren, der Verarbeitung und Zuordnung von Beweismitteln dienen, außerdem solche zur Lokalisierung, gegebenenfalls zur Festnahme und zur effektiven Vernehmung von Verdächtigen und Zeugen.[259] In beiden Zweigen sind Informationstechnologien zwar nicht absolut vorrangig, aber doch von entscheidender Rolle, wie es auch als Grundannahme für die vorliegende Untersuchung dient. Im Folgenden sollen daher die im Rahmen des polizeilichen Informationswesens wichtigsten Gattungen polizeilicher Informationstechnologien, denen insbesondere für die Massendatenverarbeitung eine zentrale Rolle zukommt, erläutert werden. Dabei handelt es sich um Datenbanken, Algorithmen und Informationssysteme.

I. Datenbanken

Datenbanken gelten als paradigmatische Medieninfrastruktur der Gegenwart,[260] auch wenn sie im Diskurs über informationstechnologische Entwicklungen nicht immer die größte Aufmerksamkeit bekommen. Die Datenbank als technologischer Begriff ist untrennbar mit dem Computerzeitalter[261] verknüpft. Die zunehmende Technisierung von Informationsverarbeitung führt – ohne dass sich das an einem genauen Zeitpunkt festmachen ließe – seit der Mitte des vergangenen Jahrhunderts zu medialen Transfor-

259 *Brey* in Michael McGuire/Holt (Hrsg.), The Routledge handbook of technology, crime and justice, 17 (29).

260 *Manovich* Convergence 5 (1999), 80; *Burkhardt,* Digitale Datenbanken, S. 24.

261 Der Begriff des Computers und seine medialen Besonderheiten können hier nicht näher erläutert werden. Es sei insoweit auf die Ausführungen von *Burkhardt,* Digitale Datenbanken, S. 73 verwiesen: „Ihr Zweck besteht darin, offen für Zwecke zu sein, die ihnen in Form von Programmen gegeben werden. Im programmierenden Gebrauch eröffnen Computer einen nahezu universellen Möglichkeitsraum optionaler Funktionen. Als programmierte Maschinen sind Computer hingegen stets auf spezifsche Funktionalitäten und Gebrauchsformen festgelegt, welche die medialen Praktiken mit Computern rahmen. Doch auch auf dieser Ebene des gebrauchenden Umgangs eröffnen sie einen Möglichkeitsraum vielfältiger Handlungsoptionen zur Artikulation, Handhabung, Verarbeitung und Distribution medialer Konstellationen. Hierin besteht eine, wenn nicht sogar die Herausforderung für das medientheoretische Denken über Computer. Sie entziehen sich nicht nur einer eindeutigen Funktionszuschreibung, vielmehr kann nahezu alles, was mit, durch und in Computern getan wird, auf unterschiedliche Weise getan werden."

mationsprozessen, die zur Konstruktion von technologischen Instrumenten führten, die computerlesbar waren, wie etwa die frühen Lochkarten der 1950er Jahre oder Index-Systeme in Bibliotheken ab Mitte der 1960er Jahre.[262] Erst in dieser Zeit entwickelt sich auch der Begriff der Datenbank[263] für diese Apparaturen:

> „Around 1964 a new term appeared in the computer literature to denote a new concept. The term was ›data base‹, and it was coined by workers in military information systems to denote collections of data shared by end-users of time-sharing computer systems. The commercial data processing world at the time was in the throes of ›integrated data processing,‹ and quickly appropriated ›data base‹ to denote the data collection which results from consolidating the data requirements of individual applications. Since that time, the term and the concept have become firmly entrenched in the computer world."[264]

In dieser „Computerwelt", insbesondere der Informatik, haben sich seitdem verschiedene, einigermaßen konsensuale Datenbankverständnisse herausgebildet. Datenbanken werden hier als Sammlungen von Daten bzw. Informationen verstanden, die von speziellen Softwareanwendungen, sogenannten Datenbankmanagementsystemen, verwaltet werden.[265] Dies darf indessen nicht darüber hinwegtäuschen, dass es weder *den* Datenbankbegriff noch *die* Datenbank gibt. Vielmehr herrscht hier eine gewisse Kontingenz, die stark von den Datenformaten abhängt. Neben der grundlegenden Bedeutung von Formaten für (digitale) Daten selbst,[266] sind Datenformate auch für Datenbanken strukturbildend:

---

262 *Neufeld/Cornog* J. Am. Soc. Inf. Sci. 37 (1986), 183 (183).

263 Während im deutschen Sprachgebrauch fast ausschließlich mit dem Begriff der Datenbank operiert wird, ist im Englischen der Begriff der data base gebräuchlicher. Der Unterschied, der sich daraus für die Bedeutungen ergibt, sollte nicht unterschätzt werden. Während mit Datenbank auf Banken als schützende und aufbewahrende Institutionen verwiesen wird, ist mit der Datenbasis ein Fundament oder eine Grundlage aus Daten angesprochen. Während erstere stärker auf eine materiell-technische Infrastruktur sowie einen durchaus auch ökonomischen Kontext anspielt, ist letztere eher eine konkrete Sammlung von Informationen selbst, die als Grundlage für etwas dienen, vgl. *Burkhardt,* Digitale Datenbanken, S. 129.

264 *McGee* IBM J. Res. & Dev. 25 (1981), 505.

265 Siehe dazu die Nachweise bei *Burkhardt,* Digitale Datenbanken, S. 121.

266 Vgl. *Krajewski* in Gugerli/Hagner/Hampe ua (Hrsg.), Nach Feierabend, 37 (37): "Daten erfordern Formate".

> „Das Format kanalisiert die Datenströme und bestimmt dementsprechend die Hegung, Bändigung oder Kontrolle der zu speichernden, zu übertragenden oder zu verarbeitenden Informationen. Mit anderen Worten, das Format determiniert nicht nur die Struktur der Datenprozessierung, sondern den Funktionsmodus des Mediums selbst."[267]

Datenbanken sind mithin vielgestaltig. In Kontrast dazu hat sich jedoch ein Begriffsverständnis herausgebildet, in dem Datenbanken vor allem Projektionsfläche sind und in dem die Kontingenz ihrer Form und auch Funktionalität von einer homogenisierenden Bedeutungszuschreibung überdeckt wird. In dieser Lesart erscheinen Datenbanken als neue Iterationen des Verlangens der Menschheit nach vollkommenem Wissen – wie es bereits in der (utopischen) Universalbibliothek zum Ausdruck kommt.[268] In ihnen verdichtet sich erneut die Hoffnung, „that all relevant information, whether internal or external, past or future, economic or human, could be accommodated within a single structure."[269] Dieses Verlangen ist als Imagination stark mit der Datenbank als Technologie verzahnt. Im dadurch geöffneten Möglichkeitsraum erscheint nicht nur die Speicherung aller möglichen Informationen denkbar, sondern auch ihre universelle Verwendung.[270] Die „grenzenlosen Möglichkeiten der Verzeichnung, Zirkulation, Präsentation, Selektion und Auswertung von Informationen in Computern" bleiben aber Imagination, die sich freilich als so stark erweist, dass sie mitunter die „Realität der computertechnischen Informationsverarbeitung" verhüllt.[271]

Um die Freilegung dieser Realitäten hat sich im deutschsprachigen Diskurs in letzter Zeit vor allem *Burkhardt* bemüht, der eine instruktive Theorie digitaler Datenbanken vorgelegt hat. Danach sind die konkreten medientechnischen Verfahren der Versammlung, Verwaltung und Verarbeitung digitaler Daten maßgeblich für eine treffende Auseinandersetzung mit Datenbanken, um zu verhindern, dass „die heterogene Vielgestaltigkeit der digitalen Datenbankkultur hinter der vermeintlichen Einheit der Datenbank als symbolischer Form" verschwindet.[272] Zentral ist somit die These, dass sich hinter dem Datenbankbegriff ein facettenreiches Tableau verschiedener Informationstechnologien sowie heterogener Praktiken im Umgang

267 *Krajewski* in Gugerli/Hagner/Hampe ua (Hrsg.), Nach Feierabend, 37 (38).
268 *Borges,* Die Bibliothek von Babel.
269 *Haigh* SIGMOD Rec. 35 (2006), 33 (34).
270 *Burkhardt,* Digitale Datenbanken, S. 149.
271 *Burkhardt,* Digitale Datenbanken, S. 10.
272 *Burkhardt,* Digitale Datenbanken, S. 9 f.

mit digitalen Informationssammlungen verbergen, die in ihren jeweiligen Eigenheiten in den Blick zu nehmen sind.[273] Auch wenn *Burkhardt* insofern davon ausgeht, dass Datenbanken sich nicht unter eine einheitliche mediale Logik bringen lassen,[274] lassen sich dennoch Regelmäßigkeiten ausmachen.

Während sich einerseits nach den Formaten der Inhalte von Datenbanken unterscheiden lässt – eine DNA-Profil-Datenbank ist anders strukturiert als eine reine Bilddatenbank – lässt sich vor allem auch fragen, wie die enthaltenen Daten verwaltet und verarbeitet werden. Neben einer reinen Speicherung oder Aufbewahrung von Daten sind Datenbanken immer mehr auch Basis für die Generierung von neuen Informationen durch entsprechende Verarbeitungsverfahren. Die Datenbank verliert damit ihre eher statische Natur als Bestand von bereits Bekanntem und wird mittels Kombination und Rekombination von Informationen zu einem Instrument für kreative Wissensproduktion, sodass „digitale Datenbanken unter Umständen etwas wissen lassen [können], was so noch nicht gewusst, was allenfalls latent und rein virtuell als potentielle Information vorhanden war."[275] Ähnliches hat bereits *Lyotard* weitsichtig vor 50 Jahren für die postmoderne Wissensproduktion festgestellt: In einer informationssaturierten Welt triumphieren diejenigen, die in ihrer Datenumgebung neue Einsichten durch Rekombination des Vorhandenen generieren können.[276] Um hierbei die bestmöglichen Ergebnisse zu erzielen, ist jedoch stets ein Bemühen um die Erhaltung einer möglichst hohen Informationskonzentration erforderlich. Mit anderen Worten müssen Datenbanken immer möglichst umfassend sein, damit sich vielfältige Verknüpfungsmöglichkeiten und damit Wissenspotenziale auftun, was wiederum zu Orientierungslosigkeit bei denjenigen führen kann, die mit der Menge an Daten nicht umgehen können. *Burkhardt* führt insoweit treffend aus, dass Datenbanken „als Reaktion auf einen Information Overload begreifen [lassen] und zugleich als Resultat eines Begehrens von immer mehr Informationen. Unsere Medienkultur ist folglich geprägt von einem Informationsüberschuss bei gleichzeitigem Informationsmangel."[277]

Doch auch hier schimmert wieder das imaginäre, projizierende Potenzial der Datenbank-Technologie durch. Denn Grundlagen und Grenzen

273 *Burkhardt,* Digitale Datenbanken, S. 17.
274 *Burkhardt,* Digitale Datenbanken, S. 331.
275 *Burkhardt,* Digitale Datenbanken, S. 183.
276 *Lyotard,* The postmodern condition, S. 51 f.
277 *Burkhardt,* Digitale Datenbanken, S. 147.

der ergebnisoffenen Wissensproduktion sind weiterhin dadurch bestimmt, welche Daten in der Datenbank überhaupt enthalten sind oder enthalten sein können sowie welche Datenverarbeitungsprozesse die technische Gestaltung der Datenbank überhaupt erlaubt. Diese Heterogenität von Datenbanken, mit denen neuerdings immer häufiger durch interaktive Datenverarbeitungspraktiken Wissen generiert werden kann, ermöglicht eine Pluralität von Wissensordnungen. So entsteht eine digitale Umwelt mit Informationsinfrastrukturen, „die auf unterschiedlichen Niveaus ansetzen, verschiedenen Logiken erfolgen und auf unterschiedliche Weise an bestehende Ordnungen anschließen."[278] Auch hier stellen sich vielfältige Fragen der Kopplung solcher Ordnungen und Übersetzung zwischen ihnen – im polizeilichen Kontext könnte man sich etwa fragen, wie die Übertragung von Daten aus Online-Steifen in sozialen Netzwerken in die Logiken der polizeilichen Datenbanken bewerkstelligt wird oder auch – ganz grundlegend – wie Beamt:innen lebensweltliche Sachverhalte in digitale Daten übersetzen und damit für die Aufnahme in eine bestimmte Datenbank anpassen.

Im Zuge dieser Koppelungsmöglichkeiten zwischen unterschiedlichen datenbankbasierten Wissensordnungen stellt sich zudem die Frage, wie mittels der Kombination von unterschiedlichen Datenbanken neues Wissen produziert werden kann. Neben dem, was innerhalb eines Datenspeichers „so noch nicht gewusst, was allenfalls latent und rein virtuell als potentielle Information vorhanden war",[279] potenzieren sich die Möglichkeiten der Wissensproduktion mittels Kombination von in technisch abgegrenzten Datenbanken manifestierten Wissensordnungen. Das betrifft einerseits die polizeiinternen Datenbanken selbst, die über informationstechnologische Verknüpfungs- und Analyseverfahren wie die hessenDATA-Plattform verkoppelt werden.[280] Darüber hinaus entsteht über die – zumindest theoretisch und scheinbar auch praktisch mögliche – Verkoppelung von polizeiinternen und polizeiexternen Datenbeständen die Möglichkeit,[281] für eine tiefergehende Produktion von Wissen über gesellschaftliche Prozesse, etwa wenn die Datenbanken sozialer Netzwerke mit in den Pool von kombinationsfähigen Daten einbezogen werden. Durch die zwar nicht un-

278 *Burkhardt,* Digitale Datenbanken, S. 113.
279 *Burkhardt,* Digitale Datenbanken, S. 307.
280 Siehe dazu näher unten S. 281 ff.
281 So auch etwa *Leman-Langlois* in Deflem (Hrsg.), The Handbook of Social Control, 347 (351).

begrenzten, aber durch ihre rechtlichen Befugnisse schon weitreichenden Zugriffsmöglichkeiten auf polizeiexterne Datenbestände entsteht so für die Polizei eine Art virtueller Informationsspeicher jenseits der eigenen Datenbanken.[282] Auch angesichts dieser vielfältigen Kopplungsmöglichkeiten von Datenbeständen könnte wieder die Imagination der Vollständigkeit der dadurch entstehenden Informationsspeicher wirkmächtig werden. Wenn schon nicht alle denkbaren Daten enthalten sind, dann doch vielleicht alle relevanten Daten. Hier kann freilich auf die bereits erläuterte Konstruiertheit von Daten verwiesen werden.[283] Was als relevantes Datum gilt, ist nicht objektiv bestimmbar, sondern bleibt Ergebnis eines Aushandlungsprozesses. Trotz der vielfältigen Ansatzpunkte für Wissensproduktion, die sich aus der Vernetzung von Datenbeständen ergeben, bleibt die dadurch konstruierte Wirklichkeit eben genau das: eine Konstruktion.[284] Die Grenzen der Datenbank(en) sind also gerade nicht die Grenzen der Wirklichkeit, auch wenn sie zunächst so wahr- und hingenommen werden mögen. Vor diesem Hintergrund ist *Burkhardt* beizupflichten, wenn er eine reflexive Auseinandersetzung mit der Datenbankpraxis fordert, „welche sich von der beschriebenen Tendenz zur Universalisierung emanzipiert, indem sie die vielfältigen Grenzen aufzeigt, die dem Versuch, alle Informationen in digitaler Form zu versammeln, stets gesetzt sind", damit ihre „technische, soziale und historische Begrenztheit erfahr- und handhabbar" bleibt.[285]

Das lässt sich auch auf das polizeiliche Informationswesen und die in ihm bestehende Datenbankenpraxis übertragen und bedeutet hierfür im Wesentlichen zweierlei: Zum einen können polizeiliche Datenbestände nie universell sein, sie enthalten also nur ein beschränktes Abbild der Realität, sodass auch die Rekombination von in ihnen enthaltenen Daten immer ein ungenaues, weil unvollständiges, Bild der Wirklichkeit zeichnen wird. Diese Limitierung der Datenbank als Instrument der Wissensproduktion gilt es zu reflektieren. Andererseits kann die Erforschung des polizeilichen Informationswesens mit seinen vielfältigen Datenbankpraktiken[286] vor dem Hintergrund der Heterogenität von Datenbanken als informationstechnologisches Phänomen nicht mittels einer singulären Perspektive auf *die* Datenbank erfolgen. Vielmehr müssen die vielfältigen Konfigurationen

282 Siehe dazu näher unten S. 314 ff.
283 Siehe dazu bereits oben S. 50 ff.
284 *Burkhardt,* Digitale Datenbanken, S. 235.
285 *Burkhardt,* Digitale Datenbanken, S. 335.
286 Siehe zu unterschiedlichen Datensammlungen der deutschen Polizeien etwa unten S. 230 ff.

verschiedener Datenbanken, wie sie sich etwa aus Datenformaten oder Informationszwecken und daran anknüpfenden Strukturierungen ergeben, sowie der darauf aufbauenden Interaktionspraktiken mit den jeweiligen Datenbanken in ihren Eigenheiten in den Blick genommen werden.

II. Algorithmen

Zentral für den Umgang mit in digitalen Datenbanken gespeicherten Daten ist die bereits erwähnte Technologie des Algorithmus, der technisch eine bestimmte Abfolge von logischen Operationen zur Erfüllung einer spezifischen Aufgabe meint. Durch einen Input wird der Algorithmus gestartet und verwandelt diesen dann in den (hoffentlich gewünschten) Output.[287] Im Kontext digitaler Datenbanken dienen verschiedene Algorithmen insofern dazu, Dateninputs in Outputs zu verwandeln, die als Informationen für Menschen nutzbar sind. Darunter fallen schon die recht simplen Suchalgorithmen in Online-Bibliothekskatalogen, die den Nutzer:innen etwa über lokale Verfügbarkeiten von Büchern informieren oder auch Kriminalaktennachweis-Systeme, die über die Auffindbarkeit von entsprechenden Kriminalakten Auskunft geben. Dabei handelt es sich allerdings nur um eine Übersetzungsmöglichkeit der Daten in Informationen, die sich aus der jeweiligen Struktur des Algorithmus ergibt. Durch die Wandlungsfähigkeit von Algorithmen enthält jede Datenbank darüber hinausgehende Potenziale, die man als virtuelle Informationen bezeichnen kann: „Virtual information is any fact which does not physically exist in the data base, but is nonetheless accessible through combinations of algorithms and other data."[288] Während *Folnius et al.* diese Konzeptualisierung bereits vor knapp 50 Jahren formulierten, ist die Realisierung der Potenziale von virtueller Information jünger, denn sie hängen ganz maßgeblich von der Evolution der Algorithmentechnologie ab. Die zunehmende Finesse und Leistungsfähigkeit von Algorithmen ist notwendige Bedingung für die gegenwärtigen Phänomene des Massendatenzeitalters. Denn Massendatenspeicherung ist letztlich schon länger eine informationstechnologische Praktik der Menschheit, auch wenn sich die Speichermedien in den letzten Jahren durchaus radikal gewandelt haben. Was sich aber in den letzten Jahren vor allem auch verändert hat, sind die Möglichkeiten, mittels algorithmisierter Datenverar-

287 *Barocas/Rosenblat/boyd* ua SSRN Journal 2014 (3).
288 *Folinus/Madnick/Schutzman* SIGMOD Rec. 6 (1974), 1 (1).

beitung neue – virtuelle – Informationen aus einem Datenbanksystem zu erhalten. Neue Terminologien wie das Data Mining[289] haben dem Algorithmus-Begriff für den Massendatendiskurs mit neuem Gehalt angereichert, sodass sich ein modifiziertes Verständnis etabliert hat: Algorithmen sind Prozesse, mit denen – zumeist unter Nutzung technischer Verfahren wie dem maschinellen Lernen oder anderer Formen künstlicher Intelligenz[290] – Computer automatisierte Aussagen oder sogar Entscheidungen über mögliche Zukünfte mithilfe eines großen Datensatzes treffen (können).[291]

Vor diesem Hintergrund erscheinen Informationssystem[292] und Datenbank aber in ihrer hergebrachten Nutzungsform – also insbesondere Speicherung von möglichst vielen Daten für Individualabfragen von einzelnen Datensätzen – bereits als anachronistisch. Automatisierte algorithmische Instrumente zur Entscheidungsunterstützung oder -findung und komplexe Datenanalyseverfahren sollen auch die informationellen Kapazitäten der Polizeien dynamisieren und in ihrer Aussagekraft intensivieren.[293] Dabei führt die Algorithmisierung der Wissensproduktion gegenwärtig häufig zu Situationen, in denen die Leistungsfähigkeit der neuen informationstechnologischen Verfahren als noch nicht völlig ausgereizt erscheint. Dies trifft auf Imaginationen der Universalisierung im Kontext von Datenbanken: Algorithmische Entscheidungssysteme bräuchten aus dieser Perspektive nur (noch) mehr Daten, um besser zu werden.[294] Dabei kann eine solche Expansionsstrategie schnell zu sich selbst verstärkende Feedbackschlaufen führen: Werden noch mehr Daten gesammelt, wird es für die menschliche Kognition noch unübersichtlicher, sodass eine stärkere Hinwendung zu Algorithmen erforderlich ist, deren kontinuierliche Verbesserung wiederum einen unablässigen Strom an neuen und bestenfalls qualitativ verbesserten

289 *Cios,* Data Mining.

290 Künstliche Intelligenz ist ein breites und bereits einige Jahrzehnte altes interdisziplinäres Forschungsfeld, in dessen Zentrum Computerwissenschaften und Informatik versuchen menschliche Intelligenz zu emulieren, regelmäßig zur Erfüllung bestimmter mehr oder weniger anspruchsvoller kognitiver Aufgaben, seltener zur Schaffung von Intelligenz selbst. Dafür wird eine Vielzahl von technischen Verfahren eingesetzt, die in der Regel auf die Verarbeitung von großen Datensätzen ausgelegt sind, in denen im weitesten Sinne Muster erkannt werden, die konkrete Entscheidungsfindungsprozesse optimieren. Siehe dazu das Einleitungskapitel des Standardwerks *Russell/Norvig,* Artificial Intelligence: A Modern Approach.

291 *Brayne,* Predict and surveil, S. 3.

292 Zur Technologie des Informationssystems sogleich im Anschluss.

293 *Završnik* in Završnik (Hrsg.), Big Data, Crime, and Social Control, 3 (7).

294 *Završnik* in Završnik (Hrsg.), Big Data, Crime, and Social Control, 3 (10)

Daten erfordert. Diese zunehmende technologische Komplexität der Datenverarbeitungsalgorithmen hat zu einer religiös-mythischen Charakterisierung dieser Techniken beigetragen, etwa wenn *Gillespie* davon spricht, dass Algorithmen Hieroglyphen produzierten, die einer priesterlichen Interpretation bedürften[295] und damit einen zwar sozial gewachsenen, aber in gewissem Maße willkürlichen Wissensproduktionsprozess impliziert.

Dieser Mystifizierung von Algorithmen als „undurchschaubare, orakelhafte" Macht[296] ist mit einem nüchterneren Analyserahmen entgegenzutreten. Ein solcher kann etwa zunächst daran anknüpfen, dass zwischen denjenigen, die die Algorithmen designen und denjenigen, die sie nutzen, eine Asymmetrie bestehen kann, die sich durch das unterschiedliche Wissen über die Wirkweisen der Algorithmen ergibt. Probleme ergeben sich hieraus, weil „die algorithmisch hergestellte Relevanzordnung kein objektives Bild der „wirklichen" Relevanz von Informationen ist."[297] Während sich dies etwa bei Algorithmen von Websuchmaschinen als Machtasymmetrie äußeren kann, ist im polizeilichen Kontext vor allem die dadurch bedingte Wissensasymmetrie bezüglich der Funktionsweisen von Algorithmen zwischen Polizeifachlichkeit und den Techniker:innen relevant, die sich etwa in der Überbewertung von Informationen durch erstere äußern kann. Insofern hängt die „richtige" Interpretation von Ergebnissen algorithmisch vermittelter Informationsanfragen an Datenbanken maßgeblich von Wissen über die Wirkweisen algorithmischer Prozesse im Hintergrund ab. Wendet man sich diesen Prozessen aufmerksamer zu, so zeigt sich eine „Vielfalt der algorithmisch gesteuerten Informationsverarbeitungsprozesse", die an die Stelle der algorithmischen Allmacht tritt.[298] Diese Vielfalt ist Ausdruck verschiedener Informationsbedürfnisse und -praktiken, deren Adäquanz für die jeweils zu erfüllenden Aufgaben variieren kann, insbesondere mit Blick auf das Anwachsen der gesellschaftlichen Datenspeicher. So erklären sich auch die – vor allem im Sicherheitsbereich – immer wieder auftretenden Fehler bei der Vorhersage von Ereignissen anhand von eigentlich bekannten Datenpunkten. Dies ist häufig nicht auf professionales Versagen der Sicherheitsbehörden zurückzuführen,

295 *Gillespie* in Gillespie/Boczkowski/Foot (Hrsg.), Media Technologies, 167 (190).
296 *Röhle,* Der Google-Komplex, S. 14.
297 *Burkhardt,* Digitale Datenbanken, S. 265.
298 *Burkhardt,* Digitale Datenbanken, S. 301 f.

> „sondern auch auf den Überschuss an Informationen, welcher die menschlichen Verarbeitungskapazitäten übersteigt und damit nur noch computergestützten Analysemethoden zugänglich ist. Diese Verfahren beruhen auf Algorithmen, die Informationsbestände gemäß bestimmter Regeln automatisch interpretieren. Hierauf gründen gleichermaßen die Chancen und Risiken der computergestützten Auswertung von Informationen. Algorithmen analysieren Informationssammlungen nach einem vorgegebenen Muster, wodurch diese in einen bestimmten Bedeutungskontext gestellt werden."[299]

Durch die Regelgebundenheit bleiben die Algorithmen immer ein stückweit begrenzt bei der Zusammenführung von Daten zu neuen virtuellen Informationen, die Menschen für die weitere Wissensproduktion und Handlungsorientierung dienen können. Einen Algorithmus, der ungebunden kreativ „outside the box" Daten verknüpfen und damit radikal neue Ansätze anbieten kann, gibt es (bisher) nicht.

Trotz dieser Zentralität von Algorithmen für die Realisierung der informationellen Potenziale von digitalen Daten ist mit der Gegenüberstellung von Datenbanken und Algorithmen der informationstechnologische Kern der menschlichen Bewältigung des Massendatenzeitalters noch nicht hinreichend erfasst. Die meisten Nutzer:innen der in Datenbanken gespeicherten Inhalten haben nicht die Fähigkeiten, direkt über die Programmierung von Algorithmen virtuelle Informationen aus den Daten zu gewinnen. Vielmehr müssen Datenbank und Algorithmus für die breite Nutzung noch miteinander verschaltet werden. Der Ort, an dem diese Verschaltung in einer bedienungsfreundlichen Art und Weise geschieht, ist das Informationssystem, das als letzter hier zu erläuternder Faktor die Informationspraktiken im Umgang mit Daten maßgeblich mit beeinflusst.[300]

III. Informationssysteme

Der Umgang mit Datenbanken ist wesentlich durch die Interaktionsmöglichkeiten strukturiert, die die entsprechenden Informationssysteme vorgeben. Spiegelbildlich zur Vision einer universellen Datenbank ist dabei auch die eines einheitlichen, universellen Informationssystems nur Imagination.

299 *Burkhardt,* Digitale Datenbanken, S. 313.
300 *Burkhardt,* Digitale Datenbanken, S. 281.

Vielmehr ist das Informationssystem im Theoretischen ähnlich zu fassen, wie es sich in seiner technisch konstruierten Manifestation zeigt: Informationssysteme unterscheiden sich in ihren Funktionalitäten und müssen anschlussfähig für die partikularen informationellen Praktiken verschiedener Gruppen und der von diesen verwalteten Datenbanken sein.[301] Anders als es die dem Informationsbegriff innewohnende Abstraktheit suggeriert, entstehen Information und Wissen immer kontextabhängig. Im Rahmen des breiten Umgangs mit den meisten digitalen Datenbanken ist es in erster Linie das Informationssystem, das den Möglichkeitsraum für die Umwandlung von losen Daten in Informationen schafft, also bestimmt „was als Information zur Erscheinung kommt, als solche adressiert, gesucht, gefunden und verarbeitet werden kann."[302] Auch im Rahmen der Technologie der Informationssysteme scheint die Imagination der Universalität immer wieder durch. So wie bereits die Datenbank häufig als umfassende Grundlage für Wissensproduktion gesehen wird, sind auch die Informationssysteme als Orte der Interaktion des Menschen mit den gespeicherten Daten Projektionsfläche für vielfältige Wunschkonstellationen. Trotz der limitierten Form und Funktion von Informationssystemen, die sich aus der konkreten technischen Ausgestaltung ergeben, treibt (auch) hier die Imagination nach umfassenderen Formen und Funktionalitäten die Innovation neuer technologischer Problemlösungsansätze an, die wiederum immer auch neue – technische, organisatorische, rechtliche – Problemen mit sich bringen.[303] So haben auch Informationssysteme als Teil der „Medienentwicklung in bestimmten Wunschstrukturen ihre Ursache" und sind damit mit der Verfolgung „impliziter Utopien" verbunden.[304] Diese Imaginationen, die auch im Bereich polizeiliche Informationsverarbeitung – etwa im Kontext von Predictive Policing – am Werk sind, überdecken mitunter die reale Leistungsfähigkeit der Informationssysteme, insbesondere „indem man die in diesen Systemen verwalteten Formen von Information universalisiert."[305] Die makellose Einfachheit dieser Vision steht indessen in auffälligem Kontrast zur verworrenen und partikularen Realität polizeilicher Informations-

301 *Burkhardt,* Digitale Datenbanken, S. 182.
302 *Burkhardt,* Digitale Datenbanken, S. 159.
303 *Burkhardt,* Digitale Datenbanken, S. 159.
304 *Winkler,* Docuverse, S. 17.
305 *Burkhardt,* Digitale Datenbanken, S. 166.

verarbeitung.[306] Vor diesem Hintergrund muss eine Untersuchung von Informationspraktiken und -architekturen versuchen,

> „die vielfältigen und unterschiedlichen Formen der computertechnischen Verarbeitung von Informationen freizulegen. Zu beschreiben sind partikulare Sofware-Hardware-Konfgurationen, die zwar nicht vorschreiben, welche Informationen in einem Informationssystem verarbeitet werden, aber was im Kontext eines solchen Systems als Information adressiert werden kann."[307]

Eine solche Analyse der Funktionsweisen eines Informationssystems ist insofern bedeutsam, weil die auf Grundlage der dort verarbeiteten Daten aktualisierte Information stets nur eine von vielen möglichen Materialisierung des in den Daten liegenden informationellen Gehalts ist.[308] Vor dem Hintergrund der kontingenten Strukturierung von Informationssystemen, öffnet sich ein Raum für Analyse und Hinterfragung ihrer jeweiligen Formen. Für die weitere Beschäftigung mit polizeilicher Informationsverarbeitung bedeutet dies zunächst, dass sich über die nähere Befassung mit den konzeptuellen Grundlagen von Informationssystemen ablesen lässt, wer konkret welche Befugnisse zum Datenumgang hat und welche informationelle Praktiken sich daraus ergeben können.[309]

Von Relevanz ist eine solche Analyse, weil polizeiliche Informationspraktiken zunehmend in technologische Umgebungen eingebettet sind, in denen eine informationssystemische Oberfläche zu bedienen ist – sei es über neue Wege, wie mobile Endgeräte, mittels derer Zugriff auf Datenbanken gewährt wird oder im Rahmen der schon länger genutzten, aber sich stetig weiterentwickelnden Auskunfts-, Auswertungs- und Analysesysteme wie die wichtigen Vorgangsbearbeitungssysteme.[310] Wegen der sozio-technischen Natur dieser Technologien beeinflussen nicht nur die technischen, sondern auch die menschlichen, organisatorischen, kulturellen, politischen, ethischen, rechtlichen und auch wirtschaftlichen Elemente den Einsatz.[311]

Diese vielfältigen Bedingungsverhältnisse erschweren generelle Aussagen über die konkreten Praktiken rund um die polizeilichen Informationssyste-

306 So generell für Informationsverarbeitung *Haigh* SIGMOD Rec. 35 (2006), 33 (44) Zu polizeilichen Informationssystemen siehe unter S. 226 ff.
307 *Burkhardt,* Digitale Datenbanken, S. 166.
308 *Burkhardt,* Digitale Datenbanken, S. 281.
309 *Burkhardt,* Digitale Datenbanken, S. 182.
310 Siehe dazu unten S. 254 ff.
311 *Egbert/Leese,* Criminal futures, S. 3; *Brayne,* Predict and surveil, S. 34 f.

me ein stückweit. Dennoch gibt es auch hier gewisse Grundformen der Datenverarbeitung, die durch die Struktur von Informationssystemen geformt werden. So dürften die meisten Systeme der Polizei klassischerweise noch mit der Query, der Suchanfrage an eine an das Informationssystem angeschlossene Datenbank über ein entsprechendes Interface, arbeiten. Damit ist der Datenumgang einigermaßen formalisiert und in seiner Reichweite begrenzt. Zudem müssen die Art, wie Suchanfragen formuliert werden, sowie spezielle Suchpraktiken beherrscht werden. Auch ist ein Verständnis für die Limitierungen der Technologien erforderlich. Werden keine Daten zu einem bestimmten Suchbegriff angezeigt, so kann es zwar sein, dass keine Daten vorliegen. Genauso kann es aber auch möglich sein, dass die Suchanfrage falsch geschrieben wurde. Umgekehrt kann auch im Trefferfall die Suchanfrage fehlerhaft gewesen sein, sodass eventuell Datenpunkte angezeigt werden, deren Abruf eigentlich gar nicht beabsichtigt war.[312] Mit verbesserten Datenauswertungstechniken wandeln sich aber auch die Interaktionsmöglichkeiten mit den Datenbeständen. Emblematisch für den Informationsumgang im Internet etwa ist das *Browsen*, bei dem kein Such-Interface mehr besteht, sondern Nutzer:innen in einem Informationsraum eigenständig navigieren können, sich aber gleichzeitig auch orientieren müssen.[313] Darunter fällt etwa „das Durchstöbern einer weitverzweigten Webseite nach bestimmten Informationen."[314] Eine weitere Flexibilisierung durchläuft der Informationsumgang mit der Praktik des *Streams*, bei der nach *Burkhardt* „das relativ ungezielte Entdecken von neuen […] Ressourcen in bestimmten Themengebieten […]" im Vordergrund steht.[315] Zwar ist diese Art der Interaktion mit Daten stark mit sozialen Medien und deren endloser Netzwerkstruktur verbunden, ist aber auch für polizeiliche Informationspraktiken bedeutsam. Einerseits findet ein zunehmender Teil des polizeilichen Arbeitsalltags im Internet und auch in sozialen Netzwerken statt (etwa in Form der Online-Streife[316]). Andererseits ist die Flexibilisierung der Interaktion mit den polizeieigenen Datenbeständen eine zu beobachtende Tendenz im polizeilichen Informationswesen, wo Anwendungen wie hessenDATA Informationspraktiken ermöglichen, die sich von der einfachen Suchanfrage wegbewegen und sich an das freie Navigieren

312 *Burkhardt,* Digitale Datenbanken, S. 298 ff.
313 *Baeza-Yates/Ribeiro-Neto,* Modern information retrieval, S. 4.
314 *Burkhardt,* Digitale Datenbanken, S. 30.
315 *Burkhardt,* Digitale Datenbanken, S. 304.
316 Siehe dazu unten S. 314 ff.

in Informationsräumen annähern.[317] Diese Evolution von Informationssystemen und darauf bezogenen (polizeilichen) Informationspraktiken hat viele Implikationen. So müssen etwa verschiedene Informationspraktiken und die stets dahinterstehenden Informationsbedürfnisse der unterschiedlichen Organisationseinheiten der Polizeien miteinander integriert werden, damit handlungsleitendes Wissen erzeugt und an den gewünschten Stellen wirksam werden kann.[318] An der Interaktion mit dem Informationssystem werden zudem am ehesten die Wirkungen eines sich verändernden Datenumgangs greifbar. Insofern erscheint diese Schnittstelle auch ein wichtiger Ort für die Rechtsordnung zu sein, da regulierende Impulse, die auf eine normative Steuerung von polizeilichen Informationspraktiken abzielen, an diesem Punkt Gestaltungspotenziale mit direkter Wirkung entfalten können.

E. Sozialkontrolle

Soziale Ordnung und Kontrolle sind in ihren zeit- und gesellschaftsgebundenen Ausprägungen notwendige Konstanten menschlichen Zusammenlebens und daher auch für moderne Gesellschaften unhintergehbar.[319] Die Art und Weise, wie Gesellschaften soziale Ordnung aufbauen, indem sie Normen ausbilden sowie durch Kontrolltechniken zu stabilisieren und durchzuhalten versuchen, ist ein fundamentaler Aspekt für jedes gesellschaftliche (Selbst-)Verständnis und Ausgangspunkt sowie Rahmen für die Entfaltung individueller und kollektiver menschlicher Möglichkeiten. Eingeführt im späten 19. Jahrhundert, diente das Konzept der Sozialkontrolle zur Erfassung der Gesamtheit der – staatlichen[320] wie privaten[321] – Institutionen, die die Grundlage für die soziale Ordnung in modernen Gesell-

317 Siehe zur Funktionsweise solcher Anwendungen unten S. 474 ff.

318 *Egbert/Leese,* Criminal futures, S. 4 f.

319 Siehe auch *R. Meier* in Deflem (Hrsg.), The Handbook of Social Control, 23 (24).

320 Darunter fallen etwa die Polizei, die Strafjustiz, Gefängnisse, aber auch andere, nicht mit Kriminalität im eigentlichen Sinne befasste Behörden und Institutionen wie Schulen, Arbeitsagenturen, die Gewerbeaufsicht und alle anderen, die Menschen in Richtung gewisser Normvorstellungen bewegen wollen bzw. sollen.

321 Die „Institutionen" der privaten Sozialkontrolle umfassen auf einer ersten Ebene vor allem den sozialen Nahbereich, wie die Familie und Freundeskreise, wobei die hier durchgesetzten Normen nicht zwangsläufig kongruent mit gesellschaftlichen Mehrheitsregeln sind. Daneben sind aber auch in der öffentlichen Sicherheitsproduktion private Akteure präsent, man denke etwa an private Sicherheitsfirmen oder zivilge-

schaften bilden, welche sich durch ein zunehmendes Maß an Individualismus und Vielfalt auszeichneten.[322] Seitdem hat sich das Begriffsverständnis verfeinert und ist heutzutage stärker an die Kontrolle von Normabweichungen geknüpft, und zwar sowohl von informellen Normen in relativ kleinen sozialen Kontexten als auch von immer stärker formalisierten Normen in großen Gesellschaften.[323] Gibt es zwar auch immer noch verschiedene Konzeptionen in der Theorielandschaft zur Sozialkontrolle,[324] wird hier ein Begriffsverständnis zugrunde gelegt, das seinen Schwerpunkt in erster Linie auf soziale Kontrolle in Bezug auf als Kriminalität definiertes abweichendes Verhalten legt, wobei ein solches kriminologisches Verständnis jedoch auch immer für seinen weiteren soziologischen Kontext empfänglich bleiben muss.[325] Dieses Verständnis steht in Durkheimscher Tradition, nach dem Sozialkontrolle vor allem die Funktion hat, Devianz entgegenzuwirken bzw. normenkonformes Verhalten zu befördern.[326]

In diesem kriminologischen Verständnis von Sozialkontrolle lassen sich wiederum drei unterschiedliche Konzeptionen der Kontrolle von delinquenten Normabweichungen ausmachen.[327] Aus der ätiologischen Perspektive, die nach den Ursachen von Kriminalität fragt, ist Sozialkontrolle vor allem eine funktionale Reaktion der Gesellschaft auf Kriminalität. Eine weitere Perspektive ist die konstruktivistische, in der Kriminologie vor allem als Etikettierungsansatz bekannt ist. Diese Perspektive schenkt der sozialen Kontrolle vor allem insoweit Aufmerksamkeit, als sie zu Kriminalisierungen in einem breiteren Prozess der Kennzeichnung von Abweichung führt. Zuletzt bauen noch konfliktsoziologische Perspektiven auf der konstruktivistischen Sichtweise auf, um soziale Kontrolle als Teil einer umfassenderen Untersuchung und Kritik der Gesellschaft und ihrer Machtstrukturen zu artikulieren. Mithilfe dieser drei unterschiedlichen Theorieansätze lassen sich sodann Institutionen und Praktiken untersuchen, die mit der Kontrolle von Devianz zu tun haben, wobei die Analyseebenen vom Level der Inter-

---

sellschaftlich organisierte Akteure, wie in der Bewährungshilfe, die gemeinsam mit staatlichen Akteuren soziale Ordnung produzieren.

322 *Deflem* in Deflem (Hrsg.), The Handbook of Social Control, 1 (1) mwN.

323 *Deflem* in Deflem (Hrsg.), The Handbook of Social Control, 1 (1).

324 Siehe etwa *Black,* Toward a General Theory of Social Control; *Cohen,* Visions of social control; *Gibbs,* A Theory About Control; *Janowitz* American Journal of Sociology 81 (1975), 82.

325 *Deflem* in Deflem (Hrsg.), The Handbook of Social Control, 1 (1).

326 *R. Meier* in Deflem (Hrsg.), The Handbook of Social Control, 23 (30).

327 Zum Folgenden siehe *Deflem* in Goode (Hrsg.), The Handbook of Deviance, 30.

aktion auf Mikroebene bis hin zu den Institutionen und ihren Vernetzungen auf Meso- und Makroebene reichen, die für die kriminalitätsbezogene formelle (d.h. staatliche) Sozialkontrolle zuständig sind, also allen voran Polizei und Strafjustiz.[328] Untersucht man, wie vorliegend, den Einfluss des Medienwandels auf Institutionen der Sozialkontrolle, so sind dabei zunächst die erste und zweite Konzeption relevant. Im Rahmen der ersten Konzeption kommt es einerseits durch einen Wandel der Kriminalität im Informationszeitalter – beispielsweise in Form dessen, was unter dem Begriff der „Cyberkriminalität" zusammengefasst wird – zu Wirkungen auf die (polizeiliche) Sozialkontrolle. Zudem erhöhen sich aber durch technische Fortschritte, wie beschrieben, auch das kriminalpräventive Potenzial und damit die Reaktionsmöglichkeiten der formellen Sozialkontrolle. Durch den zuvor beschriebenen Medienwandel mit seinen vielfältigen Implikationen für den menschlichen Zugang zur Welt ist zudem auch das konstruktivistische Verständnis der Sozialkontrolle angesprochen. Denn wie angeführt weist das Massendatenphänomen in bisher nicht dagewesener Prägnanz konstruktivistische Aspekte auf: Einerseits sind Daten immer konstruiert, andererseits ist datenbasiertes Wissen eine Konstruktion. Die informationstechnologische Entwicklung bringt insofern neue Prozesse der Kennzeichnung von abweichendem Verhalten, neue Formationen von „Verdächtigen-Identitäten"[329] (in und durch Daten) mit sich.

Von besonderer Bedeutung für die formelle soziale Kontrolle ist die Polizei, was sich am bekannten Trichtermodell veranschaulichen lässt.[330] Der nach unten hin schmaler werdende Trichter der bekannt gewordenen Straftaten beginnt mit der breitesten und damit zahlenmäßig bedeutendsten Stufe der polizeilich registrierten Fälle, die durch die Polizei selbst im Wege der Aufklärung und die weiteren Akteure der Strafjustiz nach unten hin ausgedünnt werden. Dabei ist auch die Rolle der Bevölkerung nicht zu vernachlässigen, die je nach Anzeigebereitschaft einen erheblichen Einfluss auf den Umfang der bekannt gewordenen Normabweichungen hat.[331] Nichtdestotrotz bleibt die Polizei aufgrund ihrer Definitionsmacht und der faktischen Allein- oder Hauptverantwortlichkeit für die zu führenden Ermittlungen der primäre Filter, den Informationen über abweichendes

328 *Deflem* in Deflem (Hrsg.), The Handbook of Social Control, 1 (2), auch mwN für Anwendungsbeispiele der Theorieperspektiven.
329 *Cole,* Suspect Identities.
330 Siehe etwa *Kunz/Singelnstein,* Kriminologie, S. 254.
331 *Kunz/Singelnstein,* Kriminologie, S. 254.

Verhalten aus der Gesellschaft in das strafjustizielle System der Sozialkontrolle hinein zu passieren haben.[332]

Im Zentrum der gesellschaftlichen Sozialkontrolle der Gegenwart lässt sich die moderne Polizei seit ihrer Entstehung verorten.[333] Der Wandel von sozialen Konstellationen in den Städten des beginnenden Industriezeitalters brachten ab dem 17. und 18. Jahrhundert neue soziale Unordnungsphänome hervor, für deren Ordnung und Kontrolle sich im Laufe des 18. und 19. Jahrhunderts mit der modernen Polizei eine Institution herausbildete, deren organisationales Charakteristikum ein stetiger Prozess der Technisierung und Professionalisierung ist. Nach wie vor besetzt die Polizei ihre zentrale Position in der gesellschaftlichen Sozialkontrolle, allerdings unterliegt sie seit ihrem Aufkommen als institutionalisierte Kontrolltechnik ausdifferenzierter Gesellschaften einem Wandel, der von den Wechselwirkungen mit sozialen (Un-)Ordnungsphänomenen abhängt.[334]

Bereits *Ross*, dem gemeinhin die Einführung des Sozialkontrolle-Konzepts zugeschrieben wird, hatte für das Phänomen der sozialen Kontrolle festgestellt, dass es einem stetigen Wandel unterliegt: Im Zeitverlauf verändern sich die Arten von Sozialkontrolle und ihre Grade nehmen zu und ab. Stabilität und Wandel sind mithin zentrale Dynamiken für die verschiedenen Formen von Kontrolle. Vereinfacht ließe sich sagen, dass eine instabile Sozialordnung den Bedarf an Sozialkontrolle steigen lässt, während in stabilen Sozialordnungen das Verlangen nach individueller Freiheit und Toleranz für Normabweichungen zunehmen,[335] wobei das keineswegs die tatsächliche Entwicklung sozialer Kontrolle beschreibt. So kann es in einer ohnehin nur schwach ausgeprägten sozialen Ordnung zu einer weiteren Erosion sozialer Kontrolle kommen und umgekehrt können gerade etablierte und beharrliche Sozialordnungen die Intensität ihrer Sozialkontrolle noch steigern. Mit Blick auf soziale Makrotrends wie Globalisierung und mehr noch Digitalisierung wird häufig eine Ablösung tradierter Gewissheiten und Ordnungen propagiert und auch die Dauerkrisenerfahrung der Spätmoderne ist ein Faktor, der intuitiv eher auf eine Instabilität der sozialen Ordnung(en) der Gegenwart hindeutet.[336] Auch wenn die Pauschalität dieser Aussagen wissenschaftlich etwas unbefriedigend ist, so

332 *Kunz/Singelnstein,* Kriminologie, S. 257 ff.
333 Siehe dazu ausführlicher unten S. 101 ff.
334 *Mulone* in Deflem (Hrsg.), The Handbook of Social Control, 207 (214 f.).
335 *Ross* American Journal of Sociology 6 (1901), 550 (550).
336 Gerade die hohe Veränderungsfähigkeit in der ausdifferenzierten Gesellschaft wird freilich aus Sicht der Systemtheorie zum Faktor für Stabilisierungsleistung im Sinne

ist daraus doch zumindest mit einiger Plausibilität abzuleiten, dass auch die Sozialkontrolle in derart transformativen Gesellschaften einem Wandlungsdruck unterliegt.

Dieser Wandel ergibt sich einerseits recht offensichtlich aus einer Evolution der Materie, deren Erhaltung die soziale Kontrolle dient: Normen. Das moralische Fundament moderner Gesellschaften ist spätestens seit der Mitte des vergangenen Jahrhunderts stark in Bewegung geraten und diese Tektonik hat das Abrutschen gewisser tradierter Normen zur Folge gehabt.[337] Andere Faktoren, die den gegenwärtigen Wandel der Sozialkontrolle antreiben, sind nicht ganz so einfach zu benennen, lassen sich aber wohl in ideologieinduziert und technologieinduziert aufteilen, ohne dass damit Vollständigkeit bezüglich der Erklärung der Wandlungsprozesse beansprucht wird.

Vor allem diejenigen Phänomene, die sich unter den Begriff der Reprivatisierung der Sozialkontrolle[338] fassen lassen, erscheinen in erster Linie ideologieinduziert, da sie als Ausgangspunkt häufig die neoliberale Idee eines schlanken Staates haben, der nur begrenzt für die Sicherheitsbedürfnisse von Individuum und Allgemeinheit aufkommen kann.[339] Aus dieser Perspektive nimmt die Bedeutung des Staates und insbesondere der Polizei im Zentrum der Sozialkontrolle ab, weil andere Akteure dort an Relevanz gewinnen. Die Polizei ist so nur ein Knotenpunkt in einem weitgespannten Netzwerk der Sozialkontrolle. Lediglich im Bereich des Staatsschutzes sind Staat und insbesondere die Polizei noch Inhaber ihrer Monopolstellung.[340] Während die Fassung solcher Formationen sozialer Kontrolle unter Begriffen wie etwa *nodal governance*[341] den Bruch mit Bisherigem implizieren, zeigt ein Blick in die jüngere Geschichte der gesellschaftlichen Ordnungs-

---

des Fortbestandes von Systemen, siehe etwa *Luhmann* Zeitschrift für Soziologie 6 (1977), 62.

337 Siehe zu dieser Dynamik etwa *R. Meier* in Deflem (Hrsg.), The Handbook of Social Control, 23 (33).

338 Die Reprivatisierung der Sozialkontrolle meint die – zumindest für eine Zeit – zunehmend zu beobachtende Übertragung auf bzw. Beteiligung von privaten Akteuren im Rahmen der staatlichen Sicherheitsproduktion, etwa durch private Sicherheitsdienste, aber auch durch die Responsibilisierung von Privatpersonen für Gefahren, z.B. durch Einbrüche, die vor allem auch durch privat angeschaffte Sicherheitstechnik zu adressieren sein sollen. Die Reprivatisierung steht dabei emblematisch für eine Neoliberalisierung von Kontrolle.

339 Siehe dazu etwa *Kunz/Singelnstein,* Kriminologie, S. 335 ff.

340 *Leman-Langlois* in Deflem (Hrsg.), The Handbook of Social Control, 347 (357).

341 *Shearing/Johnston,* Governing Security, S. 138 ff.

produktion, dass eine Pluralität von Akteuren im Rahmen der Produktion von sozialer Ordnung keine Neuheit ist. So hat beispielsweise *Zedner* argumentiert, dass es zwar seit den 1970er-Jahren zu einer Reprivatisierung von Sicherheitsproduktion gekommen ist, die sich ab den 1990er-Jahren noch einmal beschleunigt hat. Allerdings seien – so *Zedner* – die strukturellen Veränderungen, die damit einhergingen, vergleichbar mit der Situation im 17. und 18. Jahrhundert. Diese Deutung geht davon aus, dass die Formen der Polizeiarbeit, die vor der Institutionalisierung der modernen Polizei vorherrschten, allmählich zurückkehren: So wie Sicherheit heute käuflich geworden ist, konnte man bereits in der späten Neuzeit und frühen Industrialisierung Diebesfänger und sonstige private Personen für Sicherheitsdienste anheuern und auch der Trend zur Responsibilisierung des Einzelnen in der Gegenwart ähnelt dem Geist der Selbsthilfe, der im 17. und 18. Jahrhundert präsent war.[342] Allerdings darf dabei nicht übersehen werden, dass auch private Akteure der Sozialkontrolle in dieser Zeit entstanden sind, um in einem neuen urbanen Umfeld die Lücke zu füllen, die der Zusammenbruch traditionaler, ländlicher Gemeinschaften hinterlassen hatte. Die Zeit der Industrialisierung ist also nicht nur die Zeit, in der die moderne Polizei entsteht und sich etabliert. Vielmehr kommt es hier auch zu einer Vervielfältigung – privater wie öffentlicher – Institutionen der formellen Sozialkontrolle, sodass die Pluralität als Eigenschaft im Netzwerk sozialer Kontrolle als Konstante erscheint und der Wandel sich in erster Linie in der zu- und abnehmenden Dominanz oder Schwäche einzelner äußert.[343] Als weitere ideologieinduzierte Dynamik der Sozialkontrolle ließe sich zudem die generelle Aufwertung von Sicherheit als gesellschaftlich überall erstrebenswerter Zustand anführen, wie sie für die letzten Jahrzehnte zu beobachten ist.[344]

Die Frage, wer welche Rolle in diesem Kontrollnetzwerk spielen wird oder kann, ist dann eine Frage, die stark mit dem zweiten Strang der Wandlungsprozesse der Sozialkontrolle verbunden ist, also mit technologieinduzierten Dynamiken. Dabei ist zunächst festzustellen, dass es schon lange eine starke Verbindung zwischen sozialer Kontrolle und Technologie gibt. Legt man einen weiten Technologie-Begriff zugrunde, so ließe sich auch Sozialkontrolle selbst als gesellschaftliche Technologie bezeichnen. Die Nutzung von Technologie zur Aufrechterhaltung gesellschaftlicher Normen

342 *Lucia Zedner* British Journal of Criminology 46 (2006), 78.
343 Ähnlich *Mulone* in Deflem (Hrsg.), The Handbook of Social Control, 207 (218).
344 Siehe dazu etwa *Daase* Aus Politik und Zeitgeschichte 2010, 9.

war indessen lange Zeit nicht in erster Linie mit Informationstechnologie verbunden, sondern verwendete – dem Kontrollmodus vergangener Gesellschaften entsprechend – in erster Linie Technologien der körperlichen Züchtigung und Disziplinierung.[345] Mit Abschaffung von Körperstrafen sowie sonstigen körperlichen Disziplinierungen und Ersetzung dieser durch rechtsstaatliche(re) Strafsanktionen stand nicht mehr die öffentliche Verdeutlichung von Normen durch martialische Ahndung ihrer Übertretung im Vordergrund sozialer Kontrolle, sondern eine bürokratisierte Auf- und Bearbeitung von Devianz begann, sich als Modus gesellschaftlicher Normenkontrolle zu etablieren. Wie es für Bürokratien üblich ist, war diese Tätigkeit untrennbar mit der Verarbeitung von Informationen verbunden, sodass Informationstechnologien zum essenziellen Instrument formeller Sozialkontrolle wurden, wobei allen voran die Polizei als Organisation Innovationen in der Nutzung von Informationstechnologie zu diesem Zwecke vorantrieb.[346] Infolgedessen sind die gegenwärtigen Wandlungsprozesse, wie sie in den vorstehenden informations-, daten- und technologietheoretischen Ausführungen beschrieben worden sind, in ihren Wirkungen für die weitere Evolution der Sozialkontrolle profund.

Charakteristisch für den gegenwärtigen Modus der Massendatenverarbeitung ist eine zunehmende Ubiquität von Sensoren und sonstigen Registrierungsapparaturen, mittels derer automatisch digitale Datenspuren über Phänomene im analogen wie virtuellen Raum aufgezeichnet und gespeichert werden können. Im Wahrnehmungsbereich dieser sensorischen Apparate wird die Erfassung von Informationen über alle Menschen und Objekte sowie die Analyse ihrer Eigenschaften und Verhältnisse in einem noch nie dagewesenen Ausmaß möglich. Die Massendatenverarbeitung befördert so eine quantitativ breitere, aber auch qualitativ tiefere Überwachung, indem die mögliche Erfassbarkeit von Personenkreisen gesteigert wird und jede einzelne Person über eine größere Bandbreite lebensweltlicher Kontexte hinweg verfolgt werden kann. Die technologisch vermittelte Massendatenüberwachung ist dabei zunehmend verdachtsunabhängig, immerwährend, kumulativ, ferngesteuert, unsichtbar, automatisiert, präventiv und in lebensweltliche Routinetätigkeiten eingebettet.[347] Die Expansion von Praktiken und Verfahren der Massendatenverarbeitung führt, kumulativ betrachtet, zum Aufbau einer Art dezentrale Vorratsdatenspeicherung.

345 *Foucault,* Überwachen und Strafen, insb. 44 ff.
346 Siehe zu diesen Entwicklungen unten S. 101 ff.
347 *Brayne,* Predict and surveil, S. 39.

Zwar ist sie nicht durch eine zentrale staatliche Instanz initiiert, wie die Vorratsdatenspeicherung im Rechtssinne, ist insofern aber auch nicht auf bestimmte Kommunikationsmetadaten beschränkt, sondern kann zusammengenommen als eine informationelle Infrastruktur aufgefasst werden, in der Daten zu einem breiten Spektrum verschiedener lebensweltlicher Vorgänge bevorratet werden (können). Insbesondere in der Datenökonomie werden Daten in einer Weise vorgehalten, die vermutlich wertvoller oder zumindest ebenso wertvoll für polizeiliche Arbeit wären wie Daten im Rahmen der Vorratsdatenspeicherung im rechtlichen Sinne.[348] Mit entsprechenden Datensammlungen und Analyseinstrumenten kann durch die Zeit vor und zurückgegangen und digital kondensiertes deviantes Verhalten identifiziert werden, was die Möglichkeiten für soziale Kontrolle ausweitet. Denn vorher waren die informationellen Möglichkeiten zur Rekonstruktion von Vorkommnissen beschränkt und soziale Kontrolle konnte eher situationsbezogen ausgeübt werden.[349] Im Zeitalter der Massendaten gilt eher: „The start and finish of the criminal justice process are now indefinite and indistinct as a result of the introduction of mass surveillance."[350] Die Pervasivität bringt *Leman-Langlois* zum Ausdruck, wenn er schreibt:

> „Whether or not you are seen somewhere is already becoming unimportant, as your own smart devices will geotag you there (and, unlike cameras, are not vulnerable to dirt, rain, fog, cobwebs, bird nests, etc.). Through our connected smart devices (for the moment: thermostats, toothbrushes, forks, bras, mattresses, light bulbs, locks, fish tanks, doorbells, television sets, Barbie dolls, coffee machines, ovens, vents, fans, blood-pressure monitors, thermometers, etc.), the least of our movements leave a trace in multiple servers. Our thoughts are no better protected: any keyword we search, any paper we browse, our tweets, our books, the words and tone of voice we use when we phone a calling center, everything is already available for analysis. These interconnected practices of dataveillance may seem to amount to the information- gathering aspect of totalitarianism – total social transparency – minus only the heavy-handed social-control aspect. Yet, one key difference remains: the information is gathered and used not by a central entity such as the

348 *Leman-Langlois* in Deflem (Hrsg.), The Handbook of Social Control, 347 (351).
349 *Brayne,* Predict and surveil, S. 43, 88.
350 *Marks/Bowling/Keenan* in Brownsword/Scotford/Yeung ua (Hrsg.), The Oxford Handbook of Law, Regulation and Technology, 705 (724 f.).

state, but by a multitude of individual entities, whose interests are often at odds with one another." [351]

Zusätzlich weist die Massendatenüberwachung auch eine sozial-räumliche Komponente auf, indem die Abbildung sozialer Netzwerke in den Daten möglich wird, die durch entsprechende Analyseverfahren sodann sichtbar, erkundbar und nachvollziehbar werden.[352] Auf diese Weise entstehen „sekundäre Überwachungsnetzwerke",[353] die ihren Niederschlag etwa in den sog. Auskunfts- und Kontaktpersonen im deutschen Polizeirecht haben. Dabei handelt es sich um solche Personen, die in polizeilichen Datenbanken gespeichert werden dürfen, weil sie mit Verdächtigen oder Verurteilten in Verbindung stehen.[354]

Trotz massenhafter Erfassung richtet sich moderne[355] Sozialkontrolle indessen nicht unterschiedslos gegen jede:n. Unter der Prämisse der Effizienz, die sich aus Ressourcenknappheit speist, müssen Praktiken der Sozialkontrolle grundsätzlich selektiv ausgerichtet werden. Geeignete Ziele für die soziale Kontrolle werden vor diesem Hintergrund identifiziert, indem auf Grundlage konzeptueller Annahmen Merkmale der Zielpersonen – etwa ein bestimmtes Verhalten, Aussehen, Alter, Geschlecht, eine politische Meinung oder Zugehörigkeit zu einer ethnische oder sonstigen sozialen Gruppe – erhoben und nach den zugrundeliegenden Konzepten in Verbindung zueinander gesetzt werden, um dann über sich daraus ergebende Einschätzungen der Wahrscheinlichkeit zu deviantem Verhalten über die Notwendigkeit von Maßnahmen sozialer Kontrolle zu entscheiden. Diese prinzipielle Logik von massendatenbasierter Kontrolle ist für sich genommen äußerst affin für diskriminierende Tendenzen, wenn die konzeptuellen Grundannahmen, nach denen sich Auswahl, Erhebung und Verarbeitung der Merkmalsdaten richten, ohne von außen auferlegte ethische Regeln und Begrenzungen rein an Gesichtspunkten der Effizienz ausgerichtet sind.

---

351 *Leman-Langlois* in Deflem (Hrsg.), The Handbook of Social Control, 347 (352).

352 *Brayne,* Predict and surveil, S. 44 f.

353 *Brayne,* Predict and surveil, S. 52.

354 Siehe dazu näher unten S. 331 ff.

355 Von "moderner" Sozialkontrolle ist grundsätzlich ab der Staatenbildung bzw. Nationenbildung im Globalen Norden, welche die staatlichen Autoritäten mit dem Legitimitätsproblem, nachhaltige Kontrolle über ein bestimmtes Territorium und eine bestimmte Bevölkerung auszuüben sowie beides zu schützen, konfrontierte, zu deren Lösung sich im Laufe der Zeit (etwa ab dem 18. Jahrhundert) die Polizei-Institutionen der Gegenwart herauszubilden begannen, siehe ausführlicher dazu unten unter S. 101 ff.

Sollen Überwachungs- und Sozialkontrollprojekte begrenzt sein, müssen sie proaktiv so gestaltet werden.[356]

Neben die rekonstruktiv-retrospektive Sozialkontrolle, die eine rückschauende Identifizierung von Normabweichung in den latenten Datenspeichern der Massendatengesellschaft erleichtert, tritt zudem immer präsenter auch die umgekehrte Blickrichtung der Überwachung: Mit dem sogenannten *preventive turn*[357] soll auch die Sozialkontrolle prospektiv werden und Devianz idealerweise so früh wie möglich erkennen und unterbinden. Obwohl sich dieser Wandel von der Kriminalrepression hin zur Kriminalprävention schon seit längerem abzeichnet, sind in erster Linie die mit dem Massendatenphänomen zusammenhängenden informationstechnischen Fortschritte die zentralen Hoffnungsträger einer akkurateren und effektiveren zukunftsgerichteten Sozialkontrolle. Schon länger wird dabei im Kontext der Polizei von „intelligence-led policing" gesprochen, wobei es um eine Überwindung reaktiver Polizeitaktiken geht. Zentral ist die Ausrichtung der Polizeiarbeit auf die proaktive Erkennung und Verwaltung von Risiken über den Weg von breiter Datenbeschaffung, -auswertung und -analyse.[358] Vor diesem Hintergrund gehen *Egbert und Leese* davon aus, dass die systematische und datengetriebene Hinwendung zur Zukunft bzw. zu den vielen verschiedenen möglichen Zukünften der Kriminalität starke Auswirkungen auf die Polizeiarbeit insgesamt haben wird – das heißt darauf, wie die Polizei mit der Gesellschaft interagiert, wie abweichendes Verhalten als Sozialphänomen wahrgenommen wird, was dagegen getan werden soll und wie das getan werden soll.[359] Auch hier wird wieder die bereits beschriebene Bedeutung des gesellschaftlichen Umgangs mit Informationen für die Fortentwicklung der Gesellschaft selbst deutlich. Gerade die Auswirkungen auf die Sozialkontrolle als zentraler Mechanismus für die Stabilisierung von gesellschaftlicher Ordnung sollten dabei in ihrer Reichweite nicht unterschätzt werden. Auf die Frage, wie die Polizei tatsächlich mit dem Phänomen – und aus ihrer Perspektive auch Problem – der Massendaten umgeht und welche Schlüsse sich daraus eventuell für die polizeiliche Sozialkontrolle ziehen lassen, wird noch zurückzukommen

356 *Leman-Langlois* in Deflem (Hrsg.), The Handbook of Social Control, 347 (349).
357 Siehe dazu sowie zum Folgenden *Adam Crawford/Karen Evans* in Leibling/Maruna/McAra (Hrsg.), The Oxford Handbook of Criminology; *Carvalho,* The preventive turn in criminal law; *Singelnstein* in T. Fischer/Hilgendorf (Hrsg.), Gefahr, 95.
358 *Ratcliffe,* Intelligence-Led Policing; *Lana Merbach/Kai Seidensticker*, Bitship Troopers - Big Data und informationsgeleitete Polizeiarbeit in Deutschland, 2019.
359 *Egbert/Leese,* Criminal futures, S. 10.

sein.[360] Die Bemühungen um informationstechnologischen Fortschritt bei den Polizeien lassen sich vor diesem Hintergrund auch als ein Bemühen um Erhalt oder vielleicht auch Ausbau der polizeilichen Deutungsmacht und Deutungshoheit begreifen. In einer Welt, in der alles oder doch vieles zunehmend datenvermittelt ist, braucht es für eine solche Deutungshoheit die „epistemische Autorität" darüber, wie die Welt informationell aufbereitet wird und wie aus diesem Wissen Handlungen abzuleiten sind.[361]

Relevant im Kontext des Wandels sozialer Kontrolle ist an dieser Stelle noch die Deutung dieser Evolution – auch weil die vorliegende Arbeit ebenfalls die beschriebenen Entwicklungen untersucht und interpretiert. Vor dem Hintergrund verschiedener Formen formeller, polizeilicher Sozialkontrolle gibt es auch unterschiedliche Deutungen zu ihrem Wandel, woraus sich ein gleichzeitiges Nebeneinander von zum Teil gegenläufigen Entwicklungstendenzen ergeben kann. Auf Begriff gebracht kann man Deutungen ausmachen, die Tendenzen hin zu einer zunehmend selektiven, zunehmend totalen, zunehmend sanften oder zunehmend harten Sozialkontrolle annehmen.

Es wurde bereits erwähnt, dass polizeiliche Sozialkontrolle sich nicht unterschiedslos gegen jede:n richtet, sondern aufgrund von allgemeiner Ressourcenknappheit priorisiert werden muss. Polizeiliche Kontrolle ist insofern per se selektiv. Dabei ist nicht immer leicht zu erkennen, welche Abwendung normabweichenden Verhaltens die beste Allokation der begrenzten Ressourcen darstellt. Grundsätzlich richtet sich der Aufmerksamkeitsfokus der polizeilichen Sozialkontrolle nach der Schwere der Normabweichung, die stattgefunden hat oder droht – schwere Straftaten haben insofern prinzipiell Priorität. Insbesondere im Rahmen der Verhinderung von Normabweichung agiert die Polizei jedoch – aufgrund der Zukünftigkeit des Ereignisses – auf unsicherer Tatsachengrundlage. Durch die Verbesserung der Produktion von prognostischem Wissen, wie es Potenzial und Versprechung des Massendatenparadigmas ist, kann die Allokation der knappen Ressourcen zur sozialen Kontrolle – so der Gedanke – besser erfolgen. Statt viele Personen oder Orte zu überwachen, mit denen ein gewisses intuitives oder auch erfahrungswissentliches Devianzpotenzial in Verbindung gebracht wird, soll durch datenbasierte algorithmisierte Risikoprognosen das Risikopotenzial von Personen oder Orten präziser berechnet

360 Siehe dazu näher unten S. 377 ff.
361 *Egbert/Leese,* Criminal futures, S. 73.

werden können. In der Folge kann es zu gezielteren Steuerungshandlungen („targeted governence“[362]) kommen, indem die Polizei ihre zu ergreifenden Maßnahmen feiner auf die jeweiligen Objekte ihres Handelns kalibriert und damit ihre Ressourcen mit größerer Präzision, also effektiver, einsetzen kann.[363] Damit würde polizeiliche Sozialkontrolle sich voraussichtlich zunächst auf weniger Personen oder Orte erstrecken als zuvor, also insgesamt selektiver werden. Da diese Praktiken indessen auf bereits bestehenden Daten der Polizeien aufbauen, werden häufig ohnehin bereits im Fokus der Polizei stehende Personen und Orte noch stärker kontrolliert werden, weil man unter diesen die gefährlichsten priorisiert.[364] Allerdings könnte eine bessere Allokation der Ressourcen auch dazu führen, dass nunmehr auch in Bereichen, die zuvor als „underpoliced“ galten,[365] wie etwa Wirtschafts- oder Cyberkriminalität, polizeiliche Kontrollpotenziale entfaltet werden könnten.

Dem scheinbar entgegengesetzt tritt eine Deutung, die vor allem eine umfassendere, totalere polizeiliche Sozialkontrolle im Entstehen begriffen sieht. Die technologische Struktur des Massendatenphänomens hält zunehmend soziale Interaktionen, Prozesse und damit auch Devianz in digitalen Datenfragmenten fest. Dabei sind die Daten zwar nicht alle zentral bei den Polizeien gespeichert, aber das generell steigende Aufkommen von digitalen Daten führt zu einer Zunahme an Daten, die die Polizei, etwa gespeichert auf Endgeräten, beschlagnahmen und auslesen kann. Zudem kann die Polizei im Wege ihrer gesetzlichen Befugnisse auf private Datenbestände zugreifen und sich die dort erfassten Daten für ihre Aufgabenerfüllung zu eigen machen. Dadurch und durch Veränderungen der Datenerhebungstechnologien wachsen die polizeieigenen Datenbestände. Indem nun auch Datenverarbeitungstechnologien verbessert werden, kann in einer solchen Deutung des Wandels polizeilicher Sozialkontrolle mehr abweichendes Verhalten effektiver bearbeitet werden, wodurch zunächst das polizeiliche Hellfeld ausgeweitet wird. So könnte etwa „gewöhnliche“ Straßenkriminalität aus den von der Polizei kontrollierten Umgebungen aufgrund des

362 *Valverde/Mopas* Global governmentality: Governing international spaces 28 (2004), 233.

363 *D. Wilson* in Završnik (Hrsg.), Big data, crime and social control, 108 (121); *Ferguson* U. Pa. L. Rev. 163 (2015), 327-410 (395).

364 Siehe dazu etwa *Selbst* Georgia Law Review 52 (2018), 109 (119 ff.)

365 Ähnlich etwa *Brayne,* Predict and surveil, S. 144.

insofern erhöhten Strafverfolgungsdrucks verdrängt werden.[366] Während eine effektive Kriminalitätsbekämpfung in weiten Teilen funktional und begrüßenswert ist, muss auch beachtet werden, dass es dysfunktionale Formen der Sozialkontrolle gibt. Wirkmächtig ist in diesem Kontext etwa das Konzept der Präventivwirkung des Nichtwissen von *Popitz*, wonach eine vollständige Aufdeckung und Aburteilung von Normabweichungen das gesellschaftliche Normsystem schwächen oder sogar zum Einsturz bringen könnte, weil den Gesellschaftsmitgliedern die Ubiquität der Kriminalität klar würde, also dass sich alle oder zumindest viele andere (auch) nicht an die Normen der Gesellschaft halten.[367] Zwar ist die vollständige Ahndung von Normabweichungen nach wie vor nur ein Gedankenexperiment, doch es ist nicht auszuschließen, dass sich bereits unterhalb der Schwelle der vollständigen Sozialkontrolle unbeabsichtigte und dysfunktionale Auswirkungen auf das gesellschaftliche Normsystem zeigen. So könnte sich die Gesellschaft durch eine extensive Sozialkontrolle zunehmend als „globales Dorf"[368] wahrnehmen, ohne dass aber die positiven Aspekte dörflicher Daseinsweise damit verbunden wären, wie sie dem Begriff im Zuge von affirmativen Globalisierungskommentaren zugeschrieben wurden:

> In many ways, a surveillance society resembles the rural village of a century or so ago, with the close proximity of its dwellings, the constant visibility, the incessant gossip, and the stigma imposed on various deviants. Yet, it also differs on several key points. First, the modalities, the practice, and the consequences of proximity and „gossip" surveillance are known and have not changed for probably thousands of years. Technosurveillance, on the other hand, is evolving quickly, with unpredictable consequences. Already, it is often impossible to recognize. Second, while memory fades, technosurveillance not only never forgets, but it remembers better – and more – with time, since new analysis techniques can give entirely new meanings to old data. Third, in the village, surveillance tends toward an equilibrium of power, since everyone may watch everyone; this also creates reciprocity, where one knows when one is being watched, and by whom.[369]

366 *Brey* in M. McGuire/Holt (Hrsg.), The Routledge handbook of technology, crime and justice, 17 (31 ff.).
367 *Popitz,* Über die Präventivwirkung des Nichtwissens.
368 *McLuhan,* The global village.
369 *Leman-Langlois* in Deflem (Hrsg.), The Handbook of Social Control, 347 (356 f.).

Nach dieser Deutung wird Devianz also insgesamt sichtbarer für die Gesamtgesellschaft, wobei damit – aufgrund der schnelllebigen Entwicklungszyklen der Überwachungs- und Kontrolltechnologie – damit eine gewisse Unberechenbarkeit einhergeht. Im Sinne von *Popitz* wären in dieser Lesart der polizeilichen Sozialkontrolle vor allem auf dysfunktionale Wirkungen auf das gesellschaftliche Normgefüge zu achten.

Eher eine affirmative Perspektive auf die Entwicklung von staatlicher oder polizeilicher Sozialkontrolle entwickeln diejenigen, die in einer granularisierten, präzisierten und vorverlagerten Sozialkontrolle eine sanftere Form der Disziplinierung sehen. Als praktisches Beispiel hierfür kann das Eindhoven Living Lab gesehen werden, das dabei zudem exemplarisch für Grundkonzepte des Trends zur Smart City steht. In sensoren-saturierten Umgebungen der Smart City wird hier abweichendes, eskalierendes Verhalten, also Verhalten, das durch Aggressivität oder ähnliche Formen des individuellen Kontrollverlusts markiert wird, sensorisch aufgezeichnet und datenanalysierend erkannt. Auf dieser Wissengrundlage soll dann zielgerichtet mit Deeskalationsmaßnahmen gegengesteuert werden können. Ziel der Interventionsmaßnahmen im Eindhoven Living Lab ist es, subtile Verhaltensänderungen zu induzieren, etwa „eine Verringerung des Erregungsniveaus", die Aufmerksamkeit neu zu fokussieren, soziales Verhalten zu fördern oder das Selbstbewusstsein und die Selbstkontrolle einer Person oder Gruppe (etwa mittels interaktiver Straßenbeleuchtung) zu erhöhen.[370] Während die Beschreibung bei *Kort* eher affirmativ wirkt, lässt sich eine sanfte Sozialkontrolle auch stärker kritisch betrachten. Insbesondere die Exklusionspotenziale in einer Welt, in der Zugänge zu und Teilhabe an gesellschaftlichen Ressourcen und Prozessen zunehmend darüber vermittelt wird, dass die dafür erforderliche Erfüllung von Erwartungen über digitale Daten nachgewiesen wird, erscheinen mitunter eher als dystopisch-autoritär denn als Zivilisierung von Disziplinierungstechniken. Solche Formen der Kontrolle erinnern eher an die archaische Verbannung als schwere Strafe für Vergehen gegen die soziale Gemeinschaft. So heißt es etwa bei *Leman-Langlois*:

> „The legal frameworks, the technologies, the practices, and our own preferences are all in an agitated state of flux. To be sure, as automated bots gain access and cross-match these data, and attach them to our bodies, we might be a turn of the key away from the most perfect form

370 *Kort* ILI Magazine 2014, 10; kritisch dazu *Doorman/Pali* JEA 5 (2021), 78.

> of „big data" totalitarianism. And there will be no need for gulags this time: in the digitized world, one can be digitally excluded from the social and ostracized by smart machines, which might very well be punishment enough."[371]

Gegen die Deutung von massendatengestützter Sozialkontrolle als humanisierte und sanfte Form der Überwachung und Disziplinierung wenden sich Deutungen wie die von *Beydoun*, der vor allem für nicht-weiße Menschen überall dort, wo sie zu Minderheitsangehörigen in der Gesellschaft zählen, eine psychisch, aber auch physisch unterwerfende, also härter werdende Form der Sozialkontrolle ausmacht. Damit bringt er gegen die Idee einer sanfteren Sozialkontrolle explizit ein kontrastreiches Gegenkonzept für weite Bevölkerungsteile der verschiedenen Gesellschaften auf der Welt in Stellung. Auf Grundlage der faktischen Auseinandersetzung mit der Behandlung der Uighur:innen durch den chinesischen Staat analysiert und zeigt *Beydoun,* „how state administration of digital surveillance blurs the mandates of mass control, discipline, and punishment into a state ensemble of subjugation."[372] *Beydoun* zufolge hat der Einsatz von informationstechnologischen Überwachungs- und Kontrollinstrumenten insbesondere in den Händen von autoritären Staaten die Wirkung, Sozialkontrolle stark zu intensivieren, sodass sich nicht nur der Umfang des tatsächlich erfassten Verhaltens weitet, sondern im Zuge der staatlichen Maßnahmen gegen das abweichende Verhalten auch psychisch und physisch aus dem Ruder laufen. Während die anderen Entwicklungstendenzen durchaus je auch positive Potenziale haben, muss eine solche härter werdende Sozialkontrolle in einem Rechtsstaat ausgeschlossen bleiben.

Gerade diese Bandbreite und Divergenz der sozio-technischen Imaginationen[373] hinsichtlich der Evolution der Sozialkontrolle verlangen für den deutschen Kontext eine genaue Analyse der zugrundeliegenden Wandlungsprozesse, um eine an hiesige Verhältnisse angenäherte Deutung entwickeln zu können.

Die vorstehenden Bemerkungen sollen aber nicht den Eindruck erwecken, Sozialkontrolle wäre etwas per se Kritikwürdiges und in der Tendenz Negatives. Sozialkontrolle ist, wie eingangs angemerkt, eine unhintergeh-

371 *Leman-Langlois* in Deflem (Hrsg.), The Handbook of Social Control, 347 (359).
372 *Beydoun* Washington and Lee Law Review (Wash. & Lee L. Rev) 79 (2022), 769.
373 Siehe dazu *Jasanoff/Kim* (Hrsg.), Dreamscapes of modernity. Näher dazu unten S. 487 ff.

bare Tatsache von Gesellschaft. Vor allem im Bereich von Kriminalität gilt: Normabweichungen haben in der Regel eine inhärente Gefährlichkeit. Sie können körperliche Schäden, einschließlich Verletzungen oder Tod, finanzielle Verluste und eine Beeinträchtigung des Vertrauens und des Zusammenhalts einer Gemeinschaft zur Folge haben.[374] Insofern ist Kriminalitätsverhütung ein sinnvolles und wünschenswertes Anliegen eines Gemeinwesens. Auch ist der liberale Rechtsstaat mit Blick auf soziale Kontrolle äußerst voraussetzungsreich. Wenn *McLuhan* in seiner gewohnt kurzen und pointierten Art meint, dass „[t[he police state precedes the consumer society",[375] bringt er damit zum Ausdruck, was auch *Foucault* systematischer herausgearbeitet hat. Damit (Rechts-)Subjekte überhaupt agieren und somit auch staatlich garantierte Freiheiten wahrnehmen können, müssen sie zunächst in einem Prozess, den der französische Soziologe als Subjektivierung bezeichnet hat, mittels verschiedenen Formen staatlicher Machttechnologien, wie etwa den Disziplinen, geschaffen werden.[376] Die Funktionsfähigkeit einer Gesellschaft ist folglich immer auch auf ein bestimmtes Maß und einen bestimmten Modus der Sozialkontrolle angewiesen. Ein insofern funktionales und gleichzeitig rechtsstaatliches Maß und einen entsprechenden Modus der sozialen Kontrolle für die spätmoderne Gesellschaft mit ihren multiplen normativen Ordnungen zu finden, muss als wichtiges wissenschaftliches und insbesondere kriminologisches Forschungsfeld angesehen werden.

374 *R. Meier* in Deflem (Hrsg.), The Handbook of Social Control, 23 (32).
375 *McLuhan,* The Gutenberg galaxy, S. 236.
376 Siehe dazu die eindrucksvolle Rekonstruktion des Theoriegebäudes *Foucaults* durch *Buckel,* Subjektivierung und Kohäsion, insb. S. 182 ff.

Kapitel II. Die historische Entwicklung des polizeilichen Informationswesens

A. Einleitung

Als sozio-technisches System ist das polizeiliche Informationswesen ein sozial gemachtes Gebilde. Insofern ist sein gegenwärtiger Zustand das Ergebnis eines Koevolutionsprozesses von Technologie und damit interagierender Gesellschaft. Dieser Entwicklungsprozess hat aufgrund seiner Einbindung in und Bedingtheit durch ein bestimmtes soziales Geflecht – neben einigen Regelmäßigkeiten – eine gewisse Gesellschaftsspezifik. Das polizeiliche Informationswesen sieht in den Vereinigten Staaten anders aus als in Deutschland, die DNA-Datenbanken sind im Vereinigten Königreich signifikant umfangreicher als in anderen europäischen Ländern und der Einsatz von künstlicher Intelligenz nimmt in China andere Ausmaße an als in den meisten demokratischen Staaten. Diese unterschiedlichen Ausprägungen bei prinzipiell ähnlichen technologischen Möglichkeiten, lenken den Blick gerade auf die soziale Gemachtheit von gesellschaftlichen Kontrolltechnologien wie das polizeiliche Informationswesen. Um seinen gegenwärtigen Zustand verstehen zu können, muss also der historische Werdungsprozess beleuchtet werden. Dementsprechend werden im folgenden Kapitel die informationstechnologischen Entwicklungsprozesse der deutschen Polizei – mit zugegebenermaßen eher groben Pinselstrichen – nachgezeichnet, um zentrale Entwicklungsdynamiken und Wendepunkte hervortreten zu lassen und so auch zum besseren Verständnis der Gegenwart polizeilicher Informationsverarbeitung beizutragen.

Organisierte Macht und die von ihr zum Erhalt ihrer Ordnung ausgeübte Sozialkontrolle ist von den frühen Imperien[377] der Menschheit über die mittelalterlichen Reiche bis zu den ersten (absoluten) Staaten der Neuzeit untrennbar mit der Sammlung und Verarbeitung von Informationen verbunden. Erst mit Aufkommen moderner Staatlichkeit aber systematisiert und professionalisiert sich die herrschaftliche Informationsverarbeitung in einer Art und Weise, die es dem modernen Staat ermöglicht, nachhaltige

377 Vgl. etwa *Michael McGuire* in Michael McGuire/Holt (Hrsg.), The Routledge Handbook of Technology, Crime and Justice, 35 (47) zu den Sumerern.

informationelle Macht zur Steuerung gesellschaftlicher Prozesse aufzubauen.[378] Diese intensive Verschränkung einer Praxis hoheitlicher Informationsverarbeitung mit der Evolution moderner Herrschaftsformen lässt etwa für *Nassehi* den Schluss zu, dass die Moderne als Epoche und mit ihr die moderne Gesellschaft unterschwellig von einer informationstechnologisch bedingten, gesellschaftlichen Selbstbwusstseinswerdung angetrieben wird. Anlässlich dieses emergierenden Bewusstseins beginnt sich unsere Gesellschaft, als eine solche zu beschreiben und erkennt die beständig steigende Komplexität ihres sozialen Gefüges,[379] was einen zunehmenden Bedarf nach Steuerungsansätzen begründet.

Auch wenn diese Entwicklung nicht ausschließlich von den Polizeibehörden ausging oder getragen wurde, so waren sie doch schon früh zentral für die Sammlung und Auswertung von Informationen mit denen sich die moderne Staatlichkeit über die Regelmäßigkeiten ihrer Bevölkerungen und das in ihnen auftretende abweichende Verhalten zu informieren versuchte, um mittels der darauf fußenden Produktion handlungsleitenden Wissens soziale Ordnung zu schaffen und aufrechtzuerhalten.[380] Die Geschichte der modernen Polizei lässt sich insofern auch oder sogar insbesondere als eine Geschichte der Entwicklung polizeilicher Informationstechnologie und -verarbeitungspraktiken begreifen. Seit den Anfängen der polizeilichen Institutionalisierung in Deutschland in der zweiten Hälfte des 19. Jahrhunderts sind personen- und gruppenbezogene Informationssammlungen ein zentraler Bestandteil der polizeilichen Praxis. In den vergangenen 150 Jahren haben die deutschen Polizeibehörden verschiedene informationelle Praktiken eingesetzt, um anhand bestimmter Merkmale zu identifizieren, zu überwachen, zu kontrollieren und sogar zu eliminieren. Während dieses Zeitraums haben sich die Möglichkeiten der Informationsverarbeitung technologisch stetig weiterentwickelt[381] – von den Anfängen der buchbasierten Informationssysteme bis hin zu den fortschrittlicheren Datenbanken und innovativeren Datenverarbeitungsverfahren von heute und morgen. Unabhängig vom Grad der informationstechnologischen Finesse der zur Verfügung stehenden Mittel, ging es dabei im Prinzip stets darum,

378 Dazu ausführlicher *Lewinski* in Arndt/Betz/Farahat ua (Hrsg.), Freiheit - Sicherheit - Öffentlichkeit, 196 (201 ff.).

379 Vgl. hierzu *Nassehi,* Muster, S. 62 f.

380 *Siemann,* »Deutschlands Ruhe, Sicherheit und Ordnung«, 135 f.; *P. Becker,* Dem Täter auf der Spur, S. 70 f.

381 Die Polizei ist prinzipiell seit dem Entstehen in ihrer modernen Form eng mit Technologien aller Art verwickelt, siehe *Egbert/Leese,* Criminal futures, S. 44.

datengestütztes Wissen über Personen und die Gruppen, denen sie angehören, zu gewinnen und darauf aufbauend effektive Sozialkontrollhandlungen zu ergreifen.

Vor diesem Hintergrund sollen Veränderungen und Beständigkeiten polizeilichen Informationshandelns im Laufe der Zeit nachgezeichnet werden. Zentral geht es dabei um die übergreifenden Entwicklungen der informationellen Rahmenbedingungen, wobei auch deren Materialisierung in Form von konkreten informationstechnologischen Innovationen in den Blick genommen wird, wo diese paradigmatisch für einen vorherrschenden Modus der Verarbeitung von Informationen durch die Polizei stehen. Im Zuge dessen zeigt sich eine wachsende Bedeutung dieses informationstechnologischen Unterbaus für die moderne Polizei. Verwoben mit dieser Technologiegeschichte ist dabei auch eine Geschichte der sich wandelnden kriminalistischen Konzepte. Ausgehend von den frühen Formen der polizeilichen Informationsverarbeitung im Deutschen Kaiserreich im späten 19. Jahrhundert und endend mit einem Blick auf das polizeiliche Informationswesen der sich schnell entfaltenden Gegenwart, wird argumentiert, dass der technologische Fortschritt zwar eine bisweilen disruptive Entwicklung suggeriert, die Informationspraktiken der deutschen Polizeibehörden und die verwendeten kriminalistischen Konzepte sich jedoch als eher evolutionär erwiesen haben, also einem schrittweisen, adaptiven Wandel unterliegen, statt sich radikal zu erneuern, wie es sonst oft Rhetorik in gegenwärtigen Digitalisierungsdiskursen ist. Denn historisch gesehen haben sich, wie *Jones und Newburn* es ausdrücken, die Aufgaben der Polizei um organisierte Formen der Aufrechterhaltung der Ordnung, der Friedenssicherung, der Durchsetzung von Regeln oder Gesetzen, der Verbrechensermittlung und -verhütung und anderer Formen der Ermittlung und Informationsbeschaffung herum entwickelt.[382] Diese Grundpfeiler haben sich nicht geändert, aber die Strategien und Methoden, mit denen sie umgesetzt werden, sind immer wieder weiterentwickelt und verfeinert worden.[383] So ist es denn auch nicht abwegig, dass *Brayne* den Beginn der Datafizierung der Polizei bereits auf Anfang des 20. Jahrhunderts legt, da mit der Professionalisierung der Polizeibehörden auch das Verlangen nach objektiver Polizeiarbeit einherging, die mit wissenschaftlichen Methoden Kriminalitätsprobleme lösen wollte und dazu immer mehr empirische Daten brauchte.[384]

382 *Jones/Newburn,* Private security and public policing, S. 18.
383 *Egbert/Leese,* Criminal futures, S. 22.
384 *Brayne,* Predict and surveil, S. 18.

B. Institutionalisierung und erste Informationssammlungen

Der systematische Einsatz[385] von technologischen Innovationen erfordert einen gewissen Organisationsgrad, sodass eine Geschichte polizeilicher Informationstechnologie sinnvollerweise erst zu einem Zeitpunkt einsetzten sollte, zu dem sich die moderne Polizei im heutigen Sinne hinreichend institutionalisiert hatte.[386] Zuvor hatte es zwar ebenfalls durchaus zentralisierte Strategien zur Lösung von Ordnungsproblemen gegeben. Jedoch standen hinter den Polizeien der jüngeren Neuzeit und frühen Industrialisierung heterogene Organisationsformen mit nur schwach ausgeprägten Gemeinsamkeiten und geringem Professionalisierungsgrad, was sich etwa auch an der Beteiligung von privaten Akteuren an der Ordnungsproduktion oder defizitären und unmenschlichen Informationspraktiken[387] – wie der Identifizierung durch Brandmarkungen – ausdrückte.[388]

In Deutschland begann die anhaltende Institutionalisierung der Polizei erst nach Reichsgründung in den 70er und 80er Jahren des 19. Jahrhunderts wirklich zu greifen. Bis dahin hatten die selbständigen deutschen Staaten zwar Polizeiorganisationen gebildet und polizeiliche Ausbildungsstätten eingerichtet, doch blieben die Polizeibehörden insgesamt zahlenmäßig und einflussmäßig schwach. Selbst nach der Märzrevolution von 1848, einem Schlüsselereignis des vor-kaiserlichen Deutschlands, das von massiven gesellschaftlichen Unruhen geprägt war, blieb eine starke Polizei ein politisch eher nachrangiges Projekt.[389] Dies änderte sich erst mit den zunehmenden sozialen Spannungen, die durch Industrialisierung, Urbanisierung und eine erstarkende Arbeiterbewegung ab den 1870er Jahren hervorgerufen wurden. Anlässlich dieser Umwälzungen wurde die Polizei im Allgemeinen, ihr Ermittlungsapparat und vor allem ihr politischer Arm grundlegend ausgebaut und gestärkt,[390] wobei die frühen Polizeiinstitutionen in ihrer organisatorischen, personellen und auch technologischen Ausrichtung stark an den jeweils im Staatsgebiet bestehenden Militärorganisationen orientiert

385 Ohnehin war die Polizei seit ihrem bestehen eine eng mit Technologien aller Art verwickelte Organisation, s. *Egbert/Leese,* Criminal futures, S. 44.

386 *Hummer/Byrne* in Michael McGuire/Holt (Hrsg.), The Routledge Handbook of Technology, Crime and Justice, 375 (375).

387 *P. Becker,* Dem Täter auf der Spur, S. 72.

388 Zur Entwicklung von Polizei und Technologie vor dem hier beleuchteten Zeitraum siehe etwa *Bain* in Bain (Hrsg.), Law Enforcement and Technology, 9.

389 *Knöbl,* Polizei und Herrschaft im Modernisierungsprozeß, S. 238 ff.

390 *Graf/Hofer,* Politische Polizei zwischen Demokratie und Diktatur, S. 5 f.

waren.[391] In der Folge führten Professionalisierungsschübe zur Herausbildung eines institutionellen Musters der modernen Polizei, anlässlich dessen *Ellul* gar von dem „technischen Apparat der Polizei" spricht, also die Polizei in ihrer Gesamtheit als gesellschaftliche Kontrolltechnik auffasst, die sich aus verschiedenen untergeordneten Kontroll- und Schutztechniken und -praktiken zusammensetzt und sich im Angesicht gesellschaftlicher Desorganisationsprozesse formiert.[392]

Während sich der politische Zweig dieser neu institutionalisierten Polizei auf die Überwachung und Verfolgung von Sozialist:innen und Anarchist:innen konzentrierte, um die Arbeiterklasse allgemein in Schach zu halten,[393] war der wichtigste Motor für die Verbesserung der Informationsverfahren die Kriminalpolizei: Die soziale Desorganisation im Zuge von Industrialisierung und Urbanisierung[394] führte dazu, dass die bürgerlichen Klassen, die zunehmend an politischer Macht gewannen, eine modernisierte Polizei forderten, um die Ordnung in einer Welt (wieder)herzustellen und aufrechtzuerhalten, in der sich – zumindest nach dem Empfinden der oberen Gesellschaftsschichten[395] – auch die Kriminalität modernisiert hatte.[396]

Wenn auch nicht monokausal allein auf diese politischen Forderungen zurückführbar,[397] kam es in der Folge mit dem Aufbau systematisierter polizeilicher Informationssammlungen über Personen und Taten von po-

391 *Brayne,* Predict and surveil, S. 19; für den deutschen Kontext siehe etwa *Spencer,* Police and the social order in German cities, S. 38 et passim.

392 Zitiert nach *Michael McGuire* in Michael McGuire/Holt (Hrsg.), The Routledge Handbook of Technology, Crime and Justice, 35 (51).

393 *Knöbl,* Polizei und Herrschaft im Modernisierungsprozeß, S. 300; zur Bedeutung von Kommunikationstechnologien für die Polizei anlässlich derartiger Umwälzungen vgl. etwa *Michael McGuire* in Michael McGuire/Holt (Hrsg.), The Routledge Handbook of Technology, Crime and Justice, 35 (52).

394 *Michael McGuire* in Michael McGuire/Holt (Hrsg.), The Routledge Handbook of Technology, Crime and Justice, 35 (50).

395 Wobei die Kriminalitätsraten in den Städten der Industrialisierung tatsächlich stärker anstiegen als sie allein durch das Bevölkerungswachstum relativ zu erklären gewesen wäre, vgl. für den US-amerikanischen Kontext etwa *Michael McGuire* in Michael McGuire/Holt (Hrsg.), The Routledge Handbook of Technology, Crime and Justice, 35 (50).

396 *Funk* in Lange (Hrsg.), Staat, Demokratie und Innere Sicherheit in Deutschland, 11 (21).

397 So weist bspw. *P. Becker,* Dem Täter auf der Spur, S. 72 darauf hin, dass etwa das Verbot körperlich invasiver Kennzeichnungen ebenfalls in Teilen Deutschlands zu einem Wandel von polizeilichen Informationspraktiken beitrug.

lizeilichem Interesse und damit zu einem ersten markanten informationstechnologischen Wandel innerhalb der deutschen Polizeien. Es wurden systematische Verzeichnisse über gestohlene Gegenstände, unaufgeklärte Straftaten, Register über inhaftierte und entlassene Strafgefangene sowie Personen unter Polizeiaufsicht erstellt.[398] Zudem war mit dem sogenannten Verbrecheralbum zum ersten Mal ein informationelles Werkzeug zur Identifizierung von Delinquent:innen und Aufklärung von Taten geschaffen worden, das – letztlich multimedial – Informationen verschiedener Art, insbesondere Fotografien, Informationen zum Modus Operandi und sonstige personenbezogene Daten, zur kriminalistischen Handlungsleitung zusammenbrachte.[399] Dieses „fixierte Gedächtnis der Kriminalpolizei"[400] ermöglichte einen, wenn auch diffusen und trägen, Blick auf Kriminalität als Phänomen mit Regelmäßigkeiten, sodass sich als epistemisches Korrelat der Nutzung von Verbrecheralben durch die Polizei alsbald der sogenannte „Berufsverbrecher" als neuer, vorrangiger Typus der kriminellen Person materialisierte. Das Konzept ist im Grunde als Interpretation des Phänomens der Rückfälligkeit entwickelt worden,[401] das durch die Verbrecheralben ins Bewusstsein der Polizei gerückt war.[402] Infolgedessen kam es zu einer Strukturierung der Sammlung von Informationen entlang des Konzepts des „Berufsverbrechertums" und die Identifizierung der Berufsverbrecher:innen in der Gesellschaft avancierte zu einem allgemeinen und drängenden Problem der Polizei zu dieser Zeit. Dies war auf spezielle Weise mit dem Erkennen von Mustern in den polizeilichen Daten verbunden: Im Mittelpunkt der Vorstellung von Berufsverbrecher:innen stand die Hypothese der „Perseveranz", also die Idee, dass Täter:innen immer in einem klar definierten Bereich, z. B. bei Einbrüchen, mit immer dem gleichen Modus Operandi agierten.[403] Um diese Muster zu erkennen, war es daher notwendig, alle Arten von kriminellem Verhalten zu erfassen, um dann

398 *Heinrich,* Innere Sicherheit und neue Informations- und Kommunikationstechnologien, S. 122.
399 *P. Becker,* Dem Täter auf der Spur, S. 77.
400 *Wagner,* Volksgemeinschaft ohne Verbrecher, S. 82.
401 Wobei *Wagner,* Volksgemeinschaft ohne Verbrecher, S. 81, darauf hinweist, das auch zuvor selbstverständlich die Idee eine "kriminellen Klasse" kein Novum war. Allerdings ist die kriminalistische Formalisierung und Operationalisierung des Konzepts etwas davon abgekoppeltes und ist daher durchaus "entwickelt" worden.
402 *A. Roth,* Kriminalitätsbekämpfung in deutschen Großstädten 1850 - 1914, S. 96; *Wagner,* Volksgemeinschaft ohne Verbrecher, S. 19 ff.
403 *Wagner,* Volksgemeinschaft ohne Verbrecher, S. 22 ff.

erst in einem zweiten Schritt diejenigen Straftaten und Täter:innen herauszufiltern, die den – eher holzschnittartigen – Kriterien entsprachen, die als charakteristisch für Berufsverbrecher:innen galten.[404] Die Verbrecheralben versuchten diese Konzeptualisierung des Kriminalitätsphänomens kriminaltaktisch operationalisierbar zu machen. Ergänzt wurden sie zusätzlich durch Register mit auffälligen körperlichen Merkmalen und Handschriftensammlungen. Nach der Einführung in Berlin im Jahr 1876 verbreitete sich dieses informationelle Werkzeug schnell in den Polizeiorganisationen in ganz Deutschland. Schon nach einigen Jahren zeigten sich jedoch die Grenzen der Informationssammlungen, denn neben der Ausbreitung der Verbrecheralben in die Polizeien des Deutschen Reiches hinein, wuchsen auch die jeweiligen Sammlungen (zu) schnell: Während das erste Berliner Album aus neun Büchern mit 764 Fotografien bestand, waren es 1910 bereits 45 Bände mit 37.000 Fotografien. Sechs Beamte mussten beschäftigt werden, um die Sammlung überhaupt geordnet zu halten: Zehn Jahre alte Fotografien wurden entfernt, neue hinzugefügt und bestehende Aufzeichnungen aktualisiert, was 90-100 neue Einträge pro Tag bedeutete. Gleichzeitig schienen die Erfolge der polizeilichen Arbeit auf Grundlage der Verbrecheralben sehr begrenzt.[405]

Um die Effizienz ihres informationellen Werkzeuges zu erhöhen, begannen die Kriminalisten, die Verbrecheralben neu zu organisieren, indem sie das Format von Alben, also Büchern, auf ein flexibleres Karteikartensystem umstellten, das nach physischen Merkmalen, Art der Straftat und Modus Operandi sortiert war.[406] Darüber hinaus experimentierte die Polizei auch mit der sogenannten Bertillonage[407], einem anthropometrischen Identifizierungssystem aus Frankreich, und führte Anfang des 20. Jahrhunderts die Daktyloskopie, die Identifizierung über Fingerabdrücke, ein. In Deutschland konnte sich aufgrund der einfacheren Durchführbarkeit der

404 *A. Roth,* Kriminalitätsbekämpfung in deutschen Großstädten 1850 - 1914, S. 96; *Wagner,* Volksgemeinschaft ohne Verbrecher, S. 20 ff..

405 *A. Roth,* Kriminalitätsbekämpfung in deutschen Großstädten 1850 - 1914, S. 96 ff..

406 *A. Roth,* Kriminalitätsbekämpfung in deutschen Großstädten 1850 - 1914, S. 100; *Wagner,* Volksgemeinschaft ohne Verbrecher, S. 88 ff.

407 Namensgebend für dieses anthropometrische Verfahren ist der Franzose Alphonse Bertillon, der den polizeilichen Erkennungsdienst mit präzisen Vermessungen des Körpers zu rationalisieren versuchte, *P. Becker,* Dem Täter auf der Spur, S. 78; in Deutschland konnte sich das Verfahren indessen nicht durchsetzen und wurde zu Beginn des 20. Jahrhunderts von der Daktyloskopie abgelöst, *Wagner,* Volksgemeinschaft ohne Verbrecher, S. 98 f.

Daktyloskopie und der Verwaltung der aus ihr gewonnenen Daten diese Identifizierungsform gegenüber der Bertillonage durchsetzen. Die dafür erforderlichen Instrumente konnten zudem industriell gefertigt werden, sodass sich vor allem mit dieser Technik auch institutionell die Organisationseinheit des Erkennungsdienstes herausbilden konnte. Auch hier kam es allerdings schnell zu Problemen mit den Datenvolumina, die im Wege der Daktyloskopie entstanden und einerseits allgemeine Fragen der Informationsorganisation aufwarfen sowie andererseits einen hohen Bedarf an Fachleuten für die Arbeit mit den Fingerabdrücken verursachten. Das führte insgesamt zu einem hohen Rationalisierungsdruck auch in der daktyloskopischen Datenverarbeitung.[408]

Waren solche Entwicklungen auch im Hinblick auf die Informationspraktiken der Polizei durchaus relevant, so waren es doch die in den Verbrecheralben zusammengestellten Dossiers über verurteilte oder auch nur mutmaßliche Kriminelle, die weiterhin die Sicht der Polizei auf die Gesellschaft und ihre abweichenden Mitglieder bestimmten. Neben dem anthropologischen Verbrecherbild, wie es Lombroso formuliert hat und wie es durch naturwissenschaftliche Bemühungen – etwa angeblich durch die Vermessung des Schädels – operationalisierbar gemacht wurde, entstand so ein weiteres Konzept von Kriminellen, das viel stärker auf soziale Eigenschaften der jeweiligen Personen abstellte. Im Sinne des Berufsverbrechertums, also eines Kriminalitätsbegriffs, der von einer subkulturell verfestigten Kriminalitätsstruktur in der Gesellschaft ausgeht, waren bestimmte Eigenschaften und Lebensweisen besonders verdächtig oder galten grundsätzlich als kriminell.[409] Die frühen Verbrecheralben fungierten insofern als „Inventarisierung des Bösen".[410] Diejenigen, die in diese Sammlungen aufgenommen wurden, wurden unwiderruflich als Kriminelle stigmatisiert, ein Etikett, das damals wie heute soziale Ausgrenzung nach sich zog und zieht. Nach Deliktsarten sortiert wurden Straftäter:innen – verurteilte und mutmaßliche – in Gruppen zusammengefasst. Das Bild, das sich den Polizeidienststellen in ganz Deutschland nach diesen ersten systematischen Versuchen, Kriminalität informationell zu erfassen, bot, war das einer Untergruppe unverbesserlicher Berufsverbrecher:innen, die für die meisten Straftaten

408 *Heinrich,* Innere Sicherheit und neue Informations- und Kommunikationstechnologien, S. 129 f.

409 *Heinrich,* Innere Sicherheit und neue Informations- und Kommunikationstechnologien, S. 128, 130.

410 *Regener* Fotogeschichte 38 (1990) (1990) (24).

verantwortlich zu sein schien, die der Polizei zur Kenntnis gelangten. So schätzte Robert *Heindl*, einer der renommiertesten Kriminalisten seiner Zeit, dass 1926 in der Weimarer Republik, etwa 8.500 Berufsverbrecher:innen tätig waren. Um das sich daraus ergebende Kriminalitätsproblem zu lösen, schlug *Heindl* die lebenslängliche Sicherheitsverwahrung von etwa 10 % der Berufsdelinquent:innenen vor.[411]

In *Heindls* Vorschlag zeigt sich anschaulich, welche Wirkung diese erste systematisierte informationelle Erfassung von Kriminalitätsphänomenen wohl teilweise auf die polizeiliche Weltwahrnehmung in Kaiserreich und Weimarer Republik hatte. Die – über Fotografien sogar personalisierte – Sichtbarmachung der Kriminellen in den umfangreichen und rasch wachsenden Datenbeständen hatte die Kriminalität als scheinbar klar umgrenztes, sozial verortbares Phänomen definiert. In der Interpretation der Polizei zeigte sich so ein konkretes Problem, das mit identifizierbaren Abweichler:innen verbunden war und somit gelöst werden konnte, wenn alle oder die meisten Berufsverbrecher:innen von Straftaten abgehalten werden konnten.[412] „Dieser sozialtechnische Machbarkeitswahn", so schreibt es *Peukert*, „verbreitete sich parteiübergreifend. [...] Problemwahrnehmung wie Problemlösung erfolgten in utilitaristisch-technizistischen Schemata. [...] In den Leitbildern der modernen Sozialingenieure [...] schwang der Traum von einer endgültigen Lösung der sozialen Frage mit. So wie der Fortschritt der Medizin den Bakterien den Garaus gemacht hat, könnte die Vereinigung von Wissenschaften und Sozialtechnikern in öffentlichen Interventionen alle noch ausstehenden sozialen Probleme beseitigen."[413] Allein mit den Verbrecheralben schien dies allerdings nicht so, als sei es zu bewerkstelligen, zu schnell wuchsen die Datensammlungen mit neuen Personen und neuen kriminellen Begehungsformen. Um mit dem wandelbaren Phänomen der Kriminalität Schritt halten zu können, sollte die Polizei als Institution zu einer Organisation werden, die der Kriminalität in „Beweglichkeit und Elastizität" entsprach.[414] In einem nächsten Schritt – etwa ab Gründung der Weimarer Republik – sollte deshalb das polizeiliche Nachrichten- und Meldewesen weiter ausgebaut werden.

411 *Wagner,* Volksgemeinschaft ohne Verbrecher, S. 21.
412 *Wagner,* Volksgemeinschaft ohne Verbrecher, S. 138 ff.
413 *Peukert,* Die Weimarer Republik, S. 137 f.
414 *Lindenau* in Lindenau (Hrsg.), Die Kriminalpolizei und ihre Hilfswissenschaften (XXI).

C. Zentralisierung und Netzwerke

Das Konzept des „Berufsverbrechers" trug nicht nur die Problembezeichnung, sondern auch die Lösung bereits in sich. Ganz dem von *Peukert* als „sozialtechnischen Machbarkeitswahn" bezeichnetem Zeitgeist entsprechend, gab es so eine Lösung für den Großteil der gesellschaftlichen Devianz: Wo möglich, sollten Berufsverbrecher:innen rehabilitiert werden, wo nötig, bzw. wo Resozialisierung keine Erfolge zeigte, sollte erbarmungslos schlicht lebenslang inhaftiert werden.[415] Damit hatte die Polizei eine klare Aufgabe: So viele Berufsverbrecher:innen wie möglich identifizieren und festnehmen. Dies erwies sich jedoch schwieriger als es die Einfachheit des kriminalpolitischen Programms suggerierte. Die Datensammlungen der einzelnen Polizeibehörden, etwa in den größeren Städten und mehr noch auf dem Land – wenn es dort überhaupt Kriminalabteilungen gab – bildeten nur die jeweiligen örtlich registrierten Kriminalitätsphänomene ab und waren mithin keineswegs „beweglich und elastisch" genug, um auf die vielfältigen Formen der Devianz adäquat reagieren zu können. Mit allgemein zunehmender Mobilität innerhalb der Gesellschaft konnten sich Straftäter:innen leicht dem kontrollierenden Blick der Polizei entziehen, indem sie einfach den Ort wechselten und in eine andere Stadt reisten, was die Polizeien bereits überforderte.[416] Ab dem späten Kaiserreich begannen Polizeireformer, dieses Problem mit dem Organisationskonzept zentralisierter Informationsnetzwerke anzugehen: Es sollte eine zentrale Polizeibehörde, das sogenannte Reichskriminalpolizeiamt, geschaffen werden, in der polizeiliche Erkenntnisse aus ganz Deutschland gesammelt, ausgewertet und in verwertbarer Form an die zuständigen Polizeidienststellen zurückgeleitet werden konnten. Um einen solchen Datenaustausch zu ermöglichen, mussten die Polizeidienststellen in ein Informationsnetz eingebunden werden, in dem die örtlichen Polizeidienststellen die eingehenden Fälle standardisiert erfassen und an eine übergeordnete Ebene melden mussten, wenn bestimmte Kriterien erfüllt waren. So sollten dann überregional relevante Straftaten und Täter:innen identifiziert werden können. Informationen konnten so – zumindest theoretisch – von der Peripherie zu zentralen Knotenpunkten des Netzes fließen, um dort aggregiert und ausgewertet zu werden. Ziel solcher Bestrebungen war „die Etablierung einer schematisier-

415 *Wagner,* Volksgemeinschaft ohne Verbrecher, S. 138.

416 Siehe *Heinrich,* Innere Sicherheit und neue Informations- und Kommunikationstechnologien, S. 133 mwN.

ten und planmäßigen Verbrecherüberwachung – die andauernde Katalogisierung von Verdächtigen und Verbrechern, die durch ihre Planmäßigkeit, Systematik und Dokumentation die Überführung vereinfachen sollte."[417] Im Rahmen dieser neu konzipierten Informationsinfrastruktur entstand die Vorstellung, dass Kriminalität ein übergreifendes gesellschaftliches Phänomen ist, das in seiner Gesamtheit und nicht nur durch die Lösung der zugrundeliegenden Einzelfälle bekämpft werden muss.[418]

Während in der Weimarer Republik der Plan einer bundesweiten zentralen Polizeibehörde am Widerstand der Bundesländer scheiterte, wurde in Einzelstaaten wie Preußen und Sachsen das Organisationsprinzip der zentralen Vernetzung umgesetzt und ein feinmaschiges Netz von Datensammelstellen aufgebaut. Die Täter:innen, die sich in diesem Netz verfingen, waren jedoch in der Regel Kleinkriminelle, die wegen geringfügiger Delikte gesucht wurden. Die Delikte waren häufig aus Existenznot in einer wirtschaftlich angespannten Zeit begangen worden. Darin spiegelt sich die – bis heute nicht überwundene – Tendenz des polizeilichen Kontrollblicks, sich in nicht unerheblichem Maße auf die sozialen Subkulturen und Randschichten zu konzentrieren, wie etwa auf Arme, Wohnungslose und ethnische Minderheiten wie Sinti und Roma.[419] In Foucaultscher Lesart wurden (und werden) diese sozial Ausgegrenzten herausgegriffen und diszipliniert, um die soziale Ordnung im Allgemeinen aufrechtzuerhalten.[420]

Auch an anderen Stellen kam es trotz des Scheiterns der reichsweiten polizeilichen Zentralstelle zu informationelle Vereinheitlichungs- und Zentralisierungstendenzen. So wurde etwa 1928 das Fahndungswesen und die dazugehörigen Formulare reichsweit vereinheitlicht.[421] Auch eine Standardisierung der polizeilichen Aktenführung wurde in dieser Zeit vorangetrieben. Insgesamt konnte durch eine solche Vereinheitlichung der schriftlichen Informationsformen auch der Informationsfluss innerhalb der organisatorischen Strukturen der Polizeien verbessert werden, jedenfalls dort, wo es eine entsprechende Informationskette von Peripherie zum Zentrum und

417 *Heinrich,* Innere Sicherheit und neue Informations- und Kommunikationstechnologien, S. 131.
418 Vgl. dazu *Wagner,* Volksgemeinschaft ohne Verbrecher, S. 111 ff.
419 *Wagner,* Volksgemeinschaft ohne Verbrecher, S. 241 ff; *A. Roth,* Kriminalitätsbekämpfung in deutschen Großstädten 1850 - 1914, S. 295 ff.
420 *Foucault,* Überwachen und Strafen, S. 250 ff.
421 *Barck* Kriminalistische Monatshefte 3 (1929), 170.

dann, nach Bedarf, auch wieder umgekehrt gab.[422] Vor allem die Kriminalpolizeien profitierten von diesem sogenannten Kriminalpolizeilichen Meldedienst (KPMD). Dem Konzept des „Berufsverbrechers" entsprechend wurden so vor allem Modus Operandi-Karteien sowie Personalakten geschaffen. Letztere wurden vor allem für Personen mit mehrmaliger krimineller Auffälligkeit angelegt und dienten kriminalpolizeilichen Ermittlungen, bildeten aber zugleich auch ein „Charakterbild" der Betroffenen. Enthalten waren nicht nur Informationen aus den Ermittlungsakten, Strafregistern und zu möglichen Festnahmen, sondern auch unbewiesene Verdächtigungen und Kontakte zu anderen Verdächtigen oder Verurteilten.[423] Auch hier zeigte sich wieder eine Grenze der zugrundeliegenden analogen Technik – Akten und Indizes – bei der Verarbeitung der vielzähligen Normabweichungen und Sozialkonflikte, die bereits in der frühen Moderne in den Blick des polizeilichen Hellfeldes gelangten. Der KPMD litt unter dem zu bewältigenden Datenvolumen. Wie mit den Datenmassen umgegangen werden sollte, war innerhalb der Polizei umstritten. Während ein Lager möglichst alle Eingangsdaten verarbeiten und darüber eine effektive Informationsauswertung ermöglichen wollte, war die entgegengesetzte Position pragmatischer: Eher weniger Daten, aber dafür besser auswerten. Schon im Rahmen dieses Diskurses werden zudem Bedenken über den polizeilichen Umgang mit Informationen geäußert, die nach wie vor als relevant gelten dürfen. So wird bereits in den 1930ern befürchtet, eine zu starke Informatisierung der polizeilichen Arbeit, die vor allem im Büro erfolgt, würde ihr den Realitätsbezug rauben. Gleichzeitig wird die Sorge vor eine Überforderung des polizeilichen Informationswesens durch ein Zuviel an Daten laut. Wieder sind die schwer zu bändigenden Informationsflüsse Treiber technischer Rationalisierungsbestrebungen. Büros werden effektiver organisiert und auch die Mechanisierung – etwa in Form von Schreibmaschinen – hält zunehmend Einzug in die polizeiliche Arbeit.[424]

Die politische Blockade in Bezug auf die reichsweite Zentralisierung der polizeilichen Aufklärung wurde schließlich von den Nationalsozialisten aufgehoben, für die die Verbrechensbekämpfung eine Frage der Ideologie war: Der „Volkskörper" musste von jeglichem subversiven, korrumpieren-

422 *Heinrich,* Innere Sicherheit und neue Informations- und Kommunikationstechnologien, S. 132 f.

423 *Wagner,* Volksgemeinschaft ohne Verbrecher, S. 87 ff.

424 Siehe *Heinrich,* Innere Sicherheit und neue Informations- und Kommunikationstechnologien, S. 134 f. mwN.

den Einfluss, zu dem unter anderem Verbrecher und Kriminalität gehörten, gesäubert werden – die Ermittler wurden zu „Ärzten am Volkskörper" stilisiert, die die faulen Stellen herausschneiden.[425] Auch wenn es sich hierbei um eine übertriebene Formulierung zu ideologischen Zwecken handelte, fiel der Plan der Nationalsozialisten, die Polizei selbst effektiver zu organisieren und die Berufskriminalität strenger zu bekämpfen, in allen deutschen Polizeidienststellen auf fruchtbaren Boden, da viele der Meinung waren, dass nur die politischen Realitäten der Weimarer Republik und ihr nachsichtiger Umgang mit der Kriminalität die Ausrottung der Kriminalität behindert hatten.[426] So wurde zwischen 1936 und 1939 mit dem Reichskriminalpolizeiamt eine zentrale Polizeibehörde geschaffen, die einen wesentlichen Schritt für die Zentralisierung und Vernetzung der gesamten deutschen Kriminalpolizei und für das Vorgehen der Nationalsozialisten gegen die Kriminalität bildete.

D. „Totale Erfassung" im Dritten Reich: Strukturelle Kontinuität und ideologischer Exzess

Die nunmehr auch institutionell vollzogene Zentralisierung der Polizei war jedoch nicht der einzige Aspekt, der sich in Bezug auf die polizeiliche Informationspraxis im Dritten Reich veränderte. Mit der Machtergreifung der Nationalsozialisten im Jahr 1933 wurde „die totalitäre Versuchung als Ausweg aus den Widersprüchen und Handlungsblockaden des Modernisierungsprozesses"[427] immer verlockender für große Teile der deutschen Gesellschaft, einschließlich der meisten ihrer Polizisten. Innerhalb der Polizeiführung verband sich die Vorstellung von Kriminalität als technisch lösbarem Problem mit der absoluten ideologischen Notwendigkeit, Kriminalität als soziales Phänomen endgültig zu beseitigen, wie es Teil der Staatsraison des NS-Staates war: eine „Volksgemeinschaftsutopie", die auf die Bildung „einer ideologisch homogenen, sozial angepassten, leistungsorientierten und hierarchisch gegliederten Gesellschaft mit den Mitteln der Erziehung der „gut Gearteten" und der „Ausmerze" der vermeintlich „Ungearteten" abzielte.[428] Diese Verschmelzung von polizeilicher Kriminalitätsbekämpfung

425 *Wagner,* Volksgemeinschaft ohne Verbrecher, S. 9.
426 *Wagner,* Volksgemeinschaft ohne Verbrecher, S. 188 ff., 227.
427 *Peukert,* Die Weimarer Republik, S. 237.
428 *Peukert,* Volksgenossen und Gemeinschaftsfremde, 262 ff.

und nationalsozialistischer Ideologie zu einem kriminalpolitischen Projekt erforderte im Grunde kein radikales Umdenken. Denn dem Konzept des Berufsverbrechertums wohnte bereits ein gewisses Entgrenzungspotenzial inne.[429] Wie bereits dargelegt, wurde schon in der Weimarer Republik ein stringenteres Vorgehen gegen diese als ernstzunehmende Bedrohung konstruierte kriminelle Subkultur gefordert. Dieses Projekt konnte im Dritten Reich Anschluss finden, erforderte aber für seine Umsetzung eine Entfesselung polizeilicher Informationsarbeit.

Wie in allen totalitären Regimen war das Sammeln, Speichern, Sortieren und Auswerten von Daten über die Gesellschaft im Dritten Reich nicht alleinige Aufgabe der deutschen Polizeibehörden, sondern ein gesamtstaatliches Unterfangen: Neben den Polizeibehörden[430] waren auch die Gesundheits- und Sozialverwaltung sowie das Statistische Reichsamt Teil der Informationsmaschinerie, die ein Maximum an Wissen über alle Menschen unter deutschem Einfluss gewinnen wollte. So entstand nach 1933 in wenigen Jahren ein weit verzweigtes „bizarres und zugleich effizientes System" aus verschiedenen Karteien, Zählungen, Meldegesetzen und Kennkarten. Es diente der totalen Erfassung und Klassifizierung der Bevölkerung. Selbst für diejenigen, die als „deutschblütig" eingestuft wurden, galt eine Kategorisierung: Sie waren entweder „hochstehend" oder „hochwertig", „durchschnittlich", „tragbar und tiefstehend bzw. minderwertig".[431] Verschiedene Informationssammlungen bildeten die bürokratische Voraussetzung für ein abgestuftes System von Belohnung und Bestrafung, von Selektion und Vernichtung. Es gab „Asozialenkarteien", Sonderregister für Juden, „Zigeuner" und sonstige „Fremdvölkische".[432] Auch diejenigen, die als erbkrank galten, wurden in Kategorien eingeteilt.[433] Die deutsche Polizei war zwar nicht die einzige Akteurin bei diesen Bemühungen, aber dennoch dominant und effektiv, vor allem aufgrund des rechtlichen Status, der das Recht zur Gewaltanwendung mit sich brachte und der mit dem Fortschreiten des Dritten Reichs immer grenzenloser wurde.

Eines der ersten Datenerhebungsprojekte unter federführender Mitarbeit der Polizei war die sogenannte „Zigeunererfassung", die ab 1936 in Zusam-

429 *Wagner,* Volksgemeinschaft ohne Verbrecher, S. 146.
430 Die nationalsozialistische Polizei teilte sich auf in die uniformierte Ordnungspolizei und die Sicherheitspolizei, die sich wiederum teilte in Kriminalpolizei und Geheime Staatspolizei.
431 *Aly/K. Roth,* Die restlose Erfassung, S. 12.
432 *Aly/K. Roth,* Die restlose Erfassung, S. 12.
433 *Aly/K. Roth,* Die restlose Erfassung, S. 12.

menarbeit zwischen Kriminalpolizei und der Geheimen Staatspolizei, der Gestapo, durchgeführt wurde.[434] Gemeinsam mit der „Rassenhygienischen und bevölkerungsbiologischen Forschungsstelle" im Reichsgesundheitsministerium waren die Polizeibehörden aktiv damit beschäftigt, Sint:izze und Roma:nja zu registrieren und sie „rassenbiologisch" einzustufen. Die polizeiliche Hilfe bei diesem Unterfangen war besonders fruchtbar, weil die sogenannte „Zigeunerbekämpfung" schon vor der Machtergreifung der Nationalsozialisten eine institutionalisierte Aufgabe der deutschen Polizeidienststellen war, auch wenn diese Bemühungen eher marginal waren.[435] Doch mit der Zentralisierung des polizeilichen Nachrichtenwesens und der Macht im Dritten Reich wurde das „Zigeunertum" auch auf höchster Ebene des Reiches zu einem Thema mit Priorität.[436] Bis 1941 hatte das Reichskriminalpolizeiamt zusammen mit dem Gesundheitsministerium etwa 30.000 Menschen entsprechend registriert, was Vorbedingung für die spätere Ermordung der Sinti:zze und Rom:nja durch das Regime war.[437]

Diese in ihren Wirkungen tödlichen Datensammlungen wurde durch die informationelle Erfassung der jüdischen Bevölkerung noch überschattet. Offiziell hatte diese mit der Machtergreifung der Nationalsozialisten begonnen und wurde mit größter Akribie betrieben. Ausgangspunkt für diese Bemühungen war die „Judenstatistik" von 1933, in der zunächst Religionszugehörigkeit und Wohnort erfasst wurden. Diese Erkundung der jüdischen Bevölkerung wurde 1935 mit der Abfrage der „jüdischen Abstammung", also der staatlichen Erfassung der jüdischen Familienstrukturen, weiter verschärft. Wie es für die Nationalsozialisten typisch war, sollte das Wissen über die Bevölkerung in Deutschland allumfassend sein. Vor allem in den letzten beiden Jahren vor dem Zweiten Weltkrieg bauten die Nazis eine hocheffektive Maschinerie zur sozialen Sortierung auf: Eine allgemeine Volkszählung im Jahr 1938 zielte darauf ab, die „blutmäßige Zusammensetzung"[438] – also die ideologische Kategorie der „Rasse" – der deutschen Bevölkerung aufzuschlüsseln. Ergänzt wurde dieses Projekt durch die Volkskartei, ein zentrales Register für alle von den deutschen Behörden gesammelten Informationen über die Bevölkerung. Die Volkskartei

434 *Aly/K. Roth,* Die restlose Erfassung, S. 13.
435 *Zimmermann*, Die nationalsozialistische Verfolgung Hamburger Roma und Sinti, 9 (11 ff.).
436 *Wagner,* Volksgemeinschaft ohne Verbrecher, S. 238.
437 *Wagner,* Volksgemeinschaft ohne Verbrecher, S. 274.
438 Zitiert nach *Aly/K. Roth,* Die restlose Erfassung, S. 94.

wurde im Wesentlichen von der Ordnungspolizei, der die Kriminalpolizei ergänzende Behörde, verwaltet. Neben den Daten, die bereits durch die vielen Informationssammlungen des Staates zur Verfügung standen, waren die Polizeidienststellen auch verpflichtet, jede Interaktion mit Bürger:innen für eine informatorische Aktualisierung der Daten über die jeweilige Person zu nutzen. Das Register wurde so zu einem virtuellen Spiegelbild der Bevölkerung, in dem die Bewegungen und registrierungswürdigen Handlungen von Personen aufgezeichnet und zusammen mit deren Fotos, Fingerabdrücken und Handschriftproben auf Karteikarten gespeichert wurden. Auf diese Weise entstand – auch wenn die Volkskartei kriegsbedingt nie vervollständigt wurde – ein engmaschiges Netz der informationellen Überwachung über Millionen von Deutschen mit spezifischem gruppenspezifischem Wissen in der Hand der Polizeibehörden.[439]

Dort traf sie erneut auf die Vorstellung eines quasi-technischen Lösungsansatzes für die Kriminalität, der nun mit ideologischen Vorstellungen verwoben war. Paul Werner, eine Schlüsselfigur des NS-Sicherheitsapparates, verkündete 1942 in der führenden strafrechtlichen Zeitschrift des Landes: „Der Kriminalpolizeistelle obliegt die Bekämpfung jedes kriminellen Staatsfeindes“[440] und erklärte damit Kriminelle zu politischen Feinden und ihre „Ausrottung“ zur Staatsraison. Bereits um 1933 sahen sich deutsche Kriminalisten „befähigt und [...] berechtigt“ […] zu einer Prognose“ über das künftige Verhalten eines Verdächtigen und stützten sich dabei auf ihr persönliches Wissen sowie auf die Fülle von Daten in ihren Informationssammlungen, auch wenn die betreffende Person noch keine Straftaten begangen hatte.[441] Darin lag zum einen eine Fortführung des Heindlschen Konzepts der „Berufsverbrecher“, zum anderen aber auch eine kriminalpolitische Erweiterung, die das Konzept der gruppenbezogenen Erklärung von Kriminalität auf verschiedene Gruppen übertrug, die durch eine Mischung aus polizeilichem Wissen und nationalsozialistischer Ideologie definiert und konstruiert wurden. Der Leiter der Ordnungspolizei, *Karl Daluege*, sah 1935 in der Kriminalpolizei die Institution, die „das Verbrechertum in seiner Gesamtheit […], und zwar nicht aufgrund neuer bestimmter Einzeltaten seiner Mitglieder, sondern wegen ihrer durch ihren Lebenslauf erwiesenen bewußt asozialen Lebensführung“ bekämpfen soll-

439 *Aly/K. Roth,* Die restlose Erfassung, S. 49 ff.
440 *P. Werner* Zeitschrift für die gesamte Strafrechtswissenschaft 61 (1942), 465 (469).
441 Zitiert nach *Wagner,* Volksgemeinschaft ohne Verbrecher, S. 200.

te.[442] Der nationalsozialistische Begriff „Asoziale" überschnitt sich zwar mit dem Begriff „Berufsverbrecher", umfasste aber bald alle Arten von Menschen, die die Nationalsozialisten für sozial untauglich hielten. Ein „Asozialer" war nach einem Erlass des Reichskriminalpolizeiamtes aus dem Jahr 1937 jede:r, der oder die, „ohne Berufs- oder Gewohnheitsverbrecher zu sein, durch sein asoziales Verhalten die Allgemeinheit gefährdet". Diese vage Definition wurde 1938 etwas eingegrenzt auf „Bettler, Landstreicher (Zigeuner), Dirnen, Trunksüchtige, mit ansteckenden Krankheiten, insbesondere Geschlechtskrankheiten behaftete Personen, die sich den Maßnahmen der Gesundheitsbehörden entziehen", und „Arbeitsscheue"; eine Definition, bei der es sich allerdings ausdrücklich nur um eine beispielhafte Aufzählung handelte.[443] Personen, die in die flexible Kategorie der „Asozialen" fielen, wurden einem zunehmend intensiveren Programm zur Verbrechensbekämpfung und -prävention unterworfen, das sich insbesondere auf umfassende Überwachung und Präventivhaft stützte, wobei letztere immer häufiger angewandt wurde, da es in den Augen der Polizeiführung effizienter war, Abweichler einfach dem System der Konzentrationslager zu überantworten, als beträchtliche Ressourcen in die ständige Überwachung zu investieren.[444] *Wagner* fasst das Programm gegen „Asoziale" treffend zusammen: „Im Kern ging es – neben der Vernichtung politischer Gegner und ethnisch als nicht-deutsch klassifizierter Menschen – um die Durchsetzung der klassischen Inhalte bürgerlicher Sozialdisziplinierung, freilich in bis dato einmaliger terroristischen Form und unter Ausweitung auf noch die unbedeutendste Form der Devianz."[445] Ab 1938 bestand die Mehrheit der KZ-Häftlinge, die von der Kriminalpolizei deportiert wurden, aus Personen, die zuvor als „asozial" eingestuft worden waren.[446]

Eine letzte Eskalation der nationalsozialistischen Kriminalpolitik erfolgte in den letzten Jahren der nationalsozialistischen Herrschaft, als sogenannte Kriminalbiologen sicher waren, erbliche Ursachen für das Auftreten von kriminellem Verhalten bei Individuen identifizieren zu können.[447] Dies erforderte noch einmal mehr Daten über all jene, die im Dritten Reich als kriminell galten. Bereits 1934 war für die „allgemeine Gesund-

442 *Daluege* Deutsche Justiz 97 (1935), 1846 (1846).
443 Zitiert nach *Wagner,* Volksgemeinschaft ohne Verbrecher, S. 261.
444 *Wagner,* Volksgemeinschaft ohne Verbrecher, S. 254 ff.
445 *Wagner,* Volksgemeinschaft ohne Verbrecher, S. 263.
446 *Wagner,* Volksgemeinschaft ohne Verbrecher, S. 13.
447 *Wagner,* Volksgemeinschaft ohne Verbrecher, S. 267 ff.

heitsüberwachung des Lebens“ ein zentrales Gesundheitspassarchiv eingerichtet worden, das Daten aus den verschiedensten Institutionen erfasste, darunter auch Verurteilungen in Strafprozessen, „lückenlos, soweit es sich um Rauschgiftsachen, Gewohnheitsverbrecher oder überhaupt um solche Urteile handelt, in denen eingehende Persönlichkeitswertungen vorkommen“.[448] Dies reichte jedoch nicht aus, da man davon ausging, dass die schlechten Vererbungseigenschaften aller Kriminellen überwiegend genotypisch bei „Asozialen“ auftraten, im Gegensatz zum überwiegend phänotypischen Auftreten bei „Berufsverbrechern“. Dies bedeutete, dass „kontaminierte“ Genotypen durch Datenerhebungen insbesondere über Familienstrukturen – wie sie zuvor an der jüdischen Bevölkerung praktiziert worden waren – identifiziert werden mussten, um die genotypisch „Kranken“ zu identifizieren und dann mit verschiedenen Mitteln „ausmerzen“ zu können.[449]

Wozu die polizeiliche Wissensanhäufung von 1933-1945 führte, ist bekannt: All diese Anstrengungen zum informationellen Durchdringen der Gesellschaft wurden als Grundlage für die Entscheidungen über die Deportationen in die Vernichtungs- und Arbeitslager genutzt.[450] Diese Polizeipraktiken wurden auch in den besetzten Gebieten angewandt: Wo immer die Wehrmacht vorrückte, folgten Polizeikräfte, „um zu erfassen, zu zählen, zu trennen“.[451] Es ist kaum vorstellbar, dass das Ausmaß der nationalsozialistischen Gräueltaten ohne dieses strukturierte Vorgehen bei der Informationsbeschaffung möglich gewesen wäre. Diese Verbindung von bürokratischer Akribie und wahnhafter Ideologie ist dabei typisch für die rationale Irrationalität von Staat und Gesellschaft unter dem Nationalsozialismus.

Das Ende des Krieges und des Dritten Reiches hinterließ Millionen von Toten in den Händen des sicherheitsbehördlich gestützten Vernichtungsapparates, eine Zahl, die wahrscheinlich noch höher gewesen wäre, wenn die Nazis den Krieg nicht verloren hätten: Gegen 1945 verlangsamte sich der polizeiliche Nachrichtendienst kontinuierlich, aber er hörte nie wirklich auf, diejenigen zu erfassen, die nach ihrer „Gesamtpersönlichkeit nicht in der Lage [sind], den Mindestanforderungen der Volksgemeinschaft an [ihr] persönliches, soziales und völkisches Verhalten zu genügen“ – also

448 Zitiert nach *Aly/K. Roth,* Die restlose Erfassung, S. 119.
449 Vgl. zu diesem "rassenbiologischen" Gedankengebäude *Wagner,* Volksgemeinschaft ohne Verbrecher, S. 277 ff.
450 *Murphy,* God's jury, S. 204.
451 *Aly/K. Roth,* Die restlose Erfassung, S. 96.

praktisch alle, die sich nicht an die Normen der nationalsozialistischen Gesellschaft hielten.[452] Es scheint wahrscheinlich, dass die Kriminalpolizei „konkrete Vorbereitungen traf, um nach dem Krieg eine kriminalbiologische Rassenpolitik massenmörderischen Umfangs ins Werk zu setzen".[453] Diese Politik hätte – nach Berechnungen der NS-Kriminalbiologen *Koller* und *Kranz* – etwa 1,6 Millionen Menschen betreffen können.[454] *Ritter*, ein führender nationalsozialistischer Rassentheoretiker, der für die Identifizierung und Erfassung der Sint:izze und Rom:nja verantwortlich war, schwebte darüber hinaus die durchdringendste Form der sozialen Überwachung vor: Ein lückenloses kriminalbiologisches Datennetz, das es ermöglichen würde, „den Stellen, denen die vorbeugende Verbrechensbekämpfung obliegt, jederzeit zu melden, wann und wo Menschen heranwachsen, die [...] einer Sondererziehung, einer unauffälligen vorsorglichen Beobachtung, einer Schutzaufsicht oder gar einer halboffenen bzw. einer geschlossenen Bewahrung bedürfen".[455]

Auch wenn vor allem der ideologische Überbau der NS-Kriminalpolitik und ihrer Umsetzung als Bruch gegenüber der Weimarer Zeit erscheint, so ist das für Entwicklungen des polizeilichen Informationswesens grundsätzlich nicht zu konstatieren. Zwar war es ein Anliegen der für den Sicherheitsapparat verantwortlichen Entscheidungsträger, die Polizei unter anderem auch informationell zweckrational zu optimieren, wodurch es zu organisatorischen und auch technischen Neuerungen kam. Insgesamt wurde dabei jedoch viel an bereits bestehende Entwicklungen angeknüpft, sodass sich im Bereich der Informationstechnologie und auch der Informationspraktiken durchaus eher von Kontinuitäten sprechen lässt.[456]

E. Elektronisierung

Während es auch in den ersten Polizeigenerationen der Bundesrepublik Deutschland[457] einige, vor allem personelle, Kontinuitäten gab, hatte die

452 Zitiert nach *Aly/K. Roth,* Die restlose Erfassung, S. 124.
453 *Wagner,* Volksgemeinschaft ohne Verbrecher, S. 375.
454 *Aly/K. Roth,* Die restlose Erfassung, S. 123.
455 Zitiert nach *Wagner,* Volksgemeinschaft ohne Verbrecher, S. 378.
456 *Heinrich,* Innere Sicherheit und neue Informations- und Kommunikationstechnologien, S. 124 f.
457 Auch in der Deutschen Demokratischen Republik hat es selbstverständlich eine relevante Entwicklung polizeilicher Datenverarbeitung in den Nachkriegsjahrzehn-

nationalsozialistische Ideologie in den zentralen Polizeieinrichtungen des jungen westdeutschen Staates keinen Bestand.[458] Als Ideologie entwickelte die deutsche Polizei ab den 1960er Jahren vielmehr eine technikutopische Vision der technologiegestützten Verbrechensbekämpfung. Kontinuität gab es hingegen in der Struktur des polizeilichen Informationswesens, auch wenn hier breite Umstrukturierungen vonseiten der Siegermächte vorgenommen wurde. Allerdings waren Prinzipien wie Zentralisierung und sonstige organisatorische wie technische Rationalisierung der Informationsverarbeitung mittlerweile polizeiinstitutionelle Rationalitäten geworden. In der deutschen Nachkriegsgesellschaft wird diese Dynamik ab den 1960er Jahren zudem durch den Prozess der Elektronisierung weiter intensiviert. Diese Entwicklung ist im damaligen Westdeutschland untrennbar mit dem Bundeskriminalamt verbunden.

Während der institutionelle Rahmen für die Polizei auf der Idee der Dezentralisierung als Barriere gegen ein Wiederaufleben des Totalitarismus basierte, wurde bald deutlich, dass das polizeiliche Informationswesen nicht optimal funktionieren würde, wenn es dezentralisiert und daher fragmentiert bliebe. In der Folge kam es 1951 zur Gründung des Bundeskriminalamtes, im Wesentlichen der konzeptionelle Nachfolger des Reichskriminalpolizeiamtes, zumindest was die Aufgabe als Zentralstelle für das polizeiliche Informationswesen betraf: Es sollte nur sehr wenige exekutive Funktionen haben und war nicht als kriminalpolizeiliche Ermittlungsbehörde konzipiert. Seine Rolle war die eines Moderators der Zusammenarbeit im föderalen Polizeisystem Westdeutschlands, insbesondere in informationeller Kapazität, indem es in erster Linie Kriminalitätsentwicklungen analysierte und den Informationsaustausch zu schwereren Straftaten zwischen den Länderpolizeien unterstützte.[459]

---

ten gegeben. Zur Wende wurde jedoch die Informationstechnologie der Polizeien in den neuen Bundesländern praktisch von Grund auf erneuert oder aufgebaut, vgl. *Heinrich,* Innere Sicherheit und neue Informations- und Kommunikationstechnologien, S. 205. Das polizeiliche Informationswesen der DDR lebt mithin nicht in der heutigen Informationsarchitektur der Bundesrepublik fort und wird daher hier ausgeklammert.

458 *Wagner* in Bundeskriminalamt (Hrsg.), Der Nationalsozialismus und die Geschichte des BKA, 21 (21); Nichtsdestotrotz wurden bis 1988 offiziell und bis 2001 inoffiziell polizeiliche Nachrichtendienste explizit über Roma betrieben, vgl. *Andrej* in Bundeskriminalamt (Hrsg.), Der Nationalsozialismus und die Geschichte des BKA, 37.

459 *Harnischmacher/Semerak,* Deutsche Polizeigeschichte, S. 193 ff; *Carter* The Police Journal 49 (1976), 199.

Nach seiner Gründung war die Bedeutung des Bundeskriminalamtes für das polizeiliche Informationswesen jedoch zunächst gering geblieben: Die Rolle des Amtes wurde stark auf eine Hilfsfunktion beschränkt und wurde in dieser von den Bundesländern zudem als langsam, ineffektiv und wenig gewinnbringend wahrgenommen, was ihm den Ruf eines Aktengrabes einbrachte.[460] Dieses Urteil war indessen nicht auf das Bundeskriminalamt als institutionelle Verkörperung des polizeilichen Informationswesens auf Bundesebene beschränkt, sondern erstreckte sich auch auf den KPMD als auch nach dem Krieg weiterhin – gemeinsam mit den erkennungsdienstlichen Sammlungen – bestehendes Zentrum der überregionalen Informationsarchitektur. Der Meldedienst hatte immer noch dieselben Probleme, die er bereits seit seiner Einführung mit sich trug. Ein hohes Datenaufkommen konnte von den informationstechnologischen Strukturen und den im Rahmen des KPMD entwickelten Informationspraktiken nicht ausreichend verarbeitet werden – oder zumindest nicht so, dass ein Mehrwehrt für die polizeiliche Arbeit entstand. So gab es einerseits das Problem der mangelhaften Informationsqualität, die im Wesentlichen auf den fehlenden Professionalisierungsgrad der mit der Erfassung betrauten Beamten zurückgeführt wurde, wobei auch die auswertenden Beamten mitunter Ziel dieser Kritik wurden. Daneben war auch die formelle Systematisierung des KPMD nicht optimal: Die Formulare waren zu sehr standardisiert worden, sodass die Besonderheiten der Straftaten, also der nach wie vor relevante Modus Operandi, nicht hinreichend präzise erfasst wurden. Auch war die technische Umsetzung etwa in Form des Karteiwesens mangelhaft.[461] Der Ausweg wurde auch hier in der weiteren (informations-)technologischen Rationalisierung des KPMD-Verfahrens gesucht. In der Folge wurden erste Gehversuche in der sogenannten Automatischen und der Elektronischen Datenverarbeitung unternommen. Probleme bestanden dabei unter anderem in der Umwandlung weicher Daten, etwa über soziale Interaktionen und Prozesse, in elektronisch lesbare Formen, was aufgrund der hohen Bedeutung dieser Daten für die (kriminal-)polizeiliche Arbeit so essenziell wie anforderungsreich war.[462] Bereits im Kontext dieser frühen Elektronisierung polizeilicher Arbeitsmittel wurden auch technologiekritische Stimmen laut, die die Zweckmäßigkeit der neuen Systeme und Verfahren

460 *Mangold,* Fahndung nach dem Raster, S. 140.

461 Siehe zum KPMD in den 50er- und 60er-Jahren auch mwN *Heinrich,* Innere Sicherheit und neue Informations- und Kommunikationstechnologien, S. 145 ff.

462 *Reuter* Die Polizei 56 (1965), 265.

hinterfragten. Menschliche Intelligenz und polizeiliche Erfahrung wurden wichtigere und durch die Technik nur zu unterstützende, nicht aber zu ersetzende Größen in Stellung gebracht.[463] Trotz der Bemühungen um die informationstechnologische Evolution der deutschen Polizeien, die seit den 1950er-Jahren – wenn auch unkoordiniert – liefen, kam es vermehrt zu öffentlicher und auch interner Kritik wegen des als mangelhaft empfundenen technologischen Entwicklungsstandes. Einen Kumulationspunkt dieser Kritik am Zustand eines Großteils der westdeutschen Polizeien und auch des Bundeskriminalamts wurde – wie *Mangold* herausgearbeitet hat – ab 1965 erreicht, als überregionale Presse den Fall *Bruno Fabeyer* aufgriff. *Fabeyer*, ein gesuchter (Polizisten-)Mörder, konnte durch Pannen bei der Fahndung der Polizei entkommen und wurde erst ein Jahr später gefasst. Vor dem Hintergrund dieses Falles und der aufkommenden Elektronisierung der Datenverarbeitung wurden die deutsche Polizei und insbesondere das Bundeskriminalamt als technologisch überholte Institutionen wahrgenommen.[464] Die Kritik erstreckte sich sowohl auf die mediale Seite der Informationsverarbeitung – also auf papierne Akten und Karteikarten – als auch auf konzeptionelle Aspekte der polizeilichen Bearbeitung von Kriminalität. So geriet die Perseveranz-Hypothese – die Vorstellung, dass Täter:innen in ihrem jeweiligen Deliktsbereich verharren und immer die gleichen oder einigermaßen ähnliche Mittel anwenden würden – zunehmend in die Kritik. Von dieser ordnenden Vorstellung abzurücken, rief indessen ebenso Widerstände hervor, da sie engmaschig mit der Struktur ihre Informationssammlungen verbunden war, die die Polizei in den vergangenen Jahrzehnten über Personen angelegt hatte. Da den Kriminalisten jedoch klar geworden war, dass die Hypothese nur bedingt realitätsgetreu war, wurde sie flexibilisiert: Man hielt es nun für möglich und sogar für plausibel, dass die Täter:innen von Zeit zu Zeit ihren Modus Operandi änderten. Das machte die Perseveranz als Definitionsbegriff für einen bestimmten Täter:innen- und Deliktstypus allerdings weniger brauchbar und führte zu einer Ausdifferenzierung der Erfassungsmodalitäten und befeuerte so eine noch stärkere Ausweitung der Akten des KPMD. Nun konnten die Register nur noch über anspruchsvolle Abfragen genutzt werden.[465] Polizeiliche Informationsverarbeitung, so die damalige Wahrnehmung, be-

463 *Heinrich,* Innere Sicherheit und neue Informations- und Kommunikationstechnologien, S. 151 f. mwN.
464 *Mangold,* Fahndung nach dem Raster, S. 29 ff.
465 *Mangold,* Fahndung nach dem Raster, S. 67 ff.

stand nur noch darin „Papier zu bewegen“,[466] während die Polizei in der Flut der unzureichend strukturierten Informationen zu ertrinken schien.[467]

Nachdem die elektronische Datenverarbeitung also bereits in einigen regionalen Polizeiorganisationen – gewissermaßen graswurzelmäßig als von „unten“ angestoßene Entwicklung – als neuer Rahmen für die Sammlung, Verarbeitung und Verbreitung von Informationen eingeführt worden war, wurde diese Entwicklung ab Ende der 1960er-Jahre auch im Bundeskriminalamt aufgenommen und in den 1970er-Jahren stark intensiviert. Dies lag zum einen daran, dass der dezentrale Ansatz der elektronischen Datenverarbeitung nach Ansicht der Zentralisierungsbefürworter die Gefahr einer „informationelle[n] Fragmentierung“[468] der polizeilichen Aufklärung barg. Positiv gewendet beförderte eine Elektronisierung der Datenverarbeitung eine Zentralisierung, weil die technologische Struktur die organisatorische Struktur bedingt. Zentrale Main-Frame-Rechner mit Terminalverbindungen an der Peripherie erfordern eine zentrale Organisation mit zentraler Datenhaltung,[469] kurzum: „Computereinsatz bedeutet Zentralisierung.“[470] Die seit den 1960ern gewachsenen Anwendungen der elektronischen Datenverarbeitung bei den deutschen Polizeien hatten jedoch zu einem sehr heterogenen Informatisierungsgrad geführt, was zunehmend als Problem begriffen wurde.[471] Zum anderen übernahm mit *Horst Herold* ab 1971 ein überzeugter Befürworter von Elektronisierung und Zentralisierung für ein Jahrzehnt die Leitung des Bundeskriminalamtes.[472] *Herold* hatte, inspiriert von der Kybernetikeuphorie seiner Zeit, während er Nürnberger Polizeipräsident gewesen war, mit dem Konzept der sogenannten Kriminalgeographie experimentiert, das die flexible elektronische Berechnung von Kriminalitätsschwerpunkten im Zuständigkeitsbereich der Polizei auf der Grundlage vorhandener polizeilicher Daten beinhaltete,[473] was bereits Ähnlichkeit

466 *Kollecker* Kriminalistik 16 (1962), 49-53; 154-156 (49).
467 *Mangold,* Fahndung nach dem Raster, S. 68.
468 Zitiert nach *Bergien* Zeithistorische Forschungen/Studies in Contemporary History 258-285 14 (2017), 258 (265).
469 *Heinrich,* Innere Sicherheit und neue Informations- und Kommunikationstechnologien, S. 152.
470 *Hörath* Die Polizei 58 (1967), 129 (131).
471 *Heinrich,* Innere Sicherheit und neue Informations- und Kommunikationstechnologien, S. 165.
472 *Bergien* Zeithistorische Forschungen/Studies in Contemporary History 258-285 14 (2017), 258 (264 ff.).
473 *Mangold,* Fahndung nach dem Raster, S. 82.

mit dem heutigen raumbezogenen Predictive Policing aufwies.[474] In seinen ersten Jahren im Bundeskriminalamt knüpfte *Herold* an seine Nürnberger Konzepte der informationstechnisch fundierten Verbrechensbekämpfung an und setzte (ohne gesetzliche Grundlage)[475] die bereits geplante Zentralisierung der polizeilichen Datenverarbeitung in Form des ersten polizeilichen Informationsverbundsystems „INPOL" im Jahr 1972 um. Es sollte die „mangelnde Aktualität der Fahndungsmittel (Fahndungsbücher und Karteien) sowie Schwierigkeiten beim Auskunftsbetrieb aufgrund konventioneller Informationssammlungen" – gemeint waren die unübersichtlichen Papierakten und Karteien – beheben, die durch die „gestiegene Mobilität der Täter" verursacht wurden.[476] Dazu wurde ein sternförmig organisiertes Verbundsystem mit den Landeskriminalämtern an der Peripherie und dem Bundeskriminalamt im Zentrum geschaffen. Da zunächst nur begrenzte Polizeiaufgaben – zu Beginn die Personenfahndung – vom Verbund bewältigt werden sollten, bestand für die Länder weiterhin die auch genutzte Möglichkeit eigene Informatisierungsprojekte voranzubringen, was die Heterogenität des polizeilichen Informationswesens in seiner Gesamtheit weiter förderte.[477] Nachdem INPOL noch einige Zeit fortentwickelt werden musste, konnten die an INPOL teilnehmenden Polizeien ab 1974 Daten online an den Zentralrechner des Bundeskriminalamtes übertragen, von wo aus sie dann von etwa 500 Terminals im Bundesgebiet abgerufen werden konnten. Dies führte zu einer merklichen Verbesserung der Kontrollintensität in Form eines um 50 Prozent erhöhten Fahndungserfolg.[478] Mit Einführung der neuen Technik war auch die Idee einer sich ändernden polizeilichen Informationspraxis verbunden, die dahin gehen sollte, möglichst alle kontrollierten Personen mit dem Fahndungsbestand abzugleichen.[479]

Wie *Mangold* anschaulich beschrieben hat, begann die Elektronisierung der Informationsverarbeitung in dieser Zeit aber auch wichtiger zu werden,

474 Siehe zu solchen Frühformen von geografischen Visualisierungen des Kriminalitätsaufkommens auch *Brayne,* Predict and surveil, S. 18 f.

475 Eine solche wurde damals nicht für erforderlich gehalten, siehe *Bäumler* in *Lisken/Denninger* (Hrsg.), Handbuch des Polizeirechts, J. Rn. 151.

476 Zitiert nach *Mangold,* Fahndung nach dem Raster, S. 118.

477 *Heinrich,* Innere Sicherheit und neue Informations- und Kommunikationstechnologien, S. 167.

478 *Heinrich,* Innere Sicherheit und neue Informations- und Kommunikationstechnologien, S. 169.

479 *Heinrich,* Innere Sicherheit und neue Informations- und Kommunikationstechnologien, S. 173.

da sie mit einer neuen Art des kriminalistisch zu erfassenden Gegenübers konfrontiert war: den Terrorist:innen. Neben dem Umstand, dass sich das Konzept des persistenten „Berufsverbrechers" als zunehmend unzureichend für die polizeiliche Informationsarbeit herausgestellt hatte, stellte auch die innere Sicherheitslage der Gesellschaft ab den Siebzigern die Polizei vor bis dahin unbekannte Herausforderungen, die ein Umdenken erforderten: Fast zeitgleich mit dem Ausbau der technischen Informatisierung der Polizei hatte der Terror der Roten Armee Fraktion (RAF) begonnen.[480] Anders als das Konzept des „Berufsverbrechers", das die Vorstellung von greifbaren Täter:innen bot, waren (und sind) Terrorist:innen vor allem deshalb ein Ermittlungsproblem, weil sie im gesellschaftlichen Treiben nur flüchtig sichtbar wurden. Mobilität und Konspiration machten sie zu einem schwierigen Ziel und je mehr sich die Terrorist:innen der RAF in die Gesellschaft einfügten, desto unwahrscheinlicher wurde es, dass für die polizeilichen Ermittlungen relevante Informationen im ohnehin trägen und papiernen polizeilichen Informationswesen enthalten waren. Die Identifizierung der Terrorist:innen erforderte vielmehr, das soziale Gewebe der Gesellschaft nach Auffälligkeiten mit polizeilichem Informationswert zu durchkämmen. Nicht mehr die einzelne Person oder Tat war vorrangig ermittlungsleitend. In den Fokus rückten nunmehr die sozialen Interaktionen und Prozesse, die netzwerkartig mit Personen und Delikten verbunden waren. Statt klarer segregierter personen- oder deliktsbezogener Informationssammlungen konstruierten die westdeutschen Kriminalisten im Kampf gegen die RAF mithilfe elektronischer Informationssystemen datenbasierte Ermittlungskomplexe, die sich vor allem durch informationelle Offenheit auszeichneten, so dass der kontinuierliche Informationsfluss, den die Elektronisierung erheblich beschleunigt hatte, von den Ermittlungsbehörden besser eingebunden und genutzt werden konnte.[481] Zur Operationalisierung dieses

480 *Mangold,* Fahndung nach dem Raster, S. 15.

481 Interessant ist in diesem Zusammenhang auch die Überlegung, dass es von der Art der organisationalen und informationstechnischen Strukturierung von Ermittlungseinheiten abhängt, wie das „polizeiliche Gegenüber" wahrgenommen wird. So schreiben *Von Knickermeier und Lampe*, dass sich bezogen auf organisierte Kriminalität feststellen lässt, „dass die Wahrnemung der Beschaffenheit von Täterinnen- und Täterstrukturen sich (mitunter) nicht nur nach der tatsächlichen Beschaffenheit dieser Strukturen richtet, sondern von der Art der Organisationseinheit abhängt, in der die jeweiligen Beamtinnen und Beamten arbeiten: „Beamtinnen und Beamte, die fallübergreifend täterinnen- und täterorientiert ermittelten und so „das Gegenüber in Form einer ‚Ganzheitsbetrachtung', wahrnahmen, tendierten dahin, lose Straftäterinnen- und -täterverflechtungen zu beschreiben, während Be-

Konzepts wurde eine Datenbank geschaffen, in der Daten zu terrorismusrelevanten Personen, Institutionen und mobilen sowie immobilen Objekten digital erfasst und umfassend mehrdimensional ausgewertet wurden. Diese sogenannten PIOS-Dateien ermöglichten die zentrale Speicherung und dezentrale Bearbeitung von großen Ermittlungskomplexen und waren durch ihre Struktur besser vor Informationsdefiziten geschützt. In den Dateien konnte schnell und übergreifend nach für die Nutzer jeweils relevanten Einzelheiten gesucht werden. Durch die Möglichkeit, variabel mit Recherchewerkzeugen, Suchwörtern und ihrer logischen Verknüpfung Ermittlungen zu unterstützen, waren Datenumgangsformen bisher unbekannter Art möglich.[482] Auf diese Weise wurde ein sich ständig veränderndes, flexibles Instrumentarium geschaffen, das sich leichter an neue Daten anpassen und zur Erhellung ungeahnter Zusammenhänge genutzt werden konnte.[483] Aus dieser Perspektive war Kriminalität nicht mehr durch eine vorher vermittelte Vorstellung von dem, wonach man suchte, identifizierbar, sondern wurde vielmehr zu einem relativen Muster der Abweichung von einer Norm – einer Norm, die auf der Grundlage des vorliegenden Datensatzes ermittelt werden musste. Dies bedeutete zwar zumindest teilweise einen Fortschritt, da Vorurteile und Stereotypen in der polizeilichen Praxis an Bedeutung verloren, brachte aber auch eine Ausweitung des polizeilichen Blicks auf das soziale Gefüge mit sich, da immer mehr Daten verarbeitet werden konnten, aber auch mussten, um für die laufenden Ermittlungen relevante Erkenntnisse zu gewinnen. Die PIOS-Dateien waren in ihrer Konzeption auf die Erfassung und Speicherung des sozialen Umfeldes und gesellschaftlichen Hintergrundes von Verdächtigen ausgelegt,[484] wie etwa das Beispiel der sogenannten „Sympathisanten" der RAF zeigt.

Ab 1975 wollte die Polizei Licht in diesen „Sympathisantenszene" bringen, weil man glaubte, dass sie aktive RAF-Mitglieder beherberge und neue Terrorist:innen hervorbringe. Da die Polizeibeamten nicht sicher sein konnten, wer wirklich Sympathisant:in war und den Terror aktiv und wissentlich unterstützte, erhöhte diese Strategie die Zahl der Betroffe-

amtinnen und Beamte in Dienststellen mit deliktsspezifischer Zuständigkeit eher eigenständige Organisationen zu erkennen glaubten", vgl. *Lampe/Knickmeier,* Organisierte Kriminalität, S. 13 f.

482 *Heinrich,* Innere Sicherheit und neue Informations- und Kommunikationstechnologien, S. 173.

483 *Mangold,* Fahndung nach dem Raster, S. 131, 135.

484 *Heinrich,* Innere Sicherheit und neue Informations- und Kommunikationstechnologien, S. 173.

nen nochmals enorm. Darüber hinaus interessierte sich die westdeutsche Polizei nicht nur für diejenigen, die einer Straftat verdächtigt wurden, sondern auch für diejenigen, die in Zukunft möglicherweise Straftaten begehen könnten, was einen wichtigen Schritt in Richtung dessen darstellte, was später als präventive Wende bezeichnet wurde.[485] Nicht mehr was geschah, sondern was geschehen könnte, leitete zunehmend das polizeiliche Erkenntnisinteresse. Damit wird auch die beginnende Verschränkung von Repression und Prävention deutlich, die sich zudem generell und nicht nur auf die Terrorismusbekämpfung beschränkt im polizeilichen Aufgabenverständnis niederschlug. Die „breit angelegte, *strategisch durchdachte Bekämpfung des Gesamtkomplexes Kriminalität* im präventiven und repressiven Bereich" macht diese gesetzliche Unterscheidung zunehmend hinfällig und wurde als „fragwürdig, ja falsch" wahrgenommen.[486] *Mangold* beschreibt die fundamentale Veränderung, die dies für die Praxis der polizeilichen Informationsarbeit bedeutete, wie folgt: „Damit der Terrorismus fassbar wurde, bildete die Polizei soziale Verhältnisse in Datenstrukturen ab. Dazu erfasste, isolierte, selektierte, formatierte und strukturierte sie spezifische Informationen. Diesen Prozeduren waren die Kategorien inhärent, mit denen die Kripo ihre Welt kartierte."[487] Dieser Wandel führte zu einer neuen Informationspraxis im Umgang mit der Kriminalität und zu einem neuen Konzept der Kriminalität: Die elektronische Computer- und Datenverarbeitungstechnologie ermöglichte es, weitaus mehr Informationen zu sammeln und frei zu durchsuchen und mit komplexen, vielschichtigen Abfragen zu kombinieren, was es wiederum ermöglichte, Kriminalität als ein multidimensionales und vielschichtiges Phänomen zu begreifen.[488]

Diese informationstechnologisch fundierte Entwicklung begann sich auch in der polizeilichen Bearbeitung von allgemeiner Kriminalität abzuzeichnen. Ebenfalls als INPOL-Erweiterung sollte in den Siebzigern der KPMD auf die sogenannte Straftaten-/Straftäter-Datei (SSD) umgestellt werden, wovon man sich eine erhebliche Verbesserung des bisherigen Meldedienstes versprach. Die SSD beruhte auf der auch trotz ihres Bedeutungswandels nach wie vor präsenten Perseveranzhypothese und sollte die Daten daher nach dem Modus Operandi-Prinzip strukturieren. Mithilfe der elektronischen Datenverarbeitung sollten die enthaltenen Informationen

485 Vgl. etwa *Carvalho,* The preventive turn in criminal law.
486 *Stümper* Kriminalistik 27 (1973), 193 (172), Hervorhebung im Original.
487 *Mangold,* Fahndung nach dem Raster, S. 169.
488 *Mangold,* Fahndung nach dem Raster, S. 181 ff.

besser verknüpft und fall-, merkmals- sowie personenbezogen recherchiert werden können. Da kriminalpolizeiliche relevante Informationen möglichst umfassend erfasst werden sollten, mussten Lebenssachverhalte stark formalisiert in maschinenlesbare Teilaspekte aufgespalten werden, was neue Anforderungen für die Rolle der Kriminalbeamten mit sich brachte: Diese hatten nun Fälle kleinteilig zu analysieren und in die maschinengerechte Sprache der verpflichtenden Begriffskataloge zu bringen.[489]

In den technikutopischen Visionen von *Herold* bedeutete die beschriebene Elektronisierung der polizeilichen Informationsverarbeitung eine grundlegende Neuordnung des gesellschaftlichen Umgangs mit Kriminalität: Durch die Informationssysteme der Polizei könnten „weitreichend Einsichten in das Wesen des Verbrechens und seiner Ursachen" und „in die vielfältigen Wirkungen, Wechselwirkungen und Kausalitätsbeziehungen zwischen den verschiedenen Verbrechensursachen" gewonnen werden.[490] Damit könnte die Polizei eine Rückkopplungsschleife von Datenerhebung und Kriminalitätsbekämpfung etablieren, in der die „analytische und prognostische Beurteilung des Datenmaterials" der Kriminalpolitik zu einer Wandlungsfähigkeit verhilft, mit der sie sich „ohne Verzug aufgrund objektiver Befunde" an die Kriminalität anpassen kann, ähnlich „wie sich die Wirtschaft auf Veränderungen des Marktes einstellt".[491] Um ihr volles Potenzial auszuschöpfen, müsste diese neue Art der Verbrechensbekämpfung – ebenso wie die Wirtschaft – von einer gesellschaftlichen Vormachtstellung ausgehen, in der sich „Gesetz und Recht, Politik und Staat der permanenten Umformung unterwerfen".[492] *Herold* nannte dies die „ gesellschaftssanitär[e] Aufgabe"[493] der Polizei und erinnerte damit an die sozialhygienischen Konzepte der Nationalsozialisten. *Herolds* Vorstellung sind in dieser Form nicht verwirklicht worden, verdeutlichen aber dennoch einen Wendepunkt in der Art und Weise, wie die Polizei ihre informationellen Praktiken und auch ihr gesellschaftliches Funktionsverständnis geändert hatte: Zum einen gab es nicht länger eine klar umrissene Klasse von Kriminellen, die vermessen und erfasst werden musste. Vielmehr konnte

489 *Heinrich,* Innere Sicherheit und neue Informations- und Kommunikationstechnologien, S. 175 f.
490 *Herold* Kriminalistik 28 (1974), 385 (392).
491 Zitiert nach *L. Scholz* in Schröter/Böhnke (Hrsg.), Analog/Digital - Opposition oder Kontinuum?, 97 (106).
492 *Herold* in Deutsche Kriminologische Gesellschaft (Hrsg.), Praevention und Strafrecht, 23 (24).
493 *Herold* Kriminalistik 28 (1974), 385 (392).

abweichendes Verhalten nunmehr in der Verknüpfung von Datenpunkten sichtbar gemacht werden, so unauffällig – oder um mit den Worten des Bundesverfassungsgerichts zu sprechen: belanglos[494] – sie auch erscheinen mochte. Die Kombination von Daten mit Daten mit dem Ziel eines möglichst genauen Erkenntnisgewinns bedeutete aber auch, dass die Polizei nun einen ständigen Informationsfluss benötigte, von dem zuvor regelmäßig befürchtet worden war, dass er die Polizeiarbeit ineffektiv machen würde.[495] Zudem – auch wenn *Herolds* diesbezügliche Position eine extreme war – war die Funktion der Polizei breiter geworden: Sie hatte nicht mehr nur staatspolitischen, sondern auch gesellschaftspolitischen Zielen zu dienen.[496] Das beinhaltete neben dem Terrorismus in der Folgezeit vor allem auch die sogenannte organisierte Kriminalität, deren Bekämpfung ein weiterer Treiber der informationstechnologischen Aufrüstung der Polizei war und ist.

Insgesamt war die Bilanz der elektronischen Informationsverarbeitung bis zum Ende der 1970er-Jahre gemischt. So wurden die neuen technologischen Möglichkeiten, wie sie etwa die PIOS-Dateien in der Bekämpfung von Terrorismus und organisierter Kriminalität mich sich brachten, zwar von den spezialisierten Fachdienststellen für unverzichtbar gehalten. Im Laufe der Zeit wurde jedoch auch Kritik an PIOS und SSD laut, unter anderem weil die Recherchemöglichkeiten und Suchkriterien als unzureichend bewertet wurden. Darüber hinaus tauchte auch in diesem Kontext wieder das Problem zu vieler Informationen auf: Zu viele nutzlose Daten erschwerten die Arbeit mit den Systemen, lieferten ungenaue oder missverständliche Ergebnisse. Damit evaporierte der Mehrwert der Informationssammlungen wieder. Besonders problembelastet war die SSD. Ihr Anspruch, Straftaten möglichst in ihre Charakteristika zu zerlegen, führte zu einer hohen Komplexität in den Datensätzen, der das System selbst nicht hinreichend gewachsen war. Zudem war es nach wie vor schwierig, die subjektiven Erfahrungen der Kriminalbeamten aus ihrem Arbeitsalltag in harte, maschinenlesbare Daten zu überführen. Schließlich kamen erneut Zweifel an der Perseveranz-Hypothese auf, die durch Länderpolizeien kriminologisch in Frage gestellt wurde. Damit war die konzeptionelle Grundlage

494 BVerfGE 65, 1 (45) – Volkszählung.

495 *L. Scholz* in Schröter/Böhnke (Hrsg.), Analog/Digital - Opposition oder Kontinuum?, 97 (109 ff.).

496 Auch in anderen Staaten findet sich in dieser Zeit eine stärkere Fokussierung der Polizei auf die Ursachen von Kriminalität, vgl. *Jones/Newburn/Reiner* in Jones/Newburn/Reiner (Hrsg.), The Oxford Handbook of Criminology (781).

der SSD in Zweifel gezogen. Gepaart mit den praktischen Schwierigkeiten beim Betrieb, führte dies zur Einstellung der Datei Ende der 1970er-Jahre.

Nach ihren sicherheitspolitischen Höhenflügen in den 1970er Jahren wurde die polizeiliche Datenverarbeitung im folgenden Jahrzehnt zu einem umstrittenen Thema der inneren Sicherheitspolitik in Westdeutschland. Als der RAF-Terror langsam in Vergessenheit geriet und das Orwell-Jahr 1984 heranrückte, wurde die Kritik auch an der Informationspraxis der Polizei lauter, mündete in eine Bürgerbewegung gegen die Volkszählung von 1983 und gipfelte 1984 in der Verkündung des Grundrechts auf informationelle Selbstbestimmung durch das Bundesverfassungsgericht. Neben den polizeiinternen Kritikern des zentralisierten Informationswesens trug die damalige politische Atmosphäre dazu bei, die überwiegend positiv besetzte Entwicklung der polizeilichen Informationssysteme zu hemmen. Mit dem Konzept des Datenschutzes gab es nun eine organisierte und rechtlich operationalisierte Gegenbewegung, die erste rechtliche Beschränkungen der Datenverarbeitung durchsetzte. Aus der Perspektive des Datenschutzes war das polizeiliche Informationswesen selbst zu einem gesellschaftlichen Risiko geworden.[497] Insgesamt wurde damit in den 1980er Jahren ein Richtungswechsel im Ausbau der polizeilichen Informationsarchitektur vollzogen.[498]

So wurden etwa die Daten über Straftäter:innen und Verdächtige, die zuvor im KPMD, dann in der SSD und – in einem Zwischenschritt noch im sogenannten Zentralen Personenindex aufbewahrt worden waren – in den auch heute noch gebräuchlichen Kriminalaktennachweis (KAN) überführt.[499] Dieses von den Länderpolizeien geführte und ab 1983 aufgebaute Indexsystem sollte zwar grundsätzlich Kriminalität breit erfassen, aber nur noch schwere oder überörtlich relevante Straftaten an die Zentrale im Bundeskriminalamt melden. Als Indexsystem waren die Daten zudem nicht mehr online abrufbar. Die Struktur der KAN war dabei emblematisch für die Organisation des polizeilichen Informationswesens in den folgenden Jahren, die sich wieder stärker auf die föderalistische Polizeistruktur besann und sie im Informationswesen technisch festzuschreiben begann. Das Verbundsystem wurde von den Länderdateien getrennt und letztere wieder stärker in die landeseigenen Systeme integriert, denn hier war die Infor-

497 *Mangold,* Fahndung nach dem Raster, S. 185 ff.
498 Vgl. dazu sowie zum Folgenden *Heinrich,* Innere Sicherheit und neue Informations- und Kommunikationstechnologien, S. 180 ff.
499 Siehe dazu unten S. 240 ff.

matisierung regional ebenfalls weitergelaufen. Diese Trennung beförderte die Heterogenisierung des polizeilichen Informationswesens wieder stärker. Landes- und Bundespolizeibehörden bauten ihre Informationssysteme und Dateien nach den eigenen Bedürfnissen aus. Der Informationsverbund bestand zwar weiter, konnte aber die Ungleichheiten und Ungleichzeitigkeiten der technologischen Entwicklungsgrade der deutschen Polizeien nur noch bedingt durch eine zentrale Übersteuerung ausgleichen. Der damit verbundene Bedeutungsrückgang des Bundeskriminalamts als Zentrum im Informationswesen war aber nicht zuletzt auch den institutionellen Konflikten zwischen Zentralisierungs- und Föderalisierungsbefürwortern geschuldet, in dem sich in den 1980er Jahren letztere für den damaligen Moment stärker behaupten konnten.

Der Ausbau der elektronischen Datenverarbeitung in den Ländern, der bereits vor INPOL begonnen hatte, schritt daneben stetig voran. In fast allen Bundesländern bildeten sich Informationssysteme heraus, die strukturell dem INPOL ähnlich aufgebaut waren und ebenfalls immer neue Komponenten einführten. Die Innovationen der Länder wurden teilweise vom gesamten Informationswesen übernommen, wie etwa das Spurendokumentationssystem der Polizei (SPUDOK). Dieses war in Nordrhein-Westfalen entwickelt worden und diente als Vorfilter für PIOS-Dateien, indem zunächst alle eingehenden Daten zu einem Fall im SPUDOK gespeichert und erst nach Überprüfung auf relevante Informationen in die eigentlichen PIOS-Dateien übernommen wurden. Die Möglichkeit diesen Dateitypus flexibel in unterschiedlichen Ermittlungskonstellationen einzusetzen, führte jedoch auch dazu, dass vielfältig strukturierte Datenbanken entstanden, deren individualisierter Charakter jedoch eine Zusammenführung der Datenbestände und damit eine fallübergreifende Recherche verhinderte.[500]

F. Digitalisierung

Sowohl die Datenproduktion der Gesellschaft als auch die Möglichkeiten zur Verarbeitung dieser Daten haben sich seit den 1980er Jahren mit der Verbreitung des Personal Computers (PC) und vor allem mit dem Aufkommen des kommerziellen Internets stark beschleunigt, wodurch eine Informationsgesellschaft Form annahm, die zunehmend „well filled with

500 *Heinrich,* Innere Sicherheit und neue Informations- und Kommunikationstechnologien, S. 181, 186.

data" ist.[501] Auch in den Polizeien wurde die heraufziehende Digitalisierung durch die Einführung von PCs sichtbar. Zudem beförderten die neuen technischen Geräte die dezentralisierte Datenverarbeitung, indem die PCs zunehmend Informationsarbeit abseits der zentralistischen Großrechner-Anlagen der Frühphase elektronischer Datenverarbeitung ermöglichten. Zwar war die Verbreitung von PCs zunächst noch gering, aber schon von Beginn an wurde mit solchen dezentralisierten Kleinrechneranalagen der Versuch einer Verbesserung polizeilicher Informationsarbeit unternommen, etwa indem die Rechner zur Ermittlungsunterstützung eingesetzt wurden. Auch zur Vorgangsbearbeitung wurden PCs schon früh in Pilotprojekten eingesetzt, insbesondere um Verwaltungsabläufe zu beschleunigen, aber auch um etwa polizeiliche Erkenntnisse besser zu erfassen und über Schnittstellen in die Landessysteme und auch ins INPOL zu übertragen.[502] Mit fortschreitender Ausstattung der Polizeibehörden mit Rechnern – neben Großrechnern und Mehrplatzsystemen (Terminals) eben vor allem auch PC-Arbeitsplätze – boten sich zudem neue Möglichkeiten der Vernetzung. In den organisationsinternen Netzen konnten dann über die PCs Daten besser von einzelnen Sachbearbeiter:innen vor Ort erfasst werden. Zudem kam es vermehrt zur Entwicklung hauseigener Verfahren zur Datenverarbeitung, etwa in Form von eigenen Datenbanken und Anwendungen für die kriminalpolizeiliche Aufgabenerfüllung. Diese dezentralisierte Arbeits- und Entwicklungsweise beförderte die Heterogenität weiter, die Ende der 1980er und Anfang der 1990er Jahre ohnehin bereits hinsichtlich Stand und Form der informationellen Technologisierung bestanden hatte. Im föderalen Polizeigefüge waren die Länder je eigene Wege mit je eigenen konzeptionellen, systemtechnischen und organisatorischen Vorstellungen hinsichtlich des Einsatz von Informationstechnologie gegangen. Unterschiedliche Software- und Hardware-Konfigurationen in Bund und Ländern führten zu Kompatibilitätsproblemen und machten das Informationswesen zunehmend instabil. Gepaart mit dem Pflegeaufwand und wenig benutzer:innenfreundlichen Systemoberflächen war die polizeiliche Informationstechnik nicht mehr in der Lage die eingehenden Anfragen adäquat zu bewältigen. Die Vielfältigkeit der Anwendungen und Datenbestände erforderte spezialisiertes Personal, das nicht ausreichend vorhanden war. In der Folge waren die wenigen EDV-kundigen Beamt:innen kaum in der

501 *McLuhan,* Understanding media, S. 22.
502 *Heinrich,* Innere Sicherheit und neue Informations- und Kommunikationstechnologien, S. 189 ff.

Lage, die vielfältigen Datenerfassungen und -eingaben zu bewältigen, die aufgrund der uneinheitlichen Dateienstruktur erforderlich waren. Häufig erfolgte eine Beschränkung auf die Instandhaltung der eigenen Landessysteme, was wiederum zu Informationslücken im INPOL führte. Insgesamt ließ die Effektivität der Informationsinfrastruktur stark nach.[503] Nach einigen institutionellen Vorläufen wurden die Uneinheitlichkeit und Unübersichtlichkeit wieder zum zentralen Thema und führten 1992 zum Beschluss der Innenministerkonferenz (IMK), das alte INPOL durch INPOL-Neu zu ersetzen.

Die Neukonzeption sollte tiefgreifende Vereinheitlichung bringen, die vielfältigen Datenbestände in einen „Datenpool" überführen und so für bessere Datenauswertungsverfahren die Grundlage bieten. Es ging also im Wesentlichen um ein intelligenteres Informationsmanagement, mit dem sich die Auswertung der Daten verbessern ließe.[504] Ziel war also insgesamt die Erhöhung der Nutzbarkeit der Daten etwa für statistische Zwecke, für Lagebilder oder operative Führungsaufgaben.[505] Dazu war es insbesondere erforderlich die technischen Komponenten zu homogenisieren und den Aufbau des Informationswesens stärker an einer straffen Konzeptualisierung auszurichten. Die Leitkonzepte waren dabei der bereits erwähnte Datenpool, also ein einheitlicher, auf einem Basisdatenmodell basierender Datenbestand und eine dezentralisierte, PC-basierte Datenerfassungs- und -verarbeitungskapazität. Dazu sollten überall Vorgangsbearbeitungssysteme eingeführt werden, damit die Daten vor Ort in die einheitliche Datenbank übertragen werden könnten. Daneben versprach man sich die Automatisierung von Datenflüssen etwa zu kriminalpolizeilichen Meldezwecken. In Pyramidenform sollten lokale Dienststellen so die Daten erfassen, womit dann durch Übermittlungen an die darüber liegenden Ebenen je nach Verwendungszweck und Informationsbedürfnis alle organisationalen Informationsbedürfnisse abgedeckt werden sollten. Konzeptuell war INPOL-Neu also eine radikale Abkehr von der bisherigen Datei-Struktur mit ihren vielen unterschiedlichen Datenbeständen und Spezialanwendungen.[506] Eine Abkehr von der Trennung zwischen Landes- und Verbundsystem war

503 *Heinrich,* Innere Sicherheit und neue Informations- und Kommunikationstechnologien, S. 210.
504 *Heinrich,* Innere Sicherheit und neue Informations- und Kommunikationstechnologien, S. 215.
505 *Burczyk* Bürgerrechte & Polizei (CILIP) 2020, 16 (17 f.).
506 *Heinrich,* Innere Sicherheit und neue Informations- und Kommunikationstechnologien, S. 217.

damit nicht zwangsläufig verbunden, sie konnte prinzipiell auch in der neuen Struktur aufrecht erhalten bleiben. Für verbundrelevante Vorgänge – also vor allem überregionale Straftaten – sollte hingegen eine automatische Übertragung an die Zentrale stattfinden, sodass diese Taten für alle einsehbar werden. Neben dem Wunsch nach einer generellen Verbesserung der Datenauswertung war mit der Konzeption zusätzlich der Plan verbunden, auch den lokalen und regionalen Unterorganisationen über die Automatisierung der Vorgangsbearbeitung in ihrem Zuständigkeitsbereich eigene Auswertungskompetenzen an die Hand zu geben. Die Zentralstellen, die zuvor die gesamte Auswertungskompetenz bei sich bündeln mussten, hätten so mehr Zeit für ihre eigenen Aufgabenbereiche, während die lokalen Dienststellen mit ihren nunmehr eigenen Analysefähigkeiten alltäglichere Kriminalität besser bearbeiten könnten.[507]

Der Realisierungsprozess für INPOL-Neu startete 1998, scheiterte jedoch. Als radikaler Bruch mit der bisherigen informationstechnischen Infrastruktur erforderte die Projektumsetzung die gleichzeitige Umstellung aller polizeilichen Landessysteme auf die neuen Anforderungen. Allerdings verfügten die meisten Länder noch überhaupt nicht über ein adäquates Vorgangsbearbeitungssystem, mit dem man an INPOL-Neu in der vorgesehenen Weise hätte teilnehmen können. Die Anpassung der bestehenden Landessysteme anhand von Schnittstellen- und Anforderungsvorgaben des Bundeskriminalamts geriet zu einem Koordinierungsproblem, in dessen Folge die Projektkomplexität explodierte und unbeherrschbar wurde.[508]

Trotz des Scheiterns versuchte man sich weiter ab 2002 an einer nunmehr bescheideneren Umstrukturierung des polizeilichen Informationswesens. Konzeptuell war nun nicht mehr die volle Integration aller Dienststellen in einen Rechnerverbund beabsichtigt, sondern die Weiterentwicklung der alten INPOL-Struktur aus Großrechnern und Terminals. Die Umsetzung erfolgte 2003, indem aus der Fahndungsdatei INPOL-Z[509] ein allgemeines Fahndungs- und Auskunftssystem wurde, das insbesondere den alltäglichen Polizeieinsätzen dienen sollte. Die PIOS-Dateien wurden gemeinsam mit den weiteren bis dahin entstandenen Fachverfahren und Falldateien durch INPOL-Fall ersetzt, das vor allem der kriminalpolizeilichen

507 *Heinrich,* Innere Sicherheit und neue Informations- und Kommunikationstechnologien, S. 218 f.

508 *Heinrich,* Innere Sicherheit und neue Informations- und Kommunikationstechnologien, S. 221 f.

509 Siehe dazu unten S. 230 ff.

Aufgabenerfüllung dienen sollte. Neben den harten Daten ermöglichte INPOL-Fall[510] in Freitextfeldern die Erfassung von weichen kriminalistischen Daten, sowohl in Textform als auch als multimedialer Inhalt. Auch die freie Verknüpfung aller Objekte in den Dateien war als zentrale Funktion für die kriminalistische Fallanalyse vorgesehen. Recherchiert werden konnte in allen INPOL-Fall-Dateien gleichzeitig, wobei bereits hier ein für die hierarchische Organisationsweise der Polizei typisches Berechtigungskonzept, das sich an der fachlichen Zuständigkeit orientierte, die Sichtbarkeit von Daten beschränkte.[511]

Wie schon während der vorherigen technologischen Innovationsschübe, verlief mit Aufkommen digitaler Technik in den Ländern eine zur Verbundentwicklung parallele Technologisierung. Neben der bereits erwähnten Einführung des PCs in die polizeilichen Arbeitsabläufe, die eine dezentralisierte, aber zugleich vernetzte Arbeitsweise ermöglichte, war vor allem die Einführung bzw. der Aufbau von Informationssystemen in Form von Vorgangsbearbeitungssystemen die wohl zentrale informationstechnologische Entwicklung dieser Phase. Angestoßen wurde dies vor allem durch die beschriebene INPOL-Neu-Planung, die auf entsprechend qualitative Vorgangsbearbeitungssysteme und passende Schnittstellen in den Ländern angewiesen war. Da allerdings zuvor eine uneinheitliche Technologie-Entwicklung in den Ländern stark divergierende Pfadabhängigkeiten hervorgerufen hatte, erfolgte die Entwicklung dieser neuen Systeme zunächst gleichfalls heterogen. Da die damit verbundenen Probleme bereits bekannt waren, durch das Scheitern von INPOL-Neu an Kompatibilitätsschwierigkeiten aber nochmal in den Fokus gerieten, formierten sich in der Folge Kooperationsverbünde zwischen den Ländern zur Abstimmung technologischer Komponenten, wie etwa Schnittstellen, und teilweisen Verwendung derselben Systeme. Auch über die Einführung der Systeme hinaus sind institutionell verfestigte Kontaktpunkte entstanden, um die generellen Homogenisierungsbemühungen im polizeilichen Informationswesen nicht durch den Betrieb und die Weiterentwicklung der landesspezifischen Systeme zu unterlaufen. In der Folge wurde die Integrationsfähigkeit des polizeilichen Informationswesen merklich gesteigert. Anstelle von fragmentierten, nebeneinanderstehenden Systemen hatte man nun einigermaßen verein-

510 Siehe dazu auch unten S. 251 ff.
511 *Burczyk* Bürgerrechte & Polizei (CILIP) 2020, 16 (18 f.).

heitlichte Basiskomponenten, die einen Datenaustausch auch im Verbund grundsätzlich verbesserte.[512]

Neben diesen eher infrastrukturellen Fortentwicklungen des polizeilichen Informationswesens kamen mit zunehmender Adaption von Digitaltechnik durch die Polizeien auch Konzeptionen und Umsetzungen für neue Informationssystemtypen auf. Mit der Durchsetzung des polizeilichen Arbeitsfeldes mit Informationstechnologie gab es immer wieder Innovationen, die – häufig von einzelnen Beamt:innen entwickelt – auf die Unterstützung in speziellen Aufgabengebieten ausgelegt waren und wegen ihrer Nützlichkeit in die polizeilichen Systeme integriert wurden. Aufgrund ihrer vorrangigen Funktion der Unterstützung polizeilicher Expert:innen bei ihren Aufgaben spricht man auch von Expert:innensystemen. Abstrakt ist darunter ein Informationssystem zu verstehen, die das in einer Datenbank verfügbare Wissen eines Spezialbereichs für die Anwendung auf einen Fall bereithält. Neben einfacheren Wenn-Dann-Aussagen und statistischen Berechnungen wurde bereits seit den frühen 1990er Jahren auch mit mathematischen Verfahren experimentiert, die dem Zweig der künstlichen Intelligenz zuzuordnen sind. Mit den Systemen wurde auch der Versuch unternommen, das hochspezialisierte Wissen, dass in den Polizeiorganisationen nach wie vor stark an einzelne Personen geknüpft war, zu abstrahieren und weniger kundigen Sachbearbeiter:innen verfügbar und damit auch deren Aufgabenerfüllung effektiver zu machen. Zudem war mit den Expert:innensystemen die Hoffnung verbunden, polizeiliches Handeln insgesamt transparenter, rationaler und reproduzierbarer zu machen, wodurch die Legitimität polizeilichen Handelns gesteigert und dessen Rechtfertigung vor Öffentlichkeit und Politik erhöht werden könnte. Allerdings verliefen die ersten Versuche, insbesondere auch mit Spielarten der künstlichen Intelligenz, enttäuschend. Die Simulation sozialer Zustände war durch die Komplexität menschlichen Verhaltens mit der Technologie der 1990er Jahre kaum möglich, sodass sich auch die erhoffte automatisierte Generierung von Lösungsansätzen auf Grundlage der polizeilichen Datenbestände zu diesem Zeitpunkt als bloße Hoffnung erwies.[513] Als „völlig illusorisch" wurde es beschrieben, „kurz oder mittelfristig Erfolge bei der Entscheidungs-

512 *Heinrich,* Innere Sicherheit und neue Informations- und Kommunikationstechnologien, S. 235 ff.

513 *Heinrich,* Innere Sicherheit und neue Informations- und Kommunikationstechnologien, S. 239 f.

findung [...] mittels KI zu erwarten."[514] Auch bei Systemen, die tendenziell optimistischer betrachtet wurde wie dem ViCLAS (Violent Crime Linkage Analysis System), das zur kriminalistischen Behandlung von Gewalttaten eingesetzt wird, erfolgte eine Automatisierung von Entscheidungsabläufen noch nicht. Ganz im Sinne der Sozio-Technizität waren die Expert:innen nach wie vor zentral, um das datenbasiert vorgehaltene Wissen in den Systemen in konkrete polizeiliche Handlungsschritte umzusetzen.[515]

Mit fortschreitender Digitalisierung konnte auch die Polizei ihre Arbeitsabläufe durch entsprechende Instrumente immer stärker an die Dynamiken und auch Zwänge des Informationszeitalters anpassen. Ganz generell gesprochen ergaben und ergeben sich im Zuge des digitalen Wandels stetig neue Möglichkeiten einerseits der Erhebung, aber vor allem auch der Integration von Daten. Denn digitale Technologien ermöglichen nicht nur eine breitere optische, akustische oder sonst sensorische Erfassung von lebensweltlichen Sachverhalten in Form von Daten, sondern bieten bei passender informationstechnischer Infrastruktur auch neue Möglichkeiten der Integration und Verknüpfung und damit auch der Auswertung der erfassten Daten. Neben der Digitalisierung von klassischen Medien der Bild- oder Tonaufzeichnung war vor allem auch das Internet ein neues Umfeld und Mittel zur Erhebung von Massendaten. Die vielfältigen Möglichkeiten dieser neuen technologischen Konfigurationen realisierten sich etwa in der Digitalisierung des Erkennungsdienstes und Einführung biometrischer Verfahren, der Digitalisierung und Vernetzung der polizeiinternen Kommunikationsweisen oder auch der Digitalisierung von Spuren- und Beweisführung.[516]

Auch diese Entwicklungen verliefen indessen wenig koordiniert und häufig landesspezifisch. Zudem wurde die polizeiliche Informationssystemlandschaft mit einem Erstarken der gesamtgesellschaftlichen Bedeutung des Massendatenphänomens erneut für zu heterogen befunden. Das polizeiliche Informationswesen, so die Überzeugung, die sich zunehmend durchsetzte, sei für die dem Massendatenparadigma inhärenten Logiken und Dynamiken nicht gerüstet, sodass weitere Vernetzungs- und Homogenisie-

514 *Frühauf/W. Schneider/Schulz* in Polizei-Führungsakademie (Hrsg.), Thema heute: "Forschung und Entwicklung auf dem Gebiet der Polizeitechnik", 9-26 (20).

515 *Heinrich,* Innere Sicherheit und neue Informations- und Kommunikationstechnologien, S. 245.

516 *Heinrich,* Innere Sicherheit und neue Informations- und Kommunikationstechnologien, S. 248 ff.

rungsbemühungen vorangetrieben wurden. Während ein zentrales Projekt dazu zunächst der Polizeiliche Informations- und Analyseverbund war,[517] ist in jüngerer Zeit mit dem Projekt Polizei 2020[518] ein informationstechnologisches Großprojekt zur Überarbeitung der polizeilichen Informationsarchitektur aufgelegt worden, dessen bereits in Teilen sichtbare Auswirkungen Gegenstand der folgenden Kapitel sind.

G. Datafizierung als gegenwärtige informationstechnologische Entwicklungsstufe

Die Durchdringung der polizeilichen Arbeitsfelder mit digitalen Instrumenten und Verfahren ist im Begriff die Verarbeitung von Daten in einer Weise zu verändern, die sich nicht mehr allein unter den Begriff der Digitalisierung fassen lässt, mit der vor allem der Übergang von analoger zu digitaler Informationstechnik gemeint ist. Vielmehr ist auch hier, wie bereits aus theoretischer Perspektive beschrieben,[519] mit dem Begriff der Datafizierung zu operieren, der von vielen geprägt und von *Egbert* auf den polizeilichen Kontext angepasst wurde:

> „Mit dem Begriff Datafizierung ist dabei die zunehmende Nutzung korrelativ fundierter, statistischer Datenanalyse gemeint, die auf Entscheidungsfindung ausgerichtete und algorithmisch vermittelte (Massen-)Analyse von Daten angesprochen, deren Resultate entsprechend umgesetzt werden und somit die polizeilichen Praktiken nachhaltig prägen. Damit umfasst die Datafizierung nicht allein die verstärkte und mittlerweile nahezu flächendeckende datenmäßige Repräsentation gesellschaftlicher Aktivitäten, […] (hier als ‚Verdatung' verstanden), sondern immer auch die daran anknüpfenden algorithmisch mediatisierten Analysen sowie die daran anschließenden Entscheidungen und Denk- sowie Handlungsanpassungen."[520]

517 Siehe zu dessen Entwicklung, die eher in die Gegenwart polizeilicher Informationsverarbeitung fällt, unten S. 251 ff.

518 Auch dieser Projekt ist Teil der Gegenwart der polizeilichen Informationsverarbeitung und wird dementsprechend weiter unten behandelt, siehe dazu unten S. 271 ff. sowie S. 465 ff.

519 Siehe dazu oben S. 46 ff.

520 *Egbert* in Hunold/Ruch (Hrsg.), Polizeiarbeit zwischen Praxishandeln und Rechtsordnung, 77 (78).

Emblematisch für diesen Prozess – *Egbert* spricht insofern von einem „Türöffner" – war vor allem die seit den 2010er Jahren erfolgende Erprobung und Einführung von Verfahren die unter dem schillernden Begriff des „Predictive Policing"[521] diskutiert wurden. Abstrakt gesprochen handelt es sich dabei um kriminalprognostische Technologien, die auf der Grundlage von selbstlernenden Algorithmen in großen Datenbeständen Muster der Abweichung erkennen und darüber (besser als ein Mensch) vorhersagen können sollen, wer straffällig wird oder wo und wann Straftaten begangen werden.[522] Damit wurde die in den 1990er Jahren bereits einmal aufgekommene Hoffnung, mithilfe von künstlicher Intelligenz Expert:innensysteme zu entwickeln, mit denen die operative Sachverhaltsbearbeitung merklich verbessert werden kann, wiederbelebt und zumindest stärker als etwa zwanzig Jahre zuvor eingelöst. Insofern erweist sich die gegenwärtige Entwicklung auch weniger als Disruption, wie sie für das Digitalzeitalter häufig konstatiert wird. So knüpfen etwa Konzepte wie Predictive Policing in historischer Perspektive an bereits bestehende Entwicklungspfade an, wie etwa an die Kriminalitätsanalyse, an die präventive Wende der Polizei spätestens seit dem ausgehenden 20. Jahrhundert sowie an die Verwissenschaftlichung polizeilicher Arbeit.[523] Allerdings sind die Entwicklungspfade des polizeilichen Informationswesens keineswegs linear, sondern – wie aufgezeigt – häufig von Ungleichzeitigkeit und Uneinheitlichkeit geprägt.[524] Nichtsdestotrotz wäre es auch falsch, datafizierte Polizeiarbeit als nur kleine evolutionäre Weiterentwicklung der Polizeiarbeit zu deuten. Vielmehr entsteht hier ein qualitativ anderer Modus der Generierung von Wissen über die Gesellschaft und das in ihr auftretende (abweichende) Verhalten, da Erkenntnisbreite und Erkenntnistiefe durch den sich wandelnden Modus der Datensammlung und Wissensgenerierung intensiviert werden.[525] Mit bisherigen Divergenzen in der informationellen Technisierung der Polizeien steht auch in Einklang, dass die noch immer andauernde Entwicklung von Predictive Policing-Technologie nicht so monolithisch ist, wie der Begriff oder die personen- oder ortsbezogene Anwendungsweise suggerieren mag. Neben der Pluralität der prädiktiven Verfahren ist zusätzlich zu

521 Konkreter zum Begriff und Einsatz von Predictive Policing in Deutschland, siehe unten S. 279 ff.
522 *Ferguson,* The rise of big data policing, S. 34 ff., 62 ff.
523 *Egbert/Leese,* Criminal futures, S. 3.
524 *Heinrich,* Innere Sicherheit und neue Informations- und Kommunikationstechnologien, S. 369.
525 *Egbert/Leese,* Criminal futures, S. 3.

beachten, dass nicht allein die Technologie einem Wandlungsprozess unterliegt, sondern die Datafizierung des polizeilichen Arbeitsfeldes darüber hinaus durch erhebliche Veränderungen in der Organisation der Polizei und den polizeilichen Praktiken gekennzeichnet ist, die auf polykausale Weise mit den technologischen Innovationen interagieren.[526]

Die Dynamik der Datafizierung bedingt dabei eine expansive Dynamik des polizeilichen Informationswesens. Dessen Grundfunktion ist auf die Erfassung von sozialen Interaktionen und Prozessen mit Devianzbezug ausgerichtet, um daraus polizeihandlungsleitendes Wissen zu generieren. Wegen des Durchdringens der polizeilichen Arbeitspraktiken mit Instrumenten zur datenmäßigen Erfassung von Lebenssachverhalten entsteht ein sich ausweitender Bedarf, die so gewonnenen Informationen nutzbar zu machen. Neue Verarbeitungsverfahren sind wiederum auf einen konstanten oder sogar steigenden Datenfluss angewiesen, um das vorhandene Potenzial voll auszuschöpfen. Das Informationswesen ist in seiner Gesamtheit – wie *Heinrich* es treffend beschreibt – „auf informatorische Expansion ausgelegt, d.h. es wird ermöglicht, immer mehr technisch erhobene Informationen über soziale Handlungsweisen zu einem Abbild der Realität zu verdichten und somit die Handlungsgrundlage für eine situationsangepasste Aufgabenerledigung zu schaffen."[527]

Dieser kontinuierliche Ausbau des polizeilichen Informationswesens greift dabei immer weiter in gesellschaftliche Sphären aus, die informationell durchdrungen und datenförmig erfasst werden. Dieser Effekt tritt regelmäßig auch ohne entsprechende Intention bezüglich der Ausweitung und Vertiefung der polizeilichen Kontrollintensität auf. Das gilt umso mehr, als dass sich die Dynamik der Datafizierung besonders gut in den generellen, für bürokratische Verwaltungsapparate typischen Impetus zur Optimierung von Organisationsstrukturen und -prozessen einfügt. So ermöglicht der stetige Ausbau der informationellen Instrumente zur Optimierungszwecken der Polizeien zugleich eine Vernetzung der dadurch produzierten Daten. Deren Auswertung mit bestehenden oder sodann sinnvollerweise zu schaffenden Verfahren ermöglicht oftmals die Generierung tiefergehender Erkenntnisse bezüglich der mit den produzierten Daten abgebildeten sozialen Zusammenhänge. Auch wenn viele dieser technologischen Entwicklungsprozesse größtenteils unkoordiniert und inkrementell

526 *Egbert/Leese,* Criminal futures, S. 220.
527 *Heinrich,* Innere Sicherheit und neue Informations- und Kommunikationstechnologien, S. 377.

ablaufen, ergibt sich in der Gesamtschau eine Eigendynamik mit den beschriebenen Regelmäßigkeiten der datafizierten Polizei.

Dabei ist das Erkennen von Mustern in Informationen und Daten, um über die Identifikation von Regelmäßigkeiten auch abweichendes Verhalten sichtbar zu machen, nicht neu, sondern hat eine lange Entwicklungsgeschichte bei der modernen Polizei.[528] Wie gezeigt wurde, ist das zielorientierte Verarbeiten von Informationen mittels dazu zur Verfügung stehender Technologie eines der die moderne Polizei überhaupt erst formenden Elemente. Allerdings scheinen die gegenwärtigen informationstechnologischen Fortschritte eine nie dagewesene Analysegeschwindigkeit und -tiefe auf Grundlage entsprechend verlässlicher Daten zu erlauben,[529] was eine sorgfältige und vor allem auch kritische Auseinandersetzung mit dem Informationswesen der datafizierten Polizei erforderlich macht.

528 *Egbert/Leese,* Criminal futures, S. 20.
529 *Egbert/Leese,* Criminal futures, S. 20.

Kapitel III. Normative Rahmenbedingungen des polizeilichen Informationswesens

Nachdem die theoretischen Grundlagen und die historische Entwicklung des polizeilichen Informationswesens dargelegt worden sind, soll nun die Gegenwart polizeilicher Informationsverarbeitung in Deutschland in den Blick genommen werden. Ihren Ausgangspunkt nimmt diese Betrachtung bei den normativen Rahmenbedingungen des polizeilichen Informationswesens, also präskriptiven Strukturen, die Aufschluss darüber geben, wie das Informationswesen und die in ihm stattfindenden Informationspraktiken sein *soll*, um dann im darauffolgenden Kapitel eine Annäherung an die tatsächlichen Dynamiken dieses sozio-technischen Systems zu unternehmen.[530]

Die normativen Rahmenbedingungen des polizeilichen Informationswesens lassen sich zunächst einmal grob in die übergesetzlichen Vorgaben des Verfassungs- und Unionsrecht und die einfachgesetzlichen Vorgaben unterteilen, die sich wiederum vorrangig aus den Polizeigesetzen und dem Strafverfahrensrecht zusammensetzen. Zusätzlich könnte man noch polizeiinterne Verordnungen und Richtlinien, wie die Polizeidienstvorschrift und die Richtlinien über Kriminalpolizeiliche personenbezogene Sammlungen (KpS-Richtlinien) heranziehen, deren Abbildung eine Arbeit, die nicht auf die systematische und umfassende Darstellung des gesamten normativen Rahmens polizeilicher Datenverarbeitung abzielt, allerdings überladen würde.[531] Die folgenden Ausführungen verstehen sich daher explizit als Überblick, wobei die mangelnde Vollständigkeit einerseits der bereits angedeuteten Komplexität des polizeilichen Informationsrechts geschuldet ist und andererseits ohnehin eine selektive Darstellung erfolgen soll, die auf den normativen Rahmen der grundsätzlichen Strukturen des polizeilichen Informationswesens und der grundsätzlichen, in ihm stattfindenden Informationsverarbeitungsformen fokussiert, statt jede denkbare rechtliche Konstellation polizeilicher Informationsverarbeitung durchzuspielen. Dazu werden die Steuerungsebenen des Verfassungsrechts und Unionsrechts in

530 Siehe dazu unten S. 377 ff.

531 Zur normativen Bedeutung dieser Vorschriften in der polizeilichen Informationspraxis siehe aber unten S. 416 ff.

ihren Bezügen zur polizeilichen Informationsverarbeitung beschrieben, um daran anknüpfend den einfachgesetzlichen Rahmen für das polizeiliche Informationswesen – wo es denn normative Ankerpunkte hat – zu konturieren und Problemfelder aufzuzeigen. Dabei werden auch immer wieder Bezüge zum Datenschutzrecht gezogen, das die polizeiliche Informationsordnung durchzieht und gleichfalls verklammert.

A. Grund- und menschenrechtliche Vorgaben für polizeiliche Datenverarbeitung

Zuerst muss – vor die Klammer gezogen – eine Darstellung der verfassungsrechtlichen Vorgaben für die polizeiliche Datenverarbeitung erfolgen, die für alle Polizeibehörden des Bundes und der Länder gelten. Polizeiliches Informationshandeln betrifft eine Vielzahl verschiedener Grundrechte, die sich der „grundrechtlichen Identitätsschicht" der Privatheit[532] (*Schwabenbauer*) zuordnen lassen. Da es vorliegend jedoch vorrangig um Datenverarbeitungen geht, die an die verschiedenen Erhebungsmaßnahmen anknüpfen, also – zeitlich besehen – um solche Datenverarbeitungen, die stattfinden, nachdem die Daten in den Einflussbereich der Polizei gelangt sind, ist vor allem das Recht auf informationelle Selbstbestimmung von zentraler Bedeutung. Denn auch wenn grundrechtliche Eingriffe, etwa in das Wohnungsgrundrecht, durch weiteren Umgang mit derart erlangten Daten fortgesetzt werden, ist es das Recht auf informationelle Selbstbestimmung, das jeden Datenumgang durch die Sicherheitsbehörden verfassungsdogmatisch abbildet, sodass die übrigen Grundrechte der Identitätsschicht vorliegend vernachlässigt werden. Ausgangspunkt für das Recht ist, wie für das deutsche Datenschutzrecht insgesamt, das bereits zuvor erwähnte Volkszählungsurteil des Bundesverfassungsgerichtes aus dem Jahr 1983. Das Gericht schuf mit seinem Urteil ein neues Grundrecht auf informationelle Selbstbestimmung, als es damals proklamierte:

> „Freie Entfaltung der Persönlichkeit setzt unter den modernen Bedingungen der Datenverarbeitung den Schutz des Einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten voraus. Dieser Schutz ist daher von dem Grundrecht

532 *Müller/Schwabenbauer* in *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch des Polizeirechts, Rn. 62 ff.

des Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG umfasst. Das Grundrecht gewährleistet insoweit die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen."[533]

I. Das Recht auf informationelle Selbstbestimmung

Im System der grundrechtlichen Dogmatik findet das Recht auf informationelle Selbstbestimmung seinen Ursprung im allgemeinen Persönlichkeitsrecht,[534] das ideengeschichtlich wiederum auf das von *Warren* und *Brandeis* formulierten „right to be let alone"[535] zurückgeht.[536] Im Vergleich zum US-amerikanischen „right to be let alone", das sich zunächst auf die Interaktion zwischen Bürger:innen der Vereinigten Staaten bezog,[537] ist die deutsche Grundrechtsdogmatik hingegen stärker auf den Schutz des Einzelnen vor staatlicher Macht ausgerichtet. Das allgemeine Freiheitsrecht aus Art. 2 Abs. 1 GG als eine der beiden wesentlichen Quellen des Persönlichkeitsrechts ist dabei zentral für das Verständnis des grundrechtlichen Freiheitsverständnisses.

> „Im Wertsystem der Grundrechte macht Art. 2 Abs. 1 unbezweifelbar, worin inhaltlich (materiell) die Würde des Menschen (Art. 1 Abs. 1) vornehmlich besteht: – in der ‚freien Entfaltung seiner Persönlichkeit'."[538]

Vor diesem Hintergrund wirkt die teils herablassende Titulierung des Art. 2 Abs. 1 GG als „Auffangrundrecht" nicht angemessen, mag sie auch rechtstechnisch zutreffend sein.[539] Die, vor allem für die moderne Informationsgesellschaft, immense Bedeutung des Grundrechtes zeigt sich in seinen besonderen Ausprägungen des allgemeinen Persönlichkeitsrechts, also in Verbindung mit Art. 1 Abs. 1 GG. Diese – zunächst das Recht am eigenen Bild und das Recht am eigenen Wort – sind dabei rechtsdogmatische

533 BVerfGE 65, 1 (42) – Volkszählung.
534 *Brink* in DS-GVO Syst. C. Verfassungsrechtliche Grundlagen Rn. 10.
535 *Warren/Brandeis* Harvard Law Review, pp. 193-220. Vol. 4 (1890), 193 ff. (193).
536 *Brink* in DS-GVO Syst. C. Verfassungsrechtliche Grundlagen Rn. 5.
537 Es ging hier vor allem um die Abschirmung des privaten Lebens vor der „vierten Gewalt", insbesondere in ihrer Manifestation als invasive Reporter. Dabei stand zunächst die Privatheit der privilegierten Gesellschaftsschichten im Mittelpunkt dieses neuen, normativen Anspruchs, vgl. *Igo,* The Known Citizen.
538 *Dürig* zitiert nach *DiFabio* in *Dürig/Herzog/R. Scholz,* Grundgesetz, Art. 2 Rn. 1.
539 *Di Fabio* in *Dürig/Herzog/R. Scholz,* Grundgesetz, Art. 2 Rn. 7.

Reaktionen auf die technischen und gesellschaftlichen Entwicklungen des 19. und 20. Jahrhunderts, die eine Fixierung und Reproduzierbarkeit des eigenen Bildes sowie des gesprochenen Wortes mit sich brachten und die Sozialbezüge des Individuums in erheblichem Maße ausweiteten.[540] Die jüngeren Entwicklungen in der Informationstechnologie führten schließlich zum gegenwärtigen Stand des Möglichen: Jeder wahrnehmbare Ausdruck der Persönlichkeit ist „prinzipiell unbegrenzt fixierbar, transferierbar, multiplizierbar und digital manipulierbar".[541]

Diese Fluidität[542] von (personenbezogenen) Daten macht letztlich ihren einzigartigen Wert aus, gibt ihnen aber zeitgleich ihr Gefährdungspotenzial. Dies gilt uneingeschränkt und besonders auch für polizeiliche Datenverarbeitungen. Die Daten, die dort über tatsächliche und potenzielle Straftäter:innen, Zeugen und sonstige Personen gespeichert wurden und werden führen für die Betroffenen dazu, dass sie über diese Daten – wenn sie denn überhaupt von ihnen wissen – regelmäßig kaum noch selbst bestimmen können. Gleichzeitig ist eine Polizei ohne die Möglichkeit, zeitgemäß mit Daten umzugehen, in der modernen Informationsgesellschaft blind. Für eine weiterhin funktionale Kriminalitätskontrolle ist dementsprechend unerlässlich, dass die deutschen Polizeien die technischen und auch rechtlichen Voraussetzungen zum Umgang mit Massendaten besitzen.[543]

Dieses Spannungsfeld polizeilicher Sozialkontrolle in der digitalen Gesellschaft verfassungsrechtlich auszutarieren ist eine der wesentlichen Aufgaben des Rechts auf informationelle Selbstbestimmung im Verhältnis zwischen Bürger:innen und Staat. Insofern ist zunächst darzulegen, welche normativen Postulate für diese Beziehung aus der Verfassung abgeleitet werden. Ein besonderer Fokus liegt dabei darauf, inwiefern dabei Dynamiken des Massendatenphänomens in diesem Rahmen Berücksichtigung finden. In diesem Zusammenhang muss auch beachtet werden, wie die gegenwärtig geplante Umstrukturierung des polizeilichen Informationswesens im Lichte der Verfassung zu bewerten ist.

---

540 *Brink* in *Brink/H. Wolff*, BeckOK Datenschutzrecht, DS-GVO Syst. C. Verfassungsrechtliche Grundlagen Rn. 7, 46ff.

541 *Brink* in *Brink/H. Wolff*, BeckOK Datenschutzrecht, DS-GVO Syst. C. Verfassungsrechtliche Grundlagen Rn. 7.

542 Siehe zur Idee der Fluidität im Kontext von Daten *Cheney-Lippold,* We are data, passim.

543 Näher zu diesen Dynamiken bereits oben S. 66 ff.

I. Schutz, Eingriff, Rechtfertigung – Grundsätze und Entwicklungen

a) Schutz

Kern des Rechts auf informationelle Selbstbestimmung ist in subjektivrechtlicher Hinsicht nach wie vor die bereits im bundesverfassungsgerichtlichen Eingangszitat genannte Befugnis des Individuums, grundsätzlich selbst über die Preisgabe und Verwendung der eigenen personenbezogenen Daten zu bestimmen.[544] So soll der „Schutz des Einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten"[545] gewährleistet werden.

Grundgedanke ist hierbei, dass die Entfaltung der Persönlichkeit die Begrenzung der Wahrnehmung des Individuums durch Dritte erforderlich machen kann,[546] da sich die Persönlichkeit in erster Linie in Rückkopplung mit sozialen Prozessen bildet und weiterentwickelt,[547] also auf Grundlage von Daten bzw. Informationen konstruiert wird.[548] Erst im Kontakt zu anderen können Eigenarten der Persönlichkeit gezeigt und geschärft werden. Dazu muss es dem Individuum möglich sein, sein Selbstbild in verschiedenen sozialen Interaktionen kontextspezifisch zu präsentieren.[549] Was durch das normative Konzept der informationellen Selbstbestimmung bewahrt werden soll, ist der theoretische Facettenreichtum der individuellen Persönlichkeit in den verschiedenen Kontexten, also ihre Wandelbarkeit.[550] Ein durch Informationsvorsprung aggregiertes Gegenbild der jeweiligen Person, das sich ihrem Einfluss gänzlich entzieht, schränkt diese Entfaltungsräume ein. Eine erfolgreiche Selbstinszenierung erfordert aber gerade eine solche Einflussmöglichkeit. Nimmt der eigenen Einfluss auf das nach außen reflektierte Persönlichkeitsbild ab und nimmt damit gleichzeitig die Deutungshoheit der durch andere erzeugten Gegenbilder zu, so kann das Individuum sich nicht mehr autonom darstellen und entfalten. Zu Ende

544 BVerfGE 65, 1 (42) – Volkszählung.
545 BVerfGE 65, 1 (43) – Volkszählung.
546 BVerfGE 65, 1 (43) – Volkszählung.
547 *Brink* in *Brink/H. Wolff*, BeckOK Datenschutzrecht, DS-GVO Syst. C. Verfassungsrechtliche Grundlagen Rn. 8.
548 Siehe dazu bereits oben S. 50 ff.
549 *Britz*, Freie Entfaltung durch Selbstdarstellung, 2007, S. 37f.
550 Siehe dazu bereits *W. Steinmüller/Lutterbeck/Mallmann* ua, Grundfragen des Datenschutzes, Gutachten im Auftrag des Bundesministeriums des Innern, BT-Drs. 6/3826, 1971, 86 ff.

gedacht, führt dies zu einer überbordenden Fremdbestimmung der Persönlichkeit.[551] Damit unterstützt das Recht auf informationelle Selbstbestimmung auf der einen Seite das allgemeine Persönlichkeitsrecht, geht aber andererseits auch über den von diesem Grundrecht gewährleisteten Schutz hinaus, indem es schon in seinem Vorfeld eingreift, nämlich dort, wo das allgemeine Persönlichkeitsrecht personenbezogene Informationen nicht erfasst, weil sie im gegenwärtigen Zeitpunkt noch nicht persönlichkeitsrelevant sind oder es gegebenenfalls niemals sein werden. Das Recht auf informationelle Selbstbestimmung verlagert den grundrechtlichen Schutz des Individuums damit weg von konkreten Verletzungshandlungen – vor denen das allgemeine Persönlichkeitsrecht schützt – hin zum Schutz vor abstrakten Gefährdungen der Persönlichkeit.[552]

Um dies zu bewerkstelligen, gewährt das in dieser Hinsicht seit dem Volkszählungsurteil unverändert gebliebene Recht[553] grundsätzlich Selbstbestimmung für jeglichen Datenumgang.[554] Begrenzend wirkt insoweit, dass es sich um „personenbezogene" Daten handeln muss. Dabei orientierte sich das Bundesverfassungsgericht am ehemaligen § 2 Abs. 1 BDSG-alt[555], dessen Regelungsgehalt sich zwischenzeitlich in § 3 Abs. 1 BDSG-alt[556] fand. Heute enthält unter anderem § 46 Nr. 1 BDSG die maßgeblichen Legaldefinitionen zu „personenbezogenen Daten". Es sind dies „alle Informationen, die sich auf eine identifizierte oder identifizierbare Person (betroffene Person) beziehen." Bei allen Daten, die nicht direkt zu einer Identifizierung einer Person führen, vertrat das Bundesverfassungsgericht bereits im Volkszählungsurteil ein weites Verständnis von Identifizierbarkeit, bzw. Bestimmbarkeit und zog damit den Schutzbereich der informationellen Selbstbestimmung grundsätzlich weit: Neben dem Inhalt erhobener Daten war vor allem die durch die Informationstechnologie ermöglichte Nutzbarkeit und Verwendungsmöglichkeit für die Klassifizierung staatlicher Datenverarbeitung als Grundrechtseingriff entscheidend. Verarbeitungs- und Verknüpfungsmöglichkeiten können noch aus einem auf den ersten

551 Ähnlich *Schwabenbauer* in: *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch, G. Rn. 51f.

552 *Brink* in *Brink/H. Wolff*, BeckOK Datenschutzrecht, DS-GVO Syst. C. Verfassungsrechtliche Grundlagen Rn. 61ff.; vgl. auch BVerfGE 118, 168 (184): „Persönlichkeitsgefährdung".

553 Siehe dazu *Held,* Intelligente Videoüberwachung, 2014, S. 78 m.w.N.

554 *Di Fabio* in *Dürig/Herzog/R. Scholz,* Grundgesetz, Art. 2 Rn. 176.

555 BDSG vom 27.01.1977, BGBl. I, S. 201.

556 BDSG vom 14.08.2009, BGBl. I S. 2814.

Blick „belanglosen Datum" Bedeutung, also insbesondere Personenbezug, gewinnen. Das Bundesverfassungsgericht äußert dementsprechend bereits bei Schaffung des Rechts auf informationelle Selbstbestimmung: Es „gibt [...] unter den Bedingungen der automatischen Datenverarbeitung *kein* (Hervorh. FB) belangloses Datum mehr." Dieser Schutz von auf den ersten Blick vielleicht weniger relevanten Daten ist der unüberschaubaren Komplexität der automatisierten Datenverarbeitung geschuldet: Diese macht es dem Individuum unmöglich, die Bedeutung der es betreffenden personenbezogenen Daten in Gegenwart und Zukunft abschließend einzuschätzen. Jedes Datum kann durch Rekontextualisierung Bedeutung erlangen. Vor diesem Hintergrund besteht eine unwiderlegliche Vermutung der Relevanz aller personenbezogenen Daten.[557] Mit Blick auf den zur Zeit des Volkszählungsurteils im Gegensatz zu heute noch überschaubaren Entwicklungsstand elektronischer (Massen-)Datenverarbeitung war diese weite Konzeptualisierung schützenswerter Daten vorausschauend, auch wenn das Urteil genau unter diesem Gesichtspunkt kritisiert worden ist[558] und mit Blick auf das Datenvolumen der Gegenwart zu einer unübersehbaren Zahl von grundrechtstangierenden Situationen führt. Indessen hält gerade diese hohe Sensibilität des Rechts auf informationelle Selbstbestimmung auch neue Potenziale für die Quantifizierung seiner Beeinträchtigungen bereit.

Die Absage an die Belanglosigkeit von Daten, also an die Begrenzung des Schutzbereiches, wird im Wesentlichen auch vom EU-Datenschutzrecht gestützt. Um bei Daten einen Personenbezug herstellen zu können, kommt es in der Terminologie des unionalen Datenschutzrechts dafür maßgeblich darauf an, wann eine Identifizierbarkeit gegeben ist. Dies bestimmt sich danach, ob „nach allgemeinem Ermessen wahrscheinlich" ein Mittel zur Identifizierung eingesetzt werden würde, was sich wiederum nach objektiven Kriterien bemisst, wie Kostenaufwand, Zeitaufwand oder verfügbarer Technologie (ErwGr 21 JI-Richtlinie[559]). Wenn es dazu heißt, dass es im

557 *Brink* in *Brink/H. Wolff*, BeckOK Datenschutzrecht, DS-GVO Syst. C. Verfassungsrechtliche Grundlagen Rn. 71.

558 Siehe etwa *Aulehner,* Polizeiliche Gefahren- und Informationsvorsorge, 359 ff.

559 Die JI-Richtlinie ist die Abkürzung für die „RICHTLINIE (EU) 2016/680 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 27. April 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 und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates". Ihre Bedeutung wird unten S. 186 ff. näher erläutert.

sicherheitsrechtlichen Bereich vor allem darauf ankommen würde, „ob die Behörde als Verantwortliche über rechtliche Mittel verfügt, um sich die Daten verfügbar zu machen“[560] ist das als grundsätzlicher Rahmen einer rechtsstaatlich agierenden Polizeibehörde begrüßenswert. Allerdings dürften vor allem die technologischen Möglichkeiten regelmäßig stärker determinierend wirken.

Mit Blick auf polizeiliche Informationsinteressen bedeutet dies ganz grundsätzlich zunächst, dass informationelles Handeln der Polizei in der Regel den Schutzbereich des Rechts auf informationelle Selbstbestimmung tangieren wird, denn die Polizei interessiert sich vor allem für Personen. Selbst wenn Objekte in ihren Fokus geraten, ist fast immer auch das Verhältnis von Personen zum in Frage stehenden Objekt relevant.

So gefasst ist der Schutz, den das Recht vermittelt, indessen in erster Linie nur von individualistisch-partikularer Natur: Es sollen einzelne Grundrechtsträger:innen vor einzelnen Datenverarbeitungshandlungen geschützt werden. In eine ähnliche Richtung deutet auch die Formulierung des Bundesverfassungsgerichts, das informationelle Selbstbestimmungsrecht schütze „vor einzelne(n) Datenerhebungen“, trage aber Persönlichkeitsgefährdungen „nicht vollständig Rechnung […], die sich daraus ergeben, dass der Einzelne zu seiner Persönlichkeitsentfaltung auf die Nutzung informationstechnischer Systeme angewiesen ist und dabei dem System persönliche Daten anvertraut oder schon allein durch dessen Nutzung zwangsläufig liefert.“[561]

Vor diesem Hintergrund stellt sich die Frage, inwiefern vor der staatlichen Aggregation von Daten – denn diese stehen selten für sich allein, sondern dem Netzwerkparadigma der Gegenwart entsprechend fast ausschließlich in relationalen Verhältnissen zu anderen Daten – im Rahmen des informationellen Selbstbestimmungsrechts geschützt wird. Diese kollektive Dimension ist etwa mit der Diskussion um den Schutz vor Einschüchterungseffekten (auch: „chilling effects“[562]) angesprochen, die sich auch an einer Passage im Volkszählungsurteil des Bundesverfassungsgerichts festmachten lässt.[563] Allerdings wurde die Frage, ob dem einzelnen

560 So etwa *Müller/Schwabenbauer* in *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch des Polizeirechts, G. Rn. 434 auch mwN.

561 BVerfGE 120, 274 (312 f.) – Online-Durchsuchung.

562 *Townend* in Tumber/Waisbord (Hrsg.), The Routledge companion to media and human rights, 73.

563 BVerfGE 65, 1 (43) – Volkszählung: „Mit dem Recht auf informationelle Selbstbestimmung wären eine Gesellschaftsordnung und eine diese ermöglichende Rechts-

Bürger auch ein subjektiv-rechtlicher Schutz vor Einschüchterungseffekte zusteht, die sich aus der Unüberschaubarkeit der Wirkweisen und erfassten Daten automatisierter Datenverarbeitungsverfahren, insbesondere durch staatliche Stellen, ergeben, bisher nur wenig diskutiert.[564] Eine Auseinandersetzung damit liefert beispielsweise *Held*, der einen subjektiv-rechtlichen Schutz im Ergebnis verneint, da andere Freiheitsgrundrechte einen spezielleren Schutz der grundrechtlichen Entschließungsfreiheit vermitteln, während die informationelle Selbstbestimmung nur in wenigen Einzelfällen überhaupt einschlägig wäre.[565] Vor dem Hintergrund der eingangs erwähnten Passage des Volkszählungsurteils wäre indessen auch ein Schutz vor Einschüchterungseffekten durch die objektiv-rechtliche Dimension der informationellen Selbstbestimmung denkbar. Umfassende und kontinuierliche Beobachtung bzw. das Gefühl einer solchen sind generell geeignet, sich negativ auf das verfassungsrechtlich gewährleistete freiheitlich demokratische Gemeinwesen auszuwirken.[566]

Sinnvoller erscheint es aber den Ausgangspunkt in bereits gefestigter Dogmatik zu wählen: Informationelle Selbstbestimmung will die Freiheit gewähren, grundsätzlich selbst über die Preisgabe und Verwendung der eigenen personenbezogenen Daten zu bestimmen. Dieses Recht ist nicht nur in seinem Stellenwert für die Persönlichkeitsentwicklung zu sehen. Vielmehr ist die informationelle Selbstbestimmung in unserer zunehmend digitalisierten Umgebung von zentraler Bedeutung, insbesondere da diese Umgebungen tendenziell auf die Preisgabe und Verwendung personenbezogener Daten ausgelegt sind oder zunehmend nur darüber wirklich

ordnung nicht vereinbar, in der Bürger nicht mehr wissen können, wer was wann und bei welcher Gelegenheit über sie weiß. Wer unsicher ist, ob abweichende Verhaltensweisen jederzeit notiert und als Information dauerhaft gespeichert, verwendet oder weitergegeben werden, wird versuchen, nicht durch solche Verhaltensweisen aufzufallen. Wer damit rechnet, daß etwa die Teilnahme an einer Versammlung oder einer Bürgerinitiative behördlich registriert wird und daß ihm dadurch Risiken entstehen können, wird möglicherweise auf eine Ausübung seiner entsprechenden Grundrechte (Art. 8, 9 GG) verzichten. Dies würde nicht nur die individuellen Entfaltungschancen des Einzelnen beeinträchtigen, sondern auch das Gemeinwohl, weil Selbstbestimmung eine elementare Funktionsbedingung eines auf Handlungsfähigkeit und Mitwirkungsfähigkeit seiner Bürger begründeten freiheitlichen demokratischen Gemeinwesens ist."

564 Kritisch insoweit *Braun* in *Gola/Heckmann/Klug* ua, BDSG, § 47 Rn. 25.

565 *Held,* Intelligente Videoüberwachung, 2014, S. 82ff.

566 Vgl. dazu ausführlicher *Knierim* ZD 2011, 17, (20f.); siehe auch *Held, Intelligente Videoüberwachung*, 2014, S. 92.

funktionieren.[567] Im Hinblick auf Einschüchterungseffekte lautet die Frage dann, ob staatliches Handeln in irgendeine Richtung zwingend auf die Ausübung des Rechts (d.h. der Selbstbestimmung über Preisgabe und Verwendung personenbezogener Daten) wirkt. Denkbar ist dabei einerseits, dass Verhalten gemieden wird, das an die Verwendung oder Preisgabe der eigenen personenbezogenen Daten geknüpft ist, obwohl dies eigentlich von den Grundrechtsträger:innen gewünscht wäre.[568] Mit Blick auf normative Zwänge in Mehrheitsgesellschaften können davon etwa ohnehin bereits marginalisierte Gruppen betroffen sein.[569] Andererseits ist auch denkbar, dass personenbezogene Daten entgegen des eigenen Wunsches preisgegeben und verwendet werden, insbesondere, weil sich gesellschaftliche Normvorstellungen basierend auf den hierzu geschaffenen technologischen Möglichkeiten teilweise in die Richtung bewegen, mehr personenbezogenen Daten in den allgegenwärtigen digitalen Sphären öffentlich zu machen.[570] Um vor dem Hintergrund eines geänderten gesellschaftlichen Umgangs mit Daten potentiellen staatlichen Beobachtern nicht nachteilig aufzufallen, ist es zudem denkbar, dass sich Individuen gezwungen fühlen, mehr personenbezogene Daten preiszugegeben und zu verwenden.[571]

Dementsprechend geht es vorrangig darum, zu beantworten, wann staatliches Informationshandeln vermittelt über Einschüchterung dazu führt, dass nicht mehr selbstbestimmt über die Preisgabe von personenbezogenen Daten bestimmt wird – es handelt sich folglich stärker um eine Frage des Eingriffsverständnisses als um die Definierung des Schutzbereiches per se.

---

567 *Oermann/Staben* Der Staat 52 (2013), 630, (634);

568 Vgl. zu diesem Phänomen der „Selbst-Zensur" *Oermann/Staben* Der Staat 52 (2013), 630 (648f.), dort insb. Anm. 76 mit ausführlichen Nachweisen zu empirischen Erkenntnissen.

569 So hat sich in empirischen Untersuchungen in den Vereinigten Staaten gezeigt, dass dort lebende Muslim:innen ihr Online-Verhalten aufgrund von Online-Überwachungsmaßnahmen anpassen, siehe dazu *Sidhu* University of Maryland Law Journal of Race, Religion, Gender 7 (2007), 375 (391); gemessen wurden Einschüchterungseffekte aber auch im Zusammenhang mit den NSA-Enthüllungen durch *Edward Snowden*, vgl. etwa *Penney* Berkeley Tech. L.J. 31 (2016), 117, 117ff.; *Kaminski/Witnov* University of Richmond Law Review 49 (2015), 465 ff.; *Marthews/Tucker*, Government Surveillance and Internet Search Behavior, 2017, 2017.

570 So zeigt etwa die Studie von *Kezer/Sevi/Cemalcilar* ua Cyberpsychology 10 (2016), dass jüngere Nutzer:innen sozialer Netzwerke mehr Informationen über sich preisgeben. Gleichzeitig ssetzen sie hingegen auch häufiger Maßnahmen zum Schutz ihrer Privatsphäre in den sozialen Medien ein. .

571 So berichtet etwa *Boyd,* It's complicated, 74 ff. von strategischem Verhalten in der Informationspreisgabe in den sozialen Medien.

Während es nach Rechtsprechung des Bundesverfassungsgerichts jedenfalls einen Eingriff darstellt, wenn „Informationen […] gezielt zusammengetragen, gespeichert und gegebenenfalls unter Hinzuziehung weiterer Daten ausgewertet werden und sich daraus eine besondere Gefahrenlage für die Persönlichkeit des Betroffenen ergibt“,[572] ist es denkbar, bereits durch die einfache Möglichkeit umfassender staatlicher Beobachtung einen Eingriff anzunehmen. Einen dogmatisch schlüssigen Weg dazu liefern *Oermann und Staben*: Nehmen Grundrechtsträger:innen Einschränkungen ihrer Grundrechte aus eigenen Stücken anlässlich bestimmter staatlicher Handlungen vor, so kann ein „mittelbar-faktischer“ Eingriff vorliegen. Dazu ist es erforderlich, dass den Grundrechtsträger:innen aufgrund des staatlichen Handelns nicht mehr möglich ist, ihre Grundrechte in vollem Umfang zu verwirklichen, die Beeinträchtigung dem Staat zurechenbar ist und eine bestimmte Erheblichkeit erreicht.[573] *Oermann und Staben* erläutern mittelbare Grundrechtseingriffe durch Abschreckung vor dem Hintergrund der verbreiteten Praxis der Online-Streife, bei der es sich weitestgehend um heimliche Überwachungsmaßnahmen handelt, deren Abschreckungseffekt „nicht auf der konkreten Einzelmaßnahme und deren Wirkungen auf den einzelnen Grundrechtsträger, sondern […] aus dessen Bewusstsein über die Möglichkeit, jederzeit Betroffener einer entsprechenden Maßnahme sein zu können, [erwächst].“[574] Derartige panoptische Effekte können sich aber letztlich bei vielen staatlichen Handlungsweisen im Sicherheitsbereich ergeben, wenn sie für den Einzelnen nur unüberschaubar und undurchdringbar genug sind.

Damit wären polizeiliche Maßnahmen mit entsprechenden Wirkungen wie die Online-Streife nicht per se ausgeschlossen, nur stünden sie aufgrund ihrer freiheitsrechtlichen Wirkungen unter einem Gesetzesvorbehalt, womit sich die Möglichkeit der normativen Steuerung von informationellen Tätigkeiten der Polizei böte, die derzeit diffus und ungeregelt das Ensemble technologischer Überwachungsmöglichkeiten vergrößern.

Etwas eindeutiger ist die Verfassungslage hingegen bezüglich des Schutzes von Individuen in typischeren Massendatenverarbeitungskontexten, sowohl in individuell- als auch in kollektiv-aggregierter Hinsicht. So verbietet die Menschenwürde als Bestandteil der informationellen Selbstbestimmung

572 BVerfGE 120, 274 (344) – Onlinedurchsuchung.

573 *Oermann/Staben* Der Staat 52 (2013), 630 (637) mwN; näher zu den Einzelnen Voraussetzungen siehe a.a.O., (640ff.).

574 *Oermann/Staben* Der Staat 52 (2013), 630 (644).

eine Überwachung, die „sich über einen längeren Zeitraum erstreckt und derart umfassend ist, dass nahezu lückenlos alle Bewegungen und Lebensäußerungen des Betroffenen registriert werden und zur Grundlage für ein Persönlichkeitsprofil werden können."[575] Eine solches Totalausforschungsverbot soll aber aufgrund seiner Einzelfallbezogenheit grundsätzlich wenig materiellen gesetzgeberischen Handlungsbedarf auslösen. Vielmehr soll den potentiell beeinträchtigten individuellen Schutzbedürfnissen durch prozedurale Regelungen Rechnung getragen werden, wo es zu solchen „additiven Grundrechtseingriffen" kommt.[576] Teilkongruenzen mit der Ausforschung von tiefliegenden Persönlichkeitsstrukturen weist auch die Figur des sogenannten Kernbereichsschutzes aus, der explizit seit den Siebzigern vom Bundesverfassungsgericht ausgearbeitet wurde.[577] Zum Kernbereichsschutz „gehört die Möglichkeit, innere Vorgänge wie Empfindungen und Gefühle sowie Überlegungen, Ansichten und Erlebnisse höchstpersönlicher Art zum Ausdruck zu bringen, und zwar ohne Angst, dass staatliche Stellen dies überwachen. Vom Schutz umfasst sind auch Gefühlsäußerungen, Äußerungen des unbewussten Erlebens sowie Ausdrucksformen der Sexualität."[578] Allerdings ist auch dieses dogmatische Konzept sehr stark anhand von Eingriffsbefugnissen, wie der Wohnraumüberwachung, entwickelt worden, sodass die Frage, inwieweit durch auswertende, verknüpfende und analysierende Datenverarbeitungen möglicherweise kernbereichsrelevante Informationen zutage gefördert werden können, ungeklärt ist.[579] Im BKAG-Urteil deutet das Bundesverfassungsgericht allerdings eine Zuwendung auch der Auswertungsebene an. Anders als bei Kernbereichsgefahren die bei der Überwachung eines Ortes „privater Zurückgezogenheit" bestehen, geht es bei der Auswertung von Massendatenbeständen – im BKAG-Urteil im Kontext der Online-Durchsuchung – darum, das „Auslesens höchstvertraulicher Informationen aus einem Gesamtdatenbestand von ohnehin digital vorliegenden Informationen [zu verhindern], die in ihrer Gesamtheit typischerweise nicht schon als solche den Charakter der Privatheit wie das Verhalten oder die Kommunikation in einer Wohnung aufweisen."[580]

575 BVerfGE 109, 279 (322) – Großer Lauschangriff.
576 *Müller/Schwabenbauer* in *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch des Polizeirechts, G. Rn. 171.
577 Erstmals so bezeichnet in BVerfGE 34, 238 (245) – Tonband.
578 BVerfGE 109, 279 (313) – Großer Lauschangriff.
579 So *Müller/Schwabenbauer* in *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch des Polizeirechts, G. Rn. 146.
580 BVerfGE 141, 220 (307) – Bundeskriminalamtgesetz.

Da datenintensive Maßnahmen wie die Online-Durchsuchung dem Prinzip „ganz oder gar nicht“[581] folgten, müssen – wenn kernbereichssensible Informationen nicht bereits vor Erhebung technisch ausgesiebt werden können – Sicherungen auf der Auswertungsebene eingezogen werden. Das Gericht schlägt hier die Sichtung durch eine unabhängige Stelle vor, die „kernbereichsrelevante Informationen vor ihrer Kenntnisnahme und Nutzung“ durch die jeweilige Polizei „herausfiltert“.[582] Ein solches Verständnis von kernbereichssensiblen Informationen geht hingegen weiter davon aus, dass sich diese eindeutig als einzelne Datenpunkte identifizieren lassen. Höchstpersönliche Informationen können jedoch – und das ist die eigentliche Schwierigkeit im Bereich des persönlichkeitsrechtlichen Kernbereichsschutzes – auch durch die Verknüpfung von augenscheinlich „belanglosen“ Datenpunkten gewonnen werden.[583]

Während diese individuell-aggregierte Datenebene bisher nur begrenzt dogmatisch verarbeitet wurde, ist die akademische Diskussion um die Bevorratung von Massendaten einer großen Zahl von Menschen als kollektiv-aggregierte Datenebene insbesondere aufgrund der öffentlichen Debatte und dadurch bedingter Urteile von Bundesverfassungsgericht und Europäischem Gerichtshof wesentlich weiter. Generell gilt für das deutsche Verfassungsrecht ein Verbot der Bevorratung personenbezogener Daten zu unbestimmten oder noch nicht bestimmbaren Zwecken, was sich aus der für das informationelle Selbstbestimmungsrecht zentralen Zweck-Dogmatik ergibt.[584] Damit ist eine Bevorratung zu Zwecken der Sicherheitsgewährleistung zwar nicht per se ausgeschlossen, hängt in ihrer Verfassungsmäßigkeit aber von der konkreten Ausgestaltung im jeweiligen Gesetz ab.[585] Die Diskussion zu den zulässigen Zwecken und damit letztlich zur Reichweite des Schutzes vor der Bevorratung von Daten ist indessen noch stark

581 BVerfGE 141, 220 (307) – Bundeskriminalamtgesetz.

582 BVerfGE 141, 220 (307) – Bundeskriminalamtgesetz.

583 Bekanntes Beispiel hierfür ist etwa die Ableitung von sexueller Orientierung aus Freundschaftsbeziehungen oder sonstigem Online-Verhalten in sozialen Medien wie facebook, s. *Jernigan/Mistree* FM 2009; *Nikhil X. Bhattasali/Esha Maiti*, Machine “Gaydar”: Using Facebook Profiles to Predict Sexual Orientation, https://cs229.stanford.edu/proj2015/019_report.pdf (Stand: 01.10.2023); *Aaron Loh/Kenneth Soo/Hui-lin Xing*, Predicting Sexual Orientation based on Facebook Status, http://cs229.stanford.edu/proj2016/report/LohSooXing-PredictingSexualOrientationBasedOnFacebookStatusUpdates-report.pdf (Stand: 01.10.2023).

584 BVerfGE 65, 1 (45) – Volkszählung.

585 *Müller/Schwabenbauer in Bäcker/Denninger/Graulich* (Hrsg.), Handbuch des Polizeirechts, G. Rn. 174.

im Fluss: Zwar hat der Europäische Gerichtshof hier gerade einige Zwecke festgelegt, etwa die Bekämpfung schwerer Kriminalität, wobei hier weitere Beschränkungen wie ihre Vorhersehbarkeit postuliert wurden.[586] Jedoch geschah dies in einem Urteil, in dem zuvor der auf die deutsche Rechtslage bezogene Verfahrensteil abgetrennt worden war, sodass sich – auch in Anbetracht dann zu erwartender Gesetzgebungsaktivität und darauf antwortender Verfassungsrechtsprechung – die Rahmenbedingungen für den Schutz vor Bevorratung gegenwärtig noch in der Diskussion befinden.

Insgesamt ist auf Ebene des Schutzes, den das Recht auf informationelle Selbstbestimmung gewährleistet, eine starke individualistische Verortung auszumachen, was auch der prinzipiellen Struktur grundrechtlicher Freiheitsrechte entspricht. Da Massendaten jedoch vor allem in ihrer Vernetzung und Aggregation Aussagekraft entwickeln und zur Akkumulation von Datenmacht bei gesellschaftlichen Akteuren führen können, erscheint die Dimension eines Schutzes, die Kollektive und Datenakkumulationen stärker in den Blick nimmt, zunehmend wichtiger, worauf die Verfassungsdogmatik konzeptuell bisher eher im Eingriffs- und Rechtfertigungsverständnis reagiert hat.

b) Eingriff

Lange Zeit galt der Umgang mit personenbezogenen Daten durch Sicherheitsbehörden nicht als Grundrechtseingriff.[587] Der dogmatische Wandel hin zum heutigen Eingriffsverständnis ist in erster Linie durch das Volkszählungsurteil vollzogen worden. Dabei war nicht so sehr der Schritt vom klassischen zum modernen Eingriffsbegriff für diese Entwicklung entscheidend. Vielmehr war die „fortschreitende grundrechtliche Ausfaltung des Persönlichkeitsschutzes“[588] – auch schon in der Zeit vor dem Volkszählungsurteil[589] – derjenige Faktor, der zu dem für das Recht auf informationelle Selbstbestimmung eigenen „Informationseingriff“ führte.[590]

586 EuGH, 05.04.2022 - C-140/20, Rn. 59 ff.
587 *Schwabenbauer* in: *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch, G. Rn. 4.
588 *Schwabenbauer* in: *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch, G. Rn. 6.
589 Vgl. etwa beispielhaft das einflussreiche *Steinmüller*-Gutachten, BT-Drs. VI/3826, S. 86.
590 *Kowalczyk,* Datenschutz im Polizeirecht, S. 49

Nach diesem Verständnis stellt nunmehr prinzipiell jeder Verarbeitungsschritt im „Lebenszyklus" eines personenbezogenen Datums einen Eingriff dar.[591] Die Breite der damit erfassten Umgangsweisen mit Daten wird einfachgesetzlich adäquat durch Art. 3 Nr. 2 JI-Richtlinie, umgesetzt in § 46 Nr. 2 BDSG, abgebildet: „Verarbeitung" meint demzufolge „jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung […]".

Ein solcher Eingriff infolge der Verarbeitung von Daten ist nicht an menschliche Wahrnehmung der Daten geknüpft, sondern ist bereits bei technischer Fixierung der Daten oder bei technischem Datenumgang gegeben.[592] Vor dem Hintergrund, dass die Bejahung eines Eingriffes nicht von einem konkret festgestellten Nachteil abhängt, sondern jede Datenverarbeitung per se durch die möglicherweise daraus folgende Ent- und Neukontextualisierung benachteiligend wirkt, schlägt *Schwabenbauer* ein Wiederaufgreifen der Formulierung *Schwans* vor, die mit Blick auf das Recht auf informationelle Selbstbestimmung als zutreffende Charakterisierung eines wichtigen Teilaspektes erscheint:[593] Es gibt eine grundrechtlich geschützte „Freiheit vor staatlicher Informationssammlung und Informationsweitergabe"[594]. Darin erschöpft sich der verfassungsrechtliche Schutz der Privatheit indessen nicht. Während das Grundgesetz an verschiedenen Stellen Artikel zum Schutz unterschiedlicher Privatheitssphären[595] bereithält – etwa Art. 13 Abs. 1 GG, der eine räumliche Dimension schützt, die wiederum durch Art. 10 Abs. 1 GG bis zu einem gewissen Grad ausgedehnt wird[596]– ist für die vorliegende Arbeit vor allem die informationelle Privatheit[597] und ihr

591 *Schwabenbauer* in: *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch, G. Rn. 9.
592 *Schwabenbauer* in: *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch, G. Rn. 10.
593 Ebd.
594 *Schwan* VerwArch 66 (1975), 120 (121).
595 *Schwabenbauer* in: *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch, G. Rn. 46, spricht in diesem Zusammenhang von „Privatheit als grundrechtliche Identitätsschicht".
596 *Schwabenbauer* in: *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch, G. Rn. 59.
597 Für *Schwabenbauer* in: *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch, G. Rn. 54, beschreibt die informationelle Privatheit die Beherrschung des Einzelnen darüber, wer was von ihm weiß.

Schutz durch das informationelle Selbstbestimmungsrecht von Interesse.[598] Denn der Umgang mit den Daten im polizeilichen Informationswesen, worunter im Grunde bis auf das Erheben alle Verhaltensweisen der Legaldefinition des § 46 Nr. 2 BDSG fallen,[599] spielt sich nicht in der räumlichen oder kommunikativen Sphäre des Individuums, sondern im genuin informationellen Bereich ab. Dabei stellen alle Akte des polizeilichen Datenumgangs einen Eingriff dar, sofern sie diesen nicht gerade beenden, wie etwa die Löschung von Daten.

Neben der Frage, welche Arten des Datenumgangs als Eingriffe zu werten sind, ist aus grundrechtlicher Sicht auch zentral, wie intensiv durch bestimmte Datenverarbeitungen in das Recht auf informationelle Selbstbestimmung eingegriffen wird. Wesentliche Kriterien hierfür sind der Informationsgehalt des erhobenen Datums, die Heimlichkeit der Erhebungsmaßnahme sowie ihre Streubreite.[600]

Der Informationsgehalt ist hierbei im Sinne einer mehr oder weniger stark ausgeprägten Persönlichkeitsrelevanz zu verstehen. Insbesondere solche Daten, die informationell bestimmten grundrechtlichen Schutzbereichen wie beispielsweise Art. 3 Abs. GG zugeordnet werden können und somit als hoch persönlichkeitsrelevant einzustufen sind, steigern die Intensität eines Eingriffs. Mit Blick auf die inferenzielle Informationsgewinnung wie sie für die ständige Rekombination von einzelnen Datenpunkten im Rahmen von Massendatenverfahren typisch ist, erweist sich der Informationsgehalt *eines* Datums allerdings zunehmend als unzureichend für Eingriffsintensitätsbestimmungen. Der Informationsgehalt eines Datums wird insofern zunehmend relational. Er ergibt sich in Verbindung zu anderen verfügbaren Daten, für die wiederum dasselbe hinsichtlich ihres Informationsgehalts gilt. Diese Fluidität der informationellen Implikationen von (Massen-)Daten in die Eingriffsdogmatik zu übersetzen, steht im Wesentlichen noch aus. Zwar ist mit dem sog. „additiven" Grundrechtseingriff[601] in Ansätzen eine Figur kreiert, die Akkumulationen von Daten abbildet. Je-

598 *Schwabenbauer* in: *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch, G. Rn. 60.

599 Das heißt das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung von Daten.

600 Siehe dazu und zum Folgenden *Müller/Schwabenbauer* in *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch des Polizeirechts, G. Rn. 119 ff., der freilich noch weitere Aspekte als Kriterien nennt, die hier indessen als eher nachrangig betrachtet werden.

601 Siehe dazu weiter unten im selben Unterabschnitt.

doch bezieht sich dieser Spezialfall des Eingriffs auf eine Person und nicht auf die Aggregierung von Daten über viele Personen und den Inferenzen, die man daraus wiederum für einzelne oder mehrere Individuen ableiten kann.

Zweites wesentliches Kriterium zur Bestimmung der Intensität von Informationseingriffen ist die Heimlichkeit der Maßnahme. Ausgehend von dem Gedanken, dass die Polizei im Umgang mit Daten ganz überwiegend dem Grundsatz der Offenheit folgen soll,[602] wird mit Blick auf das praktische Erfordernis nach heimlichen Ermittlungsmaßnehmen von einer Intensitätssteigerung ausgegangen. Die Gründe dafür sind vielfältig. *Schwabenbauer* nennt etwa das der Heimlichkeit inhärente Konfliktpotenzial mit der Privatheit, mögliche Steuerungsausfälle bezüglich der Rechtskontrolle, auch im Wege des Rechtsschutzes, die Gefahr der Schwächung der exekutiven Gesetzesbindung sowie Authentizitätsprobleme, also die Schwierigkeit, die Richtigkeit der Daten ohne Mitwirkung von Betroffenen zu überprüfen.[603] Diese Kriterien wurden vor allem anlässlich von verdeckten Ermittlungsmethoden entwickelt. Aber auch Datenverarbeitungen, die sich an die originäre Erhebung anschließen, also intern im polizeilichen Informationswesen durchgeführt werden, lassen sich prinzipiell mit dem Etikett der Heimlichkeit versehen, denn sie laufen zumeist ohne Beteiligung und ohne Wissen der Betroffenen ab. Zudem sind auch diese nachgeschalteten Datenverarbeitungen mit exakt denselben Problemen behaftet wie heimliche Erhebungsmaßnahmen. Durch rekombinierende und analysierende Auswertungsverfahren etwa können Sachverhalte bekannt werden, die dem polizeilich nicht-relevanten Privatbereich zufallen. Auch die Rechtskontrolle ist erschwert, wenn fachliche Verfahren (den Bürger:innen) nicht oder (den Aufsichtsbehörden) nur begrenzt bekannt sind. Zudem bestehen bei Datenverarbeitungen im Rahmen des Informationswesens gleichfalls die Gefahr der Schwächung der Gesetzesbindung sowie das Problem der mangelnden Authentifizierbarkeit der informationellen Konstruktionen, zu denen Polizist:innen auf Grundlage von Daten gelangen. Insofern lässt sich dem Datenumgang im polizeilichen Informationswesen ganz grundsätzlich eine gesteigerte Eingriffsintensität zusprechen.

Drittes wichtiges Kriterium ist die Streubreite eines Eingriffs, also die Zahl betroffener Personen. Je höher die Streubreite, desto intensiver der

602 BVerfGE 133, 277 (328) – Antiterrordateigesetz.

603 *Müller/Schwabenbauer* in *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch des Polizeirechts, G. Rn. 126.

Eingriff, denn auch wenn mit der Streubreite als quantitativer Kategorie noch nichts über die Ausforschungstiefe gesagt ist, werden mit streuenden Maßnahmen tendenziell viele Personen erfasst, die keinen direkten Anlass hierfür gegeben haben. Auch dieses Kriterium bezieht sich im Ursprung eher auf Massendatenerhebungsmaßnahmen. Es lässt sich aber auf Datenauswertungsverfahren übertragen, die mit breiter Datenbasis agieren.

Neben dieser Intensitätsbestimmung einzelner punktueller Eingriffe ist aber mit Blick auf das Volumen an verfügbaren Daten und die Vielzahl von Verarbeitungstechniken eine Weitung der Perspektive auf Eingriffskonstellationen geboten. In diesem Sinne hat sich bereits die Figur des additiven (oder auch: kumulativer) Grundrechtseingriff herausgebildet, der das kumulative Zusammentreffen von mehreren Datenerhebungsmaßnahmen in ein und derselben Person erfassen möchte. Der oder den beteiligten Ermittlungsbehörde(n) sind insofern Verfahrensanforderung auferlegt, um einem unverhältnismäßigen additiven Grundrechtseingriff vorzubeugen.[604] Neben dem Gesetzgeber, der beobachten muss, „ob die bestehenden verfahrensrechtlichen Vorkehrungen auch angesichts zukünftiger Entwicklungen geeignet sind, den Grundrechtsschutz effektiv zu sichern", sodass „unkontrollierte Ermittlungsmaßnahmen verschiedener Behörden verlässlich verhindert werden können",[605] ist damit auch die Rechtsanwendungsebene angesprochen. Sicherheitsbehörden müssen „koordinierend darauf Bedacht nehmen, dass das Ausmaß der Überwachung insgesamt beschränkt bleibt."[606] Dogmatisch operationalisieren lässt sich dies bisher grundsätzlich über die Verhältnismäßigkeit einer neu hinzukommende Maßnahme in einem laufenden Verfahren mit bereits eingesetzten Maßnahmen.[607] Insgesamt scheint das Konzept des additiven Grundrechtseingriffs weiterhin ausbaufähig. Vor allem der starke Fokus auf Datenerhebungsmaßnahmen wirkt in Anbetracht des Umstandes, dass es die *Daten* selbst sind, die letztlich die Informationstiefe polizeilicher Erkenntnis bestimmen, etwas falsch fokussiert. Sinnvoll könnte es insofern sein, dem additiven Eingriff die Facette des *aggregierten* Eingriffes hinzuzufügen. Damit ist ein Eingriff gemeint, der durch die Anhäufung, das Zusammentragen und Zusammen-

604 BVerfGE 112, 304 (319 f.) – Global Positioning System.
605 BVerfGE 112, 304 (319 f.) – Global Positioning System, kritisch dazu *Müller/Schwabenbauer* in *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch des Polizeirechts, G. Rn. 346.
606 BVerfGE 141, 220 (280 f.) – Bundeskriminalamtsgesetz.
607 *Müller/Schwabenbauer* in *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch des Polizeirechts, G. Rn. 372.

führen von Daten über eine Person zu charakterisieren ist. Auf diese Weise könnte ein Eingriffsverständnis ermöglicht werden, das sich weniger an dem Zusammenkommen von Erhebungsmaßnahmen festmacht, sondern stärker die letztlich anfallenden Daten und deren informationellen Gehalt, wie er sich im Wege von variablen und relationalen Rekombinationen der Daten ergibt, in den Blick nimmt.

c) Rechtfertigung

Das Recht auf informationelle Selbstbestimmung wird nicht schrankenlos gewährleistet. Schon im Volkszählungsurteil hat das Bundesverfassungsgericht die Sozialbezüge von Kommunikation und Information herausgestellt und einer Daten-"Herrschaft" des Einzelnen eine Absage erteilt. Es müssen vielmehr Einschränkungen des Rechts im überwiegenden Allgemeininteresse hingenommen werden.[608] Für das verfassungsrechtlich in Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG verankerte Grundrecht finden in erster Linie die Schranken des Art. 2 Abs. 1 GG – dabei ist insbesondere die verfassungsmäßige Ordnung, d.h. die Gesamtheit der mit der Verfassung in Einklang stehenden Normen, von Belang [609] – Anwendung, sodass für Einschränkungen der informationellen Selbstbestimmung zunächst eine formalgesetzliche Grundlage erforderlich ist.[610] Eine solche muss den Grundsätzen der Verhältnismäßigkeit sowie der Bestimmtheit genügen.[611] Dreh- und Angelpunkt hierfür ist der Zweck der gesetzlichen Grundlage; ohne Bestimmung der Erhebungs- und Verarbeitungszwecke ist eine Prüfung der Rechtmäßigkeit von Eingriffen – sowohl auf Rechtsetzungs- als auch auf Rechtsanwendungsebene – in das Recht auf informationelle Selbstbestimmung nicht möglich.[612] Dieser „Grundsatz der Zweckbindung" ist das zentrale normative Instrument zur Steuerung von Informationseingriffen. Als solches kann es bei der Veränderung von informationstechnologischen

608 BVerfGE 65, 1 (42f.) – Volkszählung.
609 BVerfGE 6, 32 (38ff.) – Elfes.
610 *Brink* in *Brink/H. Wolff*, BeckOK Datenschutzrecht, DS-GVO Syst. C. Verfassungsrechtliche Grundlagen Rn. 93.
611 BVerfGE 65, 1 (43, 46) – Volkszählung.
612 Vgl. schon BVerfGE 65, 1 (45) – Volkszählung: „Erst wenn Klarheit darüber besteht, zu welchen Zwecken Angaben verlangt werden und welche Verknüpfungsmöglichkeiten und Verwendungsmöglichkeiten bestehen, läßt sich die Frage einer zulässigen Beschränkung des Rechts auf informationelle Selbstbestimmung beantworten."

Zusammenhängen nicht in Stein gemeißelt bleiben und wird dementsprechend vom Bundesverfassungsgericht fortlaufend ausgestaltet.

aa) Der verfassungsrechtliche Grundsatz der Zweckbindung

Aus dem Verhältnismäßigkeitsgrundsatz ergibt sich, dass jedwede Verarbeitung personenbezogener Daten einem (zulässigen) Ziel zu dienen hat, also nicht reiner Selbstzweck sein darf. Um nicht das Bestimmtheitsgebot zu verletzten muss dieser Zweck wiederum hinreichend bestimmt sein; eine Verarbeitung ziellos „ins Blaue hinein" darf dementsprechend nicht erfolgen. Schließlich muss die inhaltliche Bestimmung des Zweckes im Kern durch den Gesetzgeber erfolgen, soll nicht das verfassungsrechtliche Demokratiegebot missachtet werden. Für polizeiliche Datenverarbeitungen ergibt sich aus diesen Vorgaben das verfassungsrechtliche Gebot der Zweckbindung. Möglich ist die Festlegung mehrerer Zwecke innerhalb der jeweiligen Rechtsgrundlage für die Verarbeitung, wobei jeder der Zwecke nachvollziehbar begründet werden muss.[613]

Die vom Zweckbindungsgrundsatz ausgehende Steuerungswirkung ist dabei maßgeblich vom Bestimmtheitsgrundsatz abhängig. Je präziser bzw. enger eine Zweckfestlegung auf einfachgesetzlicher Ebene erfolgt, desto eher kommt es zu einem erneut rechtfertigungsbedürftigen zweckändernden Datenumgang. Diese Unterstützungswirkung des Bestimmtheitsgebots wird vom Bundesverfassungsgericht dahingehend interpretiert, dass für den öffentlichen Bereich eine hinreichend präzise Beschreibung des Verarbeitungszweckes der betroffenen personenbezogenen Daten erforderlich ist.[614] Die Beurteilung muss für jede Rechtsgrundlage einzelfallbezogen erfolgen, kann sich jedoch an einer Je-desto-Formel orientieren: Je intensiver der Eingriff, desto bestimmter muss die Zweckbestimmung sein. Kriterien für die Beurteilung der Intensität sind dabei zumindest die Art der betroffenen Daten, der Bezug der Daten zum allgemeinen Persönlichkeitsrecht, die möglichen Verwendungszusammenhänge der Daten, die Datenmenge, die Art der Datenerhebung, die Verknüpfungsmöglichkeiten, die Verbrei-

613 *Schwabenbauer* in: *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch, G. Rn. 12, vgl. auch *Wolff* in *Brink/H. Wolff*, BeckOK Datenschutzrecht, DS-GVO Syst. A. Prinzipien des Datenschutzrechts Rn. 11ff.

614 BVerfGE 120, 351 (366) – Steuerliche Auslandsdaten.

tungsfähigkeit und die Missbrauchsgefahr.[615] Im Bereich polizeilicher Datenverarbeitung, in dem es unter Effektivitätsgesichtspunkten oftmals auf die Maximierung der vorgenannten Aspekte ankommt, ist daher ein besonderes Augenmerk auf die Bestimmtheit von Datenverarbeitungsbefugnissen zu legen.

Zudem kann auch erst über die Festsetzung eines Zwecks im Sinne eines legitimen Ziels die Verhältnismäßigkeit eines Eingriffs – also seine Geeignetheit, Erforderlichkeit und Angemessenheit zur Zweckerreichung – bestimmt werden. Zwecke der polizeilichen Datenverarbeitung lassen sich mit der Verhütung, Aufklärung und Verfolgung von Straftaten sowie der Gefahrenabwehr sehr breit fassen und werden in dieser Reichweite auch häufig in den gesetzlichen Grundlagen polizeilichen Datenumgangs als Zweckbestimmungen verwendet. Im Rahmen der Verhältnismäßigkeit ist vor allem auch der Grundsatz der Erforderlichkeit für die Umsetzung des Zweckbindungsgrundsatzes von großer Bedeutung. Danach ist eine Datenverarbeitung nur dann zulässig, soweit sie zur Erreichung des Zweckes notwendig ist. Vor allem für die Ebene der Rechtsanwendung sollten vom Grundsatz der Erforderlichkeit wichtige Steuerungsimpulse ausgehen, indem Rechtsanwender:innen dazu angehalten werden, den gegenwärtigen Datenverarbeitungsprozess auf mögliche Alternativen hin zu reflektieren. Zudem lässt sich nur über den Zweck einer Datenverarbeitung ihre Angemessenheit – generell wie im Einzelfall – bewerten. Hier sind die Zwecke, aus polizeilicher Sicht also in erster Linie der Schutz vor mehr oder weniger erheblichen Gefahren oder die Verhütung, Aufklärung und Verfolgung von mehr oder weniger schweren Straftaten, mit der jeweils durch die Maßnahme im Allgemeinen oder speziellen Anwendungsfall ausgehenden Eingriffsintensität in ein ausgeglichen abgewogenes Verhältnis zu bringen.[616] Insoweit lässt sich auch von „Zweckhierarchien“[617] sprechen: Werden weniger sensible Daten verarbeitet, so können die generellen Polizeizwecke der Gefahrenabwehr und Strafverfolgung ausreichende Zweckbestimmungen darstellen. Sensiblere Daten oder sonst eingriffsintensivere Maßnahmen erfordern demgegenüber spezifischere und anspruchsvollere Zwecke wie etwa die Abwehr einer dringenden Gefahr für den Bestand oder die Sicherheit des Bundes oder eines Landes oder für Leib, Leben oder Freiheit einer

615 Siehe dazu etwa *Wolff* in *Brink/H. Wolff*, BeckOK Datenschutzrecht, DS-GVO Syst. A. Prinzipien des Datenschutzrechts Rn. 19 ff.

616 *Müller/Schwabenbauer* in *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch des Polizeirechts, G. Rn. 195 ff.

617 *Gola/Heckmann/Klug* ua, BDSG, § 47 Rn. 18.

Person oder die Verfolgung von schwere(re)n Katalogstraftaten. Auch diese Abstufung geht indessen von einer prinzipiell im Vorhinein feststellbaren Sensibilität des informationellen Gehalts eines Datums aus, was bei einem Fokus auf die Invasivität der Erhebungsmaßnahme auch noch sinnvoll sein kann. Im Rahmen der anschließenden Verarbeitung hingegen können aus der relationalen Zusammenführung wenig sensibler Daten tiefgehende Persönlichkeitsinformationen rekonstruiert werden, sodass insofern stets eine hohe Zweckschwelle in der Rechtsgrundlage festzuschreiben ist und in der Rechtsanwendung besondere Anforderungen an die Prüfung der zweckbezogenen Verhältnismäßigkeit zu stellen sind.

bb) Die zweckwahrende Weiternutzung

Im Bereich polizeilicher Datenverarbeitung hat der Grundsatz der Zweckbindung zusätzliche Konkretisierung erfahren. Dem BKAG-Urteil des Bundesverfassungsgerichts nach wird die Reichweite der Zweckbindung durch die jeweilige Datenerhebungs- bzw. Datenverarbeitungsbefugnis determiniert und diese erhalten ihren Zweck aus dem zugrundeliegenden polizeilichen Verfahren.[618] Anhand dieser einzelfallbezogenen Zweckfestlegung eines Datums kann dann beurteilt werden, ob ein Datenumgang die Zweckbindung einhält oder zweckändernd erfolgt. Dabei ist allerdings zu beachten, dass nunmehr nicht mehr jede Verarbeitung von Daten außerhalb des ursprünglichen Verfahrens eine Zweckänderung darstellt.

Während das Gericht selbst und etliche Stimmen aus dem Schrifttum bis 2016 davon ausgingen,[619] dass die Datenverarbeitung über das konkrete Anlassverfahren hinaus prinzipiell als Zweckänderung zu behandeln sei, hat das BKAG-Urteil die verfassungsrechtlichen Rahmenbedingungen neu gesteckt:

> „Eine weitere Nutzung innerhalb der ursprünglichen Zwecksetzung kommt damit nur seitens derselben Behörde im Rahmen derselben Aufgabe und für den Schutz derselben Rechtsgüter in Betracht wie für die Datenerhebung maßgeblich: Ist diese nur zum Schutz bestimmter Rechtsgüter oder zur Verhütung bestimmter Straftaten erlaubt, so

618 BVerfGE 141, 220 (325) – Bundeskriminalamtgesetz.

619 Siehe die Nachweise bei *Schwabenbauer* in: *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch, G. Rn. 16 Fn. 52, 53.

> begrenzt dies deren unmittelbare sowie weitere Verwendung auch in derselben Behörde, soweit keine gesetzliche Grundlage für eine zulässige Zweckänderung eine weitergehende Nutzung erlaubt."[620]

Damit ist der Bereich innerhalb dessen Akte polizeilicher Datenverarbeitung noch als zweckerfüllend anzusehen sind in nicht unerheblicher Weise ausgeweitet worden. Aus dem zweiten Satz des angeführten Urteilszitates scheint sich überdies noch zu ergeben, dass keine Identität zwischen den geschützten Rechtsgütern und zu verhütenden Straftaten im Anlassverfahren und im Verfahren, in dem es zur zweckwahrenden[621] Weiternutzung kommt, bestehen muss. Gewährt eine Rechtsgrundlage etwa einer Polizeibehörde die Erhebung von Daten zur Abwehr einer Gefahr für das Leben und die Freiheit einer Person, so können Daten, die im Anlassverfahren zur Abwehr einer Lebensgefahr erhoben worden sind, ebenfalls von derselben Polizeibehörde zur Abwehr einer Gefahr für die Freiheit einer Person weiter genutzt werden.[622] Damit wird insbesondere der sog. Zufallsfund erfasst.[623] Es besteht allerdings das Risiko, dass die Polizei durch eine extensive Festlegung der im Ausgangsverfahren zu schützenden Rechtsgüter oder zu verhütenden Straftaten die Reichweite der Befugnis zur zweckwahrenden Weiternutzung ausweitet und die beabsichtigte Begrenzungsfunktion leer läuft.[624]

Zudem ist für die zweckwahrenden Weiternutzung nicht erforderlich, dass dieselbe Eingriffsschwelle wie im Rahmen der Datenerhebung – etwa eine bestimmte Stufe einer Gefahr oder des Tatverdachts – erreicht ist. Diese Schwellen, die für die Datenerhebung erreicht sein müssen, gehören nicht zu „den Zweckbindungen, die für jede weitere Nutzung der Daten seitens derselben Behörde je neu beachtet werden müssen".[625] Das Bundesverfassungsgericht führt weiter aus, dass die Eingriffsschwellen lediglich „den Anlass, aus dem entsprechende Daten erhoben werden dürfen [bestimmen], nicht aber die erlaubten Zwecke, für die die Daten der Behörde

620 BVerfGE 141, 220 (325) – Bundeskriminalamtgesetz.
621 BVerfG-Urteil des Ersten Senats vom 16. Februar 2023 (Automatisierte Datenanalyse), passim.
622 Beispiel nach *Bäcker* Stellungnahme BKAG, A-Drs. 18(4)806 D, S. 12.
623 *Schwabenbauer* in: *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch, G. Rn. 18.
624 So in der Auslegung durch *Ruthig* in *Schenke/Graulich/Ruthig*, Sicherheitsrecht, § 12 BKAG Rn. 10; zu Recht kritisch dazu *Arzt* in *Möstl/Kugelmann* (Hrsg.), Beck'scher Online-Kommentar Polizei- und Ordnungsrecht Nordrhein-Westfalen, § 23 PolG NRW Rn. 17.
625 BVerfGE 141, 220 (325) – Bundeskriminalamtgesetz.

dann zur Nutzung offen stehen."[626] Neben den bereits genannten Anforderungen an eine zweckwahrende Weiternutzung der Daten ist folglich keine weitere Anforderung zu erfüllen, wenn diese als Spurenansatz für folgende Ermittlungen genutzt werden. Der entsprechenden Behörde steht es mithin – bei entsprechender Rechtgrundlage – frei,

> „die insoweit gewonnenen Kenntnisse zum Schutz derselben Rechtsgüter und im Rahmen derselben Aufgabenstellung – allein oder in Verbindung mit anderen ihr zur Verfügung stehenden Informationen – als schlichten Ausgangspunkt für weitere Ermittlungen nutzen. Dies trägt dem Umstand Rechnung, dass sich die Generierung von Wissen – nicht zuletzt auch, wenn es um das Verstehen terroristischer Strukturen geht – nicht vollständig auf die Addition von je getrennten, nach Rechtskriterien formell ein- oder ausblendbaren Einzeldaten reduzieren lässt. In den dargelegten Grenzen erkennt das die Rechtsordnung an. Diese Grenzen gewährleisten zugleich, dass damit keine Datennutzung ins Blaue hinein eröffnet ist."[627]

Etwas anderes gilt indessen für die besonders eingriffsintensiven Maßnahmen der Wohnraumüberwachung und der Online-Durchsuchung. Eine weitere Nutzung der Daten bewegt sich nur dann noch im ursprünglichen Erhebungszweck, „wenn sie auch aufgrund einer den Erhebungsvoraussetzungen entsprechenden dringenden Gefahr oder im Einzelfall drohenden Gefahr erforderlich ist." Ausgeschlossen ist hingegen eine Nutzung als Spuren- oder Ermittlungsansatz „unabhängig von einer dringenden oder im Einzelfall drohenden Gefahr."[628] Insgesamt gibt dieser als zweckwahrende Weiternutzung bezeichnete verfassungsrechtliche Spielraum den Polizeien in Deutschland die Möglichkeit, recht frei mit Daten umzugehen, ohne durch die weitergehenden verfassungsrechtlichen Anforderungen an eine Zweckänderung behindert zu werden,[629] sodass sich diese Flexibilisierung des polizeilichen Datenumgangs als verfassungsrechtliche Anpassung an das Zeitalter der Massendaten deuten lässt, womit auch weitere evolutive Entwicklungen der Zweckdogmatik in Zukunft nicht ausgeschlossen erscheinen.

---

626 BVerfGE 141, 220 (325) – Bundeskriminalamtgesetz.
627 BVerfGE 141, 220 (324f.) – Bundeskriminalamtgesetz.
628 BVerfGE 141, 220 (325) – Bundeskriminalamtgesetz.
629 *Bäuerle* in *Möstl/Mühl* (Hrsg.), Beck'scher Online-Kommentar Polizei- und Ordnungsrecht Hessen, § 20 HSOG Rn. 57, spricht von „kaum […] überprüfbare[r] Definitionsmacht."

Die Urteile zu dieser Evolution fallen in der Literatur unterschiedlich aus.[630] Vor dem Hintergrund der faktischen Außerkraftsetzung des Zweckbindungsgrundsatzes durch die Praxis der polizeilichen Datenverarbeitung schon vor dem Urteil nähert sich die Rechtsprechung des Bundesverfassungsgerichts jedenfalls klar polizeipraktischen Bedürfnissen und Realitäten an. Dieser judikative Pfad erscheint mit Blick auf die Zwänge des Massendatenphänomens insoweit nachvollziehbar, als der Polizei Handlungsmöglichkeiten im flexibleren Datenumgang eröffnet werden sollen. Allerdings lässt sich kaum von der Hand weisen, dass damit normative Stützpfeiler der Idee der informationellen Selbstbestimmungen an Tragkraft verlieren. Zwar soll diese Reduzierung materieller Grenzen wohl durch die Prozeduralisierung des Grundrechtsschutzes, wie er auch paradigmatisch für die JI-Richtlinie ist, aufgefangen werden – ob sich diese Hoffnung als zutreffend erweisen wird, gilt es jedoch aufmerksam zu beobachten.

cc) Die Zweckänderung

Der – nunmehr auch verfassungsrechtlich durch die zweckwahrende Weiternutzung aufgeweichte – Zweckbindungsgrundsatz soll die Datenverarbeitung steuern und rechtlich handhabbar machen. Eine im vorliegenden Kontext relevante und auch beabsichtigte Folge ist die Trennung staatlicher Datenbestände voneinander (sog. „informationelle Gewaltenteilung“[631]), die eine funktionierende Aufgabenerfüllung seitens der staatlichen Behörden erschwert, indem es die Zusammenführung vorhandener Informationen zu tiefergehendem Wissen an Voraussetzungen knüpft. Allerdings ist staatliches Handeln von soliden und auch möglichst umfassenden Informationen abhängig, sodass die Frage, wann es zu einer Durchbrechung des Zweckbindungsgrundsatzes und damit zu einer Zusammenführung von Daten kommen soll, als „Grunddilemma des Datenschutzrechts“[632] in Deutschland gelten kann. Dogmatisch ist es mit der Lösung des Problems letztlich nicht weit her: Der zweckentfremdende Umgang mit bereits

630 *Schwabenbauer* in *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch, G. Rn. 17, sieht hier „zumindest eine Neujustierung“; *Arzt* in *Möstl/Kugelmann* (Hrsg.), Beck'scher Online-Kommentar Polizei- und Ordnungsrecht Nordrhein-Westfalen, § 23 PolG NRW Rn. 3, sieht hingegen einen Dammbruch.

631 *Di Fabio* in *Dürig/Herzog/R. Scholz,* Grundgesetz, Art. 2 Rn. 184, siehe auch dort zu grundsätzlicher Kritik an diesem Prinzip.

632 *H. Wolff* ZG 31 (2016), 361 (380).

gespeicherten Daten ist wiederum ein rechtfertigungsbedürftiger Eingriff, dessen Rechtfertigung möglich, aber auch nötig ist – insoweit also einem neuen, bestimmten Zweck in verhältnismäßiger Weise dienen muss.[633] Tangiert werden damit die schon durch die Datenerhebung beeinträchtigten Grundrechte.[634]

Die Verfassungsrechtsprechung hat die Anforderungen an die Zweckänderung seit dem Volkszählungs-Urteil beständig weiterentwickelt und für die polizeiliche Datenverarbeitung im BKAG-Urteil konsolidiert. Wie bereits im Rahmen der Erhebung müssen die geänderten Zwecke hinreichend bestimmt festgelegt werden.[635] Zusätzlich muss die Bedeutung der Daten in verhältnismäßiger Weise berücksichtigt werden. Daten aus besonders eingriffsintensiven Maßnahmen, dürfen nur zu besonders gewichtigen, anderen Zwecken genutzt werden,[636] worin sich einmal mehr das stark auf Erhebungsmaßnahmen und nicht so sehr auf Daten fokussierte Eingriffsverständnis zeigt. Das BKAG-Urteil hat hier mit der Formulierung des Grundsatzes der hypothetischen Datenneuerhebung weitere Spezifizierung mit Blick auf die Zweckänderung im Bereich polizeilicher Datenverarbeitung gebracht. Danach ist nun ausschlaggebend für die Zulässigkeit einer Zweckänderung, ob mit ihr „grundrechtsbezogene Beschränkungen des Einsatzes bestimmter Erhebungsmethoden umgangen würden, die Informationen also für den geänderten Zweck nicht oder nicht in dieser Art und Weise hätten erhoben werden dürfen." [637] *Wolff* zufolge stellt sich in diesem Zusammenhang die Frage, ob der Gesetzgeber befugt wäre, der konkreten empfangenden Behörde eine Befugnis einzuräumen, die erhaltenen Daten mit vergleichbaren Mitteln, also vergleichbaren Eingriffen, selbst zu erheben.[638] Dabei ist indessen zu beachten, dass die hypothetische Datenneuerhebung nicht bedeutet, dass exakt dieselben Anforderungen wie bei der Datenerhebung gelten[639] sondern die Zweckänderung eine gewisse „Selbst-

633 *Schwabenbauer* in: *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch, G. Rn. 13.
634 Vgl. BVerfGE 141, 220 (327) – Bundeskriminalamtgesetz mwN.
635 *Schwabenbauer* in: *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch, G. Rn. 186.
636 BVerfGE 141, 220 (327) – Bundeskriminalamtgesetz.
637 Zuvor war darauf abgestellt worden, ob Erhebungs- und neuer Verwendungszweck miteinander (nicht) unvereinbar sind, vgl. etwa BVerfGE 130, 1 (33 f.) – Verwertungsverbot Wohnraumüberwachung; zum Rechtsprechungsverlauf, der dieses Kriterium durch den Grundsatz der hypothetischen Datenneuerhebung „konkretisiert und ersetzt" hat, vgl. hierzu und zur zitierten Stelle BVerfGE 141, 220 (327 f.) – Bundeskriminalamtgesetz.
638 *H. Wolff* ZG 31 (2016), 361 (382).
639 BVerfGE 141, 220 (327 f.) – Bundeskriminalamtgesetz.

ständigkeit" besitzt.[640] Wichtiger ist vielmehr die „Gleichgewichtigkeit der neuen Nutzung".[641] Die jeweils verfolgten Zwecke von alter und neuer Nutzung müssen also vergleichbar sein, sodass die neuen Zwecke umso gewichtiger sein müssen, je eingriffsintensiver die ursprüngliche Erhebung war.[642] Zusätzlich soll der Grundsatz der hypothetischen Datenneuerhebung davor schützen, dass mittels einer Zweckänderung grundrechtliche Erhebungsbeschränkungen unterlaufen werden.[643] Im Bereich polizeilicher Datenverarbeitung ist mit Blick auf materielle Rahmenbedingungen der Zweckänderung zudem noch relevant, dass ein „allgemeine[r] Austausch personenbezogener Daten aller Sicherheitsbehörden oder de[r] Abbau jeglicher Informationsgrenzen zwischen ihnen" unzulässig ist.[644]

Von diesen inhaltlichen Anforderungen an die Zweckänderungen sind schließlich noch die Mindestvoraussetzungen zu unterscheiden, die an den Anlass einer Zweckänderung zu stellen sind. Der Anlass zu einer Zweckänderung bedarf dabei nicht desselben „Konkretisierungsgrades der Gefahrenlage oder des Tatverdachts", da

> „[d]ie diesbezüglichen Anforderungen […] unter Verhältnismäßigkeitsgesichtspunkten primär den Anlass nur unmittelbar für die Datenerhebung selbst [bestimmen]. […] Als neu zu rechtfertigender Eingriff bedarf aber auch die Ermächtigung zu einer Nutzung für andere Zwecke eines eigenen, hinreichend spezifischen Anlasses. Verfassungsrechtlich geboten, aber regelmäßig auch ausreichend, ist insoweit, dass sich aus den Daten – sei es aus ihnen selbst, sei es in Verbindung mit weiteren Kenntnissen der Behörde – ein konkreter Ermittlungsansatz ergibt."[645]

Anders ist dies im Falle der Wohnraumüberwachung sowie des Zugriffs auf informationstechnische Systeme, bei der eine der Erhebung gleich hohe Anlassschwelle erforderlich ist.[646] Was genau aber unter dem konkreten Ermittlungsansatz zu verstehen ist, ist bis dato noch nicht abschließend

640 *H. Wolff* ZG 31 (2016), 361 (382).
641 BVerfGE 141, 220 (328) – Bundeskriminalamtgesetz; *Schwabenbauer* in: *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch, G. Rn. 190, spricht insoweit von der „alles überwölbende[n] Großformel".
642 BVerfGE 141, 220 (327) – Bundeskriminalamtgesetz.
643 Bspw. im Fall der optischen Wohnraumüberwachung, BVerfGE 141, 220 (338 f.) – Bundeskriminalamtgesetz.
644 BVerfGE 133, 277 (321) – Antiterrordateigesetz.
645 BVerfGE 141, 220 (328 f.) – Bundeskriminalamtgesetz.
646 BVerfGE 141, 220 (328) – Bundeskriminalamtgesetz.

geklärt.[647] Außerdem wird bezweifelt, ob die dadurch bewirkte Absenkung der Eingriffsschwelle für Zweckänderungen überhaupt noch rechtsstaatlich vertretbar ist.[648] Auch hier zeigen sich Anpassungsbemühungen der Verfassungsrechtsprechung an die zunehmend datengesättigten Umwelten, in denen die deutschen Polizeien mit wachsenden Datenvolumina agieren müssen.

Ebenfalls relevant im Kontext der Zweckänderung ist die Datenübermittlung zwischen unterschiedlichen (Polizei-)Behörden wie sie im polizeilichen Informationswesen mit seinen unterschiedlichen Datenbanken und Informationssystemen täglich vielfach geschieht. Daneben sind vor allem auch Datenübermittlung zwischen Polizeien und Justiz, insbesondere den Staatsanwaltschaften, besonders relevant in diesem Kontext. Kommt es zu einem zweckändernden Austausch von Daten, sind regelmäßig[649] zwei Akteure – ein abgebender und ein empfangender – beteiligt. Durch einen solchen Austausch erfolgen somit genau genommen zwei Grundrechtseingriffe, sodass auch zwei Rechtsgrundlagen erforderlich sind. Klärungsbedürftig ist nicht nur die Frage, unter welchen Bedingungen Daten abgegeben werden, sondern auch unter welchen Bedingungen sie entgegengenommen werden dürfen:

> „Ein Datenaustausch vollzieht sich durch die einander korrespondierenden Eingriffe von Abfrage und Übermittlung [*Schwabenbauer* zufolge auch „Nutzung"[650]], die jeweils einer eigenen Rechtsgrundlage bedürfen. Der Gesetzgeber muss, bildlich gesprochen, nicht nur die Tür zur Übermittlung von Daten öffnen, sondern auch die Tür zu deren Abfrage. Erst beide Rechtsgrundlagen gemeinsam, die wie eine Doppeltür zusammenwirken müssen, berechtigen zu einem Austausch personenbezogener Daten. Dies schließt – nach Maßgabe der Kompetenzordnung und den

647 So etwa *Spiecker gen. Döhmann*, Bundesverfassungsgericht kippt BKA-Gesetz: Ein Pyrrhus-Sieg der Freiheitsrechte?, https://verfassungsblog.de/bundesverfassungsgericht-kippt-bka-gesetz-ein-pyrrhus-sieg-der-freiheitsrechte/ (Stand: 01.10.2023).

648 So *Arzt* in *Möstl/Kugelmann* (Hrsg.), Beck'scher Online-Kommentar Polizei- und Ordnungsrecht Nordrhein-Westfalen, § 23 PolG NRW Rn. 35.

649 Das ist nicht der Fall, wenn Daten innerhalb der Erhebungsbehörde nicht zweckkonform weitergenutzt werden, wobei wohl letztlich dieselben verfassungsrechtlichen Anforderungen gelten, vgl. *Schwabenbauer* in: *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch, G. Rn. 177.

650 *Schwabenbauer* in: *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch, G. Rn. 176.

Anforderungen der Normenklarheit – nicht aus, dass beide Rechtsgrundlagen auch in einer Norm zusammengefasst werden können."[651]

Dieses sog. „Doppeltürmodell" ist im Bereich polizeilicher Datenbanken – vor allem mit Blick auf die starke Föderalisierung der Polizei – von großer Bedeutung und hat in den entsprechenden Rechtsmaterien einfachgesetzliche Ausgestaltung erfahren. Im Rahmen der Darstellung relevanter strafprozess- und polizeirechtlicher Regelung wird darauf zurückzukommen sein.[652] Verfassungsrechtlich jedenfalls bestehen auch hier wieder vor allem hohe Anforderungen an die Bestimmtheit der Zwecke in Übermittlungsregelung (erste Tür) und Abrufregelung (zweite Tür), sodass vor allem abrufende Stellen die verfügbaren Daten nicht unabhängig vom ursprünglichen Zweck bevorraten können.[653] Im Bereich der zweckändernden Übermittlung kommt denn auch wieder der Grundsatz der hypothetischen Datenneuerhebung zum Tragen. Dabei gilt dieser „nicht schematisch". So kann aus Vereinfachungs- und Praktikabilitätsgründen bei der Schaffung von Übermittlungsvorschriften eine geringere Detailliertheit in den Voraussetzungen im Vergleich zu Erhebungsvorschrift gerechtfertigt sein. Auch der Umstand, dass die Zielbehörde wegen ihres Aufgabenspektrums bestimmte Datenerhebungen, zu denen die Ausgangsbehörde berechtigt ist, nicht vornehmen darf, steht einem Datenaustausch nicht grundsätzlich entgegen. Zentrales Kriterium ist vielmehr die Gleichwertigkeit der neuen Datennutzung.[654] Hiermit werden, wie mit der Figur der zweckwahrenden Weiternutzung, Datenflüsse zwischen sicherheitsbehördlichen und sonstigen (staatlichen) Stellen ebenfalls flexibilisiert, wobei weiterhin Informationsgrenzen zwischen den behördenspezifischen Datenbeständen bestehen bleiben müssen.[655]

2. Aggregiert-kollektive Datenakkumulation als blinder Fleck der individualistischen Verfassung?

Mit dem fortschreitenden Ausbau der informationellen Befugnisse der Bundes- und Länderpolizeien stellt sich – ähnlich wie bereits im Rahmen

651 BVerfGE 130, 151 (184) – IP-Adresse.
652 Siehe dazu unten S. 350 ff.
653 BVerfGE 155, 119 (179 f.) – Bestandsdatenauskunft II.
654 BVerfGE 141, 220 (328) – Bundeskriminalamtgesetz.
655 BVerfGE 133, 277 (321) – Antiterrordateigesetz.

der Überlegung, ob Einschüchterungseffekte einen Eingriff darstellen können – die Frage nach den globalen gesellschaftlichen Auswirkungen des Anwachsens staatlicher bzw. spezieller: polizeilicher Datenbestände. Neben den individuellen Schranken, die das Recht auf informationelle Selbstbestimmung und andere möglicherweise betroffene Grundrechte polizeilicher Datenverarbeitung punktuell auferlegen können, wird zunehmend auch über globalgesellschaftliche Perspektiven zum Schutz vor sicherheitsbehördlicher Überwachung nachgedacht. Denn die umfassende Verfügbarkeit von Daten im polizeilichen Informationswesen erhöht die Eingriffsintensität, die in jeder Verarbeitung eines Datums liegt, insgesamt, da der potenzielle Informationsgehalt durch die Potenzierung der Verknüpfungsmöglichkeiten stark zunimmt. Gegenwärtig zentral in der Diskussion um die Auswirkungen der Expansion polizeilicher Informationsbefugnisse und Datenbestände ist die sogenannte Überwachungsgesamtrechnung, die *Roßnagel*[656] in Auseinandersetzung mit der verfassungsgerichtlichen Entscheidung zur Vorratsdatenspeicherung[657] konzeptuell formuliert hat. Seitdem hat es bereits Versuche der dogmatischen Operationalisierbarkeit, etwa in Form einer doppelten Verhältnismäßigkeitsprüfung, gegeben,[658] jedoch bisher ohne nachhaltigen Anschluss zu finden.

An das Konzept anknüpfend, aber zunächst auf die faktische Operationalisierung bedacht, ist das sogenannte „periodische Überwachungsbarometer" von *Poscher et al.*[659] Zentrales Anliegen dieses Konzepts ist zunächst eine quantitative Analyse der „Zugriffe von Sicherheitsbehörden auf Massendatenbestände in öffentlicher oder privater Hand, in denen jedermann anlasslos erfasst ist", um so statistische Aufbereitungen und Veranschaulichungen der gezogenen Erkenntnisse zu ermöglichen. So sollen sich in verschiedenen Dimensionen – etwa regional, zeitlich, behördlich – die Akkumulationen von Daten darstellen lassen. Auf der höchsten, gesamtgesellschaftlichen Aggregationsstufe ließe sich schließlich das namensgebende Überwachungsbarometer erstellen, das einen „Eindruck von dem Gesamtüberwachungsstatus durch die Sicherheitsbehörden" vermitteln soll. Erst auf Grundlage dieser empirisch-faktischen Basis sollen dann direktere dogmatische Reaktionen insbesondere durch das Bundesverfassungsgericht

656 *Roßnagel* Neue Juristische Wochenschrift 63 (2010), 1238.
657 BVerfGE 125, 260 (323 f.) – Vorratsdatenspeicherung.
658 *Knierim* ZD 2011, 17.
659 *Poscher*, Konzept für ein periodisches Überwachungsbarometer, Deutscher Bundestag, Ausschussdrucksache 19(4)732 E, 2021; siehe auch *Poscher/Kilchling/Landerer* Zeitschrift für das Gesamte Sicherheitsrecht (GSZ) 4 (2021), 225.

möglich sein, etwa indem es daraus Rechtfertigungslasten für die abstrakte Zulässigkeit neuer Überwachungsinstrumente oder auch der Anwendung bestehender Maßnahmen im Einzelfall ableitet. Daneben sind aber vor allem auch Einflussnahmen durch öffentliche Diskussion und damit letztlich Gesetzgebung beabsichtigte Folge der Aggregierung der „Überwachungslast". Zur Realisierung des periodischen Überwachungsgesamtbarometers sind drei Phasen angedacht, wobei die dritte explizit auf einen nicht näher spezifizierten zukünftigen Zeitraum verschoben ist.

Die erste Phase dient einer Exploration der einzubeziehenden Datenbestände, wobei ein Fokus auf anlasslos gespeicherte Massendaten gelegt wird. Ausdrücklich ausgeklammert werden die verschiedenen anlassbezogenen sicherheitsbehördlichen Datenbanken, wobei eine spätere Einbeziehung denkbar erscheint, sodass testweise die Antiterror-Datei mitberücksichtigt wird. Allerdings sollen auch private Datenbestände, auf die staatliche Zugriffsrechte bestehen, mit in die Zusammenschau staatlicher Datenaggregationen einbezogen werden. So sollen dann beispielsweise Datenbestände mit Telekommunikationsdaten, finanzbezogenen Daten, Mobilitätsdaten, Daten aus dem privaten Lebensbereich, Gesundheitsdaten und Meldedaten in das Barometer einfließen. Die darin zum Ausdruck kommende Modularität des Konzepts soll zudem auch in Zukunft die Erweiterbarkeit durch sonstige relevante Datensammlungen wie beispielsweise Videoüberwachungen im öffentlichen Raum ermöglichen.

In der zweiten Phase sollen einerseits die Zugriffstatbestände der Sicherheitsbehörden rechtlich analysiert und normativ bewertet werden, „um eine gewichtete Aggregation der verschiedenen Zugriffszahlen zu ermöglichen." Andererseits sollen in diesem Projektschritt aber auch die vorhandenen Dokumentationspflichten der Behörden analysiert werden, die Grundvoraussetzung für das gesamte Konzept sind. Denn ohne eine Dokumentation, aus der sich eine zahlenmäßige Beschreibung des Zugriffsverhaltens ableiten lässt, kann keine quantitative Aggregation stattfinden. Das gilt umso mehr, als dass öffentlich verfügbare Daten lückenhaft sind und insofern die „elektronisch dokumentierten Einsatzprotokolle" zentrale Erkenntnisquelle für das tatsächliche Zugriffsverhalten sind. Für den privaten Sektor sind vor allem die internen Daten zu Zugriffen durch Sicherheitsbehörden relevant. Hier besteht aufgrund der hohen Marktmacht einiger weniger Akteure eine gute Chance über deren Daten ein halbwegs repräsentatives Bild zu zeichnen.

Insbesondere die quantitative Herangehensweise des Konzepts ist sehr zu begrüßen, da sich nur so eine verlässliche und weiterführende Diskussionsgrundlage für Rechtswissenschaft und Öffentlichkeit schaffen lässt, die wesentlich faktenbasierter sein könnte als die gegenwärtige, vor allem normative Auseinandersetzung. Darüber hinaus ist auch der Fokus auf gesetzliche Dokumentationspflichten der Sicherheitsbehörden sinnvoll, da die in diesem Rahmen anfallenden Daten so endlich einer überindividualistischen Nutzung zufließen und an Wirkkraft gewinnen können. Der in diesem Zusammenhang geäußerte Vorschlag einer Standardisierung für die Aufarbeitung der Daten für das Überwachungsbarometer ist dementsprechend vollumfänglich zu unterstützen. Indessen erscheint die (bisherige und nahezu vollständige) Ausklammerung von sicherheitsbehördlichen Datensammlungen für das Konzept selbst problematisch, auch wenn sie aus forschungs- und umsetzungspraktischen Gründen natürlich nachvollziehbar ist. Nichtsdestotrotz sind die behördeneigenen Datenspeicher immer Ausgangspunkt für Überwachungsmaßnahmen wie Zugriffe auf externe Datensammlungen, sodass eine diesbezügliche Aussparung im Konzept Gefahr läuft, einen zentralen Baustein der polizeilichen Datenakkumulationsmacht zu vernachlässigen. Denn einerseits können – wie es im Konzeptpapier auch gesehen wird – solche Datenbestände bereits den Charakter einer behördlichen Vorratsdatenspeicherung annehmen und andererseits ist auch hier zu bedenken, dass sich der informationelle Gehalt von Datensammlungen durch ihre relative Modularität ergibt, wie man sie schon von der Rasterfahndung kennt: Durch die Kombination verschiedener Datenbestände, die dann wiederum mit den datenförmigen Erkenntnissen der Polizei abgeglichen werden, können sich je nach modularer Konstellation – auch in ihrem Intensitätsgehalt – ganz unterschiedliche Informationen ergeben. Insofern sollten – wie es auch geplant zu sein scheint – die sicherheitsbehördlichen bzw. polizeilichen Datensammlungen auf mittelfristige Sicht mit in das Konzept integriert werden.[660]

II. Polizeiliches Vorfeld und Verfassung

Bereits im Rahmen der historischen Rückschau auf polizeiliche Informationsverarbeitung hat sich gezeigt, dass das Sammeln von möglichst umfas-

660 Siehe dazu noch einmal unten S. 531 ff.

senden Informationen ein der Polizei als Institution inhärenter Impetus ist. Die rechtsstaatlichen Zähmungsversuche in Form von Gefahren- und Verdachtsdogmatik waren indessen nur so lange ausreichend, wie der Umgang mit Daten unabhängig von konkreten Straf- oder Gefahrenabwehrverfahren als nicht oder kaum grundrechtsbedenklich galt, sodass mit dem Volkszählungsurteil auch das polizeiliche Handeln im Vorfeld von Gefahr und Verdacht stärker in die rechtswissenschaftliche Aufmerksamkeit geraten ist. Dabei geht es allerdings längst nicht mehr nur um die Einhegung hergebrachter informationeller Praktiken der Polizei. Vielmehr befindet sich das polizeiliche Vorfeld durch gesellschaftlichen Risikodiskurses, die maßgeblich durch *Beck* explizit ins allgemeine Bewusstsein gebracht wurden,[661] bereits seit Jahrzehnten in einem Wandlungsprozess. In diesem tarieren sich die Grenzen des Nötigen, Möglichen und Erlaubten im polizeilichen Vorfeld stetig durch Wechselwirkungen zwischen den diskursiven, technischen und rechtlichen Aspekten des gesellschaftlichen Sicherheitsensembles ständig neu aus.

Relevant ist die Form der (verfassungs)rechtlichen Ausgestaltung der polizeilichen Vorfeldbefugnisse vorliegend deshalb, weil darüber die Reichweite polizeilicher Datenerhebungen und somit auch des Informationswesens strukturell erweitert werden. Statt reaktiv und einzelfallbezogen Daten zu erheben, ermöglicht das Vorfeld die proaktive Generierung von einzelfallübergreifenden Datenaggregationen.[662] Begründet wird die Notwendigkeit dieses Handlungsmodus, der in den Grenzen von Verdacht und Gefahr nicht möglich ist,[663] vor allem mit der sonst kaum zu bewältigenden Aufklärung und Bekämpfung komplexer krimineller Strukturen – also im Wesentlichen organisierte Kriminalität und Terrorismus.[664]

661 *Beck,* Risikogesellschaft.

662 *Bäcker* in *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch des Polizeirechts, D. Rn. 237 ff.

663 *Bäcker* in*Bäcker/Denninger/Graulich* (Hrsg.), Handbuch des Polizeirechts, D. Rn. 239.

664 *Bäcker* in *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch des Polizeirechts, D. Rn. 241 et passim Zur den Ausweitungsproblematiken solcher Begründungsmuster und der epistemischen Ursachen siehe bereits oben S. 124 ff.

1. Das strafverfahrensrechtliche Vorfeld

Das polizeiliche Vorfeld ist dabei konzeptuell sowohl im repressiven als auch im präventiven Handlungsfeld denkbar. Lange Zeit waren Eingriffsmaßnahmen aus beiden Feldern ausschließlich im Polizeirecht verortet. Unter der Aufgabenzuweisung der vorbeugenden Bekämpfung von Straftaten wurde neben der präventiven Verhütung auch die repressive Vorsorge für die Verfolgung von Straftaten gefasst und so kompetenziell den Polizeigesetzgebern zugesprochen.[665] Dieser Verteilung hat das Bundesverfassungsgericht jedoch in seinem „Niedersachsenurteil" einen Riegel vorgeschoben, in dem es die Gesetzgebungskompetenz des Bundes bezogen auf das Strafverfahren zweckbezogen interpretierte und „vorsorgende Maßnahmen, die sich auf die Durchführung künftiger Strafverfahren beziehen", dieser Gesetzgebungskompetenz zusprach.[666] Folglich entfaltet Art. 72 Abs. 1 GG nur insoweit Spielräume für die Landesgesetzgeber, wie der Bund von seiner strafverfahrensrechtlichen Gesetzgebungskompetenz keinen abschließenden Gebrauch gemacht hat. Nach Ansicht des Verfassungsgerichts hat der Bundesgesetzgeber jedoch gerade unterlassen, Überwachungsmaßnahmen und die mit ihnen bezweckte Datenermittlung für Zwecke zukünftiger Strafverfahren von einem Tatverdacht zu entkoppeln und damit gleichzeitig das strafverfahrensrechtliche Vorfeld insoweit gesperrt.[667] Legislative Freiheiten verbleiben den Ländern daher nur begrenzt in Fällen ohne Bezug zu Personen, worunter etwa sach- oder ortsbezogene sowie an allgemeine Bedrohungslagen anknüpfende Maßnahmen fallen, sodass vor allem das Feld der gelegenheitsorientierten Kriminalprävention auch zu Zwecken der Strafverfolgung weiter für Landesgesetzgeber offen bleibt. [668] Zudem – und wesentlich relevanter – dürfen die Landesgesetzgeber Rechtsgrundlagen für die Weiterverarbeitung von Strafverfahrensdaten nach Maßgabe der Polizeigesetze schaffen, wie es der Bundesgesetzgeber mit § 481 StPO explizit zum Ausdruck gebracht hat.

Insofern besteht bis auf punktuelle Maßnahmen wie §§ 81a, 81b StPO kein strafverfahrensbezogenes Vorfeldrecht mit präventiver Ausrichtung,[669]

665 *Bäcker* in *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch des Polizeirechts, D. Rn. 320.
666 BVerfGE 113, 348 (371) – Vorbeugende Telekommunikationsüberwachung.
667 BVerfGE 113, 348 (371 f.) – Vorbeugende Telekommunikationsüberwachung.
668 Siehe dazu *Bäcker* in *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch des Polizeirechts, D. Rn. 321, insb. auch Fn. 589 mit Fallnachweisen.
669 BVerfGE 113, 348 (373.) – Vorbeugende Telekommunikationsüberwachung.

sodass dessen Grenzen, insbesondere mit Blick auf die Entkoppelung von Maßnahmen vom Verdachtserfordernis, ungeklärt sind. Theoretisch wären eine Erschließung und Ausgestaltung durch den Gesetzgeber aber möglich. Gleichzeitig scheint sich die gesetzgeberische Energie mit Blick auf die Erschließung des Vorfelds im repressiven Bereich eher in Form eines kriminalpräventiv ausgerichteten Strafrechts zu entladen.[670]

2. Das polizeirechtliche Vorfeld

Im polizeirechtlichen Bereich wurden indessen durch iterative Runden aus Gesetzgebung und darauf antwortender Verfassungsrechtsprechung Vorfeldermächtigungen geschaffen und konturiert, sodass hier ein vom klassischen Gefahrerfordernis abweichendes polizeiliches Handlungsfeld entstanden ist. Um dieses dreht sich eine durch die judikativen Impulse der Verfassungsgerichte ständig neu angetriebene Diskussion bezüglich der Grenzen des verfassungsrechtlich Zulässigen im polizeirechtlichen Vorfeld. Während einige die Steuerungsleistung der bundesrepublikanischen Verfassung mit Blick auf derartige Entgrenzungen polizeilichen Handelns bezweifeln[671] und demgegenüber eher auf eine Grundrechtssicherung durch Verfahren setzen,[672] hat das Bundesverfassungsgericht in seiner jüngeren Rechtsprechung eine materielle Ausgestaltung des polizeirechtlichen Vorfelds unternommen.[673]

---

670 Siehe dazu unten S. 182 ff.

671 So spricht *Grimm* Kritische Vierteljahresschrift für Gesetzgebung und Rechtswissenschaft (KritV) 1 [69] (1986), 38 (54), in diesem Kontext davon, dass entsprechendes Tun "nicht mehr ausreichend normativ steuerbar" wäre; ähnlich *P.-A. Albrecht,* Der Weg in die Sicherheitsgesellschaft, 238 f.

672 Ausführlich *Bonin,* Grundrechtsschutz durch verfahrensrechtliche Kompensation bei Maßnahmen der polizeilichen Informationsvorsorge; siehe auch *Kugelmann/Dalby* in D. Busch/Roggan (Hrsg.), Das Recht in guter Verfassung?, 105; konkret am Beispiel des nach wie vor wichtigen Richtervorbehalts *Gusy* in Barton/Kölbel/Lindemann (Hrsg.), Wider die wildwüchsige Entwicklung des Ermittlungsverfahrens, 193.

673 Vgl. BVerfGE 156, 11 – Antiterrordateigesetz II; 155, 119 – Bestandsdatenabruf II; 150, 309 – Kfz-Kennzeichenerfassung III; 150, 244 – Kfz-Kennzeichenerfassung II; 141, 220 – Bundeskriminalamtgesetz; 133, 277 – Antiterrordateigesetz I; 125, 260 – Vorratsdatenspeicherung; 120, 378 – Kfz-Kennzeichenerfassung I; 115, 320 – Rasterfahndung; 113, 348 – Telekommunikationsüberwachung nach dem niedersächsischen SOG; Nachweise nach *Bäcker* in *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch des Polizeirechts, D. Rn. 251.

Die Auswirkungen auf die hergebrachte polizeirechtliche Eingriffsdogmatik hat vor allem *Bäcker* konsistent systematisiert und aufgearbeitet. Die Entkoppelung polizeirechtlicher Maßnahmen vom Erfordernis einer konkreten, ereignisbezogenen Gefahr erfolgt danach über zwei unterschiedliche Modifizierungsmöglichkeiten: Einerseits kann von einem „ereignisbezogenen Wahrscheinlichkeitsurteil auf ein individualbezogenes Wahrscheinlichkeitsurteil" umgestellt werden.[674] Andererseits lassen sich polizeiliche Vorfeldbefugnisse auch an den klassisch ereignisbezogenen Prognosemodus der Gefahr anknüpfen, wenn „die Anforderungen an die Konkretisierung des Schadensereignisses abgesenkt" werden.[675]

Die Anforderungen an Vorfeldmaßnahmen, die auf ein individualbezogenes Wahrscheinlichkeitsurteil gestützt werden sollen, hat das Bundesverfassungsgericht im BKAG-Urteil von 2016 formuliert, womit dieser polizeiliche Handlungsmodus zugleich verfassungsrechtlich abgesegnet wurde. Es wird hier wiederum in zwei verschiedene Prognosetypen, die Vorfeldmaßnahmen legitimieren können, unterteilt:

Zum einen kann eine solche Prognose eine Maßnahme legitimieren, wenn

> „sich der zum Schaden führende Kausalverlauf noch nicht mit hinreichender Wahrscheinlichkeit vorhersehen lässt, sofern bereits bestimmte Tatsachen auf eine im Einzelfall drohende Gefahr für ein überragend wichtiges Rechtsgut hinweisen. Die Tatsachen müssen dafür zum einen den Schluss auf ein wenigstens seiner Art nach konkretisiertes und zeitlich absehbares Geschehen zulassen, zum anderen darauf, dass bestimmte Personen beteiligt sein werden, über deren Identität zumindest so viel bekannt ist, dass die Überwachungsmaßnahme gezielt gegen sie eingesetzt und weitgehend auf sie beschränkt werden kann".[676]

674 *Bäcker* in *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch des Polizeirechts, D. Rn. 258.

675 *Bäcker* in *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch des Polizeirechts, D. Rn. 259.

676 BVerfGE 141, 220 (272) - Bundeskriminalamtgesetz. Nach *Bäcker* in *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch des Polizeirechts, D. Rn. 267, handelt es sich dabei um eine Reformulierung des Gefahrenverdachts, sodass hierdurch - entgegen der Intention des Gerichts keine weitere Vorverlagerung des Eingriffsanlasses erfolgt. .

Daneben können nach dem Urteil

> „[i]n Bezug auf terroristische Straftaten, die oft durch lang geplante Taten von bisher nicht straffällig gewordenen Einzelnen an nicht vorhersehbaren Orten und in ganz verschiedener Weise verübt werden, […] Überwachungsmaßnahmen auch dann erlaubt werden, wenn zwar noch nicht ein seiner Art nach konkretisiertes und zeitlich absehbares Geschehen erkennbar ist, jedoch das individuelle Verhalten einer Person die konkrete Wahrscheinlichkeit begründet, dass sie solche Straftaten in überschaubarer Zukunft begehen wird."[677]

Die in der zweiten Variante zum Ausdruck kommende Fokussierung auf individuelles Verhalten zur Kompensation der weitestgehenden Aufgabe des Ereignisbezuges in derartigen Fällen ist eine durchaus bemerkenswerte Entwicklung, da es hierdurch möglich wird, polizeiliche Maßnahmen auf eine rein personenbezogene Gefährlichkeitsprognose zu stützen.[678] Die Anwendung dieser Rechtsfigur auf rein terroristische Sachverhalte hat das Bundesverfassungsgericht in der Zwischenzeit in ein stärker relationales Konzept überführt, in dem die Anforderungen an die zu schützenden Rechtsgüter steigen, je eingriffsintensiver die Maßnahmen sind oder je weiter sie ins Vorfeld verlegt werden.[679]

Daneben können sich polizeiliche Vorfeldmaßnahmen auch gegen Personen richten, die zum Umkreis der Zielperson gehören. Erforderlich dafür sind bestimmte Nähekriterien (s. etwa § 19 Abs. 1 Nr. 3, 4 BKAG), die bloße Tatsache des Kontakts ist also nicht ausreichend. Diese Kriterien wurden vom Bundesverfassungsgericht ausdrücklich gebilligt, wobei das Gericht explizit auch das Problem der möglichen zirkelschlüssigen Rechtsanwendung (Bejahung des Nähekriteriums auf Grundlage allein des tatsächlichen Kontakts) hinweist,[680] ohne jedoch weiter auf die damit möglicherweise weitergehenden Probleme polizeilicher Definitionsmacht einzugehen.

Neben personenbezogenen Vorfeldtatbeständen besteht auch die Möglichkeit, Vorfeldmaßnahmen an sach- oder ortsbezogene Schadensprognosen zu knüpfen. Dabei werden Personen, die mit der jeweiligen Sache oder dem jeweiligen Ort in Verbindung treten, Ziel der Vorfeldmaßnahmen.

677 BVerfGE 141, 220 (272 f.) – Bundeskriminalamtgesetz.
678 *Bäcker* in *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch des Polizeirechts, D. Rn. 268.
679 BVerfGE 155, 119 (187 f.) – Bestandsdatenauskunft II.
680 BVerfGE 141, 220 (292) – Bundeskriminalamtgesetz.

Im Kontext der Kennzeichenkontrolle hat das Bundesverfassungsgericht solche Orte dahingehend charakterisiert, dass „dort Personen Straftaten verabreden, vorbereiten oder verüben, sich Personen ohne erforderliche Aufenthaltserlaubnis treffen, sich Straftäter verbergen oder Personen der Prostitution nachgehen."[681] Da sich Etwaiges für eine Vielzahl von Orten zumindest vermuten ließe, müssen darüber hinaus konkrete polizeiliche Erkenntnisse – etwa in Form von Lageerkenntnissen – bezüglich eines konkretisierten Raumbereichs vorliegen, die eine Frequentierung des Ortes durch entsprechende Personen nahelegen.[682] Ähnlich wie bei den Nähekriterien besteht auch hier eine gewisse Gefahr zirkelförmiger Pfadabhängigkeiten entsprechender polizeilicher Maßnahmen: Orte zu denen bestimmte Lageerkenntnisse bestehen werden überwacht, wodurch weitere, neue Überwachung legitimierende Lageerkenntnisse zutage gefördert werden. Besonders problematisch kann eine solche Feedback-Schlaufe sein, wenn der in Frage stehende Ort durch eine prekäre sozio-ökonomische Struktur geprägt ist und durch den polizeilichen Überwachungsdruck zusätzliche Marginalisierung erfährt.

Als niedrigste Legitimationsschwelle für Vorfeldeingriff soll es zudem noch eine unterhalb der beschriebenen Gefahrenkonturen liegende situative Konstellation geben. *Bäcker* spricht insofern von einer allgemeinen Bedrohungslage, die dann anzunehmen sei, „wenn sich die Wahrscheinlichkeit eines Schadens aus dem allgemeinen Risikorauschen abhebt, das alle immer umgibt."[683] Diese diffuse Bedrohungslage sei notwendig, da etliche wenig eingriffsintensive Regelungen der polizeilichen Datenverarbeitung (einschließlich der Erhebung) lediglich die Erforderlichkeit für die Erfüllung polizeilicher Aufgaben als Tatbestandskriterium kennen. Gäbe es mangels allgemeiner Bedrohungslage[684] überhaupt keinen Anlass, so ließe sich die Erforderlichkeit nicht prüfen, die Polizei könnte anlasslos agieren.[685] Inwiefern aber Bedrohungslagen, in denen die „drohenden Schadensereig-

681 BVerfGE 150, 244 (290) – Kennzeichenkontrolle Bayern.
682 BVerfGE 150, 244 (290 f.) – Kennzeichenkontrolle Bayern.
683 *Bäcker* in *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch des Polizeirechts, D. Rn. 286.
684 Auch geläufig sind Begriffe wie „allgemeine Gefahrenlage" (Knemeyer zitiert nach *Weßlau,* Vorfeldermittlungen, S. 138); oder "allgemeine Gefahren", s. dazu *Albers,* Die Determination polizeilicher Tätigkeit in den Bereichen der Straftatenverhütung und der Verfolgungsvorsorge, S. 42 mwN.
685 *Bäcker* in *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch des Polizeirechts, D. Rn. 288.

nisse […] sich […] räumlich, zeitlich, örtlich und hinsichtlich der Beteiligten noch nicht näher beschreiben lassen [müssen]",[686] groß Steuerungswirkung für das polizeiliche Informationshandeln entfalten sollen, erschließt sich nicht. Die gegen eine solche Bedrohungslage im Vorhof der Gefahr vorgebrachte Kritik der Entgrenzung[687] erscheint hingegen mit Blick auf den begrenzten Handlungsbereich, für den eine allgemeine Bedrohungslage als legitime Grundlage zählen darf – etwa informatorische Befragungen oder unspezifizierte Datenverarbeitungen – ebenfalls nur begrenzt stichhaltig. Problematisch dürfte hier in erster Linie das unreflektierte Heranziehen von falsch positiven Prognosen als Grundlage intensiverer polizeilicher Maßnahmen sein, für deren (der Prognosen) Auftreten es aufgrund der Diffusität in der allgemeinen Bedrohungslage besonders viel Potenzial gibt.[688] Inwieweit hiergegen durch materielle verfassungsrechtliche Vorgaben Schutz geboten werden könnte, ist jedoch fraglich.

Bemerkenswert im Kontext des Vorfelds ist schließlich die Rechtsprechung des Bundesverfassungsgerichts zu automatisierten Kennzeichenkontrollen in Bayern: Mit dem diesbezüglichen Urteil ebnet das Gericht anlasslosen Kontrollen den Weg. Demnach sind anlasslose Kontrollen nicht generell ausgeschlossen. Insbesondere kann bereits das Anknüpfen „an ein gefährliches oder risikobehaftetes Tun bzw. an die Beherrschung besonderer Gefahrenquellen" einen hinreichenden Grund für derartige Kontrollen bieten, wie es etwa im Straßenverkehr anlasslos und stichprobenhaft der Fall ist.[689] Verfahrensgegenstand war unter anderem die anlasslose Kennzeichenkontrolle als Mittel der Schleierfahndung bei Vorliegen entsprechender Lageerkenntnisse zur Verhütung oder Unterbindung des unerlaubten Aufenthalts und zur Bekämpfung der grenzüberschreitenden Kriminalität. Das Bundesverfassungsgericht hält dies in einem Grenzgebiet von bis zu 30 km Tiefe sowie an öffentlichen Einrichtungen des internationalen Verkehrs für zulässig. Lediglich Kontrollen allgemein auf Durchgangsstraßen sind ausgeschlossen, weil dazu in der zu prüfenden Norm auch „andere Straßen von erheblicher Bedeutung für den grenzüberschrei-

686 *Bäcker* in *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch des Polizeirechts, D. Rn. 286.

687 Siehe etwa *Weßlau,* Vorfeldermittlungen, S. 131 ff; *Albers,* Die Determination polizeilicher Tätigkeit in den Bereichen der Straftatenverhütung und der Verfolgungsvorsorge, S. 44 f.

688 *Bäcker* in *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch des Polizeirechts, D. Rn. 289.

689 BVerfGE 150, 244 (281) – Kennzeichenkontrolle Bayern.

tenden Verkehr" genannt waren, was eine hinreichende Konkretisierung verunmöglicht.[690] Begründet wird diese „Befugnis zu praktisch anlasslosen, nur final angeleiteten Maßnahmen", die grundsätzlich nicht mit der Verfassung vereinbar ist, mit der besonderen Rechtfertigung des Ausgleichs für den Wegfall der innereuropäischen Grenzkontrollen.[691] Dahinter steht die Idee der Kompensierung von Kontrolldefiziten durch Kontrollüberschüsse, die im Zuge der Digitalisierung in neuer Qualität produziert werden können,[692] wie man sie auch in anderen Bereichen staatlicher Risikokontrolle kennt.[693] Anders aber als beispielsweise in der Risikokontrolle durch das Atomrecht, wo ein technischer Kontrollüberschuss nicht groß genug sein kann und darüber hinaus stets ein klar umgrenzter Bezugspunkt besteht, unterliegt die Polizei mit ihrer Fokussierung auf prinzipiell jedes Verhalten, das zumindest von rechtlichen Normen abweicht, weniger sachinhärenten Begrenzungen.[694] Das erkennt auch das Bundesverfassungsgericht an, wenn es den Ausnahmecharakter anlassloser, lediglich zweckgerichteter Kontrollen hervorhebt und die Begrenzungen und Sicherungen der Maßnahme betont und auch verstärkt.[695] Nichtsdestotrotz bleibt mit Blick auf die Bedeutung staatlicher Risikopolitik für die moderne Gesellschaft[696] abzuwarten, inwieweit sich dieses Muster der Kompensation von Kontrolldefiziten als anschlussfähig erweist.

3. Die Ausweitung des Vorfelds

Das polizeiliche Vorfeld erfährt quantitativ und qualitativ zunehmende Ausweitung. Zahlenmäßig wachsen die Vorfeldermächtigungen an, die sich zwar häufig noch auf Terrorismusabwehr beschränken, teilweise aber auch (nur noch) die Verhinderung schwerer Schäden zum Zweck haben.[697] Aber auch die Qualität polizeilicher Vorfeldbefugnisse ändert sich – im Sinne einer Intensitätssteigerung – überall dort, wo imperative Eingriffe im

690 BVerfGE 150, 244 (299) – Kennzeichenkontrolle Bayern.
691 BVerfGE 150, 244 (296) – Kennzeichenkontrolle Bayern.
692 *Nassehi,* Muster, S. 43.
693 *Stoll,* Sicherheit als Aufgabe von Staat und Gesellschaft, S. 448.
694 *Albers,* Die Determination polizeilicher Tätigkeit in den Bereichen der Straftatenverhütung und der Verfolgungsvorsorge, S. 43 f.
695 BVerfGE 150, 244 (298 ff.) = NJW 2019, 827 (839 f.) – Kennzeichenkontrolle Bayern.
696 *Reckwitz* in Volkmer/K. Werner (Hrsg.), Die Corona-Gesellschaft, 241.
697 *Bäcker* in *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch des Polizeirechts, D. Rn. 274.

Vorfeld der traditionellen Gefahrenschwelle ermöglicht werden.[698] Damit einher geht eine problematische Verfestigung informationeller Repräsentationen von Personen: Denn während sich bei reinen Überwachungsmaßnahmen durch die stete Fortentwicklung der überwachten Situationen und in ihnen agierenden Personen eine mitlaufende Korrekturmöglichkeit für die Abbilder der Realität gibt, wie sich aus den polizeilichen Daten konstruiert werden, wird diese Möglichkeit durch einen imperativen Eingriff eher abgeschnitten. Wird jemand im Vorfeld mit entsprechenden Maßnahmen vom alltäglichen Sozialleben abgeschnitten – etwa durch Aufenthaltsvorgaben oder Kontaktverbote wie in § 55 BKAG geregelt oder gar durch Präventivgewahrsam wie durch Art. 17 PAG ermöglicht – wird es der betroffenen Person schwerfallen, in dieser Ausnahmesituation durch ihr an den Tag gelegtes Verhalten die Anhaltspunkte für die von ihr ausgehende Gefahr wieder zu entkräften. Gelingt ihr dies nicht, können aufgrund angenommener weiterer Gefährlichkeit weiter Maßnahmen verhängt werden.[699] Diese Entwicklung ist umso bemerkenswerter, als dass es sich bei einer drohenden Gefahr, die auf Grundlage polizeilicher Erkenntnisse angenommen wird, um eine besonders fragile und mit Unschärfen besetzte informationelle Repräsentation der Wirklichkeit handelt.

Trotz gesetzgeberischer Zurückhaltung bei der strafverfahrensrechtlichen Ausgestaltung des Vorfelds ist auch das Strafrecht indessen nicht unbeteiligt an der Ausweitung des polizeilichen Vorfelds. Hier tragen materielle Vorfeldtatbestände wie § 89a ff., 129a f. StGB und andere maßgeblich zur Ausweitung des polizeilichen Maßnahmenspektrums bei, indem Verhalten kriminalisiert wird, das weit im Voraus der eigentlich Rechtsgutverletzung anzusiedeln ist. Zudem fußt die Strafbarkeit maßgeblich auf der Aufdeckung von netzwerkartigen Verbindungen zwischen Akteur:innen (und Objekten) sowie großen Teilen der persönlichen Lebensführung. Durch die Kombination der Tatbestände mit polizeilichen Ermittlungsbefugnissen können als kriminell verdächtigte Strukturen insbesondere terroristischer oder organisierter Natur weitläufig und früh überwacht werden.[700]

Insgesamt bedeutet diese Vorfeldausweitung eine immer stärkere Erweiterung des polizeilichen Blicks. Denn heruntergebrochen gelangen durch

698 *Bäcker* in *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch des Polizeirechts, D. Rn. 276.

699 So *Bäcker* in *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch des Polizeirechts, D. Rn. 27.

700 Siehe näher dazu *Bäcker* in *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch des Polizeirechts, D. Rn. 325 ff.

mehr und breitere Vorfeldbefugnisse – seien sie nun explizit wie im Polizeirecht oder eher indirekt wie im zunehmend präventiv orientierten materiellen Strafrecht – zunächst schlicht mehr Daten über potenziell mehr Personen, Sachen und Umgebungen in die Datenspeicher der Polizei. Diese klaren Ausweitungstendenzen werden auch in der Rechtsprechung des Bundesverfassungsgerichts gespiegelt, wobei dessen Rolle mit Blick auf die Handlungsspielräume der Polizei unterschiedlich interpretiert wird, wie nun im Folgenden beschrieben wird.

III. Sicherheitsverfassungsrecht: Polizeiliches Informationswesen zwischen Hypertrophie und gesetzgeberischer Steuerungsverweigerung

Bereits die hier nur ausschnittsweise dargestellten verfassungsrechtlichen Vorgaben zur polizeilichen Datenverarbeitung deuten auf den Komplexitätsgrad der Karlsruher Rechtsprechung hin. In der Auseinandersetzung mit den vielfältigen Urteilen zu sicherheitsbehördlichen Datenverarbeitungen hat sich nicht nur das Sicherheitsrecht als Disziplin gebildet. Aus dem Wechselwirkungsverhältnis zwischen Sicherheitspolitik und Verfassungsdogmatik ist auch das Konzept des Sicherheitsverfassungsrechts entstanden, das von einem besonderen Wandlungsprozess der Verfassung im Spezialbereich sicherheitsbehördlicher Tätigkeiten ausgeht.[701] Durch immer neue verfassungsrechtliche Vorgaben, deren sicherheitspolitische Verarbeitung in Form von neuen Gesetzen wiederum neue Anknüpfungspunkte für weitere Ausgestaltungen der Sicherheitsverfassung bietet, ist der Detail- und Komplexitätsgrad aber inzwischen so stark angewachsen, dass vermehrt Kritik insbesondere am Bundesverfassungsgericht als zentraler Treiber dieser Entwicklung geäußert wird. Prägnant in diese Richtung äußert sich etwa *Löffelmann*, der die Gefahr einer Hypertrophie des Rechts sieht:

> Obwohl jedes Wort aus Karlsruhe vom Gesetzgeber auf die Goldwaage gelegt wird, um das Verdikt der Verfassungswidrigkeit zu vermeiden, gelingt es im Bereich des Sicherheitsrechts immer schwerer, Gesetze zu schaffen, die den Ansprüchen des Verfassungsrechts genügen. Die hohe Intellektualität der Karlsruher Vorgaben grenzt zuweilen an Überforde-

701 Siehe dazu beispielsweise *Steffen Tanneberger,* Die Sicherheitsverfassung; *Würtenberger/Steffen B. Tanneberger* in S. Fischer/Masala (Hrsg.), Innere Sicherheit nach 9/11, 35; *Poscher* in Korioth/Vesting (Hrsg.), Der Eigenwert des Verfassungsrechts, 245.

> rung. Das liegt nicht nur an der Komplexität der Materie, sondern auch an der Einführung immer neuer begrifflicher Differenzierungen, die Genauigkeit suggerieren, tatsächlich aber am Fehlen eines übergreifenden und schlüssigen Bezugssystems und einer induktiven, aus den Bedürfnissen der Praxis gewonnenen Herleitung leiden.[702]

Um dieser Gefahr zu begegnen, müsse man zu einer Einfachheit in der Rechtssetzung zurück, die aber nicht mit Simplifizierung zu verwechseln sein. Vielmehr brauche es statt stark technischer Normen normative Strukturen, die einen klaren handlungsleitenden Rahmen und grundsätzliche gesetzgeberische Wertungen erkennen lassen und damit für die Rechtsanwendung eine echte Orientierung und Hilfe darstellen.[703] Wie das gelingen können soll, führt *Löffelmann* an anderer Stelle in Bezug auf den Grundsatz der hypothetischen Datenneuerhebung aus. Dabei sollen vor allem Normen klarer für die Anwender:innen werden, was über die Gewichtung von Aufgabenbeschreibungen oder die Intensität von Eingriffen im Wege der ordinalen Schematisierung der Schutzwürdigkeit von Daten bewerkstelligt werden soll.[704]

Dieser Perspektive eher entgegengesetzt sind solche Stimmen, die in den gesetzgeberischen Aktivitäten im Sicherheitsrecht der letzten Jahre und Jahrzehnte eine Steuerungsverweigerung oder einen Steuerungsausfall sehen.[705] Die Folge ist eine Gesetzgebung, die eher darauf bedacht scheint, den Sicherheitsbehörden den Erhalt ihrer eingeübten Praktiken[706] und, mit Blick auf Wandlungen, eine exekutivische Selbstprogrammierung zu ermöglichen.[707]

Beide Positionen haben zwar inhaltliche Schnittmengen, widersprechen sich in ihrer Deutungsrichtung fundamental. Gemein ist ihnen aber eine Absage an den status quo gesetzgeberischer Handhabung des sicherheitsbehördlichen bzw. polizeilichen Informationsrechts. Ohne an dieser Stelle für

---

702 *Löffelmann* Zeitschrift für das Gesamte Sicherheitsrecht 3 (2020), 182 (186).
703 *Löffelmann* Zeitschrift für das Gesamte Sicherheitsrecht 3 (2020), 182.
704 *Löffelmann* Zeitschrift für das Gesamte Sicherheitsrecht 2 (2019), 16 (21 f.).
705 In diese Richtung beispielsweise *Aden/Fährmann* Zeitschrift für Rechtspolitik 2019, 175 (175). *Aden/Fährmann* vorgänge. Zeitschrift für Bürgerrechte und Gesellschaftspolitik 227 (2019), 95 (98 ff.).
706 So bereits *Riegel* Neue Juristische Wochenschrift 50 (1997), 3408 (3411).
707 Allgemein zur Selbstprogrammierung *Schuppert,* Governance und Rechtsetzung, 182 f., kritisch dazu *Habermas,* Faktizität und Geltung, S. 60, 212 f., 230 f. et passim; im Kontext der Polizei siehe etwa *Goeschel/Heyer/G. Schmidbauer,* Beiträge zu einer Soziologie der Polizei, 74 ff.

eine Seite Partei zu ergreifen ist dieser kleinste gemeinsame Nenner der Perspektiven zu befürworten. Das (Verfassungs-)Recht des polizeilichen Informationswesens wird mit einem „weiter so" in zunehmende Schwierigkeiten geraten und an normativem Steuerungs- und Strukturierungspotenzial einbüßen.[708]

B. Unionsrechtliche Vorgaben für polizeiliche Datenverarbeitung

Auch auf europäischer Ebene gibt es zunächst einen dem Grundgesetz vergleichbaren Grundrechtsschutz durch die Europäische Grundrechtecharta und die EMRK. So schützen Art. 7 GRCh und Art. 8 EMRK das Privatleben, wobei der EMRK wegen Art. 52 Abs. 3 GRCh vorrangige Bedeutung bei der Auslegung zukommt. Zudem statuiert Art. 8 GRCh das Recht auf Schutz personenbezogener Daten. Auch dieser grundrechtliche Schutz kann indessen unter Beachtung der Rechtfertigungserfordernisse eingeschränkt werden. Insgesamt spielt insoweit die verfassungsrechtliche Struktur, wie sie zuvor dargestellt wurde, für den nationalen Kontext die größere Rolle.[709]

Jedoch hat die Bedeutung des Unionsrechts für die polizeiliche Datenverarbeitung in jüngerer Zeit in erheblichem Maße zugenommen. Grund dafür ist die am 05.05.2016 in Kraft getretene und bis zum 06.05.2018 umzusetzende „Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27.04.2016 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 und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates"[710]. Diese gestaltet das Datenschutzrecht – gemeinsam mit der DS-GVO – im europäischen Raum an viele Stellen um. Für unionsrechtliche Vorgaben im Bereich polizeilicher Datenverarbeitung ist dieser sekundärrechtliche Rechtsakt zentral, weswegen im Folgenden die JI-Richtlinie und nicht die sehr viel mehr im

708 Siehe dazu auch unten S. 358 ff.

709 *Müller/Schwabenbauer* in *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch des Polizeirechts, G. Rn. 381 ff., zur Frage nach dem Verhältnis von unionalen und nationalen Grundrechten, siehe a.a.O. Rn. 385 ff.

710 EU ABl. 119 vom 04.05.2016; im Folgenden „JI-Richtlinie" (J=Justiz, I=Inneres, vgl. *Wolff* in *Brink/H. Wolff*, BeckOK Datenschutzrecht, BDSG, § 45 Rn. 4).

wissenschaftlichen und öffentlichen Fokus stehende Datenschutzgrundverordnung im Zentrum der Ausführungen steht.

Nach Art. 1 Abs. 1 JI-Richtlinie zielt der Rechtsakt auf den Schutz der Rechte und Freiheiten natürlicher Personen bei der Verarbeitung personenbezogener Daten ab. Gegenüber dem vorherigen Rahmenbeschluss ist insoweit zunächst die Regulierung auch rein innerstaatlicher Datenverarbeitung neu,[711] sodass Unionsgrundrechte nunmehr auch in diesem Bereich Anwendung finden können, sofern es sich um nationale Regelungen handelt, die auf der Richtlinie basieren, also wenn Recht der Union durchgeführt wird.[712] Die extensive Auslegung des Merkmals der „Durchführung von Unionsrecht" durch den Europäischen Gerichtshof[713] gepaart mit der inhaltlichen Weite der zugrundeliegenden Kompetenzgrundlage des Art. 16 Abs. 2 AEUV führen dabei im Ergebnis zu einer Ausweitung der unionsrechtlichen Regelungsmöglichkeiten und -inhalte: Mit dem datenschutzrechtlichen Zugriff auf das mitgliedstaatliche Polizei- und Strafverfahrensrecht als (eine) tragende Säule staatlicher Souveränität schreitet die „Europäisierung des Sicherheitsverfassungsrechts"[714] voran, was trotz gegebenenfalls bestehender praktischer Erfordernisse nicht ohne Kritik geblieben ist.[715]

I. Grundlegende Strukturen der JI-Richtlinie

Die JI-Richtlinie regelt den Bereich der personenbezogenen Datenverarbeitung „zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentlichen Sicherheit" (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 JI-Richtlinie; vgl. auch § 45 Satz 1 BDSG) und hat mit diesem Programm ein entsprechend breites Umsetzungserfordernis

711 Siehe Erwägungsgründe 6, 7 und 26 der JI-Richtlinie.
712 *Weinhold/Johannes* Deutsches Verwaltungsblatt 131 (2016), 1501, 1503.
713 *Weinhold/Johannes* Deutsches Verwaltungsblatt 131 (2016), 1501, 1504.
714 *Schwabenbauer* in: *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch, G. Rn. 337
715 Vgl. etwa *Schwabenbauer* in: *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch, G. Rn. 341 ff., der Art. 16 Abs. 2 AEUV für keine ausreichende Regelungskompetenz hält; siehe auch *H. Wolff* in Kugelmann/Rackow (Hrsg.), Prävention und Repression im Raum der Freiheit, der Sicherheit und des Rechts, 61 ff.; ebenfalls kritisch, aber Art. 16 Abs. 2 AEUV als passende Regelungskompetenz anerkennend *Bäcker*, Stellungnahme JI-Richtlinie, A-Drs. 17(4)585 B, 3 ff.

in der deutschen Gesetzteslandschaft zur Folge gehabt.[716] Nicht nur im Bundesdatenschutzgesetz, sondern auch in jeweils bereichsspezifisch betroffenen Normkomplexen des Bundes und der Länder gab es Umsetzungsbedarf.[717] Die dazu notwendigen Erläuterungen erfolgen an den jeweils relevanten Stellen der Darstellung der einfachgesetzlichen Rahmenbedingungen. Nachfolgend sollen lediglich noch einige grundlegende Aspekte zum Anwendungsbereich der JI-Richtlinie dargestellt werden.

Wesentlich für die Anwendbarkeit der JI-Richtlinie ist zunächst der Begriff der personenbezogenen Daten, der in Art. 3 Nr. 1 definiert ist als alle Informationen über eine identifizierte oder identifizierbare natürliche Person. Es sind grundsätzlich alle Arten von Informationen erfasst, wenn sie aufgrund ihres Inhalts, ihres Zwecks oder ihrer Auswirkungen mit einer bestimmten Person verknüpft sind. Lediglich reine Sachdaten sind nicht erfasst. Auch persönliche Einschätzungen über eine Person wie sie im polizeilichen Kontext häufig zustande kommen, sind personenbezogene Daten (vgl. auch Art. 7 JI-Richtlinie).[718] Die Identifizierbarkeit bemisst sich gemäß Erwägungsgrund 21 im wesentlich danach, ob der für die Verarbeitung Verantwortliche ein Identifizierungsmittel vernünftigerweise einsetzt oder ob dies etwa aus Kosten-, Zeit- oder Technikgründen nicht geschieht. Zudem wird gemäß Art. 3 Nr. 2 JI-Richtlinie die gesamte Bandbreite möglicher Datenumgangsformen erfasst.

Die nach Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 JI-Richtlinie „zuständigen Behörden" sind aufgabenbezogen zu bestimmen, d.h. erfasst werden alle Behörden, die die in Art. 1 Abs. 1 JI-Richtlinie erfassten Zwecke zu erfüllen haben. So fallen beispielsweise auch Strafgerichte darunter. In jedem Fall erfasst werden aber die hier untersuchten Polizeibehörden.[719] Mit der zunehmend flächendeckende Verbreitung elektronischer Vorgangsbearbeitungssysteme bei den Polizeibehörden dürften in Zukunft fast alle dortigen Datenverarbeitungen in den Anwendungsbereich der Richtlinie fallen,[720] denn gemäß Art. 2 Abs. 2 JI-Richtlinie genügt auch eine nicht-automatisierte Verarbeitung, wenn sie personenbezogene Daten betrifft, die in einem Dateisystem

716 So auch *Schwabenbauer* in: *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch, G. Rn. 380.
717 *Wolff* in *Brink/H. Wolff*, BeckOK Datenschutzrecht, BDSG, § 45 Rn. 4.
718 *Müller/Schwabenbauer* in *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch des Polizeirechts, G. Rn. 426, 429 ff.
719 *Schwabenbauer* in: *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch, G. Rn. 367.
720 *Bäcker/Hornung* ZD 2012, 147, 148 f.

gespeichert werden (sollen). Die Menge nicht vom Anwendungsbereich der Richtlinie erfasster personenbezogener Daten dürften marginal sein.[721]

In sachlicher Hinsicht erstreckt sich der Anwendungsbereich der Richtlinie zunächst auf die Aufdeckung, Untersuchung oder Verfolgung von Straftaten, wobei der Begriff der Straftat unionsrechtlich auszulegen ist. Darunter fällt in Deutschland jedenfalls der Bereich der in der StPO geregelten Strafverfolgung.[722] Darüber hinaus sind jedoch auch Ordnungswidrigkeiten erfasst.[723] Bis dato noch nicht vollständig geklärt ist indessen, in welchem Ausmaße auch präventivpolizeiliche Datenverarbeitung – die „Verhütung von Straftaten – von der JI-Richtlinie erfasst wird. Während nach deutschem Verständnis die Verhütung von Straftaten (und Ordnungswidrigkeiten[724]) Teil des allgemeinen Polizei- und Ordnungsrechts ist, ist dies nach unionalem Verständnis nicht unbedingt der Fall, was zu gespaltenen unionsrechtlichen Rahmenbedingungen im Bereich der Gefahrenabwehr führt.[725] Es muss jedoch noch weiter differenziert werden: Während für straftatenbezogene präventivpolizeiliche Tätigkeit die JI-Richtlinie zweifelsohne gilt, ist fraglich, ob es im Bereich der Gefahrenabwehr auch einen Anwendungsbereich der Richtlinie gibt, ohne dass ein direkter Straftatenbezug besteht. Diese Überlegung lässt sich an Art. 1 Abs. 1 aE JI-Richtlinie („Schutz vor und der Abwehr von Gefahren für die öffentliche Sicherheit“) festmachen, wodurch die Möglichkeit eines Straftaten-unabhängigen Anwendungsbereiches der JI-Richtlinie suggeriert wird. Auch Erwägungsgrund 12 scheint davon auszugehen, wenn dort von „polizeilichen Tätigkeiten, in Fällen, in denen nicht von vornherein bekannt ist, ob es sich um Straftaten handelt oder nicht“ die Rede ist. Weiter heißt es an dieser Stelle: „Solche Tätigkeiten können ferner die Ausübung hoheitlicher Gewalt durch Ergreifung von Zwangsmitteln umfassen, wie polizeiliche Tätigkeiten bei Demonstrationen, großen Sportveranstaltungen und Ausschreitungen.“ Angesichts dieses Textbefundes scheint es sinnvoll, nur dann der JI-Richtlinie im Bereich polizeilicher Tätigkeit den Anwendungsbereich zu versagen da-

721 Nach Erwägungsgrund 18 der JI-Richtlinie soll der Anwendungsbereich nur dann nicht eröffnet sein, wenn sich um personenbezogene Daten in „Akten oder Aktensammlungen sowie ihre Deckblätter, die nicht nach bestimmten Kriterien geordnet sind,“ handelt.

722 *Wolff* in *Schantz/H. Wolff,* Das neue Datenschutzrecht, Rn. 242.

723 *Wolff* in *Schantz/H. Wolff,* Das neue Datenschutzrecht, Rn. 248 ff.

724 Siehe näher dazu *Wolff* in *Brink/H. Wolff*, BeckOK Datenschutzrecht, BDSG, § 45 Rn. 40.

725 *Wolff* in *Schantz/H. Wolff,* Das neue Datenschutzrecht, Rn. 243.

mit und der DS-GVO, bei unionsrechtlichem Bezug, die Anwendung zu eröffnen, wenn von vornherein aus ex-ante-Sicht (aus verständiger Beamt:innensicht) überhaupt keinen Straftaten- oder Ordnungswidrigkeitenbezug gibt.[726] Für den von der vorliegenden Untersuchung erfassten Tätigkeitsbereich der Polizeien des Bundes und der Länder gilt die JI-Richtlinie damit umfassend.

II. Wesentliche Inhalte der JI-Richtlinie

Die JI-Richtlinie macht weitreichende und umfassende Vorgaben für den polizeilichen Umgang mit personenbezogenen Daten. Während Grundsätze wie der des Gesetzesvorbehalts (Art. 8 Abs. 1 JI-Richtlinie) oder der Zweckbindung (Art. 4 Abs. 1 lit. c JI-Richtlinie) bereits aus dem nationalen Recht bekannt sind, hat der unionale Rechtsakt auch originäre Neuerungen für das Recht des polizeilichen Informationswesens mit sich gebracht.

So ist aufgrund der Ambivalenz der JI-Richtlinie bezüglich der Einwilligung als möglicher Rechtsgrundlage für polizeiliche Datenverarbeitungen die Frage aufgekommen, inwieweit diese noch als Anknüpfungspunkt für polizeiliche Maßnahmen wie etwa 81e, 81g und 81h StPO herangezogen werden kann. Die Frage besitzt also eine nicht unerhebliche Praxisrelevanz für die deutschen Polizeien. Problematisch ist in erster Linie die Frage nach der Freiwilligkeit einer Einwilligung im Angesicht des durch die Polizei verkörperten staatlichen Gewaltmonopols. Die Diskussion ist in vielen speziellen Fragen zu diesem Problem noch im Fluss.[727] Allerdings erscheint insgesamt zweifelhaft, wie weit die legitimierende Wirkung einer Einwilligung mit Blick auf die Komplexitäten des polizeilichen Informationswesens reichen kann. Die Verwendung von Daten, die auf dieser Grundlage verarbeitet werden, muss von vornherein durch entsprechende Vorkehrungen auf das vorgegebene Maß begrenzt werden. Auch wird der überwiegende Teil der polizeilichen Datensammlungen nicht aus solcherart mehr oder weniger „freiwillig" preisgegebenen Daten bestehen.

726 So *Schwabenbauer* in: *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch, G. Rn. 375 ff.; denkbare Fälle sind Selbstgefährdung, der Schutz privater Rechte und sonstiges datenschutzrechtliches Verhalten der Polizei wie das Führen von Personalakten, vgl. a.a.O. G. Rn. 377.

727 Siehe dazu *Müller/Schwabenbauer* in *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch des Polizeirechts, G. Rn. 472 ff.

Neu, zumindest in dieser Ausdrücklichkeit, ist auch der Verarbeitungsgrundsatz der Richtigkeit und Aktualität in Art. 4 Abs. 1 lit. d JI-Richtlinie. Da es sich bei der sachlichen Richtigkeit um ein objektives Kriterium handelt, fallen polizeiliche Einschätzungen als Werturteile nicht darunter. Entsprechende Bewertungen sind damit einer Kontrolle insoweit entzogen.[728] Ferner sind die Daten auch auf dem neusten Stand zu halten, was Nacherhebungen notwendig machen kann, damit neue Maßnahmen nicht auf veraltete und möglicherweise nicht mehr zutreffende Erkenntnisse gestützt werden.[729] Die Norm, über deren Umsetzung bisher nichts bekannt ist, stellt die Polizei einerseits vor die durchaus herausfordernde Aufgabe, den Datenbestand im Grunde laufend auf Richtigkeit und Aktualität zu überprüfen, was praktisch wohl eher anlassbezogen geschehen wird. Gleichzeitig ist dem Grundsatz aber auch eine nicht unproblematische, expansive Dynamik inhärent. Denn die Prüfung von Richtigkeit und Aktualität legt eher nahe, mehr oder häufiger Daten zu beschaffen, wenn die vorhandenen Daten möglicherweise veraltet oder falsch sein könnten.

Weniger auf den Schutz der kontextuellen als vielmehr auf den der physischen Unversehrtheit bedacht ist der Grundsatz der Integrität und Vertraulichkeit in Art. 4 Abs. 1 lit. f JI-Richtlinie. Dazu müssen Daten „in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich des Schutzes vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen." Erwägungsgrund 28 spezifiziert insofern, dass Unbefugte weder Zugang zu Daten haben, noch Verarbeitungsgeräte nutzen können sollen sowie dass die technischen Verarbeitungsprozesse risikoadäquat geschützt werden müssen. Nähere Ausgestaltung erfährt der Grundsatz zudem in Art. 29 JI-Richtlinie. Auch dieser Aspekt des Datenumgangs wird immer wichtiger und in seiner Umsetzung schwieriger. Denn Schutz muss etwa nicht nur vor böswilligen Akteur:innen geboten werden, die im Wege von Cyberattacken auf Polizeien neben dem analogen nun auch einen virtuellen Zugang erlangen können. Vielmehr muss auch der Zugang von mit den Polizeien kooperierenden Privaten reglementiert werden. Zuletzt besteht auch innerhalb der Behörde,

728 *Müller/Schwabenbauer* in *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch des Polizeirechts, G. Rn. 494.

729 *Müller/Schwabenbauer* in *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch des Polizeirechts, G. Rn. 495.

wie man immer wieder aus Medienberichten erfährt,[730] ein Problem mit unberechtigten Zugängen zu polizeifremden Zwecken.

Rechtliche Abbildung in Form der sogenannten Auftragsverarbeitung findet nun auch die in den komplexen Strukturen des polizeilichen Informationswesens nicht ausbleibende Delegation von Datenverarbeitungsvorgängen an – rechtlich gesehen – andere Stellen als den Verantwortlichen. Die Daten können nur nach Weisung des Verantwortlichen verarbeitet werden und demnach auch nur nach dessen Zweckbindungen, Art. 22, 23 JI-Richtlinie. Durch die Beauftragung darf das Schutzniveau der JI-Richtlinie nicht unterlaufen werden, sodass Vorgaben bezüglich technischer und organisatorischer Maßnahmen zum Schutz der Prozesse ebenso gelten. Problematisch wird im polizeilichen Informationswesen die Verarbeitung von Daten der Länderpolizeien durch das Bundeskriminalamt im Auftrag ersterer gesehen, wenn hiervon Informationen betroffen sind, die mangels überregionaler Relevanz eigentlich nur auf Landesebene verarbeitet werden dürften. Hier drohe, „dass die von den jeweiligen Gesetzgebern getroffenen Aufgabenverteilungen zwischen Bundes- und Länderpolizeien unter dem „Etikett der Auftragsverarbeitung" unterlaufen werden", sodass § 2 Abs. 1 BKAG, der Unterstützung bei der Datenverarbeitung durch das Bundeskriminalamt ermöglicht, nunmehr als Ausnahmeregelung zu verstehen sein soll.[731]

Mit Blick auf die Relevanz von Kontext und informationellem Gehalt von Daten versucht die JI-Richtlinie zudem über die Kategorisierung von Daten Steuerungsimpulse für deren angemessene Verarbeitung zu setzen. Die Kategorisierung erfolgt nach betroffenen Personen, Datengrundlage und informationellem Gehalt. Art 6 JI-Richtlinie verpflichtet die Mitgliedstaaten zunächst dazu, soweit wie möglich zwischen den verschiedenen Kategorien betroffener Personen klar zu unterscheiden. Unterschieden werden soll zwischen a) Personen, gegen die ein begründeter Verdacht besteht, dass sie eine Straftat begangen haben oder in naher Zukunft begehen werden, b) verurteilten Straftäter:innen, c) Opfern einer Straftat oder Personen,

730 Siehe etwa *Dachwitz* Netzpolitik.org; *Völlinger* Zeit Online v. 1. November 2019; *A. Becker* Nordkurier v. 31.05.2022 Damit soll nur ein kursorischer Überblick über entsprechende Medienberichte gegeben werden. Meistens sind Anfragen oder Tätigkeitsberichte der aufsichtsbehördlichen Datenschutzbeauftragten Anlass, mitunter aber auch Skandale wie die als „NSU 2.0" bezeichnete Affäre. Insgesamt deutet sich ein systemisch-strukturelles Defizit an.

731 *Müller/Schwabenbauer* in *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch des Polizeirechts, G. Rn. 507.

bei denen bestimmte Fakten darauf hindeuten, dass sie Opfer einer Straftat sein könnten, und d) anderen Parteien im Zusammenhang mit einer Straftat, wie Personen, die bei Ermittlungen in Verbindung mit der betreffenden Straftat oder beim anschließenden Strafverfahren als Zeug:innen in Betracht kommen, Personen, die Hinweise zur Straftat geben können, oder Personen, die mit den unter den Buchstaben a) und b) genannten Personen in Kontakt oder in Verbindung stehen. Diese Kategorien decken sich nicht vollständig mit denen des deutschen Polizeirechts, das vor allem die Begriffe Beschuldigte:r, Verdächtige:r und sonstige Kontakt- oder Anlasspersonen anknüpft. Weil die Richtlinie insoweit aber nicht abschließend ist, kann die deutsche Kategorisierung beibehalten oder nach hiesigen gesetzgeberischen Vorstellungen abgeändert werden, sofern damit weiter im Wesentlichen der Richtlinie entsprochen wird.[732] Daneben differenziert die JI-Richtlinie zwischen faktenbasierten Daten und auf persönlichen Einschätzungen beruhenden Daten, Art. 7 Abs. 1 JI-Richtlinie. Diese Kategorisierung soll insbesondere vor Übermittlungen Überprüfungen der Datenqualität initiieren und gegebenenfalls dazu anhalten, kontextuelle Daten für die empfangende Stelle mit zu übermitteln, soweit dies durchführbar ist. Dadurch wird die Kategorisierung bzw. die an sie anknüpfende Pflicht stark relativiert, wenngleich sie anders sicherlich kaum in die Praxis der Polizeibehörden eingefügt werden könnte. Die letzte Kategorisierung erfolgt entlang des (besonders sensiblen) informationellen Gehalts von Daten. Das sind gem. Art. 10 JI-Richtlinie solche Daten, aus denen die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie genetische Daten, biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung. Die Verarbeitung ist nur dann erlaubt, wenn sie unbedingt erforderlich ist, vorbehaltlich geeigneter Garantien für die Rechte und Freiheiten der betroffenen Person erfolgt. Zudem muss a) die Verarbeitung nach dem Unionsrecht oder dem Recht der Mitgliedstaaten zulässig sein b) der Wahrung lebenswichtiger Interessen der betroffenen oder einer anderen natürlichen Person dienen oder c) sich auf Daten beziehen, die die betroffene Person offensichtlich öffentlich gemacht hat. Zu geeigneten Garantien gehört gemäß Erwägungsgrund 37 „beispielsweise

732 *Müller/Schwabenbauer* in *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch des Polizeirechts, G. Rn. 500 ff.

[…], dass diese Daten nur in Verbindung mit anderen Daten über die betroffene natürliche Person erhoben werden dürfen, die erhobenen Daten hinreichend gesichert werden müssen, der Zugang der Mitarbeiter der zuständigen Behörde zu den Daten strenger geregelt und die Übermittlung dieser Daten verboten wird." Die Umsetzung in § 48 BDSG enthält neben technisch-organisatorischen Maßnahmen zudem auch die Sensibilisierung der an der Verarbeitung Beteiligten. Insbesondere aber das Regulativ der unbedingten Erforderlichkeit für die Aufgabenerfüllung darf als weitestgehend ungeklärt gelten, sodass auch bezüglich dieser – in der Sache begrüßenswerten – Kategorisierung fraglich ist, inwieweit sie nachhaltigen Einfluss auf die polizeiliche Datenverarbeitungspraxis haben wird, vor allem weil die Kategorisierung selbst ohne Rechtsfolge ist.[733] Darüber hinaus ist auch bezüglich des besonders sensiblen informationellen Gehalts bestimmter Daten problematisch, dass sich dieser nicht nur ex- sondern, wie bereits dargelegt, auch implizit aus der Zusammenschau eher „belanglos" scheinender Daten ergeben kann.[734] Da einige der besonderen Dateninhalte, wie etwa sexuelle Orientierung, auch den Kernbereichsschutz tangieren, darf hier für den deutschen Rechtsraum als offen gelten, wie mit solchen in den Daten enthaltenen virtuellen Informationen[735] zu verfahren ist. Es bleibt vor dem Hintergrund des Art. 10 JI-Richtlinie insgesamt abzuwarten, wie sich der Umstand auswirken wird, dass sich die in der Norm genannten Informationen – wenn auch nur unbeabsichtigt – aus Datensätzen mit entsprechenden Analysemethoden zunehmend herauslesen lassen können.

Im Rahmen der immer stärkeren Nutzung von Massendatenverarbeitungsverfahren rückt ein gegenwärtig überall aufscheinendes Problem auch im polizeilichen Handlungsfeld in den Fokus: Entscheiden noch Menschen auf der Grundlage der zur Verfügung stehenden Daten oder wird bereits von maschinellen „Intelligenzen", von Algorithmen, in Sachverhalten entschieden, die andere Menschen betreffen? Die JI-Richtlinie greift dies in Art. 11 JI-Richtlinie auf und postuliert ein Verbot für eine ausschließlich auf einer automatischen Verarbeitung beruhende Entscheidung, die eine nachteilige Rechtsfolge für die betroffenen Personen hat oder sie erheblich beeinträchtigt, es sei denn – das Verbot ist mithin nicht absolut – die

733 *Schwichtenberg* in *Kühling/Buchner,* Datenschutz-Grundverordnung, Bundesdatenschutzgesetz: DS-GVO / BDSG, Vor §§ 45 ff. Rn. 2.

734 Siehe dazu bereits oben S. 147 ff. Siehe dort insb. auch Fn. 583, in der es um die Ableitung von sexueller Orientierung aus banal scheinenden sozialen Netzwerkdaten ging.

735 Zum Phänomen der virtuellen Informationen siehe bereits oben S. 74 f.

Entscheidung ist nach dem Unionsrecht oder dem Recht der Mitgliedstaaten erlaubt, das zudem geeignete Garantien für die Rechte und Freiheiten der betroffenen Person, mindestens ein Recht auf menschliches Eingreifen seitens des Verantwortlichen, bieten muss. Fließen in eine solche Entscheidung besondere Kategorien personenbezogener Daten nach Art. 10 JI-Richtlinie ein, sind die Anforderungen noch einmal erhöht – erforderlich sind dann, dass geeignete Maßnahmen zum Schutz der Rechte und Freiheiten sowie der berechtigen Interessen der betroffenen Person getroffen werden. Bisher ist kein technisches System bei den deutschen Polizeien bekannt, dass aufgrund einer einzelfallbezogenen Entscheidung durch es selbst unter die skizzierten Vorgaben fallen würde. Zwar dürften Datenanalyseinstrumente wie die in 25a HSOG geregelte hessenDATA-Plattform menschliche Entscheidungen in einem nicht unerheblichen Maße vorstrukturieren und damit beeinflussen. Diese vorgelagerte Form des Einflusses auf die letztlich immer noch menschliche Entscheidung der handelnden Polizeibeamt:innen ist indessen nicht von Art. 11 JI-Richtlinie erfasst. Ob sich in Zukunft ein Anwendungsbereich hierfür auftun wird oder ob die technische Entwicklung weiter darauf achten wird, den „human in the loop" zu halten, ist offen.

Einen wesentlichen Schritt in Richtung einer vom Individuum abgelösten Datenschutzkontrolle geht die Rechenschaftspflicht aus Art. 4 Abs. 4 JI-Richtlinie. Der Verantwortliche (Art. 3 Nr. 8 JI-Richtlinie) muss demnach die Einhaltung der Datenschutzgrundsätze des Art. 4 Abs. 1-3 JI-Richtlinie nachweisen. Ergänzt wird die Vorschrift durch Art. 19 JI-Richtlinie. Danach hat der Verantwortliche „unter Berücksichtigung der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen geeignete technische und organisatorische Maßnahmen [umzusetzen], um sicherzustellen und den Nachweis dafür erbringen zu können, dass die Verarbeitung in Übereinstimmung mit dieser Richtlinie erfolgt." Diese Maßnahmen sind zudem laufend zu überprüfen und erforderlichenfalls nachzubessern. Die explizite einfachgesetzliche Umsetzung hat der Bundesgesetzgeber scheinbar unterlassen.[736] Nichtsdestotrotz ist die aus der JI-Richtlinie fließende Pflicht der Polizei, Rechenschaft über ihre Datenverarbeitungsprozesse abzulegen ein integraler Be-

736 *Müller/Schwabenbauer* in *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch des Polizeirechts, G. Rn. 499.

standteil einer massendatenverarbeitenden Polizei, deren Kontrolle längst nicht mehr über individuellen Rechtsschutz organisiert werden kann.

Damit ist auch die wesentliche Innovation der JI-Richtlinie im Vergleich zur nationalen Rechtssituation angesprochen. Datenschutz oder genauer: die Kontrolle des polizeilichen Datenumgangs durchläuft mit dem unionalen Rechtsakt eine Prozeduralisierung bisher unbekannten Ausmaßes.[737] Neue technische, organisatorische und institutionelle Arrangements sollen den Datenschutz als Querschnittsmaterie in der polizeilichen Praxis verankern und so zu einen normativ angeleiteten und (besser) steuerbaren Datenumgang im sensiblen Aufgabenspektrum der Polizei führen, auch weil sich dieses Ziel nicht mehr durch das schlichte Aufstellen insbesondere materieller Vorgaben bewerkstelligen lässt.[738] Zentral dafür ist ein innerbehördliches Prüfungs- und Kontrollsystem, das durch die Betroffenenrecht in Art. 12 ff. JI-Richtlinie und das System der Aufsichtsbehörden gemäß Art. 41 ff. JI-Richtlinie ergänzt und vervollständigt wird. Dieses innerbehördliche Datenschutzkontrollregime ist auf den drei Säulen der behördlichen Datenschutzbeauftragten, der Dokumentationspflichten sowie der technisch-organisatorischen Datenschutzinstrumente errichtet.

Als personale Ausprägung des polizeiinternen Prüfungs- und Kontrollsystems schreibt die JI-Richtlinie in Art. 32 Abs. 1 zunächst die behördlichen Datenschutzbeauftragten vor. Nach Art. 34 JI-Richtlinie ist deren Aufgabe neben weiteren Aspekten vor allem die Überwachung der Einhaltung der datenschutzrechtlichen Vorschriften und die Beratung der mit den Datenverarbeitungsprozessen betrauten Beamt:innen. Dabei geht es vor allem um die Anleitung der polizeilichen Fachlichkeit.[739] Um die Wirkmacht der Position zu maximieren sind die behördlichen Datenschutzbeauftragten gemäß Art. 33 Abs. 1 JI-Richtlinie frühzeitig in alle mit dem Schutz personenbezogener Daten zusammenhängenden Fragen einzubinden. Die Datenschutzbeauftragten dürfen daher nicht vor vollendete Tatsachen gestellt werden, sondern sind bereits von Beginn an in konzeptuelle Entwicklungen in einer Weise miteinzubeziehen, die ihren Anmerkungen Berücksichtigung verschafft.[740] Daneben sind die Datenschutzbeauftragten

737 *Müller/Schwabenbauer* in *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch des Polizeirechts, G. Rn. 461.
738 *Borell/Schindler* Datenschutz und Datensicherheit 43 (2019), 767 (768).
739 *Müller/Schwabenbauer* in *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch des Polizeirechts, G. Rn. 510.
740 *Borell/Schindler* Datenschutz und Datensicherheit 43 (2019), 767 (768).

auch Kontaktpunkte für die äußere Kontrolle durch die Aufsichtsbehörde, also für Bundes- und Landesdatenschutzbeauftragte. Mit diesen sind die behördlichen Datenschutzbeauftragen nach Art. 26 JI-Richtlinie zur Zusammenarbeit verpflichtet, wobei aber kein proaktives Tätigwerden der polizeilichen Beauftragten vorgesehen ist.[741] Flankiert wird das allgemeine Postulat der Zusammenarbeit durch spezielle Kooperationspflichten etwa im Rahmen des Verzeichnisses von Verarbeitungstätigkeiten (Art. 24 Abs. 2 Satz 2 JI-Richtlinie), Protokollierungen (Art. 25 Abs. 3 JI-Richtlinie) und der Datenschutz-Folgenabschätzung (Art. 28 Abs. 1 lit. a JI-Richtlinie). Im Vergleich zur DSGVO ist die Stellung der polizeilichen Datenschutzbeauftragten hingegen schwächer ausgestaltet, da insbesondere das Gebot der Weisungsfreiheit und das Verbot der Abberufung bzw. Benachteiligung aufgrund ihrer Tätigkeit fehlt, wobei dies hingegen durch Erwägungsgrund 63 JI-Richtlinie abgemildert wird, der eine Auftrags- und Aufgabenerfüllung in unabhängiger Weise nahelegt.

Diese drei eben genannten Instrumente bilden auch den Kern der Säule der Dokumentationspflichten. Das gemäß Art. 24 JI-Richtlinie zu führende Verzeichnis von Verarbeitungstätigkeiten soll einen Überblick über die in einer Behörde durchgeführten Datenverarbeitungen bieten und so einen ersten Anhaltspunkt für die Prüfung der Rechtmäßigkeit eröffnen. Daneben dienen die Verzeichnisse auch der internen Bestandsaufnahme und damit der Vergegenwärtigung des Umfangs der polizeibehördlichen Datenverarbeitungen.[742] Der Analyse einzelner Datenverarbeitungsverfahren dient ergänzend die Datenschutz-Folgenabschätzung aus Art. 27 Abs. 1 JI-Richtlinie. Eine solche ist durchzuführen bei Verarbeitungsvorgängen, bei denen ein hohes Risiko für die Rechte und Freiheiten betroffener Personen anzunehmen ist. Ein solches ist wiederum gegeben, wenn die Verarbeitung zu einem physischen, materiellen oder immateriellen Schaden führen kann, was umfassend erhebliche wirtschaftliche oder gesellschaftliche Nachteile erfasst, die sich aus der fehlenden Kontrolle über die eine Person betreffenden Daten ergibt.[743] Relevant ist das insbesondere im Kontext der Verwendung neuer Technologien, wozu etwa moderne Videoanalyse-Verfahren,[744] sonstige moderne Datenanalyse-Verfahren aber auch niedrigschwelligere

741 *Borell/Schindler* Datenschutz und Datensicherheit 43 (2019), 767 (768).
742 *Petri* in *Simitis/Hornung/Spiecker genannt Döhmann* (Hrsg.), Datenschutzrecht, Art. 30 Rn. 1.
743 Siehe die noch umfassendere Formulierung in Erwägungsgrund 75 DSGVO.
744 *Borell/Schindler* Datenschutz und Datensicherheit 43 (2019), 767 (769).

Technologien wie etwa die Einführung von Bodycams zählen dürften. Zu enthalten hat die Folgenabschätzung gemäß Art. 27 Abs. 2 JI-Richtlinie „eine allgemeine Beschreibung der geplanten Verarbeitungsvorgänge und eine Bewertung der in Bezug auf die Rechte und Freiheiten der betroffenen Personen bestehenden Risiken sowie der geplanten Abhilfemaßnahmen, Garantien, Sicherheitsvorkehrungen und Verfahren, durch die der Schutz personenbezogener Daten sichergestellt und der Nachweis dafür erbracht wird, dass diese Richtlinie eingehalten wird." Infolge einer Datenschutzfolgenabschätzung kann sich, wie erwähnt, eine Pflicht zur Konsultation der Aufsichtsbehörde ergeben, wenn trotz festgestellten hohen Risikos keine Eindämmungsmaßnahmen ergriffen werden (Art. 28 Abs. 1 lit. a JI-Richtlinie), etwa weil es keine technologischen Lösungen gibt.[745] Dass dies nur bei „neu anzulegenden Dateisystemen" gilt, dürfte Praktikabilitätsüberlegungen im Kontext der Polizei geschuldet sein, ist aber mit Blick auf Altsysteme bedenklich, insbesondere, wenn es zu Umstrukturierungen von bestehenden Systemen kommt. Sowohl die Datenschutz-Folgenabschätzung als auch das Verzeichnis von Verarbeitungstätigkeiten helfen den Behörden selbst aber auch der Aufsicht, die Rechtmäßigkeit des polizeilichen Datenumgangs besser zu beurteilen. Allerdings vermitteln sie eher eine statische Momentaufnahme der Gesamtheit der Verfahren bzw. der Einzelheiten eines Verfahrens. Die Dynamiken der tatsächlich durchgeführten Datenverarbeitungen wird hingegen durch Protokollierungen dokumentiert und damit der Rechtmäßigkeitskontrolle zugeführt. Die Polizeibehörden haben gemäß Art. 25 Abs. 1 JI-Richtlinie bei automatisierten Verarbeitungssystemen die Erhebung, Veränderung, Abfrage, Offenlegung einschließlich Übermittlung, Kombination und Löschung von Daten zu protokollieren, wobei Begründung, Darum und Uhrzeit und – soweit möglich – Identität der abfragenden bzw. offenlegendenden und empfangenden Person zu protokollieren sind. Der Begriff der automatisierten Verarbeitung ist in seinem Bedeutungsgehalt aus den Texten der europäischen Datenschutzreform nur implizit ableitbar, was auch die inhaltliche Erfassung des Begriffs der „automatisierten Verarbeitungssysteme" erschwert. Anzunehmen ist, dass „alle Verfahren [erfasst werden], bei denen ein Datenverarbeitungsvorgang anhand eines vorgegebenen Programms ohne weiteres menschliches Zutun selbsttätig erledigt wird", wobei die Digitalisierung eines Prozesses

745 *Borell/Schindler* Datenschutz und Datensicherheit 43 (2019), 767 (769).

hinreichend, aber nicht notwendig sein soll.[746] Noch extensiver ist ein Verständnis, dass darunter „sämtliche heute gebräuchlichen rechnergestützten Verarbeitungen personenbezogener Daten" fasst.[747] Vor allem mit Blick auf die vermehrte Umstellung auf die elektronische Akte nimmt die Bedeutung der Protokollierungspflicht somit weiter zu. Während sich gegenwärtig der Umgang mit in Papierakten gespeicherten Daten nicht festhalten lässt, hält die Digitalisierung insofern ein erhebliches Potenzial für die Kontrolle des polizeilichen Datenumgangs in seiner Gesamtheit bereit.[748]

Die letzte Säule des polizeiinternen Datenschutzkontrollregimes sind die technischen Datenschutzinstrumente. Mit Art. 20 legt die JI-Richtlinie fest, dass Technikgestaltung und datenschutzrechtliche Voreinstellungen die Rechtmäßigkeit der Datenverarbeitung durch entsprechende Designs sicherstellen oder zumindest fördern sollen. Den dahinterstehenden Gedanken hat *Roßnagel* bereits 2005 prägnant auf den Punkt gebracht:

> „Ohne technische Unterstützung droht Recht in einer technikgeprägten Welt folgenlos zu bleiben. Recht ist auf rechtsgemäße Technik angewiesen. Informationelle Selbstbestimmung ist durch, nicht gegen Technik zu ermöglichen. Schutz durch Technik ist oft die einzig mögliche Antwort auf Probleme der Globalisierung der Datenflüsse, der dynamischen Technikentwicklung und der zunehmenden Intransparenz der Systeme."[749]

Nach Art. 20 JI-Richtlinie müssen Polizeibehörden unter Berücksichtigung des Stands der Technik, der Kosten sowie von Art, Umfang, Umständen und Zwecken der Verarbeitung und der Risiken für die Rechte und Freiheiten betroffener Personen durchgängig angemessene technische und organisatorische Maßnahmen vornehmen, um die Datenschutzgrundsätze (Art. 4 JI-RL) und die übrigen Anforderungen der JI-RL wirksam umzusetzen. Dabei ist durch die explizite Nennung der Datenminimierung diese wohl leitendes Gestaltungskriterium. Offenkundig wird dadurch ein Spannungsverhältnis zur Arbeit einer modernen Polizei geschaffen, die im Wesentlichen auf die Verarbeitung von Informationen angewiesen ist. Verschärft wird dieser Konflikt durch die zunehmende Entwicklung hin „zu neuen, stark

746 *Bäcker* in *Brink/H. Wolff*, BeckOK Datenschutzrecht, DS-GVO Art. 2 Rn. 2
747 *Zerdick* in *Ehmann/Selmayr/J. Albrecht,* DS-GVO, Art. 2 Rn. 3.
748 *Roßnagel* in *Simitis/Hornung/Spiecker genannt Döhmann* (Hrsg.), Datenschutzrecht, Art. 4 Nr. 6 Rn. 12.
749 *Roßnagel* Informatik Spektrum 28 (2005), 462 (469).

datengetriebenen Ermittlungs- und Gefahrenabwehrwerkzeugen öffentlicher Stellen wie beispielsweise Predictive Policing oder automatisiert ausgewerteter Kameraüberwachung zur Gesichts- und Verhaltenserkennung."[750] Zwar ist bezüglich der genannten Technologien eine datensparsame Funktionsweise denkbar, etwa durch die direkte Löschung im Nichttrefferfall bei biometrischer Videoüberwachung oder die Nutzung von raumbezogenen Formen des Predictive Policings. Allerdings ist durchaus fraglich, ob eine unter dem Paradigma der Massendaten operierende Polizei das Postulat der Datenminimierung und -sparsamkeit auf Dauer wird durchhalten können. Unter die technischen Datenschutzprinzipien lässt sich auch die Datensicherheit fassen, die in Art. 29 JI-Richtlinie näher spezifiziert wird. Wie bereits in Art. 20 JI-Richtlinie sind auch hier der Stand der Technik, die Kosten sowie Art, Umfang, Umstände und Zwecke der Verarbeitung sowie die Risiken für die Rechte und Freiheiten betroffener Personen zu berücksichtigen. Der Katalog des Art. 29 Abs. 2 JI-Richtlinie enthält verschiedene Mittel zur Gewährleistung der Datensicherheit, wie Speicherkontrolle, Benutzerkontrolle, Zugangskontrolle, Eingabekontrolle oder Übertragungskontrolle. Diese dienen der Nachverfolgung des Datenumgangs durch einzelne Beamt:innen. Wesentlich sind auch Zuverlässigkeit, also die Gewährleistung, dass alle Funktionen des Systems zur Verfügung stehen, auftretende Fehlfunktionen gemeldet werden und Datenintegrität, das heißt dass gespeicherte personenbezogene Daten nicht durch Fehlfunktionen des Systems beschädigt werden können. Diese Instrumente spielen auch bei der Verarbeitung besonderer Kategorien personenbezogener Daten eine wesentliche Rolle.[751]

Kommt es trotz dieser Vorkehrungen zu Verstößen gegen das polizeiliche Datenschutzrecht, so muss die jeweilige Polizeibehörde gemäß Art. 30 JI-Richtlinie dies der Aufsichtsbehörde melden, es sei denn – was im polizeilichen Kontext aufgrund der Sensibilität der Daten selten anzunehmen sein wird – dass die Verletzung des Schutzes personenbezogener Daten voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt. Auch die betroffene Person ist zu benachrichtigen, wobei Art. 31 JI-Richtlinie hier mehr Ausnahmen als bei der aufsichtsbehördlichen Meldepflicht kennt und in Abs. 3 i.V.m. Art. 13 Abs. 3 JI-Richtlinie den

750 *Marnau* in *Gola/Heckmann/Klug* ua, BDSG, § 71 Rn. 23 f.
751 *Müller/Schwabenbauer* in *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch des Polizeirechts, G. Rn. 531 f.

praktisch wohl bedeutendsten Ausnahmefall der Behinderung behördlicher Ermittlungstätigkeit aufstellt.

Insgesamt wird man bezüglich der Neuerungen der JI-Richtlinie zustimmen können, dass sie den polizeilichen Datenumgang nicht „von Grund auf neu gestalte[t]" hat.[752] Nichtsdestotrotz scheint die Prozeduralisierung und personale sowie technische Institutionalisierung von Schutzmechanismen ein sinnvoller Weg für eine Polizei zu sein, die zunehmend Datenaggregationen handhaben muss, die weit über individuelle Verfahren und die von ihnen betroffenen Personen hinausgehen. Hier ein individuenzentriertes Datenschutzkonzept zu verfolgen, erscheint für sich genommen nicht weiter zukunftsfähig, sodass die Innovationen der europäischen Datenschutzreform als notwendiger Schritt in Richtung eines eingehegten polizeilichen Informationswesens gesehen werden müssen, was die Steuerungskraft des Rechts durch ein robustes Datenschutzkontrollregime sowohl intern wie extern erhöhen kann.

C. Einfachgesetzliche Rahmenbedingungen des polizeilichen Informationswesens

Die bisher dargestellten verfassungsrechtlichen und unionalen Normenkomplexe haben zwar durchaus auch direkte Auswirkungen auf die praktische Ebene der polizeilichen Datenverarbeitung. Mehrheitlich handelt es sich dabei aber um Vorgaben für Bundes- und Landesgesetzgeber, die verpflichtet sind, das polizeiliche Informationswesen mit dem Erlass entsprechender Gesetze zu strukturieren und zu steuern. Zu diesem Zweck gibt es im Wesentlichen seit dem Volkszählungsurteil einen Gesetzgebungsschub in den Polizeigesetzen und der Strafverfahrensordnung, um diesem legislativen Gestaltungsauftrag nachzukommen. Daraus ist ein komplexes Gesetzessystem evolviert, das aufgrund seiner Eigenständigkeit und Relevanz besser als polizeiliches Informationsrecht[753] oder polizeiliche Informationsordnung[754] denn als polizeiliches Datenschutzrecht bezeichnet werden kann. Die Schwierigkeit eines jeden Rechts, Lebensweltliches möglichst umfassend und für das übrige Rechtssystem anschlussfähig mit Begriffen und Verhältnissen zu erfassen, wird für das polizeilichen Informationswe-

752 *Borell/Schindler* Datenschutz und Datensicherheit 43 (2019), 767 (772).
753 So bereits oben S. 25.
754 *Bäcker,* Kriminalpräventionsrecht, S. 473.

sen allerdings dadurch erheblich erschwert, dass es prälegal, also weit vor seiner rechtlichen Erschließung, entstanden und zunächst weitestgehend unabhängig vom Recht gewachsen ist.[755] Insofern steht die rechtliche Rahmung polizeilicher Datenverarbeitung vor der Herausforderung, die Institutionen, Infrastrukturen und Praktiken des Informationswesen normativ zu erfassen und damit gesetzgeberisch gestaltbar zu machen. Im Folgenden sollen diese gesetzlichen Strukturen in ihren Grundzügen dargelegt und einer kritischen Überprüfung unterzogen werden.

Die systematische Darstellung der in diesem Kontext relevanten Normkomplexe ist indessen kein leichtes Unterfangen. Die Polizeilandschaft Deutschlands ist föderalistisch strukturiert. Sowohl Bundes- als auch Landespolizeibehörden verarbeiten im Rahmen ihrer wesentlichen Aufgaben – Strafverfolgung und Gefahrenabwehr – personenbezogene Daten, auf Grundlage unterschiedlicher Gesetze bzw. im Anwendungsbereich mehrerer Rechtsgrundlagen, etwa wenn Daten zweckändernd übertragen werden. Die folgende Darstellung der einfachgesetzlichen Rahmenbedingungen orientiert sich auf einer ersten Ebene nicht an den jeweiligen Gesetzesmaterien, sondern unternimmt den Versuch einer Systematisierung anhand von für das polizeiliche Informationswesen wesentlichen technischen Strukturen und Praktiken, da diese beiden Aspekte das polizeiliche Informationswesen im Kern ausmachen. Nach einem generellen Überblick über die einfachrechtliche Terminologie und Prinzipien der polizeilichen Datenverarbeitung erfolgt deshalb eine Darstellung der normativen Verankerung der informationstechnologischen Infrastrukturen des polizeilichen Informationswesens. Im Anschluss daran werden die normativen Vorgaben für die Praktiken der Informationsverarbeitung erläutert. Abschließend wird noch auf das interne Datenschutzkontrollregime eingegangen, das ebenfalls von zentraler Bedeutung für das polizeiliche Informationswesen sowie den empirischen Teil der Arbeit ist.

I. Einfachrechtliche Terminologie und Prinzipien der polizeilichen Datenverarbeitung

Für die unterschiedlichen Arten des Datenumgangs sahen und sehen die jeweiligen polizeirechtlichen Normenkomplexe auf Bundes- und Lan-

755 Siehe dazu bereits oben S. 101 ff.

desebene grundsätzlich eine einheitliche Terminologie vor. So unterscheiden die Gesetze oft zwischen Datenspeicherung, -veränderung. -nutzung, -übermittlung, -berichtigung, und -löschung. Diese Unterscheidung wurde jedoch von der JI-Richtlinie hinsichtlich der Verarbeitungsvoraussetzungen nicht aufgegriffen, sodass vermutet wird, die begriffliche Differenzierung zwischen den einzelnen Verarbeitungsphasen würde nach Umsetzung der unionsrechtlichen Vorgaben in den Landespolizeigesetzen weitestgehend bedeutungslos werden.[756] Zudem enthalten die entsprechenden Gesetze die den gesamten Prozess der Datenverarbeitung leitenden, verfassungsrechtlich geformten Verarbeitungsprinzipien. Gesetzestechnisch sind diese Grundsätze entweder isoliert geregelt oder in den jeweiligen Rechtsgrundlagen zur Datenverarbeitung inkorporiert.

I. Terminologie

Die Terminologie in den Landespolizeigesetzen ist insgesamt (noch) sehr einheitlich und differenziert zumeist zwischen den bereits genannten Verarbeitungsschritten der Datenspeicherung, -veränderung. -nutzung, -übermittlung, -berichtigung, und -löschung. Obwohl diese Differenzierung im europäischen Datenschutzrecht nunmehr obsolet zu sein scheint, halten etliche Landespolizeigesetze auch nach der Umsetzung der JI-Richtlinie daran fest. Aber die unionale Vereinheitlichung der Verarbeitungsschritte zeigt auch Wirkung: Auf Bundesebene, etwa im BKAG, ist diese Differenzierung nicht mehr in ihrer Detailliertheit vorhanden: Die zentrale Kategorie ist dort nunmehr die sog. Weiterverarbeitung, was insbesondere die Speicherung, Veränderung und Nutzung von Daten zusammenfassend meint. Auch einige Länder – wie etwa Nordrhein-Westfalen – haben die europarechtliche Terminologie übernommen. Im dortigen Polizeigesetz ist aber beispielsweise die Speicherung als eigenständige informationelle Befugnis erhalten geblieben. Mithin sind gegenwärtig sowohl traditionelle als auch neue Terminologie nebeneinander zu beachten.

756 So etwa *Petri* in *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch, G. Rn. 843.

a) Datenspeicherung

Die Datenspeicherung meint das Erfassen, Aufnehmen oder Aufbewahren von Daten auf (irgend)einem Datenträger zum Zwecke ihrer weiteren Verwendung. Fixiert die Polizei die Daten nicht selbst auf einem Speichermedium, sondern bekommt sie von dritter Stelle, ist ein Fall des Aufbewahrens gegeben.[757] Unerheblich ist im Rahmen der Speicherung der eingesetzte Träger. Diese für die rechtliche Einordnung zunächst bestehende Irrelevanz des gewählten Speichermediums macht die in einigen Polizeigesetzen noch bestehende Differenzierung zwischen der Speicherung in Dateien und in Akten prinzipiell überflüssig.[758] Auch die Polizeipraxis, in der physische Akten zunehmend vollständig oder zumindest ihr Index digitalisiert werden und in ihnen enthaltene Daten so besser auffindbar sind, zeugt von der schwindenden Bedeutung der Unterscheidung zwischen analoger Akte und digitaler Datei. Die sich aufgrund einer solchen Datenerfassung in automatisierten Dateien ergebenden tiefergehenden Verarbeitungsmöglichkeiten sind allerdings rechtlich alles andere als irrelevant: Es besteht hier regelmäßig eine höhere Eingriffsqualität, da größere Datenvolumina aufbewahrt, durchsucht und verknüpft werden können.[759] Darüber hinaus ist der Akt der Datenspeicherung für die polizeiliche Informationsverarbeitung ein schlechthin essenzieller Punkt, denn hierauf baut sie letztlich auf. Für die Speicherdauer kann jedes gespeicherte personenbezogene Datum – im Rahmen der gesetzlichen Befugnisse – in vielerlei Hinsicht genutzt werden. Mit dem Akt der Speicherung werden die Weichen hierfür gestellt. Gerade diese zentrale Position der Datenspeicherung müsste sie zum Gegenstand erhöhter legislativer Aufmerksamkeit machen.[760]

757 *Von der Grün* in *Möstl/Trurnit* (Hrsg.), Beck'scher Online-Kommentar Polizeirecht Baden-Württemberg, § 37 PolG BW, Rn. 16.

758 *Aulehner* in *Möstl/Schwabenbauer* (Hrsg.), Beck'scher Online-Kommentar Polizei- und Sicherheitsrecht Bayern, Art. 53 PAG Rn. 6a.

759 So auch *Arzt* in *Möstl/Kugelmann* (Hrsg.), Beck'scher Online-Kommentar Polizei- und Ordnungsrecht Nordrhein-Westfalen, § 20 PolG NRW, Rn. 26.1; *Petri* in *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch, G. Rn. 847.

760 Ähnlich *Petri* in *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch, G. Rn. 847; siehe dazu auch *Bäcker,* Kriminalpräventionsrecht, S. 473.

b) Datenveränderung

Werden gespeicherte Daten inhaltlich derart umgestaltet, dass es ihren Informationsgehalt und nicht nur ihre Darstellungsweise modifiziert, liegt eine Datenveränderung vor.[761] Neben dem Hinzufügen oder Löschen von Daten ist die Herstellung eines neuen Zusammenhang ein bedeutsamer Unterfall der Datenveränderung: Werden Daten etwa in eine einschlägige Datensammlung übertragen, kann diese Rekontextualisierung den Informationsgehalt erheblich beeinflussen, ohne dass an den Daten selbst inhaltliche Änderungen vorgenommen werden.[762] Das Risiko fluider und rekombinatorischer Informationsgehalte personenbezogener Daten betonte das Bundesverfassungsgericht bereits im Volkszählungsurteil.[763] Die rechtförmige Einhegung dieser Art des Datenumgangs hat dementsprechend vor der Verfassung besonderes Gewicht. Problematisch sind vor diesem Hintergrund Rechtsgrundlagen, die die Datenveränderung pauschal und niedrigschwellig freigeben, etwa soweit und solange sie zur Aufgabenerfüllung erforderlich sind.[764]

c) Datenübermittlung

Der Informationsfluss zwischen verschiedenen Polizeibehörden und zwischen Polizei und sonstigen (nicht-)öffentlichen Stellen wird rechtlich durch die sog. Datenübermittlung abgebildet. Übermitteln war bislang das Bekanntgeben personenbezogener Daten an einen Dritten in der Weise, dass die Daten an den Dritten weitergegeben werden oder der Dritte zur Einsicht oder zum Abruf bereitgehaltene Daten einsieht oder abruft.[765] Rechtlich beachtenswert ist diese Verwaltungspraxis vor allem deshalb, weil durch die Erweiterung des Kreises derjenigen Stellen, die Kenntnis von

761 *Von der Grün* in *Möstl/Trurnit* (Hrsg.), Beck'scher Online-Kommentar Polizeirecht Baden-Württemberg, § 37 PolG BW, Rn. 17.
762 *Petri* in *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch, G. Rn. 884.
763 BVerfGE 65, 1 (44) – Volkszählung.
764 Siehe etwa § 15 Abs. 1 PolG BW, Art. 54 BayPAG, § 42 ASOG Berlin, § 36 PolDVG Hamburg. Ein Positivbeispiel ist etwa Bremen, dessen § 36a BremPolG Rechtmäßigkeit und Zweckbindung besonders betont, ähnlich ist es in Niedersachen § 38 NPOG.
765 *Röcker* in *Möstl/Trurnit* (Hrsg.), Beck'scher Online-Kommentar Polizeirecht Baden-Württemberg, § 41 PolG BW, Rn. 5.

den Daten haben, die Intensität des grundrechtlichen Risikos Betroffener erhöht wird.[766] Der Akt der Datenübermittlung erscheint im Bereich der polizeilichen Datenverarbeitung in verschiedenen Ausführungen, abhängig bspw. davon von wem, an wen, auf wessen Verlangen oder auf welche Weise Daten übermittelt werden.

Im Angesicht der JI-Richtlinie ist allerdings noch nicht sicher, ob und inwieweit die bisherige Terminologie unverändert beibehalten werden kann, da das EU-Datenschutzrecht insofern Bedeutungsverlagerungen auslösen könnte.[767] Zwar spielt die Übermittlung von Daten – obwohl nicht explizit definiert – auch in der Richtlinie eine Rolle. Kapitel V der Richtlinie soll sicherstellen, dass ihr Datenschutzniveau nicht durch Übermittlungen unterlaufen wird, womit das europarechtliche Begriffsverständnis weiter als das hiesige ist: Erfasst ist jeder Verarbeitungsvorgang, durch den personenbezogene Daten den Geltungsbereich der JI-Richtlinie verlassen und die Endbestimmung der Daten außerhalb des Unionsgebiets liegt oder die Daten von außerhalb der Union zugänglich sind.[768]

d) Datenberichtigung

Die Datenberichtigung, die als Pflicht auf Seiten der Polizei und korrespondierend zum Anspruch Betroffener besteht, wird dann relevant, wenn personenbezogene Daten unrichtig sind, d.h. ein unzutreffendes Bild von der Wirklichkeit vermitteln. Im Wege der Berichtigung wird der Informationsgehalt des in Frage stehenden Datums wieder in Übereinstimmung mit der Realität gebracht.[769] Sind die personenbezogenen Daten aktenförmig, so ist die Berichtigung zu bewerkstelligen, indem die Unrichtigkeit in der Akte vermerkt oder auf sonstige Weise festgehalten wird.[770] Bei der Datenberichtigung handelt es sich strenggenommen um eine besondere Form der Datenveränderung, sodass etwa auch durch die Speicherung neuer Daten berichtigt werden kann.[771]

766 *Petri* in *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch, G. Rn. 483.
767 *Petri* in *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch, G. Rn. 489.
768 So *Zerdick* in *Ehmann/Selmayr/J. Albrecht* ua (Hrsg.), DS-GVO, Art. 44 DS-GVO, Rn. 7, für die DS-GVO.
769 *Graulich* in *Schenke/Graulich/Ruthig,* Sicherheitsrecht, § 9 BKAG Rn. 14.
770 *Ogorek* in *Möstl/Kugelmann* (Hrsg.), Beck'scher Online-Kommentar Polizei- und Ordnungsrecht Nordrhein-Westfalen, § 32 PolG NRW, Rn. 3.
771 *Graulich* in *Schenke/Graulich/Ruthig,* Sicherheitsrecht, § 9 BKAG Rn. 14.

e) Datenlöschung

Das Löschen von Daten hat die Unkenntlichmachung gespeicherter personenbezogener Daten zum Gegenstand. Umfasst ist jede Form von Unkenntlichmachung vom Ausradieren, Schwärzen, Übermalen bis hin zur physischen Vernichtung. Entscheidend ist, dass die Information der verantwortlichen Stelle irreversibel nicht mehr zur Verfügung steht.[772] Nicht ausreichend ist eine Änderung der Datenorganisation derart, dass der gezielte Zugriff auf die zu löschenden Daten verhindert wird. Vor allem mit Blick auf Rekonstruktionsmöglichkeiten von Daten befindet sich der Bedeutungsgehalt der Datenlöschung im Wandel und hängt vom Stand der Technik ab.[773]

f) Datensperrung bzw. Einschränkung der Weiterverarbeitung

Sperren von Daten meint die Kennzeichnung von personenbezogenen Daten, um ihre weitere Verarbeitung einzuschränken,[774] etwa weil ihre Richtigkeit angezweifelt wurde. Im Rahmen der Umsetzung der JI-Richtlinie auf Bundes- und Landesebene ist der Begriff der Sperrung in etlichen Gesetzen durch denjenigen der Einschränkung der (Weiter)Verarbeitung ersetzt worden. Inhaltliche Änderungen sollen damit nicht verbunden sein.[775]

g) Datennutzung

Als Datennutzung gilt jede sonstige Verwendung, die nicht Erhebung, Speicherung, Veränderung, Übermittlung, Berichtigung, Sperrung, Löschung oder Vernichtung ist. Es handelt sich dementsprechend um einen Auffangtatbestand, der greift, wenn die Daten mit einer bestimmten Zweckrichtung ausgewertet, zusammengestellt, abgerufen oder zielgerichtet zur Kenntnis

772 *Hermesmeier/Brenz* in *Möstl/Trurnit* (Hrsg.), Beck'scher Online-Kommentar Polizeirecht Baden-Württemberg, § 46 PolG BW, Rn. 2.
773 Vgl. *Arzt* in *Schenke/Graulich/Ruthig,* Sicherheitsrecht, § 35 BPolG, Rn. 13.
774 *Hermesmeier/Brenz* in *Möstl/Trurnit* (Hrsg.), Beck'scher Online-Kommentar Polizeirecht Baden-Württemberg, § 46 PolG BW, Rn. 12.
775 *Ruthig* in *Schenke/Graulich/Ruthig,* Sicherheitsrecht, § 78 Rn. 6; *Ogorek* in *Möstl/Kugelmann* (Hrsg.), Beck'scher Online-Kommentar Polizei- und Ordnungsrecht Nordrhein-Westfalen, § 32 PolG NRW Rn. 33.

genommen werden.[776] Als Verarbeitungsform spielt sie nur in denjenigen Polizeigesetzen noch eine Rolle, die noch zwischen Datenerhebung, Datenverarbeitung und Datennutzung unterscheiden und soll in ihren rechtlichen Voraussetzungen analog zur Datenspeicherung zu behandeln sein.[777]

h) Der neue Begriff der Weiterverarbeitung

In einigen Landespolizeigesetzen und auch im novellierten BKAG findet sich nunmehr der Begriff der „Weiterverarbeitung" personenbezogener Daten in den zentralen Datenverarbeitungsbefugnissen. Während sich in den Landespolizeigesetzen neben oder eher zwischen Datenerhebung und Weiterverarbeitung oft noch Befugnisnormen zum Akt der Datenspeicherung finden, ist die Datenweiterverarbeitung im BKAG zur Kernbefugnis für Datenumgang avanciert. Die Nivellierung der unterschiedlichen Datenverarbeitungsphasen, die mit der Einführung des Begriffs der Weiterverarbeitung einhergeht, ist vor allem auf die europäische Datenschutzreform zurückzuführen. Art. 3 Nr. 2 JI-Richtlinie kennt als übergeordnete Form der Datenumgangs allein noch die Verarbeitung, also jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung. Das BDSG und die jeweiligen Landesdatenschutzgesetze übernehmen diese Terminologie, sodass die darauf Bezug nehmenden Bundes- und Landespolizeigesetze nunmehr vom europarechtlichen Begriff der Verarbeitung geprägt sind. Es ist letztlich – bewusst auf Differenzierung, wie sie das deutsche Datenschutzrecht vorher kannte, verzichtend[778] – jeder Umgang mit Daten erfasst.[779]

776 *Graf* in *Möstl/Weiner* (Hrsg.), Beck'scher Online-Kommentar Polizei- und Ordnungsrecht Niedersachsen, § 38 NPOG, Rn. 30.
777 *Petri* in *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch, G. Rn. 885.
778 *Bäuerle* in *Möstl/Mühl* (Hrsg.), Beck'scher Online-Kommentar Polizei- und Ordnungsrecht Hessen, § 20 HSOG, Rn. 22.
779 *Schild* in *Brink/H. Wolff*, BeckOK Datenschutzrecht, Art. 4 DS-GVO Rn. 32.

Während die Intention einer möglichst lückenlosen Erfassung und damit eines möglichst lückenlosen Schutzes per se zu begrüßen ist, bringt die begriffliche Einebnung auch ein Problem mit sich: Die mit verschiedenen Formen des Datenumgangs verbundene Eingriffsintensität lässt sich so begrifflich im Gesetz nur begrenzt operationalisieren. Wenn etwa das (eher administrativ anmutende) Ordnen terminologisch mit dem (tendenziell invasiveren) Verknüpfen[780] unter einen Oberbegriff vermengt wird und beide beispielsweise pauschal zur polizeilichen Aufgabenerfüllung freigegeben werden, ist die verhältnismäßige Handhabung der unterschiedlichen Intensitätsgrade in der Polizeipraxis zusätzlich erschwert. Eine begriffliche Trennung kann also dazu beitragen, ein differenziertes Bewusstsein und eine reflektiertere Anwendungspraxis zu schaffen.

2. Prinzipien der polizeilichen Datenverarbeitung

Neben der Terminologie der polizeilichen Datenverarbeitung enthalten die Polizeigesetze regelmäßig auch Ausführungen zu den allgemeinen, für jede Art des Datenumgangs geltenden Verarbeitungsprinzipien. Die Grundsätze sind verfassungs- oder europarechtlich determiniert, werden aber durch ihre einfachgesetzliche Umsetzung in der Gesetzessystematik konkretisiert und überhaupt erst wirkungsvoll gegenüber Rechtsanwender:innen. Die wichtigsten von ihnen sind der Zweckbindungsgrundsatz mit der darauf bezogenen Regelung der Zweckänderung sowie die Grundsätze der Erforderlichkeit und Verhältnismäßigkeit.

a) Zweckbindung

Als zentrales Prinzip des deutschen Datenschutzrechtes ist auch in der polizeilichen Datenverarbeitung der Zweckbindungsgrundsatz normativ fest verankert.[781] In diesem Kontext bedeutet es zunächst für jedes in die Sphäre der Polizei gelangte Datum eine Beschränkung der Verarbeitung auf den ursprünglichen (zumeist Erhebungs-)Zweck. Ebenfalls noch im Rahmen der Zweckbindung enthalten, ist seit dem BKAG-Urteil des Bundesverfas-

780 Siehe zu den jeweiligen Begriffsinhalten *Müller/Schwabenbauer* in *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch des Polizeirechts, G. Rn. 594.

781 *Braun* in *Gola/Heckmann/Klug* ua, BDSG, § 47 Rn. 15.

sungsgerichts auch die zweckwahrende Weiternutzung.[782] So soll die multifunktionelle Nutzbarkeit von Daten in rechtlich zulässige Bahnen gelenkt werden.[783]

Die Übersetzung des Zweckbindungsgrundsatzes in seiner für die polizeiliche Datenverarbeitung seit dem BKAG-Urteil geltenden Form in einfaches Recht ist dabei nicht immer ganz unproblematisch, da oftmals lediglich der Urteilstext Wort für Wort übernommen wurde. Dabei wird zunächst missachtet, dass sich die Vorgaben des Bundesverfassungsgerichts an den Gesetzgeber und nicht an die Rechtsanwender:innen richten.[784] Durch die Schaffung wortlautgetreuer Rechtsnormen enthält sich der Gesetzgeber seiner legislativen Gestaltungsaufgabe und wälzt die Verantwortung zur verfassungskonformen Datenverarbeitung direkt auf die Exekutive ab,[785] der so nur die Möglichkeit der Selbstprogrammierung[786] bleibt. Die normative Orientierungslosigkeit auf Ebene der Rechtsanwendung wird zudem noch dadurch verstärkt, dass die Datenerhebungsbefugnisse in den Polizeigesetzen regelmäßig keine konsistente Zweckbestimmung enthalten. Vielmehr lassen solche sich im Wege der Auslegung aus dem Tatbestand extrahieren oder die Befugnisse verweisen generell auf die zu Beginn des Gesetzes definierten abstrakten Behördenaufgaben.[787] Eine dem Bestimmtheitsgrundsatz angemessene einfachgesetzliche Ausfüllung des verfassungsrechtlichen Zweckbindungsgrundsatzes wird so für den Bereich polizeilicher Datenverarbeitung höchstens ansatzweise geleistet.[788]

782 Siehe dazu bereits die Ausführungen oben S. 164 ff.

783 *Von der Grün* in *Möstl/Weiner* (Hrsg.), Beck'scher Online-Kommentar Polizei- und Ordnungsrecht Niedersachsen, § 38 Rn. 24.

784 Siehe zu dieser Differenzierung allgemein *Härting* Neue Juristische Wochenschrift 2015, 3284.

785 *Bäuerle* in *Möstl/Mühl* (Hrsg.), Beck'scher Online-Kommentar Polizei- und Ordnungsrecht Hessen, § 20 HSOG Rn. 36.

786 Allgemein zur Selbstprogrammierung *Schuppert,* Governance und Rechtsetzung, 182 f., kritisch dazu *Habermas,* Faktizität und Geltung, 60, 212 f., 230 f. et passim; im Kontext der Polizei siehe etwa *Goeschel/Heyer/G. Schmidbauer,* Beiträge zu einer Soziologie der Polizei, 74 ff.

787 *Bäuerle* in *Möstl/Mühl* (Hrsg.), Beck'scher Online-Kommentar Polizei- und Ordnungsrecht Hessen, § 20 HSOG Rn. 40.

788 So auch *Bäuerle* in *Möstl/Mühl* (Hrsg.), Beck'scher Online-Kommentar Polizei- und Ordnungsrecht Hessen, § 20 HSOG Rn. 41.

b) Zweckänderung

Die mangelnde Bestimmtheit der Zweckbindung und die Zulässigkeit weitreichender Zweckänderungen[789] machen das verfassungsrechtliche Zweckbindungsprinzip zu einem normativen Luftschloss: Die gesetzlich gewünschte Zweckbindung gibt es tatsächlich kaum.[790]

Nichtsdestotrotz finden auch die im BKAG-Urteil konsolidierten verfassungsrechtlichen Vorgaben für die Zweckänderung nunmehr Eingang in die Polizeigesetze. Vor allem das „Zentralparadigma des Sicherheits-Datenschutzverfassungsrechts",[791] der Grundsatz der hypothetischen Datenneuerhebung, erfordern gesetzgeberische Umsetzungshandlungen. Auch diese beschränken sich überwiegend darauf, die Verfassungsrechtsprechung in Paragraphenform zu gießen.[792] Von den verschiedenen Gesetzgebern ebenfalls zu beachten sind dabei die europarechtlichen Anforderungen an Zweckänderungen, die sich für die vorliegende Untersuchung aus Art. 4 Abs. 2, 3 JI-Richtlinie ergeben, wobei die Mitgliedstaaten strengere Anforderungen an die zweckändernde Verarbeitung stellen können, Art. 1 Abs. 3 JI-Richtlinie, was wohl auf die verfassungsrechtlichen Vorgaben zutrifft.

Vor dem Hintergrund der detaillierten verfassungsrechtlichen Vorgaben in diesem Bereich ist zweifelhaft,[793] ob diejenigen polizeilichen Zweckänderungsbefugnisse, die die Zweckänderung recht knapp dann erlauben, wenn die Polizei die in Frage stehenden Daten auch zu dem neuen Zweck hätte speichern und nutzen (also verarbeiten) können,[794] noch verfassungsgemäß sind. Sie müssten jedenfalls unter Berücksichtigung des Grundsatzes der hypothetischen Datenneuerhebung ausgelegt werden. Darüber hinaus

789 § 12 Abs. 2 BKAG, § 29 Abs. 1 S. 4 BPolG, § 15 Abs. 3 BW PolG, Art. 53 Abs. 2 S. 2 BayPAG, § 42 Abs. 2 S. 2 ASOG Bln, § 38 Abs. 1 S. 2 BbgPolG, § 36b Abs. 1 BremPolG, § 34 Abs. 2 PolDVG Hamburg, § 20 Abs. 2 HSOG, § 36 Abs. 2 SOG M-V, § 39 NPOG, § 23 Abs. 2 PolG NRW, § 50 Abs. 2 S. 2 RP POG, § 23 Abs, 2 SPolDVG, § 13b Abs. 2 SOG LSA, § 79 Abs. 2 SächsPVDG, § 188 Abs. 1 S. 2 LVwG SH. Die Zweckänderung ist in Thüringen, soweit ersichtlich, gestreckt über § 40 TPAG gergelt.

790 *Petri* in *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch, G. Rn. 855.

791 *Gärditz* Zeitschrift für das Gesamte Sicherheitsrecht 2017, 1, 3.

792 Vorschriften, die den Grundsatz der hypothetischen Datenneuerhebung inkorporieren sind § 12 Abs. 2 BKAG, § 15 BW PolG, § 20 Abs. 2 HSOG, § 36 Abs. 2 SOG M-V, § 23 Abs. 2 PolG NRW, § 51 Abs. 3 RP POG, § 23 Abs, 2 SPolDVG, § 13b Abs. 2 SOG LSA, § 79 Abs. 2 SächsPVDG, § 188a Abs. 2 LVwG SH.

793 Zum Problem der „Erdrosselung" des Gesetzgebers siehe *Gärditz* Zeitschrift für das Gesamte Sicherheitsrecht 2017, 1 (3).

794 Siehe dazu bereits Fn. 789.

fehlen jedoch auch oftmals sonstige, durch Verfassungs- und Europarecht determinierte Tatbestandsvoraussetzungen, wie die der Erforderlichkeit. Zentrale Rechtmäßigkeitsvoraussetzungen des Datenumgangs der Auslegungskompetenz der jeweiligen Rechtsanwender:innen anheimzustellen, ist in Anbetracht der Bedeutung des Rechts auf informationelle Selbstbestimmung sowie europarechtlicher Parallelgrundrechte kaum angemessen. Daher kann die Tauglichkeit der entsprechenden Rechtsgrundlagen in den Polizeigesetzen bezweifelt werden.[795] Neben der fehlenden Umsetzung des Grundsatzes der hypothetischen Datenneuerhebung verfehlen die jeweiligen Regelungen dementsprechend auch sonstige Vorgaben und sind daher dringend verfassungs- und europarechtskonform auszugestalten.

Allerdings ist auch die seit dem BKAG-Urteil vorherrschende Form der einfachgesetzlichen Formulierung von Zweckänderungsbefugnissen[796] nicht zufriedenstellend: Während einige der neuen Vorschriften ebenfalls keine Erforderlichkeitsvoraussetzung kennen,[797] besteht auch hier das Problem der wortlautgetreuen Übernahme der Verfassungsrechtsprechung. Die in erster Linie für den Gesetzgeber geltenden Anforderungen, die der Grundsatz der hypothetischen Datenneuerhebung aufwirft,[798] werden so ungefiltert an die Rechtsanwender durchgereicht. Mangels eines Beurteilungsmaßstabes für die vom Bundesverfassungsgericht geforderte Vergleichbarkeit der Schwere von Straftaten oder Gewichtigkeit von Rechtsgütern ist diese Verantwortungsverlagerung auf die einzelnen Polizeibeamt:innen unter Bestimmtheitsgesichtspunkten sowie mit Blick auf das Demokratieprinzip kritikwürdig.[799]

Insgesamt hat sich die polizeiliche Datenverarbeitung durch die Ausweitung der Zweckbindung durch die Möglichkeit der sogenannten zweckwahrenden Weiternutzung, weitreichender Ausnahmen vom Grundsatz der Zweckbindung durch Zweckänderungsbefugnisse in den Polizeigesetzen

795 So zu recht *Arzt* in *Möstl/Kugelmann* (Hrsg.), Beck'scher Online-Kommentar Polizei- und Ordnungsrecht Nordrhein-Westfalen, § 23 Rn. 7 f. mwN.

796 Siehe dazu Fn. 792.

797 Eine Ausnahme ist etwa die Hessische Regelung, die allerdings so verschachtelt aufgebaut ist, dass ihre praktischen Anwendung nichtsdestotrotz herausfordernd ist, vgl. *Bäuerle* in *Möstl/Mühl* (Hrsg.), Beck'scher Online-Kommentar Polizei- und Ordnungsrecht Hessen, § 20 HSOG Rn. 10 ff.

798 Siehe dazu bereits Fn. 784.

799 So – bis auf die Bedenken hinsichtlich des Demokratieprinzips – auch *Arzt* in *Möstl/Kugelmann* (Hrsg.), Beck'scher Online-Kommentar Polizei- und Ordnungsrecht Nordrhein-Westfalen, § 23 Rn. 31.

und die mangelnde Ausgestaltung dieser Befugnisse in eine nur noch lose mit dem Rechtssystem und seinen materiellen Vorgaben gekoppelte Sphäre verschoben. Mangels klarer normativer Vorgaben wird vor allem auch die Kontrolle durch Gerichte und Datenschutzbehörden schwieriger.[800] Diese Loslösung von einem das exekutive Handeln direkt steuernden Programm, das auch durch subjektiven Rechtsschutz einforderbar ist, lässt sich nach Vorstellung des Bundesverfassungsgerichts indessen durch aufsichtliche Kontrolle und Implementierung von Transparenzanforderungen in der behördlichen Praxis gegenüber der Öffentlichkeit kompensieren.[801]

Die verblassende Normwirkung des Zweckbindungspostulats wird auch an der gesetzgeberisch ermöglichten Nutzung von sogenannten doppelfunktionalen Maßnahmen durch die Polizei sichtbar. Will die strafverfolgende Polizei Maßnahmen zur Informationserlangung einsetzen, die sie nach Strafverfahrensrecht nicht oder nur mit erhöhten Anforderungen vornehmen könnte, so kann auch die entsprechende polizeirechtliche Gefahrenabwehrmaßnahme ergriffen und die erlangten Daten dann zweckändernd ins Strafverfahren überführt werden.[802] Die Bedeutung der rechtlichen Vorgaben verschiebt sich auf diese Weise immer mehr von einem wertegebundenem Verhaltensrahmen hin zu instrumentalisierbaren „Werkzeugkästen".[803]

c) Erforderlichkeit und Verhältnismäßigkeit

Bedeutsam im einfachgesetzlichen polizeilichen Datenverarbeitungsrecht ist neben dem Grundsatz der Zweckbindung auch der Begriff der Erforderlichkeit, der sowohl für gefahrabwehrrechtliche als auch für strafverfahrensrechtliche Zwecksetzungen gilt. Neben dem Verfassungsrecht verlangt dies nunmehr auch das Unionsrecht. Art. 4 Abs. 1 lit. c JI-Richtlinie fordert unter anderem, dass die Datenverarbeitung in Bezug auf den Verarbeitungszweck nicht übermäßig sein darf. Hieraus ergibt sich das Gebot der Datenminimierung. Die Zahl der verarbeiteten Daten und die Zahl der

800 *Arzt* in *Möstl/Kugelmann* (Hrsg.), Beck'scher Online-Kommentar Polizei- und Ordnungsrecht Nordrhein-Westfalen, § 23 Rn. 33.
801 BVerfGE 141, 220 (281) – Bundeskriminalamtgesetz.
802 Siehe dazu *Müller/Schwabenbauer* in *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch des Polizeirechts, G. Rn 580.
803 *Bäcker* in *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch des Polizeirechts, D. Rn. 314.

Datenverarbeitungsvorgänge ist demnach auf das geringstmögliche Maß zu beschränken.[804] Auch soll das Erforderlichkeitsprinzip einer Sammlung von Daten auf Vorrat zu unbestimmten oder zu noch nicht bestimmten Zwecken einen Riegel vorschieben.[805] Besonders virulent wird die Erforderlichkeit im Bereich der Datenverarbeitung von Nichtbeschuldigten und unverdächtigen Personen. Datenverarbeitungen, die diese Personen betreffen, sind überhaupt nur unter strikten Voraussetzungen möglich; insbesondere bedarf es tatsächlicher Anhaltspunkte, dass die Datenverarbeitungen zur polizeilichen Aufgabenerfüllung nötig sind.[806]

Vor diesem Hintergrund ist bedenklich, wenn die Erforderlichkeit nicht als Tatbestandsvoraussetzung für die normierte Datenverarbeitungshandlung gesetzlich vorgesehen ist.[807] In Anbetracht der verfassungs- und unionsrechtlichen Bedeutung dieses Prinzips erscheint es zumindest zweifelhaft, ob die jeweiligen Normen taugliche Rechtsgrundlage für die mit ihnen beabsichtigten Datenverarbeitungsakte sein können.[808] Insofern wird man die Erforderlichkeit als ungeschriebenes Tatbestandsmerkmal in die entsprechenden Normen hineinzulesen haben, wobei diese Lösung insbesondere mit Blick auf die strukturierende Funktion der Vorschriften für die Praxis des polizeilichen Datenumgangs äußerst unbefriedigend ist.

Für die polizeiliche Datenpraxis ist zudem auch die einfachgesetzliche Nennung und Ausgestaltung des Verhältnismäßigkeitsgrundsatzes zentral. Neben seiner Bedeutung für die Dogmatik des Zweckbindungsgrundsatzes ist er zudem stets in der konkreten Rechtsanwendung zu beachten. Ein Datenverarbeitungsvorgang muss der Erfüllung seines Zwecks in geeigneter und erforderlicher Weise dienen und darf die betroffene Person nicht unangemessen beeinträchtigen. Die polizeilichen Sachbearbeiter:innen haben somit einzelfallbezogen die Eignung zu prüfen und potenzielle Alternativen zu berücksichtigen. Dabei ist auch eine Güterabwägung durchzuführen, in der die Eingriffsintensität mit dem verfolgten Zweck kontrastiert wird. Die Bestimmung der Eingriffsintensität ist ein komplexer Vorgang, in dem beispielsweise anhand einer Analyse der verwendeten Daten oder Datenverarbeitungsinstrumente die Tiefe der Privatheitsbeeinträchtigung bestimmt

804 *Braun* in *Gola/Heckmann/Klug* ua, BDSG, § 47 Rn. 21.
805 BVerfGE 125, 260 (321) – Vorratsdatenspeicherung m.w.N.
806 *Petri* in *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch, G. Rn. 863.
807 Soweit ersichtlich nur § 23 PolG NRW, der lediglich für die Speicherung Erforderlichkeit fordert.
808 Ablehnend *Arzt* in *Möstl/Kugelmann* (Hrsg.), Beck'scher Online-Kommentar Polizei- und Ordnungsrecht Nordrhein-Westfalen, § 23 PolG NRW Rn. 8.

werden muss.[809] Inwiefern diese fordernden Ansprüche der Rechtsordnung in der polizeilichen Praxis – vom Streifenbeamten bis zur Datenanalystin – beachtet werden (können), ist eine offene Frage.

d) Unional determinierte Verarbeitungsprinzipien

Mit der Umsetzung der JI-Richtlinie im Bundes- und den Landesdatenschutzgesetzen sind auch die unional vorgegebenen Verarbeitungsprinzipien greifbarer für die Rechtsanwendungsebene geworden, wenngleich sie wegen ihrer teilweisen Neuartigkeit noch nicht denselben Beachtungsgrad haben dürften wie die drei vorgenannten Grundsätze – zumal schon deren Beachtung in der polizeilichen Praxis als nicht (umfassend) gesichert gelten darf.

Neu, zumindest in dieser expliziten Form, ist der Grundsatz der Rechtmäßigkeit in § 47 Nr. 1 Alt. 1 BDSG, der allerdings nichts an der bisherigen Praxis der Verwendung von rechtswidrig erhobenen Daten in Polizei- und Strafverfahrensrecht ändern soll.[810] Theoretisch weitreichende Bedeutung für die Praxis der polizeilichen Informationsverarbeitung hat der Grundsatz der sachlichen Richtigkeit und Aktualität aus § 47 Nr. 4 BDSG. Ob und wie die Polizeien die damit verbundenen Aufwände werden bewältigen können, wird wesentlich über die generelle Qualität und Effektivität des polizeilichen Informationswesens sowie seine Akzeptanz entscheiden. So hat der Fall Amad A. in erschreckender Weise vergegenwärtigt, dass ein nachlässiger Informationsumgang im Extremfall tödlich sein kann: Amad A. war aufgrund einer in ihren Ursachen nicht ganz klaren Verwechslung auf Grundlage von Informationen in polizeilichen Datenbanken inhaftiert worden, wo er unter ungeklärten Umständen in seiner Zelle infolge eines Brands verstarb.[811] Noch expliziter als zuvor im Verfassungsrecht ist nunmehr auch der Grundsatz der Datensicherheit im nationalen Recht festgeschrieben, § 47 Nr. 6 BDSG. Da mit steigender Aussagekraft der gespeicherten Daten die ökonomischen Erwägungen als eine gegenüber der

809 *Müller/Schwabenbauer* in *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch des Polizeirechts, G. Rn. 601 f.
810 *Müller/Schwabenbauer* in *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch des Polizeirechts, G. Rn. 596.
811 *Golla*, Der virtuelle Mr. Hyde, 2019.

Datensicherheit zu beachtende Größe in ihrer Bedeutung abnimmt,[812] ist die technologische Fortentwicklung des Informationswesens, die auch eine bessere Nutzbarkeit der Daten mit sich bringt, zunehmend technisch abzusichern. Bisher fehlt auf Ebene des BDSG die Rechenschaftspflicht der für die Datenverarbeitung Verantwortlichen. Da diese dazu verpflichtet, die Einhaltung der Datenschutzgrundsätze laufend nachzuweisen, ist ihre Auslassung im Gesetz mit Blick auf den Aufbau eines internen Datenschutzkontrollsystems problematisch. Zwar lässt sich insoweit die JI-Richtlinie direkt heranziehen, aber der Gesetzgeber unterlässt es auf diese Weise, mittels normativer Leitsterne den Grundstein für eine Kultur der internen Kontrolle als Grundlage für die nach außen zu leistende Rechenschaft zu legen. Eine solche Signalwirkung für die interne Polizeikultur wäre indessen neben dem Ausbau der technischen, organisatorischen und institutionellen Grundlagen für ein internes Datenschutzkontrollregime angezeigt.[813]

II. Normative Verankerungen der Infrastruktur des polizeilichen Informationswesens

Nähert man sich ausgehend von dieser Terminologie und den einfachgesetzlichen Verarbeitungsprinzipien nun den Strukturen und Praktiken, die das polizeiliche Informationswesen ausmachen, so drängt sich zunächst die Frage nach der technischen Infrastruktur der deutschen Polizeien auf. Einen Zugang hierzu bekommt man jedoch nicht „von oben" oder „unten" und auch nicht „vom Anfang" oder gar „Ende", sondern gewissermaßen über die „Mitte". Stellt man sich die polizeiliche Datenverarbeitung als Netzwerk der verschiedenen deutschen Polizeibehörden vor, so ist das Bundeskriminalamt zentraler Knotenpunkt in diesem. Seine Bedeutung innerhalb der deutschen Polizeilandschaft hat in den letzten Jahrzehnten kontinuierlich zugenommen,[814] eine Entwicklung, die auch mit Blick auf die laufende Umgestaltung der polizeilichen Datenbank-Strukturen nicht abgeschlossen zu sein scheint.[815]

812 BVerfGE 125, 260 (326) – Vorratsdatenspeicherung.

813 Siehe näher dazu unten S. 361 ff. sowie S. 536 ff.

814 Siehe dazu etwa *Abbühl,* Der Aufgabenwandel des Bundeskriminalamtes.

815 Im Jahr 2016 hat das BKA seine Zentralstellen-Funktion nach Angaben des BMI aufgrund einer „heterogenen" IT-Verbundarchitektur – gemeint sind in erster Linie zu viele dezentrale Datenbanken mit unzureichend aufeinander abgestimmten Schnittstellen - nur unzureichend ausfüllen können: So waren von 151.000 Woh-

Um die Bedeutung des Bundeskriminalamtes für die polizeiliche Datenverarbeitung zu verdeutlichen, ist in einem ersten Schritt zunächst auf die rechtliche Rahmung der Behörde und insbesondere ihre Zentralstellen-Funktion gem. § 2 BKAG einzugehen, um dann darauf aufbauend die vom Bundeskriminalamt institutionell getragenen, aber auch wesentlich durch die anderen deutschen Polizeibehörden mitgeprägten Infrastrukturen des polizeilichen Informationswesens darzustellen.

I. Die Zentralstellenfunktion des Bundeskriminalamts

Das Bundeskriminalamt unterstützt gem. § 2 BKAG als Zentralstelle für das polizeiliche Auskunfts- und Nachrichtenwesen und für die Kriminalpolizei die Polizeien des Bundes und der Länder bei der Verhütung von Straftaten mit länderübergreifender, internationaler oder erheblicher Bedeutung. Damit werden dem Bundeskriminalamt die in Art. 87 Abs. 1 S. 2 GG genannten Aufgaben zugewiesen. Die zuletzt 2018 novellierte Regelung des § 2 BKAG zielt in seiner neuen Form insbesondere auch darauf ab, dem Bundeskriminalamt die erforderlichen Koordinierungs- und Unterstützungsaufgaben hinsichtlich der Polizeien von Bund und Ländern in adäquater Weise möglich zu machen.[816]

a) Verfassungsrechtlicher Inhalt des Zentralstellenbegriffes

Der Begriff der Zentralstelle stammt aus dem Verfassungsrecht, er wird dort aber lediglich einmal, in der eben genannten Vorschrift des Grundgesetztes, erwähnt. Die bereits 1985 von *Ahlf* konstatierte mangelhafte „wissenschaftlich-analytische Durchdringung der Zentralstellenfunktion des BKA“[817] ist bis heute nicht befriedigend geleistet worden. Weder für den Begriff der Zentralstelle noch für den der Zusammenarbeit gem. Art. 87 Abs. 1 S. 2 GG hat sich bisher eine allgemein anerkannte Interpretation durchsetzen können.[818] Einigkeit besteht indessen bezüglich der folgenden Aspekte des verfassungsrechtlichen Zentralstellenbegriffs: Zunächst ist der

---

nungseinbruchsdiebstählen im Jahr 2016 nur 2.100 zentral beim BKA erfasst, vgl. zum Ganzen Bundesministerium des Inneren, Polizei 2020 White Paper, S. 4f.

816 *Graulich* in *Schenke/Graulich/Ruthig,* Sicherheitsrecht, § 2 BKAG Rn. 1.

817 *Ahlf,* Bundeskriminalamt, S. 2.

818 *Graulich* in *Schenke/Graulich/Ruthig,* Sicherheitsrecht, § 2 BKAG Rn. 3.

Zentralstellenbegriff ausschließlich für Bundesbehörden reserviert, wie es sich insbesondere aus dem Systemzusammenhang des Art. 87 Abs. 1 S. 2 GG ergibt. Gegen die naheliegende Bezeichnung der Landeskriminalämter als Zentralstellen auf Landesebene hat sich der Bundesgesetzgeber mit der klaren Formulierung des § 1 Abs. 2 BKAG (§ 3 Abs. 1 S. 1 BKAG a.F.) bewusst entschieden.[819] Wie Bundesoberbehörden verfügen Zentralstellen nicht über einen eigenen Verwaltungsunterbau. Allerdings besitzt die Zentralstelle nicht die vollständige Kompetenz im ihr zugeordneten Aufgabenbereich, das heißt, sie nimmt nicht allein die zugewiesenen Aufgaben wahr. Vielmehr verbleiben auch den Ländern Reste an Verwaltungszuständigkeit.[820] Gerade diese Selbstständigkeit soll der Zentralstellenbegriff wohl ermöglichen. Während der Begriff der „bundeseigenen Verwaltung" in Art. 87 Abs. 1 S. 1 GG nach dem Prinzip der geteilten Verwaltungsräume bei gesetzlicher Einführung einer solchen eine Länderverwaltung auf demselben Gebiet vollständig verdrängt,[821] ermöglicht die Form der Zentralstelle eine „weiche Verknüpfung der Kriminalpolizeien des Bundes und derjenigen der Länder."[822] Insofern lässt sich von einer abgeschwächten Durchbrechung des verfassungsrechtlichen Verbots der Mischverwaltung sprechen.[823] Fraglich bleibt indessen, welche Kompetenzen nun tatsächlich inhaltlich dem Bund in diesem Bereich zugeordnet sind. Klarheit besteht insofern nur bezüglich der informationellen Verklammerung und Koordinierung der Landespolizeibehörden durch die als Zentralstelle eingerichtete Bundesbehörde – also das Bundeskriminalamt – in den Bereichen der Kriminalpolizei und des internationalen Verkehrs. Zudem ist unumstritten, dass die Länder durch die Einrichtung des Bundeskriminalamtes ihre Verwaltungszuständigkeit im Sicherheitsbereich nicht eingebüßt haben.[824]

b) Der Zentralstellenbegriff aus § 2 Abs. 1 BKAG

Von Interesse ist darüber hinaus der einfachgesetzliche Zentralstellenbegriff in der Prägung, die er durch das BKAG erfährt. Für die Zwecke der vorliegenden Untersuchung sind dabei insbesondere diejenigen Aspekte der

819 *Ahlf,* Bundeskriminalamt, S. 53.
820 *Hermes* in *H. Dreier,* Grundgesetz, Art. 87, Rn. 47.
821 *Graulich* in *Schenke/Graulich/Ruthig,* Sicherheitsrecht, § 2 BKAG Rn. 3.
822 *Graulich* in *Schenke/Graulich/Ruthig,* Sicherheitsrecht, § 2 BKAG Rn. 3.
823 *Ahlf,* Bundeskriminalamt, S. 31 spricht insoweit von „legaler Mischverwaltung".
824 *Graulich* in *Schenke/Graulich/Ruthig,* Sicherheitsrecht, § 2 BKAG Rn. 3.

Zentralstellenfunktion des Bundeskriminalamtes relevant, die einen Bezug zur Informationsverarbeitung aufweisen.

Das BKAG nennt diesbezüglich zunächst in § 2 Abs. 1 „das polizeiliche Auskunfts- und Nachrichtenwesen". Gegenständlich erfasst werden damit gefahrenabwehr- und strafverfolgungsrelevante Daten sowie ihre Sammlung, Auswertung und Weitergabe.[825] Dabei sollen diese polizeilichen Aufgaben nicht auf das Bundeskriminalamt übertragen, sondern dort koordiniert und informationell verklammert werden, um anderen Polizeibehörden einen effektiven Umgang mit derartigen Informationen zu ermöglichen. Es lässt sich vor diesem Hintergrund auch von einer „Servicefunktion" des Bundeskriminalamtes sprechen. [826] *Ahlf* beschreibt den „typischen Ablauf" im Rahmen dieser „eigentlichen Zentralstellenaufgabe" für die achtziger Jahre, aber prinzipiell wohl immer noch gültig, folgendermaßen:

> „Eine Basiseinheit benötigt bei ihrer konkreten Ermittlungsarbeit eine Information, die überregionalen Bezug hat, so daß die landeseigenen Nachrichtenzentralen, die Zentralstellen im weiten, kriminalistischen Sinne [gemeint sind hier wohl die Landeskriminalämter FB], über diese Information nicht verfügen. Derartige Informationen sind allerdings beim BKA als Zentralstelle vorhanden, weil dieselben durch die Polizeidienststellen der Länder […] zugeleitet worden sind. Das BKA erteilt nun als Zentralstelle die erwünschte Auskunft. Entweder auf den traditionellen Wegen […] oder auf elektronischem Wege."[827]

In seiner Funktion als Zentralstelle für das polizeiliche Auskunfts- und Nachrichtenwesen fehlt es dem Bundeskriminalamt indessen – abgesehen von der eingeschränkten Befugnis des § 9 Abs. 1 BKAG – grundsätzlich an Exekutivbefugnissen zur eigenen Erhebung personenbezogener Daten in Fällen, in denen der eigene Informationsbestand das gegebenenfalls indizieren würde.[828] Allerdings verfügt das Amt in seiner Funktion als Strafverfolgungs- und Gefahrenabwehrbehörde mitunter über weitreichende Erhebungsbefugnisse.

Zudem ist das Bundeskriminalamt der Knotenpunkt für die internationale polizeiliche Zusammenarbeit – insbesondere mit Interpol und Europol. In dieser Funktion kann das Bundeskriminalamt Daten aus dem

825 *Hermes* in *H. Dreier,* Grundgesetz, Art. 87, Rn. 50.
826 *Bäcker,* Terrorismusabwehr, S. 23.
827 *Ahlf,* Bundeskriminalamt, S. 409.
828 Ausführlicher hierzu siehe *Barczak* in *Barczak* (Hrsg.), BKAG, § 2 Rn. 6 ff.

Ausland anfordern und auf Anforderungen aus dem Ausland reagieren.[829] Insgesamt ist die Zentralstellenfunktion des Bundeskriminalamtes im Laufe der Jahre immer relevanter geworden.[830] Neben einer Gesetzesnovellierung von 1997, die die informationellen Regelungen erweitertet hat,[831] sieht *Bäcker* den Grund hierfür insbesondere im Wandel des polizeilichen Aufgabenprofils, das heute neben Strafverfolgung und Gefahrenabwehr in konkreten Fällen vor allem auch übergreifende Präventionsmaßnahmen beinhaltet, die regelmäßig eine möglichst breiten Informationsbasis benötigen. Daneben sind auch Fortschritte in der Informationstechnologie ausschlaggebend: Daten können sehr leicht aus ihren bisherigen Kontexten gelöst und für neue Zwecke mit anderen Daten kombiniert werden. Wegen der Erfahrung des Bundeskriminalamtes bei der Wahrnehmung zentraler informationeller Aufgaben und der bereits vorhandenen Technik, lag und liegt es weiterhin nahe, die Behörde mit der Erfüllung dieses neuen Aufgabenprofils (zumindest mit) zu betrauen.[832]

c) Formen der Ausübung der Zentralstellenfunktion aus § 2 BKAG

Die Essenz der Zentralstellenfunktion des Bundeskriminalamts ist der in § 2 Abs. 3 BKAG geregelte „polizeiliche Informationsverbund", also eine Vernetzung innerhalb der Sicherheitsarchitektur,[833] zu dessen Unterhaltung die Norm das Bundeskriminalamt verpflichtet und berechtigt. Dieses Verbundsystem ist ein Kernstück der alten wie neuen IT-Architektur des Bundeskriminalamtes.[834] Die genauere Ausgestaltung des nur losen normativen Programms des § 2 Abs. 3 BKAG erfolgt über das Gesetz verteilt und wird aufgrund seiner integralen Bedeutung im Anschluss dargestellt.[835]

In diesem Kontext ebenfalls von Bedeutung ist die Unterhaltung zentraler Einrichtungen und Sammlungen nach § 2 Abs. 4 BKAG, die gemäß Satz 2 der Norm elektronisch geführt werden können, was heute auch über-

829 *Bäcker,* Terrorismusabwehr, S. 23.
830 *Barczak* in *Barczak* (Hrsg.), BKAG, § 2 Rn. 3.
831 BGBL. I 1997, S. 1650.
832 *Bäcker,* Terrorismusabwehr, 24 f.
833 *Barczak* in *Barczak* (Hrsg.), BKAG, § 2 Rn. 9.
834 *Graulich* in *Schenke/Graulich/Ruthig,* Sicherheitsrecht, § 29 BKAG Rn. 4.
835 Siehe dazu unten S. 226 ff.

wiegend der Fall ist.[836] Für die zentralen – also erkennungsdienstlichen sowie die Fahndung nach Personen und Sachen betreffenden – Einrichtungen und Sammlungen gilt nicht die Einschränkung, dass es um Straftaten mit länderübergreifender und internationaler oder erheblicher Bedeutung gehen muss.[837] Tätigkeiten in diesem Bereich der Zentralstellenfunktion des Bundeskriminalamtes umfassen unter anderem die Koordinierung der Polizeien des Bundes und der Länder, die Bereitstellung von Personen und Sachen sowie „kreative Mitgestaltung i.S.v. informationeller Mitwirkung und Förderung eines konkreten Ermittlungsverfahrens einer Polizeibehörde" etwa in Form von Analysen und Auswertungen.[838] Die zentralen Einrichtungen und Sammlungen sind integrale Bestandteile des polizeilichen Informationswesens, gestalten es also näher inhaltlich aus.

Neben diesen strukturellen Vorgaben erfolgt die Wahrnehmung der Zentralstellenaufgaben des Bundeskriminalamtes gem. § 2 Abs. 2 BKAG in praktischer Hinsicht durch die Sammlung und Auswertung aller hierfür erforderlichen Informationen (Nr. 1) und die unverzügliche Unterrichtung der Strafverfolgungsbehörden des Bundes und der Länder über die sie betreffenden Informationen und die in Erfahrung gebrachten Zusammenhänge von Straftaten (Nr. 2).

Erfasst werden dabei Informationen jeder Art, unabhängig von dem Medium der technischen Übermittlung. Neben verkörperten Informationen (etwa Akten oder Ähnliches) sind insbesondere auch mittels elektronischer Datenverarbeitung übermittelte Informationen gemeint.[839] Inhaltlich geht es vor allem um Informationen, die für eine zentrale Auswertung zur Verhütung und Verfolgung von Straftaten mit erheblicher Bedeutung geeignet und erforderlich sind.[840] „Hierzu", so heißt es in der Gesetzesbegründung, „zählen auch Informationen, die als solche noch nicht von länderübergreifender und internationaler oder erheblicher Bedeutung sind. Es reicht aus, daß sie im Zusammenhang mit anderen Informationen der Zentralstelle diese Qualität erreichen können."[841] Damit wird die inhaltliche Begrenzung der Übermittlungsmöglichkeiten in nicht unerheblicher Weise abge-

836 *Graulich* in *Schenke/Graulich/Ruthig,* Sicherheitsrecht, § 2 BKAG Rn. 41; *Barczak* in *Barczak* (Hrsg.), BKAG, § 2 Rn. 61.
837 *Graulich* in *Schenke/Graulich/Ruthig,* Sicherheitsrecht, § 2 BKAG Rn. 37.
838 *Graulich* in *Schenke/Graulich/Ruthig,* Sicherheitsrecht, § 2 BKAG Rn. 37f.
839 *Ahlf,* Bundeskriminalamt, S. 294.
840 Zu den sonstigen Informationen siehe *Graulich* in *Schenke/Graulich/Ruthig,* Sicherheitsrecht, § 2 BKAG Rn. 32.
841 BT-Drs. 13/1550, S. 21.

schwächt, da sich argumentieren ließe, dass zu übermittelnde Daten erst durch Kombination mit den Informationsbeständen der Zentralstelle eine entsprechende Bedeutung erlangen werden, zumal die Bestimmung unter die polizeiliche Deutungsmacht fällt und nur begrenzt einer rechtlichen Überprüfung offensteht.

Der Begriff des „Sammelns" ist in seinem Gehalt etwas ambivalent: Neben der passiven Entgegennahme fremderhobener Informationen, etwa durch die Landeskriminalämter, also dem sogenannten „passiven Sammeln" könnte auch das „aktive Sammeln", also die Erhebung von Informationen aufgrund eigeninitiativer (exekutiver) Maßnahmen, erfasst sein.[842] Das Amt ist für die Koordination im polizeilichen Informationsverbund zuständig und grundsätzlich kein exekutives Ermittlungsorgan.[843] Zwar dürfte nach wie vor als Konsens gelten, dass mit dem Bundeskriminalamt gerade keine große Behörde zur bundesweiten Informationsbeschaffung kreiert werden sollte.[844] Ob allerdings seine Informations*verarbeitungs*funktion nach wie vor die allein dominierende im bundeskriminalamtlichen Aufgabenspektrum ist, darf bezweifelt werden. Vor dem Hintergrund der durchaus weitreichenden Datenverarbeitungsbefugnisse, die an die §§ 4, 5 BKAG geknüpft sind, erscheint das alte Konzept vom Bundeskriminalamt zunehmend in Richtung der Idee einer aktiveren, im klassischen Sinne polizeilich agierenden, Behörde verschoben zu haben, die sich zusätzlich aber durch eine starke Informationsmacht auszeichnet.

Insofern muss dem Begriff des „Sammelns" auch ein aktiver Gehalt zugeschrieben werden. So soll „Sammeln" in der Funktion des Bundeskriminalamtes als Zentralstelle auch in begrenztem Rahmen die aktive Informationsbeschaffung insoweit erlauben, wie es im Befugnisteil geregelt ist.[845] Diese, einer Gesetzesbegründung von 1995 entnommene, Interpretation des „Sammeln"-Begriffes nimmt auf den inzwischen geänderten § 7 Abs. BKAG Bezug, der die Erhebung von personenbezogenen Daten bei den Polizeien des Bundes und der Länder sowie bei anderen öffentlichen und nicht-öffentlichen Stellen regelte.[846] Die Norm ist vor allem im neugeschaffenen § 9 BKAG aufgegangen. Mit Blick auf die zusätzlichen Befugnisse im Rahmen der Strafverfolgung (§§ 34 ff. BKAG) und insbesondere zur

842 *Ahlf,* Bundeskriminalamt, S. 310.
843 *Graulich* in *Schenke/Graulich/Ruthig,* Sicherheitsrecht, § 2 BKAG Rn. 33.
844 *Ahlf,* Bundeskriminalamt, S. 313.
845 BT-Drs. 13/1550, S. 21f.
846 BT-Drs. 13/1550, S. 7.

Abwehr von Gefahren des internationalen Terrorismus (§§ 38 ff. BKAG) ist allerdings von einer untergeordneten Rolle des aktiven Sammelns von Informationen im Aufgabenspektrum des Amts kaum mehr zu sprechen, wobei nicht ganz klar ist, wie Daten aus diesen Maßnahmen in die Erfüllung der Zentralstellenfunktion hineinspielen. Insgesamt bedeutet „Sammeln" i.S.d. § 2 Abs. 2 BKAG zumindest die Entgegennahme von fremderhobenen Informationen und ihre systematische Aufbewahrung.[847] Der aktive Gehalt des Begriffes umfasst indessen nur die Erhebung von Informationen zur Ergänzung bereits vorhandener Sachverhalte oder sonst zu Zwecken der Auswertung mittels Auskünften oder Anfragen bei öffentlichen und nichtöffentlichen Stellen, soweit dies zur Erfüllung der Zentralstellenaufgabe aus § 2 Abs. 1 BKAG erforderlich ist.[848]

In seinem Begriffsgehalt klarer ist dagegen der Begriff des „Auswertens". Es handelt sich um ein „analytisch-intellektuelles" Verfahren, d.h. eine Bewertung und Interpretation von beim Bundeskriminalamt (oder den Landeskriminalämtern[849]) vorhandenen Informationen, bei dem „die anfallenden Informationen nach kriminalistischen Gesichtspunkten sortiert und verglichen werden müssen, um ihre Bedeutung und ihren Informationswert für die Verbrechensbekämpfung intensiv auszuloten."[850] Dabei können die Bedeutung und Informationswert auch nur marginale Relevanz haben.[851]

Zusätzlich wird die Zentralstellenfunktion des Bundeskriminalamtes noch durch die Unterrichtung der Strafverfolgungsbehörden wahrgenommen. Strafverfolgungsbehörden im Sinne des § 2 Abs. 2 Nr. 2 BKAG sind entsprechend der Aufgabenstellung des Bundeskriminalamtes Staatsanwaltschaft und Polizei, wobei eine Pflicht zur Unterrichtung der Staatsanwaltschaft nur dann besteht, wenn das Bundeskriminalamt bereits in Erfahrung bringen konnte, welche Staatsanwaltschaft die Ermittlungen leitet. Häufiger wird vermutlich die zuständige Polizeibehörde bekannt sein, sodass es seltener einen Informationsfluss zur Staatsanwaltschaft geben dürfte. Dementsprechend hat das Amt nur spezielle Erkenntnisse über bestimmte Täter

847 *Ahlf,* Bundeskriminalamt, S. 314.
848 *Graulich* in *Schenke/Graulich/Ruthig,* Sicherheitsrecht, § 2 BKAG Rn. 33; *Barczak* in *Barczak* (Hrsg.), BKAG, § 2 Rn. 42.
849 *Graulich* in *Schenke/Graulich/Ruthig,* Sicherheitsrecht, § 2 BKAG Rn. 34.
850 *Hessel* zitiert nach *Ahlf,* Bundeskriminalamt, S. 316.
851 *Graulich* in *Schenke/Graulich/Ruthig,* Sicherheitsrecht, § 2 BKAG Rn. 34 spricht insofern von einer Relevanz „auch nur als Mosaikstein".

und Taten zu übermitteln, nicht dagegen „bloße Routinenachrichten" und „massenstatistisches Material".[852]

Die Zentralstellenfunktion des Bundeskriminalamts verändert sich hingegen nicht bloß durch den Wandel der Aufgaben der Behörde, sondern auch ganz unmittelbar. So hat § 2 Abs. 5 BKAG, der ursprünglich nur die Unterstützung der Polizeien der Länder durch das Bundeskriminalamt bei der Datenverarbeitung regelt, infolge der Novellierung des BKAG Änderungen erfahren. Ziel dieser Neuerungen war, das Bundeskriminalamt nach dem Vorbild Europols umzugestalten, also insbesondere seine Stellung als zentraler Dienstleister der Polizeien des Bundes und der Länder auszubauen.[853] Für die hier untersuchten Bereiche des polizeilichen Informationswesens sind vor allem § 2 Abs. 5 S. 1 Nr. 4 und § 2 Abs. 5 S. 2 BKAG erwähnenswert: Satz 1 Nr. 4, der weiterhin die Unterstützung der Länder bei der Datenverarbeitung regelt, ist etwas Selbstverständliches für elektronische Informationsverbünde, da solche Abstimmung und Kooperation erfordern. Die Zentralstelle bestimmt dabei prinzipiell die technischen Standards an denen sich die Bundesländer dann zu orientieren haben.[854] Satz 2 der Vorschrift gestattet schließlich in ausgewählten Fällen (§ 2 Abs. 5 Satz 1 Nr. 3 und 4 BKAG) eine Auftragsverarbeitung personenbezogener Daten durch das Bundeskriminalamt. Dabei sieht sich die Regelung Kritik ausgesetzt: Im Rahmen der Auftragsverarbeitung erfolgt keine Datenübermittlung, sondern nur eine Weitergabe der Daten (Art. 9 DSRL-JI; § 62 BDSG 2017/2018). Es werden von Seiten des Verantwortlichen Verarbeitungsaufgaben an den Auftragsverarbeiter delegiert, der die dabei übertragenen Daten in der Regel nur im Rahmen der Weisungen des Verantwortlichen verwenden darf (Art. 23 DSRL-JI). Bedenklich ist es insoweit, wenn das Bundeskriminalamt eine solche Auftragsverarbeitung für Länderpolizeien betreibt und davon Daten erfasst werden, die aus verfassungsrechtlichen Gründen nur auf Länderebene verarbeitet werden dürfen. Solche nicht bundesweit relevanten Daten können die von den jeweiligen Gesetzgebern festgelegte Aufgabenverteilung zwischen Bundes- und Länderpolizeien unter dem „Etikett der Auftragsverarbeitung" unterlaufen. *Petri* plädiert insofern dafür, § 2 Abs. 5 S. 2 BKAG Ausnahmecharakter zuzuerkennen.[855] Für *Barczak* kommt dieser Charakter schon dadurch zum Ausdruck, dass das BKA hier

852 *Graulich* in *Schenke/Graulich/Ruthig,* Sicherheitsrecht, § 2 BKAG Rn. 35.
853 BT-Drs. 18/11163, S. 85.
854 So *Graulich* in *Schenke/Graulich/Ruthig,* Sicherheitsrecht, § 2 BKAG Rn. 47.
855 *Petri* in *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch, G. Rn. 487f.

zum einen nicht eigeninitiativ, sondern nur auf ein entsprechendes Ersuchen und bei einer grundsätzlichen Pflicht zur Kostenerstattung hin tätig würde und sich zum anderen § 2 Abs. 5 S. 2 BKAG nach der ursprünglichen Intention des Normgebers von vorneherein auf Fälle beschränkt, in denen allein die Datenverarbeitungsanlagen und -anwendungen des BKA eine sachgerechte Verarbeitung der erhobenen Daten erwarten ließen.[856] Das mag zutreffen, nichtsdestotrotz begünstig diese normative Konstruktion eine weitere Aufwertung der informationellen Bedeutung und Kompetenzen des Bundeskriminalamts im polizeilichen Informationsverbund und forciert damit eine (weitere) Zentralisierung von Datenbeständen, wie es letztlich auch explizit als sicherheitspolitisches Projekt geplant ist.[857]

Schließlich hält auch Absatz 6 des § 2 BKAG für die vorliegende Untersuchung noch erwähnenswerte Aspekte bereit. Neben § 2 Abs. 6 Nr. 4 BKAG, der das Bundeskriminalamt verpflichtet, die technischen und organisatorischen Vorkehrungen zur Erfüllung der Datenschutzgrundsätzen zu treffen, ist vor allem Nr. 1 der Vorschrift von Bedeutung. Die Erstellung von strategischen und operativen kriminalpolizeilichen Analysen, Statistiken und Lageberichten sowie die dafür erforderliche Beobachtung und Auswertung der Kriminalität sind stark auf Datensammlungen und -verarbeitungen angewiesen. Es geht dabei vorrangig um die Identifizierung von Kriminalitätsphänomenen aller Art, um so insbesondere die Verhütung künftiger Straftaten zu ermöglichen.[858] Ein wesentlicher Teil der Zentralstellenaufgabe bezieht sich auf die allgemeine Auswertung und Analyse der gesammelten Informationen in operativer und strategischer Hinsicht; nur so kann das „unverzichtbare Hintergrundwissen" generiert werden, das zur Aufschlüsselung und kriminalstrategischen Bearbeitung der unterschiedlichen Kriminalitätsfelder notwendig ist. Dem Präsidenten des Bundeskriminalamtes, *Münch*, zufolge, gilt (auch) hier das Gebot, „aus bereits vorhandenen Daten die größtmögliche Aussagekraft für die polizeiliche Arbeit zu extrahieren und dieses Wissen mit anderen Polizei- und Sicherheitsbehörden zu teilen."[859] Vor dem Hintergrund des Massendatenparadigmas, nach dem vor allem schon bestehende große Datenbestände für noch granularere Einsichten angereichert werden sollen, ist anzunehmen, dass die zentrale

856 *Barczak* in *Barczak* (Hrsg.), BKAG, § 2 Rn. 73.
857 Siehe dazu unten S. 271 ff.
858 *Graulich* in *Schenke/Graulich/Ruthig,* Sicherheitsrecht, § 2 BKAG Rn. 52; *Barczak* in *Barczak* (Hrsg.), BKAG, § 2 Rn. 79.
859 *Münch*, A-Drs. 18(4)806 C S. 4.

Rolle des Bundeskriminalamtes im polizeilichen Informationswesen weiter an Bedeutung gewinnen wird.

2. Informationsverbund und Informationssysteme

Die tatsächlichen Strukturen des polizeilichen Informationswesens sind vor allem im BKAG auch teilweise rechtlich abgebildet. Mit der Novellierung des Gesetzes wurde hingegen, neben der Reaktion auf das BKAG-Urteil des Bundesverfassungsgerichts, auch die grundlegende Überarbeitung des Informationswesens angestoßen.[860] Die Entwicklung hin zu einem einheitlichen Verbundsystem mit zentraler Datenhaltung beim Bundeskriminalamt (sog. „gemeinsames Datenhaus der deutschen Polizei") ist weder technisch noch organisatorisch abgeschlossen.[861] Die folgenden Ausführungen sind daher nur eine Momentaufnahme in einem stark unter Wandlungsdruck stehenden System der polizeilichen Informationsverarbeitung. Nichtsdestotrotz scheinen mit der Neufassung des BKAG die normativen Rahmenbedingungen für die neue Informationsarchitektur auf mittelfristige Sicht gesetzt zu sein, da ein originärer gesetzgeberischer Wille für weitere Reformen gegenwärtig nicht vorhanden scheint. Insofern können die einschlägigen Vorschriften des BKAG als Grundlage für eine weitere Annäherung an das polizeiliche Informationswesen dienen. Zusätzlich werden hier im Zusammenhang mit den jeweiligen technischen Komponenten des Informationssystems rechtstatsächliche Aspekte dargestellt, weil sich nur über diese überhaupt die Bedeutung der jeweiligen Systeme, Dateien und so weiter erfassen lässt.

Wie bereits beschrieben trifft das Bundeskriminalamt im Rahmen der Zentralstellenfunktion aus § 2 Abs. 3 BKAG die Pflicht, einen einheitlichen polizeilichen Informationsverbund zu unterhalten. Diese Pflicht wird durch die §§ 29-31 BKAG näher ausgestaltet. An diesem Informationsverbund nimmt das Bundeskriminalamt wiederum gem. § 13 Abs. 1 BKAG mit seinem eigenen Informationssystem teil. Auch die übrigen Bundes- und Länderpolizeien unterhalten je eigene Informationssystemtypen für unterschiedliche polizeiliche Aufgabenfelder.

860 *Petri* in *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch, G, Rn. 390.
861 Bundesministerium des Inneren, Polizei 2020 White Paper, S. 2, 11.

a) Der gegenwärtige Wandel des polizeilichen Informationsverbundes

Hauptelement des einheitlichen polizeilichen Informationsverbundes ist INPOL, das „polizeiliche Informationssystem",[862] wobei es sich um das gemeinsame, arbeitsteilige, elektronische Informationsverbundsystem der Polizeien des Bundes und der Länder zur Unterstützung vollzugspolizeilicher Aufgaben handelt, in dem informationstechnische Einrichtungen des Bundes und der Länder in einem Verbund zusammenwirken.[863] Während INPOL im neuen Gesetz auf § 29 BKAG fußen sollte, wurden alle beim Bundeskriminalamt bestehenden Dateien,[864] die INPOL derzeit ausmachen, auf nicht mehr geltenden Rechtsgrundlagen errichtet,[865] die den neuen Anforderungen an den Grundsatz der hypothetischen Datenneuerhebung und den damit verbundene Kennzeichnungspflichten nicht entsprechen.[866]

Die in INPOL vorgehaltenen Datenbestände sind (gegenwärtig noch) überwiegend in Dateien und Verarbeitungssystemen organisiert.[867] Es gliedert sich in ein zentrales System, INPOL-Z, das den zentralen Datenbestand enthält, und die Teilnehmersysteme, INPOL-Bund bzw. INPOL-Land (die INPOL-Land-Systeme haben mitunter Eigennamen), mit denen die Daten abgerufen und eingegeben werden können.[868] Dies soll im Zuge des IT-Großprojekts *Polizei 2020* unter anderem stark modifiziert werden, indem ein gemeinsamer Datenbestand mit verschiedenen Zugriffsrechten geschaffen werden soll.[869] In der ursprünglichen Konzeption, die INPOL durch die Ständige Konferenz der Innenminister und -senatoren der Län-

862 *Graulich* in *Schenke/Graulich/Ruthig,* Sicherheitsrecht, § 29 BKAG Rn. 1.
863 BT-Drs. 13/1550, S. 28.
864 Unterschieden wird zwischen Amts- Zentral- und Verbunddateien. Verbunddateien sind solche Dateien im INPOL, in die die verschiedenen Teilnehmer in eigener Zuständigkeit dezentral Daten eingeben und abrufen können. Zentraldateien sind hingegen solche Dateien, die das Bundeskriminalamt führt und mit von anderen Polizeien im Rahmen seiner Zentralstellenfunktion angelieferten Daten befüllt, woraufhin diese Daten dann von beteiligten Stellen abgerufen werden können. Amtsdateien sind schließlich solche Dateien, die das Bundeskriminalamt zur Erfüllung der eigenen Aufgaben unterhält und worauf keine anderen Stellen Zugriff haben, siehe dazu Graulich in *Schenke/Graulich/Ruthig,* Sicherheitsrecht, § 13 BKAG Rn. 2 ff.
865 BT-Drs. 19/15346, S. 3.
866 Siehe dazu auch unten S. 320 ff.
867 *Petri* in: *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch, G. Rn. 390.
868 *Arzt* in *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch des Polizeirechts, G. Rn. 1199.
869 Siehe dazu unten S. 271 ff.

der (IMK) im Jahre 1990 in Form der „INPOL-Grundsätze" erhalten hatte, gehörten im Wesentlichen die Personen- und die Sachfahndung, der Kriminalaktennachweis, die Haftdatei, der Erkennungsdienst und die Daktyloskopie, Arbeitsdateien für besondere Kriminalitätsbereiche (PIOS[870]) Hinweis-/Spurendokumentation in Ermittlungsverfahren von länderübergreifender Bedeutung (SPUDOK) sowie die Polizeiliche Kriminalstatistik zum Verbund.[871] Das gegenwärtig in Betrieb befindliche polizeiliche Informationssystem, genannt INPOL-neu,[872] ist 2003 an den Start gegangen und weist gegenüber seinem Vorgänger einige Modifikationen auf.[873]

Normative Anknüpfungspunkte hierfür bietet indessen weniger das BKAG als vielmehr die erst[874] 2010 in Kraft getretene BKADV.[875] Diese ursprünglich auf Grundlage von § 7 Abs. 11 BKAG a.F. erlassene Verordnung gilt auch nach der Novellierung des BKAG weiterhin.[876] Sie dient der Konkretisierung der Datenarten und Dateiformen, die im polizeilichen Informationswesen verarbeitet und errichtet werden dürfen.[877] Problematisch ist in diesem Zusammenhang indessen der Umstand, dass die BKADV in ihrem Wortlaut noch immer auf die vorherige Fassung des BKAG verweist, obwohl im Normtext teils erhebliche Veränderung vorgenommen wurden. Es fehlt insoweit an einem „Übersetzungsschlüssel", der die BKADV für künftige Weiterverarbeitung von personenbezogenen Daten handhabbar macht.[878] Es ist zwar grundsätzlich denkbar, im Wege der Auslegung mit

870 PIOS steht für „Personen – Institutionen – Objekte – Sachen".

871 BT-Drs. 13/1550, S. 28; so auch *Zöller,* Informationssysteme, S. 140 ff.; zu weiteren damaligen Anwendungen im Bereich elektronischer Datenverarbeitung vgl. *Zöller*, a.a.O., S. 147.

872 In Abgrenzung zu „INPOL-aktuell", vgl. *Graulich* in *Schenke/Graulich/Ruthig,* Sicherheitsrecht, § 29 BKAG Rn. 8.

873 Siehe zu der diesbezüglichen historischen Entwicklung bereits oben S. 131 ff.

874 Zum langen Streit um die BKADV siehe *Kehr,* Datei Gewalttäter Sport, S. 191 ff. mwN.

875 *Spiecker gen. Döhmann/Kehr* Deutsches Verwaltungsblatt 2011, 930.

876 Einerseits ist anerkannt, dass das nachträgliche Erlöschen oder auch nur die nachträgliche Änderung ohne Einfluss auf den Rechtsbestand einer ordnungsgemäßen Rechtsverordnung ist, vgl. BVerfG, Beschluss vom 23. März 1977 – 2 BvR 812/74, Rn, 26; *Graulich,* Die Zustimmungsbedürftigkeit der Aufhebung, Verlängerung und Änderung von Gesetzen und Rechtsverordnungen, S. 146. Zudem trat aber gem. Art. 13 Abs. 2 des Gesetzes zur Neustrukturierung des Bundeskriminalamtgesetzes v. 1.6.2017 I 1354 der neue § 20 BKAG bereits am Tag nach Verkündung in Kraft.

877 *Tetzlaff* Verwaltungsrundschau (vr) 57 (2011), 403.

878 *Graulich* in *Schenke/Graulich/Ruthig,* Sicherheitsrecht, § 20 BKAG Rn. 6.

der BKADV zu arbeiten,[879] schon zur Klarstellung und damit auch besseren Rechtswendung wäre indessen der Erlass einer angepassten BKADV dringend erforderlich.[880] Zudem hat das Bundesverwaltungsgericht bereits 2010 festgestellt, dass die Datenerhebung und -speicherung in den Dateien grundsätzlich so lange unzulässig ist, wie es an einer Rechtsverordnung i.S.d. § 7 Abs. 11 (vormals § 7 Abs. 6) BKAG a.F. fehlte.[881] Zwar ist fraglich, ob man die bis dato unterlassene Anpassung mit einem kompletten Fehlen gleichsetzen kann. Mit Blick auf das Urteil des Bundesverwaltungsgerichts zur Vorgängervorschrift der Verordnungsermächtigung des § 20 BKAG ließe sich das durchaus annehmen.[882] Das Untätigbleiben des Verordnungsgebers lässt sich aber vor allem auch als Sinnbild für das Verhältnis zwischen dem normativem Steuerungsanspruch des Rechts der polizeilichen Informationsverarbeitung und den faktischen Organisations- und Wirkweisen des polizeilichen Informationssystems lesen. Was faktisch getan wird, wird entweder in nicht unerheblichem Maße überhaupt nicht vom Recht erfasst oder findet in diesem in eher deskriptiver Weise seinen Niederschlag. Trotz des Stellenwertes, den Daten im gesellschaftlichen Bewusstsein mittlerweile haben, ist die BKADV weder mit Erlass des BKAG, noch zum geplanten Termin, Mitte 2020,[883] angepasst worden. Mit Blick auf den Umstand der geplanten Auflösung der Dateienstruktur scheinen die Anpassungsbedarfe zudem nicht lediglich redaktioneller Art zu sein. Zwar scheint es schon länger einen Entwurf zu geben,[884] der aber, soweit ersichtlich, nicht öffentlich zugänglich ist.

Die folgenden, an der BKADV orientierten Darstellungen der einzelnen INPOL-Bestandteile sind vor diesem Hintergrund zu lesen. Auch ist die normative Grundlage trotz der dazu in der BKADV enthaltenen Vorschrif-

879 So etwa die Wissenschaftliche Dienste des Bundestages, vgl. WD 3 - 3000 - 063/19, S. 6, Fn. 8.

880 Anders hingegen *Graulich* in *Schenke/Graulich/Ruthig,* Sicherheitsrecht, § 20 BKAG Rn. 6, der die Umstellungen des neuen BKAG für so gravierend hält, „dass jedes Bemühen, mit einer sinnvollen Gesetzesauslegung den fehlenden Übersetzungsschlüssel ersetzen zu wollen, scheitern muss."; vgl. auch *Schenke/Ruthig* in *Schenke/Graulich/Ruthig,* Sicherheitsrecht, Einf. Rn. 4: „Die ehemalige BKADV bezieht sich auf das alte BKAG und hat deshalb keine Funktion mehr."

881 BVerwGE 137, 113-123, Rn. 20.

882 So *Bäcker*, A-Drs. 18(4)806 D, S. 4 Fn. 9.

883 Dieser Termin wurde dem Verfasser in einer schriftlichen Anfrage beim BMI genannt.

884 *Schenke/Graulich/Ruthig* in *Schenke/Graulich/Ruthig,* Sicherheitsrecht, Einführung A. Rn. 4.

ten schmal. Die Dateien werden nur knapp mit ihren Zweckausrichtungen benannt. Technische Strukturen, wie das ansatzweise für den polizeilichen Informationsverbund mit dem neuen BKAG geschaffen wurde, finden sich für die Dateien in der BKADV nicht. Hier hat also die normative Kraft des Faktischen einen weiten Wirkraum. Zudem ist sich immer zu vergegenwärtigen, dass die alte Dateienstruktur der Verrechtlichung der polizeilichen Informationsverarbeitung zeitlich vorgelagert ist, sodass sich neue Gesetze eher nach den bestehenden Strukturen als umgekehrt gerichtet haben und richten. Zu betonen ist in diesem Zusammenhang zudem, wie es auch die Verordnungsbegründung wiederholt tut, dass die Rechtsverordnung nicht die Voraussetzungen, unter denen die Daten im Einzelfall im Informationsverbund des Bundeskriminalamtes erfasst werden dürfen, definiert. Dies richtet sich nach wie vor nach den konkreten polizei- und strafverfahrensrechtlichen Erhebungsvorschriften.[885]

b) Komponenten von INPOL

aa) INPOL-Z und INPOL-Bund bzw. -Land

INPOL-Z ist nicht explizit geregelt. Rechtsgrundlage ist § 11 BKAG a.F. in Verbindung mit § 91 BKAG.[886] Enthalten sind die Grunddaten zur Person, die Fahndungsdateien, der zentrale Kriminalaktennachweis (KAN), erkennungsdienstliche Daten, personengebundene- und ermittlungsunterstützende Hinweise (PHW, EHW) sowie weitere Daten zu den gespeicherten Personen, womit es sich um die wesentliche technische Infrastruktur für den Datenaustausch der deutschen Polizeien handelt.[887] Dies ergibt sich auch nur mittelbar aus der BKADV, die „INPOL" als Bezeichnung aber nicht explizit nennt. Obwohl INPOL auf alten Rechtsgrundlagen errichtet wurde, richten sich Funktionsweise für alle Daten, die nicht unter die zweifelhafte Regelung des 91 BKAG[888] fallen, nunmehr nach den geltenden Bestimmungen des BKAG, sodass die Arbeit mit den größtenteils noch alten Komponenten, wie sie zuvor durch die alte Rechtslage angeleitet

885 Etwa BR-Drs. 329/10, S. 15.
886 BT-Drs. 19/15346, S. 3.
887 *Arzt* in *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch des Polizeirechts, G. Rn. 1204.
888 Siehe dazu unten S. 275 ff.

wurde, nun mit der gegenwärtigen Rechtslage zum Informationsverbund in Übereinklang gebracht werden muss.

Der polizeiliche Informationsverbund dient gem. § 29 Abs. 2 Satz 1 BKAG der Erfüllung der in § 13 Abs. 2 BKAG genannten Grundfunktionen.[889] Teilnehmende Stellen können gemäß § 29 Abs. 3 Satz 1 BKAG neben dem Bundeskriminalamt und seinen Länderpendants prinzipiell alle sonstigen Polizeibehörden auf Bundes- und Landesebene sein, wobei das Bundeskriminalamt wegen der Parallelität der Grundfunktionen in seinem Informationssystem und im Informationsverbund „strukturbestimmend" ist.[890]

Die Grundfunktionen, zumal nur Regelbeispiele polizeilicher Tätigkeit bezüglich der Verarbeitung von Informationen, erlauben die Nutzung des Informationsverbundes in wenig beschränkter Weise. Eine strikte Zweckbindung sähe anders aus. Neben verfassungsrechtlichen Bedenken ergeben sich auch mit Blick auf die JI-Richtlinie Probleme: Während es sich bei den Grundfunktionen jeweils um strafjustizielle Zwecke im Sinne des Art. 1 Abs. 1 JI-Richtlinie handelt, fordert Art. 4 Abs. 1 lit. b JI-Richtlinie bei einer Verarbeitung zu neuen Zwecken, dass diese „festgelegt und eindeutig" sind, was als Zweckänderung nach verfassungsrechtlichen Vorgaben „hinreichend spezifische Verarbeitungsanlässe erfordert."[891]

In den Informationsverbund sollen – man muss wohl aufgrund des Umsetzungsgrades von *Polizei 2020*[892] sagen: zukünftig – nicht mehr Dateien, sondern Daten einbezogen werden, was Ausdruck des nunmehr gegenüber der technischen Zusammenfassung in Dateien vorrangigen Themenbezuges der Daten sein soll. So sollen etwa Dateien zur Personen- und Sachfahndung als abgegrenzte Datensilos im Informationsverbund wegfallen. Personen- und sachfahndungsrelevante Informationen würden jedoch weiterhin, entsprechend gekennzeichnet, bestehen und dann ohne ihre dateiförmige Strukturierung in die zentrale Datenbank des Bundeskriminalamtes eingestellt,[893] wo sie dann im Wege eines Rechte- und Rollenkonzepts

889 *Petri* in *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch, G. Rn. 969; *Barczak* in *Barczak* (Hrsg.), BKAG, § 29 Rn. 11.
890 *Graulich* in *Schenke/Graulich/Ruthig,* Sicherheitsrecht, § 13 BKAG Rn. 1.
891 Vgl. *Petri* in *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch, G. Rn. 969 in Bezug auf BVerfGE 141, 220, 328 – Bundeskriminalamtgesetz.
892 Siehe dazu unten S. 465 ff.
893 BT-Drs. 18/11163, S. 109.

für verschiedene Akteur:innen in der Polizei unterschiedlich verfügbar wären.[894]

Ihre wesentliche Eingrenzung erfahren die im Informationsverbund zur Weiterverarbeitung zugelassenen Daten durch das Kriterium der „Verbundrelevanz" nach § 30 Abs. 1 BKAG. Das Kriterium, dem eine Schlüsselstellung im Verbund zukommt,[895] hat zwei Funktionen: Einerseits dient es dem Schutze des Informationsverbundes vor Überfrachtung mit irrelevanten Daten und soll so die Effektivität des Verbundes unterstützen. Vorbild für den Begriff der Relevanz im normativen Sinne war dabei das Recht der Nachrichtendienste, insbesondere § 5 Abs. 3 Satz 2 Nr. 1 BVerfSchG. Wie diese Norm findet auch in § 30 Abs. 1 BKAG eine Konkretisierung der datenschutzrechtlich stets zu beachtenden Erforderlichkeit statt, um durch die im Verbund aufgestellten, strikt einzuhaltenden Relevanzkriterien den Informationsfluss zu verbessern.[896] Andererseits soll mit der „Verbundrelevanz" die künftige, durch die Umstrukturierung der polizeilichen Informationsarchitektur bewirkte Irrelevanz des Instruments der Errichtungsanordnung kompensiert werden.[897]

Gemäß § 29 Abs. 3 BKAG haben die am polizeilichen Informationsverbund teilnehmenden Stellen das Recht, Daten zur Erfüllung der Verpflichtung nach § 32 BKAG im automatisierten Verfahren einzugeben und, soweit dies zur jeweiligen Aufgabenerfüllung erforderlich ist, abzurufen. Bisher wurde in Errichtungsanordnungen festgelegt, welcher Teilnehmer in welchem Umfang in welcher Datei personenbezogene Daten eingeben und abrufen darf.[898] Aufgrund des Wegfalls[899] der Errichtungsanordnungen für weite Teile des polizeilichen Informationsbestandes beim Bundeskriminalamt kommt es somit für die Eingabe auf die Verpflichtung nach § 32 BKAG sowie für den Abruf auf die jeweilig rechtlich bestimmten Aufgaben der einzelnen teilnehmenden Stellen an.[900] Dieses Berechtigungserfordernis soll gem. § 29 Abs. 4 Satz 1 BKAG vom Bundeskriminalamt

894 *Bundesministerium des Innern*, Polizei 2020.
895 *Barczak* in *Barczak* (Hrsg.), BKAG, § 30 Rn. 1.
896 *Graulich* in *Schenke/Graulich/Ruthig,* Sicherheitsrecht § 30 BKAG Rn. 2, 4.
897 BT-Drs. 18/11163, S. 110.
898 BT-Drs. 13/1550, S. 28.
899 Da die Dateienstruktur aufgegeben wird, fällt auch das Instrument der Errichtungsanordnung auf langfristige Sicht weg. Diese Lücke soll unter anderem durch die unionsrechtlich vorgeschriebenen Datenschutzinstrumente aufgefangen werden, siehe dazu unter S. 361 ff.
900 *Barczak* in *Barczak* (Hrsg.), BKAG, § 32 Rn. 20.

durch organisatorische und technische Maßnahmen sichergestellt werden. Der Gesetzesbegründung zufolge ersetzt diese Vorschrift den § 11 Abs. 2 Satz 2 BKAG a.F., der aufgrund des Wegfalls der Errichtungsanordnungen überflüssig wird.[901] Diese Verpflichtung des Bundeskriminalamtes zur Implementierung organisatorischer und technischer Sicherungsmaßnahmen kompensiert letztlich ebenfalls die Abnahme normativer Konturen der polizeilichen Datenbestände. Über § 29 Abs. 4 Satz 2 BKAG gelten zudem die auch für das Bundeskriminalamt geltenden Verarbeitungsbestimmungen, insbesondere der Grundsatz der hypothetischen Datenneuerhebung sowie die zu seiner Implementierung erforderliche Kennzeichnung für die Datenspeicherung im Informationsverbund,[902] für alle anderen Teilnehmer des Verbundes.[903]

Aufgrund des Zusammentreffens verschiedener Datenquellen im Informationsverbund, muss die Befugnis zur Verarbeitung jedes einzelnen Datums festgelegt sein. Dies geschieht durch § 29 Abs. 5 BKAG. Dessen Satz 1 statuiert, dass nur diejenige Behörde, die die Daten eingegeben hat, befugt ist, diese zu ändern, zu berichtigen oder zu löschen. Dabei handelt es sich um das sogenannte Besitzerprinzip.[904] Als Besitzer gilt diejenige Stelle, die die Daten in den Verbund eingegeben hat. Wird ein so eingegebenes Datum von anderen Stellen in Vorgänge aufgenommen, sollen diese Stellen eine Besitzanwartschaft begründen, sodass bei Löschung durch den Erstbesitzer diejenige Stelle mit der ältesten Anwartschaft Besitzer wird. Vor allem mit Blick auf Löschungsansprüche von Betroffenen kann diese Praxis dazu führen, dass zu löschende Daten weiterhin im Informationswesen erhalten bleiben.[905] Mit dem Datenbesitz korreliert die datenschutzrechtlichen Verantwortung gemäß § 31 BKAG, was vor allem mit Blick auf individuellen Rechtsschutz relevant ist.[906] Gemäß § 29 Abs. 5 Satz 2 BKAG ist bei Anhaltspunkten über die Unrichtigkeit eines Datums jeder Teilnehmer des Verbundes verpflichtet, der gemäß Satz 1 zuständigen Behörde umgehend darüber Mitteilung zu machen. Die zuständige Behörde ist in einem solchen Fall verpflichtet, die in Frage stehenden Daten unverzüglich zu prüfen und erforderlichenfalls die Daten unverzüglich zu berichtigen, zu löschen

901 BT-Drs. 18/11163, S. 109.
902 Siehe dazu und zu Problemen in diesem Kontext unten S. 323 ff.
903 BT-Drs. 18/11163, S. 109.
904 *Graulich* in *Schenke/Graulich/Ruthig,* Sicherheitsrecht § 31 BKAG Rn. 4.
905 *Petri* in *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch, G. Rn. 915.
906 *Graulich* in *Schenke/Graulich/Ruthig,* Sicherheitsrecht, § 29 BKAG Rn. 28; *Barczak* in *Barczak* (Hrsg.), BKAG, § 29 Rn. 25.

oder in ihrer Verarbeitung einzuschränken. Darüber hinaus ist in Satz 3 des § 29 Abs. 5 BKAG noch die Ergänzung von Daten geregelt: Sind personenbezogene Daten gespeichert, können von jeder teilnehmenden Stelle ergänzend Daten eingeben werden. Probleme kann dies allerdings verursachen, wenn mehrere verantwortliche Stellen Daten zu einer Person gespeichert haben. Neben der Frage nach der letztendlichen datenschutzrechtlichen Verantwortung ist dies vor allem der Fall, wenn eine Behörde ihren Datenbesitz löschen will, andere Stellen ihn jedoch erhalten wollen. In solchen Fällen kann der Datenbesitz auf die erhaltungswillige Stelle übergehen, wobei aber eine einzelfallspezifische rechtliche Bewertung hierüber zu treffen und zu dokumentieren ist. Aus der Parallelstruktur von INPOL-Z und INPOL-Land ergibt sich darüber hinaus die Pflicht, bei Löschungen in den Landessystemen für eine parallele Bereinigung in der Verbunddatei zu sorgen.[907] Mit einem stetig anschwellenden Datenvolumen in den Systemen, wie es Massendatendynamiken erwarten lassen, steht diese Form der Datenpflege vor gravierenden Herausforderungen, die sich vermutlich nur durch bestimmte Automatisierungslösungen adressieren lassen werden.

INPOL-Z stellt für den Datenumgang im Verbund keine eigene Benutzungsoberfläche bereit,[908] was sich mittelbar auch aus § 13 Abs. 3 BKAG ableiten lässt. Die verschiedenen Polizeiorganisationen nutzen vielmehr ihre eigenen Informationssysteme, mit denen sie an INPOL-Z teilnehmen. Konzeptuell spricht man von INPOL-Bund (§ 13 BKAG) und INPOL-Land. Tatsächlich sind die Systeme allerdings anders benannt. Am breitesten genutzt wird das System POLAS, das von allen Polizeibehörden, auch dem Bundeskriminalamt, dem Zollkriminalamt und der Bundespolizei, außer Nordrhein-Westfalen, (dort ViVa) Berlin (dort: POLIKS) und Rheinland-Pfalz (dort: POLIS) genutzt wird. Konturierende Rechtsvorschriften finden sich für diese Systeme kaum. Lediglich § 13 SOG LSA enthält noch eine dem § 13 BKAG vergleichbare Vorschrift. Ansonsten wird als Rechtsgrundlage in der Regel die Datenverarbeitungsgeneralklausel herangezogen werden (müssen), wie etwa in § 37 Abs. 1 S. 1 PolG BW: „Die Polizei kann personenbezogene Daten speichern, verändern und nutzen, soweit und solange dies zur Wahrnehmung ihrer Aufgaben erforderlich ist."

Dieser Befund ist mit Blick auf die Vielschichtigkeiten und Komplexitäten des Informationsumgangs in den Systemen einigermaßen ernüchternd.

907 *Arzt* in *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch des Polizeirechts, G. Rn. 1209 f.

908 BT-Drs. 14/7734, S. 2.

Instruktiv wird er für die baden-württembergische POLAS-Version von *Kathke* geschildert[909]: POLAS BW ermöglicht einerseits den Zugang zu INPOL-Z, aber auch zu Auskunftssystemen externer Behörden. Anderseits fungiert POLAS BW für das Land Baden-Württemberg gleichfalls als regionales Verbundsystem für alle dortigen Polizeibehörden. Es ist dort „Landesdatenhaltungssystem und Auskunftssystem" für alle polizeilich gespeicherte Daten. Insofern fungiert POLAS BW „als Auskunfts- und Fahndungssystem zur repressiven und präventiven Kriminalitätsbekämpfung, zur Erfassung der für die PKS erforderlichen Daten und als Fallregistratur aller Anzeigen nicht geklärter Straftaten, die den Staatsanwaltschaften vorgelegt werden." Das Informationssystem besteht aus einer Auskunfts- und einer Änderungskomponente. Die Auskunftskomponenten steht allen Sachbearbeiter:innen über eine Webanwendung über eine Intranetseite zur Verfügung, wobei Suchen nach raumbezogenen Parametern (etwa regional oder national) angepasst werden können. Die Änderungskomponente ist weniger verfügbar. Sie ist „als Client-Server-Anwendung bei den Datenstationen der Polizeipräsidien als den zentral zuständigen Stellen lokalisiert." Nur hierüber können Daten manuell eingepflegt oder verändert werden, wobei dann eine automatische Plausibilitätsprüfung erfolgen soll.

Die Interaktion mit dem System erfolgt entlang drei verschiedener Entitäten, die so die polizeiliche Arbeit strukturieren: Personen, Sachen, Fälle. In den Entitäten sind die Daten wiederum in verschiedenen Gruppen organisiert, die untereinander miteinander verknüpft werden können und durch ihre Kategorisierung die Dateistruktur in INPOL-Z bilden, wie sie im Anschluss an diesen Unterabschnitt näher dargestellt wird. Für Personen enthält die Datengruppe „Rechtmäßige Personalien" (P-Gruppe) die personenbezogene Grunddaten, zudem können Daten aber auch als „Andere Personalien" und damit der A-Gruppe zugehörig referenziert werden, womit dann etwa die Aufnahme von Aliasnamen oder anderen Schreibweisen der Namen in die Datenbank ermöglicht wird. In der Datengruppe „Personenfahndung" (F-Gruppe) werden Ausschreibungen von Personen verwaltet, von Straftäter:innen über Zeug:innen bis hin zu vermissten Per-

909 Siehe zum Folgenden *Kathke*, Überlieferungsbildung aus, Fachverfahren Überlegungen zu POLAS BW der Polizei Baden-Württemberg, 2015, S. 12 ff.; es kann davon ausgegangen werden, dass trotz der oft erwähnten Heterogenität des polizeilichen Informationswesens die Informationssysteme, mit denen an INPOL-Z teilgenommen wird, im Wesentlichen dieselben Funktionalitäten aufweisen, sodass die Beschreibung von POLAS BW als repräsentativ angesehen werden darf, zumal POLAS von den meisten Polizeibehörden genutzt wird.

sonen. Die Datengruppe „Dokumente“ (Q-Gruppe) erfasst Dokumente, die einen Personenbezug aufweisen, also etwa Haftbefehle oder strafverfahrensrechtliche Beschlüsse, nach einem Scan der Papierform digital. In der Datengruppe „Haftdatei“ (H-Gruppe) werden die spezifischen Haftdaten von erfassten Personen gespeichert. Die Datengruppe „Erkennungsdienst“ (E-Gruppe) enthält erkennungsdienstliche Daten. Daneben bestehen noch die L-Gruppe („Personenbeschreibung“), über die eine detaillierte Personenbeschreibung vorgenommen werden kann, sowie die W-Gruppe („Personenbezogene Hinweise“) und Z-Gruppe („Zusätzliche Personeninformationen“), die detaillierte Informationen zu den verwalteten Personen enthalten, etwa die Einstufung als gewalttätig, links- oder rechtsextrem oder als Drogenkonsument:in sowie berufliche Ausbildungen und Tätigkeiten. *Kathke* zufolge sind die Daten der Gruppe „Unterlagen“ (U-Gruppe) von besonderer Bedeutung für den Bereich der Personen, da sie den „Verweis auf die kriminalaktenführende Polizeidienststelle (KAN-Nachweis), das Aussonderungsprüfdatum der Unterlagen, die vorhandenen Fall- und Ereignisdaten, die Entscheidung bzw. die Mitteilung über den Verfahrensausgang und ein Verzeichnis der durchgeführten DNA-Maßnahmen enthält.“ Über diese Gruppe findet somit eine Vernetzung der aus Polizeiperspektive zentralen Daten statt, weil „über das Datenfeld Ereignisse eine Zuordnung von bekannten Fällen erfolgt, die Erfassung einer U-Gruppe Voraussetzung einer Erfassung von A-, E-, L- und W-Gruppe ist und der Dateninhalt maßgeblich für die Aufnahme von personenbezogenen Daten eines Tatverdächtigen in den Kriminalaktennachweis beim BKA ist.“ Insofern können über den Zugang zu dieser Gruppe neben einer tiefgehenden Analyse der Person, insbesondere über die Hinweise, auch alle Verbindungen der Person zu bekannten Taten dargestellt werden. Gemeinsam mit den Haftdaten lassen sich so kriminelle Karrieren rekonstruieren und darüberhinausgehende Zusammenhänge ableiten.

Weniger facettenreich ist POLAS BW mit Blick auf Sachdaten. Hier können Kennzeichen, Ausweisnummern, Banknoten, Waffen oder andere mit numerischen Zeichen versehene Gegenstände erfasst und abgefragt werden. Dazu werden die Sachfahndungsnotierung (N-Gruppe) und die Sachbeschreibung (S-Gruppe) gebildet: Die N-Gruppe enthält vorrangig Daten zu rechtlichen oder faktischen Personen-Sachen-Beziehungen, die S-Gruppe spezifische Informationen zur Sache.

Die letzte Entität, Fälle, enthält schließlich straftatenbezogene Einzelhinweise bezüglich geklärter wie ungeklärter Fälle. In der sog. T-Gruppe gespeichert werden Daten der Tat, Opferdaten und Deliktsdaten.

Nicht nur innerhalb einer Entität, sondern auch die Entitäten untereinander können miteinander verknüpft werden. So kann eine Person mit mehreren Fällen und ein Fall mit mehreren Personen verbunden sein. Diese Netzwerkstruktur spiegelt sich auch in den Suchmöglichkeiten wider. So ist „ein Wechsel von einer Personenrecherche zu einem verbundenen Fall und umgekehrt [...] innerhalb der Datenbank jederzeit möglich." Genauso verhält es sich mit Sachen und Fällen. Die Entität Fall ist somit zentral im Datenmodell von POLAS BW, da hier Personen und Sachen in polizeirelevanter Weise miteinander verklammert werden.

Die Daten für POLAS BW kommen aus dem Vorgangsbearbeitungssystem[910] der Polizei in Baden-Württemberg (ComVor). Wenn die Daten übertragen werden, erfolgt eine Prüfung und erforderlichenfalls eine Korrektur bei der zuständigen Datenstation. Anschließend erfolgt die Übertragung zu POLAS auf Knopfdruck. Eine vollautomatisierte Übertragung erfolgt gegenwärtig nicht. Auch müssen einige Datenarten noch manuell in POLAS BW erfasst werden, so etwa Sachfahndungsdaten oder auch von der Justiz übermitteltete Fahndungs- und Haftdaten. Einmal in POLAS angekommen, können die Daten dort noch weiter ergänzt werden, ein Rückfluss der Informationen nach ComVor ist hingegen nicht möglich. Sowohl das Vorgangsbearbeitungssystem als auch POLAS BW verfügen aber über eine Schnittstelle, über die Schnittstelle mit ComVor gibt es außerdem eine Verbindung zu X-Justiz, also insbesondere für strafverfahrensrechtliche Daten. Die weit wichtigere Schnittstelle – und hier schließt sich der Kreis zu INPOL-Z – ist jedoch die Teilnahme von POLAS BW (und allen anderen äquivalenten INPOL-Land-Systemen) an INPOL-Z. So sind Sach- und Personenfahndungsdaten parallel gespeichert, denn die Daten, die in POLAS gespeichert werden und Verbundrelevanz besitzen, werden an das vom Bundeskriminalamt geführte INPOL-Z weitergeleitet und von dort in die anderen Informationssysteme der 16 Bundesländer sowie die Systeme vom Bundeskriminalamt selbst, von Bundespolizei und Zollkriminalamt übertragen. Über die INPOL-Z-Schnittstelle liefert POLAS BW auch Daten in das Gesichtserkennungssystem (GES), das Automatische-Fingerabdruck-Informationssystem (AFIS), die DNA-Analyse-Datei International (DAD-i) sowie das nationale Schengener Informationssystem (NSIS), wo europaweite Fahndungen eingetragen werden. Umgekehrt können diese Datenbanken auch alle über POLAS BW für die polizeiliche Aufgabenerfüllung genutzt werden. Schließlich hält POLAS BW auch noch

910 Näher zu Vorgangsbearbeitungssystemen siehe unten S. 254 ff.

Schnittstellen zu nicht-polizeilichen öffentlichen Datenbanken wie zu MeldIT, dem Meldedatenbestand, dem Bundeszentralregister (BZR), dem Zentralen Staatsanwaltschaftlichen Verfahrensregister (ZStV), dem Zentralen Verkehrsinformationssystem für die Polizei beim Kraftfahrbundesamt (ZEWIS) oder dem Ausländerzentralregister bereit.

Vor dem Hintergrund der vielfältigen Funktionalitäten von INPOL ließe sich zwar argumentieren, dass eine detailgetreue(re) Abbildung dieser Strukturen und Verarbeitungsmöglichkeiten im Gesetz die Rechtslage eher noch verworrener machen würde und auch, dass die BKADV doch eine Präzisierung des INPOL-Betriebes enthält. Neben dem Umstand, dass diese jedoch – wie bereits dargelegt – gegenwärtig veraltet ist, wurde sie zudem wie ein Großteil der geltenden Regelungen stets nach den technischen Strukturen erlassen, sodass selbst die präzisierende BKADV lediglich bereits Bestehendes und Praktiziertes abbildet, ohne in irgendeiner Weise einen eigenen rechtlichen Steuerungsanspruch zu entwickeln. Auf dieser Linie liegt auch weiterhin die Gesetzgebung. Das gilt einerseits, wenn sie lediglich Datenverarbeitungsgeneralklauseln für komplexe Informationssysteme schafft, die eine ganz andere Eingriffsintensität entfalten, als wenn Sachbearbeiter:innen lediglich mit Papierakten arbeiten würden – beide Arbeitsformen sollen aber anscheinend ihre Rechtsgrundlage in den Generalklauseln finden. Andererseits wird die mangelnde gesetzgeberische Eigeninitiative auch evident, wenn der Gesetzgeber versucht – wie das in 29 ff. BKAG geschehen ist – einen im Wesentlichen aus der Exekutive stammenden Innovationsimpuls, *Polizei 2020*, in Gesetzesform zu gießen.

bb) Personen- und Sachfahndungsdateien

Kernstück des gegenwärtigen INPOL-Verbundsystems sind die Personen- und Sachfahndungsdateien.[911] Die Befugnis des Bundeskriminalamtes zum Führen von Personenfahndungsdateien ergibt sich aus § 16 Abs. 2 Satz 1 BKAG.[912] Im Polizeialltag spielt sie eine übergeordnete Rolle. Zwar bezieht sich § 16 Abs. 2 Satz 1 BKAG seinem Wortlaut zufolge auf die Weiterverar-

911 https://www.bka.de/DE/UnsereAufgaben/Ermittlungsunterstuetzung/ElektronischeFahndungsInformationssysteme/polizeilicheInformationssysteme_node.html (Stand: 01.10.2023); vgl. auch *Arzt* Neue Juristische Wochenschrift 2011, 352, S. 353, der von „Grundpfeilern" polizeilicher Datenverarbeitung spricht.

912 *Eichenhofer* in *Barczak* (Hrsg.), BKAG, § 16 Rn. 13.

beitung im Informationssystem des Bundeskriminalamtes. Über § 29 Abs. 4 Satz 2 BKAG findet die Norm aber Anwendung auf den gesamten Informationsverbund. Die Datei enthält Daten über Personen, die von der Polizei aufgrund eines Haftbefehls, einer Ingewahrsamnahme, einer Aufenthaltsermittlung, einer Ausreiseuntersagung sowie bei Ausländer:innen wegen beabsichtigter Abschiebung oder Zurückweisung gesucht werden.[913] Zudem ermöglicht sie dem Bundeskriminalamt die Weiterverarbeitung von personenbezogenen Daten, soweit dies zur polizeilichen Beobachtung oder gezielten Kontrolle erforderlich ist.[914] Sowohl bei Personen- als auch bei Sachfahndungsdateien, die beide in der BKADV in § 9 Abs. 2 Nr. 1 konkretisiert werden, handelt es sich um Verbunddateien. Welche personenbezogenen Daten in der Personenfahndungsdatei gespeichert werden dürfen, wird umfänglich in § 6 Abs. 1 BKADV geregelt. Demgegenüber bestimmt § 6 Abs. 2 BKADV die Personen, von denen die in Absatz 1 genannten Daten verarbeitet werden dürfen. Dabei ist – wie auch bei allen anderen Datenspeichern, die personenbezogene Daten enthalten – ein hoher Anspruch an die Datenrichtigkeit zu stellen, wie er insbesondere durch die JI-Richtlinie nunmehr für das nationale Recht, etwa in § 75 Abs. 1 BDSG, postuliert wurde.[915] Denn die hohe Dynamik der datenverarbeitenden Operationen und damit die Dynamik des Informationswesens selbst eröffnen laufend Spielräume für Datenfehler, etwa in Form von Verwechslungen. Mit Blick auf die darin für Betroffene liegenden Gefahren[916] muss der Datenqualität ein höherer Stellenwert als ihrer Quantität eingeräumt werden.[917] Gegenwärtig[918] sind in der INPOL-Personenfahndungsdatei 274.894 Ausschreibungen zur Festnahme und 426.962 Ausschreibungen zur Aufenthaltsermittlung enthalten.[919]

913 *Petri* in *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch, G., Rn. 424.

914 Zudem muss das Bundeskriminalamt oder die die Ausschreibung veranlassende Stelle nach dem für sie geltenden Recht befugt sein, die mit der Ausschreibung für Zwecke der Strafverfolgung, des Strafvollzugs, der Strafvollstreckung oder der Abwehr erheblicher Gefahr vorgesehene Maßnahme vorzunehmen oder durch eine Polizeibehörde vornehmen zu lassen.

915 Siehe dazu bereits oben S. 215 ff.

916 Siehe dazu bereits den Fall in Fn. 811.

917 So zutreffend *Arzt* in *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch des Polizeirechts, G. Rn. 1212.

918 Stand 01.10.2023.

919 https://www.bka.de/DE/UnsereAufgaben/Ermittlungsunterstuetzung/ElektronischeFahndungsInformationssysteme/polizeilicheInformationssysteme_node.html (Stand: 01.10.2023).

Die Sachfahndungsdatei wird nicht in 16 Abs. 2 Satz 1 BKAG geregelt. Erwähnt wird sie in § 2 Abs. 4 Nr. 2, § 13 Abs. 2 Nr. 2 sowie 27 Abs. 2 BKAG. Während die beiden erstgenannten Normen keine Befugnisnormen wie etwa § 16 Abs. 2 Satz BKAG sind, setzt § 27 Abs. 2 BKAG die Sachfahndungsdatei vielmehr voraus, als sie zu regeln. Mangels Personenbezug ist für die Sachfahndungsdatei hingegen grundsätzlich keine besondere Befugnis erforderlich. In der BKADV findet sich in § 6 Abs. 3 eine Regelung für diejenigen Daten und Personen, die im Zusammenhang mit zur Fahndung oder zur polizeilichen Beobachtung ausgeschriebenen Sachen gespeichert werden dürfen, wo also doch ein Personenbezug der Sachen besteht. Gegenwärtig[920] sind etwa 16 Mio. Gegenstände erfasst, die wegen eines möglichen Zusammenhangs mit Straftaten gesucht werden.[921]

cc) Kriminalaktennachweis (KAN)

Im INPOL wird ein Kriminalaktennachweis (KAN) über Straftaten von erheblicher Bedeutung und überregional bedeutsame Straftaten,[922] also ein Indexsystem für die bei den Polizeien vorgehaltenen Kriminalakten, als Verbunddatei geführt. Erhebliche Straftaten sind Verbrechen gem. § 12 Abs. 1 StGB sowie die Katalogstraftaten des § 100a StPO. Die überregionale Bedeutung wird kasuistisch bestimmt.[923] So können beispielsweise auch Akten indexiert werden, deren Bedeutung per se unterhalb dieser Schwellen liegt, bei denen sich aber mittels Prognose ergibt, dass sie zur Verhütung von Straftaten mit länderübergreifender, internationaler oder (sonst) erheblicher Bedeutung beitragen können.[924] Die im KAN indexierten Kriminalakten stellen zudem kriminalpolizeiliche personenbezogene Sammlungen (KpS) dar. Da über die Rahmenbedingungen der KpS im Wesentlichen geregelt wird, was an Informationen überhaupt in Kriminalakten aufgenommen wird und damit auch potenziell im KAN verfügbar ist, besteht ein enger Konnex zwischen beiden Strukturen. KAN und KpS sind allerdings trotz dieses inhaltlichen Konnexes nicht zusammenhängend

920 Stand 01.10.2023.
921 https://www.bka.de/DE/UnsereAufgaben/Ermittlungsunterstuetzung/ElektronischeFahndungsInformationssysteme/polizeilicheInformationssysteme_node.html (Stand: 01.10.2023).
922 § 9 Abs. 1 Nr. 2 BKADV.
923 Siehe *Zöller,* Informationssysteme, S. 141.
924 NdsLT-Drs. 16/2770, Anlage 5, S. 1.

geregelt. Während der KAN im Wesentlichen im BKAG und der BKADV geregelt ist, finden sich für die KpS verschiedene Richtlinien in den Ländern.

Zwar verweisen die KpS-Richtlinien darauf, dass Datenverarbeitungen zu kriminalpolizeilichen Zwecken nur auf Basis entsprechender Rechtsgrundlagen erfolgen dürfen. Allerdings dürften die KpS-Richtlinien aufgrund ihrer kohärenten Darstellung der Vorgaben zur Verarbeitung von Daten zu kriminalpolizeilichen Zwecken in der Praxis einen wesentlichen normativen Rahmen bei der formalen und auch inhaltlichen Ausgestaltung der kriminalpolizeilichen Datenverarbeitung spielen. So stellen die KpS-Richtlinien etwa an einem Ort zusammen, welche Personen oder welche Datentypen – etwa Verhaltensdaten – in die Sammlungen aufgenommen werden dürfen.[925] Es ist zwar zu begrüßen, dass den Polizeibeamt:innen ein kohärenter Leitfaden für die Arbeit mit kriminalpolizeilichen Daten an die Hand gegeben wird. Allerdings entstammen diese normativen Vorgaben nicht dem demokratischen Deliberationsprozess, sodass sich auch am neuralgischen Punkt der kriminalpolizeilichen Datenverarbeitung eine Entkoppelung der polizeilichen Institutionen von direkten legislativen Steuerungsimpulsen zeigt. Das ist mit Blick auf die Bedeutung der KpS für die polizeiliche Informationsverarbeitung problematisch: Sie gelten als „polizeiliches Gedächtnis" für Kriminalität und sind ein zentrales Instrument polizeilicher Informationsarbeit.[926]

Gesetzlich geregelt ist hingegen der KAN, über den Zugriff auf die kriminalpolizeilichen Daten hergestellt werden kann. Die den KAN vormals regelnden §§ 7 bis 9 BKAG a.F. sind unter anderem in § 18 BKAG aufgegangen.[927] Im Aktennachweissystem sind Grunddaten, die den Personendaten nach § 1 Abs. 1 BKADV entsprechen,[928] soweit erforderlich, andere zur Identifizierung geeignete Merkmale, die kriminalaktenführende Stelle und die Kriminalaktennummer sowie die nähere Bezeichnung der Straftat nach Tatzeiten, Tatorten und Tatvorwürfen enthalten. Bedeutsam sind dabei insbesondere die anderen zur Identifizierung geeigneten Merkmale gem. § 1 Abs. 2 BKADV, denen auch Informationen unterfallen, die eine

925 Siehe Richtlinien über Kriminalpolizeiliche personenbezogene Sammlungen (KpS-Richtlinien) KpS-Richtlinien vom 2. Oktober 2008 (Brem.ABl. 2008, S. 893).

926 So *Arzt* in *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch des Polizeirechts, G. Rn. 1215.

927 *Graulich* in *Schenke/Graulich/Ruthig,* Sicherheitsrecht, § 18 Rn. 1.

928 *Graulich* in *Schenke/Graulich/Ruthig,* Sicherheitsrecht, § 18 BKAG Rn. 15.

Verhaltensbeurteilung der gespeicherten Person ermöglichen können oder sogar sollen.[929] Aufgrund unklarer Zugriffsberechtigungen wird der KAN in der Praxis nicht nur als Aktennachweis, sondern auch als Personenindex genutzt. Vor dem Hintergrund der zunehmenden Elektronisierung der Aktenbestände,[930] nimmt so auch die Intensität eines Eingriffs durch Speicherung im KAN zu, da die dort gespeicherten Informationen so zunehmend breit und schnell verfügbar sind. Die im KAN gespeicherten Daten, die in der Regel die wichtigsten Informationen der zugrundeliegenden Kriminalakte zusammenfassen, können in ihrer Komprimiertheit eine gewisse Voreingenommenheit erzeugen – vor allem, wenn eine detaillierte Auseinandersetzung mit der in Frage stehenden Person durch den jeweiligen Polizeibeamten durch den Abruf der Daten aus dem KAN unterbleibt.[931] Das ist umso gravierender, wenn auch Kontakt- und Begleitpersonen sowie Auskunftspersonen in den KAN gelangen.[932] Voraussetzung für die Aufnahme in den KAN ist eine Negativprognose, wie sie beispielsweise in § 18 Abs. 1 Nr. 4 BKAG für Anlasspersonen vorgeschrieben wird. Umfasst sind also solche Personen, bei denen ohne Verurteilung, Beschuldigung oder Verdacht (nur) tatsächliche Anhaltspunkte die Annahme zukünftiger Straftaten rechtfertigen. Aufgrund des Umstandes, dass die Weiterverarbeitung von personenbezogenen Daten des Personenkreises von § 18 BKAG im Ermessen der jeweiligen Behörde steht, das jedoch vom Gesetz in keinerlei Hinsicht angeleitet wird, hat *Bäcker* zudem weitere Eingrenzungen vorgeschlagen: So soll der Anwendungsbereich von § 18 Abs. 1 und 2 BKAG auf Straftaten von hinreichendem Gewicht beschränkt werden und die Weiterverarbeitung, die vor allem in der Bevorratung der Daten liegt, zeitlich begrenzt sowie der Verarbeitungsanlass dahingehend konkretisiert werden, dass konkrete Tatsachen auf die Begehung von Straftaten schließen lassen.[933]

929 *Petri* in *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch, G. Rn. 406.

930 Siehe den Nachweis bei *Arzt* in *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch des Polizeirechts, G. Rn. 1215.

931 *Arzt* in *Möstl/Kugelmann* (Hrsg.), Beck'scher Online-Kommentar Polizei- und Ordnungsrecht Nordrhein-Westfalen, 11. Edition, § 24 PolG NRW Rn. 33; *Petri* in *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch, G. Rn. 406.

932 *Arzt* in *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch des Polizeirechts, G. Rn. 1216 Siehe näher zu diesen Personenkazegorien unten S. 324 ff.

933 *Bäcker*, Schriftsatz der Verfassungsbeschwerde im Verfahren 1 BvR 1160/19, S. 51 f., abrufbar unter: https://freiheitsrechte.org/home/wp-content/uploads/2019/10/2019-05-21-BKA-Gesetz-VB-anonymisiert.pdf (Stand: 01.10.2023).

Die im KAN gespeicherten Daten besitzen dabei aufgrund der praktischen Handhabung von Kriminalakten besondere Beharrungskräfte, denn die Polizei speichert die Daten auch über den reinen Abschluss der Ermittlungen oder Verfahren hinaus, wenn ein Restverdacht besteht, selbst wenn die betroffene Person wegen Beweismangels freigesprochen oder das Verfahren sanktionslos eingestellt worden ist.[934] Diese Praxis wird durch § 18 Abs. 5 BKAG bestätigt, der eine obligatorische Löschung nur für Fälle vorschreibt, in denen das Urteil explizit angibt, dass jemand eine Tat nicht oder nicht rechtswidrig begangen hat. Die Norm scheint indessen in einem Spannungsverhältnis zu verfassungs- und menschenrechtlichen Vorgaben zu stehen. Während das Bundesverfassungsgericht entschieden hat, dass es „nach einem Freispruch […] für die Annahme eines fortbestehenden Tatverdachts aber besonderer, von der speichernden Polizeibehörde darzulegender Anhaltspunkte [bedarf], die sich insbesondere aus den Gründen des freisprechenden strafgerichtlichen Urteils selbst ergeben können",[935] es also nur in Ausnahmefällen zu einer weiteren Speicherung kommen kann, ist der Europäische Gerichtshof für Menschenrechte insoweit strenger: „Tatsächlich gilt die Unschuldsvermutung nicht nur während eines laufenden Strafverfahrens. Damit sie praktisch und wirksam ist, dürfen Behörden und Gerichte im Fall der Einstellung eines Strafverfahrens oder des Freispruchs in den Gründen ihrer Entscheidung keinen Schuldvorwurf gegenüber dem Betroffenen äußern."[936] Daraus ergibt sich zumindest eine intensivere Prüfungspflicht für die der weiteren Speicherung zugrunde liegende Negativprognose, insbesondere in den Fällen des § 18 Abs. 5 BKAG. Da hierzu zunächst der Ausgang des Verfahrens als initiale Information benötigt wird, müssen die Staatsanwaltschaften gem. § 482 Abs. 2 S. 1 StPO in Verbindung mit Nr. 88 S. 2 RiStBV Mitteilung über den Ausgang machen, wobei aber nicht immer die Gründe für die Verfahrensbeendigung mitgeteilt werden, sodass die Verpflichtung zur automatisierten Mitteilung derselben in § 32 Abs. 2 BKAG zu begrüßen ist, wenngleich Zweifel hinsichtlich der technischen Umsetzbarkeit bestehen.[937]

934 *Bundesbeauftragter für Datenschutz und Informationssicherheit*, A-Drs. 18(4)806 A, S. 20 ff.

935 BVerfG, 16.05.2002 - 1 BvR 2257/01 (NJW 2002, 3231).

936 EGMR, Urteil vom 15.01.2015 - EGMR Aktenzeichen 48144/09 (NJW 2016, 3225).

937 *Arzt* in *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch des Polizeirechts, G. Rn. 1221 Ausführlicher zum Verfahren rund um § 18 Abs. 5 BKAG auch unten S. 329 ff.

dd) Haftdatei

Ebenfalls starken kriminaljustiziellen Bezug hat die Haftdatei, die in § 18 Abs. 4 BKAG hinsichtlich der Verarbeitung geregelt und in § 9 Abs. 2 Nr. 2 BKADV hinsichtlich ihrer Struktur erwähnt ist. Sie dient dem Nachweis über Personen, die wegen rechtswidriger Straftat oder des Verdachts einer rechtswidrigen Straftat einer richterlich angeordneten Freiheitsentziehung unterliegen. Zweck sind die Verhinderung unnötiger Fahndungen, Alibiüberprüfungen und das Informiertsein über bevorstehende Haftentlassungen, sodass die Haftdatei vor allem der Vorsorge künftiger Strafverfolgung, aber auch der Gefahrenabwehr dient.[938] Voraussetzung für eine Verarbeitung in der Datei ist eine richterlich angeordnete Freiheitsentziehung anlässlich einer rechtswidrigen Tat. Die BKADV legt näher fest, welche Daten von der Polizei in entsprechenden Fällen verarbeitet werden dürfen.

ee) Erkennungsdienstliche Dateien und DNA-Analyse-Dateien (DAD)

Die schon seit den Anfängen der modernen Polizei bestehende Aufgabe der fehlerfreien Identifizierung von Personen hat in INPOL ihren strukturellen Niederschlag in Form der erkennungsdienstlichen Dateien gefunden. Die gespeicherten Daten, die gemäß § 16 Abs. 5 i.V.m. § 2 Abs. 4 BKAG zu repressiven und präventiven Zwecken verarbeitet werden dürfen, sollen eine möglichst präzise Identifizierung ermöglichen. Die BKADV sieht daher in § 9 Abs. 1 Nr. 4 in Verbindung mit § 5 Abs. 1 einen breiten Katalog an Datentypen vor, die diesem Zweck dienen. Gegenwärtig dürften in diesem Rahmen nach wie vor die daktyloskopischen Bestände und Systeme den größten praktischen Nutzen mit sich bringen. Hier gibt es unterschiedliche technische Lösungen wie die Automatisierten Fingerabdruck-Identifizierungssysteme für den polizeirechtlichen (AFIS-P) bzw. asylrechtlichen Bereich (AFIS-A), die dem Abgleich von Mustern dienen, sowie die Nationale Datenbank für digitalisierte Fingerabdrücke für Polizei (NatDB P) und Asyl (NatDB A), die als digitale Sammlung der vorhandenen Fingerabdruckblätter fungieren.[939] Zum zuletzt von Behördenseite aktualisierten Stand (April 2022) sind so 5,3 Millionen Personen und 440.000 Spuren

938 *Graulich* in *Schenke/Graulich/Ruthig,* Sicherheitsrecht, § 18 BKAG Rn. 37; *Eichenhofer* in *Barczak* (Hrsg.), BKAG, § 18 Rn. 11.

939 BT-Drs. 17/14735, 17.

in den Datenbanken gespeichert.[940] Der informationelle Wert dieser Daten für die polizeiliche Arbeit steigt mit zunehmend verbesserter Identifizierungstechnologie. So gibt es bereits seit einigen Jahren die Möglichkeit Fingerabdrücke im Einsatz zu erfassen und digital in Echtzeit abzugleichen.[941] Mit fortschreitender Leistungsfähigkeit von sogenannter „intelligenter" Videotechnik[942] und der verbreiteten Nutzung von digitalen Kameras im Einsatz zur Personenidentifizierung innerhalb weniger Augenblicke[943] ist aber auch ein Bedeutungszuwachs der visuellen Daten, etwa von Lichtbildern und sonstigen besonderen körperlichen Merkmalen, zu erwarten.

Neben diesen klassischen Identifizierungsformen ist seit den 1990er-Jahren auch die Speicherung von DNA-Analyse-Mustern zum Zwecke der Identifizierung ein Thema von zunehmender Relevanz im polizeilichen Informationswesen. § 5 Abs. 5 BKADV regelt dazu, welche Muster und damit zusammenhängende oder dafür relevante Daten wie etwa hinsichtlich der dazugehörigen Tat in der in § 9 Abs. 1 Nr. 5 vorgesehenen DNA-Analyse-Datei gespeichert werden können, wo sie dann gemäß § 16 Abs. 5 Nr. 1 BKAG weiterverarbeitet werden dürfen. Ein Großteil der 836.000 Personen, die in der Datei gespeichert sind, dürfte auf § 81g StPO beruhen, der nunmehr aber auch von präventiven Landesregelungen flankiert wird. Daneben liegen zusätzlich 386.000 Spuren in der Datenbank vor (Stand: April 2022). In der DAD kann bei Spurenfunden dann auf Direkttreffer abgeglichen werden, ein Abgleich mit Beinahetreffern war hingegen 2018 weder möglich noch geplant.[944] Die polizeiliche Nutzung von Beinahetreffern („familial searching") bleibt somit zunächst auf DNA-Reihenuntersuchungen beschränkt (§ 81h Abs. 1 StPO), wobei aber die gegenwärtige Ausweitung von genetischen Ermittlungsbefugnissen der Polizei auch der DAD und der in ihr gespeicherten Daten einen weiteren Bedeutungszuwachs verschaffen könnte.[945]

940 https://www.bka.de/DE/UnsereAufgaben/Ermittlungsunterstuetzung/Erkennungsdienst/erkennungsdienst_node.html#doc19616bodyText3 (Stand: 01.10.2023).
941 *Arzt* in *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch des Polizeirechts, G. Rn. 1174.
942 Siehe dazu etwa *Held,* Intelligente Videoüberwachung.
943 *Arzt* in *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch des Polizeirechts, G. Rn. 1174.
944 BT-Drs. 19/4354, 6.
945 Siehe dazu (auch in anderen Staaten) *Butz* NK 33 (2021), 316.

ff) Delikts- und phänomenbezogene Dateien

Neben diesen integralen Bestandteilen von INPOL zeichnet sich nun schon seit einigen Jahrzehnten das Bedürfnis einer zumindest teilweisen Durchbrechung der logischen Trennung der Datenbestände ab, die durch die Zuordnung zu Datengruppen eingezogen werden. Mit einem zunehmenden Vorfeldfokus der Polizei, der sich als wesentliches Merkmal der auf Prävention bedachten Sicherheitsgesellschaft materialisiert hat, reicht es immer weniger aus, anlässlich eines Akts abweichenden Verhaltens zu prüfen, ob die in Frage stehende Person bekannt sein könnte. Mit Ausweitung und Intensivierung des polizeilichen Blicks im Namen der Prävention wird die Produktion von Wissen aus der Verknüpfung von datenförmig vorhandenen Informationen immer wichtiger. In der technischen Infrastruktur des polizeilichen Informationswesens spiegelt sich dieser Wandel in delikts- und phänomenbezogenen Dateien wider, die bestimmte soziale Interaktionsfelder, denen Devianz zugeschrieben wird, abzubilden versuchen.

Zu diesem Zweck wurden über die Jahre verschiedene Verbunddateien in INPOL eingerichtet, in denen der Datenaustausch zu verschiedenen Bereichen[946] – „Innere Sicherheit", „Gewalttäter Links", „Gewalttäter Rechts", „Gewalttäter Sport", „politische Ausländerkriminalität" oder auch „APOK" (Aufklärung / vorbeugende Bekämpfung von Straftaten der Organisierten Kriminalität) – stattfindet. Daneben gibt es auch deliktsspezifischere Dateien, wie Falldateien zum „Rauschgift", „Falschgeld" oder „ViCLAS" (Violent Crime Linkage Analysis System) für Gewaltdelikte.[947]

Die in diesen Informationsbeständen stattfindenden Datenverarbeitungen müssen durchweg als intensive Eingriffe gehandelt werden, da beim Kontakt der Betroffenen mit der Polizei regelmäßig eine alerte Reaktion der jeweiligen Polizist:innen ausgelöst werden soll und wird, was mit weiteren polizeilichen Maßnahmen verbunden sein kann.[948] Dem wird der Grad der rechtlichen Regulierung dieser informationellen Instrumente nur begrenzt gerecht. Rechtsgrundlage für fast alle diese Verbunddateien ist § 8 BKAG a.F., wobei stets eine Konkretisierung von Dateizweck und -funktionalitäten durch Errichtungsanordnungen erfolgt. Über IfSG-Anfragen konnten einige dieser nicht-öffentlichen Dokumente der Öffentlichkeit zugänglich

946 Kritisch zu den Gewaltäterdateien *Ruch/Feltes* NK 17 (2016), 62.
947 Siehe dazu die Übersicht bei BT-Drs. 17/14735, S. 9 ff.
948 *Arzt* in *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch des Polizeirechts, G. Rn. 1257.

gemacht werden, womit Einblicke in die Rahmenbedingungen der Dateien möglich werden.[949] Auch die Errichtungsanordnungen begrenzen das polizeiliche Informationshandeln nur bedingt. So können in Phänomenbereichen etwa Daten zu Kontakt- und Begleitpersonen zum Zwecke der Straftatenverhütung oder -vorsorge gespeichert werden, was eine weitreichende, prinzipiell nur von polizeilicher Definitionsmacht begrenzte Befugnis ist, die es im Übrigen schon vor der großen Verrechtlichung polizeilichen Informationshandelns in dieser im Wesentlichen unbeschränkten Form gegeben hat.[950] Zudem ist über die Möglichkeit der Freitextfeldspeicherung der Weg offen für eine ungefilterte Abbildung polizeilicher Interpretationen und Zuschreibungen in den polizeilichen Informationsbeständen. Jahrelang wurden die Verbunddateien zudem ohne die konkretisierende Rechtsgrundlage der BKADV betrieben, die erst 2010 nach einem dreizehnjährigen Disput über deren rechtliche Erforderlichkeit im Anschluss an die Novellierung des BKAG 1997 erlassen wurde.[951] Allerdings verblasst die Bedeutung der Dateienstruktur mit dem gegenwärtigen Wandel des polizeilichen Informationswesens, wie er durch Projekte wie PIAV oder *Polizei 2020*[952] angestoßen wird. Damit verliert zwar die konkrete Frage nach den rechtlichen Rahmenbedingungen dieser Dateien an Relevanz. Das Problem präsentiert sich aber angesichts der Frage nach den normativen Konturen der geplanten technologischen Infrastruktur mit mindestens ebenso großer Dringlichkeit in neuem Gewand.

gg) Zusätzliche Datenakkumulation in INPOL durch Hinweise

Neben den Dateistrukturen, in denen sich dateizweckspezifische Daten ansammeln, hat sich in der polizeilichen Informationsverarbeitung über die Zeit hinweg ein Hinweissystem etabliert. Im Rahmen dieses Systems können zu bereits gespeicherten Personen – aus Perspektive der Polizei – sinnvolle Ergänzungen in die Informationsbestände aufgenommen werden. So werden polizeiliche Beobachtungen der Realität, vor allem aber auch

949 Siehe dazu und zum Folgenden etwa die Errichtungsanordnung zur Datei „Gewalttäter Links", https://fragdenstaat.de/dokumente/5281-ifg_bka_pmk-links_eao/ (Stand: 01.10.2023).

950 Siehe zur informationellen Durchleuchtung der sogenannten „Sympathisantenszene" im Zuge des RAF-Terrors oben S. 126 ff.

951 Siehe dazu *Arzt* Neue Juristische Wochenschrift 2011, 352.

952 Zu beiden Entwicklungen unten S. 268 ff.

Deutungen und Interpretationen derselben in Form sogenannter personengebundener (PHW) oder ermittlungsunterstützender (EHW) Hinweise, Teil der Datenakkumulationen zu einzelnen Personen. Das mag den Datendoubles[953] mehr Kontur und Greifbarkeit für die polizeiliche Arbeit verschaffen. Das Labeln mit solchen Hinweisen ist aber immer auch verkürzend und reproduziert eingeübte und stabilisierte Bilder, die die Polizei von ihren „Gegenübern" hat.

Die Rechtsgrundlage zur Verarbeitung für PHW und EHW ist nunmehr in § 16 Abs. 6 Nr. 1 und 2 BKAG geregelt. Die Hinzuspeicherung von Hinweisen kann anlasslos erfolgen, was mit Blick auf den Verhältnismäßigkeitsgrundsatz problematisch ist,[954] auch wenn § 16 Abs. 6 Nr. 1 BKAG sich auf Personen nach § 18 Abs. 1 BKAG bezieht.[955] Insbesondere § 16 Abs. 6 Nr. 2 BKAG ermöglicht zudem eine kaum eingegrenzte Speicherung von Hinweisen – auch über „Dritte", wenn auch zu deren Schutz – nach polizeilichem Ermessen und wird deshalb auch als aufgrund von Unverhältnismäßigkeit für verfassungswidrig gehalten.[956]

PHW werden in der BKADV in § 2 Abs. 1 Nr. 15 konkretisiert: Es sind solche Hinweise, die dem Schutz des Betroffenen dienen wie „Freitodgefahr" oder die die Eigensicherung der ermittelnden Bediensteten bezwecken wie „bewaffnet", „gewalttätig", „Explosivstoffgefahr". Dabei handelt es sich allerdings nur um beispielhafte Nennungen von Hinweisen. In der polizeilichen Praxis werden so etwa Hinweise verwendet wie: BEWA, Bewaffnet; GEWA, Gewalttätig; AUSB, Ausbrecher; ANST, Ansteckungsgefahr; GEKR, Geisteskrank; BTMK, BtM-Konsument; FREI, Freitodgefahr; PROS, Prostitution; VEMO, Straftäter verbotener militanter Organisation/Vereinigung/Partei/Gruppe; REMO, Straftäter rechtsmotiviert; LIMO, Straftäter linksmotiviert; AUMO, Straftäter politisch motivierter Ausländerkriminalität; EXPL, Explosivstoffgefahr; SEXT, Sexualtäter; HWAO, Häufig wechselnder Aufenthaltsort.[957] Deren Festlegung und die Kriterien für ihre Vergabe sind in einem nicht-öffentlichen PHW-Leitfaden niedergelegt.[958] Zur Vergabepraxis ist quasi nichts bekannt. Es soll bei Vergabe von Hin-

953 Siehe zu diesem Begriff bereits oben S. 55 ff.
954 *Bäcker*, A-Drs. 18(4)806 D, S.16.
955 *Eichenhofer* in *Barczak* (Hrsg.), BKAG, § 16 Rn. 21.
956 So *Bäcker*, Schriftsatz der Verfassungsbeschwerde im Verfahren 1 BvR 1160/19, S. 62 f., abrufbar unter: https://freiheitsrechte.org/home/wp-content/uploads/2019/10/2019-05-21-BKA-Gesetz-VB-anonymisiert.pdf (Stand: 01.10.2023).
957 ULD, Tätigkeitsbericht 2010, S. 41.
958 WD 3 - 3000 - 063/19, S. 6.

weisen eine Einzelfallprüfung mit Blick auf Geeignetheit, Erforderlichkeit und Angemessenheit erfolgen.[959] Allerdings gibt es abweichende Praktiken bei der Verwendung bestimmter Hinweise,[960] was eine länder- und polizeispezifische Informationspraxis impliziert und auf die Grenzen normativer Steuerbarkeit polizeilicher Informationspraktiken durch opake Richtlinien hindeutet. So gibt es beispielsweise zusätzlich zu den oben genannten PHW in Sachsen noch JUNI, Jugendlicher Intensivtäter; LAST, Land- oder Stadtstreicher; SGRB, Sogenannter Reichsbürger; DROG, Konsument harter Drogen oder auch SPRY, Sprayer.[961] Solche länderspezifische Hinweise sind vor allem dann nicht unproblematisch, wenn Hinweise, wie es regelmäßig geschieht, aus den Ländern heraus in INPOL-Z gespeichert werden. Auf diese Weise können verschiedene Hinweispraktiken zu Diskrepanzen in der Kategorisierung führen, was unter Gerechtigkeitsgesichtspunkten, aber auch mit Blick auf die Richtigkeit von Daten – sofern man davon bei den stark interpretatorisch geprägten PHW überhaupt sprechen kann – kritikwürdig ist. Rechtlich einschlägig für viele der Hinweise oder der ihnen zugrundeliegenden Daten wäre auch § 48 BDSG, der die Vorgaben der JI-Richtlinie zur Verarbeitung besonderer Kategorien personenbezogener Daten umsetzen soll. Inwieweit das Kriterium der unbedingten Erforderlichkeit der Verarbeitung sowie die Garantien für die Rechtsgüter der Betroffenen eingehalten wurde bzw. umgesetzt worden sind, ist nicht bekannt – beides erscheint indessen mit Blick auf die langjährige Hinweispraxis zweifelhaft.

Zusätzlich sind PHW inhaltlichen Bedenken ausgesetzt: Hinweise wie „Häufig wechselnder Aufenthaltsort" lassen zudem vermuten, dass sich dort diskriminierende Polizeipraktiken gegenüber Minderheiten wie Sinti:zze und Rom:nja lediglich nominal verändert fortschreiben.[962] Noch 2017 wurde aber auch von ganz expliziten Hinweisen wie „Sinti", „Roma" oder sogar „Zigeuner" berichtet.[963] Die Problematik, dass es sich bei „HWAO" zudem um im Wesentlichen legales Verhalten handelt, trifft auch auf Hinweise wie „Ansteckungsgefahr", „Geisteskrank" oder „Prostitution" zu. Durch eine solche Gefahrenwahrnehmung, die einen prüfenden Blick auf legales Ver-

959 Hamburger Bürgerschaft-Drs. Drucksache 20/13106, S. 2.
960 Hamburger Bürgerschaft-Drs. Drucksache 20/13106, S. 1.
961 Sächs. LT-Drs. 6/16086, Anlage 1.
962 Ausführlicher dazu *Töpfer*, (Dis-)Kontinuitäten antiziganistischen Profilings im Zusammenhang mit der Bekämpfung „reisender Täter", Forschungsbericht zur Vorlage bei der Unabhängigen Kommission Antiziganismus, 2020.
963 *Mayer* Süddeutsche Zeitung v. 17. Juni 2021.

halten institutionalisiert, werden mehr Teile des Sozialen unter polizeiliche Aufsicht gestellt, als durch einen reinen Fokus auf strafrechtlich relevantes Verhalten.[964] Dass PHW zudem Interaktionen zwischen gespeicherten Personen und der Polizei eskalativ vorstrukturieren können, legt der polizeiliche Umgang mit psychisch kranken und gestörten Personen nahe, bei dem es in der Vergangenheit immer wieder auch zum Tod der Betroffenen kam.[965] Ähnliche Wirkungen dürften alle PHW haben, die eine gewisse personeninhärente Gefährlichkeit implizieren.

Ermittlungsunterstützende Hinweise werden in § 2 Abs. 1 Nr. 16 BKADV konkretisiert: Es handelt sich um solche, die Ermittlungsunterstützung dienen wie „Sexualstraftäter", „Straftäter politisch links motiviert" oder „Straftäter politisch rechts motiviert". Auch hierbei handelt es sich nur um Beispiele. Verwendet werden Hinweise wie BTKU, BTM-Handel (Kurier); BTMA, BTM-Handel (Abnehmer); BTMH, BTM-Handel (Händler); BTML, BTM-Handel (Lieferant); BTMP, BTM-Handel (Produzent); EINB, Einbrecher; GEFB, Gefährdung (Brandstifter); GEFH, Gefährdung (Häusliche Gewalt); GEFS, Gefährdung (Stalker); IDDO, Identität (Dokumentenbeschaffer); IDEN, Identität; IDPA, Identität (Passüberlasser); INTS, Intensivtäter (Sportveranstaltungen); JIHA, Reisender in/aus Jihad-/Krisengebiet; KFZD, Kraftfahrzeug-Dieb; MENA, Menschenhandel (Anwerber); MENS, Menschenhandel (Schleuser); MENV, Menschenhandel (Vermieter); MENZ, Menschenhandel (Zuhälter); PMKA, Politisch motivierter Straftäter (PMK -ausländische Ideologie-); PMKL, Politisch motivierter Straftäter (PMK -links-); PMKN, Politisch motivierter Straftäter (PMK -nicht zuzuordnen-); PMKR, Politisch motivierter Straftäter (PMK -rechts-); PMRE Politisch motivierter Straftäter (PMK -religiöse Ideologie-); REIB, Reichsbürger/Selbstverwalter; REIT, Reisender Täter; ROCK, Rocker; SCHM, Schmuggler; SEXT, Sexualtäter; TDIE, Trick-/Taschendieb[966] oder neuerdings auch CLAN, Clankriminalität und CLAN-UMFELD, Clankriminalität Umfeld.[967]

Bei diesen EHW sind Überschneidungen mit einigen PHW zu beobachten (etwa REIT und HWAO). Bei den EHW ist indessen (noch) weniger deutlich, welchem polizeilichen Zweck die Hinweise dienen sollen. So

964 *Kretschmann* in Legnaro/Klimke (Hrsg.), Kriminologische Diskussionstexte II, 139 (155).
965 *Derin/Singelnstein,* Die Polizei: Helfer, Gegner, Staatsgewalt, 152 f.
966 Diese Hinweise werden ersichtlich aus Sächs. LT-Drs. 6/18032, Anlage 1.
967 Bln. AH-Drs. 18/24342, S. 1.

findet sich beispielsweise die Ansicht, EHW seien „Hinweise auf Besonderheiten einer natürlichen Person, die primär dazu geeignet sind, einen polizeilichen Kontext zu verdeutlichen, polizeiliches Handeln zielgerichteter zu steuern bzw. zu unterstützen, oder die dem Schutz Dritter dienen. Sie sind darüber hinaus auch geeignet, Datenbestände für Ermittlungen zu kennzeichnen bzw. zu selektieren."[968] Da auch die EHW anhand einer nicht-öffentlichen Richtlinie vergeben werden, ist diese Form der Datenverarbeitung aufgrund der schwächer ausgeprägten Zweckbestimmung der EHW im Vergleich zu den PHW problematisch, ein Zustand, der durch die anscheinend geplante Umwandlung von PHW in EHW[969] verschärft wird. Insofern ist *Arzt* zuzustimmen, der anlässlich der EHW von „eine[r] rechtlich schwer abzugrenzende[n] und normenklar einzuhegende[n] Gemengelage" spricht.[970]

hh) Der Polizeiliche Informations- und Analyseverbund

Eine besondere und jüngere Entwicklung des polizeilichen Informationswesen in seinen verbundmäßigen Ausformungen stellt das Projekt des Polizeilichen Informations- und Analyseverbundes (PIAV) dar. PIAV kann als Antwort auf eine empfundene Trägheit des polizeilichen Informationswesens gelesen werden. Die eher starre Struktur konnte auch durch die verschiedenen delikts- und phänomenbezogenen Dateien nicht in einer befriedigenden Weise dynamisiert werden, sodass als Lösung der PIAV konzipiert wurde, in welchem übergreifende, auf bestimmte Kriminalitätsphänomene bezogene Dateien – nach Relevanzprüfung – einschlägige Informationen und personenbezogene Daten zusammenfassen.[971] Es handelt sich nach Angaben des Bundesministeriums des Innern um einen Informationsverbund zur länderübergreifenden Kriminalitätsanalyse, der aus einer operativen und einer strategischen Komponente besteht und technisch durch das BKA bereitgestellt wird. Zweck des Verbundes ist es, einen medienbruchfreien und durchgängigen Informationsaustausch zwischen den Teilnehmern zu ermöglichen, um Tat-Tat, Tat-Täter- und Täter-

968 BT-Drs. Drucksache 18/5659, S. 18.
969 BT-Drs. Drucksache 18/5659, S. 18.
970 *Arzt* in *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch des Polizeirechts, G. Rn. 1248.
971 BT-Drs. 16/12600, S. 56.

Täter-Zusammenhänge delikt- und phänomenübergreifend zu erkennen.[972] Strukturell ähnelt der PIAV dem INPOL-Verbund: Der Informationsverbund besteht aus dem PIAV-Zentralsystem und den 19 Teilnehmersystemen von Bund (Bundeskriminalamt, Zollkriminalamt und Bundespolizei) und Ländern. PIAV gilt als „das derzeit bedeutsamste föderale Software- und Organisationsentwicklungsvorhaben zur Fortentwicklung der Polizeiarbeit in Deutschland" und „hat den Anspruch, die Auswertungs- und Ermittlungsarbeit im Verbund zu stärken und die Informationszusammenarbeit der Polizeien des Bundes und der Länder auf eine technisch, fachlich und organisatorisch zeitgemäße Basis zu stellen."[973]

Neben der strukturellen Verbesserung des Informationsflusses im polizeilichen Informationswesen soll PIAV auch der Verbesserung des nicht mehr ganz zeitgemäßen Kriminalpolizeilichen Meldedienstes (KPMD) dienen.[974] Dieses alte Informationsinstrument[975] soll dafür sorgen, dass Polizeidienststellen bei Delikten, bei denen der Verdacht auf überregionale Relevanz besteht, Meldung an ihr jeweiliges Landeskriminalamt machen können, das dann wiederum nach Prüfung der Relevanz an das Bundeskriminalamt weiterleiten kann, wo die Daten dann gesammelt zur Verfügung gestellt werden können.[976] Vor allem diese Meldewege sowie die häufig notwendigen Mehrmalerfassungen, die durch den KPMD bedingt werden, sollen durch den PIAV wesentlich verbessert werden. Die Verbundstruktur des PIAV soll hier Abhilfe schaffen, indem die Daten zentral gesammelt und dann einem „transbehördlichem Zugriff" freigegeben werden.[977] Im Anschluss sollen die Daten über eine gemeinsame webbasierte Oberfläche durchsuchbar sein.[978] In der operativen Komponente des PIAV (PIAV-O) werden so Module, ähnlich den dadurch gleichfalls abzulösenden alten INPOL-Falldateien, zu bestimmten Phänomenbereichen eingerichtet. So sind die Bereiche "Waffen- und Sprengstoffkriminalität", „Rauschgiftkriminalität" und „Gewaltdelikte/gemeingefährliche Straftaten"

---

972 BT-Drs. 19/15346, S. 8.
973 Bundesministerium des Inneren, White Paper Polizei 2020, S. 28.
974 https://police-it.net/category/polizeiliche-informationssysteme/polizeiliche-bund-laender-informationssysteme/piav-polizeilicher-informations-und-analyseverbund (Stand: 01.10.2023).
975 Siehe dazu bereits oben S. 112 ff.
976 Amtsblatt für Brandenburg – Nr. 9 vom 28. Februar 2001, S. 190.
977 *Egbert* in Hunold/Ruch (Hrsg.), Polizeiarbeit zwischen Praxishandeln und Rechtsordnung, 77 (85).
978 *Burczyk* Bürgerrechte & Polizei (CILIP) 2020, 16 (19).

seit 2016 bzw. 2018 aktiv. Die Umsetzung von „Cybercrime", „Dokumentenkriminalität", „Schleusung/Menschenhandel/Ausbeutung", „Sexualdelikte" und „Eigentumskriminalität/Vermögensdelikte" erfolgte 2020.[979] Weitere Komponenten, wie „Politische motivierte Kriminalität", „Organisierte Kriminalität" und „Wirtschaft- und Umweltkriminalität" sollten 2021 in den Wirkbetrieb gehen.[980] Diese Komponenten werden über Schnittstellen mit den Fall- bzw. Vorgangsbearbeitungssystemen[981] der jeweiligen Polizeien mit den jeweils freigegebenen Daten gespeist.[982]

Die operative Komponente ergänzen soll PIAV-S, also die strategische Nutzung der Daten im PIAV. PIAV-S soll dabei helfen, Schwerpunkte zu setzen und die polizeilichen und politischen Führungs- und Entscheidungsebenen zu beraten. Dafür soll es ausgewählte Personen-, Fall- und Sachdaten aus den Vorgangs- oder Fallbearbeitungssystemen der Polizeibehörden bereitstellen und eine tagesaktuelle, orts- und personenbezogene Zählung von Straftaten ermöglichen. Da die dabei verwendeten Daten nach Ansicht des Bundesbeauftragten für Datenschutz und Informationssicherheit nur pseudonymisiert sind und somit weiterhin Personenbezug bestünde, würde die Verarbeitung von Daten in PIAV-S derzeit ohne eigentlich erforderliche Rechtsgrundlage erfolgen.[983]

Überhaupt werden die Konturen des PIAV, soweit bisher ersichtlich, vor allem durch die konzeptuellen Grundlagen und tatsächliche technische Umsetzungsbemühungen gezogen. Worauf der Verbund rechtlich fußt, ist nicht eindeutig klar. Denkbar wäre es, dass PIAV einen rechtlichen Ankerpunkt ebenfalls in § 29 BKAG hat, da INPOL durch den neuen Verbund eine gewisse Ergänzung erfahren soll. Auch eine Errichtungsanordnung, wie sie zumindest für andere Verbundsysteme vorliegt, scheint für PIAV jedoch zu fehlen. In einer IfSG-Anfrage wird vom Bundeskriminalamt im Zusammenhang mit PIAV auf die Errichtungsanordnungen der Quelldateien verwiesen.[984] Diese Errichtungsanordnungen können aber keinen, quasi mosaikhaften, rechtlichen Rahmen für den PIAV bilden. Die Bun-

979 BT-Drs. 19/27083, S. 7.
980 BT-Drs. 19/15346, S. 8.
981 Zu beiden Systemtypen siehe unten S. 254 ff. sowie S. 259 ff.
982 BT-Drs. 19/15346, S. 8.
983 BfDI, Tätigkeitsbericht für das Jahr 2020 (29. Tätigkeitsbericht), BT-Drs. 19/26681, S. 56 f.
984 https://fragdenstaat.de/anfrage/errichtungsanordnungen-im-zusammenhang-mit-polizei-analyse-system-piav/17859/anhang/20140613antwort-bka.jpg (Stand: 01.10.2023).

desregierung scheint davon auszugehen, dass die Teilkomponenten der PIAV-Teilnehmerbehörden im Wesentlichen auf polizeirechtliche Generalklauseln und die strafverfahrensrechtlichen Vorschriften (§§ 438 ff. StPO) zur Datenverarbeitung gestützt werden können.[985] Mit Blick auf die beabsichtigte informationelle Schlagkraft des PIAV sind diese angenommenen Rechtsgrundlagen nicht ausreichend. In der Folge scheint dieses so relevante neue Verbundsystem der Polizei gegenwärtig keine hinreichende Rechtsgrundlage aufzuweisen. Damit wird das hergebrachte Verhältnis zwischen technologischer Entwicklung des polizeilichen Informationswesens und diesbezüglicher legislativer Steuerungsverantwortung – erst entwickeln, dann rechtlich (unzureichend) abbilden – auch bei gegenwärtigen Entwicklungen für die Zukunft fortgeschrieben.

c) Vorgangsbearbeitungssysteme

Neben den bundesweiten polizeilichen Datennetzen wie INPOL und neuerdings auch PIAV haben die Bundes- und Landespolizeiorganisation zudem alle Vorgangsbearbeitungssysteme,[986] die jeweils absolut integraler Bestandteil des polizeilichen Informationshandelns und damit der polizeilichen Alltagsarbeit in den entsprechenden Organisationen sind. Die administrativ anmutende Bezeichnung dieser Informationssysteme ist dabei indessen nur teilweise treffend. Administrative Tätigkeiten wie die Vorgangsverwaltung und Dokumentation sind Teil des Funktionsumfangs, aber die Systeme dienen darüber hinaus vor allem der polizeilichen Aufgabenerfüllung im Allgemeinen, womit die beiden klassischen Zwecke der Strafverfolgung und Gefahrenabwehr mit ihren jeweiligen Unterfällen, aber auch die Strafverfolgungsvorsorge und Straftatenverhütung als Vorfeldbefugnisse angesprochen sind. Auch Ordnungswidrigkeiten werden mitunter in den Vorgangsbearbeitungssystemen untergebracht. Kurz: „In polizeilichen Vorgangsbearbeitungssystemen werden alle polizeilich relevanten Vorgänge

985 So zumindest für die PIAV-Komponenten der Bundespolizei, vgl. BT-Drs. 19/15436, S. 24 ff.

986 Zu den verschiedenen Bezeichnungen siehe *Arzt* in *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch des Polizeirechts, G. Rn. 1180 mwN; in ihren Funktionalitäten sollen sich diese hingegen nur wenig unterscheiden, siehe *Konferenz der Leiterinnen und Leiter der Archivverwaltungen des Bundes und der Länder*, Bewertung von Fachverfahren der Polizeibehörden von Bund und Ländern, Abschlussbericht, (Version 1.1, 2020), S. 5.

aus dem operativen Kernbereich der polizeilichen Arbeit erfasst und geführt."[987] Als Informationsinstrument weisen die Vorgangsbearbeitungssysteme also eine hohe Multifunktionalität auf, was sich auch in der von den Polizeien für sie angenommenen Rechtsgrundlagen[988] ablesen lässt: Neben den strafverfahrensrechtlichen Vorschriften der §§ 161, 163, 483 ff. StPO sind vor allem diejenigen Vorschriften in den jeweiligen Polizeigesetzen einschlägig, die die Datenverarbeitung generell zur Aufgabenerfüllung nach jeweiligem Polizeigesetz, aber auch zu anderen Zwecken wie der Dokumentation, der Vorgangsverwaltung, der Datenschutzkontrolle oder zur Datensicherung freigeben. Während hierbei auch Aspekte der Kontrolle polizeilichen Handelns angesprochen sind, ergibt sich mit einem Verweis auf die gesetzliche Aufgabenerfüllung und die regelmäßig in Polizeigesetzen enthaltene Befugnis, strafverfahrensrechtlich relevante Daten auch zum Zwecke der Gefahrenabwehr weiterzuverarbeiten, ein breites Feld an gesetzlich freigegebenem Datenumgang, das mit Blick auf das verfassungsrechtliche Zweckbindungsprinzip wenig beschränkt erscheint. Hinzu kommt, dass es keine die Systeme als technische Infrastruktur ordnenden Vorschriften gibt, wie es beispielsweise mit §§ 29 ff., 13 BKAG für INPOL-Z und INPOL-Bund der Fall ist.[989] Auch die Vorgangsbearbeitungssysteme werden aber mitunter noch weiter durch Errichtungsanordnungen konkretisiert.[990]

Um die Polizeien bei der Erfüllung ihrer Aufgaben zu unterstützen, sind in den Vorgangsbearbeitungssystemen in großem Umfang auch personenbezogene Daten über Beschuldigte, Geschädigte, Zeug:innen und andere, wie etwa Kontakt- und Anlasspersonen enthalten, wobei die unterschiedlichen Verarbeitungsvoraussetzungen zu beachten sind. Umfassend werden auch Sachverhalte zu Gefahrenabwehr- oder Strafverfolgungsvorgängen aufgenommen, sodass für sämtliche polizeilich erfassten Vorgänge der jüngeren Zeit zahlreiche Datenpunkte zu Personen, Objekten und

987 *Konferenz der Leiterinnen und Leiter der Archivverwaltungen des Bundes und der Länder*, Bewertung von Fachverfahren der Polizeibehörden von Bund und Ländern, Abschlussbericht, (Version 1.1, 2020), S. 11.

988 Siehe dazu beispielhaft die Rechtsgrundlagen von Nivadis, dem niedersächsischen Vorgangsbearbeitungssystem, NdsLT-Drs. 16/2770, Anlage 1, S. 3.

989 Ausnahme ist § 13c SOG LSA, der aber im Wesentlichen nur § 13 BKAG kopiert und damit vor allem einen normativen Anknüpfungspunkt für die INPOL-Land-Komponente aus Sachsen-Anhalt bietet dürfte, nicht hingegen für das dortigen Vorgangsbearbeitungssystem.

990 Siehe etwa Errichtungsanordnung ViVA, https://fragdenstaat.de/dokumente/3242-verfahren-zur-integrierten-vorgangsbearbeitung-und-auskunft/ (Stand: 01.10.2023).

Vorgängen vorliegen. Mit mehreren hundert festgelegten Datenkategorien[991] und zusätzlichen Freitext-Speicherungen[992] bieten die Vorgangsbearbeitungssysteme die Möglichkeit zur granularen Wirklichkeitserfassung. Mit ihrem breiten Informationsfundament bilden die Systeme auch eine Grundlage für Ermittlungsakten der Polizeien, wobei hier auch häufig zusätzlich noch mit Fallbearbeitungssystemen[993] gearbeitet wird. Die vorgangsbezogene Struktur der Systeme wird in einem solchen Fall durch eine parallele personenbezogene Struktur ergänzt, womit die Führung der (elektronischen) Kriminalakte nach der bereits erwähnten KpS-Richtlinie im selben System ermöglicht wird.[994] Geht bereits diese Funktionalität streng genommen über die reine Vorgangsbearbeitung hinaus,[995] so vereinen einige Vorgangsbearbeitungssysteme unter einer Oberfläche neben der Vorgangsbearbeitung noch weitere Komponenten, wie INPOL-Land, und verzahnen beides dann mit Schnittstellen zu anderen Informationssystemen wie INPOL-Z, staatsanwaltschaftlichen Systemen, Fallbearbeitungssystemen und sonstigen Datenspeichern, die zu polizeilichen Analyse-, Dokumentations- und Informationszwecken genutzt werden können.[996] Die Verarbeitung von personenbezogenen Daten zur Aufgabenerfüllung in den polizeilichen Vorgangsbearbeitungssystemen kann vor dem Hintergrund der Vielfalt möglicher Datenpunkte als zumindest potentiell sehr eingriffsintensiv eingestuft werden. Umso mehr gilt dies in Fällen, in denen wiederum „besondere Kategorien personenbezogener Daten" betroffen sind, denn auch die Vorgangsbearbeitungssysteme enthalten das zuvor besprochene Hinweissystem[997] und arbeiten darüber hinaus mit festgelegten Da-

991 NdsLT-Drs. 16/2770, Anlage 1, S. 4 ff.

992 *Konferenz der Leiterinnen und Leiter der Archivverwaltungen des Bundes und der Länder*, Bewertung von Fachverfahren der Polizeibehörden von Bund und Ländern, Abschlussbericht, (Version 1.1, 2020), S. 11.

993 Dazu sogleich unter S. 259 ff.

994 *Konferenz der Leiterinnen und Leiter der Archivverwaltungen des Bundes und der Länder*, Bewertung von Fachverfahren der Polizeibehörden von Bund und Ländern, Abschlussbericht, (Version 1.1, 2020), S. 11.

995 So *Konferenz der Leiterinnen und Leiter der Archivverwaltungen des Bundes und der Länder*, Bewertung von Fachverfahren der Polizeibehörden von Bund und Ländern, Abschlussbericht, (Version 1.1, 2020), S. 11.

996 Siehe Errichtungsanordnung ViVA, S. 1 f., https://fragdenstaat.de/dokumente/3242-verfahren-zur-integrierten-vorgangsbearbeitung-und-auskunft/ (Stand: 01.10.2023).

997 Siehe dazu oben S. 247 ff.

tenpunkten, die Kategorien des § 48 BDSG berühren, etwa im Kontext von Staatschutzdelikten oder von als ausländisch klassifizierten Täter:innen.[998]

Neben den originären polizeilichen Zwecken dienen die Vorgangsbearbeitungssysteme, wie bereits erwähnt, auch noch weiteren, eher administrativen Zwecken. Ist die Aufgabenerfüllung einmal abgeschlossen, sollten die dazu verarbeiteten Daten nicht mehr zu repressiv- oder präventivpolizeilichen Zwecken zur Verfügung stehen. Nach einem Statuswechsel sollten die Vorgänge in einen durch technisch-organisatorische Maßnahmen abgegrenzten Bereich gelangen, der nicht mehr ohne Weiteres für die alltägliche Informationsarbeit zur Verfügung steht, sondern nur noch für Zwecke der Vorgangsverwaltung, Dokumentation oder Datenschutzkontrolle genutzt werden kann.[999] Vorgangsverwaltung meint dabei das Auffinden von Vorgängen zur Dokumentation und Überprüfung, dass polizeiliches Handeln rechtmäßig war, insbesondere im Zusammenhang mit verwaltungsgerichtlichen Klagen.[1000] Allerdings gestatten die Polizeigesetze regelmäßig einen Durchbruch dieser eher archivisch-administrativen Zweckbindung zu Zwecken der Aufgabenerfüllung, also für Gefahrenabwehr und Strafverfolgung. In der Regel erfolgt allerdings eine Beschränkung der neuen alten Zwecke auf Maßnahmen, die dem Schutz von Leib, Leben oder Freiheit bzw. der Verhütung schwerer, in der Regel „terroristischer" Straftaten dienen. Dabei ist die Möglichkeit, die Daten wieder zur – wenn auch im Umfang beschränkten – originären polizeilichen Aufgabenerfüllung verarbeitbar zu machen, nicht trivial: So speichert etwa die Bundespolizei in ihrem Aktennachweis etwa 40 Millionen Datensätze zu mehr als 830.000 Personen.[1001] Wenn solche Daten, die grundsätzlich nur noch zu Zwecken der Vorgangsverwaltung und Dokumentation verarbeitet werden dürfen, für eine Personensuche in den polizeilichen Systemen genutzt werden können, konterkariert das die bestehende Zweckbindung in erheblichem Ausmaß – das gilt auch, wenn nur sichtbar gemacht werden kann, dass die betroffene Person in irgendeiner Weise mit bestimmten Sachverhalten in Verbindung steht, weil die Daten im Wesentlichen gesperrt sind. Denn bereits hieraus ergeben sich Anhaltspunkte für polizeiliches Handeln, zumal gesperrte Daten mitunter – je nach technischer Ausgestaltung – über zweckdurchbre-

998 NdsLT-Drs. 16/2770, Anlage 1, S. 4 ff.
999 NdsLT-Drs. 16/2770, Anlage 1, S. 2.
1000 *Arzt* in *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch des Polizeirechts, G. Rn. 1192.
1001 BT-Drs. 19/15346, S. 23.

chende Maßnahmen wieder sichtbar gemacht werden können.[1002] In der Vergangenheit wurde aber auch schon von Vorgangsbearbeitungssystemen berichtet, die diese Trennung überhaupt nicht kannten, was eine unrechtmäßig zweckdurchbrechende Verarbeitung durch die Polizei befördert.[1003] Auch zeitlich zwecküberschreitende Verarbeitungen gibt es häufig in den Vorgangsbearbeitungssystemen, was nicht zuletzt an der Vielfalt der möglichen Verarbeitungszwecke liegt. Zwar gibt es sogenannte Aussonderungsprüffristen, nach denen überprüft werden muss, ob bestimmte Daten noch benötigt werden – das sind grundsätzlich fünf Jahre bei Erwachsenen.[1004] Allerdings fehlt es einerseits mitunter an klaren Regelungen zu solchen Prüf- und damit potenziell auch Löschfristen[1005] und andererseits können die damit beabsichtigten temporalen Begrenzungen der Speicherung im Vorgangsbearbeitungssystem durch sogenannte Mitziehautomatiken ausgehebelt werden. Dabei handelt es sich um Regelungen, die bei jeder Speicherung eines neuen Datenpunkts – etwa auch im Rahmen der Anzeige eines Bagatelldelikts – zu einer Person die Speicherfrist hinsichtlich aller gespeicherter Daten wieder auf Anfang setzt.[1006] Diese – treffend auch als „Jungbrunnen" bezeichnete – Regelung begünstigt strukturell ein zunehmendes Anwachsen der Datenbestände der Polizeien, was insgesamt im Widerspruch zu den normativen Postulaten von Erforderlichkeit, Datensparsamkeit und Datenminimierung steht.[1007]

Zudem verkomplizieren die Multifunktionalität der mit den Vorgangsbearbeitungssystemen verknüpften Quell- und Zielsysteme und die Vielfältigkeit der sich in den Systemen überlagernden Zwecke die Einhaltung dieser rechtlichen Vorgaben und machen aufwändige technisch-organisatorische Maßnahmen erforderlich, mit denen die Daten und ihre Verarbeitung auf ihre Rechtmäßigkeit hin überprüft und gegebenenfalls gelöscht werden können. Die wenigen, aber dafür häufig breiten und unübersichtlichen

1002 OVG Lüneburg 11. Senat, Urteil vom 11.07.2017, 11 LC 222/16, ECLI:DE:OVGNI:2017:0711.11LC222.16.00, Rn. 38.

1003 So der BfDI zum Vorgangsbearbeitungssystem der Bundespolizei, 26. Tätigkeitsbericht 2015/2016, S. 133 f. und auch zum System des Bundeskriminalamts, 28. Tätigkeitsbericht 2019, S. 55 f.

1004 Siehe dazu etwa die Erläuterung des Verfahrens durch den TLfDI, 11. Tätigkeitsbericht zum Datenschutz: öffentlicher Bereich 2014/2015, S. 231.

1005 BfDI, 28. Tätigkeitsbericht 2019, S. 56.

1006 *Bundesbeauftragte für Datenschutz und Informationssicherheit*, A-Drs. 18(4)806 A, S. 13 ff.

1007 So zutreffend *Arzt* in *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch des Polizeirechts, G. Rn. 1194.

Normen, die die Vorgangsbearbeitung regeln sollen, führen also zu einem nur wenig regulierten Datenumgang in den Vorgangsbearbeitungssystemen. Vor dem Hintergrund der in ihnen gespeicherten Datenvolumina[1008] gibt dieser Umstand Anlass zu Besorgnis, insbesondere mit Blick auf das zu erwartende weitere Anwachsen der Datenbestände des polizeilichen Informationswesens und auf die vielfältigen schnittstellenbasierten Vernetzungen der Vorgangsbearbeitungssysteme mit den übrigen Teilen des Informationswesens.[1009]

d) Kriminalpolizeiliche Informationsinstrumente: Strafverfolgungsdateien und Fallbearbeitungssysteme

Neben den bisher beschriebenen Verfahren und Systemen, die prinzipiell polizeirechtlich fundiert sind, existieren auch informationstechnische Instrumente, die in erster Linie der kriminalpolizeilichen und damit strafverfahrensrechtlichen Aufgabenerfüllung dienen.

Nach den Kriminalakten ist die nächstgrößte informationstechnische Einheit der Strafverfolgungsbehörden die Strafverfahrensdatei gem. § 483 ff. StPO. Die Grundnorm des § 483 StPO gibt dafür die Errichtung von Dateien recht breit – für Zwecke des Strafverfahrens – und niedrigschwellig – soweit es für diese erforderlich ist[1010] – frei, womit ein flexibles Informationsinstrument für die Strafverfolgungsbehörden, also auch die Polizei, besteht. Auch hinsichtlich der Datentypen besteht keinerlei Beschränkung. Der Gesetzgeber hatte auf eine solche Festlegung mit Blick auf die polizeiliche und auch staatsanwaltschaftliche Praxis bewusst verzichtet, wobei er davon ausging, dass die möglichen und erforderlichen Daten sowie die Spannbreite der notwendigen Datenfelder im Hinblick auf die jeweiligen

1008 So waren etwa in Sachsen 2018 9,1 Millionen Personen in 3,4 Millionen Datensätzen erfasst, SächsLT-Drs. 6/11770, Anlage, S. 1. In Niedersachsen waren 2010 3,8 Millionen Personen im dortigen Informationssystem erfasst, NdsLT-Drs. 16/2770, Anlage 1, S. 3. Diese Zahlen sind umso frappierender, wenn man bedenkt, dass die Vorgangsbearbeitungssysteme „landesbezogen" und „auf das Land […]" beschränkt sein sollen, a.a.O., S. 1.

1009 Siehe dazu etwa S. 439 ff.

1010 Gemeint ist hier die Erforderlichkeit der Verarbeitung in Dateisystemen, also eine Erforderlichkeit, die über die zur Datenverarbeitung in herkömmlicher Weise – regelmäßig gegenwärtig noch in Akten – hinausgeht. Das kann etwa aus Gründen der Wirtschaftlichkeit oder sonstigen Effizienz der Fall sein, vgl. Weßlau/Deiters in *J. Wolter* (Hrsg.), SK-StPO, § 483 Rn. 7.

fall- bzw. deliktspezifischen Bedürfnisse der speichernden Stelle sehr unterschiedlich sind, weswegen eine gesetzliche Eingrenzung nicht möglich sei.[1011] Insofern kann eine Kriminalakte komplett in einer solchen Datei abgebildet werden.[1012] Einschränkungen können und sollen sich aber für einzelne Dateien aus ihren jeweiligen Errichtungsanordnungen gem. § 490 StPO ergeben.[1013] Nichtsdestotrotz besteht hier mangels einer der BKADV vergleichbaren datenkonkretisierenden Verordnung eine normative Leerstelle, die vor allem durch die faktischen Datenverarbeitungspraktiken der Strafverfolgungsbehörden gefüllt werden dürfte.

In der Praxis verbreitete Dateitypen sind etwa solche zur Spurendokumentation, sogenannten „Spudok"-Dateien, in großen Verfahren. In Wirtschaftsstrafverfahren kommen zur Auswertung von Bilanzen, Buchhaltung und Finanzfluss eines Wirtschaftsunternehmens sogenannte intelligente Programme zur Anwendung, die Analysen und Verknüpfungen aufgrund einprogrammierter Suchkriterien vornehmen. Dateien können auch maßnahmenspezifisch etwa zur Auswertung im Anschluss an massenhafte Datengewinnung im Rahmen von Telekommunikationsüberwachungsmaßnahmen nach § 100a StPO oder Verkehrsdatenabfragen nach § 100g StPO errichtet werden. Zudem werden in Strafverfahren der Massenkriminalität zur arbeitsökonomischen Erledigung Dateien eingerichtet, um mit Textverarbeitungsprogrammen mit Eingabemasken automatisiert Schriftstücke zu erstellen.[1014] Dabei können die hier als getrennt beschriebenen Dateizwecke und weitere Funktionen auch mit Systemen zur dateiübergreifenden Arbeit verbunden werden.[1015] Die Möglichkeit zur stärkeren informationellen Verknüpfung der in einer Strafverfahrensdatei gespeicherten Daten bietet auch die Möglichkeit der Lokalisierung der Datei in einem polizeilichen Informationssystem gemäß § 483 Abs. 1 S. 2 StPO. Da eine solche Verknüpfung mit Blick auf die prinzipielle Bindung der Daten an den Zweck eines spezifischen Strafverfahrens aber zunächst möglichst zu unterbinden ist, legt § 483 Abs. 1 S. 3 StPO fest, dass die Daten entsprechend ihrer konkreten Strafverfahrensbindung zu konkretisieren sind (Nr. 1), ein Zugriffsberech-

1011 BT-Drs. 14/1484, S. 31.

1012 *Kersten* in *Abel,* Datenschutz in Anwaltschaft, Notariat und Justiz, S. 188.

1013 BT-Drs. 14/1484, S. 31.

1014 Als wenig geklärt gilt allerdings, inwiefern bestimmte Teile von und auch Metainformationen über Strafverfolgungsdateien zu den staatsanwaltschaftlichen Strafakten genommen werden müssen, vgl. etwa *Weßlau/Deiters* in *J. Wolter* (Hrsg.), SK-StPO, § 483 Rn. 9.

1015 *Weßlau/Deiters* in *J. Wolter* (Hrsg.), SK-StPO, § 483, Rn. 6.

tigungskonzept zu implementieren ist (Nr. 2) und Löschungsprüffristen festzulegen sind (Nr. 3). Dieser Versuch, die Zweckbindung normativ abzusichern, wird indessen bereits in § 483 Abs. 2 StPO relativiert, der die Datenverarbeitung auch für andere Strafverfahren freigibt, wobei begrenzend die für Übermittlung (§ 487 StPO) bestehenden Kautelen zu beachten sind – freilich nur, wenn für die zweckändernde Nutzung eine Übermittlung überhaupt erforderlich ist. Auch die Möglichkeit zum automatisierten Abruf gem. § 488 StPO schwächt die Zweckbindung, da eine Einzelfallprüfung der Übermittlungsvoraussetzungen entfällt. Zudem ist der Steuerungsanspruch der Strafprozessordnung mit § 483 StPO für Dateien, die in Informationssystemen der Polizei angesiedelt sind und auch Daten auf polizeirechtlicher Grundlage verarbeiten, relativiert, da hier auch für die strafverfahrensrechtlichen Daten nunmehr das Recht der Polizeien gilt. Der Einwand, der Bundesgesetzgeber behalte ohnehin über das BKAG erhebliche Regelungsmöglichkeiten,[1016] greift nur sehr bedingt durch: Einerseits ist diskutabel, inwieweit das dem BKAG unterfallende INPOL-System normativ tatsächlich durch das BKAG hinreichend konturiert wird. Andererseits gilt das BKAG gerade nicht für die rechtlich nur wenig geregelten Vorgangsbearbeitungssysteme, in denen aber auch Daten zu konkreten sowie künftigen Strafverfahren verarbeitet werden.[1017] Das prinzipielle Postulat der Zweckbindung von Strafverfahrensdaten, die regelmäßig als sensibel gelten dürften, erweist sich mithin schon aufgrund der gegenwärtigen Regelungslage als illusionär.[1018]

Neben den Vorgangsbearbeitungssystemen, die die polizeiliche Arbeit – wie beschrieben – sehr breit stützen, haben sich im strafverfahrensrechtlichen bzw. kriminalpolizeilichen Kontext ebenfalls breitere Informationssysteme, die sogenannten Fallbearbeitungssysteme, herausgebildet. Sie dienen der Unterstützung von kriminalpolizeilichen Ermittlungsverfahren, ermöglichen die vernetzte Darstellung und Auswertung von Ermittlungserkenntnissen und kommen mitunter auch im Bereich der Kriminalprävention zum Einsatz. In Fallbearbeitungssystemen werden einzelne Datenpunkte aus polizeilichen Ermittlungen gespeichert wie etwa Person, Adresse, Beruf, Straftaten, Veranstaltung, Firma, Waffe, et cetera. Diese Einzelinforma-

1016 *Weßlau/Deiters* in *J. Wolter* (Hrsg.), SK-StPO, § 483 Rn. 16.

1017 So etwa in @rtus-Bund, dem Vorgangsbearbeitungssystem der Bundespolizei, vgl. BT-Drs. 19/15346, S. 22.

1018 In ähnlichen Worten so bereits *Arzt* in *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch des Polizeirechts, G. Rn. 1287.

tionen können dann miteinander verknüpft werden. Zusätzlich können andere mediale Datenformate wie Fotografien, Filme oder Dokumente in die Datenbank geladen werden und sind wiederum verknüpfbar.[1019] Fallbearbeitungssysteme arbeiten dabei in erster Linie ereignisorientiert. Die vorhandenen personenbezogenen Daten werden also mit einem Ereignis verknüpft, das seinerseits mit weiteren Personen, Ereignissen, Institutionen oder Sachen verknüpft werden kann. Die Zahl der Verknüpfungsebenen ist nicht begrenzt, sodass die zu einer Person gespeicherten Daten zunehmend in größeren Datenbeständen diffundieren.[1020] Die Systeme dienen komplexeren Ermittlungen wie in bestimmten Phänomenbereichen oder Fällen mit umfassenden Sachverhalten. Entsprechend umfangreich sind die in den Systemen vorgehaltenen Daten. Es werden allerdings nicht nur Daten in den Systemen selbst vorgehalten. Vielmehr können bei entsprechenden Ermittlungen über Schnittstellen verschiedene polizeiliche Auskunftssysteme angesprochen werden und die Trefferdaten als neue Objekte in die Bearbeitung übernommen werden. Dabei richtet sich die Rechtsgrundlage der Systeme danach, wie die Fallbearbeitungssysteme konkret zur Ermittlungsunterstützung genutzt werden.[1021] Mangels konkreter Vorschriften ist die Rechtsgrundlage der Fallbearbeitungssysteme im allgemeinen Regelungskonzept der Strafprozessordnung zur Verarbeitung von Daten, den §§ 483 ff., zu suchen. Hier gilt dasselbe, wie auch für Strafverfolgungsdateien – als im Vergleich zu Fallbearbeitungssystemen eher untergeordnete informationstechnologische Einheit: Rechtlich möglich sind Ausgestaltung rein auf strafverfahrensrechtlicher Basis oder als Informationssysteme nach polizeirechtlichen Regelungen.[1022] Zur rechtlichen Konkretisierung kommen zudem auch Errichtungsanordnungen zum Einsatz,[1023] von denen allerdings, soweit ersichtlich, keine einzige veröffentlicht ist. Auf Grundlage der gesetzlichen Vorgaben ist es insofern – wie es für polizeiliche Informationssysteme typisch ist – nur begrenzt möglich, Aussagen über die Fallbearbeitungssysteme zu treffen. Bekannt ist aber, dass sie üblicherweise bei ge-

1019 *Konferenz der Leiterinnen und Leiter der Archivverwaltungen des Bundes und der Länder*, Bewertung von Fachverfahren der Polizeibehörden von Bund und Ländern, Abschlussbericht, (Version 1.1, 2020), S. 15.

1020 BfDI, 26. Tätigkeitsbericht 2015/2016, S. 110.

1021 *Konferenz der Leiterinnen und Leiter der Archivverwaltungen des Bundes und der Länder*, Bewertung von Fachverfahren der Polizeibehörden von Bund und Ländern, Abschlussbericht, (Version 1.1, 2020), S. 15.

1022 Siehe auch BfDI, 26. Tätigkeitsbericht 2015/2016, S. 110 f.

1023 BT-Drs. 17/8544 (neu), S. 32.

nerell umfangreichen und komplexen Ermittlungsverfahren, bei Mord- und Branddelikten in Sonderkommissionen, bei Serienstraftaten, in besonderen Phänomenbereichen (etwa Organisierte Kriminalität oder politisch motivierte Kriminalität) sowie bei Gefahrenabwehrlagen mit massenhaft anfallenden Informationen genutzt werden. Damit sind Fallbearbeitungssysteme eine informationstechnologische Weiterentwicklung der analogen kriminalpolizeilichen Karteikartensammlungen, Spurenakten und Handakten.[1024] Sind die polizeilichen Ermittlungen abgeschlossen, werden die Ergebnisse, die die Hauptspur der Ermittler stützen, in (wohl gegenwärtig überwiegend noch) analoger Form an die Staatsanwaltschaft übergeben. Diese Akte für die Staatsanwaltschaft enthält dann regelmäßig die wesentlichen Ermittlungsergebnisse, was nicht alle Inhalte aus dem Fallbearbeitungssystem miteinschließt. Neben nicht verfolgten Spuren finden etwa Massendaten wie etwa DNA-Proben, TKÜ-Daten, telefonische Abfragen oder andere digitale oder digitalisierte Daten, die mittels Schnittstelle oder Schreibkraft in das Fallbearbeitungssystem importiert wurden, normalerweise keinen Aktenrückhalt.[1025]

Neben der retrospektiven Ermittlungsarbeit bei begangenen Straftaten werden Fallbearbeitungssysteme aber auch prospektiv zum Zwecke der Kriminalprävention genutzt. Konkret geht es dabei zumeist um die Überwachung bestimmter Phänomenbereiche. Die Fallbearbeitungssysteme werden in diesem Kontext zur Speicherung und Analyse von Daten zum Zwecke der Beobachtung devianter Organisationen und Strukturen und zur Verhinderung der daraus drohenden Straftaten genutzt.[1026] Für die Speicherung von Personen zu diesem Zweck ist stets eine Negativprognose wie etwa in § 18 Abs. 1 Nr. 3 BKAG[1027] erforderlich, das heißt die betroffene Person muss einer Straftat verdächtig sein und wegen der Art oder Ausführung der Tat, der Persönlichkeit der betroffenen Person oder sonstiger Erkennt-

1024 *Konferenz der Leiterinnen und Leiter der Archivverwaltungen des Bundes und der Länder*, Bewertung von Fachverfahren der Polizeibehörden von Bund und Ländern, Abschlussbericht, (Version 1.1, 2020), S. 16.

1025 *Konferenz der Leiterinnen und Leiter der Archivverwaltungen des Bundes und der Länder*, Bewertung von Fachverfahren der Polizeibehörden von Bund und Ländern, Abschlussbericht, (Version 1.1, 2020), S. 16.

1026 *Konferenz der Leiterinnen und Leiter der Archivverwaltungen des Bundes und der Länder*, Bewertung von Fachverfahren der Polizeibehörden von Bund und Ländern, Abschlussbericht, (Version 1.1, 2020), S. 16.

1027 Die Vorschriften des BKAG, die in diesem Absatz zitiert werden, stehen beispielhaft für vergleichbare Regelungen in den Polizeigesetzen.

nisse muss Grund zu der Annahme bestehen, dass zukünftig Strafverfahren gegen sie zu führen sind. Daneben können aber auch Anlasspersonen – das sind Personen, bei denen Anlass zur Weiterverarbeitung der Daten besteht, weil tatsächliche Anhaltspunkte dafür vorliegen, dass die betroffenen Personen in naher Zukunft Straftaten von erheblicher Bedeutung begehen werden (§ 18 Abs. 1 Nr. 4 BKAG), mit in kriminalpräventive Datensammlungen aufgenommen werden.[1028] Dasselbe gilt auch für Kontaktpersonen gem. § 19 Abs. 1 Nr. 3 BKAG, wobei es sich um Personen handelt, bei denen tatsächliche Anhaltspunkte dafür vorliegen, dass sie mit in § 18 Abs. 1 Nr. 1-3 BKAG bezeichneten Personen nicht nur flüchtig oder in zufälligem Kontakt und in einer Weise in Verbindung stehen, die erwarten lässt, dass Hinweise für die Verfolgung oder vorbeugende Bekämpfung dieser Straftaten gewonnen werden können, weil Tatsachen die Annahme rechtfertigen, dass die Personen von der Planung oder der Vorbereitung der Straftaten oder der Verwertung der Tatvorteile Kenntnis haben oder daran mitwirken. Darüber hinaus existiert auch die Praxis sogenannter Prüffälle, in denen eine vorsorgliche Speicherung zur vorbeugenden Kriminalprävention erfolgt, mit anderen Worten also erst noch geprüft werden muss, ob die ohnehin eher vagen und in der Praxis nicht immer beachteten Voraussetzungen[1029] einer Negativprognose oder die noch weiter heruntergefahrenen Voraussetzungen für die Bejahung einer Anlasspersoneneigenschaft vorliegen. Zwar sind diese Daten nur begrenzt verarbeitbar (siehe etwa § 18 Abs. 3 BKAG), stehen aber dennoch für die polizeiliche Arbeit im Kontext von vermuteter devianter Neigung und damit in stigmatisierender Weise zur Verfügung, ohne dass eine stichhaltige Tatsachengrundlage – verlässliche tatsächliche Anhaltspunkte fehlen in solchen Fällen gerade – vorläge.[1030] Konkret werden die Daten, die im Rahmen der Ermittlungen erhobenen wurden, zum Zweck der Kriminalitätsverhütung unterschiedlichen Phänomenbereichen zugeordnet (Rauschgift, Falschgeld, Organisierte Kriminalität, Staatsschutz etc.) und mit weiteren Ermittlungsinformationen der jeweils zuständigen Dienststellen angereichert, neu verknüpft und strukturiert. Im Gegensatz zum reinen Ermittlungsbereich können die Daten – je nach Rechtemodell

1028 Mit Einwilligung können auch die in § 19 Abs. 1 Nr. 1, 2, 4 BKAG genannten Personen in entsprechende Datensammlungen aufgenommen werden.

1029 HmbLfDI, 26. Tätigkeitsbericht 2016/2017, S. 33.

1030 Die zuvor ungeregelte und damit rechtswidrige Praxis, Personen mit dem Ziel der „Anreicherung" der Daten zu speichern (so und kritisch dazu BfDI, 24. Tätigkeitsbericht 2011/2012, S. 97; 26. Tätigkeitsbericht 2015/2016, S. 111) ist mit dem neuen § 18 Abs. 3 BKAG in begrenzter Form legalisiert worden.

– verfahrensübergreifend auf Landesebene ausgewertet werden. Allerdings kann es bei Bestehen von lokalen Kriminalitätsstrukturen aus polizeilicher Sicht sinnvoll sein, dass die diesbezüglichen Informationen auch von den lokalen Polizeiorganisationen bearbeitet werden.[1031] Der Umstand, dass eine solche Datenverarbeitung zu Zwecken der strukturellen Kriminalprävention dazu führt, dass Informationen weit über das einzelne anlassgebende Ermittlungsverfahren hinaus behalten werden, macht auch Fallbearbeitungssysteme zu invasiven Informationsinstrumenten.

e) Sonstige Informationssystemtypen

Darüber hinaus arbeiten die Polizeien in Bund und Ländern mit einer – mitunter als verwirrend bezeichneten[1032] – Vielzahl weiterer elektronischer Anwendungen und Systemen. Neben den bereits beschriebenen Komponenten des polizeilichen Informationswesens gibt es noch drei informationstechnische Fachverfahren, welche zentral für die polizeiliche Arbeit sind: Einsatzleit-, Einsatzprotokoll- und Lageinformationssysteme.

Einsatzleitsysteme ermöglichen in den Einsatzleitstellen der deutschen Polizeien die Koordinierung der Einsatzkräfte in den aktuellen Einsätzen und ermöglichen so einen Echtzeit-Überblick über laufende Einsätze und die darin eingesetzten Kräfte. Zu den einzelnen Einsätzen werden bestimmte Daten dokumentiert. Hierzu gehören der Einsatzanlass, die Einsatzmittel (etwa Funkrufname und Kategorisierung der eingesetzten Fahrzeuge), der Status („frei auf Wache“ oder „Einsatz übernommen“), die Einsatzobjekte (inkl. Gefahrenhinweise, Anfahrtshinweise, Hinweise zu Ansprechpartnern) sowie Geodaten zum Anzeigen von Einsatzorten in einem Geoinformationssystem. Es handelt sich dabei überwiegend um nicht-personenbezogene Daten. Für diejenigen Daten, die einen Personenbezug zulassen, gibt es in den Polizeigesetzen vereinzelte Rechtsgrundlagen, die die Aufzeichnung der Büger:in-Polizei- und Polizei-Polizei-Kommunikation im Kontext der Einsätze gestatten (vgl. etwa § 20 Abs. 11 HSOG). Die Daten

1031 *Konferenz der Leiterinnen und Leiter der Archivverwaltungen des Bundes und der Länder*, Bewertung von Fachverfahren der Polizeibehörden von Bund und Ländern, Abschlussbericht, (Version 1.1, 2020), S. 16.

1032 *Konferenz der Leiterinnen und Leiter der Archivverwaltungen des Bundes und der Länder*, Bewertung von Fachverfahren der Polizeibehörden von Bund und Ländern, Abschlussbericht, (Version 1.1, 2020), S. 5.

werden wenige Monate im Einsatzleitsystem gespeichert und dann automatisch gelöscht. Entwickelt sich jedoch aus einem Einsatz ein Ermittlungsvorgang, werden die relevanten Daten aus dem Einsatzleitsystem in das Vorgangsbearbeitungssystem und gegebenenfalls in das Fallbearbeitungssystem übernommen (vgl. etwa § 20 Abs. 11 S. 3 HSOG). Bei besonderen Einsatzlagen kann ein Löschverbot für alle mit dem Ereignis verbundenen Daten ausgesprochen werden. Die Einsatzleitsysteme sind temporäre Spiegelbilder des polizeilichen Alltagsgeschäfts. Hier gehen verschiedenste Meldung zu allen Fallarten ein und werden für eine gewisse Zeit gespeichert. So entsteht eine Momentaufnahme derjenigen gesellschaftlichen Problemlagen, die die Bevölkerung als polizeirelevant einstuft.[1033] Aufgrund der nur kurzen Speicherung und weil die Daten bei Relevanz in die genannten Informationssysteme diffundieren, ist die sehr oberflächliche Regelung dieser Systeme in den Polizeigesetzen für sich genommen akzeptabel. In den unterschiedlichen Informationssystemen angekommen, treten jedoch die bereits beschriebenen rechtlichen Problemlagen auf.

Einsatzprotokollsysteme (auch Einsatzdokumentationssysteme genannt) werden von den Polizeibehörden von Bund und Ländern bei der Bewältigung und Dokumentation größerer Einsätze eingesetzt, die einer Besonderen Aufbauorganisation bedürfen. Mit ihnen wird der Informationsfluss zwischen Einsatzführung und Einsatzkräften gewährleistet und protokolliert, so dass alle Beteiligten über alle benötigten Informationen verfügen.[1034]

Daneben treten schließlich noch die Lageinformationssysteme. Eine Lage im polizeilichen Sinne meint eine Situation, in der polizeiliches Handeln erforderlich ist, um der gesetzlichen Aufgabenerfüllung der Gefahrenabwehr und der Strafverfolgung nachzukommen. Lagen können angesichts vielfältiger Einsatzrealitäten sehr unterschiedlich aussehen. Eine grundsätzliche Unterscheidung besteht zwischen einsatzorientierten Lagen und eher größer dimensionierten Kriminalitätslagen oder Speziallagen. Letztere beschreiben große umfassende Phänomene und werden zumeist in Lagebildern erfasst (etwa Lagebild Rauschgiftkriminalität, Lagebild Organisierte

1033 *Konferenz der Leiterinnen und Leiter der Archivverwaltungen des Bundes und der Länder*, Bewertung von Fachverfahren der Polizeibehörden von Bund und Ländern, Abschlussbericht, (Version 1.1, 2020), S. 10.

1034 *Konferenz der Leiterinnen und Leiter der Archivverwaltungen des Bundes und der Länder*, Bewertung von Fachverfahren der Polizeibehörden von Bund und Ländern, Abschlussbericht, (Version 1.1, 2020), S. 13.

Kriminalität, Lagebild Cybercrime). Einsatzorientierte Lagen beziehen sich dagegen auf konkrete Einsatzsituationen und beschreiben Ausgangssituation und Geschehen vor Ort. Die Einsatzkräfte vor Ort übermitteln Lagemeldungen an die Einsatzführung. Die so zustande kommenden Lagebilder sind die Voraussetzung für ein zielgerichtetes polizeiliches Handeln und dienen dem Erkennen, der Analyse und der Prognose relevanter Ereignisse und Entwicklungen. Eine weitere spezielle und für das polizeiliche Handeln wichtige Form ist die sogenannte Tageslage (auch: tägliches Lagebild, Präsidiallage, Landeslage). Diese umfasst mindestens die wesentlichen Einsatzaktivitäten der vergangenen 24 Stunden. Mit Blick auf die Tageslage können alle Polizist:innen, v.a. aber auch die Polizeiführer:innen, einen schnellen Überblick über das jüngste Einsatzgeschehen ihrer Polizeibehörde erhalten, womit die Kontinuität der polizeilichen Aufgabenerfüllung gewährleistet wird. Die Tageslage ist zumeist in unterschiedliche Bereiche wie Einsatzlage, Kriminalitätslage und Verkehrslage gegliedert, womit eine Übersicht über bekannte Störungen des gesellschaftlichen Lebens – etwa in Form von Bränden, Wohnungseinbrüchen oder Verkehrsunfällen – im Zuständigkeitsbereich der jeweiligen Polizeiorganisation ermöglicht wird. Die Tageslage wird weiter durch Informationen wie Fahndungen, Festnahmen und Ähnliches ergänzt. Alle konkreten Lageinformationen beschreiben kurz das Geschehen sowie den Einsatz der Polizei. Lagen können bei der Polizei durch sogenannte Lageinformationssysteme elektronisch erstellt werden. Diese Funktionalität kann auch ins Vorgangsbearbeitungssystem integriert sein. Aus Einsatzleitsystem und Vorgangsbearbeitungssystem, in denen alles Einsatzhandeln dokumentiert ist, werden bestimmte Daten automatisiert in das Lageinformationssystem übernommen. Dort werden die Geschehnisse mit einer kurzen Beschreibung in chronologischer und/oder geographischer Ordnung dargestellt, wobei häufig die Möglichkeit der Kartendarstellung implementiert ist. Je nach polizeilichem Bedarf können Lagen gefiltert dargestellt werden. Ungeachtet des traditionellen Begriffs der Tageslage können Lageinformationssysteme auch Zeiträume von mehr als 24 Stunden abdecken und somit über größere Zeiträume das Einsatzgeschehen nachhalten. Die Tageslagen werden wenige Monate im System gespeichert und dann automatisiert gelöscht.[1035] Ähnlich wie auch andere neuere Systeme dienen Lageinformationssysteme der Dynamisierung der

1035 *Konferenz der Leiterinnen und Leiter der Archivverwaltungen des Bundes und der Länder*, Bewertung von Fachverfahren der Polizeibehörden von Bund und Ländern, Abschlussbericht, (Version 1.1, 2020), S. 14.

polizeilichen Informationsbestände und damit einer Nutzung der vorgehaltenen Daten zur möglichst optimalen Aufgabenerfüllung durch die Polizeien in ihren jeweiligen Tätigkeitsfeldern.

Neben diesen einsatzunterstützenden Systemen wurden in jüngerer Zeit und im Kontext von Massendatentechnologien zudem sogenannte Analysesysteme entwickelt, die zunehmend in der Polizei zur bestmöglichen Informationsgewinnung aus den weitläufigen Datenbeständen eingesetzt werden, die der Polizei zur Verfügung stehen. Da diese Systeme jedoch paradigmatisch für den Wandel des polizeilichen Informationswesens stehen, werden sie auch im Rahmen dieser nun zu behandelnden Entwicklung dargestellt.

3. Die neue Informationsarchitektur der Polizei

Als Agglomeration von Datenbeständen, Informationssystemen und sonstigen informationstechnischen Anwendungen sowie unterschiedlichen Informationspraktiken ist das polizeiliche Informationswesen ein aus vielen beweglichen Teilen zusammengesetztes Ganzes – und als solches ist es ständig in Bewegung und im Wandel begriffen. Gegenwärtig durchläuft es jedoch eine Entwicklung – so ist es auch die der Arbeit zugrundeliegende Annahme – neuer Qualität, die gleichzeitig erzwungen wird, aber auch gewollt ist. Erzwungen wird der Wandel einerseits, weil das medienevolutive Massendatenphänomen, das informationstechnologisch angestoßen wurde und bereits jetzt mit vielfältigen sozialen Prozessen verzahnt ist, sich als makrostrukturelles Kraftfeld in den menschlichen Gesellschaften weder revidieren noch ignorieren lässt. Insofern zwingt es gesellschaftlich mächtige Akteure, wie die Polizei, zu reagieren. Andererseits ist der Wandel des polizeilichen Informationswesens auch von menschlicher Intentionalität getragen, denn innerhalb des massendatenbedingten Reaktionszwangs gibt es Handlungs- und Gestaltungsspielräume, die sicherheitspolitisch beeinflussbar sind. Insofern sind die vielfältigen, mittlerweile großteilig unter der Ägide des *Projekts 2020* versammelten Bemühungen zur technologiegemäßen Ausgestaltung des polizeilichen Informationswesens auch Ausdruck einer gewollten Evolution polizeilicher Informationsverarbeitung im Rahmen eines überwiegend technologiebegeisterten Sicherheitsdiskurses.

a) Rechtspolitische Ausgangslage

Die beschriebenen, sich gegenwärtig noch in Benutzung befindlichen Dateien im INPOL-Verbund sollen in den nächsten Jahren ihre klaren Grenzen verlieren und im Wesentlichen in einen großen polizeilichen Datenbestand überführt werden, um die Schaffung einer gemeinsamen, modernen, einheitlichen Informationsarchitektur zu ermöglichen. Seinen konkreten politischen Ursprung hat dieses Projekt in der sogenannten Saarbrückener Agenda, einem Papier der „Innenministerkonferenz" (IMK).[1036] Dieser den Logiken des Massendatenparadigmas entsprechende Schritt wurde hingegen im dazugehörigen Gesetzgebungsprozess als rechtspolitisch zwingend notwendiges Projekt präsentiert. Der Entwurf zur Gesetzesreform des BKAG nennt vorrangig das Urteil des Bundesverfassungsgerichts zum BKAG[1037] als primären Grund für die geplante Umstrukturierung der IT-Infrastruktur des Bundeskriminalamtes.[1038] Ob die Umstrukturierung nur aufgrund des verfassungsgerichtlichen Urteils alternativlos ist, lässt sich bezweifeln.[1039] Das Argument der verfassungsrechtlich bedingten Notwendigkeit der Umstrukturierung wirkt auch vor dem Hintergrund der historischen Entwicklung des Informationswesens vorgeschoben: Bereits die gegenwärtige Ausführung von INPOL, die mal als INPOL-neu geplant wurde und die bis dahin (2003) bestehende ursprüngliche Ausführung von INPOL („INPOL-alt") ablöste, war einmal sehr ähnlich zu gegenwärtigen Planungen konzipiert. Beamt:innen sollten von den an ihren Arbeitsplätzen verfügbaren Vorgangsbearbeitungssystemen je nach Berechtigung auf sämtliche Polizeidaten zugreifen können. Das Projekt scheiterte jedoch mit seinen konzeptuellen Ansprüchen wegen der vielfältigen Inkompatibilitäten der bis dahin wildgewachsenen Systeme auf Bundes- und Landesebene und

1036 *Innenministerkonferenz*, Saarbrücker Agenda zur Informationsarchitektur der Polizei als Teil der Inneren Sicherheit, 2016.

1037 BVerfGE 141, 220 – 378 – Bundeskriminalamtgesetz.

1038 BT-Drs. 18/11163, S. 1 f.

1039 Siehe etwa *Bäcker*, Der Umsturz kommt zu früh: Anmerkungen zur polizeilichen Informationsordnung nach dem neuen BKA-Gesetz, https://verfassungsblog.de/der-umsturz-kommt-zu-frueh-anmerkungen-zur-polizeilichen-informationsordnung-nach-dem-neuen-bka-gesetz/ (Stand: 01.10.2023), demzufolge es nicht ohne weiteres ersichtlich sei, „warum es nicht auch auf der Grundlage der hergebrachten Dateistruktur möglich sein soll, die Informationsbestände von Bund und Ländern zu vernetzen und Querbezüge zwischen unterschiedlichen Kriminalitätsfeldern zu erkennen" und die Grundrechte nicht dazu zwängen, „die hergebrachte Dateistruktur generell aufzugeben, wie es die Gesetzesbegründung nahelegt".

wurde in abgewandelter, oben beschriebener Form umgesetzt.[1040] Als Idee ist die bessere Vernetzung und Nutzbarkeit der polizeilichen Daten in Form eines gemeinsamen Datenbestandes jedoch lebendig geblieben und hat mit zunehmender Präsenz des Massendatenphänomens und anwachsender gesellschaftlicher Bedeutung von Sicherheit[1041] wieder neue Auftriebskraft erhalten, die auch durch zwei weitere konkrete rechtspolitische Ansprüche an die polizeiliche Informationsverarbeitung verstärkt wurde: Einerseits war das Ergebnis des NSU-Untersuchungsausschusses des Deutschen Bundestages in die Informationsverarbeitung zu implementieren.[1042] Eine zentrale Forderung des Ausschusses betraf dabei die Forderung nach Herstellung von Interoperabilität der Datensysteme, die „zügig zu einem guten, verfassungsrechtlich einwandfreien" Abschluss gebracht werden sollten.[1043] Und andererseits war die infolge der Europäischen Datenschutzreform erlassene JI-Richtlinie vom Gesetzgeber umzusetzen. In dieser rechts- und sicherheitspolitischen Gemengelange konnte das Konzept zur Vereinheitlichung, Konsolidierung und Effektivierung des polizeilichen Informationswesens ein neues legitimierendes Substrat finden, aus dem heraus sich die gegenwärtig laufende Umstrukturierung der informationstechnologischen Strukturen der deutschen Polizeien entwickelte. Vorrangiges Ziel ist und bleibt dabei aber die Homogenisierung und stärkere Integration des als zu heterogen empfundenen polizeilichen Informationswesens.[1044]

Legislativ entschloss sich der Bundesgesetzgeber, die komplexen und mitunter widersprüchlichen Vorgaben – Interoperabilität der Datensysteme ist etwa datenschutzrechtlichen Belangen nicht ohne weiteres zuträglich – im Wesentlichen in einem einzigen Gesetzesvorhaben, der Novellierung des BKAG, umzusetzen. Auch in den Stellungnahmen im Innenausschuss wurde mit deutlichen Worten Kritik daran geübt. *Bäcker* sprach in Bezug auf die Informationsordnung von dem „anspruchsvollsten Teil des Ent-

1040 Siehe dazu sowie zum gesamten Entwicklungsprozess bis 2003, *H. Busch* Bürgerrechte & Polizei (CILIP) 25 (2003), 12.

1041 *Legnaro/Klimke* in Legnaro/Klimke (Hrsg.), Kriminologische Diskussionstexte II, 89.

1042 *Graulich* in *Schenke/Graulich/Ruthig,* Sicherheitsrecht, § 29 BKAG Rn. 3.

1043 BT-Drs. 17/14600, S. 862.

1044 Siehe etwa Bundesministerium des Inneren, White Paper Polizei 2020, S. 5, 9, 20; diese Einschätzung bezüglich der Heterogenität findet sich auch in *Konferenz der Leiterinnen und Leiter der Archivverwaltungen des Bundes und der Länder*, Bewertung von Fachverfahren der Polizeibehörden von Bund und Ländern, Abschlussbericht, (Version 1.1, 2020), S. 5.

wurfs“[1045] und empfahl die Zurückstellung dieses Vorhabens.[1046] Diesem Appell wurde nicht entsprochen, sodass der gegenwärtig bestehende, oben bereits in Teilen erläuterte Rechtsrahmen[1047] der polizeilichen Informationsarchitektur die Umstrukturierung des Informationswesens normativ tragen und absichern soll.

b) Polizei 2020: Aspekte der neuen informationstechnologischen Architektur und Umsetzungsverlauf

Die Umstrukturierung der polizeilichen Informationsarchitektur erfolgt durch das IT-Großprojekt und Organisationsentwicklungsvorhaben[1048] „Polizei 2020“,[1049] mit dem die Polizei die digitale Transformation bewältigen soll.[1050] Ein zentrales Anliegen des geplanten Umbaus ist dabei das „gemeinsame Datenhaus der deutschen Polizei“, also die bereits angesprochene Abschaffung der bisher bestehenden Dateienlandschaft zugunsten eines gemeinsamen Datenbestandes, wobei der Zugriff „zielgerichtet über ein dynamisches und modernes Zugriffsmanagement geregelt“ werden soll. Verbundrelevante Informationen sollen allen Teilnehmern zur Verfügung stehen. Die Verantwortung verbleibt aber beim Datenbesitzer. Daten ohne Verbundrelevanz sollen hingegen nur für die jeweiligen Datenbesitzer einsehbar sein.[1051] So müssen „Anpassungen für das Verbundsystem […] nur einmal vorgenommen und nicht 19 Mal (in den Systemen der 16 Länder

1045 *Bäcker*, A-Drs. 18(4)806 D, S.4.
1046 *Bäcker*, A-Drs. 18(4)806 D, S. 2, 10.
1047 Siehe dazu oben S. 230 ff.
1048 Die Bundesregierung weist darauf hin, dass es sich beim Polizei 2020 nicht primär um ein IT-Großprojekt handle, da ebenfalls „die die entsprechenden fachlichen und technischen Prozesse sowie die föderalen Bedarfe“ zu berücksichtigen seien, BT-Drs. 19/25651, S. 2. Gerade diese vielfältigen Bedarfe machen das im Kern informationstechnologische Projekt aber zu einem großen. Dass es auch organisationale Komponenten aufweist ist auch nichts Ungewöhnliches bei IT-Projekten, die zumeist auch auf Umstrukturierung von organisatorischen Prozessen abzielen. Zu den einzelnen Komponentprojekten siehe BT-Drs. 19/27083, S. 4 f.
1049 Mittlerweile wird es offiziell auch P20 genannt, siehe https://www.bmi.bund.de/DE/themen/sicherheit/programm-p20/programm-p20-node.html (Stand: 01.10.2023). „Polizei 2020“ ist jedoch die weitaus verbreitetere Bezeichnung.
1050 BT-Drs. 19/25651, S. 2.
1051 Bundesministerium des Inneren, White Paper Polizei 2020, S. 11 f.; vgl. auch BT-Drs. 18/11163, S. 84 f.

sowie den Polizeien des Bundes) nachvollzogen werden."[1052] Neben einer verbesserten Verfügbarkeit polizeilicher Informationen soll dadurch auch die Wirtschaftlichkeit polizeilicher Datenverarbeitung erhöht und der Datenschutz durch Technikgestaltung verbessert werden können.[1053] Relevant soll in Zukunft damit „nicht mehr die technische Zusammenfassung von Informationen in Dateien, sondern der Themenbezug der Information sein."[1054] Über den technisch gesteuerten Zugriff soll auch der Grundsatz der hypothetischen Datenneuerhebung umgesetzt werden können. Dazu muss die Eingriffstiefe der jeweils vorhandenen Daten bestimmt werden.[1055] Die Protokollierung dieser Zugriffe an zentraler Stelle wird ebenfalls als Verbesserung des Datenschutzes angeführt.[1056] Daneben soll die Rolle des Bundeskriminalamtes als dienstleistungsorientierte Zentralstelle gestärkt werden, was insbesondere bedeutet, dass das Amt den anderen Polizeibehörden Anwendungen und Dienste für die polizeiliche Arbeit bereitstellen wird.[1057] Außerdem soll „moderne und zukunftsfähige Technologie" zum Einsatz kommen.[1058] Neben der geplanten INPOL-Modernisierung sind auch der bereits seit 2008 geplante[1059] Polizeiliche Informations- und Analyseverbund (PIAV),[1060] der einen bruchlosen Datenaustausch zur Aufklärung länder- oder phänomenübergreifender Tatzusammenhänge ermöglichen soll,[1061] sowie die Entwicklung eines für die Bundespolizeibehörden vereinheitlichten Fallbearbeitungssystems (einheitliches Fallbearbeitungssystem – eFBS) als Teilprojekte in das Polizei 2020-Vorhaben integriert worden.[1062]

Neben diesen beiden wichtigen Teilprojekten und der zentralen Modernisierung von INPOL sind unter dem Dach von Polizei 2020 gegenwärtig noch 23 weitere Projekte zur abgestimmten Bearbeitung versammelt. Angegliedert sind dort etwa die elektronische Akte in Strafsachen, der Gesamtansatz Auswertung und Analyse, die Anbindung der Staatsanwaltschaften

1052 BT-Drs. 18/11163, S. 84.
1053 Bundesministerium des Inneren, White Paper Polizei 2020, S. 8 ff.
1054 BT-Drs. 18/11163, S. 109.
1055 Bundesministerium des Inneren, White Paper Polizei 2020, S. 12.
1056 Bundesministerium des Inneren, White Paper Polizei 2020, S. 10.
1057 Bundesministerium des Inneren, White Paper Polizei 2020, S. 13.
1058 Bundesministerium des Inneren, White Paper Polizei 2020, S. 14.
1059 BT-Drs. 16/12600, S. 56.
1060 Siehe dazu bereits oben S. 251 ff.
1061 *Aden/Fährmann* Zeitschrift für Rechtspolitik 2019, 175177.
1062 Bundesministerium des Inneren, White Paper Polizei 2020, S. 6.

an INPOL, ein Projekt zur Konzeptionierung der mobilen Verfügbarkeit der Fachanwendungsmodule durch mobile Anwendungen oder ein Projekt zur automatisierten Erkennung Kinderpornografischen Materials mittels eines KI-basierten Verfahrens. Dies unterstreicht den Charakter von Polizei 2020 als tiefgreifendes Transformationsprogramm, das zudem weiter offen für die bedarfsmäßige Integration neuer Projekte bleibt.[1063]

Für den Erfolg von Polizei 2020 sind aber insbesondere das eFBS und mehr noch ein einheitliches Vorgangsbearbeitungssystem,[1064] da durch letztere ein Großteil der polizeilich verwertbaren Daten generiert wird, denn aus jedem Einsatz und aus jeder Strafanzeige wird zunächst ein Vorgang.[1065] Ohne die Einbindung eines einheitlichen Vorgangsbearbeitungssystems in das Projekt ist das angestrebte Ziel der Einmalerfassung der Daten nicht erreichbar.[1066] Denn ein gemeinsames polizeiliches Informationssystem, wie es die INPOL-Modernisierung in Form des gemeinsamen Datenhauses vorsieht, funktioniert nur dann effektiv, wenn die Quellsysteme bei allen beteiligten Behörden einheitlich funktionieren.[1067] Vor dem Hintergrund großer Heterogenität bei den polizeilichen Vorgangsbearbeitungssystemen liegt darin eine große Hürde des gesamten Projekts. Gegenwärtig scheinen Bedarfe und Bestände in den Teilnehmerländern und den teilnehmenden Behörden ermittelt zu werden. Auf Grundlage dieser Prüfungsergebnisse sollen zunächst drei Interims-Vorgangsbearbeitungssysteme festgelegt werden. Ein viertes soll sich zudem noch in Prüfung befinden. Die Entscheidung für die Ausgestaltung des jeweiligen Vorgangsbearbeitungssystems ist dabei nicht trivial, da sie die Art der Sachbearbeitung für die kommenden Jahre maßgeblich beeinflussen wird.[1068]

Konkreter scheinen die Pläne zum eFBS zu sein, das für die Homogenisierung der kriminalpolizeilichen Datenerfassung zentral ist und somit ebenfalls mit über den Erfolg von Polizei 2020 entscheiden dürfte. Das System wurde durch das Programm im Mai 2020 in den Wirkbetrieb überführt. Insgesamt soll das eFBS derzeit durch sechs Teilnehmer von Bund und Ländern (BKA, Bundespolizei, Baden-Württemberg, Branden-

1063 Siehe zur vollständige Liste BT-Drs. 19/27083, S. 4 f.
1064 Zu Vorgangsbearbeitungssystemen siehe bereits oben S. 254 ff.; zur Bedeutung der Vorgangsbearbeitungssysteme für die gescheiterte INPOL-neu-Konzeption siehe oben S. 131 ff.
1065 *Geerdts* Moderne Polizei: Magazinreihe 2021, 6 (6).
1066 Behördenspiegel zitiert nach *Burczyk* Bürgerrechte & Polizei (CILIP) 2020, 16 (21).
1067 *Burczyk* Bürgerrechte & Polizei (CILIP) 2020, 16 (20).
1068 *Geerdts* Moderne Polizei: Magazinreihe 2021, 6 (6 f.).

burg, Hamburg, Hessen) genutzt werden, wobei die Zuschaltung weiterer Teilnehmer geplant ist.[1069] Auch die Protokollierung von Anlass und Zweck der Abfragen soll schon zentral auf einem Server beim Bundeskriminalamt erfasst werden können.[1070] Die Vereinheitlichung solcher Systeme erfolgt über die Beachtung des „Informationsmodell Polizei" bei der Programmierung, womit dann Informationen in identischer Weise Daten- und Objektkategorien zugewiesen würden. Nur so können Daten nach Übermittlung in ein zentrales System von anderen angeschlossenen Behörden einheitlich abgefragt und verwendet werden.[1071]

Die Umsetzung des Gesamtprojekts ist dementsprechend noch lange nicht abgeschlossen, viele der Schritte, von denen berichtet wird, wirken wie eher vage Konzeptionierungsarbeiten oder kleinteilige Schritte im Rahmen der einzelnen Teilprojekte.[1072] Auch wird von Widerständen aus den Länderpolizeien berichtet, weil Systeme aufgegeben werden sollen, die teilweise selbst entwickelt wurden und auch individueller an die jeweiligen fachlichen Vorgaben angepasst sind.[1073]

Die historisch gewachsene IT- sowie Prozesslandschaft der Polizeien in Bund und Ländern beweist hinsichtlich ihrer Vielfältigkeit und Heterogenität einige Beharrungskräfte. Auch in den nächsten Jahren werden die Herausforderungen bezüglich der Umsetzung des Projekts vor allem in der Harmonisierung und Konsolidierung der unterschiedlichen Ist-Zustände der einzelnen Teilnehmer und der Erarbeitung gemeinsamer Standards liegen. Gleichzeitig ist Polizei 2020 Projektarbeit an einem laufenden System. Die laufende polizeiliche Informationsarbeit soll möglichst wenig gestört werden. Deshalb erfolgt die Umsetzung modul- und phasenweise. Zunächst sollen daher die verschiedenen in Bund und Ländern bestehenden Einzelsysteme, sogenannte Monolithen, so weit wie möglich reduziert werden, um dann ausgehend von einem einheitlicheren Zwischenstand des polizeilichen Informationswesens die Transformation in die schlussendliche Zielarchitektur zu bewerkstelligen.[1074] Das Projekt, dem ein Zeitrahmen von mehr als 10 Jahren zugesprochen wird[1075] und für das kein Abschlusszeit-

1069 BT-Drs. 19/25651, S. 3.
1070 BT-Drs. 19/25651, S. 6.
1071 *Burczyk* Bürgerrechte & Polizei (CILIP) 2020, 16 (20).
1072 BT-Drs. 19/25651, S. 4.
1073 *Burczyk* Bürgerrechte & Polizei (CILIP) 2020, 16 (21).
1074 BT-Drs. 19/27083, S. 13.
1075 BfDI, 28. Tätigkeitsbericht 2019, S. 50.

punkt festgesetzt wurde,[1076] wird die Polizei und ihr Informationssystem also im kommenden Jahrzehnt maßgeblich beschäftigen und prägen.

c) Normativität und Faktizität

Die strukturellen Neuerungen, die der Umbau des polizeilichen Informationswesens mit sich bringen wird, sind rechtlich in erster Linie im neuen BKAG und dort vor allem in §§ 12-19 sowie §§ 29-32 abgebildet. Angesichts der nicht unbeträchtlichen Umwälzungen, die mit Polizei 2020 einhergehen, wirken diese rechtlichen Konturen indessen eher blass.[1077] Geändert wurde im Zuge der das Projekt begleitenden Gesetzgebung auch nichts am bestehenden Problem der unzureichenden Einhegung vieler Komponenten des Informationswesens. Zudem fährt das neue BKAG die rechtliche Rahmung der neuen zentralen Datenhaltung beim Bundeskriminalamt auch an anderer Stelle zurück: Für die gegenwärtige Dateien-Struktur der polizeilichen Informationsverarbeitung konkretisieren Errichtungsanordnungen den zulässigen Umfang und rechtlichen Rahmen bei der Verarbeitung personenbezogener Daten. Da die Errichtungsanordnung den Zweck der Dateien näher bezeichnet, ist eine Verarbeitung zu in ihr nicht vorgesehenen Zwecken nicht gestattet.[1078] Künftig werden diese – mit Ausnahme von gemeinsamen projektbezogenen Dateien nach § 17 BKAG[1079] – jedoch wegfallen, wie es dem neuen Konzept eines gemeinsamen Datenbestandes entspricht und beispielsweise auch in § 91 BKAG indirekt zum Ausdruck kommt. Gibt es keine abgrenzbaren Dateien mehr, sind Errichtungsanordnungen überflüssig. An ihre Stelle treten die von §§ 80 BKAG

1076 BWLT-Drs. 16/7932, S. 4.

1077 So *Graulich* in *Schenke/Graulich/Ruthig,* Sicherheitsrecht, § 29 BKAG Rn. 4, der zum rechtlichen Rahmen der neuen IT-Architektur des Bundeskriminalamtes im Wesentlichen sogar nur §§ 12 und 29 BKAG zählt.

1078 Siehe etwa AbgHBln-Drs. 17/14375, S.

1079 Errichtungsanordnungen finden weiter im Rahmen sog. projektbezogener gemeinsamer Dateien Anwendung, vgl. § 17 Abs. 6 S. 1 BKAG. Damit soll jedoch vor allem der Besonderheit und Bedeutung der Zusammenführung von Erkenntnissen und der gemeinsamen Verarbeitung von personenbezogenen Daten von Polizeien, Nachrichtendiensten und Zollkriminalamt Rechnung getragen werden, vgl. BT-Drs. 18/11163, S. 98. Für den davon insoweit abzugrenzenden Bereich der ausschließlich polizeilichen Informationsverarbeitung gilt das Erfordernis einer Errichtungsanordnung nach der Neukonzeption des BKAG also gerade nicht mehr.

i.V.m. 70 BDSG in Umsetzung der JI-Richtlinie vorgeschriebenen Verarbeitungsverzeichnisse,[1080] die jedoch nicht dieselbe normative Ordnungskraft entwickeln.[1081] Sind die Errichtungsanordnungen auch „nur" Verwaltungsvorschriften,[1082] so verringert ihre Abschaffung in wesentlichen Bereichen zweifellos die Konturenschärfe der normativen Grenzen des zukünftigen „Datenhauses der deutschen Polizei". Dies schien auch dem Gesetzgeber bewusst gewesen zu sein, der mit dem neueingefügten § 30 BKAG den Versuch einer ausgleichenden Konkretisierung unternimmt. Danach haben die am Informationsverbund teilnehmenden Stellen nunmehr festzulegen, welche Straftaten als verbundrelevant im Sinne des § 30 Abs. 1 Nr. 1 BKAG gelten sollen. Das ist indessen ein eindeutig niedrigerer Anspruch an Konkretisierung, denn Errichtungsanordnungen legen demgegenüber mit einiger Detailliertheit fest, welche Datenkategorien von wem zu welchen Zwecken verarbeitet werden dürfen.[1083] Von rechtsstaatlicher Warte aus betrachtet lässt sich diese Entwicklung kaum anders denn als Rückschritt bewerten: Statt die rechtliche Flankierung des gemeinsamen Datenhauses zu verstärken, wie es die Abschaffung der Dateistruktur und damit die weitere Relativierung der Zweckbindung von Daten geboten hätten, wird mit dem Konzept der Verbundrelevanz ein gegenüber der bisherigen Rechtslage schwächeres Begrenzungsinstrument gewählt. Ohne Errichtungsanordnungen ist die polizeiliche Informationsverarbeitung in Zukunft noch stärker normativer Anknüpfungspunkte beraubt.[1084] Insgesamt wird der rechtliche Regelungsanspruch damit gegenüber der normativen Kraft der tatsächlichen informationstechnischen Strukturen und der an ihnen eingeübten polizeilichen Informationspraktiken zurückgefahren. Ob sich dieses Ungleichgewicht durch einen Datenschutz prozeduraler Färbung ausgleichen lässt, wie es insbesondere im Wege der JI-Richtlinie erfolgen soll, muss sich erst noch zeigen.[1085]

1080 *Petri* in *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch, G. Rn. 458.
1081 Siehe dazu unten S. 401.
1082 *Ruthig* in *Schenke/Graulich/Ruthig,* Sicherheitsrecht, § 91 BKAG Rn. 1.
1083 *Petri* in *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch, G. Rn. 459.
1084 Ähnlich *Graulich* in *Schenke/Graulich/Ruthig,* Sicherheitsrecht, § 29 BKAG Rn. 4.
1085 Siehe näher zum Datenschutz im neuen Informationswesen S. 361 ff.

d) Neues Recht und alte Dateienlandschaft nach § 91 BKAG: Verfassungsrecht und Polizeiwirklichkeit

Der Primat des Faktischen in der polizeilichen Informationsverarbeitung wird gerade auch im Übergang von alter zu neuer Architektur deutlich. Denn während INPOL-Z noch auf Grundlage alten Fassung des BKAG betrieben wird, ist die Arbeit im polizeilichen Informationsverbund durch neue Normen geregelt, die andere rechtliche Anforderungen an den Datenumgang im Informationsverbund stellen.[1086] Diesen potenziellen Konflikt hat auch der Gesetzgeber gesehen und mit der Übergangsregelung des § 91 BKAG zu lösen versucht. Die Vorschrift erlaubt dem Bundeskriminalamt eine Weiterverarbeitung seiner Datenbestände nach den Bestimmungen der für die Daten am 24. Mai 2018 jeweils geltenden Errichtungsanordnung nach § 34 a.F. BKAG in der bis zum 24. Mai 2018 geltenden Fassung. Diese Errichtungsanordnungen gelten bis zur vollständigen Umsetzung von Polizei 2020 fort.[1087] Diese legislative Entscheidung ist aus verfassungsrechtlicher Perspektive höchst problematisch.

Nachdem das verfassungsrechtliche Prinzip der Zweckbindung in Form des Grundsatzes der hypothetischen Datenneuerhebung konkretisiert wurde, muss dieser nun gem. § 12 Abs. 5 BKAG durch technische und organisatorische Vorkehrungen sichergestellt werden. Diese Verpflichtung ist einfachgesetzlich wiederum in den §§ 14, 15 BKAG ausgestaltet, die die Kennzeichnung von Daten sowie die Regelung von Zugriffsberechtigungen in einer Art und Weise erfordern, die die Einhaltung der Vorgaben des § 12 BKAG gewährleisten. Die dafür erforderlichen Änderungen in der bundeskriminalamtlichen IT-Architektur konnten indessen, aufgrund ihres nicht unerheblichen Aufwandes, mit dem Ablauf der im BKAG-Urteils vorgegebenen Frist nicht umgesetzt werden.[1088] Die infolgedessen bestehende Diskrepanz zwischen gesetzlicher Vorgabe, wie sie in den §§ 14, 15 BKAG zum Ausdruck kommt, und tatsächlicher Situation in der IT-Architektur soll nach Vorstellung des Gesetzgebers durch geeignete Maßnahmen[1089] seitens des Bundeskriminalamtes behoben werden. Grundsätzlich soll das Problem

1086 Siehe dazu bereits oben S. 230 ff.

1087 BT-Drs. 19/5923, S. 7, 9 f.; BT-Drs. 19/15346, S. 3.

1088 *Schenke/Ruthig* in *Schenke/Graulich/Ruthig,* Sicherheitsrecht, Einf. Rn. 18.

1089 Damit sind ausweislich der Gesetzesbegründungen Maßnahmen gemeint, die ein hohes Maß an Beachtung des Grundsatzes der hypothetischen Neuerhebung gewährleisten, gleichzeitig jedoch nicht dazu führen, dass – gerade auch vor dem Hintergrund der zeitaufwändigen Prozesse innerhalb des derzeitigen INPOL-Ver-

aber durch § 91 BKAG neutralisiert werden. Die Norm statuiert eine Ausnahme von der Weiterverarbeitungssperre des § 14 Abs. 2 BKAG von nicht gekennzeichneten, personenbezogenen Daten, wenn die Bestimmungen der für die Daten am 24. Mai 2018 jeweils geltenden Errichtungsanordnung nach § 34 BKAG in der bis zum 24. Mai 2018 geltenden Fassung eingehalten werden. Damit soll unumstritten die Weiterverarbeitungsmöglichkeit der bereits in den Dateien gespeicherten Altdaten in der Transitionsphase von alter Dateienlandschaft zu neuem einheitlichen Informationsbestand lückenlos gewährleistet werden.[1090] Offengelassen wurde, ob die Ausnahme auch für nach dem 24.5.2018 gespeicherte Daten gilt. Dagegen sprechen jedenfalls der Wortlaut der Übergangsregelung und die verfassungsrechtlichen Vorgaben, auf deren Grundlage man die Verfassungsmäßigkeit von § 91 BKAG insgesamt bezweifeln muss.

Auf diese Weise werden die Vorgaben des Bundesverfassungsgerichts zwar textlich im Gesetz implementiert. Die im Urteil gesetzte Umsetzungsfrist von zwei Jahren bis Mai 2018 wird aber durch § 91 BKAG faktisch missachtet. Da im derzeitigen INPOL-Z auch für neu zu speichernde Daten zumindest Ende 2019 eine Kennzeichnungspflicht nicht umgesetzt werden konnte,[1091] ist die tatsächliche Umsetzung des vom Bundesverfassungsgericht aufgestellten Grundsatz der hypothetischen Datenneuerhebung zunächst auf einen unbekannten Zeitpunkt in der Zukunft vertagt.[1092] Denn für die Praxis polizeilicher Datenverarbeitung heißt dies mit Blick auf § 12 Abs. 2 BKAG: Ist ein Datum nicht nach § 14 Abs. 1 gekennzeichnet, wird sich nur begrenzt feststellen lassen, ob eine Weiterverarbeitung über den Grundsatz der hypothetischen Datenneuerhebung möglich ist. Eine solche Nichtbeachtung des Grundsatzes der hypothetischen Datenneuerhebung verletzt das verfassungsrechtliche Verhältnismäßigkeitsprinzip, dessen Ausfluss der Zweckbindungsgrundsatz im Kontext der informationellen Selbstbestimmung ist.[1093] Mangels einer der gesetzlichen Lage entsprechenden IT-Architektur ist unklar, ob oder inwieweit die gesetzlichen und insbesondere verfassungsrechtlichen Vorgaben im Bereich polizeilicher Informationsverarbeitung gegenwärtig Beachtung finden.[1094] Auch dieser Vorgang ist

bundes, für den die Vorschrift gemäß § 29 gilt – die technische Implementierung behindert oder verzögert wird, BT-Drs. 11163, S. 95.

1090 *Ruthig* in *Schenke/Graulich/Ruthig,* Sicherheitsrecht, § 91 BKAG Rn. 1 ff.

1091 BT-Drs. 19/15346, S. 10.

1092 *Graulich* in *Schenke/Graulich/Ruthig,* Sicherheitsrecht, § 14 BKAG Rn. 1.

1093 *Graulich* in *Schenke/Graulich/Ruthig,* Sicherheitsrecht, § 14 BKAG Rn. 1.

1094 *Graulich* in *Schenke/Graulich/Ruthig,* Sicherheitsrecht, § 14 BKAG Rn. 6.

ein eindrucksvoller Beleg für die Schwächen des Rechts (und seiner legislativen Akteure) bei der verfassungsgemäßen Regulierung des polizeilichen Informationswesens.

e) Informationstechnologische Evolutionen mit rechtlichem Niederschlag

Neben den zentralen Projekten von Polizei 2020 bildet das polizeiliche Informationswesen auch weitere, seinen Wandel indizierenden informationstechnologische Strukturen aus, die als Reaktionen auf das Massendatenphänomen aufgefasst werden müssen. Die konkreten Ausformungen des technischen Wandels sind dabei mehrzweigig und betreffen unterschiedliche Bereiche des polizeilichen Tätigkeitsfelds.

aa) Predictive Policing

Für die möglichst optimale Nutzung der eigenen Datenbestände rücken Systeme, mit denen sich die Daten algorithmisch analysieren lassen, immer stärker in die polizeiliche Informationsverarbeitung. Viele der technologischen Anwendungen werden dabei unter dem aus dem englischsprachigen Raum importierten Begriff des Predictive Policing versammelt,[1095] was für den deutschsprachigen Diskurs häufig mit „vorausschauender Polizeiarbeit" übersetzt wird.[1096] Wenn auch verschiedene Begriffsverständnisse zirkulieren, scheint ein gemeinsamer definitorischer Nenner zu sein, dass es sich um computergestützte Anwendungen handelt[1097] deren primäres Ziel darin besteht, aus Daten der Vergangenheit und der Gegenwart räumlich-zeitlich möglichst exakte Vorhersagen für das Auftreten von Ereignissen zu generieren.[1098] Dabei ermöglicht die informationstechnologische Fundierung die Verarbeitung großer Datenvolumina, wie sie rein menschlicher Infor-

1095 Viel zitiert und einflussreich im englischsprachigen Diskurs etwa *Perry/McInnis/Price* ua, Predictive policing.
1096 *Gluba* Die Polizei 107 (2016), 53 (53).
1097 *Gerstner,* Predictive Policing als Instrument zur Prävention von Wohnungseinbruchdiebstahl, S. 3.
1098 *Gluba* Die Polizei 107 (2016), 53 (53).

mationsverarbeitung versagt wäre.[1099] Neu ist insofern vor allem die vom Menschen losgelöste Analyseleistung.

Unterschieden wird klassischerweise zwischen raumbezogenem und personenbezogenem Predictive Policing.[1100] In der ersten Spielart dieser neuen Form der Polizeiarbeit werden der Polizei zur Verfügung stehende Daten mit Blick auf das Aufkommen von abweichendem Verhalten an einem speziellen Ort ausgewertet, um dann auf dieser Grundlage die Häufigkeit von diesem Verhalten am untersuchten Ort zu einem zukünftigen Zeitpunkt zu prognostizieren. Es ist diejenige Variante, die weltweit am stärksten verbreitet ist.[1101] In Deutschland kommt vorausschauende Polizeiarbeit dementsprechend auch bisher quasi ausschließlich in ihrer raumbezogenen Dimension zum Einsatz, wobei deliktisch der Fokus auf Wohnungseinbrüchen liegt.[1102] Dabei wird prinzipiell darauf geachtet, dass keine personenbezogenen Daten verarbeitet werden,[1103] wobei sich der Personenbezug je nach eingesetzter Software anscheinend durchaus wieder herstellen lassen könnte.[1104] Insofern gelten Anwendungen raumbezogenen Predictive Policings als rechtlich weniger bedenklich und finden wegen des fehlenden Personenbezuges auch derzeit keinen gesetzlichen Niederschlag. Anders ist dies allerdings bei der personenbezogenen Variante gelagert.[1105] Dabei geht es darum, das Risiko für die Begehung oder auch Opferwerdung von Straftaten über die Analyse der zur Verfügung stehenden Daten zu prognostizieren und polizeilich nutzbar zu machen.[1106] In Deutschland wird eine solche Form des Predictive Policing explizit nicht praktiziert, wenngleich auch das vom Bundeskriminalamt genutzte Prognoseinstrument RADAR-

1099 *Gerstner,* Predictive Policing als Instrument zur Prävention von Wohnungseinbruchdiebstahl, S. 3.

1100 *Sommerer,* Personenbezogenes Predictive Policing, 36 ff.

1101 *Egbert/Krasmann*, Predictive Policing. Eine ethnographische Studie neuer Technologien zur Vorhersage von Straftaten und ihre Folgen für die polizeiliche Praxis., Projektabschlussbericht, 2019, 20 f.

1102 *Gerstner,* Predictive Policing als Instrument zur Prävention von Wohnungseinbruchdiebstahl, S. 1; zu den eingesetzten Systemen s. den Überblick bei Arzt in *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch des Polizeirechts, G. Rn. 1300.

1103 *Gerstner,* Predictive Policing als Instrument zur Prävention von Wohnungseinbruchdiebstahl, S. 3.

1104 BWLfDI, 32. Tätigkeitsbericht 2014/2015, S. 44.

1105 Grundlegend *Sommerer,* Personenbezogenes Predictive Policing.

1106 *Egbert/Krasmann*, Predictive Policing. Eine ethnographische Studie neuer Technologien zur Vorhersage von Straftaten und ihre Folgen für die polizeiliche Praxis., Projektabschlussbericht, 2019, 12 f.

iTE (Regelbasierte Analyse potenziell destruktiver Täter zur Einschätzung des akuten Risikos – islamistischer Terrorismus) oder auch die Fluggastdatenspeicherung als diesem Kontext unterfallend diskutiert werden.[1107]

bb) Analysesysteme

Neben diesen Formen des Predictive Policing ist in letzter Zeit noch ein weiterer informationstechnologischer Verfahrenstyp aufgekommen, um die Datenbestände des polizeilichen Informationswesens besser nutzbar zu machen. Anders als raum- oder personenbezogenes Predictive Policing, das regelmäßig mit Risikoscores arbeitet[1108] und damit – auch bei Risikoskalen – häufig ein binäres Ergebnis (eingriffsrelevante Risikoschwelle überschritten: ja oder nein) liefert, wodurch das anschließende polizeiliche Handeln prinzipiell vorstrukturiert wird, arbeiten diese Systeme offener. Dazu gehört etwa die „Automatisierte Anwendung zur Datenanalyse" in § 25a HSOG, die „Automatisierte Anwendung zur Auswertung von Daten" in § 49 HmbPolDVG oder auch das „System zur Datenbankübergreifenden Analyse und Recherche" (DAR) in Nordrhein-Westfalen gemäß § 23 Abs. 6 PolG NRW.[1109] Mit diesen Systemen werden die in heterogenen Datenspeichern vorgehaltenen Daten der Polizei virtuell in einer Analyseplattform vereinigt. Diese greift auf die grundsätzlich voneinander getrennte INPOL-Auskunftskomponente, das Vorgangsbearbeitungs- sowie das Fallbearbeitungssystem zu und macht die Daten, die in diesen für die polizeiliche Informationsarbeit wichtigsten Quellsysteme vorgehalten werden, zur datenbankübergreifenden Recherche, Verknüpfung und Analyse verfügbar.[1110] Durch die Anwendungen werden die heterogenen Datenbestände virtuell homogenisiert und lassen sich damit einfacher und schneller durchsuchen

1107 Siehe etwa *Arzt* in *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch des Polizeirechts, G. Rn. 1302, 1330.

1108 Vgl. *Egbert/Krasmann*, Predictive Policing. Eine ethnographische Studie neuer Technologien zur Vorhersage von Straftaten und ihre Folgen für die polizeiliche Praxis., Projektabschlussbericht, 2019, 20, 29, 31, 33.

1109 Auch Bayern hat einen Rahmenvertrag mit dem Unternehmen Palantir geschlossen, der es anderen Ländern erlaubt, das ausgewählte Produkt, eine verfahrensübergreifende Recherche- und Analyseplattform (VeRA), ohne Vergabeverfahren selbstständig abzurufen, s. BVerfG-Urteil des Ersten Senats vom 16. Februar 2023 (Automatisierte Datenanalyse), Rn. 15.

1110 HessLT-Drs. 20/660, S. 1 ff.

und vernetzen. Zudem können weitere Datenquellen integriert werden.[1111] Mit den Systemen ist folglich eine enorme Steigerung des informationellen Gehalts der polizeilichen Datenbestände beabsichtigt. Analysesysteme stehen emblematisch für die polizeiliche Informationsverarbeitung im Massendatenkontext und sollen aufgrund dieser Relevanz hier eingehender mit Blick auf ihre rechtlichen Implikationen analysiert werden.

(1) Das Urteil des Bundesverfassungsgerichts vom 16. Februar 2023

Alle vorgenannten Anwendungen setzen maßgeblich auf komplexere informationstechnische Algorithmen, die teilweise automatisiert auf die Rechercheimpulse ihrer Nutzer:innen reagieren. Mittlerweile ist bekannt, welche Problemlagen der gesellschaftliche Einsatz von Algorithmen mit sich bringen,[1112] woraus sich ein besonderes rechtliches Anforderungsprogramm bei der Regulierung von Algorithmen ergibt.[1113] Auch der Erste Senat des Bundesverfassungsgerichts hat sich nunmehr mit einem Urteil vom 16. Februar 2023 zu den Rechtsgrundlagen der Anwendungen zur automatisierten Datenanalyse in Hamburg und Hessen geäußert und beide Vorschriften in ihrer gegenwärtigen Form für verfassungswidrig erklärt. Bereits zuvor hatte das Gericht begonnen, im Kontext des nachrichtendienstlichen Informationsrechts Leitlinien für die Nutzung von Datenanalyse-Instrumenten zu entwickeln. Diese sollen hier kurz nachgezeichnet werden, um darauf aufbauend das Urteil zur polizeilichen automatisierten Datenanalyse darzustellen.

Zunächst hatte das Gericht in der BND-Entscheidung in diesem Kontext Regelungen insbesondere bezüglich der Sicherstellung der grundsätzlichen Nachvollziehbarkeit für unabhängige Kontrolle für erforderlich gehalten.[1114] Wichtiger, weil ausführlicher, waren für polizeiliche Analysesysteme aber insofern die Ausführungen des Gerichts in seinem zweiten Urteil zum ATDG. In der Entscheidung hatte das Bundesverfassungsgericht unter anderem zu klären, ob die sogenannte erweiterte projektbezogene Datennutzung der Antiterrordatei den Anforderungen des Rechts auf informatio-

1111 HessLT-Drs. 19/6864, S. 18.
1112 *O'Neil,* Weapons of math destruction; *Pasquale,* The Black Box Society; *Noble,* Algorithms of oppression.
1113 Siehe grundlegend dazu *Martini,* Blackbox Algorithmus – Grundfragen einer Regulierung Künstlicher Intelligenz, 27 ff.
1114 BVerfGE 154, 152 (260) – BND: Ausland-Ausland-Fernmeldeaufklärung.

nelle Selbstbestimmung genügte. Eine solche Datennutzung meint gemäß § 6a Abs. 5 S. 1 ATDG das Herstellen von Zusammenhängen zwischen Personen, Personengruppierungen, Institutionen, Objekten und Sachen, der Ausschluss von unbedeutenden Informationen und Erkenntnissen, die Zuordnung eingehender Informationen zu bekannten Sachverhalten sowie die statistische Auswertung der gespeicherten Daten. Darin wird vom Gericht ein typischer Fall des „Data-Mining" gesehen, was nach einer Definition der Bundesregierung vorläge, wenn Verfahren und Methoden eingesetzt werden, „mit deren Hilfe bereits vorhandene große Datenbestände, zumeist auf statistisch-mathematischen Verfahren basierend, selbständig auf Zusammenhänge analysiert werden, um auf diesem Wege neues Wissen zu generieren." Da eine solche Verknüpfung von Daten etwa mehrstufige Analysen ermögliche, die neue Verdachtsmomente erst erzeugen, sowie weitere Analyseschritte oder auch daran anschließende operative Maßnahmen denkbar mache, gehen von der Maßnahme erhebliche Beeinträchtigungswirkungen aus.[1115] Neben der hier auszuklammernden Frage, wie sich die Verschränkung der Informationsbestände von Polizeien und Nachrichtendiensten in diesem Kontext konkret auswirkt, war vor allem das das eigentliche Verfahren der Verknüpfung gespeicherter Daten zur Erzeugung neuer Erkenntnisse und Zusammenhänge verfassungsrechtlich zu bewerten. Dieses könne eine erhebliche Persönlichkeitsrelevanz aufweisen, wobei das Eingriffsgewicht noch weiter erhöht ist, wenn die neuen Erkenntnisse und Zusammenhänge sodann auch durch die Polizeien operativ nutzbar gemacht werden können.[1116] Mit diesem Urteil knüpft das Bundesverfassungsgericht an eine Idee am ursprünglichen konzeptuellen Fundament der informationellen Selbstbestimmung an: Die informationstechnologischen Verarbeitungs- und Verknüpfungsmöglichkeiten begründen überhaupt erst die Notwendigkeit des Schutzes von Daten und bestimmen ganz maßgeblich über die Eingriffstiefe mit.[1117] Allerdings war bereits das zweite Urteil zur Rasterfahndung davon ausgegangen, dass angesichts der Menge und Vielfalt der personenbezogenen Daten, die heute über nahezu jede Person vorhanden sind, die Rasterfahndung nahe an die von der Verfassung verbotene Praxis der Erstellung von teilweisen oder vollständigen Persönlich-

1115 BVerfGE 156, 11 (40) – Antiterrordateigesetz II.
1116 BVerfGE 156, 11 (52) – Antiterrordateigesetz II.
1117 BVerfGE 65, 1 (44) – Volkszählung.

keitsbildern rücke.[1118] Insofern bestehen auch für das Data-Mining hohe Hürden für eine verfassungsrechtliche Zulässigkeit.

Für die Nutzung solcher Verfahren durch die auch operativ tätigen Polizeien sah das Gericht vor allem die zu schützenden Rechtsgüter und die diesbezüglichen Eingriffsschwellen als neuralgischen Punkt für die verfassungsrechtliche Bewertung.[1119] So ist sicherheitsbehördliches Data-Mining grundsätzlich zum Schutze besonders gewichtiger Rechtsgüter wie Leib, Leben und Freiheit der Person sowie Bestand oder Sicherheit des Bundes oder eines Landes zulässig.[1120] Allerdings sind weiterhin spezifische Anforderungen an die Eingriffsschwelle zu stellen. Geht es um die Abwehr von Gefahren muss eine „wenigstens hinreichend konkretisierte Gefahr in dem Sinne (…) [gegeben sein], dass zumindest tatsächliche Anhaltspunkte für die Entstehung einer konkreten Gefahr vorliegen."[1121] Dabei „genügt es nicht, wenn das Gesetz allein verlangt, dass Tatsachen vorliegen, die die Annahme rechtfertigen, dass eine Straftat begangen werden soll, weil dies nicht ausschließt, dass sich die behördliche Prognose allein auf Erfahrungssätze stützt."[1122] Die Behörde muss vielmehr ein „wenigstens seiner Art nach konkretisiertes und absehbares Geschehen" erkennen oder erkennen, „dass das individualisierte Verhalten einer Person die konkrete Wahrscheinlichkeit begründet, dass sie in absehbarer Zeit terroristische Straftaten begeht."[1123] Während darin keine Verschärfung des herkömmlichen Gefahrerfordernisses liegt, ist das Bundesverfassungsgericht im repressiven Bereich strenger. Ein einfacher Tatverdacht genügt nicht, vielmehr muss die etwaige Rechtsgrundlage verlangen, dass bestimmte, den Verdacht begründende Tatsachen vorliegen", also „dass insoweit konkrete und in gewissem Umfang verdichtete Umstände als Tatsachenbasis für den Verdacht vorhanden" sind.[1124]

Diese Vorgaben hat das Bundesverfassungsgericht in seinem Urteil vom 16. Februar 2023 nunmehr aktualisiert und spezifiziert. Der Prüfungsgegenstand des Urteils beschränkte sich dabei auf die Eingriffsschwelle in

1118 BVerfGE 115, 320 (350 f.) – Rasterfahndung II.
1119 BVerfGE 156, 11 (49) – Antiterrordateigesetz II.
1120 BVerfGE 156, 11 (56) – Antiterrordateigesetz II.
1121 BVerfGE 156, 11 (54) – Antiterrordateigesetz II.
1122 BVerfGE 156, 11 (61) – Antiterrordateigesetz II.
1123 BVerfGE 156, 11 (61) – Antiterrordateigesetz II.
1124 BVerfGE 156, 11 (55) – Antiterrordateigesetz II.

§ 25a HSOG, § 49 HmbPolDVG;[1125] im Übrigen waren die Verfassungsbeschwerden als unzulässig verworfen worden. Explizit ausgeklammert war damit die Frage, „ob die Gesetzgeber verfassungsrechtlich ausreichende Regelungen zu den durch die Datenanalyse oder -auswertung nach § 25a HSOG und § 49 HmbPolDVG zu schützenden Rechtsgütern getroffen haben." Auch wurde nicht überprüft, „ob die für Transparenz und Rechtsschutz sorgenden Verfahrens- und Organisationsregelungen verfassungsrechtlichen Anforderungen genügen, ob insbesondere auch mit Blick auf komplexe Formen automatisierten Datenabgleichs bis hin zu selbstlernenden Systemen hinreichende verfahrensrechtliche Sicherungen bestehen." Ferner wurde nicht verfassungsrechtlich überprüft, „ob der verfassungsrechtliche Grundsatz der Zweckbindung bereits erhobener personenbezogener Daten gewahrt ist, ob also insbesondere auch hinreichend begrenzt ist, inwiefern Daten, die unter Eingriff in Art. 13 Abs. 1 GG oder Art. 10 Abs. 1 GG erhoben worden sind, weiter genutzt werden dürfen. Auch gelten die Ausführungen des Urteils nur für den Einsatz der Datenanalyse zu Zwecken der vorbeugenden Straftatbekämpfung." Die Befugnis zur Abwehr von Gefahren blieb also von den Ausführungen des Gerichts unberührt.[1126]

(2) Verfassungsrechtliche Anforderungen an Analysesysteme

Die dem Verfahren zugrundeliegenden[1127] Vorschriften ermöglichen grundsätzlich zwei Formen des Informationseingriffes, mit je eigenem Eingriffsgewicht[1128]: Einerseits liegt in der automatisierten Auswertung der gespeicherten Daten eine weitere Nutzung, d.h. eine erneut nach dem Grundsatz der Zweckbindung rechtfertigungsbedürftige Datenverarbeitung. Darüber hinaus liegt ein Grundrechtseingriff „nicht nur in der weiteren, zusammenführenden Verwendung vormals getrennter Daten, sondern [auch] in der Erlangung besonders grundrechtsrelevanten neuen Wissens, das durch die

1125 Siehe dazu und zu den folgenden zitierten Passagen BVerfG-Urteil des Ersten Senats vom 16. Februar 2023 (Automatisierte Datenanalyse), Rn. 48.

1126 BVerfG-Urteil des Ersten Senats vom 16. Februar 2023 (Automatisierte Datenanalyse), Rn. 49.

1127 Die Ausführungen beanspruchen indessen Geltung für andere Datenanalyse-Rechtsgrundlagen bzw. -verfahren.

1128 BVerfG-Urteil des Ersten Senats vom 16. Februar 2023 (Automatisierte Datenanalyse), Rn. 54.

automatisierte Datenanalyse oder -auswertung geschaffen werden kann."[1129] Als insofern erforderlichen legitimen Zweck für den Erlass der Vorschriften hat das Gericht den Zweck anerkannt, „vor dem Hintergrund informationstechnischer Entwicklung die Wirksamkeit der vorbeugenden Bekämpfung schwerer Straftaten zu steigern, indem Anhaltspunkte für bevorstehende schwere Straftaten gewonnen werden, die im Datenbestand der Polizei ansonsten unerkannt blieben."[1130] Dies sei der Fall, da – wie es die hessische Landesregierung dargelegt habe – „die Polizeibehörden […] infolge der insbesondere in den Bereichen terroristischer und extremistischer Gewalt sowie der organisierten und schweren Kriminalität zunehmenden Nutzung digitaler Medien und Kommunikationsmittel mit einem ständig anwachsenden und nach Qualität und Format zunehmend heterogenen Datenaufkommen konfrontiert [seien]."[1131]

Wie jeder Informationseingriff sind auch Rechtsgrundlagen für die Datenanalyse zunächst an den Rechtfertigungsanforderungen zu messen, die der Grundsatz der Zweckbindung und Zweckänderung aufstellt. Insofern ist die im Urteil zum Bundeskriminalamtsgesetz entwickelte Dogmatik der zweckwahrenden und zweckändernden Weiternutzung zu beachten.[1132] Das Gericht fordert im Rahmen der „zweckwahrenden" Weiternutzung von Daten für die Wahrung der Zweckbindung grundsätzlich[1133] nicht, dass erneut die Anlassschwelle (etwa in Form eines Anfangsverdacht) der Datenerhebungsnorm erfüllt ist, sodass eine Nutzung als bloßer Spurenansatz auch im Rahmen der Verarbeitung im Wege der automatisierten Datenanalyse denkbar ist.[1134] Auch für die zweckändernde Weiternutzung ergeben sich im Kontext der automatisierten Datenanalyse insofern keine über das Urteil zum Bundeskriminalamtsgesetz hinausgehenden Besonderheiten.[1135] Da die

1129 BVerfG-Urteil des Ersten Senats vom 16. Februar 2023 (Automatisierte Datenanalyse), Rn. 50.
1130 BVerfG-Urteil des Ersten Senats vom 16. Februar 2023 (Automatisierte Datenanalyse), Rn. 52.
1131 Ebd.
1132 BVerfG-Urteil des Ersten Senats vom 16. Februar 2023 (Automatisierte Datenanalyse), Rn. 55; siehe dazu bereits oben S. 164 ff.
1133 Anders ist dies nach wie vor für Daten aus Wohnraumüberwachungen und Online-Durchsuchungen, siehe BVerfG-Urteil des Ersten Senats vom 16. Februar 2023 (Automatisierte Datenanalyse), Rn. 59.
1134 BVerfG-Urteil des Ersten Senats vom 16. Februar 2023 (Automatisierte Datenanalyse), Rn. 58.
1135 Vgl. BVerfG-Urteil des Ersten Senats vom 16. Februar 2023 (Automatisierte Datenanalyse), Rn. 60 ff.

Vorschriften aus Hamburg und Hessen beide Weiterverarbeitungsmodalitäten zulassen, ist aus bundesverfassungsrechtlicher Sicht die Kennzeichnung der Daten zentral, um die Einhaltung der Zweckbindungsregeln überhaupt überprüfen zu können.[1136]

Neben diesen Aspekten, bei denen es im Wesentlichen um das Eingriffsgewicht der einer Datenanalyse vorangegangenen Datenerhebungen geht, stellt das Bundesverfassungsgericht weitere befugnisspezifische Rechtfertigungsanforderungen auf, die in den der automatisierten Datenanalyse per se inhärenten Belastungseffekten begründet liegen. Dabei ist das Eingriffsgewicht der Datenanalyse als solche nicht statisch, sondern hängt variabel von der näheren Ausgestaltung der Befugnis – und damit auch der Anwendung – ab.[1137] Die automatisierte Datenanalyse kann dabei ein über die ursprüngliche Erhebung hinausgehendes Eingriffsgewicht haben. Denn sie ist darauf gerichtet, neues Wissen zu generieren, indem – wie es die dem Verfahren zugrundeliegenden Vorschriften ermöglichen sollten – Zusammenhänge zwischen Personen, Personengruppierungen, Institutionen, Organisationen, Objekten und Sachen hergestellt werden. Damit – so das Gericht – kann die „handelnde Behörde aus den zur Verfügung stehenden Daten mit praktisch allen informationstechnisch möglichen Methoden weitreichende Erkenntnisse abschöpfen sowie aus der Auswertung neue Zusammenhänge erschließen. Die Verknüpfung von Daten ermöglicht etwa mehrstufige Analysen, die neue Verdachtsmomente erst erzeugen, sowie weitere Analyseschritte oder auch daran anschließende operative Maßnahmen."[1138] Zwar ist dies grundsätzlich ein Bestandteil polizeilicher Kerntätigkeiten.[1139] Gerade die Ermöglichung der Verarbeitung komplexer Informationsbestände ist jedoch neu. Die Maßnahme „erschließt die in den Daten enthaltenen Informationen […] intensiver als zuvor." Insofern können nicht nur verborgene Informationen über eine Person zutage gefördert werden, sondern es findet eine Annäherung an Profiling-Verfahren (Art. 4 Nr. 4 DS-GVO) statt, da „sich softwaregestützt neue Möglichkeiten einer Vervollständigung des Bildes von einer Person ergeben [können], wenn Daten

1136 BVerfG-Urteil des Ersten Senats vom 16. Februar 2023 (Automatisierte Datenanalyse), Rn. 65.
1137 BVerfG-Urteil des Ersten Senats vom 16. Februar 2023 (Automatisierte Datenanalyse), Rn. 66.
1138 BVerfG-Urteil des Ersten Senats vom 16. Februar 2023 (Automatisierte Datenanalyse), Rn. 67.
1139 BVerfG-Urteil des Ersten Senats vom 16. Februar 2023 (Automatisierte Datenanalyse), Rn. 68.

und algorithmisch errechnete Annahmen über Beziehungen und Zusammenhänge aus dem Umfeld der Betroffenen einbezogen werden."[1140] Zudem kann „auch die Kombination personenbezogener und nicht personenbezogener Daten und gegebenenfalls die algorithmentypische Berücksichtigung bloßer Korrelationen neue, sonst nicht sicht- oder ermittelbare persönlichkeitsrelevante Aufschlüsse geben."[1141] Das besondere Eingriffsgewicht der automatisierten Datenanalyse ergibt sich für das Bundesverfassungsgericht – in konsequenter Aktualisierung der schon im Volkszählungsurteil angelegten Grundgedanken – in der Überwindung der tatsächlichen Kapazitäts- bzw. praktischen Erkenntnisgrenzen der bisherigen informationellen Polizeiarbeit. Es kann insoweit aus der Sicht des Gerichts zu einer entscheidenden Veränderung von Arbeitsweise und Erkenntnismöglichkeiten der Polizei kommen, der dann allein mit dem verfassungsrechtlichen Grundsatz der Zweckbindung nicht mehr Rechnung getragen werden kann.[1142]

Anlässlich dieser neuen Eingriffsqualität der automatisierten Datenanalyse als informationelle Maßnahme hat das Bundesverfassungsgericht generelle Maßstäbe für die Bestimmung des – aufgrund der vielen Ausgestaltungsmöglichkeiten gesetzlicher Vorschriften variierenden – Eingriffsgewichts festgelegt.[1143] Grundsätzlich gilt, dass bei einer Begrenzung der Befugnis auf schlichte Formen des Abgleichs einer begrenzten Zahl von Daten näher eingegrenzter Herkunft nur ein geringes befugnisspezifisches Eingriffsgewicht anzunehmen ist. Es nimmt umgekehrt zu, je weiter die Möglichkeiten durch die gesetzliche Ausgestaltung reichen; dann reicht auch der Grundsatz der Zweckbindung für sich genommen zunehmend weniger zur Rechtfertigung aus.[1144] Bei schweren Informationseingriffen durch Anwendungen der automatisierten Datenanalyse – etwa die Erstellung von genaueren Bewegungs-, Verhaltens- oder Beziehungsprofilen oder Einbeziehung von Personen, die objektiv nicht zurechenbar in das relevante Geschehen verfangen sind – gelten die Voraussetzungen für eingriffs-

1140 BVerfG-Urteil des Ersten Senats vom 16. Februar 2023 (Automatisierte Datenanalyse), Rn. 69.
1141 BVerfG-Urteil des Ersten Senats vom 16. Februar 2023 (Automatisierte Datenanalyse), Rn. 69.
1142 BVerfG-Urteil des Ersten Senats vom 16. Februar 2023 (Automatisierte Datenanalyse), Rn. 70.
1143 BVerfG-Urteil des Ersten Senats vom 16. Februar 2023 (Automatisierte Datenanalyse), Rn. 71.
1144 BVerfG-Urteil des Ersten Senats vom 16. Februar 2023 (Automatisierte Datenanalyse), Rn. 72.

intensive heimliche Überwachungsmaßnahmen.[1145] Grundsätzlich finden insofern die bereits bekannten Faktoren für die Bestimmung des Eingriffsgewichts Anwendung.[1146] Im Kontext der automatisierten Datenanalyse betont das Bundesverfassungsgericht neben dem Ausmaß des persönlichkeitsrelevanten Wissens sowie der Frage, ob eine Person durch ihr Verhalten zurechenbar Anlass für eine sie treffende Datenanalyse und daran anschließende operative Maßnahmen gegeben hat, vor allem auch den Umfang von Diskriminierungsrisiken – diese sind umso weniger hinzunehmen, „je mehr sich die Wirkungen der automatisierten Datenanalyse […] einer nach Art. 3 Abs. 3 GG unzulässigen Benachteiligung annähern können."[1147]

Vor allem Art und Umfang der Daten – wie es generell für polizeiliche Informationseingriffe und ganz besonders für die elektronische Datenverarbeitung gilt – bestimmen das Eingriffsgewicht einer automatisierten Datenanalyse.[1148] Hier sind verschiedene Variierungen möglich, die sich auf die informationelle Intensität einer Datenanalyse auswirken können: Denkbar ist, die Datenherkunft zu begrenzen, etwa auf von der Polizei (eines Bundeslandes) oder einer inländischen Behörde selbst erhobene Daten, oder Daten aus sozialen Netzwerken auszuschließen.[1149] Eine Eingrenzung kann auch mit Blick auf die „Umstände der Ersterhebung gesetzlich nach Art und Menge" insofern erfolgen, als – in der Regel durch technisch-organisatorische Sicherungen – gewährleistet wird, dass Daten nur gemäß ihrer rechtlichen Verwendbarkeit verarbeitet werden; in der Sache geht es also um eine strikte Beachtung der Zweckbindung.[1150] Allerdings ist auch eine aufgabenbezogene[1151] (etwa: „Terrorismusbekämpfung") oder stark auf die

1145 BVerfG-Urteil des Ersten Senats vom 16. Februar 2023 (Automatisierte Datenanalyse), Rn. 73; letztlich handelt es sich bei der automatisierten Datenanalyse auch um eine heimliche Überwachungsmaßnahme; siehe grundlegend dazu *Schwabenbauer,* Heimliche.

1146 BVerfG-Urteil des Ersten Senats vom 16. Februar 2023 (Automatisierte Datenanalyse), Rn. 76; siehe dazu bereits oben S. 156 ff. sowie BVerfGE 156, 11 48 f. mwN.

1147 BVerfG-Urteil des Ersten Senats vom 16. Februar 2023 (Automatisierte Datenanalyse), Rn. 77.

1148 BVerfG-Urteil des Ersten Senats vom 16. Februar 2023 (Automatisierte Datenanalyse), Rn. 78.

1149 BVerfG-Urteil des Ersten Senats vom 16. Februar 2023 (Automatisierte Datenanalyse), Rn. 79.

1150 BVerfG-Urteil des Ersten Senats vom 16. Februar 2023 (Automatisierte Datenanalyse), Rn. 80.

1151 BVerfG-Urteil des Ersten Senats vom 16. Februar 2023 (Automatisierte Datenanalyse), Rn. 82.

Erforderlichkeit[1152] fokussierende Eingrenzung der einzubeziehenden Daten denkbar. Verfassungsrechtlich ist eine Begrenzung nach den Eingriffsmodalitäten besonders dort zu beachten, wo Daten aus besonders schwerwiegenden Grundrechtseingriffen stammen, wobei hier ohnehin bereits die insofern entwickelten anlass- und zweckbezogenen Schwellen des sicherheitsbehördlichen Informationsverfassungsrechts für solche eingriffsintensiven Maßnahmen zu beachten sind.[1153] Eingriffsmildernd soll zudem eine Beschränkung der verwendeten Daten dahingehend sein, dass diese von Anlass- oder Kontaktpersonen stammen.[1154] Auch über Aufbewahrungs- und Löschfristen lässt sich die Intensität der Datenanalyse modulieren – hier gelten vor allem im Zusammenhang mit der Einbeziehung von Verkehrsdaten erhöhte Anforderungen mit Blick auf die Begrenzung der erfassbaren Datenmengen sowie die Höchstspeicherungsdauer.[1155] Ferner ist der Automatisierungsgrad der Anwendung von Relevanz. Müssen Dateien für jeden Analysevorgang händisch hinzugezogen werden, schwächt es die informationelle Intensität des Eingriffs; umgekehrt wirkt beispielsweise eine Anbindung ans Internet eingriffsverstärkend.[1156] Ähnlich wirkt die technisch-organisatorische Ausgestaltung des Betriebs der automatisierten Datenanalyse: Darf diese nur von einem begrenzten Mitarbeiter:innen-Kreis verwendet werden, so ist das Eingriffsgewicht geringer, denn „[j]e weniger Personen Zugriff auf das Analyseinstrument haben und je zielgenauer der Zugriff erfolgt, umso weniger Analyse- und Auswertungsvorgänge dürften tendenziell in Gang gesetzt und werden und umso weniger Daten werden verarbeitet."[1157] Bezüglich der Datenarten gilt schließlich: Je beschränkter die einbeziehbaren Dateiformate (etwa Bilder-, Video- oder

1152 BVerfG-Urteil des Ersten Senats vom 16. Februar 2023 (Automatisierte Datenanalyse), Rn. 83

1153 BVerfG-Urteil des Ersten Senats vom 16. Februar 2023 (Automatisierte Datenanalyse), Rn. 81.

1154 BVerfG-Urteil des Ersten Senats vom 16. Februar 2023 (Automatisierte Datenanalyse), Rn. 84; das Gericht verwendet nicht genau diese Terminologie (siehe näher dazu unten S. 324 ff.), meint aber letztlich dasselbe.

1155 BVerfG-Urteil des Ersten Senats vom 16. Februar 2023 (Automatisierte Datenanalyse), Rn. 85.

1156 BVerfG-Urteil des Ersten Senats vom 16. Februar 2023 (Automatisierte Datenanalyse), Rn. 88.

1157 BVerfG-Urteil des Ersten Senats vom 16. Februar 2023 (Automatisierte Datenanalyse), Rn. 89.

Audioaufnahmen oder biometrische Daten), desto weniger eingriffsintensiv die Rechtsgrundlage.[1158]

Daneben sind die durch die gesetzliche Regelung zugelassenen Methoden der Datenanalyse maßgebend. Generell gilt hier, dass der Komplexitätsgrad der Methode bestimmend ist, denn die Methode ist „umso eingriffsintensiver, je breitere und tiefere Erkenntnisse über Personen dadurch erlangt werden können, je höher die Fehler- und Diskriminierungsanfälligkeit ist und je schwerer die softwaregestützten Verknüpfungen nachvollzogen werden können."[1159] Das Bundesverfassungsgericht zieht hier als wenig(er) eingriffsintensive Vergleichskategorie die Maßnahme des Datenabgleichs[1160] heran, bei dem regelmäßig Daten eines Betroffenen an gespeicherten Daten vorbeigeführt werden, um Übereinstimmungen festzustellen, oder aber Daten eines Bestandes in einen anderen überführt werden. Das Eingriffsgewicht ist hier vor allem an die Zahl der vorprogrammierten, also ohne menschliches Zutun veranlassten, Abgleichschritte und Verknüpfungen gekoppelt.[1161] Umgekehrt wirkt dementsprechend die zunehmende Offenheit eines Suchvorgangs, der nur begrenzt „durch – auch mit Erkenntnissen und Annahmen zu dem konkreten Sachverhalt gespeiste – polizeiliche Suchmuster" strukturiert ist, eingriffsintensivierend.[1162] Das gilt vor allem wenn – wie im Kontext der vorbeugenden Straftatenbekämpfung in besonderer Weise der Fall – ohne konkreten Sachverhaltsbezug durch die Analyse überhaupt erst Anhaltspunkte für polizeiliches Tätigwerden generiert werden, insbesondere dann, wenn es um die Identifizierung von statistischen Auffälligkeiten in den Datenmengen und deren (automatisierte) weitere Verknüpfung mit bestimmten Datenbeständen zur Generierung vollkommen neuer, zuvor außerhalb des polizeilichen Suchfokus liegender Informationen geht.[1163] Ferner gewinnt der Informationseingriff an Gewicht, „wenn Suchvorgänge nicht auf näher

1158 BVerfG-Urteil des Ersten Senats vom 16. Februar 2023 (Automatisierte Datenanalyse), Rn. 87.
1159 BVerfG-Urteil des Ersten Senats vom 16. Februar 2023 (Automatisierte Datenanalyse), Rn. 90.
1160 Siehe näher dazu unten S. 351 ff.
1161 BVerfG-Urteil des Ersten Senats vom 16. Februar 2023 (Automatisierte Datenanalyse), Rn. 91.
1162 BVerfG-Urteil des Ersten Senats vom 16. Februar 2023 (Automatisierte Datenanalyse), Rn. 93.
1163 BVerfG-Urteil des Ersten Senats vom 16. Februar 2023 (Automatisierte Datenanalyse), Rn. 93.

umschreibbare Personen ausgerichtet sind und keine sachliche Verbindung zwischen dem gefährdeten Rechtsgut und den von der automatisierten Anwendung Betroffenen vorausgesetzt wird", da ein Personenbezug dann überhaupt erst durch die Maßnahme hergestellt wird und damit das Risiko steigt, „dass Personen in weitere polizeiliche Maßnahmen einbezogen werden, die dafür keinen zurechenbaren Anlass gegeben haben."[1164] Die mit einer offenen Suche verbundenen Gefahren können aber durch eine „anspruchsvoll gestaltete Eingriffsschwelle verringert" oder „durch eine Einschränkung der Datenverarbeitungsmethode gesenkt werden". Verfassungsrechtlich unzulässig ist jedenfalls „[e]ine weder im Einzelfall durch einen konkreten Anlass getragene noch durch Vorgaben zur Verarbeitungsmethode inhaltlich eingeschränkte automatisierte Durchsuchung großer Bestände personenbezogener Daten auf bislang unbekannte Gesetzmäßigkeiten und gefahrenabwehrrechtlich bedeutende Zusammenhänge hin".[1165] Im Kontext der Auswertung großer Datenmengen, insbesondere auf statistische Zusammenhänge hin, statuiert das Gericht ferner eine Pflicht zur Sicherstellung ausreichender Datenqualität sowie zum Treffen von Vorkehrung dagegen, „dass die Auswahl der einbezogenen Daten unangemessen verzerrende, diskriminierende Wirkungen entfalten kann."[1166] Eine weitere grundlegende Weiche für das Eingriffsgewicht ist das Erkenntnisobjekt – das Bundesverfassungsgericht spricht hier von der „Art von Suchergebnissen":[1167] Weniger eingriffsintensiv ist die Erkennung gefährlicher oder gefährdete Orte,[1168] besonders eingriffsintensiv hingegen, „wenn Ergebnis der automatisierten Anwendung personenbezogene Erkenntnisse sind und dieses Ergebnis maschinelle Sachverhaltsbewertungen enthält, die also über die bloße Anzeige von Übereinstimmungen zwischen dem Suchkriterium und den durchsuchten Daten hinausgehen", wobei insbesondere eingriffsintensivierend wirkt, „wenn im Sinne eines „predictive policing" maschinell

1164 BVerfG-Urteil des Ersten Senats vom 16. Februar 2023 (Automatisierte Datenanalyse), Rn. 94.
1165 BVerfG-Urteil des Ersten Senats vom 16. Februar 2023 (Automatisierte Datenanalyse), Rn. 95.
1166 BVerfG-Urteil des Ersten Senats vom 16. Februar 2023 (Automatisierte Datenanalyse), Rn. 95.
1167 BVerfG-Urteil des Ersten Senats vom 16. Februar 2023 (Automatisierte Datenanalyse), Rn. 96.
1168 BVerfG-Urteil des Ersten Senats vom 16. Februar 2023 (Automatisierte Datenanalyse), Rn. 97.

Gefährlichkeitsaussagen über Personen getroffen werden."[1169] Dabei kann der Informationseingriff, der in der Generierung neuen Wissens durch eine Anwendung automatisierte Datenanalyse besteht, dadurch abgemildert werden, dass eine weitere Schwelle für die Weiterverwendung entsprechender Erkenntnisse eingezogen wird.[1170] Für das Eingriffsgewicht von besonderer Bedeutung ist schließlich die Frage, ob lernfähige Systeme, also Anwendungen Künstlicher Intelligenz, Verwendung finden.[1171] Deren spezifische Gefahren liegen nach Auffassung des Verfassungsgerichts im Bereich der polizeilichen Datenanalyse darin, dass Erkenntnismuster automatisiert weiterentwickelt oder überhaupt erst generiert und dann in weiteren Analysestufen weiter verknüpft werden, wodurch besonders weitgehende Informationen und Annahmen über Personen erzeugt, diese regelmäßig aber zugleich nur unter erschwerten Bedingungen nachgeprüft werden können; derartige selbstlernende, aber bei entsprechender Komplexität auch deterministische,[1172] Systeme dürfen in der Polizeiarbeit nur unter besonderen verfahrensrechtlichen Vorkehrungen zur Anwendung kommen, die trotz der eingeschränkten Nachvollziehbarkeit ein hinreichendes Schutzniveau etwa vor Diskriminierungseffekten oder – bei Verwendung einer von privaten entwickelten Software – vor Manipulation sowie unbemerktem Zugriff auf Daten durch Dritte aufweisen.[1173] Damit eng verknüpft ist auch die generelle Fehleranfälligkeit der eingesetzten Technologien sowie die Möglichkeit, problematische Abläufe zu identifizieren – je schwieriger dies ist, desto eingriffsintensiver wird die Datenanalyse.[1174]

Das informationelle Gewicht einer Rechtsgrundlage zur automatisierten Datenanalyse wird neben den soeben dargelegten befugnisspezifischen Belastungseffekten zudem noch durch korrespondierende Eingriffsvoraussetzungen bestimmt. Das Gebot der Verhältnismäßigkeit im engeren Sinne statuiert insofern Anforderungen an das mit der Maßnahme zu schützende

1169 BVerfG-Urteil des Ersten Senats vom 16. Februar 2023 (Automatisierte Datenanalyse), Rn. 98.
1170 BVerfG-Urteil des Ersten Senats vom 16. Februar 2023 (Automatisierte Datenanalyse), Rn. 99.
1171 Siehe dazu bereits oben S. 77 ff.
1172 BVerfG-Urteil des Ersten Senats vom 16. Februar 2023 (Automatisierte Datenanalyse), Rn. 101.
1173 BVerfG-Urteil des Ersten Senats vom 16. Februar 2023 (Automatisierte Datenanalyse), Rn. 100.
1174 BVerfG-Urteil des Ersten Senats vom 16. Februar 2023 (Automatisierte Datenanalyse), Rn. 102.

Rechtsgut wie auch an die Eingriffsschwelle, also den Anlass der Maßnahme.[1175] Ist die Befugnis zur Datenverarbeitung in einer nach den genannten Kriterien sehr belastenden Weise ausgestaltet, so sind hohe Anforderungen an die Rechtsgüter – erfasst sind nur der Schutz vor und die Verhütung von Straftaten im Kontext von besonders gewichtigen Rechtsgütern wie Leib, Leben und Freiheit der Person sowie Bestand des Bundes oder eines Landes, aber auch Sachen von bedeutendem Wert, deren Erhaltung im öffentlichen Interesse geboten ist[1176] – und Eingriffsanlass – erforderlich ist eine hinreichend konkretisierte Gefahr[1177] – zu stellen.[1178] Darunter erfolgt eine Abstufung: Auf mittlerer Stufe stehen durch Einschränkung von Art und Umfang der Daten sowie Verarbeitungsmethode begrenzte „weniger gewichtigen Eingriffen", bei denen es genügt, wenn die gesetzliche Ermächtigungsnorm eine konkretisierte Gefahr oder den Schutz von Rechtsgütern von zumindest erheblichem Gewicht voraussetzt.[1179] Noch darunter stehen Maßnahmen, bei denen Art und Umfang der einbeziehbaren Daten sowie die Verarbeitungsmethoden in einer Weise eingeschränkt sind, „dass eine auf die Befugnis gestützte Maßnahme nicht zu tieferen Einsichten in die persönliche Lebensgestaltung der Betroffenen führt als sie die Behörde, wenngleich aufwendiger und langsamer, auch ohne automatisierte Anwendung realistisch erlangen könnte"; dasselbe gilt, wenn „die Befugnis von vornherein nur darauf [zielt], gefährliche oder gefährdete Orte zu identifizieren, ohne dabei personenbezogene Informationen zu generieren" – hier kann dann bereits die Einhaltung des Grundsatzes der Zweckbindung ausreichen, um die weitere Verarbeitung der Daten in einer automatisierten Anwendung zu rechtfertigen.[1180] Neben diesen Eingriffsvoraussetzungen fließen aus dem Verhältnismäßigkeitsgrundsatz im Rahmen der automatisierten Datenanalyse schließlich Anforderungen an Transparenz, individuellen Rechtsschutz und aufsichtliche Kontrolle, wobei insbesondere einer

1175 BVerfG-Urteil des Ersten Senats vom 16. Februar 2023 (Automatisierte Datenanalyse), Rn. 103.

1176 Sofern hier ein enges Verständnis zugrundgelegt (das Bundesverfassungsgericht spricht von „Anlagen mit unmittelbarer Bedeutung für das Gemeinwesen").

1177 Siehe dazu bereits oben S. 177 ff.

1178 BVerfG-Urteil des Ersten Senats vom 16. Februar 2023 (Automatisierte Datenanalyse), Rn. 104 ff.

1179 BVerfG-Urteil des Ersten Senats vom 16. Februar 2023 (Automatisierte Datenanalyse), Rn. 107.

1180 BVerfG-Urteil des Ersten Senats vom 16. Februar 2023 (Automatisierte Datenanalyse), Rn. 108.

sachgerechten Ausgestaltung der Kontrolle große Bedeutung zukommt. Neben der Befassung der (unabhängigen und behördlichen) Datenschutzbeauftragten ist für das Bundesverfassungsgericht dabei „unerlässlich", „dass eigenständig ausformulierte Begründungen dafür gegeben werden, warum bestimmte Datenbestände zur Verhütung bestimmter Straftaten im Wege automatisierter Anwendung analysiert werden."[1181] Steigt der Komplexitätsgrad der eingesetzten Software sind zudem „Vorkehrungen gegen eine hiermit spezifisch verbundene Fehleranfälligkeit erforderlich, was auch gesetzliche Regelungen zu einem staatlichen Monitoring der Entwicklung der eingesetzten Software erfordern kann."[1182]

Hinsichtlich der abstrakten verfassungsrechtlichen Vorgaben für die Regulierung der automatisierten Datenanalyse führt das Bundesverfassungsgericht zudem noch aus, dass auf die Schwelle einer wenigstens konkretisierten Gefahr für besonders gewichtige Rechtsgüter – wie etwa im Bereich der vorbeugenden Bekämpfung von Straftaten regelmäßig der Fall – auch verzichtet werden kann, allerdings nur, „wenn die zugelassenen Analysemöglichkeiten normenklar und hinreichend bestimmt in der Sache so eng begrenzt sind, dass das Eingriffsgewicht der Maßnahme erheblich gesenkt ist."[1183] Hier muss der Gesetzgeber grundsätzlich den Wesentlichkeitsvorbehalt beachten, kann aber aufgrund „der besonderen Technizität und der raschen Fortentwicklungsbedürftigkeit der hier zur Milderung des Eingriffs benötigten Regelungen […], soweit eine tiefergehende gesetzliche Normierung nicht praktikabel erscheint, die Verwaltung zur näheren Regelung organisatorischer und technischer Einzelheiten ermächtigen", wobei er aber „sicherstellen [muss], dass im Zusammenwirken der gesetzlichen Vorgaben mit den Regelungsermächtigungen und -verpflichtungen der Verwaltung Art und Umfang der Daten und die Verarbeitungsmethoden insgesamt inhaltlich ausreichend, normenklar und transparent begrenzt sind."[1184] Egal wie die Konkretisierung durch die Verwaltung in einem solchen Fall ausgestaltet wird, muss gesetzlich sichergestellt werden, dass die Verwaltung ihre

1181 BVerfG-Urteil des Ersten Senats vom 16. Februar 2023 (Automatisierte Datenanalyse), Rn. 109.

1182 BVerfG-Urteil des Ersten Senats vom 16. Februar 2023 (Automatisierte Datenanalyse), Rn. 109; nähere Ausführungen zum flankierenden Schutz tätigt das Gericht nicht, da dies nicht Gegenstand des Verfahrens war.

1183 BVerfG-Urteil des Ersten Senats vom 16. Februar 2023 (Automatisierte Datenanalyse), Rn. 110.

1184 BVerfG-Urteil des Ersten Senats vom 16. Februar 2023 (Automatisierte Datenanalyse), Rn. 112.

Konkretisierungen und Standardisierungen der gesetzlichen Regelung in einer vom Gesetzgeber vorgeschriebenen Weise nachvollziehbar dokumentiert und veröffentlicht; diese Transparenzanforderungen sind vor allem deshalb geboten, „weil die Durchführung einer automatisierten Datenanalyse oder -auswertung in der Regel von den Betroffenen nicht wahrgenommen wird und sich die Konkretisierung der gesetzlichen Vorgaben damit kaum im Wechselspiel von Verwaltungsakt und gerichtlicher Kontrolle vollzieht", womit „ein zentraler Mechanismus notwendiger Begrenzung konkretisierungsbedürftiger Befugnisnormen weitgehend [ausfällt]."[1185] Auf diese Weise sollen vor allem die Datenschutzbeauftragten in die Lage versetzt werden, die Anwendung der Befugnis durch die Polizeien zu kontrollieren.[1186] Zu den wesentlichen Aspekten, die der Gesetzgeber aber in einem solchen Fall jedenfalls selbst regeln muss, gehört die Frage, welche Datenbestände einbezogen werden dürfen und inwiefern dies automatisiert erfolgen darf, wobei auch hier wieder eine das Eingriffsgewicht erhöhende oder senkende Flexibilisierung der Regelung möglich ist.[1187] Erfolgt keine inhaltliche und mengenmäßige „sehr eng[e]" Begrenzung, ist eine mitarbeiter:innenbezogene Einschränkung der Zugriffsmöglichkeiten gesetzlich festzuschreiben und über technisch-organisatorische Maßnahmen abzusichern.[1188] Ebenfalls durch das Gesetz zu regeln sind die Einbeziehung von Daten aus schwerwiegenden Grundrechtseingriffen – wobei Daten aus Online-Durchsuchung und Wohnraumüberwachung nicht mit in die Datenanalyse zur vorbeugenden Bekämpfung von Straftaten einbezogen werden dürfen – und die technisch-organisatorischen Maßnahme – etwa Kennzeichnungspflichten – zur Absicherung dieser Regelungen.[1189] Auch die Methode einer Datenanalyse zur vorbeugenden Bekämpfung von Straftaten muss vorab normenklar und hinreichend bestimmt gesetzlich festgelegt werden: Neben dem Ausschluss des Einsatzes selbstlernender System muss der Gesetzgeber grundlegende Maßgaben zur Begrenzung des Auto-

1185 BVerfG-Urteil des Ersten Senats vom 16. Februar 2023 (Automatisierte Datenanalyse), Rn. 113.
1186 BVerfG-Urteil des Ersten Senats vom 16. Februar 2023 (Automatisierte Datenanalyse), Rn. 113.
1187 BVerfG-Urteil des Ersten Senats vom 16. Februar 2023 (Automatisierte Datenanalyse), Rn. 115 f.
1188 BVerfG-Urteil des Ersten Senats vom 16. Februar 2023 (Automatisierte Datenanalyse), Rn. 117.
1189 BVerfG-Urteil des Ersten Senats vom 16. Februar 2023 (Automatisierte Datenanalyse), Rn. 118 f.

matisierungsgrades, der Suchfunktionalitäten und den Analyseergebnissen – wie etwa den Ausschluss maschineller Sachverhaltsbewertungen, die über die Anzeige von Übereinstimmungen zwischen Suchkriterien und durchsuchten Datenbeständen hinausgehen, oder Gefährlichkeitsaussagen über Personen – treffen und darf die Ausgestaltung nicht dem faktischen Vollzug durch die Polizeien überlassen.[1190]

Vor diesem Hintergrund hat das Bundesverfassungsgericht § 49 Abs. 1 Alt. 1 HmbPolDVG für nichtig und § 25a Abs. 1 Alt. 1 HSOG – da, anders als für die Hamburger Polizei der Fall, die hessische Polizei bereits auf Grundlage der Landesvorschrift eine Anwendung der automatisierten Datenanalyse betrieb – für unvereinbar mit der Verfassung erklärt, da die in den Vorschriften enthaltenen Befugnisse der automatisierten Datenanalyse zur vorbeugenden Bekämpfung von Straftaten aufgrund ihrer daten- und methodenoffenen Formulierung ein sehr hohes Eingriffsgewicht aufwiesen, ohne dabei zugleich mit den von Verfassungs wegen insofern erforderlichen strengen Eingriffsvoraussetzungen versehen worden zu sein. Vor Ablauf der Übergangsfrist am 30.09.2023 hat der hessische Gesetzgeber eine umfassende Umgestaltung der Vorschrift vorgenommen, die voraussichtlich Vorbild für weitere Gesetzgebungsvorhaben in Bund und Ländern sein wird.

(3) Gegenwärtige Regelungslage und kritische Würdigung

Die Novellierung des § 25a HSOG hat die Vorschrift konkretisiert und erweitert. Im Ersten Absatz wird die automatisierte Datenanalyse als polizeiliches Informationswerkzeug abstrakt-generell beschrieben, der zweite Absatz enthält die Eingriffsvoraussetzungen, d.h. die prinzipiellen Zweckrichtungen, die geschützten Rechtsgüter bzw. erfassten Straftaten sowie die jeweiligen Eingriffsschwellen. Im dritten bis fünften Absatz werden im Wesentlichen Regelung für Verfahren und Kontrolle im Kontext der automatisierten Datenanalyse getroffen.

Der erste Absatz erlaubt es der Polizei, rechtmäßig gespeicherte personenbezogene Daten auf einer Analyseplattform automatisiert zusammenzuführen. Unter Beachtung der übrigen Regelungsaspekte der Sätze 3 bis 6 und der Abs. 2 bis 5 dürfen die hessischen Polizeibehörden – dies ist die eigentliche Beschreibung der automatisierten Datenanalyse – die zu-

1190 BVerfG-Urteil des Ersten Senats vom 16. Februar 2023 (Automatisierte Datenanalyse), Rn. 120 f.

sammengeführten Daten, auch gemeinsam mit weiteren rechtmäßig erhobenen personenbezogenen Daten, verknüpfen, aufbereiten und auswerten sowie für statistische Zwecke anwenden. Dies ist die Legaldefinition der automatisierten Anwendung zur Datenanalyse. Nach Angaben des Gesetzgebers besteht die automatisierte Datenanalyse somit aus „zwei logisch aufeinander aufbauenden, aber praktisch zeitgleich stattfindenden Schritten, nämlich dem Zusammenführen unterschiedlicher „Datentöpfe" auf der Analyseplattform und der sich daran anschließenden Recherche innerhalb des so zusammengeführten Datenbestands".[1191] Der erste Schritt solle „das strukturelle Problem, dass in den Beständen der Polizei Daten in unterschiedlichen Formaten und disparaten Dateien gespeichert und damit nicht im selben Bearbeitungskontext gleichzeitig verfügbar sind, [überwinden], der zweite führt zu der verfassungsrechtlich relevanten Frage, was genau die Polizei mit den so zusammengeführten Daten machen darf und was nicht."[1192] Satz 3 konkretisiert dies noch etwas näher dahingehend, dass die automatisierte Anwendung zur Datenanalyse ein technisches Hilfsmittel ist, das es den Polizeibehörden bei der Erfüllung ihrer Aufgaben nach Maßgabe der folgenden Absätze ermöglichen soll, ihre Bewertungen, Prognosen und Entscheidungen auf der Grundlage möglichst verlässlicher Tatsachenfeststellungen zu treffen. Damit solle sichergestellt werden, „dass immer – und natürlich immer auch in all seiner Fehlerhaftigkeit – der Mensch am Anfang und am Ende des Entscheidungsprozesses steht."[1193] Die Analyseplattform dürfe „die Arbeitsweise der Polizei also nicht „entscheidend verändern", sondern sie soll helfen, ihre bewährte Arbeitsweise zu verbessern, nämlich Informationen aus verschiedenen Quellen zusammenzustellen und sie zu bewerten."[1194] Damit soll ausgeschlossen werden, „dass etwa eine polizeiliche Sachbearbeiterin bei Dienstbeginn das Analysetool gleichsam befragt, was heute denn zu tun sei." [1195] Die automatisierte Datenanalyse – so schreibt es Satz 4 vor – erfolgt immer anhand anlassbezogener und zielgerichteter Suchkriterien. Hiermit soll gewährleistet werden, „dass eine Analysesoftware nicht etwa ein wie immer geartetes Eigenleben oder gar eigene Gesetzmäßigkeiten entwickelt, sondern dass sie bleibt, was sie derzeit

1191 HessLT-Drs. 20/11235, S. 7.
1192 HessLT-Drs. 20/11235, S. 7.
1193 HessLT-Drs. 20/11235, S. 7.
1194 HessLT-Drs. 20/11235, S. 7.
1195 HessLT-Drs. 20/11235, S. 7.

schon ist, nämlich ein bloßes Hilfsinstrument."[1196] Ferner (Satz 5) ist sie manuell auszulösen und soll regelbasiert auf einer von Menschen definierten Abfolge von Analyse- und Verarbeitungsschritten ablaufen. Spezifiziert wird dies dahingehend, dass der Analysevorgang „aus einer Reihe simultan ausgelöster und miteinander in Verbindung gesetzter, auf Wenn-Dann-Operatoren beruhender Suchaktionen über den zuvor zusammengeführten Datenbestand [besteht]. Als regelbasierte oder, gleichbedeutend, deterministische Datenanalyse folgt sie einem klar definierten, unveränderlichen Ablauf und erzeugt deshalb auch konsistente und reproduzierbare Ergebnisse, die einer Gegenkontrolle leichter zugänglich sind als die Datenanalyse unter Einbeziehung selbstlernender Systeme."[1197] Satz 6 schließt zudem eine direkte Anbindung an Internetdienste aus. „Erforderlichenfalls", so die Gesetzesbegründung, „können aber die bei der Bearbeitung eines konkreten Fallkomplexes gezielt ermittelten und zuvor von den Polizeibehörden gespeicherten Daten, die bei einer Internetrecherche angefallen sind, in die automatisierte Datenanalyse einbezogen werden."[1198]

Damit greift Abs. 1 Einiges aus dem Urteil des Bundesverfassungsgerichts aus. Offen ist auch nach der Umformulierung aber, ob die hessische Anwendung der automatisierten Datenanalyse die gesetzlichen Vorgaben faktisch entspricht, was zu überprüfen vor allem der Kontrolle durch den hessischen Landesdatenschutzbeauftragten anheimgestellt werden muss. Dabei könnte eine Schwierigkeit darin bestehen, dass Begrifflichkeiten wie „anlassbezogene und zielgerichtete Suchkriterien" oder eine „vom Menschen definierte Abfolge von Analyse- und Verarbeitungsschritten" Raum für interpretierende Ausgestaltung seitens der Verwaltung lassen, sodass hiermit die Datenverarbeitungsmethode nur begrenzt bestimmt beschrieben ist. Auch die Abgrenzung zwischen einer „Analyseplattform" und einer „automatisierten Anwendung zur Datenanalyse" ist unklar. Zu begrüßen ist der Ausschluss einer direkten Anbindung an Internetdienste. Hier stellt sich aber die Frage, ob bzw. inwiefern eine indirekte Anbindung an Internetdienste erfolgt. Daten von Internetdiensten werden jedenfalls von der Polizei im Rahmen ihrer Aufgabenerfüllung regelmäßig erhoben werden. Falls das Verfahren der Speicherung von solchen Daten im polizeilichen Informationsbestand eher automatisiert erfolgt – etwa im Rahmen von

1196 HessLT-Drs. 20/11235, S. 7.
1197 HessLT-Drs. 20/11235, S. 7.
1198 HessLT-Drs. 20/11235, S. 7.

Online-Wachen[1199] oder sonstigen potenziellen virtuellen Meldestellen – und derartige Informationen als dann Daten aus dem polizeilichen Informationsbestand mit in die automatisierte Datenanalyse einbezogen werden, könnte sich eine solche indirekte Anbindung einer direkten Anbindung durchaus annähern.

Nach § 25a Abs. 2 Satz 1 ist die Weiterverarbeitung von rechtmäßig[1200] gespeicherten personenbezogenen Daten erlaubt, wenn (Nr. 1) dies zur Abwehr einer Gefahr für den Bestand oder die Sicherheit des Bundes oder eines Landes oder Leib, Leben oder Freiheit einer Person oder Sachen von bedeutendem Wert, deren Erhaltung im öffentlichen Interesse geboten ist, oder wenn gleichgewichtige Schäden für die Umwelt zu erwarten sind, erforderlich ist (nunmehr legaldefiniert als „Abwehr konkreter Gefahren"), wenn (Nr. 2) tatsächliche Anhaltspunkte die Annahme rechtfertigen, dass innerhalb eines übersehbaren Zeitraumes auf eine zumindest ihrer Art nach konkretisierte Weise Straftaten mit erheblicher Bedeutung begangen werden und dies zur Verhinderung dieser Straftaten erforderlich ist (nunmehr legaldefiniert als „Abwehr konkretisierter Gefahren") sowie wenn (Nr. 3) tatsächliche Anhaltspunkte die Annahme rechtfertigen, dass schwere oder besonders schwere Straftaten begangen werden sollen, und die Weiterverarbeitung erforderlich ist, um diese Straftaten zu verhüten (nunmehr legaldefiniert als „Vorbeugende Bekämpfung von Straftaten"). In Satz 2 werden die in die Analyse einbeziehbaren Datenbestände bestimmt; einbezogen werden können Vorgangsdaten, Falldaten, Daten aus den polizeilichen Auskunftssystemen, Verkehrsdaten, Telekommunikationsdaten, Daten aus Asservaten und Daten aus dem polizeilichen Informationsaustausch. Gemäß Satz 3 können zudem Datensätze aus gezielten Abfragen in gesondert geführten staatlichen Registern sowie einzelne gesondert gespeicherte Datensätze aus Internetquellen ergänzend in die Datenanalyse miteinbezogen werden. Satz 3 zufolge ist der Einbezug von Verkehrsdaten in Maßnahmen nach § 25 Abs. 2 Satz 1 Nr. 3 nicht gestattet.

Dem Gesetzgeber zufolge überträgt Abs. 2 das in Abs. 1 Satz 2 normierte „Prinzip der Anlass-, Fall- und Zielbezogenheit der automatisierten Daten-

1199 Siehe dazu S. 461 et passim.

1200 Abs. 2 enthält anders als Abs. 1 nicht mehr den Zusatz der „rechtmäßig" gespeicherten Daten. Da nach Abs. 1 aber nur rechtmäßig gespeicherte Daten auf einer Analyseplattform zusammengeführt werden dürfen, ist davon auszugehen, dass auch eine Weiterverarbeitung nur rechtmäßige Daten erfassen darf.

analyse in die Polizeirechtsdogmatik."[1201] Die drei Tatbestandsvarianten des Abs. 2 sollen dabei dem „verfassungsrechtliche[n| Erfordernis einer gleichsam auf dem Hintergrund unterschiedlicher Ebenen, Sektoren und Skalen auszudifferenzierenden Rechtsgrundlage für ein und dasselbe Instrument" Rechnung tragen, wobei [w]egen der dem Gefahrenbegriff eigentümlichen Wechselwirkung zwischen Schadenshöhe und Eintrittswahrscheinlichkeit jede der drei Varianten einen Korridor, dessen Grenzen schon für sich beweglich sind," beschreibe.[1202] Zudem geht die Gesetzesbegründung davon aus, dass diese „Korridore" nicht trennscharf nebeneinander stehen, sondern einander überlappen und ineinander übergehen können. Die grundlegende Überlegung bei dieser Beschreibung scheint zu sein, dass ein Sachkomplex im Laufe seiner Entfaltung nacheinander die verschiedenen „Korridore" durchlaufen kann und mit dieser Progression eine Intensivierung der informationellen Durchleuchtung des Sachkomplexes vorgenommen werden soll. Zugleich hat es der Gesetzgeber ausweisliche der Begründung unternommen, die aus dem Grundsatz der Zweckbindung fließenden Anforderungen sowie das rechtsstaatliche Gebot, die Rechte Unbeteiligter zu schützen, mit im Kontext der Eingriffsgrundlagen in Abs. 2 zu regeln, wobei sich insbesondere zu letzterem Aspekt auch in Abs. 3 wesentliche Regelungsgehalte finden. Der Schutz Unbeteiligter wird dem Gesetzgeber zufolge vor allem durch die Ausklammerung der Nutzung von Verkehrsdaten, in denen regelmäßig viele Daten Unbeteiligter enthalten sind, bei Maßnahmen im Rahmen der vorbeugenden Straftatenbekämpfung gewährleistet.[1203] Der ansonsten nach Abs. 2 Satz 2 kaum begrenzte Einbezug von „Datentöpfen"[1204] in die automatisierte Datenanalyse soll wohl durch das Rechte- und Rollenkonzept aus Abs. 3 kompensiert werden. Der Gesetzesbegründung zufolge soll die „gebotene Reduzierung der Datenmenge und damit die Verringerung der Eingriffsintensität […] deshalb schwerpunktmäßig funktional [erfolgen], indem unter Berücksichtigung und Fortentwicklung bewährter arbeitsteiliger Organisations- und Rechtsformen […] die Schaffung zeitgemäßer, an situativen Anforderungen ausgerichteter Rollen- und Rechtekonzepte durch die Verwaltung verbindlich vorgeschrieben wird mit der Folge, dass die im Einzelfall jeweils zu verarbeitende Datenmenge immer nur ein – mehr oder weniger großer –

1201 HessLT-Drs. 20/11235, S. 8.
1202 HessLT-Drs. 20/11235, S. 8.
1203 HessLT-Drs. 20/11235, S. 8.
1204 Zu den einzelnen Datenbeständen siehe die Ausführungen S. 230 ff.

Ausschnitt des auf der Plattform zusammengeführten und damit potentiell verfügbaren Datenbestandes ist." Weiter heißt es: „Die Datentöpfe sind also zwar vorhanden. Ihr Inhalt darf aber jeweils nur in Teilen entnommen werden. Weil der Gesetzgeber in seinem an die Verwaltung adressierten Regelungsauftrag hierfür nur übergeordnete Ziele, abstrakte Maßstäbe und beispielhafte Kriterien vorgibt, ist es der Verwaltung nicht verwehrt, in Fällen dringender Gefahren für höchstrangige Rechtsgüter – etwa bei einem drohenden Terroranschlag – erforderlichenfalls auch das „volle Programm" zuzulassen, also einzelnen Anwendern den Zugriff auf den vollständigen Inhalt aller Datentöpfe zu erlauben."[1205] Die Eingriffsvoraussetzungen selbst, wie sie in den Nr. 1 bis 3 des Abs. 2 Satz 1 festgelegt sind, sind bereits durch die Rechtsprechung des Bundesverfassungsgerichts konturiert.[1206] Beachtenswert sind insofern noch die gesetzgeberischen Ausführungen zu Abs. 2 Satz 3, wonach es sich bei Datensätzen aus Internetquellen „vor allem um die Ergebnisse polizeilicher Recherchen in für jedermann offenen sozialen Netzwerken" handelt.[1207]

Sehr umfangreich und im Regelungsinhalt einigermaßen komplex ist Abs. 3 geraten. Satz 1 erklärt zunächst – klarstellend – die Geltung des Zweckbindungsgrundsatzes (§ 20 Abs. 1 und 2 HSOG) im Kontext der automatisierten Datenanalyse, was gemäß Satz 2 durch eine zu veröffentlichende Verwaltungsvorschrift sicherzustellen ist. Konkretisiert wird deren Inhalt durch die folgenden Regelungsgehalte: Satz 3 verlangt ein Rechte- und Rollenkonzept sowie ein Konzept der Kategorisierung und Kennzeichnung personenbezogener Daten. Diese Komponenten werden in den Nr. 1 und 2 des Abs. 3 sodann spezifiziert. Zuvor legt Satz 4 allerdings noch fest, dass sich diese Konzepte unter Berücksichtigung der in Abs. 2 Satz 1 nach Schutzgütern und Eingriffsschwellen unterschiedenen Lagebilder an dem übergeordneten Ziel der Reduzierung des jeweils zu analysierenden Datenvolumens, der Angemessenheit der jeweils angewandten Analysemethode und des größtmöglichen Schutzes Unbeteiligter orientieren; legaldefiniert wird dies als funktionale Reduzierung der Eingriffsintensität. Nr. 1 statuiert sodann, dass das Rollen- und Rechtekonzept die zweckabhängige Verteilung sachlich eingeschränkter Zugriffsrechte anhand von Phänomenbereichen regelt. Nach Satz 2 sind Maßstab für dieses Konzept das Gewicht der zu schützenden Rechtsgüter und der Grad der Dringlichkeit des poli-

1205 HessLT-Drs. 20/11235, S. 9.
1206 Siehe HessLT-Drs. 20/11235, S. 9 ff für entsprechende Nachweise.
1207 HessLT-Drs. 20/11235, S. 14.

zeilichen Einschreitens. Weiter ist es nach dem Prinzip auszugestalten, wonach mehr Berechtigte Zugriff auf weniger und wenige Berechtigte Zugriff auf mehr der in der Analyseplattform zusammengeführten Daten haben dürfen. Satz 4 schreibt schließlich vor, dass im Konzept mindestens die einzelnen Phänomenbereiche, ihre Gewichtung und ihr Verhältnis zueinander umschrieben und die dienstrechtliche Stellung der Berechtigten, ihre Funktion und ihre spezifische Qualifizierung bezogen auf den Umfang der jeweiligen Berechtigung festgelegt werden müssen. Nr. 2 konkretisiert das Konzept der Kategorisierung und Kennzeichnung personenbezogener Daten. Dieses regelt anhand der Maßstäbe des Veranlassungszusammenhangs und der Grundrechtsrelevanz, welche personenbezogenen Daten in welcher Weise in die automatisierte Analyse einbezogen werden dürfen. In lit. a) wird weiter ausgeführt: Der Maßstab für dieses Konzept ist zum einen der sachliche Bezug der von der Analyse betroffenen Personen zum jeweiligen Phänomenbereich, legaldefiniert als sog. „Veranlassungszusammenhang". Dies folgt dem Prinzip, wonach eine automatisierte Datenanalyse umso komplexer sein darf, je gewichtiger der Veranlassungszusammenhang ist, und dass sie umso einfacher sein muss, je weniger gewichtig der Veranlassungszusammenhang ist. Nach Satz 3 ist Ausgangspunkt die Differenzierung nach verurteilten, beschuldigten, verdächtigen Personen und sonstigen Anlasspersonen sowie deren Kontaktpersonen einerseits und unbeteiligten Personen andererseits. Zum Schutz Unbeteiligter werden deren personenbezogene Vorgangsdaten in eine automatisierte Datenanalyse nicht einbezogen. Auch hier regelt das Nähere eine Verwaltungsvorschrift, die insbesondere für Verkehrsdaten eine Speicherfrist von regelmäßig zwei Jahren in der Analyseplattform vorsieht. Eine weitere Konkretisierung erfolgt sodann noch in lit. b). Danach ist Maßstab für das in Abs. 3 Nr. 2 geregelte Konzept neben dem Veranlassungszusammenhang die Kategorisierung personenbezogener Daten nach der Schwere des Eingriffs in das Recht auf informationelle Selbstbestimmung bei ihrer Erhebung, legaldefiniert als Grundrechtsrelevanz. Diese Grundrechtsrelevanz erfordert, dass abstrakte Regelungen getroffen werden müssen, die der eingeschränkten Verwendbarkeit von Daten aus schwerwiegenden Grundrechtseingriffen Rechnung tragen, und es muss durch technisch-organisatorische Vorkehrungen sichergestellt werden, dass diese Regelungen praktisch wirksam werden. Schließlich werden in die automatisierte Anwendung zur Datenanalyse keine personenbezogenen Daten einbezogen, die aus Wohnraumüberwachung und Online-Durchsuchung gewonnen wurden.

Der in Abs. 3 enthaltene regulatorische Ansatz verknüpft ausweislich der Gesetzesbegründung die Folgerungen aus dem verfassungsrechtlichen Zweckbindungsgrundsatz mit Regelungen über materielle Rechtfertigungsanforderungen und gelangt auf diese Weise zu einer „Kombination aus organisatorischen und materiellen Elementen, die […] als funktionale Reduzierung der Eingriffsintensität bezeichnet wird."[1208] Dabei soll Abs. 3 einerseits das Zweckbindungsprinzip mit „dem auf einem zeitgemäßen und flexiblen, die Funktionalität einer Analyseplattform unterstützenden, an vorhandene Organisationsstrukturen anschließbaren Rollen- und Rechtekonzept" verschränken. Andererseits soll der Absatz eine „eingriffsreduzierenden Vorauswahl [vorschreiben], nämlich [eine] Kategorisierung und Kennzeichnung personenbezogener Daten anhand der materiellen Kriterien des Veranlassungszusammenhangs und der Grundrechtsrelevanz, die dazu führt, dass bestimmte grundrechtssensible Daten von vornherein nur in begrenztem Umfang oder überhaupt nicht in die automatisierte Datenanalyse einbezogen werden dürfen."[1209] Ziel dieses Ansatzes ist die Reduzierung des Datenvolumens, die Angemessenheit der Analysemethode sowie Schutz Unbeteiligter.[1210] Mit den ersten beiden Aspekten greift die Regelung die zentralen Eingriffsgewichtstopoi aus dem Urteil des Bundesverfassungsgerichts auf und auch der Schutz Unbeteiligter, der letztlich auch an die Datenart aus dem Urteil anknüpft, ist wesentlich in der Argumentation des Gerichts. Das Rollen- und Rechtekonzept[1211] wirkt der Dynamik der automatisierten Datenanalyse zur Zusammenführung von Daten auf einer Plattform der Gesetzesbegründung nach entgegen, „weil es dazu führt, dass im normalen Polizeialltag sozusagen niemand in alle der zusammengeführten Datentöpfe schauen kann, sondern immer nur einen Ausschnitt der zusammengeführten Daten sieht."[1212] Die Ausgestaltung des Rollen- und Rechtekonzepts soll sich am Gewicht der zu schützenden Rechtsgüter und der Dringlichkeit der Sache ausrichten, wobei die drei Tatbestandsvarianten des Abs. 2 Satz 1 als abstrakter Maßstab, die kriminologischen Phänomenbereiche, denen innerhalb einer Behörde die verschiedenen Sachbearbeiter:innen zugeordnet sind, als konkreter Anknüpfungspunkt für Rechte

1208 HessLT-Drs. 20/11235, S. 14.
1209 HessLT-Drs. 20/11235, S. 14 f.
1210 HessLT-Drs. 20/11235, S. 15.
1211 Siehe dazu unter anderem unten S. 366 ff.
1212 HessLT-Drs. 20/11235, S. 15.

und Rollen fungieren soll.[1213] Der Gesetzgeber sieht insofern vor, dass etwa „nur wenige und besonders geschulte Berechtigte Zugriff auf Verkehrsdaten oder Daten aus Asservaten haben, weil es sich dabei um große Datenmengen handelt, die typischerweise viele personenbezogene Daten Unbeteiligter beinhalten und deshalb mit besonderer Sensibilität zu behandeln sind", wobei die nähere Ausgestaltung einer Verwaltungsvorschrift überlassen bleibt.[1214] Ferner soll das Rechte- und Rollenkonzept auch dokumentiert und technisch – insbesondere durch eine Zugangskontrolle – abgesichert werden.[1215] Die zweite Stellschraube zur Minimierung der Eingriffsintensität ist in der gesetzgeberischen Konzeption die nähere Kategorisierung der einzubeziehenden Daten und der damit einhergehende Ausschluss bestimmter Datenarten. Hier arbeitet das Gesetz einerseits mit dem sogenannten Veranlassungszusammenhang, was letztlich an die Terminologie der relevanten Personen etwa im BKAG[1216] anknüpft und verlangt, dass einzubeziehende Daten von Personen stammen, die verurteilt, beschuldigt oder verdächtigt sind oder als sonstige Kontakt- oder Anlasspersonen nach § 15 Abs. 2 Nr. 4 HSOG gelten. Daten von Unbeteiligten sollen hingegen „gewissermaßen unsichtbar gemacht werden, obwohl sie in den Quellsystemen, etwa einem Vorgangsbearbeitungssystem, noch auffindbar sind."[1217] Der Schutz dieser Personen sei „dadurch gewährleistet, dass mangels spezifischer Erfassung dieser Daten im Quellsystem ihre elektronische Verknüpfung und somit auch ihre automatisierte Weiterverarbeitung nicht möglich ist."[1218] Hier soll eine menschliche Bewertungsebene vor einer weiteren Verarbeitung eingezogen werden. In der Gesetzesbegründung heißt es: „Der polizeiliche Sachbearbeiter kann also das entsprechende Dokument und darin enthaltene Namen zwar lesen. Er kann diese Namen aber nicht automatisch weiterverarbeiten, ohne zuvor eine überprüfbare Bewertung darüber abgegeben zu haben, dass die betreffende Person nunmehr als Anlassperson (oder als Begleitperson einer Anlassperson) einzustufen ist."[1219] Zur Verringerung der Eingriffsintensität arbeitet der Gesetzgeber andererseits mit Begrenzung oder sogar Ausschluss von personenbezogenen Daten aus schwerwiegenden Grundrechtseingriffen. Verfassungsrechtlich ausge-

1213 HessLT-Drs. 20/11235, S. 15.
1214 HessLT-Drs. 20/11235, S. 15.
1215 HessLT-Drs. 20/11235, S. 16.
1216 Siehe dazu S. 324 ff., 331 ff.
1217 HessLT-Drs. 20/11235, S. 16.
1218 HessLT-Drs. 20/11235, S. 16.
1219 HessLT-Drs. 20/11235, S. 16.

schlossen sind Daten aus Online-Durchsuchungen und Wohnraumüberwachungen.[1220] Alle Daten aus Eingriffen, die bezüglich der Eingriffsintensität darunter liegen, sollen regelmäßig weiter – wenn die verfassungsrechtlichen Voraussetzungen wie etwa das Vorliegen eines konkreten Ermittlungsansatzes erfüllt sind – in die Datenanalyse mit einbezogen werden können, wobei in der Gesetzesbegründung darauf hingewiesen wird, es sei Aufgabe der Verwaltung, „Ausnahmekonstellationen zu identifizieren und sie gegebenenfalls normativ zu erschließen.[1221]

In Abs. 4 hat der Gesetzgeber „Regelungen zur Gewährleistung von Kontrolle, Transparenz, Richtigkeitsvergewisserung und Rechtsschutz aufgenommen."[1222] Satz 1 statuiert eine Zugangskontrolle zur automatisierten Anwendung zur Datenanalyse, wobei Zugriffe nach Satz 2 der ständigen Protokollierung unterliegen. Zudem ist jeder Fall der automatisierten Anwendung zur Datenanalyse von der Anwenderin oder dem Anwender zu begründen, was der Selbstvergewisserung und der nachträglichen Kontrolle dienen soll. Näheres regelt eine Verwaltungsvorschrift. Schließlich ermächtigt Satz 6 behördliche Datenschutzbeauftragte zur Durchführung stichprobenartiger Kontrollen. Die Zugriffskontrolle ist letztlich eine Absicherung des Rechte- und Rollenkonzepts, die etwa eine technische Sperrung für nicht autorisierte Personen vorsieht.[1223] Die nach Satz 5 durch eine Verwaltungsvorschrift zu konkretisierende Begründungspflicht soll nach den gesetzgeberischen Vorstellungen jedenfalls ein Freitextfeld enthalten, um die verfassungsrechtlichen Anforderungen – „eigenständig ausformulierte Begründungen"[1224] – zu erfüllen.[1225]

Die Regelung in Abs. 5 schließlich entspricht dem bisherigen Abs. 3 und schreibt einen (nicht ganz strikten) Behördenleiter:innen-Vorbehalt sowie die Anhörung des oder der hessischen Datenschutzbeauftragten vor.

Grundsätzlich erscheint die neue Regelung der Anwendung zur automatisierten Datenanalyse – insbesondere im Kontrast zu ihrer Vorgängerregelung – ein Fortschritt zu sein, was gesetzgeberische Auseinandersetzung mit dem Regelungsgegenstand angeht; dies schlägt sich auch in einer prinzipiell ausdifferenzierten und entsprechend anspruchsvollen Vorschrift

1220 HessLT-Drs. 20/11235, S. 16.
1221 HessLT-Drs. 20/11235, S. 17.
1222 HessLT-Drs. 20/11235, S. 17.
1223 HessLT-Drs. 20/11235, S. 17.
1224 BVerfG-Urteil des Ersten Senats vom 16. Februar 2023 (Automatisierte Datenanalyse), Rn. 109.
1225 HessLT-Drs. 20/11235, S. 17.

nieder, deren Stärken vor allem in der verfahrensrechtlichen Absicherung der Maßnahme liegen. Allerdings bleibt abzuwarten, ob hier eine Regelung gelungen ist, die den praktischen Datenumgang im Rahmen der automatisierten Datenanalyse in einer Weise zu steuern vermag, welche den verfassungsrechtlichen Anforderungen an diese neue Form der informationellen Polizeiarbeit entspricht. Hier ist vor allem der oder die unabhängige Datenschutzbeauftragte, sind aber auch die behördlichen Datenschutzbeauftragten der damit befassten Polizeibehörden, gefragt, durch eine minutiöse Kontrolle regulative Fehlleistungen zu identifizieren und der weiteren rechtspolitischen Diskussion zuzuleiten. Dabei sollten vor allem auch die teilweise recht präzisen Vorstellungen des Gesetzgebers hinsichtlich des Umgangs mit der Maßnahme der automatisierten Datenanalyse bei den Kontrollen berücksichtigt werden.

Allerdings konnte die Neuregelung einige, bereits zuvor in der Diskussion geäußerte Problemaspekte nicht wirklich ausräumen. So enthält die Vorschrift nach wie vor – wie es zugegebenermaßen auch vom Bundesverfassungsgericht dem Grunde nach bestätigt wurde – den Schutz von Sachen von bedeutendem Wert, deren Erhaltung im öffentlichen Interesse geboten ist, als schützenswertes Rechtsgut. Das Verfassungsgericht versteht darunter wesentliche Infrastruktureinrichtungen oder sonstige Anlagen mit unmittelbarer Bedeutung für das Gemeinwesen.[1226] Der Infrastruktur-Begriff taucht in der Verfassungsrechtsprechung insbesondere im Kontext der Terrorismusabwehr auf und steht dabei etwa im Zusammenhang mit „Brücken" und „Behörden".[1227] Es geht dabei nicht um den Schutz des Eigentums oder Sachwerte als solcher.[1228] Ob sich dieses Verständnis auch in der polizeilichen Praxis niederschlagen wird, bleibt abzuwarten. Mit der durch den Bundesgerichtshof anerkannten Wertgrenze von 750 Euro[1229] für Sachen von bedeutendem Wert fallen darunter beispielsweise schon Parkbänke oder Geräte auf Kinderspielplätzen.[1230] Daneben könnten beispielsweise auch die aus der Sprayer:innen-Szene drohenden Sachbeschädigungen in Form von Graffitis an entsprechenden Sachen durch den Einsatz von Datenanalysen als Gefahren abgewehrt werden. Es wäre insofern zu begrüßen,

1226 BVerfG-Urteil des Ersten Senats vom 16. Februar 2023 (Automatisierte Datenanalyse), Rn. 105.
1227 BVerfGE 133, 277 (303) – Antiterrordateigesetz.
1228 BVerfGE 133, 277 (364) – Antiterrordateigesetz.
1229 BGH NStZ 2011, 215.
1230 *Golla* Neue Juristische Wochenschrift 74 (2021), 667 (671).

wenn das Schutzgut, das dem Bundesverfassungsgericht zufolge funktional zu verstehen ist, entsprechend durch eine gesetzliche Formulierung enger gefasst würde. Zudem hat der Gesetzgeber das Schutzgut der Umwelt mit aufgenommen und insoweit qualifiziert, als dass „gleichwertige Schäden" für diese zu erwarten sein müssen. Hier ist völlig offen, was damit genau gemeint ist. In der Zusammenschau mit dem Veranlassungszusammenhang könnte man zumindest annehmen, dass nur Umweltstraftaten davon erfasst sein sollen, was aber – auch mit Blick auf nebenstrafrechtliche Bestimmungen – den Kreis erfasster Verhaltensweisen nicht wirklich präzise eingrenzt. Letztlich hat auch die Neufassung der Eingriffstatbestände in § 25a Abs. 2 S. 1 Nr. 1 bis 3 HSOG nur wenig Begrenzung bezüglich des Einsatzes der Maßnahme gebracht. Nach wie vor ist mit der vorbeugenden Bekämpfung von Straftaten eine Phase vor jeder konkreten oder konkretisierten Gefahr (und jedem konkreten Tatverdacht) angesprochen, sodass *Bäuerles* Feststellung nach wie vor treffend ist, dass nach dem Wortlaut bereits niedrigschwellige und diffuse Anhaltspunkte für mögliche Gefahren oder Straftaten ausreichen könnten. Insofern könnten schon „Tatsachenlagen, die durch eine hohe Ambivalenz der Bedeutung einzelner Beobachtungen gekennzeichnet sind", zum Anlass für eine Datenanalyse genommen werden, obwohl noch nicht verlässlich festgestellt werden kann, ob überhaupt von den dann konkret betroffenen Personen in irgendeiner Weise Gefährdungspotenzial ausgeht.[1231] Zwar ist der Anwendungsbereich auf schwere oder besonders schwere Straftaten, also solche mit einer Höchststrafe von mindestens fünf[1232] bzw. zehn[1233] Jahren, begrenzt. Neben dem Umstand, dass unter die erstere Kategorie bereits eine Vielzahl strafrechtlicher Delikte fällt, ist auch im Bereich der besonders schweren Straftaten mit Delikten wie § 89a StGB und § 129a StGB eine hohe Tatbestandsambivalenz nach wie vor Teil der Eingriffsvoraussetzungen. Das Bundesverfassungsgericht hatte hierzu ausgeführt, dass sich „allein aus der Gefahr der Verwirklichung eines Vorfeldtatbestands […] nicht notwendigerweise bereits solche Gefahren für Rechtsgüter [ergeben]", es aber gerade „auf eine Gefahr für die geschützten Rechtsgüter" ankomme.[1234] Dies spiegelt sich nicht in der Vorschrift wider.

1231 *Bäuerle* in *Möstl/Bäuerle* (Hrsg.), Polizei- und Ordnungsrecht Hessen, § 25a Rn. 37 ff.
1232 BVerfGE 129, 208 (243) – TKÜ-Neuregelung.
1233 BVerfGE 109, 279 (348) – Großer Lauschangriff.
1234 BVerfG-Urteil des Ersten Senats vom 16. Februar 2023 (Automatisierte Datenanalyse), Rn. 170.

Zudem zieht die Erstreckung der Maßnahme auf Anlasspersonen sowie – ausweislich der Gesetzesbegründung – auch auf Begleitpersonen[1235] der Anlasspersonen den Kreis potenziell Betroffener nach wie vor weit.[1236]

Davon abgesehen hat die Regelung aber auch weiterhin grundsätzliche Probleme, die allerdings weniger in der gesetzestechnischen Ausarbeitung selbst begründet sind. Vielmehr ergeben sie sich aus dem Konflikt, der aus der Konzeption der automatisierten Datenanalyse als solcher und dem Zweckbindungsgrundsatz als einem der Grundpfeiler der informationellen Selbstbestimmung erwächst. Denn die Datenanalysen ermöglicht nach wie vor einen wenig beschränkten Umgang mit Daten.[1237] Zwar muss insoweit auch gesehen werden, dass in bestimmten Kriminalitätsbereichen aufgrund des Gewichts der in Rede stehenden Rechtsgüter ohnehin auch „normalerweise" eine zweckändernde Nutzung der meisten oder sogar aller bei der Polizei verfügbarer Daten möglich wäre. Jedoch erscheint mit Blick auf die verfassungsrechtliche Dogmatik der informationellen Selbstbestimmung bei der automatisierten Datenanalyse vor allem problematisch, dass zweckändernde Datenverarbeitungen im Wege dieses informationellen Instruments weiter normalisiert, verfestigt und auf Dauer gestellt werden. Insofern ist es auch nach wie vor zutreffend, von „Zweckänderungsautomaten"[1238] zu sprechen. Letztlich sollte auch nicht vergessen werden, dass in der Regelung auch nach ihrer Neufassung ein altes sicherheitspolitisches Muster präsent bleibt: Es wird versucht ein bereits geplantes oder bestehendes informationstechnologisches Projekt, rechtlich abzubilden, damit – zumindest bis zur nächsten verfassungsgerichtlichen Entscheidung – Daten mit der neuen Anwendung (weiter)verarbeitet werden können.[1239] Wie bereits dargelegt bleibt nunmehr zu beobachten, ob die Eingriffsschwellen, Transparenzpflichten und das Kontroll- und Aufsichtsregime inklusive umfassender Datenprotokollierung zu einem rechtsstaatlich eingehegten Nutzungsverhalten der Polizeien führen. Darüber hinaus erscheint auch, wie von *Golla* vorgeschlagen, eine unabhängige Instanz[1240] zur Kontrolle der

1235 HessLT-Drs. 20/11235, S. 16.
1236 Siehe zu Anlasspersonen unten S. 324 ff.
1237 *Bäuerle* in *Möstl/Bäuerle* (Hrsg.), Polizei- und Ordnungsrecht Hessen, § 25a Rn. 9.
1238 *Will* in Nolte/Poscher/H. Wolter (Hrsg.), Die Verfassung als Aufgabe von Wissenschaft, Praxis und Öffentlichkeit, 429.
1239 So erfolgte die Einführung des § 25a HSOG in Hessen erst nachdem das damit geregelte Verfahren bereits personenbezogene Daten verarbeitet hat, s. HessLT-Drs. 19/6864, Teil B, S. 6 f.
1240 *Golla* Neue Juristische Wochenschrift 74 (2021), 667 (672).

technischen Dimension von Befugnissen zum polizeilichen Einsatz komplexer Informationstechnologie sowie die Sicherstellung der Datenqualität und stete Durchführung einer Datenschutz-Folgenabschätzung sinnvoll.[1241]

Schließlich bleibt im Rahmen solcher Analysesysteme stets auch das unionsrechtliche Verbot automatisierter Einzelfallentscheidungen aus Art. 11 JI-Richtlinie zu beachten. Die in Bundes- und Landesdatenschutzgesetze übernommene Norm untersagt prinzipiell jede ausschließlich auf einer automatischen Verarbeitung beruhende Entscheidung, die mit einer nachteiligen Rechtsfolge für die betroffene Person verbunden ist oder sie erheblich beeinträchtigt. Die Vorschrift des § 25a HSOG hat insoweit versucht Abhilfe zu schaffen, indem ein menschliches Handlungselement im Normtext verankert wurde. Nichtsdestotrotz muss auch hier genau geschaut werden, ob es nicht doch schlicht zur menschlichen Bestätigung eines automatisierten Verarbeitungsvorgangs ohne inhaltliche Überprüfung – ob intentional oder aufgrund eines Automation Biases[1242] – kommt. Dabei handelt es sich um ein Szenario, für das die Entwicklung von (rechtlichen) Kontrollmöglichkeiten noch am Anfang steht.[1243]

cc) Digitalisierung der Informationsträger: Elektronische Strafakte

Eine weitere Innovation, die das polizeiliche Informationswesen der näheren Zukunft tangiert, ist die elektronische Strafakte. Mit ihr sollen die papiernen Strafakten bei Polizei und Staatsanwaltschaft durch eine digitalisierte Form der Informationsträger ersetzt werden. Die Einführung einer elektronischen Akte ist dabei Voraussetzung für einen Medienwechsel, der den technischen Fortschritt nachvollzieht und die Strafjustiz modernisiert.[1244] Neben einer beabsichtigten Vereinfachung und Beschleunigung des Rechtsverkehrs ist mit der sogenannten E-Akte auch die Vereinfachung der Verfügbarkeit und Übermittlung der Dokumente sowie eine einfachere und schnellere Durchsuchung, Filterung oder Verknüpfung von Daten angestrebt.[1245] Um die zuweilen kritisierte[1246] IT-Infrastruktur hierfür zu

1241 *Golla* Kriminologisches Journal 52 (2020), 149 (159).
1242 Siehe dazu etwa *Butz/Christoph/Sommerer* ua Bewährungshilfe 68 (2021), 241 (254 f.).
1243 *Golla* Neue Juristische Wochenschrift 74 (2021), 667 (672).
1244 BT-Drucks. 18/9416, S. 1.
1245 *Puschke* in *J. Wolter* (Hrsg.), SK-StPO, § 496 Rn. 2.
1246 Claus, jurisPR-StrafR 2/2018 Anm. 1.

schaffen oder auszubauen haben sich drei Entwicklungsverbünde gebildet, die jeweils Softwarelösungen entwickeln. Dabei müssen die E-Akten-Softwarelösungen auch Schnittstellen zu den bisherigen staatsanwaltschaftlichen Fachverfahren (MEDSTA und web.sta) enthalten.[1247] Insofern besteht hier IT-architektonisch ähnlich wie im polizeilichen Informationswesen ein gewisses Heterogenitätspotenzial, das sich in Kompatibilitätsproblemen äußern könnte.

Geregelt sind Einführung und Handhabung der elektronischen Strafakten in den §§ 32 ff., § 496 ff. StPO. So war im Zuge der Einführung etwa zu klären, wie sich die bisherige analoge Akte in eine digitale Form überführen lässt, also insbesondere welche Inhalte die E-Akte haben kann und soll und in welcher Form diese dargestellt werden können und sollen.[1248] Herausforderungen betreffen die Gewährleistung von Aktenwahrheit, Aktenklarheit und Aktenvollständigkeit sowie Zugangsmöglichkeiten der Verfahrensbeteiligten.[1249] Vor allem die datenschutzrechtlichen Implikationen der elektronischen Strafakte sind weitreichend, da ein zunehmend digitalisierter Aktenbestand durch die darin bestehenden Recherche- und Verknüpfungsmöglichkeiten eine hohe informationelle Durchdringung von Sachverhalten ermöglichen kann, was durch die Multimedialität einer digitalisierten Akte prinzipiell noch gesteigert wird. Insofern war eine rechtliche Sicherung gegenüber derart ausufernden Informationsmaßnahmen zu schaffen.[1250] Das hat der Gesetzgeber mit § 498 Abs. 2 StPO getan, der einen maschinelle Abgleich personenbezogener Daten mit elektronischen Akten oder elektronischen Aktenkopien gemäß § 98c StPO untersagt, es sei denn, er erfolgt mit einzelnen, zuvor individualisierten Akten oder Aktenkopien.[1251]

Allerdings treffen die Neuerungen rund um die elektronische Strafakte die Polizeien mehr indirekt. Denn mit den tatsächlichen E-Akten arbeiten nur Gerichte und Staatsanwaltschaften, die Polizeien, wenn sie die Vorgänge nicht ohnehin in ihren Vorgangs- oder Fallbearbeitungssystemen haben, sollen regelmäßig nur die sogenannten Repräsentate bekommen.[1252]

1247 *Mitterer* in Anders/Graalmann-Scheerer/Schady (Hrsg.), Innovative Entwicklungen in den deutschen Staatsanwaltschaften, 353 (355 f.).
1248 Vertiefend dazu *Growe/Gutfleisch* Neue Zeitschrift für Strafrecht 40 (2020), 633.
1249 *Puschke* in *J. Wolter* (Hrsg.), SK-StPO, § 496 Rn. 3.
1250 *Singelnstein* in *Knauer/Hartmut Schneider* (Hrsg.), Münchener Kommentar zur Strafprozessordnung Bd. 3: §§ 333-500 StPO, Vorb. zu § 496 Rn. 4.
1251 *Puschke* in *J. Wolter* (Hrsg.), SK-StPO, § 498 Rn. 4.
1252 BR-Drs. 633/19, S. 7 f.

Nichtsdestotrotz dürfte es die polizeiliche Arbeit, insbesondere ihre Effektivität, dadurch verändern, dass Daten bei flächendeckender Nutzung der E-Akte schneller und eventuell auch umfassender zwischen Polizeien und Staatsanwaltschaften zirkulieren. Inwieweit dadurch polizeiliche Informationen zügiger durch das Strafjustizsystem be- und verarbeitet werden können, wird sich zeigen – es ist allerdings anzunehmen. Effizienzsteigerungen sind immerhin eines der expliziten Ziele der Aktendigitalisierung. Wo die Polizeien auch tangiert sein könnten, ist der Bürger:innenkontakt. So ermöglicht es § 32c S. 2 StPO, in einer Rechtsverordnung die Einreichung bestimmter Daten in strukturierter maschinenlesbarer Form vorzuschreiben. Dadurch soll eine durchgehende IT-gestützte Vorgangsverarbeitung ermöglicht und häufig auftretende Verfahrensabläufe – etwa die Einreichung einer Strafanzeige, eines Strafantrags, eines Zeugenentschädigungsantrags oder eines Einspruchsgegen einen Strafbefehl – effizienter gestaltet werden.[1253] Soweit ersichtlich, ist dies noch nicht geschehen, sodass gegenwärtig nicht absehbar ist, an welche Stelle etwa Strafanzeigen geleitet und wie sie dort verarbeitet werden würden.

dd) Mobile Ausformungen des polizeilichen Informationssystems

Digitaltechnik zeichnet sich nebst anderem insbesondere auch durch die Miniaturisierung von Geräten und Instrumenten aus, was ein Mehr an und größere Mobilität von informationstechnischem Gerät in Polizeieinsätzen bedeutet. Emblematisch ist hier zunächst das Smartphone, das gegenwärtig flächendeckend bei deutschen Polizeien ausgerollt wird.[1254] Es kann eine Plattform für verschiedene appsystembasierte Polizeianwendungen bieten und als Aufnahmegerät für verschiedene Medienformate dienen. So sind etwa Messenger-Dienste für Kommunikation zwischen Beamt:innen, Auskunftsapps zum Abgleich mit dem polizeilichen Datenbestand und ein Dokumentenscanner mit KI-getriebener Bilderkennungssoftware denkbare Anwendungen. Daneben sollen in naher Zukunft – zumindest kleinere – Vorgänge vollständig digital erfasst oder etwa Fingerabdrücke digital abgeglichen werden könne.[1255] Damit wird es voraussichtlich zu einer nicht unerheblichen Steigerung der Effektivität informationeller Vorgänge kommen.

1253 BT-Drs. 18/9416, S. 50.
1254 Siehe dazu unten S. 471 ff.
1255 So die konkreten Pläne in NRW, https://www.im.nrw/smartphone-loesung-fuer-die-nrw-polizei (Stand: 01.10.2023).

Zudem ist eine durch die Technizität der Geräte und durch die eingesetzten Softwares bedingte Opazität des polizeilichen Handelns für Betroffene denkbar. Trotz dieser Aspekte, von denen man wohl eine intensitätssteigernde Wirkung behaupten könnte, gibt es keine Rechtsgrundlagen für den Einsatz von Smartphones. Es ist zugegebenermaßen auch fraglich, welchen substanziellen Mehrwert eine solche für ein Informationsinstrument bringen würde, das massenhaft eingesetzt werden soll. Ein prozeduraler Grundrechtsschutz ist indessen möglich. Die Geräte müssen dementsprechend durch technische und organisatorische Maßnahmen eingehegt und auch ansonsten datenschutzrechtlich eng kontrolliert werden.

Ebenfalls vermehrt im Einsatz sind mobile Formen der Videoüberwachung, was vor allem in Form sogenannter Bodycams auch zunehmend im alltäglichen Streifendienst der Fall wird. Diese werden von Polizeibeamt:innen an den Uniformen getragen und zeichnen Bild- und Tondaten im Rahmen des Einsatzes auf, können aber Personen in einem räumlich immer weiteren Umfeld erfassen. Der Aufzeichnungsmodus kann dabei unterschiedlich ausgestaltet sein. Häufig gibt es aber das Erfordernis der Aktivierung durch die Einsatzkräfte, wobei allerdings ein anlassloses Pre-Recording stattfindet. Die Kamera ist also quasi im Dauerbetrieb, überschreibt aber alle 30 oder 60 Sekunden die bis dahin erhobenen Daten. Über diese Zeitspanne hinaus erfasst wird dann nur bei Aktivierung der Bodycam.[1256] Rechtlich zugelassen[1257] sind diese Sonderformen der Videoüberwachung regelmäßig nur in der Öffentlichkeit und nur dann, wenn Polizeibediensteten oder Dritten eine Gefahr für Leib, Leben oder Freiheit droht, wobei die Tatbestandsvoraussetzungen und Ausgestaltungen mitunter divergieren. Ausweitungstendenzen zeichnen sich aber bereits ab, etwa in Form des Einsatzes der Bodycam auch in privaten Wohnräumen.[1258] Daneben müssen Bodycams auch als videotechnische Plattform begriffen werden, die etwa mit Gesichts- oder Verhaltenserkennungssoftware kombiniert werden könnten, wie es in einigen – auch demokratischen – Staaten

1256 *Müller/Schwabenbauer* in *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch des Polizeirechts, G. Rn. 693.

1257 § 27a BPolG; § 44 Abs. 5 BWPolG; Art. 33 Abs. 4 BayPAG; § 24c ASOG; § 33 BremPolG; § 18 Abs. 5 HmbPolDVG; § 14 Abs. 6 HSOG; § 32a SOG M-V; § 15c PolG NRW; § 31 Abs. 1 POGRP; § 27 Abs. 3 SPolG; § 16 Abs. 3 SOG LSA; § 184 Abs. 3 SchlHLVwG.

1258 Siehe dazu etwa *Lehmann*, Stellungnahme Einsatz Bodycam in privaten Wohnräumen (SPolG), Gesetz zur Neuregelung der polizeilichen Datenverarbeitung im Saarland (Drucksache 16/1180), 2020.

bereits entwickelt wird.[1259] Ob eine solche Konfiguration der Bodycams, die neben einer besonders invasiven Gefahrenabwehr auch eine massive Intensivierung von Fahndungen bedeuten könnte, überhaupt mit der Verfassung vereinbar ist, erscheint zweifelhaft, da dies einen flächendeckenderen Einsatz voraussetzt, der sich stark einer anlasslosen Vorratsdatenspeicherung annähern würde.[1260]

Eine Mobilisierung der Erkenntnisquellen des polizeilichen Informationssystems erfolgt zudem auch durch mobile Formen der automatisierten Kennzeichenkontrolle, wie sie sei einigen Jahren eingesetzt und ausgeweitet wird. Die Maßnahme, die sowohl in den Polizeigesetzen als auch in der StPO (§ 163g) geregelt ist, ermöglicht punktuelle aber dafür intensive Überwachung wichtiger Verkehrsströme. Die Regelungen sind verfassungsrechtlich nicht unproblematisch[1261] und es bleibt abzuwarten, inwiefern polizeiliche Verkehrsüberwachung ausgeweitet werden wird.

ee) Private Datenbestände als latente Datenquellen der Polizei

Die gleichen Merkmale, die das Internet im Allgemeinen und soziale Medien im Besonderen für Massenkommunikation so attraktiv machen – große Reichweite und vielfältige Vernetzungsebenen – machen sie ebenso attraktiv als Überwachungstechnologie. Insofern hat die Polizei Informationspraktiken entwickelt, um die im Internet verfügbaren (personenbezogenen) Daten nutzbar zu machen. Diese werden unter den Begriffen der Online-Streife und Online-Rasterfahndung sowie Open Source Intelligence (OSINT) besprochen. Geregelt sind diese Verfahren nur unzureichend. Zwar sind konkrete, häufig schwerwiegende Maßnahmen wie die Online-Durchsuchung oder die Quellen-Telekommunikationsüberwachung nach den verfassungsrechtlichen Vorgaben reguliert. Während es noch denkbar wäre, oberflächliche und sporadische Online-Streifen auf die Datenerhebungsgeneralklausel zu stützen, bedarf es für systematische Auswertungen

1259 Etwa in Israel, siehe *Cheslow* Times of Israel v. 22. Januar 2022; auch in den USA, *Westrope*, Wolfcom Embraces Body Cam Face Recognition Despite Concerns, https://www.govtech.com/biz/wolfcom-embraces-body-cam-face-recognition-despite-concerns.html (Stand: 01.10.2023).

1260 *Müller/Schwabenbauer* in *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch des Polizeirechts, G. Rn. 692.

1261 *Arzt* in *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch des Polizeirechts, G. Rn. 1164.

der virtuellen Kommunikationssphären des Internets, etwa in Form von zielgerichteten verdeckten Ermittlungen oder dem systematischen Zusammentragen von Informationen aus sozialen Medien, konkrete Rechtsgrundlagen, die bereichsspezifisch verfassungsrechtliche Anforderungen umsetzen.[1262]

Streng genommen handelt es sich dabei jedoch um Datenerhebungsmaßnahmen, die nicht zum primären Fokus der vorliegenden Arbeit gehören. Als sich zunehmend etablierende Informationspraktiken weisen sie jedoch auf eine strukturelle Ausprägung des polizeilichen Informationswesens hin, die bisher nur wenig in der Diskussion um polizeiliche Datenbestände thematisiert wurde: Die Nutzung privater Datenbestände im Rahmen der polizeilichen Aufgabenerfüllung. Zwar ist dieses Phänomen im Kern nicht neu. Rasterfahndung, Telekommunikationsüberwachung und Online-Durchsuchung sind für ihren Erfolg häufig auf die Kooperation mit privatwirtschaftlichen Akteuren angewiesen. Aber die Nutzbarmachung der massiven Datenbestände der Datenökonomie, die ihrerseits – worauf *Zubroff* hingewiesen hat – über inhärente Überwachungsdynamiken verfügt,[1263] scheint noch am Anfang zu stehen. In welcher Form sich eine Verschränkung von polizeilichen und privaten Akteuren, insbesondere den Betreibern von großen Social Media-Plattformen, auf die von der Polizei ausgeübte Sozialkontrolle auswirken wird, ist dabei noch nicht im Detail abzusehen.

Allerdings ist die Polizei bereits heute stark auf eine Beweisfindung und -sicherung im Digitalen angewiesen, sodass die Plattformbetreiber insofern eine wichtige Vermittlerrolle einnehmen und die Strategien, die sie zur Inhaltsmoderierung einsetzen, Einfluss auf die Arbeit der Polizei haben.[1264] So wurden vor allem in Europa besondere Stellen bei vielen Polizeien eingerichtet, um auf Rechtsverletzungen im Internet auch angemessen strafverfolgend reagieren zu können.[1265] In Deutschland ist diese Kopplung zwischen Plattformen und Polizeien für den Fall eventuell strafrechtsrelevanter Online-Kommunikation mit § 3a Abs. 2 NetzDG zentral beim Bundeskriminalamt verankert. Betreiber sozialer Netzwerke müssen diesem zum Zwecke der Ermöglichung der Verfolgung von Straftaten Inhalte über-

1262 Siehe dazu *Müller/Schwabenbauer* in *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch des Polizeirechts, G. Rn. 705 mwN.

1263 *Zuboff,* The age of surveillance capitalism.

1264 *Bloch-Wehba* Law & Society: Private Law - Intellectual Property eJournal 2021, 102 (103).

1265 Siehe dazu etwa *Chang* COLUM. HUM. RTS. L. REV. 49 (2018), 114.

mitteln, die dem Anbieter in einer Beschwerde über rechtswidrige Inhalte gemeldet worden sind, die der Anbieter entfernt oder zu denen er den Zugang gesperrt hat und bei denen konkrete Anhaltspunkte dafür bestehen, dass sie mindestens einen der Tatbestände der §§ 86, 86a, 89a, 91, 126, 129 bis 129b, 130, 131 oder 140 des Strafgesetzbuches, des § 184b des Strafgesetzbuches oder des § 241 des Strafgesetzbuches in Form der Bedrohung mit einem Verbrechen gegen das Leben, die sexuelle Selbstbestimmung, die körperliche Unversehrtheit oder die persönliche Freiheit erfüllen und nicht gerechtfertigt sind. Darüber hinaus sind Metadaten des entsprechenden Inhalts gem. § 3a Abs. 4 NetzDG zu übermitteln. Nach einem Urteil des Verwaltungsgerichts Köln ist § 3a NetzDG jedoch zunächst aufgrund von Unvereinbarkeit mit dem Unionsrecht für unanwendbar erklärt worden.[1266]

Allerdings ist damit mitnichten das letzte Wort in der Verschränkung von Digitalökonomie und Strafverfolgungsbehörden gesprochen, vielmehr ist es der Auftakt der Ausgestaltung dieses Verhältnisses. Die bereits abzusehenden und recht sicher zu erwartenden Dynamiken in dieser Beziehung hat *Bloch-Wehba* bereits konturiert. Einerseits weiten die Strafverfolgungsbehörden ihren Einfluss auf die Plattformbetreiber aus. Nicht nur Meldepflichten wie in § 3a NetzDG, sondern auch die generellen Belange der Strafverfolgungsbehörden veranlassen Plattformbetreiber dazu, ihre Moderierung entsprechend anzupassen. Zudem spiegeln die technischen Infrastrukturen der Inhaltsmoderation – in dem Maße, in dem Plattformunternehmen auf Automatisierung und „künstliche Intelligenz" setzen, um ihre Bemühungen zur Bekämpfung schädlicher Online-Inhalte zu verstärken – zunehmend die Einflüsse von staatlichen Sicherheitsentscheidungen wider.[1267] Umgekehrt sind jedoch auch die Strafverfolgungsbehörden einem Einfluss seitens der Plattformbetreiber unterworfen. Die technische Affordanzstruktur der jeweiligen Plattformen und sozialen Netzwerke bestimmt entschieden darüber mit, was etwa Polizeien bei ihren Online-Streifen als mögliche Beweise für eine vorgefallene Straftat sehen und sichern können. Werden Inhalte vorher gelöscht, ist auch das Delikte mitunter nicht mehr aufklärbar, wenn keine Instrumente zur Wiederherstellung der Daten bestehen.[1268] Gerade bei der Überwachung von und Ermittlung in devianten

1266 VG Köln, Beschluss vom 1.3.2022 – 6 L 1277/21 – Google = MMR 2022, 330.

1267 *Bloch-Wehba* Cornell Int'l L.J. 53 (2020), 41 (69 f.); *Fourcade/Gordon* JLPE 1 (2020) sprechen insoweit treffend von "dataist statecraft".

1268 *Bloch-Wehba* Law & Society: Private Law - Intellectual Property eJournal 2021, 102 (104 f.).

Gruppierungen, die regelmäßig über einen längeren Zeitraum erfolgen, kann es für die Polizeien wichtig sein, dass Inhalte nicht möglichst schnell verschwinden.[1269] Insofern spielen inhaltsbezogenen Entscheidungen der Plattformen eine zunehmend größere Rolle für Strafverfolgungsbehörden – private und staatliche Akteure sind insofern beidseitig und komplex miteinander verflochten.[1270] Auch könnte der Prozess der Inhaltsmoderation selbst zu einem immer attraktiveren Ziel für die Strafverfolgungsbehörden werden, wenn die Plattformen zunehmend proaktiv und automatisiert filtern. Setzen Plattformen automatische Moderationsverfahren ein, erhalten sie regelmäßig Zugang zu einer großen Menge an Inhalten, die entweder tatsächlich gegen das Gesetz verstoßen oder diesen Anschein erwecken. Denn die Technik ist häufig noch nicht ausgereift genug, nur tatsächlich strafrechtliche Inhalte zu identifizieren und mit Blick auf die normative Natur strafrechtlicher Normen ist auch zweifelhaft, ob eine fehlerfreie Identifizierung überhaupt möglich ist. Deshalb sind die automatisierten Techniken oft zwangsläufig zu umfassend und erfassen mehr Inhalte, als beabsichtigt war.[1271] Neben dieser vorrangig digitalen Sphäre kommt durch das Internet der Dinge aber auch der digital augmentierte analoge Raum (auch: Onlife[1272]-Sphäre) in einen – durch die jeweiligen Unternehmen der Digitalökonomie vermittelten – Fokus der Polizei. Statt eine Wohnung tatsächlich in Raum und Zeit zu durchsuchen, könne eine retrospektive Durchsuchung über eine Reihe von vernetzen Haustechnologien erfolgen.[1273]

Insofern lassen sich Entwicklungstendenzen erkennen, die reichhaltigen Datenbestände der Digitalökonomie (auch) zu latenten polizeilichen Datenspeichern umzufunktionieren: Die vorgehaltenen Daten sind nicht direkt Teil des polizeilichen Informationswesens, sondern fungieren als Ressource im Leerlauf, die bei Bedarf oder durch gesetzlichen Impuls als informationelle Quelle in die polizeiliche Arbeit eingebunden werden kann. Neben der bedenklichen Informationsfülle, die dadurch „an den Fingerspitzen" der Polizeien liegt, wirft eine umfassendere Zusammenarbeit zwischen Strafverfolgungsbehörden und Plattformen zusätzlich schwierige

1269 *Bloch-Wehba* Law & Society: Private Law - Intellectual Property eJournal 2021, 102 (117 f.).
1270 *Bloch-Wehba* Law & Society: Private Law - Intellectual Property eJournal 2021, 102 (118).
1271 *Gorwa/Binns/Katzenbach* Big Data & Society 7 (2020), 1-15 (5).
1272 *Floridi,* The 4th revolution, passim.
1273 *Bloch-Wehba* Law & Society: Private Law - Intellectual Property eJournal 2021, 102 (136).

Fragen darüber auf, wie integrale Bestandteile des Rechtsstaats wie Rechenschaftspflicht und Transparenz am besten in diesem verflochtenen Feld umgesetzt werden können.[1274]

III. Die einfachgesetzliche Normierung polizeilicher Informationspraktiken

Nachdem nun das Recht der Infrastrukturen des polizeilichen Informationswesens dargestellt und erläutert wurde, soll dies nun in einem zweiten Schritt auch für den normativen Rahmens der im Informationswesen ausgeübten Informationspraktiken erfolgen. Die Darstellung ist dabei nochmals zweigeteilt und geht zunächst auf Datenverarbeitungen im polizeilichen Informationsverbund ein. Danach erfolgt noch eine Auseinandersetzung mit Datenverarbeitungen in den polizeibehördeneigenen Systemen. Die Fülle an nicht unerheblichen Divergenzen in den Polizeirechtsordnungen der Länder- und Bundesbehörden erschweren jedoch eine umfassende Gesamtdarstellung, weshalb der Fokus stattdessen auf zentrale Strukturprinzipien gelegt wird.[1275]

1. Polizeiliche Datenverarbeitung im Informationsverbund

Zentral für die (rein) polizeiliche Datenverarbeitung im Informationsverbund sind die §§ 16, 18 und 19 BKAG, deren Beachtung über § 29 Abs. 4 S. 2 BKAG im Wesentlichen auch für alle anderen Polizeibehörden, die am Verbund teilnehmen, vorgeschrieben ist. Die Vorschriften sind dabei auch – wie bereits dargelegt[1276] – für bestimmte Ausformungen des Informationsverbundes relevant, etwa für Fahndungs-, Haft- und erkennungsdienstliche Dateien. Im Folgenden soll hingegen auf die konkreten Verarbeitungsmöglichkeiten geschaut werden, die die Normen ermöglichen. Dabei adressieren die §§ 16, 18 und 19 BKAG in ihrer direkten Anwendung das Bundeskriminalamt und dessen Datenweiterverarbeitungen im eigenen Informationssystem nach § 13 BKAG. Nicht ganz klar ist, welche Bedeu-

1274 *Bloch-Wehba* Law & Society: Private Law - Intellectual Property eJournal 2021, 102 (107).

1275 So auch *Müller/Schwabenbauer* in *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch des Polizeirechts, G. Rn. 578, siehe dort auch Fn. 1419.

1276 Siehe dazu bereits oben S. 230 ff.

tung die drei Vorschriften für die teilnehmenden Polizeibehörden konkret haben, die Gesetzesbegründung ist insoweit unverständlich.[1277] Zwar lässt sich sagen, dass die Normen dem Informationsverbund zugrunde liegen,[1278] aber gleichzeitig findet sich die Berechtigung für Eingabe und Abruf von Daten im Informationsverbund durch die teilnehmenden Stellen gesondert in § 29 Abs. 3 BKAG geregelt. Als relativ sicher kann insofern allerdings wohl gelten, dass die in § 29 Abs. 4 S. 2 BKAG genannten Vorschriften des 2. Unterabschnitts im 2. Abschnitt des BKAG für die Eingabe und den Abruf durch die am Informationsverbund beteiligten Behörden zu beachten sind. Da – was *Bäcker* eindrücklich für seine Stellungnahme anlässlich der Gesetzesberatungen zum BKAG herausgearbeitet hat – bereits die direkte Anwendung der §§ 16, 18 und 19 BKAG im Rahmen der bundeskriminalamtlichen Datenverarbeitung mit erheblichen Problemen behaftet sind, beschränkt sich die nachfolgende Darstellung auf diesen Anwendungsfall, da eine Beschäftigung mit der entsprechenden Anwendung einer strukturell defizitären, änderungswürdigen Rechtslage kaum Erkenntnisgewinne verspricht.

a) Verarbeitung personenbezogener Daten durch das Bundeskriminalamt nach § 16 BKAG

Gemäß § 16 Abs. 1 BKAG kann das Bundeskriminalamt personenbezogene Daten unter Berücksichtigung des § 12 BKAG im Informationssystem ver-

1277 Danach entspricht Satz 2 „dem bisherigen § 11 Absatz 1 Satz 3, wobei die Verweise der neuen Rechtslage angepasst werden. Durch den Verweis in Satz 3 auf die §§ 12, 14 und 15 wird sichergestellt, dass der Grundsatz der hypothetischen Datenneuerhebung und die zu dessen Implementierung erforderliche Kennzeichnung für die Eingaben im INPOL-Verbund für alle Teilnehmer Geltung besitzt." Der alte § 11 Abs. 1 S. 3 BKAG schreibt lediglich vor, dass § 36 BKAG a.F. unberührt bleibt; die Vorschrift betrifft eine für das alte BKAG geltende Verordnungsermächtigung. Denkbar ist, dass es sich dabei um einen inhaltlichen Fehler in der Gesetzesbegründung handelt und eigentlich § 11 Abs. 2 S. 3 gemeint war, der für die Eingabe durch die teilnehmenden Behörden im „alten" Informationsverbund die §§ 7-9 BKAG a.F. für anwendbar erklärt. Strukturell ist dieser Verweis näher an § 29 Abs. 4 S. 2 BKAG n.F., der wiederum Datenverarbeitungsregeln im „neuen" Informationsverbund für entsprechend anwendbar erklärt. Auch die bisher einzige Kommentierung zu § 29 Abs. 4 S. 2 BKAG erschließt die Vorschrift nur bedingt, denn sie bezieht sich unter anderem auf § 29 Abs. 2 S. 4 BKAG, vgl. Graulich in *Schenke/Graulich/Ruthig,* Sicherheitsrecht, § 29 Rn. 26.

1278 So *Bäcker*, A-Drs. 18(4)806 D, S. 3 ebenfalls auf § 29 Abs. 4 S. 2 BKAG verweisend.

arbeiten, soweit dies zur Erfüllung seiner Aufgaben erforderlich ist und das BKAG keine zusätzlichen besonderen Voraussetzungen vorsieht. Das Bundeskriminalamt ist damit berechtigt, im Zusammenhang mit bestimmten gesetzlichen Aufgaben angefallene Daten auch für die Erfüllung einer anderen Aufgabe zu nutzen. So können etwa im Rahmen der Zentralstellenaufgabe angefallene Daten auch für die Aufgabenerfüllung nach §§ 4 bis 8 BKAG genutzt werden. Im Zuge einer solchen Zweckänderung ist, worauf § 16 Abs. 1 BKAG explizit verweist, der Grundsatz der hypothetischen Datenneuerhebung einzuhalten.[1279] Der Begriff der Verarbeitung ist im Sinne des § 46 Nr. 2 BDSG weit zu verstehen und beinhaltet damit jeden Umgang mit Daten, der nicht Datenerhebung ist.

aa) Verfassungsrechtliche Bedenken bzgl. § 16 Abs. 1 BKAG i.V.m. der Figur der zweckwahrenden Weiternutzung

Im Gegensatz zur bisherigen Rechtslage, die § 16 Abs. 1 BKAG nur abbilden soll,[1280] ermöglicht die Norm neuerdings jedoch auch weitreichende Weiterverarbeitungen im Rahmen einer ursprünglichen Aufgabe („zweckwahrende Weiternutzung“[1281]), wie *Bäcker* am Beispiel der Terrorismusabwehr gemäß § 5 BKAG darlegt: Im Rahmen dieser Aufgabe sind regelmäßig hochrangige Rechtsgüter bedroht, was den Einsatz eingriffsintensiver Datenerhebungsmaßnahmen ermöglicht und so typischerweise besonders sensible Daten in die Sphäre des Bundeskriminalamtes gelangen lässt. Die Weiterverarbeitung innerhalb derselben Aufgabe erfordert dabei mangels Zweckänderung nicht, dass die Voraussetzungen des Grundsatzes der hypothetischen Datenneuerhebung, also insbesondere ein konkreter Ermittlungsansatz, vorliegen. Darüber hinaus ist Voraussetzung für die Weiterverarbeitung lediglich noch, dass diese zur Aufgabenerfüllung erforderlich ist. Dabei handelt es sich um eine niedrigschwellige Voraussetzung.[1282] Das Bundeskriminalamt kann unter diesen Voraussetzungen etwa einmal im Rahmen der Terrorismusabwehr erhobene Daten langfristig bevorraten, um die gegebenenfalls später innerhalb derselben Aufgabe zu nutzen. Einschränkend wirkt dabei nur die nach wie vor nicht an die neue Rechtslage

1279 *Graulich* in *Schenke/Graulich/Ruthig,* Sicherheitsrecht § 16 BKAG Rn. 6.
1280 BT-Drs. 18/11163, S. 97.
1281 Siehe dazu bereits oben S. 164 ff.
1282 *Bäcker*, A-Drs. 18(4)806 D, S. 4.

angepasste BKADV[1283], die die zu speichernden Datenarten konkretisiert. Restriktivere Speicherungsanlässe zur Bevorratung von Daten innerhalb einer Aufgabenzuweisung sieht das BKAG nicht vor. Auch die Verwertung der so anfallenden und bevorrateten Daten wäre als Unterfall des Weiterverarbeitungsbegriffes im Rahmen derselben Aufgabe auf § 16 Abs. 1 BKAG zu stützen und hinge damit allein von der Erforderlichkeit zur jeweiligen Aufgabenerfüllung ab. Hinzu kommt, dass die in § 79 Abs. 1 S. 1, 1. HS BKAG anlässlich Zweckerreichung aufgestellte Löschungspflicht gem. § 79 Abs. 1 S. 1, 2. HS BKAG nicht für nach den Vorschriften des Abschnitts 1, Unterabschnitt 2 verarbeiteten Daten gilt, worunter unter anderem die Weiterverarbeitung nach § 16 Abs. 1 BKAG fällt.[1284] Insofern ist § 16 BKAG als Bevorratungsermächtigung zu lesen, die sich an den dafür bestehenden verfassungsrechtlichen Vorgaben messen lassen muss. Die Breite und tendenzielle Sensibilität der erfassbaren Daten haben eine hohe Grundrechtsbelastung zur Folge. Mithilfe der bevorrateten Daten ist eine granulare Abbildung der hinter den Daten stehenden Personen möglich.[1285] Eine so eingriffsintensive Bevorratungsermächtigung bedarf eines hinreichenden Anlasses[1286] und erfordert, dass dem Eingriffsgewicht der Bevorratung auf Ebene der Datenverwertung Rechnung getragen wird. Dem wird § 16 Abs. 1 BKAG mit seinem einfachen Erforderlichkeitskriterium nicht gerecht.[1287] Hier zeigt sich auch ein Problem in der unreflektierten Übernahme der unionrechtlichen Datenschutz-Terminologie. Indem mit dem Weiterverarbeitungsbegriff operiert wird, werden alle möglichen Datenverarbeitungsschritte tatbestandlich vermengt, obwohl ihnen unterschiedliches Eingriffsgewicht zukommen kann, zumal auch die unionsrechtliche Dogmatik eine anlass- und unterschiedslose Speicherung insbesondere von sensiblen Daten nicht erlaubt.[1288] Auch der Verweis auf eine verfassungskonforme Auslegung, wie man ihn im polizeilichen Informationsrecht anlässlich gesetzgeberischer Unterregulierung immer wieder findet,[1289] kann für § 16 Abs. 1

1283 Siehe dazu bereits oben S. 227 ff.
1284 *Bäcker*, A-Drs. 18(4)806 D, S. 4 f.
1285 Siehe *Bäcker*, A-Drs. 18(4)806 D, S. 5, Fn. 15 zu „maßgeblichen Intensitätskriterien".
1286 BVerfGE 133, 277, 339 ff. – Antiterrordatei; EuGH, 21.12.2016 - C-203/15, C-698/15 – Tele2 Sverige u.a., 96 ff.; EGMR, 04.12.2008 - 30562/04, 30566/04 – S. und Marper gegen Vereinigtes Königreich, Rn. 101 ff.
1287 Vgl. *Bäcker*, A-Drs. 18(4)806 D, S. 5 f.
1288 Siehe dazu, auch mwN., *Eichenhofer* in *Barczak* (Hrsg.), BKAG, § 16 Rn. 11.
1289 *Schenke* in *Schenke/Graulich/Ruthig,* Sicherheitsrecht, § 45 BKAG Rn. 26, 33; *Müller/Schwabenbauer* in *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch des Po-

BKAG nicht ernsthaft in Erwägung gezogen werden, dafür ist die Norm zu zentral für das System der Datenverarbeitung im polizeilichen Informationswesen.[1290]

bb) Spezielle Datenverarbeitungsformen nach § 16 BKAG

Neben der Weiterverarbeitungsgeneralklausel, die an den beschriebenen Mängeln leidet und damit das Informationshandeln des Bundeskriminalamts als wichtigstem Akteur im polizeilichen Informationsverbund normativ unzureichend einhegen, geschweige denn steuern kann, enthält § 16 BKAG noch spezielle Verarbeitungsbefugnisse. Sie erlauben die Verarbeitung der Daten in den wichtigen Dateien bzw. zukünftig den durch Zugriffsrechte abgegrenzten Teilen des „gemeinsamen Datenhauses". Geregelt ist dort die Verarbeitung zu Fahndungs-, Strafverfolgungsvorsorge- und erkennungsdienstlichen Zwecken sowie die Verarbeitung von Hinweisen. Auch hier ist gegenwärtig die fehlende Konkretisierung durch die BKADV ein Problem. Welche Daten genau verarbeitet werden dürfen, lässt sich insoweit nicht sagen.

Daneben erlaubt § 16 Abs. 4 S. 1 BKAG Datenabgleiche, wenn Grund zu der Annahme besteht, dass dies zur Erfüllung einer Aufgabe erforderlich ist. Der Datenabgleich ermöglicht die Feststellung, ob zu einer Person bereits eine Speicherung in einer polizeilichen Datei bzw. im „gemeinsamen Datenhaus der Polizei" enthalten ist. Der Maßnahme wird nur eine geringe Eingriffsintensität zugesprochen,[1291] was angesichts der umfangreichen Datenbestände der Polizeien nicht ohne Weiteres einleuchtet, zumal im Trefferfall denkbar ist, dass sich weitere Maßnahmen anschließen, die allerdings auch ihre eigenen Eingriffsschwellen haben. Dennoch ist fraglich, ob angesichts des Anwachsens der polizeilichen Datenbestände, wie es in Folge der Datafizierung halbwegs sicher zu erwarten ist, bei der Kategorisierung von Datenabgleichen als wenig eingriffsintensiv stehen geblieben werden kann.

---

lizeirechts, G. Rn. 618, 961; *Schenke* in *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch des Polizeirechts, E. Rn. 404.

1290 Siehe zur verfassungsrechtlichen Problematik des § 16 Abs. 1 BKAG auch die Ausführungen bei *Eichenhofer* in *Barczak* (Hrsg.), BKAG, § 16 Rn. 7 ff.

1291 *Graulich* in *Schenke/Graulich/Ruthig,* Sicherheitsrecht § 16 BKAG Rn. 36; kritisch zur Eingriffsintensität etwa *Golla* Kriminologisches Journal 52 (2020), 149 (158).

b) Datenverarbeitung durch das Bundeskriminalamt und im Informationsverbund nach §§ 18, 19 BKAG

Neben § 16 BKAG sind die §§ 18, 19 BKAG integrale Normen für die Verarbeitung von personenbezogenen Daten im bundeskriminalamtlichen Informationssystem und im Informationsverbund. Neben der Zentralstellenaufgabe (§ 18 Abs. 1 i.V.m. § 2 Abs. 1 bis 3 BKAG) darf die Verarbeitung, über § 16 Abs. 3 BKAG, vor allem auch zu Zwecken der Strafverfolgungsvorsorge erfolgen. Es geht hierbei also um die wichtige Frage, zu welchen Personen Daten im polizeilichen Informationsverbund bevorratet werden dürfen.

Das Gesetz unterscheidet insofern zwischen (Nr. 1) Verurteilten, (Nr. 2) Beschuldigten, (Nr. 3) Personen, die einer Straftat verdächtig sind, sofern die Weiterverarbeitung der Daten erforderlich ist, weil wegen der Art oder Ausführung der Tat, der Persönlichkeit der betroffenen Person oder sonstiger Erkenntnisse Grund zu der Annahme besteht, dass zukünftig Strafverfahren gegen sie zu führen sind, und (Nr. 4) Personen, bei denen Anlass zur Weiterverarbeitung der Daten besteht, weil tatsächliche Anhaltspunkte dafür vorliegen, dass die betroffene Person in naher Zukunft Straftaten von erheblicher Bedeutung begehen wird (sog. Anlasspersonen). Dieser „personenbezogene Eingriffstatbestand“,[1292] den es auch vorher bereits gab, ist nunmehr auch unionsrechtlich erforderlich und setzt insofern Art. 6 JI-Richtlinie um, der die Mitgliedstaaten verpflichtet, die personenbezogenen Daten unterschiedlicher Personenkategorien unterscheidbar zu machen.[1293] Diese Vorgabe ergibt sich aus Erwägungsgrund 31 der JI-Richtlinie, wonach es bei der Verarbeitung personenbezogener Daten im Rahmen der justiziellen Zusammenarbeit in Strafsachen und der polizeilichen Zusammenarbeit naturgemäß um betroffene Personen verschiedener Kategorien geht.

1292 So *Bäcker*, Der Umsturz kommt zu früh: Anmerkungen zur polizeilichen Informationsordnung nach dem neuen BKA-Gesetz, https://verfassungsblog.de/der-umsturz-kommt-zu-frueh-anmerkungen-zur-polizeilichen-informationsordnung-nach-dem-neuen-bka-gesetz/ (Stand: 01.10.2023), für §§ 18, 19 BKAG.

1293 BT-Drs. 18/11163, S. 99.

aa) Personenkategorien nach § 18 BKAG

Eine erste Gruppe ist die der Verurteilten, die gegenüber der Vorgängerregelung neu aufgenommen wurde. Eine Erweiterung der Befugnisse soll damit nicht einhergehen.[1294] Verurteilte im Sinne der Norm sind gemäß § 4 BZRG diejenigen, bei denen ein deutsches Gericht (§ 4 Nr. 1 BZRG) wegen einer rechtswidrigen Tat auf Strafe erkannt, (Nr. 2) eine Maßregel der Besserung und Sicherung angeordnet, (Nr. 3) jemanden nach § 59 des StGB mit Strafvorbehalt verwarnt oder (Nr. 4) nach § 27 JGG die Schuld eines Jugendlichen oder Heranwachsenden festgestellt hat.[1295] Der Begriff des Beschuldigten ist dem Strafverfahrensrecht entlehnt.[1296] Darunter fallen diejenigen Tatverdächtigen, gegen die das Verfahren als Beschuldigte betrieben wird. Um diese Eigenschaft zu begründen, bedarf es eines Willensakts der zuständigen Strafverfolgungsbehörde.[1297] Ebenfalls erfasst sind die unterschiedlichen, von der jeweiligen Phase des Strafverfahrens abhängigen, Formen des Beschuldigtenstatus.[1298] Die Kategorien von verurteilten und beschuldigten Personen verweisen folglich auf formale Stadien des Strafverfahrens; dieser Formalisierungsgrad gilt hingegen bereits nicht mehr bei der Kategorie der Verdächtigen gem. Nr. 3, obgleich es auch hier einen strafprozessualen Konnex gibt.[1299] Denn der Begriff des Verdächtigen stammt zwar aus dem Strafverfahrensrecht, ist dort aber nicht präzise definiert. Entscheidend ist, dass der strafprozessual relevante Verdacht hinsichtlich einer Tat sich auf bestimmte Tatsachen stützen muss, bloße Vermutungen reichen hingegen nicht aus.[1300] Neben der Verdächtigeneigenschaft ist noch das Bejahen der in § 18 Abs. 1 Nr. 3 BKAG genannten Prognose (sogenannte Negativprognose) für eine zulässige Weiterverarbeitung erforderlich. Die Prognose ist – wie in § 16 Abs. 1 und 5 BKAG – gerichtlich überprüfbar.[1301] Die letzte Personenkategorie, für die § 18 Abs. 1 Nr. 4 BKAG die Weiterverarbeitung gestattet, ist die der Anlassperson. Das

1294 BT-Drs. 18/11163, S. 99.
1295 *Graulich* in *Schenke/Graulich/Ruthig,* Sicherheitsrecht, § 18 BKAG Rn. 3.
1296 *Graulich* in *Schenke/Graulich/Ruthig,* Sicherheitsrecht, § 18 BKAG Rn. 4.
1297 *Diemer* in *Hannich* (Hrsg.), Karlsruher Kommentar zur Strafprozessordnung, § 136 Rn. 4.
1298 Angeschuldigte:r und Angeklagte:r.
1299 Eichenhofer in *Barczak* (Hrsg.), BKAG, § 18 Rn. 7.
1300 *Kölbel* in *Hartmut Schneider* (Hrsg.), Münchener Kommentar zur Strafprozessordnung, § 170 Rn. 15.
1301 *Graulich* in *Schenke/Graulich/Ruthig,* Sicherheitsrecht, § 18 BKAG Rn. 5.

Erfordernis der tatsächlichen Anhaltspunkte für die Begehung einer Straftat von erheblicher Bedeutung durch die von der Verarbeitung betroffene Person ist sehr niedrigschwellig. Vor allem im direkten Vergleich zu Nr. 3 der Vorschrift, die eine Verarbeitung neben der Verdächtigeneigenschaft noch an weitere täter- oder tatbezogene Voraussetzungen knüpft, ist die Norm zu unbestimmt. Dass die betroffene Person in der Vergangenheit beschuldigt oder verdächtig war, ist nicht erforderlich, sodass personenbezogene Daten von bisher an Straftaten völlig unbeteiligten Personen verarbeitet werden können.[1302] Zudem ist das Erfordernis der tatsächlichen Anhaltspunkt für die Begehung einer Straftat von erheblicher Bedeutung gesetzlich nicht weiter definiert, was die Unbestimmtheit der Norm zusätzlich erhöht.[1303] Wie dieses Erfordernis durch die polizeiliche Datenverarbeitungspraxis entgrenzt werden kann, haben *Ruch und Feltes* am Beispiel der Gewalttäterdateien dargelegt.[1304] Inhaltlich handelt es sich bei der Prognose nach § 18 Abs. 1 Nr. 4 BKAG um eine Einzelfallprüfung nach kriminalistischen Erfahrungsgrundsätzen,[1305] bei der „von dem speichernden Beamten eine alle Umstände des Einzelfalls berücksichtigende Individualprognose erwartet wird, die einer […] schematischen Darstellung nicht zugänglich ist. Je nach Lebenssachverhalt und je nach Datei kommen beispielsweise Ankündigungen einer Straftat, Offenbarungen gegenüber Dritten oder andere Hinweise in Betracht. Der wesentliche Unterschied zu Verdächtigen und Beschuldigten ist damit nicht das Merkmal einer vermeintlichen Beliebigkeit, sondern dass die Straftat, um die es geht, noch nicht begangen wurde."[1306] Die Regelung hat keinen strafprozessualen Anknüpfungspunkt mehr und dient daher rein präventiven Zwecken.[1307] Während die Datenverarbeitung in diesem Kontext in der Vergangenheit noch durch die für die jeweiligen Dateien erforderlichen Errichtungsanordnungen konkretisiert wurde,[1308] fehlt diese ermessensleitende Begrenzung nunmehr. Unter all diesen Gesichtspunkten ist der Auffangtatbestand des § 18 Abs. 1 Nr. 4 BKAG verfassungsrechtlich schwer tragbar, da bei polizeilicher Betrachtung

1302 *Graulich* in *Schenke/Graulich/Ruthig,* Sicherheitsrecht, § 18 BKAG Rn. 6.
1303 Vgl. *Arzt* Neue Juristische Wochenschrift 2011, 352, 354 für die Vorgängerversion des § 18 Abs. 1 Nr. 4 BKAG (§ 8 Abs. 5 BKAG a.F.).
1304 *Ruch/Feltes* NK 17 (2016), 62 (71 f.).
1305 BT-Drs. 16/13563, S. 8, zur Vorgängerversion des § 18 Abs. 1 Nr. 4 BKAG (§ 8 Abs. 5 BKAG a.F.).
1306 BT-Drs. 17/2803, S. 4.
1307 *Eichenhofer* in *Barczak* (Hrsg.), BKAG, § 18 Rn. 7.
1308 BT-Drs. 17/2803, S. 4.

individueller Lebenspraktiken wohl nicht selten Anhaltspunkte auftreten können, die eine entsprechende Annahme rechtfertigen können und so die Gefahr für Betroffene bergen, zum polizeilichen „Informationsobjekt" zu werden.[1309] Das gilt insbesondere in den Bereichen des Strafrechts, die stark von dessen kriminalpräventiven Neujustierung betroffen sind, wie etwa §§ 89a, 129a StGB. Auch eine sehr enge Ermessenspraxis, wie es *Graulich* zur verfassungsrechtlichen Bewahrung der Norm vorschlägt,[1310] ist mit Blick auf den Wesentlichkeitsgrundsatz eher abzulehnen: Eine exekutive Selbstprogrammierung in einem derart sensiblen Bereich kann – vor allem auch mit Blick auf die Geschichte der normativen Einhegung polizeilicher Informationsverarbeitung[1311] – nicht (mehr) hingenommen werden.

Ferner gestattet § 18 Abs. 3 BKAG es dem Bundeskriminalamt, sogenannte Prüffälle zu verarbeiten,[1312] also zu schauen, ob bei ihm eingegangene Erkenntnisse und Angaben zu Personen, die bisher unbekannt waren, dazu führen, dass die betroffene Person einer der in Abs. 1 genannten Kategorien unterfällt. Das Bundeskriminalamt muss dann zunächst feststellen, ob die personenbezogenen Daten für seine Aufgabenerfüllung erforderlich sind und, wenn dies zu bejahen ist, welcher Personenkategorie sie zugeordnet werden müssen.[1313] Die Daten sind gesondert im Informationssystem zu speichern, § 18 Abs. 3 S. 2 BKAG. Die Löschung hat gemäß Satz 3 nach Abschluss der Prüfung, spätestens jedoch nach zwölf Monaten zu erfolgen, wobei der Gesetzgeber zur Begründung dieser nicht unerheblichen Verarbeitungsdauer auf die vorhandenen Erfahrungen im internationalen Dienstverkehr und erhebliche Dauer von Strafverfahren im In- und Ausland verweist.[1314] Damit ist die Möglichkeit eröffnet, noch unter dem personenbezogenen Eingriffstatbestandes der sogenannten Anlassperson Daten zu speichern und zu verarbeiten, wenn auch – zumindest rechtlich – nur begrenzt.

1309 *Zöller,* Informationssysteme, S. 164.
1310 *Graulich* in *Schenke/Graulich/Ruthig,* Sicherheitsrecht, § 18 BKAG Rn. 11.
1311 Siehe dazu bereits oben S. 119 ff.
1312 Siehe dazu bereits oben S. 259 ff.
1313 BT-Drs. 18/11163, S. 99 f.
1314 BT-Drs. 18/11163, S. 100.

bb) Datenarten im Rahmen der Personenkategorien des § 18 BKAG

Die Arten der personenbezogenen Daten, die von den in § 18 Abs. 1 BKAG genannten Personen verarbeitet werden können, werden in § 18 Abs. 2 BKAG genannt und durch die BKADV konkretisiert. Demnach kann das Bundeskriminalamt (Nr. 1) von Personen nach Abs. 1 Nr. 1 bis 4 (lit. a) die Grunddaten, (lit. b) soweit erforderlich, andere zur Identifizierung geeignete Merkmale, (lit. c) die kriminalaktenführende Polizeidienststelle und die Kriminalaktennummer, (lit. d) die Tatzeiten und Tatorte und (lit. e) die Tatvorwürfe durch Angabe der gesetzlichen Vorschriften und die nähere Bezeichnung der Straftaten weiterverarbeiten. Darüber hinaus (Nr. 2) kann es von Personen nach § 18 Abs. 1 Nr. 1 und 2 BKAG weitere personenbezogenen Daten verarbeiten, soweit die Weiterverarbeitung erforderlich ist, weil wegen der Art oder der Ausführung der Tat, der Persönlichkeit der betroffenen Person oder sonstiger Erkenntnisse Grund zu der Annahme besteht, dass zukünftig Strafverfahren gegen sie zu führen sind. Dasselbe gilt auch für Personen nach § 18 Abs. 1 Nr. 3 und 4 BKAG, wobei hier keine solche Prognose durchzuführen ist, § 18 Abs. 2 Nr. 3 BKAG.

Diese noch recht weiten Beschreibungen der Arten personenbezogener Daten müssen durch die BKADV weiter eingegrenzt werden. Mangels aktueller und tatsächlich auf Grundlage von § 20 BKAG erlassener BKADV findet eine solche Eingrenzung gegenwärtig wohl nur auf Grundlage der alten BKADV statt. Eine Limitierung bewirkt zudem die für die Verarbeitung vorausgesetzten Erforderlichkeitsgründe des § 18 Abs. 2 Nr. 2. Diese sind strafrechtsakzessorisch auszulegen, wofür insbesondere spricht, dass § 18 Abs. 2 BKAG über § 16 Abs. 3 BKAG der Strafverfolgungsvorsorge dient und nicht der Gefahrenabwehr.[1315] „Art oder Ausführung der Tat" beinhaltet insofern, angelehnt an die Auslegung des § 46 Abs. 2 StGB, die Tat begleitende oder sie sonst prägende Aspekte, also etwa Tatmodaliäten von Zeit, Ort, Dauer und Mitteln.[1316] Um für die Datenverarbeitung erforderlich zu sein, müssen Merkmale der Persönlichkeit des Betroffenen in Zusammenhang mit dem bisherigen Verhalten stehen. Elemente der Lebensführung, die in keinerlei Zusammenhang zu dem Tatvorwurf stehen, können nicht als relevant berücksichtigt werden.[1317] Darüber hinaus können auch „sonstige Erkenntnisse" die Erforderlichkeit der Datenverarbeitung von

1315 *Graulich* in *Schenke/Graulich/Ruthig,* Sicherheitsrecht, § 18 BKAG Rn. 24.
1316 *Bußmann* in *Matt/Renzikowski,* Strafgesetzbuch: StGB, § 46 Rn. 17.
1317 *Kühl* in *Lackner/Kühl* (Hrsg.), Strafgesetzbuch, § 46 Rn. 36, 47.

Personen nach § 18 Abs. 1 Nr. 1 und 2 BKAG begründen. Dieser Auffangtatbestand räumt bei der Bestimmung des Verarbeitungsanlasses – ähnlich wie auch § 18 Abs. 1 Nr. 4 BKAG – in verfassungsrechtlich problematischer Weise einen normativ kaum gesteuerten Spielraum ein. So steht etwa zu befürchten, dass bestehende Erkenntnisse zu Personen – es geht um Verurteilte und Beschuldigte – den Bedarf an weiterer Datenverarbeitung aus sich selbst heraus legitimieren und so die datengestützten Einschätzungen bezüglich der Betroffenen perpetuieren.[1318]

Ist zumindest eine dieser Erforderlichkeitsvoraussetzungen erfüllt muss darüber hinaus noch Grund zu der Annahme bestehen, dass Strafverfahren gegen den Beschuldigten oder Tatverdächtigen zu führen sind. Der Gesetzesbegründung zufolge muss die durchzuführende Prognose neben der Persönlichkeit des Betroffenen alle Umstände des Einzelfalls berücksichtigen. Dabei muss es konkrete Anhaltspunkte für einen Verarbeitungsanlass geben, wofür aber ausreichen soll, wenn als Ergebnis einer summarischen Prüfung anhand der entsprechenden Anhaltspunkte nach allgemeinen Erfahrungswerten, wie etwa kriminalistischer Erfahrung, die Möglichkeit besteht, dass gegen den Betroffenen künftig Strafverfahren zu führen sein werden.[1319] Nötig ist dementsprechend eine Wiederholungsgefahr,[1320] wobei diese bei erstmalig Beschuldigten i.S.d. § 18 Abs. 1 Nr. 2 BKAG auch für ein erwiesenermaßen relevantes Verhalten in der Vergangenheit nicht ohne Weiteres – quasi schematisch – bejaht werden darf. Diese Prognose ist gerichtlich überprüfbar.[1321] Auch hier besteht indes ein weiter Deutungsspielraum bei den Polizeien.

Die Verarbeitung weiterer personenbezogener Daten ist gemäß § 18 Abs. 2 Nr. 3 BKAG zudem auch für die Personen nach Abs. 1 Nr. 3 und 4 gestattet. Da hier bereits für die Zuordnung zu einer der beiden Personenkategorie jeweils eine Prognose erforderlich ist, ist diese Voraussetzung im Rahmen des Abs. 2 Nr. 3 BKAG nachvollziehbarerweise nicht noch einmal genannt, wie in § 18 Abs. 2 Nr. 2 BKAG. Dennoch ist es nicht ohne Weiteres einsichtig, weshalb auch für die in Abs. 1 Nr. 3 und 4 genannten Personen ohne Weiteres die Verarbeitung weitere personenbezogener Daten möglich sein soll. Während sich argumentieren ließe, dass der Unterschied zwischen Beschuldigten und Tatverdächtigen eher formaler Natur

1318 So *Graulich* in *Schenke/Graulich/Ruthig,* Sicherheitsrecht, § 18 BKAG Rn. 27.
1319 BT-Drs. 13/1550, S. 25.
1320 *Graulich* in *Schenke/Graulich/Ruthig,* Sicherheitsrecht, § 18 BKAG Rn. 28.
1321 *Graulich* in *Schenke/Graulich/Ruthig,* Sicherheitsrecht, § 18 BKAG Rn. 28.

ist, ist doch jedenfalls für die Anlasspersonen von einem eher kategorischen Unterschied zu den restlichen Personenkategorien auszugehen, da – wie bereits ausgeführt wurde[1322] – ein breiter Personenkreis von der Regelung erfasst werden kann. Die bereits im Kontext des § 18 Abs. 1 BKAG problematische Gleichbehandlung setzt sich mithin auch in Abs. 2 fort. Das Gesetz gestattet damit nicht nur, dass überhaupt Daten zu Anlasspersonen gespeichert werden können, sondern ermöglicht auch die informationell tiefergehende Verarbeitung weiterer personenbezogener Daten.

Ähnlich wie § 16 BKAG enthält § 18 BKAG in seinem vierten Absatz eine Verarbeitungsermächtigung für die Haftdatei oder im geplanten „gemeinsamen Datenhaus" haftrelevante Daten. Er ersetzt den vormaligen § 9 Abs. 2 BKAG a.F., der die Haftdatei regelte.[1323]

cc) Weiterverarbeitungssperre im Rahmen des § 18 BKAG

Gemäß § 18 Abs. 5 BKAG ist die Weiterverarbeitung unzulässig, wenn der Beschuldigte rechtskräftig freigesprochen, die Eröffnung des Hauptverfahrens gegen ihn unanfechtbar abgelehnt oder das Verfahren nicht nur vorläufig eingestellt wird und sich aus den Gründen der Entscheidung ergibt, dass die betroffene Person die Tat nicht oder nicht rechtswidrig begangen hat. Bei fehlender Schuld und Strafausschließungsgründen ist einzelfallbezogen zu prüfen, ob die Prognose dennoch zu bejahen ist.[1324] Zudem sind die Daten nach den allgemeinen Löschungsregeln der §§ 77 ff. BKAG zu löschen, wenn sie nicht mehr erforderlich sind.[1325] Bei nicht ausreichendem Tatverdacht kann die Verarbeitung hingegen weitergeführt werden.[1326] Die Regelung ist mithin sehr relevant für die Grenzen kriminalpolizeilicher Datenverarbeitung.

Zentral für die Beurteilung der Unzulässigkeit der Weiterverarbeitung ist, dass sich aus den Gründen der Entscheidung positiv ergibt, dass die betroffene Person die Tat nicht oder nicht rechtswidrig begangen hat. Ergibt sich diese positive Feststellung nicht aus der Entscheidung, ist dem Bundesverwaltungsgericht zufolge der Tatbestand des § 18 Abs. 5 BKAG

1322 Siehe dazu oben S. 324 f.
1323 Siehe zur Haftdatei bereits oben S. 244.
1324 BT-Drs. 13/1550, S. 25.
1325 Siehe dazu unten S. 370 f.
1326 BT-Drs. 13/1550, S. 25.

nicht erfüllt. Die positive Bestätigung eines Restverdachts durch die jeweilige Entscheidung ist für die Zulässigkeit der Weiterverarbeitung nach dem Gesetz demzufolge nicht notwendig. Dem Bundesverwaltungsgericht nach ist dies auch nicht als Verstoß gegen die in Art. 6 Abs. 2 EMRK verbürgte Unschuldsvermutung zu werten, da die „Berücksichtigung von Verdachtsgründen, die auch nach einer Verfahrensbeendigung durch Freispruch oder Einstellung fortbestehen können, keine Schuldfeststellung oder -zuweisung [darstellt], wenn und soweit sie bei Wiederholungsgefahr anderen Zwecken, insbesondere der vorbeugenden Straftatenbekämpfung, dient."[1327] Wie bereits dargelegt, erscheint diese Ansicht zweifelhaft.[1328] Zudem ist dieses Verständnis mit Blick auf die Konstellation der Verfahrenseinstellung nach § 170 Abs. 2 StPO problematisch. Die staatsanwaltschaftliche Begründung richtet sich in diesem Fall nach den Richtlinien für das Strafverfahren und das Bußgeldverfahren (RiStBV), in deren Nr. 88, „Mitteilungen an den Beschuldigten", vorgesehen ist, dass bei einer Einstellung nach § 170 Abs. 2 StPO die Gründe der Einstellung der beschuldigten Person nur auf Antrag und dann auch nur soweit bekannt zu geben sind, als kein schutzwürdiges Interesse entgegensteht. Hat sich die Unschuld herausgestellt oder besteht kein begründeter Verdacht mehr, so ist dies ebenfalls mitzuteilen. Obwohl die Begründung des § 170 Abs. 2 StPO auch im Rahmen des § 18 Abs. 5 BKAG relevant wird, hat es der Gesetzgeber unterlassen, kompatible Kategorien zu schaffen. Aus der Mitteilung der Staatsanwaltschaft ergibt sich somit nicht unmittelbar, ob Beschuldigte die Tat nicht oder nicht rechtswidrig begangen haben, wie es für § 18 Abs. 5 BKAG erforderlich wäre. Das Bundesverwaltungsgericht spricht sich anlässlich dieser Rechtslage für eine „Anpassung der Begrifflichkeiten in § 170 StPO, Nr. 88 RiStBV, § 8 Abs. 3 BKAG und § 484 Abs. 2 Satz 2 StPO" aus, um „die Folgen der Einstellung eines strafrechtlichen Ermittlungsverfahrens für die Befugnis zur Datenspeicherung aus Gründen der vorbeugenden Verbrechensbekämpfung oder der Strafverfolgungsvorsorge normklarer zu gestalten."[1329] Gleichzeitig zieht es allerdings nicht die Konsequenz, die Verarbeitungsvoraussetzungen wegen der inkompatiblen Kategorien zu verneinen.[1330] Vielmehr will das Gericht die Entscheidung über die Unzulässigkeit der Weiterverarbeitung auf die Mittelung der Staatsanwaltschaft an die Polizeibehörde, die im Rah-

1327 Vgl. BVerwGE 137, 113, Rn. 26 zu der Vorgängerregelung § 8 Abs. 3 BKAG a.F.
1328 Siehe dazu bereits oben S. 243 f.
1329 BVerwGE 137, 113, Rn. 29.
1330 So wohl *Graulich* in *Schenke/Graulich/Ruthig*, Sicherheitsrecht, § 18 BKAG Rn. 51.

men des polizeilichen Informationssystems die datenschutzrechtliche Verantwortung für die beim Bundeskriminalamt gespeicherten Daten gemäß § 16 Abs. 2 trägt, stützen. Nach § 482 Abs. 2 StPO hat die Staatsanwaltschaft die mit der Angelegenheit befasste Polizeibehörde über den Ausgang des Verfahrens zu unterrichten. Grundsätzlich geschieht dies durch Mitteilung der Entscheidungsformel, kann aber erforderlichenfalls auch durch die mit Gründen versehene Einstellungsentscheidung erfolgen. Auch soll die entsprechende Polizeibehörde gegebenenfalls bei der Staatsanwaltschaft um eine solche begründete Entscheidung nachsuchen, bevor sie über weitere Datenverarbeitungen entscheidet.[1331]

Damit ergibt sich indessen ein etwas inkonsistenter Zustand im Rahmen der Rechtsanwendung des § 18 Abs. 5 BKAG: Bei Freispruch oder Nichteröffnung des Hauptverfahrens ist die Verarbeitung nach der Vorschrift unzulässig. Bei einer Einstellung nach § 170 Abs. 2 StPO, für die erforderlich ist, dass bei Durchführung der Hauptverhandlung ein Freispruch wahrscheinlicher ist als eine Verurteilung, ist dies jedoch nach Rechtsprechung des Bundesverwaltungsgerichts nicht der Fall. Trotz des Umstandes also, dass die drei Varianten des § 18 Abs. 5 BKAG in ihrer Implikation für das Vorliegen einer Straftat vergleichbar sind, werden sie unterschiedlich gehandhabt. Zudem besteht für den Betroffenen aufgrund der positiven Wirkung des § 170 Abs. 2 StPO keine Möglichkeit eine Einstellungsentscheidung im oben genannten Sinne herbeizuführen.[1332] Im Ergebnis bedeutet dies für die Praxis polizeilicher Informationsverarbeitung, dass personenbezogene Daten von einem wohl nicht unerheblichen Teil der Beschuldigten auch nach Beendigung des Strafverfahrens im Wege der Einstellung weiterverarbeitet werden dürfen.

dd) Datenverarbeitungen nach § 19 BKAG

Der „personenbezogene Eingriffstatbestand“[1333] des § 19 BKAG gestattet über die Kategorien des § 18 BKAG hinaus Daten zu anderen Personen zu verarbeiten. Auch § 19 BKAG Abs. 1 S. 1 BKAG nennt in Umsetzung des Art. 6 lit. d JI-Richtlinie abgegrenzte Personengruppen, bei denen tatsächliche Anhaltspunkte dafür vorliegen, dass (Nr. 1) sie bei einer zukünftigen Strafverfolgung als Zeugen in Betracht kommen, (Nr. 2) bei einer künftigen

1331 BVerwGE 137, 113, Rn. 30.
1332 *Graulich* in *Schenke/Graulich/Ruthig,* Sicherheitsrecht, § 18 BKAG Rn. 51.
1333 Siehe dazu bereits Fn. 1292.

Straftat als Opfer in Betracht kommen, (Nr. 3) sie mit in § 18 Abs. 1 Nr. 1 bis 3 BKAG bezeichneten Personen nicht nur flüchtig oder in zufälligem Kontakt und in einer Weise in Verbindung stehen, die erwarten lässt, dass Hinweise für die Verfolgung oder vorbeugende Bekämpfung dieser Straftaten gewonnen werden können, weil Tatsachen die Annahme rechtfertigen, dass die Personen von der Planung oder der Vorbereitung der Straftaten oder der Verwertung der Tatvorteile Kenntnis haben oder daran mitwirken, oder (Nr. 4) es sich um Hinweisgeber und sonstige Auskunftspersonen handelt.

Auch hier müssen im Rahmen der Erforderlichkeitsvoraussetzung des Tatbestandes konkrete Anhaltspunkte vorliegen, dass die Verarbeitung der personenbezogenen Daten zur Verhütung von Straftaten oder Strafverfolgungsvorsorge notwendig ist; allgemeine Nützlichkeitserwägungen sind nicht ausreichend.[1334] Der Wortlaut des § 19 Abs. 1 S. 1 BKAG drückt durch die Nennung von Verhütung von Straftaten, die im Polizeirecht wurzelt, und Strafverfolgungsvorsorge, die aus dem Strafrecht herrührt, ein kompetenzrechtliches Verständnis der Verschränkung beider Bereiche aus, was unter dem Gesichtspunkt der legislatorisch grundsätzlich getrennten Verantwortung problematisch ist. Dies trägt zur Vermischung von Präventiv- und Repressivdaten bei. Ferner ist in § 16 Abs. 3 BKAG nur der Verweis auf die Strafverfolgungsvorsorge enthalten, sodass sich § 19 Abs. 1 S. 1 BKAG innerhalb des BKAG widersprüchlich verhält.[1335] Der Begriff der erheblichen Straftat ist identisch mit dem in § 2 Abs. 1 BKAG. Die Prognose diesbezüglich folgt demselben Schema wie im Rahmen des § 18 Abs. 1 Nr. 4 BKAG.[1336] Da personeller Anknüpfungspunkt die zukünftige Straftat eines Dritten ist, muss diese erläutert und überprüfbar festgehalten werden, damit der Verarbeitungszweck erkennbar wird und bleibt.[1337] Auffällig ist zudem die Eingriffsschwelle der „tatsächliche[n] Anhaltspunkte", die dem Recht der Nachrichtendienste entlehnt ist und keine Berührungspunkte mit den Eingriffsschwellen der konkreten Gefahr der Gefahrenabwehr bzw. des Anfangsverdachts der Strafverfolgung hat. Die demgegenüber niedrigere Schwelle im nachrichtendienstlichen Kontext kann mit Blick auf die regelmäßig weniger eingriffsintensiven Maßnahmen der Dienste gerechtfertigt

1334 *Graulich* in *Schenke/Graulich/Ruthig,* Sicherheitsrecht, § 19 BKAG Rn. 4.
1335 *Zöller,* Informationssysteme, S. 165 zum insoweit identischen § 20 BKAG a.F.
1336 Siehe dazu bereits oben S. 324 ff.
1337 *Graulich* in *Schenke/Graulich/Ruthig,* Sicherheitsrecht, § 19 BKAG Rn. 6.

werden, ist allerdings im Rahmen der polizeilichen Datenverarbeitung problematischer.[1338]

Liegen die Tatbestandsvoraussetzungen vor, so kann das Bundeskriminalamt personenbezogene Daten der vier genannten Personenkategorien verarbeiten, wobei für Zeug:innen, Opfern und Hinweisgeber:innen zudem noch deren Einwilligung erforderlich. Bei Kontakt- oder Begleitpersonen nach § 19 Abs. 1 Nr. 3 BKAG handelt es sich um Auffangkategorien. Nachdem die Vorgängerregelung des § 8 Abs. 4 BKAG a.F. nach heutigen verfassungsrechtlichen Maßstäben, wie sie im Antiterrordatei-Urteil zum Ausdruck gekommen sind,[1339] keinen Bestand mehr hätte, hat sich der Gesetzgeber bei der Novellierung des BKAG für den Zusatz entschieden, dass Tatsachen die Annahme rechtfertigen müssen, dass die Kontakt- oder Begleitpersonen maßgebliche Kenntnis der Straftaten besitzen oder daran mitgewirkt haben müssen. Der Begründung zufolge entspricht dies wesentlichen verfassungsrechtlichen Vorgaben und stellt einen „objektiven Tatbezug" her.[1340] Das ist hinsichtlich der einer jeden Prognose innewohnende Unsicherheit allerdings nur bis zu einem gewissen Grad der Fall.[1341] Der Bestimmtheitsgrad dieser Kategorie ist dementsprechend zumindest kritisierbar.

Die Arten der personenbezogenen Daten sind allerdings gemäß § 19 Abs. 1 S. 2 BKAG gegenüber dem insofern extensiveren § 18 Abs. 1 BKAG eingeschränkt: Die Weiterverarbeitung ist demnach beschränkt auf die in § 18 Abs. 2 Nr. 1 lit. a bis lit. c BKAG bezeichneten Daten sowie auf die Angabe, in welcher Eigenschaft der Person in Bezug auf welchen Sachverhalt die Speicherung der Daten erfolgt. Das Fehlen einer aktualisierten BKADV wirkt sich auch hier auf die Konkretisierung der Datenverarbeitung aus.

Die in § 19 Abs. 1 S. 1 Nr. 3 BKAG genannten Personen müssen dabei mit einer Personenkategorie des § 18 Abs. 1 BKAG in Verbindung gebracht werden, wobei nur Verurteilte, Beschuldigte und Tatverdächtige taugliche Anknüpfungspersonen sein können, Der damit zum Ausdruck kommende Ausschluss von Anlasspersonen gemäß § 18 Abs. 1 Nr. 4 BKAG ist aufgrund der unbestimmten personellen Reichweite dieser Norm verfassungsrechtlich zu begrüßen. Eine Datenverarbeitung wäre ansonsten von einer doppelten personenbezogenen Prognose abhängig, deren Hintereinanderschal-

1338 *Graulich* in *Schenke/Graulich/Ruthig,* Sicherheitsrecht, § 19 BKAG Rn. 7.
1339 BVerfGE 133, 277, 347 ff. – Antiterrordateigesetz.
1340 BT-Drs. 18/11163, S. 100.
1341 Siehe etwa *Schöch* in Hans Schneider (Hrsg.), Grundlagen der Kriminologie, 359 (S. 361).

tung erhebliches Potenzial für Falschpositive mit sich brächte. Allerdings bedeutet die Einbeziehung von Tatverdächtigen (und, in abgeschwächter Form auch von Beschuldigten) ebenfalls eine Verkettung zweier Prognosen, denn auch bei dieser Personenkategorie ist noch nicht sicher, ob sie tatsächlich eine Straftat begangen haben.

Wie bereits § 18 Abs. 3 BKAG hat auch § 19 BKAG in seinem Abs. 3 eine insoweit identische Prüffallregelung. Diese ist mit Blick auf die mitunter unsichere Tatsachengrundlage für Datenverarbeitungen nach § 19 Abs. 1 Nr. 3 BKAG problematisch, denn eine Prüfung dahingehend, ob eine Person in der tatbestandlich relevanten Weise mit (potenziell) delinquenten Personen gemäß § 18 Abs. 1 Nr. 1-3 BKAG in Verbindung steht, kann theoretisch bei allen Personen durchgeführt werden, die irgendwie in Kontakt mit einer Person aus den Kategorien des § 18 Abs. 1 Nr. 1-3 BKAG gekommen sind.

ee) Konstruktionsfehler in der neuen Informationsarchitektur?

Wie *Bäcker* herausgearbeitet hat, tun sich – wie bei § 16 BKAG – auch im Rahmen der §§ 18, 19 BKAG strukturelle Probleme auf, die aus dem Zusammentreffen der novellierten Gesetzessystematik und den verfassungsrechtlichen Anforderungen herrühren[1342]: Das unklare Verhältnis der beiden personenbezogenen Eingriffstatbestände der §§ 18, 19 BKAG zu § 16 Abs. 1 BKAG und damit mittelbar zu § 12 BKAG verursacht Schwierigkeiten bei der Auslegung: Dem Wortlaut des § 16 Abs. 1 BKAG zufolge sind Verarbeitungen nach dieser Datenverarbeitungsgeneralklausel möglich, „soweit dieses Gesetz keine zusätzlichen besonderen Voraussetzungen vorsieht." Da die §§ 18, 19 BKAG die Datenverarbeitung jedoch an andere Voraussetzungen als die Erforderlichkeit des § 16 Abs. 1 BKAG knüpfen, gehen diese beiden Normen dem § 16 Abs. 1 BKAG „soweit" vor. Nun verweist § 16 Abs. 1 BKAG über seine eigenen Voraussetzungen hinaus auch auf § 12 BKAG, der den verfassungsrechtlichen Grundsatz der hypothetischen Datenneuerhebung einfachgesetzlich abbildet. Einen entsprechenden Verweis findet man in den §§ 18, 19 BKAG indessen nicht. Bei Speicherungen von Daten nach §§ 18, 19 BKAG kommt es allerdings regelmäßig zu einer Zweckände-

1342 Siehe zu den weiteren Ausführungen die äußerst instruktive Stellungnahme *Bäckers* vor dem Innenausschuss des Deutschen Bundestages, *ders.*, A-Drs. 18(4)806 D, S. 6 ff.

rung, wenn Daten nunmehr der bundeskriminalamtlichen Zentralstellenfunktion unterfallen sollen. Anlässlich einer solchen Zweckänderung wäre prinzipiell erforderlich, dass die Voraussetzungen der hypothetische Datenneuerhebung, wie sie in § 12 BKAG zum Ausdruck kommen, gegeben sind. Die Datenverarbeitungsgeneralklausel des § 16 Abs. 1 BKAG scheint ihrem Wortsinn nach ebenfalls davon auszugehen, insofern dort die Rede davon ist, dass Subsidiarität nur insoweit eintritt, als „zusätzliche" Erfordernisse aufgestellt werden. Der Gesetzgeber spricht hingegen davon, dass „spezifische Weiterverarbeitungsbefugnisse" dem § 16 Abs. 1 „vorgehen"[1343] und legt damit eher eine totale Subsidiarität nahe. Zudem findet sich im Wortlaut der §§ 18, 19 BKAG keinerlei Verweis auf § 12 BKAG.

Die gesetzliche Systematik lässt damit zwei Auslegungsalternativen zu: Entweder findet der Grundsatz der hypothetischen Datenneuerhebung auch im Rahmen der §§ 18, 19 BKAG Anwendung, oder eben nicht. Während die Notwendigkeit zur Gesetzesauslegung prinzipiell kein Problem, sondern dem Recht vielmehr inhärent ist, ist die Situation im Rahmen der §§ 18, 19 BKAG problematisch, weil beide Auslegungsalternativen gänzlich unerwünschte Ergebnisse liefern.

In der ersten Auslegungsvariante – über den nur teilweise subsidiären § 16 Abs. 1 BKAG findet der in § 12 BKAG verkörperte Grundsatz der hypothetischen Datenneuerhebung im Rahmen der §§ 18, 19 BKAG Anwendung – wäre eine polizeipraktisch ungünstige Situation das Ergebnis. Die §§ 18, 19 BKAG dienen dem Bundeskriminalamt dazu, personenbezogene Daten für künftige Verfahren vorzuhalten. Die Befugnis dazu knüpft an die strafprozessuale Rolle einer Person oder an eine auf bestimmte Tatsachen gestützte Prognose einer zukünftigen Rolle der Person an. Die damit verbundenen Erwartungen sind hingegen rein personenbezogen und sehen keine situationsbezogene Schadensprognose im Einzelfall vor. Hingegen fordert die hypothetische Datenneuerhebung, dass ein „konkreter Ermittlungsansatz" vorliegt, wenn Daten zweckändernd weiterverarbeitet werden sollen.[1344] Dieses relativ neue verfassungsrechtliche Erfordernis ist vom Gesetzgeber insoweit konkretisiert worden, dass der Ermittlungsansatz zu bejahen ist wenn „sich eine Gefahr für mindestens vergleichbar bedeutsame Rechtsgüter, zu deren Schutz die ursprüngliche Datenerhebung vorgenommen wurde, nicht nur abstrakt, sondern vielmehr als eine in ersten Um-

1343 BT-Drs. 18/11163, S. 94.
1344 Siehe dazu bereits oben S. 168 f.

rissen absehbare und konkretisierte Möglichkeit eines Schadenseintrittes für ein solches Rechtsgut darstellt."[1345] Wäre dies nun im Rahmen von zweckändernden Datenverarbeitungen im Bereich der §§ 18, 19 BKAG zu beachten, wäre bei jeder Datenverarbeitungshandlung, also bereits bei der initialen Datenspeicherung, ein konkreter Ermittlungsansatz erforderlich. Ein solcher lässt sich jedoch nicht bereits aus einer gemäß §§ 18, 19 BKAG anzustellenden rein personenbezogenen Prognosen ableiten; gleiches gilt für den Umstand, dass jemand in der Vergangenheit verurteilt oder beschuldigt worden ist. Vielmehr bedürfte es einer darüberhinausgehenden Schadensprognose, um ein einzelnes Datum überhaupt erst zu speichern. Damit hätte der Gesetzgeber die Verarbeitungsbefugnisse des Bundeskriminalamtes gegenüber der vorherigen Rechtslage eingeschränkt. Die Intention, einen umfassenden Informationsbestand für noch nicht absehbare Lagen zu schaffen, würde konterkariert und die Aufgabe des Bundeskriminalamtes, als Zentralstelle im Informationsverbund zu fungieren, wäre erheblich beeinträchtigt, was die polizeiliche Informationsverarbeitung insgesamt empfindlich treffen würde.

Folgt man hingegen der zweiten Auslegungsalternative– § 16 Abs. 1 BKAG tritt gegenüber §§ 18, 19 BKAG vollständig subsidiär zurück – entstehen verfassungsrechtliche Probleme. Der Grundsatz der hypothetischen Datenneuerhebung gemäß § 12 BKAG käme im Rahmen der § 18, 19 BKAG nie zur Anwendung. Damit wären Datenverarbeitungen in diesem Bereich lediglich daran geknüpft, dass die personenbezogenen Eingriffstatbestände erfüllt sind, die letztlich nur Prognosen über zukünftiges Verhalten sind. Einmal auf diese Weise gespeicherte Daten könnten beliebig verarbeitet werden. Mit Blick auf die bundesverfassungsrechtliche Rechtsprechung zur Verarbeitung personenbezogener Daten ist dies widersprüchlich: Wenn schon für zweckändernde Verarbeitungen, die sich unmittelbar an die Erhebung anschließen, der Grundsatz der hypothetischen Datenneuerhebung gilt, muss dies erst recht gelten, wenn die Daten zwischenzeitlich im Informationsbestand vorgehalten worden sind. Ein solcher grenzenloser Umgang mit einmal gespeicherten Daten würde den Grundsatz der Zweckbindung für die in Frage stehenden Verarbeitungsformen mithin auch in rechtlicher Hinsicht abschaffen.

Eine dritte, sinnvollere Auslegungsvariante, etwa dass der Grundsatz der hypothetischen Datenneuerhebung nicht bei der Datenspeicherung nach

1345 BT-Drs. 18/11163, S. 91.

§§ 18, 19 BKAG, sondern erst bei der dann folgenden Verwertung Anwendung findet – ebenfalls ein Vorschlag *Bäckers* – lässt sich mit dem gegebenen Regelungen indessen nicht konstruieren, da in Anlehnung an den Begriff der Weiterverarbeitung von Daten, wie ihn die JI-Richtlinie kennt, unterschiedslos jeder Umgang von Daten von der insoweit indifferenten Terminologie des BKAG erfasst wird, mithin keine Trennung zwischen Speicherung und Verwertung möglich ist.[1346]

Insgesamt ist *Bäckers* Kritik an den zentralen Normen der neuen Informationsarchitektur des Bundeskriminalamtes zuzustimmen: Die Novellierung hat den Versuch unternommen, verfassungs- und unionsrechtliche Vorgaben möglichst sparsam und kompakt in das bisherige Gesetz einzupassen und hat damit eine für die vorgesehene Praxis der polizeilichen Datenverarbeitung unpassende normative Struktur geschaffen. Um den problematisch ausufernden Anwendungsbereich des § 16 Abs. 1 BKAG[1347] einzugrenzen, ist die inhaltliche Begrenzung des Begriffs der „weiteren Nutzung" dahingehend sinnvoll, dass nur Datennutzungen erfasst werden, die sich unmittelbar an das polizeiliche Verfahren anschließen, aus dem die Daten stammen. Werden die Daten über das Verfahren hinaus nicht mehr gebraucht, ist aus Verhältnismäßigkeitsgesichtspunkten eine Löschung vorzunehmen. Das bedeutet nicht, dass eine Speicherung ausgeschlossen wäre, aber sie sollte an andere Voraussetzungen geknüpft werden, als diejenigen, die für die weitere Nutzung ausschlaggebend sind. Auch Datenspeicherung und Datenverwertung scheinen kaum zusammengefasst unter dem Begriff der Weiterverarbeitung regelbar zu sein, wie die vorangegangenen Ausführungen zu §§ 18, 19 BKAG und ihr Verhältnis zu § 16 Abs. 1 in Verbindung mit § 12 BKAG gezeigt haben sollten. *Bäcker* schlägt hier eine Trennung der jeweiligen Phasen der Datenverarbeitung vor.[1348] Die Datenspeicherung ließe sich dementsprechend, wie es bereits zuvor angeklungen ist und auch der gegenwärtigen Rechtslage entspricht, auf die personenbezogene Prognose stützen. Die Datenverwertung hingegen bedürfte dann einer eigenen Verwertungsbefugnis, die bestimmte Anlässe festlegt oder allgemein auf den Grundsatz der hypothetischen Datenneuerhebung verweist. Dabei ist insgesamt zu beachten, dass Datenspeicherung und -verwertung miteinander in rechtlicher Wechselwirkung stehen: Je niedrigschwelliger der Speicherungsanlass, desto höher müssen die Voraussetzungen an die

1346 *Bäcker*, A-Drs. 18(4)806 D, S. 9 f.
1347 Siehe dazu bereits oben S. 320 ff.
1348 *Bäcker*, A-Drs. 18(4)806 D, S. 10.

sich anschließende Verwertung sein, und umgekehrt. Demnach müssen in unterschiedlichen Konstellationen diese beiden Formen des Datenumgangs in einer austarierten Weise aufeinander eingestellt werden. Die undifferenzierte Regelungsweise des BKAG schafft ein solches Austarieren, wie es für die verschiedenen Datenverarbeitungsbereiche des Bundeskriminalamtes notwendig wäre, nicht, sondern versucht die polizeiliche Datenverarbeitung in eine datenrechtliche Einheitsgröße zu zwängen. Das ist umso bedenklicher, als es nicht nur darum geht, eine bestehende Praxis rechtlich neu einzukleiden, sondern der Weg für einen neuen Modus der Informationsverarbeitung geebnet werden soll. Mit der Abschaffung der Dateien und der Errichtung eines einheitlichen Informationsbestandes, der „rechtlich primär durch den Grundsatz der hypothetischen Datenneuerhebung gesteuert werden" soll[1349] , wurde eine ambitionierte Zielvorstellung für das polizeiliche Informationswesen gesetzt. Die Umsetzung, so zeigen die vorstehenden Ausführungen, ist nicht nur technisch, sondern auch rechtlich so komplex, dass *Bäcker* zufolge eine „rechtlich tragfähige Fundierung" für die Neugliederung der Informationsordnung derzeit noch nicht in Sicht ist. Zwar wird die vage und vor allem fehlerbehaftete Normierung des Vorhabens vor diesem Hintergrund verständlich.[1350] Die Oberflächlichkeit und fehlende Stringenz der legislativen Befassung, die in den rechtlichen Mängeln der §§ 16, 18, 19 BKAG zum Ausdruck kommen, zeigen jedoch erneut den peripheren Stellenwert des Rechts im Rahmen der polizeilichen Informationsverarbeitung auf äußerst bedenkliche Weise.

c) Datenübermittlung im Rahmen des Informationsverbundes: Eingabe und Abruf

Der Informationsaustausch zwischen den deutschen Polizeien, der neben der Errichtung eines einheitlichen polizeilichen Datenbestandes die Hauptfunktion des Informationsverbundes ist, geschieht durch Eingabe und Abruf von Daten, wobei es sich rechtlich um Datenübermittlungen handelt.

1349 *Bäcker*, A-Drs. 18(4)806 D, S. 10.

1350 Ähnlich *Bäcker*, A-Drs. 18(4)806 D, S. 10, der eindringlich dazu riet, den die Informationsordnung betreffenden Teil des Gesetzesvorhabens zurückzustellen und eventuell auch die alte Dateienstruktur mit Blick auf die verfassungsrechtlichen Vorgaben normativ zu modernisieren. Der Gesetzgeber hat keine seiner Anmerkungen und Vorschläge aufgegriffen.

aa) Datenübermittlung an den polizeilichen Informationsverbund

Die Übermittlung der Daten an das Bundeskriminalamt zur Speicherung im Informationsverbund ist im Wesentlichen durch § 32 BKAG geregelt. Dessen Abs. 1 Satz 1 verpflichtet zunächst die einzelnen Landeskriminalämter, dem Bundeskriminalamt nach Maßgabe der Rechtsverordnung nach § 20 BKAG die zur Erfüllung seiner Aufgaben als Zentralstelle erforderlichen Informationen zu übermitteln. Die in der Vorschrift in Bezug genommene Rechtsverordnung ist die BKADV[1351], welche die Datenarten konkretisieren soll. Die Landeskriminalämter sind damit wesentlich für den polizeilichen Informationsaustausch mitverantwortlich.[1352] Neben den Landeskriminalämtern kann die Verpflichtung zur Datenübermittlung auch von anderen Polizeibehörden des Landes erfüllt werden, § 32 Abs. 1 Satz 2 BKAG. Gemäß § 32 Abs. 1 Satz 3 BKAG legt das Bundeskriminalamt zudem im Benehmen mit den Landeskriminalämtern Einzelheiten der Informationsübermittlung fest. Damit wird eine Koordination der Informationsübermittlung, insbesondere formal und inhaltlich, ermöglicht.[1353] Um Einzelheiten überhaupt zu festlegen zu können, ist zunächst eine Konkretisierung durch die BKADV als Grundlage erforderlich,[1354] von der es gegenwärtig keine auf die aktuelle Rechtslage angepasste Version gibt. Mit der Verpflichtung aus § 32 korrespondiert für die am polizeilichen Informationsverbund teilnehmenden Stellen nach § 29 Abs. 3 Satz 2 BKAG das Recht, Daten zur Erfüllung der Verpflichtung nach § 32 BKAG im automatisierten Verfahren einzugeben. Besondere Regelung für die Einrichtung von automatisierten Datenabrufen ist verfassungsrechtlich geboten, weil sich Verfahrensstruktur gegenüber herkömmlichen Übermittlungen unterscheidet, was für Betroffene zusätzliche informationelle Risiken birgt: Raum-zeitliche Schranken des Datenzugriffs bestehen nicht mehr, die Daten sind für potenzielle Datenempfänger jederzeit verfügbar. Zudem erfolgt beim Online-Zugriff regelmäßig keine Prüfung der Rechtmäßigkeit vor der jeweiligen Datenübermittlung durch die übermittelnde Stelle, sondern die empfangende Stelle entscheidet durch ihren Abruf, ob und wann es zu einer Übermittlung kommt.[1355]

1351 Siehe dazu bereits oben S. 227 ff.
1352 BT-Drs. 13/1550, S. 30.
1353 BT-Drs. 13/1550, S. 30.
1354 OVG Lüneburg NdsVBl. 2009, 135 Rn. 17.
1355 *Petri* in *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch, H. Rn. 467.

Einen weiteren zentralen Aspekt der Datenübermittlung regelt § 32 Abs. 2 BKAG. Während in dessen Satz 1 eine grundsätzliche und unverzügliche Mitteilungspflicht der Justiz- und Verwaltungsbehörden der Länder gegenüber dem jeweils zuständigen Landeskriminalamt bezüglich Unterbrechungen und Beendigungen von Freiheitsentziehungen statuiert, die durch ein Gericht wegen des Verdachts oder des Nachweises einer rechtswidrigen Tat angeordnet worden sind, ist es vor allem § 32 Abs. 2 Satz 2 BKAG, der in der polizeilichen Informationsarchitektur eine wichtige Funktion einnimmt: Danach teilen die Justizbehörden des Bundes und der Länder bei Mitteilungspflicht nach Abs. 1 dem jeweils zuständigen Landeskriminalamt unverzüglich und, soweit technisch möglich, automatisiert mit, ob die beschuldigte Person rechtskräftig freigesprochen wurde (Nr. 1 lit. a), die Eröffnung des Hauptverfahrens unanfechtbar abgelehnt wurde (Nr. 1 lit. b) oder das Verfahren nicht nur vorläufig eingestellt wurde (Nr. 1 lit. c). Nach § 32 Abs. 2 Satz 2 Nr. 2 BKAG sind zudem die tragenden Gründe der Entscheidung mitzuteilen. Dieser Zusatz im Rahmen der Mitteilungspflicht ist neu durch das BKAG von 2018 eingefügt worden und soll sicherstellen, dass die Polizeien des Bundes und der Länder in die Lage versetzt werden, Speicherungen in ihren Informationssystemen und im Informationsverbund nach Abschluss des justiziellen Verfahrens auf die Notwendigkeit der weiteren Speicherung hin zu überprüfen, die entsprechenden Löschungen vorzunehmen und hierdurch ungerechtfertigte Speicherungen, also Datenverarbeitungen Unschuldiger,[1356] zu vermeiden. Gegenwärtig ist das Meldeverhalten der Justizbehörden beschränkt und uneinheitlich, was die Überprüfung erschwert oder verhindert.[1357]

Neben den Landeskriminalämtern und -polizeibehörden sind gemäß § 32 Abs. 3 BKAG auch Bundespolizeibehörden dem Abs. 1 entsprechend verpflichtet, sofern die Informationen Vorgänge betreffen, die sie in eigener Zuständigkeit bearbeiten. Gleiches gilt für das Bundeskriminalamt und seine nach den §§ 3 bis 8 BKAG gewonnenen Informationen. Neben den direkt erlangten Informationen handelt es sich dabei um aus vorhandenen Daten neu abgeleitete Informationen, wobei nicht erforderlich ist, dass es sich um ein Produkt automatisierter Datenverarbeitung handelt.[1358]

1356 *Barczak* in *Barczak* (Hrsg.), BKAG, § 32 Rn. 14.
1357 BT-Drs. 18/11163, S. 110.
1358 *Graulich* in *Schenke/Graulich/Ruthig,* Sicherheitsrecht § 32 BKAG Rn. 16.

bb) Datenübermittlungen aus dem Informationsverbund

Datenübermittlungen aus dem Informationsverbund heraus erfolgen regelmäßig[1359] in Form des (automatisierten) Abrufs, zu dem teilnehmenden Stellen nach § 29 Abs. 3 Satz 2 BKAG berechtigt sind, soweit dies zur jeweiligen Aufgabenerfüllung erforderlich ist. Dies bezieht sich auf die generelle Aufgabenzuweisung eines INPOL-Teilnehmers. Da die Dateistruktur zunächst weiter Bestand hat, wird bisher noch durch Errichtungsanordnungen festgelegt, welcher Teilnehmer in welchem Umfang Daten eingeben und abrufen darf.[1360] In Zukunft wird dies weniger trennscharf durch das Kriterium der Verbundrelevanz gesteuert werden.[1361] Zentral für eine verfassungsgemäße Ausgestaltung ist die Beachtung der in § 29 Abs. 4 Satz 2 BKAG erwähnten Regulative wie der Grundsatz der hypothetischen Datenneuerhebung (§ 12 Abs. 2–5 BKAG), die dafür nötigen Kennzeichnungspflichten (§ 14 BKAG), die Bindung an die Erforderlichkeit der Kenntnis der Daten für mehr oder weniger konkretisierte Aufgaben und Pflichten (beispielsweise § 15 Abs. 1 Nr. 2 BKAG) sowie sachlich oder personell mehr oder weniger differenzierte Schwellen für die Datenverarbeitung (§§ 16, 18 und 19 BKAG), deren Einhaltung das Bundeskriminalamt organisatorisch und technisch sicherzustellen hat.[1362]

Neben diesen Übermittlungen aus dem Verbund kann auch das Bundeskriminalamt, das vom Verbund getrennte Datenbestände unterhält, an andere Polizeien Daten übermitteln. Neben der grundsätzlichen Übermittlungsbefugnis in § 25 Abs. 1 BKAG enthält § 25 Abs. 7 zudem ebenfalls die Möglichkeit, ein automatisiertes Abrufverfahren für die Datenbestände in eigenen Informationssystemen, also insbesondere Zentraldateien, einzurichten. Der Kreis der abrufberechtigten Behörden ist beschränkt auf die Behörden, die vollzugspolizeiliche Aufgaben wahrnehmen.[1363]

Normen, die den Datenaustausch zwischen Polizeibehörden unterschiedlicher Bundesländer bzw. den beiden föderalen Ebenen ermöglichen,

1359 Es wird für INPOL-Teilnehmer grundsätzlich angenommen, dass sie aufgrund der Vielzahl der Datenübermittlungen und der Eilbedürftigkeit regelmäßig die Berechtigung zum Abruf im automatisierten Verfahren haben, BT-Drs. 13/1550 S. 28.

1360 *Graulich* in *Schenke/Graulich/Ruthig,* Sicherheitsrecht, § 29 BKAG Rn. 23.

1361 Siehe dazu bereits oben S. 232 ff.

1362 *Barczak* in *Barczak* (Hrsg.), BKAG, § 29 Rn. 22.

1363 *Graulich* in *Schenke/Graulich/Ruthig,* Sicherheitsrecht, § 25 BKAG Rn. 37.

also die andere „Tür" in der Doppeltür-Dogmatik darstellen,[1364] finden sich in allen Polizeigesetzen.[1365] Der Datenaustausch zwischen diesen unterschiedlichen Polizeien ist dabei indes nicht so unproblematisch, wie man es angesichts der scheinbar übereinstimmenden Zwecke der Behörden annehmen könnte: Bundesebene, insbesondere das Bundeskriminalamt, und Landesebene haben unterschiedliche Aufgaben und auch unter den Bundesländern ist die Reichweite der polizeilichen Aufgabenkreise mitunter nicht identisch.[1366] Zudem ist seit dem BKAG-Urteil des Bundesverfassungsgerichts jede Übermittlung von Daten aus eingriffsintensiven Erhebungsmaßnahmen an andere Sicherheitsbehörden regelmäßig als Zweckänderung anzusehen.[1367] Sollen solche Daten zu einem anderen Zweck verarbeitet werden, so muss dies zumindest dem Schutz von Rechtsgütern oder der Aufdeckung von Straftaten eines solchen Gewichts dienen, die verfassungsrechtlich eine Neuerhebung mit vergleichbar schwerwiegenden Mitteln gerechtfertigt hätte.[1368] Auch unionsrechtlich verlangt der Übermittlungsvorgang mit Blick auf Art. 4 Abs. 2 JI-Richtlinie die Beachtung besonderer Anforderungen.

Insoweit ist – auch wenn sie prinzipiell den Logiken und Dynamiken des Massendatenparadigmas entspricht – die Einrichtung von automatisierten Abrufverfahren, wie es die Regel im polizeilichen Informationswesen ist, stets auch kritisch zu hinterfragen. Polizeiliche Interessen an einem solchen ubiquitären Zugriff auf die verschiedenen Datenbestände können nur dann die Betroffeneninteressen überwiegen, wenn gewichtige Vorteile durch die Automatisierung bestehen, etwa weil besonders schnell oder besonders große Mengen Daten benötigt werden.[1369] Zudem müssen in entsprechender Anwendung des § 81 Abs. 2 BKAG der Zeitpunkt, die Angaben, die die Feststellung der aufgerufenen Datensätze ermöglichen, sowie die für den Zugriff verantwortliche Stelle vom Bundeskriminalamt protokolliert werden.[1370] Im Zusammenhang mit automatisierten Abrufsystemen ist eine Protokollierung seitens der übermittelnden Stelle geboten, die Verarbeitungskategorie, Anlass, Inhalt, Empfänger und Datum der Übermittlung

1364 Siehe dazu bereits oben S. 170 ff.
1365 *Petri* in *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch, G. Rn. 950.
1366 *Petri* in *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch, G. Rn. 951.
1367 BVerfGE 141, 220, 336 f. – Bundeskriminalamtgesetz.
1368 BVerfGE 141, 220, 328 – Bundeskriminalamtgesetz.
1369 *Graulich* in *Schenke/Graulich/Ruthig,* Sicherheitsrecht, § 25 BKAG Rn. 42.
1370 *Graulich* in *Schenke/Graulich/Ruthig,* Sicherheitsrecht § 25 BKAG Rn. 43.

erfasst.[1371] Zudem ist aufseiten der empfangenden Stelle eine Vollprotokollierung geboten, da die zugreifende Stelle voll verantwortlich für die Rechtmäßigkeit des Datenabrufs ist.[1372] Nur eine solch umfassende Protokollierung, die auch den zugreifenden Rechner erfassen sollte,[1373] ermöglicht eine nachträgliche Feststellung möglicher Rechtsverstöße, etwa in Form von Abrufen durch Polizeibedienstete ohne entsprechende dienstliche Berechtigung, wobei es sich um eine Straftat handeln kann.[1374]

2. Polizeiliche Datenverarbeitung in den polizeibehördeneigenen Informationssystemen

Neben der Datenverarbeitung im Informationsverbund findet ein weiterer großer Teil des Informationsumgangs in den polizeibehördeneigenen Informationssystemen statt. Dabei lässt sich zunächst – wie bei Datenerhebungen – zwischen strafverfahrensrechtlicher und polizeirechtlicher Datenverarbeitung unterscheiden. Dementsprechend können für alle Polizeibehörden – je nach konkreter Aufgabengestaltung einzelner Organisationsteile – sowohl das jeweilige Polizeigesetz als auch die Strafprozessordnung bei ihrer informationellen Arbeit zu beachten sein. Insofern besteht eine gewisse Parallelität zwischen den Gesetzesmaterien, wobei dennoch auch weiter Diskrepanzen zwischen den einzelnen Rechtsordnungen existieren, sowohl im Verhältnis zwischen repressiver Strafprozessordnung und den präventiven Polizeirechtsordnungen als auch im Verhältnis der Polizeirechtsordnungen untereinander. In der Folge beschränken sich die Ausführungen auf die grundsätzlichen Strukturen der behördeneigenen Datenverarbeitung im polizeilichen Informationswesen.[1375]

Einmal in den behördenspezifischen Bereich des polizeilichen Informationswesens gelangt – im Wege der Datenerhebung oder Übermittlung durch staatliche oder auch nicht-staatliche Stellen – bedarf es spezifischer Rechtgrundlagen, um den daran anschließenden Umgang mit Daten zu erlauben. Dafür ist nunmehr das unionsrechtliche Konzept der Weiterverarbeitung

1371 *Müller/Schwabenbauer* in *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch des Polizeirechts, G. Rn. 883.
1372 *Graulich* in *Schenke/Graulich/Ruthig,* Sicherheitsrecht, § 25 BKAG Rn. 47.
1373 *Graulich* in *Schenke/Graulich/Ruthig,* Sicherheitsrecht, § 25 BKAG Rn. 47.
1374 Siehe dazu etwa *Golla* Legal Tribune Online v. 16.08.2019.
1375 *Müller/Schwabenbauer* in *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch des Polizeirechts, G. Rn. 577.

maßgeblich. Wenn einige Polizeigesetze noch mit der alten Terminologie von Datenspeicherung, Datenveränderung, Datenberichtigung, Datennutzung und so weiter operieren, so sind darin Teilaspekte des weiten Weiterverarbeitungsbegriffes zu sehen. Mit diesem Begriff sollen dann, wie Art. 3 JI-Richtlinie und die nationalen Umsetzungsnormen zeigen, zunächst einmal alle denkbaren Datenverarbeitungsprozessschritte erfasst sein.[1376] Da sich für bestimmte Datenumgänge spezielle verfassungsrechtliche Anforderungen ergeben, sind diese durch die jeweiligen Gesetzgeber im Bundes- oder Landesrecht spezifisch zu regeln. Dazu gehören die Datenübermittlung, der Datenabgleich und neuere Formen der Datenanalyse.[1377] Zudem sind Datenumgänge, die den mit der Informationsverarbeitung verbundenen Grundrechtseingriff abschwächen oder aufheben, sowie die Einschränkung der Verarbeitung oder die Löschung separat geregelt.

a) Datenverarbeitungsgeneralklausel

Zentral für den Datenumgang nach Datenerhebung durch oder -übermittlung an die Polizeien sind Datenverarbeitungsgeneralklauseln, die wahlweise mit den alten, aufgegliederten Begrifflichkeiten oder der neuen Weiterverarbeitungsterminologie arbeiten. Entsprechende Vorschriften finden sich sowohl in den Polizeirechtsordnungen als auch in der Strafprozessordnung.

Im Polizeirecht[1378] wird die generelle Befugnis zur Datenverarbeitung regelmäßig an die Erforderlichkeit der Verarbeitung zur Aufgabenerfüllung, den Zweckbindungsgrundsatz sowie die Rechtmäßigkeit der Erhebung geknüpft. Während es sich beim Rechtmäßigkeitserfordernis noch um die beharrlichste Verarbeitungsschranke handelt, findet eine Begrenzung des Datenumgangs durch Erforderlichkeit und Zweckbindung nur oberflächlich statt. Der Erforderlichkeitsgrundsatz stellt im Rahmen der Generalklauseln zunächst sicher, dass Daten nicht anlasslos und zeitlich unbegrenzt gespeichert oder sonst wie verarbeitet werden können. Im konkreten Da-

1376 Siehe zu den einzelnen Bedeutungen der Unterbegriffe *Müller/Schwabenbauer* in *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch des Polizeirechts, G. Rn. 594.

1377 Siehe dazu bereits oben S. 281 ff.

1378 Vgl. § 16 BKAG; § 29 BPolG; § 15 BWPolG; Art. 53 BayPAG; § 42 ASOG Bln; § 39. BbgPolG; § 36a BremPolG; § 36 HmbPolDVG; § 20 HSOG; § 36 SOG M-V; § 38 NPOG; § 23 PolG NRW; § 52 RP POG, § 21 SPolDVG; § 22 SOG LSA; § 80 SächsVDG; § 188 SchlHLVwG; § 40 TPAG.

tenumgang bedeutet Erforderlichkeit hingegen keine hohe Hürde, sondern verlangt zunächst nur, dass ein Bedarf an der Verarbeitung bestimmter Daten zur Erfüllung der Aufgaben besteht. Die Breite der Aufgaben macht aber eine weitere Limitierung durch den Zweckbindungsgrundsatz erforderlich. Auch dieser ist einfachgesetzlich durchweg in den Polizeigesetzen normiert, dasselbe gilt aber auch für seine Durchbrechung in Form von Zweckänderungen oder von Ausnahmen vom Zweckbindungsgrundsatz.

Die wichtigste Ausnahme dürfte mittlerweile die sogenannte zweckwahrende Weiternutzung sein, die eine weitere Nutzung von Daten im Rahmen derselben Aufgabe und zum Schutz vergleichbarer Rechtsgüter ohne weitere Anforderungen an den Eingriffsanlass gestattet. Die darin liegende schlichte Übernahme der verfassungsrechtlichen Vorgaben ist jedoch aus verschiedenen Gründen problematisch. So ist etwa nicht klar, wie weit eine weitere Nutzung reichen soll. Während Anschlussverfahren gefahrenabwehr- oder strafverfahrensrechtlicher Art dem wohl unterfallen, wäre eine längerfristige Bevorratung im Rahmen einer Aufgabe nicht auf die die Datenverarbeitungsgeneralklausel zu stützen, sondern bedarf spezifische Regelungen, die dem Eingriffsgewicht von Datenbevorratung Rechnung tragen.[1379] Diese Situation kann durch sehr weite Aufgabenbeschreibungen verschärft werden. So haben etwa Bundeskriminalamt und Bundespolizei vergleichsweise enge Aufgabenbeschreibungen, die allerdings durch gesetzgeberische Interpretation aufgeweicht werden können. So will der Gesetzgeber bei der Novellierung des BPolG unter den Aufgaben der Bundespolizei die Gefahrenabwehr und die Strafverfolgung verstanden wissen und nicht die Einzelaufgaben der Bundespolizei, wie beispielsweise Grenzschutz, Sicherheit von bestimmten Verkehrsanlagen usw.[1380] Auf diese Weise interpretiert franst die ohnehin schon durch die Figur der zweckwahrenden Weiternutzung aufgeweichte Zweckbindung im polizeilichen Datenumgang weiter aus.[1381] Ein solch weites Verständnis der Aufgabenbereiche ist jedoch sogar explizit gesetzlich verankert, wenn die zweckwahrende Weiternutzung als grundsätzliches Prinzip der Verarbeitung in allgemeine

1379 *Bäcker*, A-Drs. 18(4)806 D, S. 3 ff.

1380 *Bundesministeriums des Innern und für Heimat*, Gesetzesentwurf zur Neustrukturierung des Bundespolizeigesetzes und Änderung anderer Gesetze (Referentenentwurf), S. 125, abrufbar unter https://www.bmi.bund.de/SharedDocs/gesetzgebungsverfahren/DE/Downloads/referentenentwuerfe/B1/ref-neustrukturierung-bundespolizeigesetz.pdf?__blob=publicationFile&v=5 (Stand: 01.10.2023).

1381 Kritisch und instruktiv dazu bereits *Arzt*, A-Drs. 19(4)772 B, S. 15 f.

Polizeirechtsordnung aufgenommen wird.[1382] Denn hier ist der Verweis auf die Aufgaben dann tatsächlich im Sinne des maximal weiten Verständnisses von präventiver und repressiver polizeilichem Tätigwerden samt den jeweiligen Vorfeldaufgaben zu lesen. Damit wirkt dann lediglich das Erfordernis der Rechtsgutsidentität, wie es die zweite Voraussetzung der zweckwahrenden Weiternutzung ist, einschränkend.[1383] Insofern ist unterhalb der Zweckänderungsschwelle ein Freiraum für Datenverarbeitungen geschaffen worden, von dem zwar fraglich ist, wie er konkret polizeipraktisch genutzt werden wird. Eine Steuerung des polizeilichen Datenumgangs wird er jedoch nicht mit sich bringen.

Das ist umso bedenklicher, als dass auch die im Rahmen der Zweckänderung zu beachtenden Erfordernisse nur sehr eingeschränkt die ihnen zugedachte Einhegung der polizeilichen Datenverarbeitung bewirken können. Denn die Zweckänderung wird in allen Polizeigesetzen nach dem Grundsatz der hypothetischen Datenneuerhebung gestattet, sodass die Polizeien präventiv erlangte Daten zu anderen Gefahrenabwehrzwecken nutzen können, soweit sie diese Daten auch zu diesen Zwecken hätten erheben können. Hinzukommt, dass auch strafverfahrensrechtlich erlangte Daten regelmäßig zweckändernd für präventiv-polizeiliche Zwecke umgewidmet werden können, was § 481 Abs. 1 StPO von bundesrechtlicher Seite aus möglich macht. Auch umgekehrt können gem. § 161 Abs. 3 StPO Daten ins Strafverfahren überführt werden. Eine etwas höhere Hürde besteht lediglich bei eingriffsintensiven Maßnahmen, wo neben Rechtsgutsidentität zwischen altem und neuem Zweck nunmehr auch ein konkreter Ermittlungsanlass erforderlich ist.[1384] Zwar sind diese Öffnungsvorschriften zur Vornahme von zweckändernden Datenverarbeitungen größtenteils keinen erheblichen rechtstechnischen Einwänden ausgesetzt, aber die recht breite einfachgesetzliche Freigabe der zweckändernden Datenverarbeitung lässt von der Zweckbindung, die als Prinzip einen Regelcharakter haben sollte, schon einfachgesetzlich wenig übrig. Es ist deshalb durchaus treffend, wenn *Petri* anlässlich dieser Regelungslage urteilt, der Zweckbindungsgrundsatz werde gesetzlich lediglich „vorgetäuscht".[1385]

1382 Siehe etwa § 20 HSOG.
1383 Siehe dazu *Graulich* in *Schenke/Graulich/Ruthig,* Sicherheitsrecht, § 12 BKAG Rn. 10.
1384 Siehe dazu bereits S. 168 ff.
1385 *Petri* in *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch, G. Rn. 855.

Neben diesen strukturellen Problemen der polizeirechtlichen Datenverarbeitungsgeneralklauseln zeichnet sich zudem die problematische Entwicklung zumindest für manche Polizeigesetze ab, unreflektiert die unionsrechtliche Terminologie der Weiterverarbeitung zu übernehmen. Die schlichte Übernahme einer Begriffsbestimmung in eine Rechtsgrundlage ist jedoch – worauf *Arzt* richtigerweise hingewiesen hat – mit den verfassungsrechtlichen Vorgaben von Normenbestimmtheit und -klarheit nicht vereinbar, da durch die Verwendung der Weiterverarbeitungsterminologie nicht klar ist, welche Datenverarbeitungsschritte genau zulässig sind.[1386]

Auch für den kriminalpolizeilichen Datenumgang finden sich generalklauselartige Datenverarbeitungsvorschriften in den §§ 161 Abs. 3 und 4 sowie 483 StPO. Während § 483 StPO mit seiner Formulierung, auch für den strafprozessualen Teil der polizeilichen Datenverarbeitung, die Grundsätze der Erforderlichkeit und Zweckbindung aufstellt, findet sich in § 161 Abs. 3 und 4 StPO der Grundsatz der hypothetischen Datenneuerhebung, wenn auch nicht in der expliziten Form wie zunehmend im Polizeirecht. Die grundsätzliche Bindung der repressiv erlangten Daten ans Strafverfahren wird indessen durch § 481 StPO und daran anknüpfende polizeirechtliche Regelungen stark relativiert. Zudem verlangt der Grundsatz der hypothetischen Datenneuerhebung bei der zweckändernden Weiterverarbeitung nicht die Erfüllung der ursprünglichen, bei der Datenerhebung zu erfüllenden prozeduralen Sicherungen, wie beispielsweise einen Richter:innenvorbehalt, sodass eine externe Kontrolle insofern nicht erfolgt. Um dies zu kompensieren, wird eine strenge Erforderlichkeitsprüfung für die Weiterverarbeitung – auch für die Nutzung als sogenannter Spurenansatz – verlangt, um die Verhältnismäßigkeit im Einzelfall zu wahren.[1387] Damit bleibt es allerdings bei einer polizeilichen Definition von Erforderlichkeitsschwellen. Eine nähere Überprüfung wäre zwar über die Protokollierungen von Verarbeitungsschritten, wie etwa Datenabfragen, möglich, hängt aber in ihrer Effektivität stark vom generellen Stand insbesondere der innerbehördlichen Datenschutzkontrolle ab. Ob zudem auch rechtswidrig erlangte Daten strafprozessual (nach einer entsprechenden Verhältnismäßigkeitsprüfung) weiterverarbeitet werden können, ist nach wie vor umstritten.[1388]

1386 *Arzt*, A-Drs. 19(4)772 B, S. 14 f.

1387 Siehe dazu mwN *Müller/Schwabenbauer* in *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch des Polizeirechts, G. Rn. 828.

1388 Die Möglichkeit zur Verwendung zumindest bejahend als gegenwärtige Rechtslage beschreibend *Müller/Schwabenbauer* in *Bäcker/Denninger/Graulich* (Hrsg.),

Damit ergibt sich für den generellen Datenumgang rund um die vollzugspolizeilichen Vorgangsbearbeitungssysteme und die kriminalpolizeilichen Fallbearbeitungssysteme ein Bild wenig beschränkter Datenverarbeitungsmöglichkeiten. Ausnahmen betreffen vor allem Daten aus eingriffsintensiven Maßnahmen, die tief in die Privatsphäre von Betroffenen eingreifen. Darüber hinaus ist – der hierarchischen und spezialisierten Struktur der Polizei entsprechend – der Datenzugang nicht für alle Polizeibediensteten derselbe. Der Streifenpolizist hat weniger Zugriff und damit auch weniger Datenverarbeitungsmöglichkeiten als die Staatsschützerin. Im Rahmen der Verfügbarkeiten erlauben die gegenwärtigen Vorschriften aber einen grundsätzlich flexiblen Datenumgang, wie es zwar auch in Grundzügen für eine „moderne" Polizei in einer sich selbst zunehmend datafizierenden Gesellschaft sinnvoll erscheint, was jedoch an den beschriebenen verfassungsrechtlichen und rechtsstaatlichen Defiziten des polizeilichen Informationswesens nichts ändert.

b) Datenverarbeitung zum Zweck der Bevorratung strafprozessualer Daten

Ein im vorliegenden Kontext ebenfalls noch relevante Form des Datenumgangs ist die Bevorratung von strafverfahrensrechtlich erlangten Daten zu präventiv-polizeilichen Zwecken, also zur Bevorratung – insbesondere zur vorbeugenden Straftatenbekämpfung – wie sie bereits in den Ausführungen zum KAN als strukturellem Bestandteil des polizeilichen Informationswesens zur Sprache gekommen ist.[1389] Die Möglichkeit hierzu wird über den soeben bereits erwähnten § 481 Abs. 1 S. 1 StPO eröffnet, die von allen Polizeirechtsordnungen durch eine entsprechend spiegelnde Vorschrift genutzt wird. Datenverarbeitungen zur vorbeugenden Bekämpfung von Straftaten setzen voraus, dass wegen der Art, Ausführung oder Schwere der Tat und der Persönlichkeit des Betroffenen die Besorgnis der Begehung weiterer Straftaten besteht. Sie beziehen sich also auf Wiederholungstäter:innen. Neben dieser spezifischen Ausprägung des Verhältnismäßigkeitsgrundsatzes verbietet dieser zudem, die erstmalige Begehung von Bagatelldelikten zum Anlass für eine Bevorratung zu nehmen. Ferner ist bei jeder Speicherung

---

Handbuch des Polizeirechts, G. Rn. 830; explizit dagegen etwa *Singelnstein* in *Knauer/Hartmut Schneider* (Hrsg.), Münchener Kommentar zur Strafprozessordnung Bd. 3: §§ 333-500 StPO, § 483 Rn. 7.

1389 Siehe dazu bereits oben S. 240 ff.

zu prüfen, ob diese mit Blick auf das Ziel der Strafverfolgungsverhütung überhaupt im Einzelfall zweckmäßig ist.[1390] Auch hier ist den speichernden Beamt:innen ein nicht unerheblicher Ermessensspielraum zugeteilt. Selbst bei Freispruch oder Einstellung des Ermittlungsverfahrens nach § 170 Abs. 2 StPO können Daten im Rahmen der Bevorratung ausnahmsweise weiterverarbeitet werden, wenn es Verdachtsmomente und eine Wiederholungsgefahr gibt,[1391] wobei dies konkret geprüft und dargelegt werden muss.[1392] In diesen Kontext fällt auch das Problem der Mitteilung vonseiten der Staatsanwaltschaften an die Polizeibehörden.[1393] Eine vergleichbare Abwägungssituation besteht auch im Rahmen der Einstellung nach § 153 oder § 153a StPO, wo die Geringfügigkeit der Schuld eine Speicherung trotz bestehenden Restverdachts nicht ohne Weiteres erlauben kann. Während bei Ersttäter:innen im Falle von Bagatellkriminalität auch hier meistens eine Bevorratung nicht angemessen sein wird, kann es etwa anders aussehen, wenn eine Person bereits einige Male nachweislich straffällig geworden ist und die Daten aus dem einzustellenden Verfahren „das Gefährderprofil des Beschuldigten" abrunden können.[1394] Auch hier lassen sich wieder einige Unschärfen in den Beurteilungsmöglichkeiten erkennen, die zumindest in der Vergangenheit zu einer extensiven Anwendung der Bevorratungsermächtigungen geführt haben.[1395] Um die Ermessensausübung pragmatisch zu vereinfachen verzichten einige Polizeigesetze auf entsprechende Beurteilungsspielräume wie die Wiederholungsgefahr und setzen Speicherhöchstfristen ein, innerhalb derer sich wohl klären soll, ob es sich um Täter:innen handelt, die erneut straffällig werden.[1396] Damit wird zwar eine

1390 *Müller/Schwabenbauer* in *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch des Polizeirechts, G. Rn. 840.

1391 BVerfG, 16.05.2002 - 1 BvR 2257/01 = NJW 2002, 3231.

1392 VGH Hessen, 01.02.2017 - 8 A 2105/14.Z = NVwZ 2017, 982.

1393 Siehe dazu bereits oben S. 243 f.

1394 *Petri* in *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch, G. Rn. 877.

1395 So berichtet es etwa *Petri* in *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch, G. Rn. 880; s. auch BayLfD 24. Tätigkeitsbericht, 2010, 3.5.3.

1396 Sieh etwa § 75 Abs. 3 BWPolG wonach eine „Speicherung personenbezogener Daten bis zu einer Dauer von zwei Jahren [erforderlich ist], wenn aufgrund tatsächlicher Anhaltspunkte der Verdacht besteht, dass die betroffene Person eine Straftat begangen hat", es sei denn es die betroffene Person im Strafverfahren rechtskräftig freigesprochen, die Eröffnung des Hauptverfahrens gegen sie unanfechtbar abgelehnt oder das Verfahren nicht nur vorläufig eingestellt wurde und sich aus den Gründen der Entscheidung ergibt, dass die betroffene Person die Straftaten nicht oder nicht rechtswidrig begangen hat. Ähnlich ermöglicht § 37 Abs. 2 S. 1 SOG M-V, dass eine Speicherung zunächst für drei Jahre erfolgen darf, wenn

etwas unsichere Verwaltungspraxis vereinheitlicht, gleichzeitig bewirken solche Bevorratungsvorgaben aber selbstverständlich eine Ausweitung der gespeicherten Personen und Daten, da hierdurch die Möglichkeit, trotz Strafverfahrens nicht zu speichern, quasi aufgehoben wird.

c) Datenübermittlung

Aufgrund der föderalen und auch sonst nochmals zergliederten Struktur der deutschen Polizeien ist das polizeiliche Informationswesen für seine Funktionsfähigkeit in einem hohen Maße auf Datenübermittlungen[1397] angewiesen. Grundsätzlich müssen Übermittlungsrechtsgrundlagen – wie alle Datenverarbeitungsschritte – dem Grundsatz der Zweckbindung Rechnung tragen, auch ansonsten die Verhältnismäßigkeit wahren und besonders sensible Daten schützen. Obwohl in der Übertragung bereits eine Zweckänderung liegt,[1398] erfordert der Zweckbindungsgrundsatz, dass die empfangende Stelle an den ursprünglichen Zweck gebunden ist. Hiervon machen die Polizeigesetze allerdings, wie im Rahmen der generalklauselartigen Datenverarbeitungsermächtigungen, weitreichende Ausnahmen, sodass die empfangende Stelle die erhaltenen Daten regelmäßig zweckändernd weiterverarbeiten kann, soweit diese Daten auch zu diesem Zweck hätten übermittelt werden dürfen. Mit dieser „hypothetischen Datenneuerhebung" soll ein erneuter Übermittlungsvorgang an die Stelle, die die Daten ohnehin bereits besitzt, überflüssig gemacht werden.[1399] Übermittlungsvorschriften zwischen den Polizeibehörden und zwischen der Strafjustiz und den Polizeien ermöglichen dementsprechend einen flexiblen Datenaustausch zu präventiv-polizeilichen und repressiv-polizeilichen Zwecken sowie zwischen beiden Zweckdomänen.[1400]

---

zum Speicherungszeitpunkt der Verfahrensausgang nicht bekannt ist. Auch in diese Richtung erlaubt § 20 Abs. 6 S. 2 HSOG bei Tatverdächtigen die Speicherung solange, wie der Tatverdacht nicht ausgeräumt worden ist, was – mit Blick auf Einstellungen etwa nach §§ 153, 153a aber auch § 170 Abs. 2 StPO regelmäßig zur Bevorratung von Daten führen kann.

1397 Siehe zu den verfassungsrechtlichen Anforderungen bereits oben S. 170 f. ff. sowie zum Begriff S. 205 ff.

1398 BVerfGE 141, 220 (341) – BKAG-Urteil.

1399 *Müller/Schwabenbauer* in *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch des Polizeirechts, G. Rn. 871.

1400 § 482 Abs. 1 S. 2 StPO; § 25 Abs. 1 BKAG, § 32 Abs. 1 BPolG; Länder: § 59 BW PolG; Art. 56 Abs. 1 Nr. 1 BayPAG; § 44 Abs. 1 ASOG; § 42 Abs. 1 BbgPolG; § 36c ff.

Ein Großteil der für die polizeiliche Informationsarbeit erforderlichen Datenübermittlungen erfolgt dabei wie bereits dargelegt innerhalb des Informationsverbundes nach § 29 BKAG im automatisierten Abrufverfahren. Dabei ist eine Überprüfung und Steuerung der Datenverwendung durch die übermittelnde Stelle nicht möglich.[1401] Der Bedeutung dieser Form der Teilnahme entsprechend finden sich entsprechende Rechtsgrundlagen sowohl in der Strafprozessordnung als auch in allen Polizeigesetzen des Bundes und der Länder.[1402] Aufgrund der fehlenden rechtlichen Prüfung, die bei einer „händischen" Übermittlung zumindest ansatzweise noch von der übermittelnden Stelle zu leisten wäre, ist die Rechtmäßigkeit zunächst maßgeblich vom Abrufverhalten abhängig, das in der Vergangenheit durch Missachtung der Abrufrahmenbedingungen aufgefallen ist.[1403] Da indessen eher zu erwarten ist, dass automatisierte Abrufverfahren noch größere Bedeutung für die Polizeien im Angesicht des Massendatenphänomens erlangen werden, muss vor allem eine lückenlose Protokollierung der massenhaften Eingaben und Abrufe erfolgen wie etwa in § 81 BKAG für den Informationsverbund vorgeschrieben ist. Sodann kann über das interne Datenschutzkontrollregime und gegebenenfalls die Aufsichtsbehörden eine Identifizierung und Korrektur von unrechtmäßigen Datenübermittlungen erfolgen.

d) Datenabgleich

Zunehmende Bedeutung in einem immer weiter digitalisierten Informationswesen gewinnt zudem das Instrument des Datenabgleichs, der in al-

---

BremPolG; § 40 HmbPolDVG; § 22 Abs. 1 HSOG; § 39b Abs. 1 SOG M-V; § 41 NPOG; § 27 Abs. 1 PolG NRW; § 57 Abs. 1 RH POG; § 84 SächsPVDG; § 27 Abs. 1 SOG LSA; § 192 Abs. 1 SH LVwG; § 41 Abs. 1 TPAG.

1401 Siehe dazu bereits oben S. 341 f.

1402 § 488 StPO; § 29 BKAG; § 33 Abs. 7 und 8 BPolG; § 22 AZRG; §§ 30a, 30b StVG; Länder: § 59 Abs. 5 BWPolG; Art. 63 BayPAG; § 46 ASOG Bln; § 49 BbgPolG; § 36c BremPolG; § 62 HmbPolDVG; § 24 HSOG; § 42 SOG M-V; § 42 NPOG; § 70 Abs. 2 DSG NRW iVm § 6 Abs. 1 DSG NRW; § 64 RH POG; § 46 SPolDVG; § 7 DSG LSA, § 85 SächsPVDG; § 194 SH LVwG; § 42 ThürPAG.

1403 *92. Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder*, Gemeinsame Prüfung der Falldatei Rauschgift deckt gravierende Mängel auf - Konsequenzen für polizeiliche Datenverarbeitung notwendig, 2016.

len einschlägigen Rechtsordnungen eine Rechtsgrundlage findet.[1404] Beim Datenabgleich werden die der Polizei bekannt gewordenen Daten einer Person – etwa im Rahmen einer polizeilichen Kontrolle – verwendet, um zu überprüfen, ob in den polizeiinternen Datenbeständen bereits (weitere) Daten zu ihr vorliegen. Abzugrenzen ist die Maßnahme insofern von der Rasterfahndung, die polizeiexterne Datenbestände zum Abgleich heranzieht. Der Datenabgleich gilt häufig als wenig intensives informationelles Instrument.[1405] Dem ist zu widersprechen. Der Datenabgleich gestattet – je nach Ausgestaltung – die Nutzbarmachung eines nicht unerheblichen Teils der polizeilichen Datenbestände im konkreten Bürger:innenkontakt und mobilisiert gerade durch die Überprüfung, ob oder was an Daten bereits zu einer Person vorhanden ist, einen wesentlichen Aspekt der informationellen Macht polizeilicher Datenbestände. Zwar werden strenggenommen keine neuen Daten erhoben, aber für die Polizeibediensteten in der konkreten Situation ist der Datenabgleich ein Erkenntnisinstrument, das anderswo vorhandene Daten für die aktuelle lebensweltliche Situation verfügbar macht und zu ihrer informationellen Neubewertung mit potenziell nachteiligen Folgen in Form von Folgemaßnahmen für Betroffene führen kann.[1406] Dabei ist die Datengrundlage, insbesondere im Bereich von insoweit besonders problematischen Dateien, wie den Gewalttäterdateien, häufig nicht verlässlich.[1407] Zudem ist die handlungsleitende Verwendung von eventuell im Informationswesen vorhandenen, auf Datenverknüpfungen beruhenden Datendoubles gerade konträr zur Prinzip der informationellen Selbstbestimmung im zwischenmenschlichen Kontakt.[1408]

1404 § 98c StPO; § 16 Abs. 4 BKAG; § 34 Abs. 1 BPolG; Länder: § 47 BWPolG; Art. 61 BayPAG; § 28 ASOG; § 40 BbgPolG; § 36h BremPolG; § 48 HmbPolDVG; § 25 HSOG; § 43 SOG M-V; § 45 Abs. 1 NPOG; § 25 PolG NRW; § 65 RH POG; § 28 SPolDVG; § 30 SOG LSA; § 87 SächsPVDG; § 195 SH LVwG; § 43 TPAG.

1405 So etwa Schmidbauer in *W. Schmidbauer/Steiner,* Polizeiaufgabengesetz, Polizeiorganisationsgesetz, Art. 61 PAG Rn. 1; auch *Aulehner* in *Möstl/Schwabenbauer* (Hrsg.), Beck'scher Online-Kommentar Polizei- und Sicherheitsrecht Bayern, Art. 61 PAG Rn. 1; ebenso *Graulich* in *Schenke/Graulich/Ruthig,* Sicherheitsrecht, § 16 BKAG Rn. 36.

1406 Zu dieser Dynamik etwa im Kontext von Gewalttäterdateien siehe etwa *Ruch/Feltes* NK 17 (2016), 62 (77 f.).

1407 *Ruch/Feltes* NK 17 (2016), 62 (76 f.).

1408 So auch *Müller/Schwabenbauer* in *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch des Polizeirechts, G. Rn. 933; *Arzt* in *Möstl/Kugelmann* (Hrsg.), Beck'scher Online-Kommentar Polizei- und Ordnungsrecht Nordrhein-Westfalen, § 25 Rn. 6; *Bäuerle* in *Möstl/Bäuerle* (Hrsg.), Polizei- und Ordnungsrecht Hessen, § 25 Rn. 3a.

Die Ausgestaltung des Datenabgleichs ist in der Regel dreigeteilt: Möglich sind Fahndungsabfragen, der Datenabgleich bei Störer:innen und der Datenabgleich bei anderen Personen. Zumindest der Fahndungsabgleich ist nicht auf die Datenbestände der jeweiligen Polizeiorganisation (also etwa: Polizei eines bestimmten Landes) beschränkt, sondern gleicht mindestens Personen- und Sachfahndungsdateien,[1409] also Verbunddateien, ab. Der Fahndungsbegriff ist dabei nicht legaldefiniert, sondern wird im Wesentlichen nach Polizeidienstvorschrift bestimmt, wonach es sich um die „planmäßige, allgemeine oder gezielte Suche nach Personen oder Sachen unter anderem auch im Rahmen der Strafverfolgung" handelt. Insofern kann ein Abgleich mit dem Fahndungsbestand auch dahingehend verstanden werden, dass zusätzlich zu den eigentlichen Fahndungsdateien Datenbestände zur Strafverfolgungszwecken einbezogen werden können. Demgegenüber ist der Datenabgleich bei Störer:innen und auch bei Nichtverantwortlichen prinzipiell nicht beschränkt. Hier können also grundsätzlich alle einem Abgleich technisch offenstehenden Datenbestände abgefragt werden. Während manche Normen so formuliert sind, dass eine Begrenzung auf die Bestände der jeweiligen Polizeiorganisation, also etwa einer bestimmten Landespolizei oder Polizeibehörde, denkbar ist,[1410] beziehen andere Vorschriften, etwa § 25 HSOG, explizit Datenbestände der Bundes- und Länderpolizeien mit ein. Auf Grundlage solcher Normen kann also mit allen in den Informationssystemen verfügbaren Datenbeständen abgeglichen werden.[1411] Man spricht beim Fahndungsabgleich, da nur ein begrenzter Teil der polizeilichen Datenbestände abgefragt wird, vom einfachen und bei dem Abgleich mit dem nicht beschränkten Datenbestand vom erweiterten Datenabgleich.[1412]

Die Eingriffsschwellen für die verschiedenen Datenabgleichformen sind teilweise etwas unterschiedlich formuliert. Grundsätzlich besteht aber das folgende Schema: Der erweiterte Datenabgleich ist in der ersten Alternative lediglich von der gefahrenabwehrrechtlichen Verantwortlichkeit abhängig, ansonsten bestehen keine weiteren Schwellen (vgl. etwa § 25 Abs. 1 S. 1

1409 Siehe dazu bereits oben S. 238 ff.

1410 So etwa *Arzt* zur nordrhein-westfälischen Rechtsgrundlage und mWn in *Möstl/Kugelmann* (Hrsg.), Beck'scher Online-Kommentar Polizei- und Ordnungsrecht Nordrhein-Westfalen, § 25 Rn. 13 f.

1411 *Bäuerle* in *Möstl/Bäuerle* (Hrsg.), Polizei- und Ordnungsrecht Hessen, § 25 Rn. 12; vgl. auch *Graf* in *Möstl/Weiner* (Hrsg.), Beck'scher Online-Kommentar Polizei- und Ordnungsrecht Niedersachsen, § 45 Rn. 32.

1412 *Bäuerle* in *Möstl/Bäuerle* (Hrsg.), Polizei- und Ordnungsrecht Hessen, § 25 Rn. 16.

HSOG: „[…] können […] abgleichen."). In der zweiten Alternative richtet sich die Maßnahme gegen Nichtverantwortliche und ist nur erlaubt, wenn dies zur Aufgabenerfüllung erforderlich ist. Da es sich bei Abgleich um einen Grundrechtseingriff handelt, muss die Erforderlichkeitsvoraussetzung allerdings immer mindestens erfüllt sein, sodass sie dort hineinzulesen ist, wo der Abgleich gegen Verantwortliche ansonsten voraussetzungslos gestattet wird. Auch der Fahndungsabgleich ist bei Erforderlichkeit für die Aufgabenerfüllung gestattet. Höhere Eingriffsschwellen sind regelmäßig nicht vorgesehen. Praktisch bedeutet dies, dass ein Datenabgleich immer durchgeführt werden kann, solange sich ein, wenn auch nur schwacher, Bezug zur polizeilichen Aufgabenerfüllung herstellen lässt. Damit sind nur evident willkürliche Abgleiche verboten. Als „Auffangtatbestand" kann zudem regelmäßig die Eigensicherung herangezogen werden.[1413] Im Einsatz wird sich – zumindest unter gegenwärtigen Bedingungen – die Rechtmäßigkeit kaum überprüfen lassen. Zwar ist im Falle von Störer:innen eine konkrete Gefahr erforderlich. Da aber auch von Nichtverantwortlichen Daten im Grunde unter denselben Voraussetzungen – Erforderlichkeit zur Aufgabenerfüllung – abgeglichen werden dürfen, erübrigt sich diese Einschränkung. Hinzukommt, dass in einigen Informationssystemen eine reine Fahndungsabfrage überhaupt nicht möglich ist, sodass regelmäßig ein kompletter Datenabgleich mit den verfügbaren Datenbeständen durchgeführt werden wird,[1414] was aufgrund von Unverhältnismäßigkeit rechtswidrig ist.

Eine stärkere Einhegung des Datenabgleichs erfolgt auch nicht unter Zweckgesichtspunkten. Die Vorschriften verweisen nur auf die sehr breiten Aufgabenbereiche der Polizeien und stellen keine Zweckvorgaben dar.[1415] Zudem ist zu beachten, dass es bei Datenabgleichen häufig zu Zweckänderungen kommt: Die Datenbestände der Polizeien sind häufig Mischdateien gem. § 483 Abs. 1 S. 2 StPO, sodass dort sowohl repressiv als auch präventiv erhobene Daten enthalten sein werden. Im Rahmen eines Abgleichs etwa zur Eigensicherung würden dann mitabgeglichene strafverfahrensrechtliche Daten zweckändernd zur Gefahrenabwehr genutzt werden. Dies wird

1413 *Bäuerle* in *Möstl/Bäuerle* (Hrsg.), Polizei- und Ordnungsrecht Hessen, § 25 Rn. 13 f.

1414 *Bäuerle* in *Möstl/Bäuerle* (Hrsg.), Polizei- und Ordnungsrecht Hessen, § 25 Rn. 15.

1415 *Müller/Schwabenbauer in Bäcker/Denninger/Graulich* (Hrsg.), Handbuch des Polizeirechts, G. Rn. 934.

von den entsprechenden Vorschriften nicht kenntlich gemacht und insofern auch nicht mit eventuell erhöhten Voraussetzungen versehen.[1416]

Insgesamt weisen die Normen also mit Blick auf Anlass, Zweck und Umfang der einzubeziehenden Daten durchaus gravierende Bestimmtheitsdefizite auf.[1417] Es ist natürlich nicht von der Hand zu weisen, dass die Polizeien ihre Datenbestände auch nutzen können sollen und insbesondere in gefahrreichen Einsatzsituationen zu einer besseren Einschätzung und Reaktionsweise im Wege der informationellen Durchdringung ihres Gegenübers in der Lage sein sollen. Es scheint aber durchaus möglich insoweit zu einer befriedigenderen Regelungslage zu kommen. Denn die gegenwärtige Möglichkeit, in breitem Umfang und im Anlass wenig beschränkt personenbezogene Daten mit dem Datenbestand abzugleichen, wird mit einem zunehmenden Anwachsen des polizeilichen Informationswesens, wie es wohl bei der Zunahme der verfügbaren Daten zu erwarten ist, immer eingriffsintensiver. Durch ein Mehr an Daten zu einer Person oder mehr Personen, über die Daten in den Datenbeständen enthalten sind, nimmt die informationelle Durchschlagkraft des Datenabgleichs zu, da entweder detailliertere Datendoubles zur Verfügung stehen oder mehr Treffer, gleich welchen Inhalts, erzielt werden können.

Die Bedeutung des Datenabgleichs wird zudem durch neuere technologische Entwicklungen aufgewertet. So sieht etwa Art. 61 Abs. 2 BayPAG vor, dass ein Datenabgleich „auch unter Verwendung bildverarbeitender Systeme und durch Auswertung biometrischer Daten erfolgen" darf, „wenn andernfalls die Erfüllung polizeilicher Aufgaben gefährdet oder wesentlich erschwert würde". Damit ist insbesondere eine „Gesichtsfelderkennung[1418]", also eine automatisierte Erkennung biometrischer Merkmale gemeint. Die relativ erhöhte Erforderlichkeitsschwelle ist notwendig, da biometrische Daten zu den besonderen Kategorien personenbezogener Daten im Sinne von Art. 10 DRL-JI gehören. Zudem ist „stets" eine Datenschutzfolgenabschätzung gem. Art. 64 Abs. 2 S. 2 BayPAG vorzunehmen.[1419] Ob die Maßnahme nur stationär, in bestimmten Einsatzformen oder aber schon

1416 *Müller/Schwabenbauer in Bäcker/Denninger/Graulich* (Hrsg.), Handbuch des Polizeirechts, G. Rn. 941.

1417 So auch *Arzt* in *Möstl/Kugelmann* (Hrsg.), Beck'scher Online-Kommentar Polizei- und Ordnungsrecht Nordrhein-Westfalen, § 25 passim.

1418 Gemeint ist wohl die biometrische Gesichtserkennung, das Gesichtsfeld ist ein augenärztlicher Fachbegriff.

1419 *Schmidbauer* in *W. Schmidbauer/Steiner,* Polizeiaufgabengesetz, Polizeiorganisationsgesetz, Art. 61 Rn. 8 ff.

im einfachen Streifendienst zum Tragen kommen soll, ist nicht bekannt. Jedenfalls erhöht insbesondere die Datenschutzfolgeabschätzung, die immer durchzuführen ist, die Wissensanforderungen an Polizeibeamt:innen merklich, da es sich um ein technisch komplexes und in der rechtlichen Bewertung anspruchsvolles Verfahren handelt. Vor dem Hintergrund neuer technischer Möglichkeiten zur Durchführung komplexerer Datenabgleiche, für die die bayerische Regelung nur ein Beispiel und den Anfang darstellen dürfte, ist zudem die Charakterisierung dieser Datenverarbeitungsform als wenig invasiv unhaltbar geworden.[1420]

e) Massendatenverarbeitungen: Rasterfahndung und Datenanalyse

Neben diesen Datenverarbeitungsformen, die einigermaßen begrenzt Daten für die Verarbeitung erfassen, treten zudem zunehmend Massendatenverarbeitungsverfahren.

Die klassische Form dieser Massendatenverarbeitung ist die Rasterfahndung, die polizeifremde Datenbestände untereinander oder auch mit polizeilichen Datensammlungen abgleicht, um nach einem bestimmten positiven oder negativen Muster wenige Daten aus dem ursprünglichen Massendatensatz auszusieben. Dafür müssten die Daten erhoben, abgeglichen und gespeichert werden. Das Verfahren wird auf nicht-öffentliche Daten angewendet, die bei öffentlichen oder privaten Stellen vorliegen.[1421] Vor allem da eine Vielzahl an Personen betroffen ist und deren Daten kombinatorisch ausgewertet werden, gilt die Rasterfahndung als besonders eingriffsintensiv. Einerseits wird durch die Maßnahme der Zweckbindungsgrundsatz stark angetastet und andererseits bewegt sie sich je nach Umfang der einbezogenen Datenbestände in Richtung einer anlasslosen Vorratsdatenspeicherung.[1422] Deshalb besteht ein Richter:innenvorbehalt und ein eng umgrenzter Anwendungsbereich für die Rasterfahndung.

Neben dieser nach außen gerichteten Form der polizeilichen Massendatenverarbeitung gibt es aber auch zunehmend Möglichkeiten der internen Massendatenverarbeitung. Die bereits erläuterte – defizitär geregelte –

1420 *Golla* Kriminologisches Journal 52 (2020), 149 (158).

1421 *Müller/Schwabenbauer* in *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch des Polizeirechts, G. Rn. 947.

1422 *Müller/Schwabenbauer* in *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch des Polizeirechts, G. Rn. 953.

automatisierte Datenanalyse hat strukturelle Ähnlichkeiten zur Rasterfahndung. So hebt das Verfahren die Zweckbindung der polizeiintern vorhandenen Daten auf. Zudem kann man mit dem Anwachsen der Datenbasis, also der polizeilicher Datensammlungen, ebenfalls von einer Intensitätssteigerung der Maßnahme ausgehen, auch wenn damit vielleicht noch keine Nähe zur anlasslosen Vorratsdatenspeicherung begründet würde. Aber je mehr Daten das Informationswesen in miteinander verknüpfbarer Form und Struktur enthält – etwa: ein umfassender, barrierefreier Datenspeicher, in dem Daten prinzipiell miteinander kombinierbar, abgleichbar et cetera sind, wie im Zuge von Polizei 2020 geplant – desto mehr kann die Polizei auch ihre eigenen Daten „rastern" und mit anderen erkenntnisgewinnbringenden Verarbeitungsverfahren auswerten, sodass sich tiefgehendere Erkenntnisse daraus ergeben. Aufgrund der strukturellen Ähnlichkeiten von Massendatenverarbeitungsverfahren ließe sich zumindest darüber nachdenken, ob eventuell ein verfassungsrechtlicher Richter:innenvorbehalt für diese invasiven Informationseingriffe besteht.[1423] Es ist zu erwarten, dass sich derartige Verfahren zukünftig noch stärker ausdifferenzieren und insgesamt weiterentwickeln werden, was bereits jetzt neue Herausforderungen für das Recht der polizeilichen Informationsverarbeitung mit sich bringt.[1424]

f) Verarbeitungen mit dem Zweck des Schutzes der informationellen Selbstbestimmung

Abgesehen von Datenverarbeitungsformen, die in das Recht auf informationelle Selbstbestimmung eingreifen, gibt es auch Verarbeitungspflichten der Polizei, die gerade der Gewährleistung, dem Schutz oder der Wiederherstellung der informationellen Selbstbestimmung dienen.[1425] Dabei handelt es sich um die Berichtigung, Löschung oder Einschränkung der Verarbeitung von Daten. Aus dem Datenschutzrecht folgt zunächst, dass nur valide Daten verarbeitet werden dürfen, sodass bei entsprechend festgestellter Un-

1423 Siehe dazu *Müller/Schwabenbauer* in *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch des Polizeirechts, G. Rn. 962, im Kontext der Rasterfahndung.

1424 Siehe dazu bereits die Ausführungen zur Regelung der automatisierten Datenanalyse oben S. 281 ff.

1425 Siehe dazu etwa *Ruthig* in *Schenke/Graulich/Ruthig,* Sicherheitsrecht, § 77 BKAG Rn. 3 ff; *Ogorek* in *Möstl/Kugelmann* (Hrsg.), Beck'scher Online-Kommentar Polizei- und Ordnungsrecht Nordrhein-Westfalen, § 32.

richtigkeit eine Berichtigung erfolgen muss. Eine Löschung hat zu erfolgen, wenn dies eine gesetzliche Bestimmung vorschreibt, die Speicherung unzulässig (geworden) ist oder die Daten nicht mehr zur Aufgabenerfüllung erforderlich sind. Eine Einschränkung der Verarbeitung hingegen muss erfolgen, wenn eine Löschung – etwa, weil sie schutzwürdige Belange Betroffener beeinträchtigen würde oder noch für datenschutzrechtliche Überprüfungen erforderlich sind – nicht interessengerecht wäre. Der Umgang mit diesen Verpflichtungen ist von nicht zu unterschätzender Bedeutung für das Informationswesen in seiner Gänze, da etwa massenhaft falsche Daten oder entgegen entsprechenden Verpflichtungen nicht gelöschte Daten zu problematischen Zuständen führen können. Es ist also vor allem eine systematische Einhaltung der Verpflichtungen geboten.

IV. Fazit zu den rechtlichen Rahmenbedingungen des polizeilichen Informationswesens

Bis hierhin erfolgte die rechtliche Betrachtung der informationstechnologischen Infrastruktur und dem in ihr praktiziertem Informationshandeln fragmentarisch. Fügt man die einzelnen Detailbetrachtung zu einem mosaikhaften Ganzen zusammen, so zeichnet sich keine makellose normative Architektur zur Regulierung des polizeilichen Informationswesens ab. Vielmehr wird deutlich, dass die informationstechnologische Infrastruktur nur punktuell und zumeist unzureichend durch das Recht strukturiert wird und polizeiliche Informationspraktiken nur unzureichend normativ eingehegt werden. Vielfach sind Regelungen an entscheidenden Stellen vage und räumen der Polizei in der Bestimmung der zu speichernden Daten und Personen sowie im weiteren Umgang mit diesen Informationen einen erheblichen exekutiven Spielraum und eine große Definitionsmacht ein. Die Datenverarbeitung ist recht weitgehend zur Aufgabenerfüllung freigegeben, materiell-rechtliche Beschränkungen wirken hierbei kaum begrenzend. Limitationen sind eher prozeduraler Natur. Sie werden am meisten noch durch Rechte- und Rollenkonzepte – also: funktionsbezogene Zugriffsrechte auf bestimmte Daten oder eben nicht – als Ausgestaltung des Postulats der technisch-organisatorischen Datenschutzmaßnahmen errichtet. Ähnlich wie die technische Infrastruktur des polizeilichen Informationswesens befindet sich auch die rechtliche Architektur der polizeilichen Informationsordnung in keinem guten Zustand und bedarf der Sanierung.

Ohne weiteres wird sich diese allerdings nicht bewerkstelligen lassen. So führt etwa *Bäcker* angesichts der BKAG-Novellierung, die für den Informationsverbund als integralen Teil des polizeilichen Informationswesens essenziell ist, an: „Die Mängel dieser Regelungen lassen sich nicht mit punktuellen Änderungen des Entwurfs abstellen. Dieser Befund berührt […] die beabsichtigte Neugliederung der Informationsordnung des Bundeskriminalamts fundamental. Dieses Vorhaben sollte daher zurückgestellt werden, bis die derzeit offene Frage geklärt ist, ob sich hierfür grundrechtskonforme und praktikable Rechtsgrundlagen finden lassen."[1426] Gemeint sind hier die besprochenen Fehlkonstruktionen der §§ 16, 18, 19 BKAG,[1427] die aber zwischenzeitlich Gesetz geworden sind. Die Neugliederung wird aber auch sonst durch die Polizeigesetze bisher nicht hinreichend abgebildet. Erforderlich für eine adäquate Regulierung wäre gerade auch und zuallererst die Beantwortung der von *Bäcker* aufgeworfenen, bedeutsamen Frage, ob sich für das Konzept des neuen Informationsverbundes als gemeinsamem Datenhaus, in dem Daten nur noch einmal erfasst und dann anschließend im Rahmen der Rechtsgrundlagen beliebig verarbeitet werden sollen, überhaupt ein passendes Regelungskonzept wird finden lassen. Es geht also nicht nur im Bereich von neuen, informationstechnologisch fundierten Erhebungsmaßnahmen, sondern auch für die informationstechnologische Infrastruktur und ihre Weiterentwicklung um die Frage, ob die bestehenden Befugnisse und Regelungsformen auch zur effektiven Polizeiarbeit in der digitalisierten Gesellschaft herangezogen werden können oder ob es perspektivisch der Entwicklung und Konturierung neuer Regelungskonzepte bedarf.[1428]

Das gilt einmal für die Regelungen der Strukturen des polizeilichen Informationswesens, aber auch für die sich ändernde Qualität des polizeilichen Datenumgangs. Denn mit einer zunehmenden Datafizierung der Gesellschaft geht auch ein zunehmend datafiziertes Arbeiten der Polizei einher, was sich – nicht nur, aber auch – in einem spürbaren Anwachsen des polizeilichen Informationswesens bemerkbar macht, sowohl in Volumen als auch in Granularität der Daten. In der Folge werden die polizeilichen Datenbestände zunehmend zu einem Spiegel der sozialen Konflikte in der Gesellschaft. Zwar wird es sich immer um ein Zerrbild handeln, aber mit

1426 *Bäcker*, A-Drs. 18(4)806 D, S. 3.
1427 Siehe dazu bereits oben S. 334 ff.
1428 So *Müller/Schwabenbauer* in *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch des Polizeirechts, G. Rn. 607 im Kontext neuer polizeilicher Ermittlungsmethoden.

sich stetig vergrößerndem Umfang und sich verbessernder Auflösung. Eine solche Abbildung von Ereignissen abweichenden Verhaltens und damit zusammenhängender Personen, Objekte, Institutionen und sonstiger Entitäten im polizeilichen Informationswesen ermöglicht es mit wachsender Akkuratheit, Devianz für die Polizei retrospektiv erfahrbar zu machen.

Dabei können sich – auch über die Multimedialität der Daten – Akkumulationen ergeben, die sonst eher auf eingriffsintensiven Maßnahmen wie längerfristigen Observationen beruhen, die eine Beobachtung durch die Polizei über einen längeren Zeitraum beschreibt und als Maßnahme aufgrund ihrer Intensität regelmäßig hohen Anforderungen inhaltlicher und verfahrensrechtlicher Art unterliegt. Solche Überwachungsmaßnahmen sind darauf ausgerichtet „unter Nutzung moderner Technik (…) möglichst alle Äußerungen und Bewegungen zu erfassen und bildlich wie akustisch festzuhalten",[1429] wobei neben der bloßen menschlichen Beobachtung („Verfolgung") als besagte „moderne Technik" etwa Fotoapparate, Kameras, Peilsender, GPS-Geräte, Richtmikrofone und ähnliche Geräte zum Einsatz kommen.[1430] Dabei ist gar nicht entscheidend, dass die Überwachung durchgängig durchgeführt wird, ausschlaggebend ist vielmehr die Wiederholung.[1431] In einer immer stärker digital vermittelten Welt ist es indessen nicht mehr ungewöhnlich, dass bei den Polizeien häufiger auch Daten in Form von (bewegten) Bildern, Standorten in Raum und Zeit oder sogar Äußerungen – man denke an Sprach- und Videonachrichten, die zunehmend zum digitalen Kommunikationsverhalten zählen – anfallen. Zugegebenermaßen erfolgen längerfristige Observationen in der Gegenwart und in Echtzeit, das heißt, die erhobenen Daten finden mit einer hohen Aktualität Eingang in das polizeiliche Informationswesen. Nichtsdestotrotz behalten die so zusammengetragenen Daten, auch über die Gegenwart ihrer Erhebung hinaus, ihre hohe Persönlichkeitsrelevanz. Ein Persönlichkeitsbild wird sich auch nach einigen Jahren damit noch zeichnen lassen. Ob es noch zutreffend ist, ist eine davon zu unterscheidende Frage. Für Daten, die über einen längeren Zeitraum durch verschiedene Polizeikontakte wegen (mutmaßlich) deviantem Verhalten zu einer Person akkumuliert worden sind, kann bezüglich der Persönlichkeitsrelevanz nur begrenzt eine andere

1429 BVerfGE 141, 220 (287) – Bundeskriminalamtgesetz.

1430 *Müller/Schwabenbauer* in *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch des Polizeirechts, G. Rn. 796.

1431 *Müller/Schwabenbauer* in *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch des Polizeirechts, G. Rn. 800.

Wertung hinsichtlich der Invasivität gelten. Hier wie da können sich durch wiederholte Datenerhebungen und Speicherungen im polizeilichen Informationswesen für Polizist:innen, die die Daten retrospektiv auswerten und für ihre Aufgabenerfüllung analysieren – alles Schritte, die prinzipiell von der Datenverarbeitungsgeneralklausel gedeckt werden – Persönlichkeitsbilder von (nicht unerheblich) grundrechtstangierender Auflösung ergeben. Ähnliches gilt für das Sozialprofil von Betroffenen, das durch die auf sie bezogenen Daten von und über Kontakt- und Begleitpersonen sichtbar wird. Hierdurch kann eine Analyse von Daten bezogen auf Erkenntnisse wie das Sozialprofil in die Nähe der Eingriffsintensität der Ausschreibung zur polizeilichen Beobachtung rücken.[1432] Der hierin liegende Eingriff wird zwar indirekt dadurch etwas abgefedert, dass nur Organisationseinheiten, die besonders gravierende Kriminalitätsformen bearbeiten, einen entsprechend breiten Zugriff auf die polizeilichen Datenbestände haben. Nichtsdestotrotz zeigt das Fehlen von materiell-rechtlichen Regelungskonzepten für diese Formen polizeiinterner Datenakkumulationen, dass eine wirkliche Auseinandersetzung mit diesen internen Datenverarbeitungsprozessen und ihren grundrechtlichen Implikationen bisher zu wenig stattgefunden hat.

V. Das interne Datenschutzkontrollregime

Die bisherigen Ausführungen haben auf die Aspekte des polizeilichen Informationswesens fokussiert, die den polizeilichen Kernaufgaben – Strafverfolgung und Gefahrenabwehr, jeweils auch mit den Vorfeldkompetenzen der Straftatenverhütung und Strafverfolgungsvorsorge – dienen und damit wesentlich für Umfang und Form der polizeiliche Sozialkontrolle sind. Neben diesem größten und aus polizeifunktionaler Sicht wichtigsten Teil des polizeilichen Informationswesens gibt eine weitere integrale Komponente, deren Bedeutung insbesondere mit der EU-Datenschutzreform von 2016 zugenommen hat und wohl auch weiter zunehmend wird. Begrifflich soll dieser Aspekt als internes Datenschutzkontrollregime gefasst werden. Ziel dieser Struktur ist es, über die Einhaltung der – wie dargestellt an etlichen Stellen problematischen – normativen Rahmenbedingungen des polizeilichen Informationswesens zu wachen. Seine Ausprägung findet das

1432 Siehe zu dieser Maßnahme und dem Faktor des Sozialrpofils *Müller/Schwabenbauer* in *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch des Polizeirechts, G. Rn. 998.

interne Datenschutzkontrollregime im Wesentlichen in zwei Dimensionen: Einerseits in den behördlichen Datenschutzbeauftragten und andererseits in den technisch-organisatorischen Maßnahmen, die von den Datenschutzbeauftragten, aber auch anderen Teilen der Polizei zur Einhaltung der rechtlichen Vorgaben implementiert werden (müssen). Zudem sind beide Dimensionen Aufprägungen eines prozeduralen Grundrechtsschutzes. Schon im Volkszählungsurteil wurde die Bedeutung einer solchen internen verfahrensrechtlichen Kontrolle betont.[1433] Indem mit diesen Regulativen die polizeiliche Datenverarbeitungstechnologie und der Umgang mit dieser kontrolliert werden soll, haben die rechtlichen Vorgaben und die praktische Umsetzung des internen Datenschutzkontrollregimes direkten Einfluss darauf, wie die Polizei Informationen für ihre Aufgabenerfüllung verarbeiten kann und somit auch darauf, wie sich polizeiliche Sozialkontrolle materialisiert und entwickelt. Daneben treten offenkundig auch weitere Formen, denen sich der Datenschutz zur Kontrolle des polizeilichen Informationshandelns bedient. Zentral sind hier die Betroffenenrechte und die Datenschutzaufsicht durch die Landes- und den Bundesdatenschutzbeauftragten. Beide Instrumente sind aber kein integrierter Teil des polizeilichen Informationswesens und werden daher vorliegend weitestgehend ausgeklammert.

1. Personelle Ausprägung des internen Datenschutzkontrollregimes: Behördliche Datenschutzbeauftragte

Die Ausgestaltung der rechtlichen Rolle des Datenschutzbeauftragten erfolgt regelmäßig in den jeweiligen Datenschutzgesetzen und übernimmt im Wesentlichen die Regelungsinhalte, die die JI-Richtlinie vorgegeben hat. Geregelt werden die Aspekte der Benennung, der Stellung sowie der Aufgaben der behördlichen Datenschutzbeauftragten. Die gesetzlichen Vorgaben finden sich etwa in §§ 5, 6, 7 BDSG und den Entsprechungsvorschriften in den Landesdatenschutzgesetzen, die im Wesentlichen inhaltsgleich ausgestaltet sind. Zudem finden sich noch einige Sondervorschriften in den Bundes- und Landespolizeigesetzen (vgl. etwa §§ 70, 71, 72 BKAG).

Zunächst besteht eine Pflicht zur Benennung für alle Polizeibehörden, wobei aber unter Berücksichtigung ihrer Größe und Organisationsstruktur

1433 BVerfGE 65, 1 (44) – Volkszählung.

gemeinsame Datenschutzbeauftragte benannt werden können[1434] – etwa können mehrere untergeordnete Polizeibehörden eine Person als Datenschutzbeauftragte:n zugeordnet bekommen. Benannte müssen eine hinreichende berufliche Qualifikation sowie insbesondere Fachwissen auf dem Gebiet des Datenschutzrechts und der Datenschutzpraxis innehaben und auf der Grundlage ihrer Fähigkeit zur Erfüllung ihrer gesetzlichen Aufgaben in der Lage sein.[1435] Dabei ist es regelmäßig ausreichend, wenn die Datenschutzbeauftragten ihr spezifischen fachlichen Schwerpunkt haben – etwa im rechtlichen, technischen oder organisatorischen Gebiet – und ansonsten über Grundwissen in den anderen Bereichen verfügen, das sie mit organisationsintern zu gewährender Unterstützung in die Lage versetzt, ihre Aufgaben zu erfüllen.[1436]

Zentrale Stellschraube für die Effektivität der polizeilichen Datenschutzbeauftragten ist ihre Stellung innerhalb der Behördenstruktur. Sie müssen frühzeitig in datenschutzrechtliche Fragen eingebunden werden und sind bei ihrer Arbeit durch die datenschutzrechtlich verantwortliche Stelle zu unterstützen, etwa durch Ressourcen, aber auch durch Zugang zu den entsprechenden Verarbeitungsvorgängen. Auch wenn es die JI-Richtlinie selbst nicht vorschreibt, haben Bundes- und Landesgesetzgeber die Weisungsfreiheit der polizeilichen Datenschutzbeauftragten gesetzlich festgelegt.[1437] Diese Unabhängigkeit wird weiterhin durch ein Abberufungsverbot, den Schutz vor Sanktionierungen und – als spezielle polizeiorganisatorische Ausformung[1438] – die direkte Unterstellung unter die Leitungsebene verstärkt.[1439] Letzteres dient vor allem auch dem Einfluss der Datenschutzbeauftragten auf die polizeiinternen Regelungsprozesse. Jedoch ist die Unabhängigkeit im polizeilichen Bereich hier mitunter eingeschränkt. So kann sich etwa der oder die Datenschutzbeauftragte des Bundeskriminalamts in Zweifelsfällen nur im Benehmen mit der Behördenleitung an die Auf-

1434 *Körffer* in *Paal/Pauly/Ernst* (Hrsg.), Datenschutz-Grundverordnung, Bundesdatenschutzgesetz, § 5 Rn. 3.

1435 *Bergt/Schnebbe* in *Kühling/Buchner,* Datenschutz-Grundverordnung, Bundesdatenschutzgesetz: DS-GVO / BDSG, § 5 Rn. 5.

1436 *Gola* in *Gola/Heckmann/Klug* ua, BDSG, § 5 Rn. 10.

1437 *Körffer* in *Paal/Pauly/Ernst* (Hrsg.), Datenschutz-Grundverordnung, Bundesdatenschutzgesetz, § 6 Rn. 2.

1438 *Ruthig* in *Schenke/Graulich/Ruthig,* Sicherheitsrecht, § 72 BKAG Rn. 3.

1439 Die allgemeinen Vorschriften der Datenschutzgesetze schreiben nur eine Berichtslinie an die oberste Leitungsebene vor, nehemen aber insoweit keine organisatorische Einordnung vor, vgl. etwa *Bergt/Schnebbe* in *Kühling/Buchner,* Datenschutz-Grundverordnung, Bundesdatenschutzgesetz: DS-GVO / BDSG, § 6 Rn. 6.

sicht, also den oder die Bundesdatenschutzbeauftragte:n wenden, im Konfliktfall soll das Bundesministerium des Innern entscheiden. Eine solche Limitierung ist weder verfassungs- noch unionsrechtlich zulässig, da so die verfahrensrechtlichen Sicherungen von Datenverarbeitungsprozessen unzulässig beschränkt werden.[1440] Während eine klärende Kommunikation mit der Behördenleitung in Zweifelsfragen unproblematisch ist, muss sich also der oder die Datenschutzbeauftragte auch im Konfliktfall ohne weitere Beschränkung an die Aufsicht wenden können.[1441] Ferner ist in der Position der Datenschutzbeauftragten auch der Kontaktpunkt für von polizeilicher Datenverarbeitung betroffene Personen und insoweit mit externen datenschutzrechtlichen Kontrollmechanismen verzahnt. Dieser Aspekt der Stellung wird durch eine Verschwiegenheitspflicht hinsichtlich betroffener Personen und der mit ihnen verbundenen Vorgänge flankiert. Zudem haben polizeiliche Datenschutzbeauftragte Verschwiegenheitspflichten und gegebenenfalls Zeugnisverweigerungsrechte, da sie regelmäßig mit sensiblen Informationen aus den und über die Polizeiorganisationen in Kontakt kommen.

Die größte Bedeutung kommt den eigenständigen Aufgaben der Datenschutzbeauftragten zu. Zusammengefasst haben sie die Aufgabe der Beratung, der Überwachung bzw. Kontrolle sowie der Kooperation. Die datenschutzrechtlich verantwortliche Stelle ist über datenschutzrechtliche Vorgaben zu unterrichten und im Rahmen der Gestaltung der Datenverarbeitung lösungsorientiert so zu beraten, dass gesetzliche Vorgaben eingehalten werden.[1442] Dabei handelt es sich um eine Pflicht, die proaktiv zu erfüllen ist.[1443] Vor dem Hintergrund der hohem Komplexität des polizeilichen Informationsrechts ist diese Aufgabe als anspruchsvoll anzusehen.

Gegenüber der alten Rechtslage hat insbesondere die Überwachungsaufgabe der Beauftragten eine Intensivierung erfahren. Umfassend zu überwachen ist nunmehr sowohl die Einhaltung des gesamten anwendbaren Datenschutzrechts als auch die Einhaltung der Datenschutz-Strategien, die vom Verantwortlichen zur Umsetzung des Datenschutzes entwickelt werden. Dazu gehören neben Aspekten des technischen Datenschutzes etwa

1440 *Smitis* in *Simitis* (Hrsg.), Bundesdatenschutzgesetz, § 4g Rn. 27.
1441 *Ruthig* in *Schenke/Graulich/Ruthig*, Sicherheitsrecht, § 72 BKAG Rn. 4.
1442 *Paal* in *Paal/Pauly/Ernst* (Hrsg.), Datenschutz-Grundverordnung, Bundesdatenschutzgesetz, Art. 39 DS-GVO Rn. 5.
1443 *Bergt* in *Kühling/Buchner,* Datenschutz-Grundverordnung, Bundesdatenschutzgesetz: DS-GVO / BDSG, Art. 39 DS-GVO Rn. 11.

auch Zuständigkeitsregelungen sowie Sensibilisierungen und Schulungen der Beamt:innen.[1444] Da ein Großteil der Regelungen, die es zur technischen Infrastruktur des polizeilichen Informationswesens gibt, und alle Formen des polizeilichen Umgangs mit personenbezogenen Daten entsprechende datenschutzrechtliche Implikationen aufweisen, müssen die Datenschutzbeauftragten einen weiten Teil der polizeilichen Informationsarbeit überwachen. Dabei können sie sich regelmäßig nicht auf eine Art papierne Überwachung, etwa anhand eines Verzeichnisses von Verarbeitungstätigkeiten, beschränken. Vielmehr muss die informationstechnologische Infrastruktur und der Umgang mit ihr etwa in Vor-Ort-Kontrollen überprüft werden.[1445] Eine Mischung aus Beratung und Kontrolle stellt die ebenfalls dem Aufgabenspektrum unterfallende Datenschutz-Folgenabschätzung dar. Diese ist – etwa gem. § 67 Abs. 1 BDSG – immer dann durchzuführen, wenn „eine Form der Verarbeitung, insbesondere bei Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich eine erhebliche Gefahr für die Rechtsgüter betroffener Personen zur Folge" hat. Im Rahmen einer solchen Abschätzung sind die polizeilichen Datenschutzbeauftragten zu beteiligen, ihre Mitwirkung ist für sie verpflichtend und – da sie ihre Tätigkeiten risikobasiert priorisieren müssen (vgl. etwa § 7 Abs. 3 BDSG) – bevorzugt zu erledigen. Während die Beauftragten für die Durchführung selbst nicht zuständig sind, müssen sie im Rahmen ihrer Durchführung konsultieren und das Ergebnis kontrollieren.[1446] Hiermit sind insbesondere informationstechnologische Neuerungen ebenfalls der Kontrolle der Datenschutzbeauftragten überantwortet.

Schließlich sind die Datenschutzbeauftragten über ihre jeweilige Behörde hinaus auch kooperativ tätig. Einerseits gibt es gesetzlich vorgeschriebene innerpolizeiliche Kooperationspflichten. So gibt es in § 72 BKAG die Pflicht für den oder die Beauftragte:n des Bundeskriminalamts mit den Datenschutzbeauftragten der Landeskriminalämter, der Bundespolizei und des Zollkriminalamts zusammenzuarbeiten. Hier sollen insbesondere Synergieeffekte im Rahmen des Umgangs mit den normativen Rahmenbe-

1444 *Bergt* in *Kühling/Buchner,* Datenschutz-Grundverordnung, Bundesdatenschutzgesetz: DS-GVO / BDSG, Art. 39 DS-GVO Rn. 13.
1445 *Bergt* in *Kühling/Buchner,* Datenschutz-Grundverordnung, Bundesdatenschutzgesetz: DS-GVO / BDSG, Art. 39 DS-GVO Rn. 15.
1446 *Gola* in *Gola/Heckmann/Klug* ua, BDSG, § 7 BDSG Rn. 8.

dingungen des polizeilichen Informationswesens genutzt werden.[1447] Daneben ist aber auch eine Vereinheitlichungswirkung im Umgang mit Daten, insbesondere im polizeilichen Informationsverbund, theoretisch aber auch darüber hinaus, denkbar. Zudem sind aber die polizeilichen Datenschutzbeauftragten jeweils Kontaktpunkt für die Aufsichtsbehörden in Bund und Ländern. Vor allem aber besteht eine Kooperationspflicht mit der Aufsichtsbehörde des Bundes bzw. des jeweiligen Landes. Die polizeilichen Datenschutzbeauftragten sind die ersten Ansprechpersonen in datenschutzrechtlichen Angelegenheiten. Damit ist nochmal die besondere Relevanz der Position der polizeiinternen Datenschutzbeauftragten hervorgehoben. Mit der Kooperationspflicht, wenn der Kontakt von der Aufsichtsbehörde ausgeht, ist auch das Recht zur Hinzuziehung der Aufsichtsbehörde zur Beratung verbunden. Insoweit besteht das Potenzial, dass sich zwischen internen Datenschutzbeauftragten und der Aufsicht eine datenverarbeitungshemmende Achse bildet, die mit den Anliegen der polizeilichen (Informations-)Arbeit zum Zwecke von Gefahrenabwehr und Strafverfolgung in Konflikt tritt.[1448]

Insgesamt haben die polizeilichen Datenschutzbeauftragten damit aus rechtlicher Sicht eine zentrale Position im polizeilichen Informationswesen, da sie über ihre Stellung und Aufgaben umfassend mit Datenverarbeitungsvorgängen und der diesen zugrundeliegenden Technologien befasst sind und beides unter Rechtmäßigkeitsgesichtspunkten überwachen und kontrollieren. Sie sind zudem vor allem im Rahmen ihrer Beratungsaufgaben durch ihre Einbindung in die technisch-organisatorischen Maßnahmen auch mit der zweiten Ausprägung des internen Datenschutzkontrollregimes des polizeilichen Informationswesens eng verwoben.

2. Technisch-organisatorische Ausprägungen des internen Datenschutzkontrollregimes

Die Datenschutzbeauftragten – selbst, wenn sie noch Mitarbeiter:innen haben – können das polizeiliche Informationswesen jedoch nicht allein mit den ihnen zur Verfügung stehenden (menschlichen) Fähigkeiten überwachen und kontrollieren. Vielmehr haben sich im internen Datenschutzkontrollregime, zunächst anlässlich verfassungsrechtlicher Vorgaben, seit 2016

1447 *Ruthig* in *Schenke/Graulich/Ruthig,* Sicherheitsrecht, § 72 BKAG Rn. 4.
1448 *Bergt* in *Kühling/Buchner,* Datenschutz-Grundverordnung, Bundesdatenschutzgesetz: DS-GVO / BDSG, Art. 39 DS-GVO Rn. 17 ff.

vor allem aufgrund unionsrechtlicher Vorschriften, Instrumente zur Unterstützung der Datenschutzbeauftragten bei ihren Aufgaben und generell zur Einhaltung datenschutzrechtlicher Bestimmungen herausgebildet. So schreibt Art. 19 JI-Richtlinie nunmehr vor, dass „geeignete technische und organisatorische Maßnahmen" implementiert werden, „um sicherzustellen und den Nachweis dafür erbringen zu können, dass die Verarbeitung in Übereinstimmung mit dieser Richtlinie erfolgt." Diese Grundnorm wird durch die JI-Richtlinie und die jeweiligen Umsetzungsgesetz in konkretere Bahnen gelenkt, wobei der Konkretisierungsgrad sich unterscheidet.

Nochmals aufgegriffen wird der Begriff der technisch-organisatorischen Maßnahmen in Art. 29 JI-Richtlinie, der zu diesen verpflichtet, „um ein dem Risiko angemessenes Schutzniveau zu gewährleisten, insbesondere im Hinblick auf die Verarbeitung besonderer Kategorien personenbezogener Daten."[1449] Beabsichtigt ist damit die Etablierung eines Sicherheitsstandards für die personenbezogenen Daten der Betroffenen, nicht für das polizeiliche Informationswesen als vulnerable Infrastruktur.[1450] Dazu sollen etwa Pseudonymisierung und Verschlüsselung beitragen (vgl. § 64 Abs. 2 S. 1 BDSG). Vor allem sind aber die Maßnahmen bei automatisierten Verarbeitungen, wie sie meistens im polizeilichen Informationswesen auftreten, umzusetzen, wozu etwa gemäß § 64 Abs. 3 S. 1 BDSG Zugriffskontrollen, Speicherkontrollen, Benutzerkontrollen, Übertragungskontrollen, Eingabekontrollen und weitere Maßnahmen gehören. Vor allem für die Vorgangsbearbeitungs- und Fallbearbeitungssysteme, in denen ein Großteil des polizeilichen Datenumgangs stattfindet, sind verhältnismäßig austarierte Zugriffs- und Berechtigungskonzepte notwendig, mit denen einerseits gewährleistet wird, dass die jeweilige Organisationseinheit oder Beamt:in alle Daten hat, die zur jeweilig aktuellen Aufgabenerfüllung benötigt werden. Andererseits müssen solche Verarbeitungsvorgänge unterbunden werden, die sich gegen gesetzliche Bestimmungen richten, wie beispielsweise die Nutzung von Daten aus abgeschlossenen Vorgängen, die grundsätzlich nur noch zur Vorgangsverwaltung und Dokumentation genutzt werden.[1451]

Besondere Bedeutung erlangen Zugriffsberechtigungen zudem im polizeilichen Informationsverbund, in dem gemäß § 29 Abs. 4 BKAG auch § 15 BKAG zu beachten ist, der die Zugriffsberechtigungen regelt. Die

1449 Siehe dazu bereits oben S. 192 f.

1450 *Bock* in *Brink/H. Wolff*, BeckOK Datenschutzrecht, § 64 Rn. 1.

1451 Arzt in *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch des Polizeirechts, G. Rn. 1196. Zu diesem Problem siehe bereits oben S. 254 ff.

Vorschrift dient – wie aber letztlich alle Zugriffsberechtigungen im polizeilichen Bereich – zumindest auch der Einhaltung des Grundsatzes der hypothetischen Datenneuerhebung. Durch das Berechtigungskonzept soll festgelegt werden, wer auf die gemäß § 14 BKAG gekennzeichneten Daten zugreifen kann. Die Zugriffsberechtigungen sind dabei inhaltlich so zu gestalten, dass nur Daten zur Verfügung stehen, deren Kenntnis zur Erfüllung der jeweiligen Dienstpflichten erforderlich ist, sodass etwa anhand des „jeweiligen Dienstposten[s] eines Mitarbeiters ergebenden Dienstpflichten (zum Beispiel Durchführung von Ermittlungen im Bereich des islamistischen Terrorismus, §§ 129a, 129b StGB) [zu] bestimmen [ist], wie die Zugriffsberechtigung auszugestalten ist."[1452] Dasselbe gilt für die Befugnis zur Änderung, Berichtigung oder Löschung von personenbezogenen Daten.[1453] Die Vergabe orientiert sich an einem zugrundeliegenden Rechte- und Rollenkonzept, in dem festgelegt ist, „für welche Funktionen und Dienstposten welche Berechtigungen – sowohl hinsichtlich des Zutritts zu Arbeitsbereichen als auch hinsichtlich des Zugriffs auf Daten – erforderlich sind."[1454] Zudem soll eine formale Gestaltung der Systeme in einer Weise erfolgen, dass die Abfragegründe, die Polizist:innen angeben, standardisiert sind, um eine effektivere Dokumentation zu ermöglichen und den Datenumgang besser steuern zu können, gleichzeitig aber auch eine höhere Nutzer:innenfreundlichkeit zu gewährleisten.[1455] Auch hier ist die Verpflichtung zur technisch-organisatorischen Ausgestaltung an den Stand der Technik gekoppelt. Diese offene Formulierung der Vorgaben zu den technisch-organisatorischen Maßnahmen ist allerdings nicht unbedenklich. Zwar ist sie mit Blick auf die Differenzen zwischen einzelnen Polizeien, etwa was Stand der Technik oder auch Ressourcen angeht, grundsätzlich nachvollziehbar. Rekapituliert man jedoch, dass der Datenschutz zur Einhegung polizeilichen Informationshandelns beitragen soll, ist die graduelle Beliebigkeit der Implementierung technisch-organisatorischer Maßnahmen problematisch, weil ihre inhaltliche Ausgestaltung der verantwortlichen Stelle überlassen wird.[1456]

1452 BT-Drs. 18/11163, S. 96.
1453 BT-Drs. 18/11163, S. 96.
1454 BT-Drs. 18/11163, S. 97.
1455 BT-Drs. 18/11163, S. 97.
1456 In ähnlichem Kontext *Arzt* in *Möstl/Kugelmann* (Hrsg.), Beck'scher Online-Kommentar Polizei- und Ordnungsrecht Nordrhein-Westfalen, § 22 Rn. 55.

In eine ähnliche Richtung zielen auch die Vorgaben des Art. 20 JI-Richtlinie, der den Verantwortlichen zum Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen (auch privacy by design und privacy by default genannt) verpflichtet. Unter die erstgenannte Ausgestaltungsmaxime fällt etwa die Datenminimierung oder ebenfalls die Pseudonymisierung.[1457] So wäre etwa eine Ausgestaltung des Datenabgleichs in einer Weise, die abfragenden Polizist:innen nur eine sehr begrenzte Datenauswahl an die Hand gibt, eine solche Technikgestaltung.[1458] Datenschutzrechtliche Voreinstellungen haben für von der Polizei eingesetzte Datenverarbeitungssysteme Bedeutung.[1459] So kann es schon einen Unterschied machen, welche Daten wie in einem Informationssystem auf einen Suchbefehl angezeigt werden. Hier wäre etwa darauf zu achten, dass nur zweckerforderliche Daten angezeigt werden. Im Zusammenhang mit Datenschutz durch Technikgestaltung ist auch vorgeschlagen worden, eine regelmäßige automatisierte Erkundigung der Polizeibehörden bei den Staatsanwaltschaften über den Stand von relevanten Strafverfahren einzurichten. Damit könnte rechtswidrigen Datenverarbeitungen vorgebeugt werden, die sich daraus ergeben, dass die Polizeien weiter Daten verarbeiten, obwohl das zugehörige Verfahren längst in einer den Rechtsgrund für die Verarbeitung entziehenden Weise beendet worden ist.[1460] Auch beim Datenschutz durch Technikgestaltung ist allerdings eine recht flexible Ausgestaltung der Maßnahmen durch eine offene gesetzliche Formulierung möglich, was jedoch insbesondere im Bereich von Technikregulierung nachvollziehbar ist. Recht breit sind auch die Vorgaben zu technisch-organisatorischen Maßnahmen anlässlich der Verarbeitung besonderer Kategorien personenbezogener Daten, wie sie etwa in § 48 Abs. 2 BDSG vorgeschrieben werden.

1457 *Schwichtenberg* in *Kühling/Buchner,* Datenschutz-Grundverordnung, Bundesdatenschutzgesetz: DS-GVO / BDSG, § 71 Rn. 1 f.

1458 Zur Gebotenheit einer solchen Gestaltung siehe etwa *Müller/Schwabenbauer* in *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch des Polizeirechts, G. Rn. 940: "Es ist nicht zulässig, dass die Polizei beispielsweise im Rahmen einer allgemeinen Verkehrskontrolle den Zugriff auf sämtliche gespeicherten Daten über einen Betroffenen erhält, obwohl dies weder für die konkrete Aufgabe noch zu Fahndungszwecken erforderlich ist. Wenn man es überhaupt für zulässig hält, dass solche Daten in allgemein zugänglichen Fahndungsbeständen erfasst werden, muss zumindest die Einhaltung des Erforderlichkeitsprinzips technisch durch Zugriffsbeschränkungen gewährleistet werden".

1459 *Schwichtenberg* in *Kühling/Buchner,* Datenschutz-Grundverordnung, Bundesdatenschutzgesetz: DS-GVO / BDSG, § 71 Rn. 4.

1460 BayLfD, 27. Tätigkeitsbericht 2015/2016, S. 60; *Müller/Schwabenbauer* in *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch des Polizeirechts, G. Rn. 845.

Eine konkrete technische Maßnahme, die der Kontrolle der Rechtmäßigkeit polizeilichen Informationshandelns dienlich ist, sind die Protokollierungspflichten im Datenumgang, wie sie Art. 25 JI-Richtlinie für automatisierte Verarbeitungssysteme aufstellt, also für einen Großteil der Datenverarbeitung im polizeilichen Informationswesen. So schreibt die auf Bundesebene umsetzende Regelung des § 76 BDSG vor, dass die Verarbeitungsvorgänge der Erhebung, Veränderung, Abfrage, Offenlegung einschließlich Übermittlung, Kombination und Löschung protokolliert werden müssen. Protokolle zu Übermittlungen müssen es ermöglichen, die Begründung, das Datum und die Uhrzeit und so weit wie möglich – idealerweise lückenlos – die Identität der abfragenden und empfangenden Person festzustellen. Nur so kann – was Zweck der generierten personenbezogenen Protokolldaten ist – die Rechtmäßigkeit der Datenverarbeitung vom Verantwortlichen selbst, zumeist durch den oder die polizeiliche:n Datenschutzbeauftragte:n oder durch die Aufsichtsbehörde, überprüft werden. Die Protokolle können sodann auch zweckändernd in Strafverfahren wegen unrechtmäßiger Datenverarbeitung genutzt werden.[1461] Die Löschungsfrist solcher Protokolldaten – am Ende des auf deren Generierung folgenden Jahres, § 76 Abs. 4 BDSG – ist jedoch problematisch kurz, da vor allem die anlassunabhängigen Kontrollen der Aufsichtsbehörden diesem Turnus nicht unbedingt folgen können.[1462] Im Bereich der polizeilichen Informationsverbundes gelten zudem noch besondere Protokollierungsvorschriften aus § 81 BKAG, wobei die Löschungsfrist noch kürzer bemessen ist, was ebenfalls verfassungs- und unionsrechtswidrig sein dürfte, weil es eine ausreichende prozedurale Sicherung der Datenverarbeitung verhindert. Positiv ist hingegen, dass den polizeilichen Datenschutzbeauftragten die Protokolldaten in elektronisch auswertbarer Form zur Verfügung gestellt werden, was eine effektive Kontrolle fördern dürfte.

Auch der technisch-organisatorischen Dimension des internen Datenschutzkontrollregimes zuzuordnen sind Aussonderungsprüffristen, die der Einhaltung der Löschungsverpflichtung aus § 75 BDSG dienen. Dieses Pflichtenregime ist eine der zentralen Stellschrauben für den Umfang des polizeilichen Informationssystems. Es bestimmt entscheidend darüber mit, wie weit zurück und wie detailliert das polizeiliche Gedächtnis abwei-

1461 *Schwichtenberg* in *Kühling/Buchner,* Datenschutz-Grundverordnung, Bundesdatenschutzgesetz: DS-GVO / BDSG, § 76 Rn. 5.

1462 Müller/Schwabenbauer in *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch des Polizeirechts, G. Rn. 1044.

chendes Verhalten und damit zusammenhängende Informationen erinnern kann. Damit sind die Aussonderungsprüffristen auch eine Einflussgröße für die Intensität der von der Polizei ausübbaren Sozialkontrolle. Grundsätzlich ist dabei keine laufende Überprüfung des Datenbestandes vorgesehen, weil es die Arbeitskraft der Polizeien übersteigen würde. Stößt jedoch jemand im Rahmen der Sachbearbeitung oder – was wohl praktisch eher der Fall sein wird – im Rahmen eines konkreten Löschungsantrags eines Betroffenen auf die Unrechtmäßigkeit einer Datenverarbeitung, so kann auch abseits der sonst festgelegten Fristen gelöscht werden. Regelmäßig wird jedoch nach einer Fristenregelung verfahren. In der Regel – § 77 BKAG kann hier gut als Maßstab stehen, da die Norm auch für den polizeilichen Informationsverbund gilt – sind dabei die Daten bei Erwachsenen nach zehn, bei Jugendlichen nach fünf und bei Kindern nach zwei Jahren auf ihre mögliche Aussonderung hin zu prüfen. Bei sonstigen Personen im Sinne des § 19 BKAG sind diese Fristen nochmals herabgesetzt (Erwachsene: fünf Jahre, Jugendliche: drei Jahre). Ohne Zustimmung ist die Speicherung dieser Personendaten grundsätzlich auf ein Jahr beschränkt, wobei eine Verlängerung bei weiterem Vorliegen der Voraussetzungen des § 19 Abs. 1 BKAG vorgenommen werden kann. Hier gibt es eine abgestufte Limitierung auf drei, fünf oder zehn Jahre. Danach ist die Speicherung dann zu beenden. Es ist zu betonen, dass es sich bei den übrigen Fristen nicht um Höchstspeicherfristen handelt, nach denen unbedingt zu löschen wäre. Vielmehr ist zu prüfen, ob weiter gespeichert und damit auch verarbeitet werden kann. Mit Ablauf der Fristen ist jedoch regelmäßig von einem Wegfall der Erforderlichkeit auszugehen, wobei eine Prognose ergeben kann, dass es je nach Person und Lebensumfeld nicht ausgeschlossen erscheint, dass es erneut zu einer Straffälligkeit kommen wird.[1463] Insgesamt dürfte damit nicht gerade eine großzügige Löschungspraxis befördert werden, was das polizeiliche Informationswesen eher erinnerungsfähig macht. Dass gilt umso mehr, wenn eine weitergehende Speicherung zur Vorgangsverwaltung möglich ist, diese aber nur unzureichend vor zweckentfremdendem Datenumgang abgeschirmt wird.[1464]

Ein mit der europäischen Datenschutzreform eingeführtes Instrument, das die bisherige Vorabkontrolle ersetzt, ist die Datenschutz-Folgenabschätzung.[1465] Mit ihr sollen bei Verarbeitungsvorgängen mit besonders hohem

1463 *Ruthig* in *Schenke/Graulich/Ruthig,* Sicherheitsrecht, § 77 BKAG Rn. 16, 18.
1464 Siehe dazu bereits oben S. 254 ff.
1465 *Hansen* in *Brink/H. Wolff*, BeckOK Datenschutzrecht, § 67 Rn. 5.

Risikopotenzial für Betroffene diese Risiken möglichst frühzeitig analysiert und durch entsprechende Datenschutz-Maßnahmen nach Möglichkeit kompensiert werden.[1466] Sie ist immer dann durchzuführen, wenn eine Form der Verarbeitung, insbesondere bei Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich eine erhebliche Gefahr für die Rechtsgüter betroffener Personen zur Folge hat (vgl. etwa § 67 Abs. 1 BDSG). So soll eine strukturelle Stärkung des Datenschutzes bewirkt werden.[1467] Grundsätzlich sollen nicht einzelne Verarbeitungsvorgänge, sondern die übergeordneten Systeme und Verfahren zu überprüfen sein und zwar bei der Einführung neuer Verarbeitungssysteme bzw. -verfahren oder wesentlichen Veränderungen an bestehenden.[1468] Insgesamt bleiben die Umstände, die eine Datenschutz-Folgenabschätzung notwendig machen allerdings eher vage.[1469] Allerdings droht im Bereich der Datenverarbeitungstätigkeiten der Polizei- und Strafverfolgungsbehörden regelmäßig ein Eingriff in die Rechtsgüter natürlicher Personen. Insbesondere im Rahmen der repressiven Kriminalitätsbekämpfung, wo die Daten als belastendes Beweismaterial im Strafverfahren verwendet werden sollen, drohen häufig empfindliche Freiheitseinbußen für Betroffene.[1470] Insofern ist im polizeilichen Bereich regelmäßig von einer Gefahr für Betroffene auszugehen.

Im Rahmen einer Datenschutz-Folgenabschätzung sind die jeweiligen Datenschutzbeauftragten zu beteiligen, was diesen wiederum einen maßgeblichen Einfluss auf die Verwirklichung des Datenschutzes in sensiblen und risikoreichen Verarbeitungsbereichen geben kann. Auch inhaltlich sind die Folgenabschätzungen nicht komplett determiniert, müssen aber gewisse Mindestinhalte aufweisen. Dazu gehören eine systematische Beschreibung der geplanten Verarbeitungsvorgänge und der Zwecke der Verarbeitung, eine Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge in Bezug auf deren Zweck, eine Bewertung der Gefahren

1466 *Nolden* in *Paal/Pauly/Ernst* (Hrsg.), Datenschutz-Grundverordnung, Bundesdatenschutzgesetz, § 67 Rn. 2.
1467 *Johannes/Weinhold* in *Sydow* (Hrsg.), Bundesdatenschutzgesetz, § 67 Rn. 14.
1468 *Johannes/Weinhold* in *Sydow* (Hrsg.), Bundesdatenschutzgesetz, § 67 Rn. 14.
1469 *Schwichtenberg* in *Kühling/Buchner,* Datenschutz-Grundverordnung, Bundesdatenschutzgesetz: DS-GVO / BDSG, § 67 Rn. 2 Das hat auch zur Folge, dass der Einsatz dieses wichtigen Datenschutzinstruments nicht ohne Probleme abläuft, siehe dazu unten S. 398.
1470 *Schwichtenberg* in *Kühling/Buchner,* Datenschutz-Grundverordnung, Bundesdatenschutzgesetz: DS-GVO / BDSG, § 67 Rn. 21 f.

für die Rechtsgüter der betroffenen Personen und schließlich die Maßnahmen, mit denen bestehenden Gefahren abgeholfen werden soll. Nur wenn diese Mindestanforderungen beachtet werden, kann das bewertete System oder Verfahren auf seine Gefahrenträchtigkeit hin eingeschätzt werden. Die getroffenen Maßnahmen zur Risikominimierung müssen, soweit erforderlich, durch den Verantwortlichen überprüft werden, was die Datenschutz-Folgenabschätzung zu einem iterativen Prozess macht.[1471] Da das Risikopotenzial von Verarbeitungsvorgängen von vielen verschiedenen Faktoren bestimmt werden kann, die sich in einem ständigen insbesondere technischen Anpassungsprozess befinden und dann Auswirkungen auf die mit ihnen in Verbindung stehenden Verarbeitungsvorgängen haben können, trägt diese mitlaufende Überprüfungspflicht der Dynamik des polizeilichen Informationswesens in sinnvoller Weise Rechnung.

Neben die Datenschutz-Folgenabschätzung, die bereits teilweise auch der Dokumentation von risikoreichen Verarbeitungsvorgängen dient, tritt nunmehr noch das Verzeichnis von Verarbeitungstätigkeiten, das eine umfassende Dokumentation der im Zuständigkeitsbereich eines Verantwortlichen durchgeführten Datenverarbeitungen leisten soll. Neben der Effektivierung der Datenschutzaufsicht, der dieses Verzeichnis die Kontrolle erleichtern soll, hilft es auch der verantwortlichen Stelle, den Überblick zu behalten.[1472] Ein solches Verzeichnis hat etwa die Kategorien der im polizeilichen Informationsverbund durchgeführten Datenverarbeitungen zu enthalten, aber auch die Datenverarbeitungen in den polizeieigenen Informationssystemen.[1473] Enthalten sein müssen zudem etwa Informationen zum Verarbeitungszweck, zur Verwendung von Profiling (Art. 4 Nr. 4 DS-GVO), zum Verfahren bei Übermittlungen oder auch zur Protokollierung.[1474] Mit dem Wegfall der Dateienstruktur in Teilen des polizeilichen Informationswesens ersetzt das Verzeichnis von Verarbeitungstätigkeiten die bisherigen Errichtungsanordnungen an einigen Stellen,[1475] wodurch der Grad der

1471 *Nolte/Werkmeister* in *Gola/Heckmann/Klug* ua, BDSG, § 67 Rn. 34.

1472 *Paal* in *Paal/Pauly/Ernst* (Hrsg.), Datenschutz-Grundverordnung, Bundesdatenschutzgesetz, § 70 Rn. 3.

1473 *Ruthig* in *Schenke/Graulich/Ruthig,* Sicherheitsrecht, § 80 BKAG Rn. 4.

1474 *Müller/Schwabenbauer* in *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch des Polizeirechts, G. Rn. 1038.

1475 Etwa im Informationsverbund, nicht hingegen im Regelungsbereich der StPO, vgl. BT-Drs. 19/4671, 46. Allerdings ist dieser Bereich im Vergleich eher von geringerer Bedeutung für das polizeiliche Informationssystem in seiner Gesamtheit.

inhaltlichen Konkretisierung von Datenverarbeitungen absinkt.[1476] Zum Zweck der Selbstkontrolle kann das Instrument aber dennoch nützlich sein, etwa indem durch das Vergegenwärtigen von Zweckbindungen „Überwachungsauswüchse" eingehegt werden.[1477]

3. Abschließende Bemerkungen

Das interne Datenschutzkontrollregime ist in seinem Kern – auch wenn es für seine verschiedenen Instrumente Vorläufer gab – ein Ergebnis der europäischen Datenschutzreform. Dieses unionrechtliche Gesetzgebungspaket hat vor allem eine Prozeduralisierung des Datenschutzes mit sich gebracht.[1478] Das interne Datenschutzkontrollregime ist ein direkter Ausdruck davon, denn es handelt sich dabei ganz überwiegend um eine verfahrensrechtliche Sicherung von Datenverarbeitungsprozessen, die dem Schutz der Betroffenen dient. Wie einleitend erläutert, sind die Regelungen dieses Kontrollsystems und ihre praktische Ausgestaltung überaus relevant für die originäre Polizeiarbeit. Besondere Bedeutung kommt insofern den internen Datenschutzbeauftragten zu, die neben ihren Aufgaben auch in viele der technisch-organisatorischen Maßnahmen des Datenschutzkontrollregimes involviert sind. Sie sind neben den anderen (auch polizeiexternen) Akteuren des Datenschutzes gleichfalls ein wichtiges Element, das dazu beiträgt, „dass Vertrauen und Rechtssicherheit entstehen können und der Umgang mit Daten in einen demokratischen Diskurs eingebunden bleibt."[1479] Auch wenn sie nicht dieselben Möglichkeiten zur Beseitigung von Missständen wie die jeweiligen Aufsichtsbehörden haben, sind die internen Datenschutzbeauftragten aufgrund ihrer Nähe zu den Technologien, Prozessen und Beamt:innen eine zentrale Ressource für die Aufsichtsbehörden. Gleichzeitig sind sie aufgrund ihrer vorgeschriebenen Involvierung in alle wichtigen Datenverarbeitungsprozesse in der Lage, wichtige Steuerungsimpulse für die polizeiliche Informationsverarbeitung zu geben. Ihre Stellung und Einbindung in die Dynamiken des polizeilichen Informationswesens – zumindest wie es sich im jeweiligen Zuständigkeitsbereich darstellt – machen sie außerdem zu einer relevanten Informationsquelle für die tat-

1476 Siehe dazu bereits oben S. 233 sowie unten S. 401.
1477 *Johannes/Weinhold* in *Sydow* (Hrsg.), Bundesdatenschutzgesetz, § 70 Rn. 38.
1478 *Ruthig* in *Schenke/Graulich/Ruthig,* Sicherheitsrecht, Vorb. § 69 BKAG Rn. 1.
1479 So BVerfGE 133, 277 (365) – Antiterrordateigesetz-Urteil in dem etwas engeren, aber angrenzenden Kontext der Transparenz der Datenverarbeitung.

sächlichen Wirkweisen polizeilicher Informationsverarbeitung, worum es im Folgenden gehen soll.

Kapitel IV. Mosaikhafte Rekonstruktion des polizeilichen Informationswesens auf Grundlage der Deutungen behördlicher Datenschutzbeauftragter

A. Methodische Aspekte der Expert:inneninterviews mit polizeilichen Datenschutzbeauftragten

Das polizeiliche Informationswesen erscheint aus rechtswissenschaftlicher Perspektive häufig undurchsichtig und dadurch unnahbar in seiner Rechtswirklichkeit.[1480] Auch aus soziologischer Perspektive wird dem rechtlichen Diskurs vorgehalten sich nicht hinreichend mit den tatsächlichen Prozessen der polizeilichen Informationsverarbeitung auseinanderzusetzen, was die Regulierung inadäquat mache.[1481] Vor allem auch aufgrund der Sozio-Technizität des polizeilichen Informationswesens ist für ein Verständnis der gegenwärtigen informationstechnologischen Phase der Datafizierung eine empirische Annäherung an die Wirklichkeit polizeilichen Informationshandelns vonnöten – eine Analyse der nur rechtlichen oder technischen Strukturen würde insoweit zu kurz greifen.[1482]

Vor diesem Hintergrund war es ein Anliegen der vorliegenden Untersuchung, das polizeiliche Informationswesen als dynamisches Ensemble aus polizeilicher Informationstechnik und polizeilichen Informationspraktiken aufbauend auf bereits Bekanntem weiter zu erhellen. Das Erkenntnisziel war dabei dreigeteilt: Erstens ging es vor dem Hintergrund des begrenzten Wissensstandes generell um die weitere Exploration des Informationswesens der Polizei. Zweitens sollte mit Blick auf die Auswirkungen der digitalen Transformation auf die Polizei als Institution organisations- und prozesssoziologisches Wissen über Wandlungsprozesse innerhalb der Polizei generiert werden. Das dritte Ziel war schließlich, einen Einblick in die rechtstatsächliche Umsetzung der Normen zu erlangen, die das Informationshandeln der Polizei rechtlich steuern sollen, also in das polizeiliche Datenschutzrecht, da sich hieraus – so die Annahme – auch Implikationen

1480 Siehe etwa *Arzt* in *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch des Polizeirechts, G. Rn. 1129, demzufolge eine abschließende Darstellung der tatsächlich betriebenen Systeme der Polizei nicht möglich.

1481 So *Brayne,* Predict and surveil, S. 119.

1482 *Egbert/Leese,* Criminal futures, S. 5.

für den Modus polizeilicher Sozialkontrolle ablesen lassen können. Die drei Erkenntnisziele stehen dabei nicht gesondert nebeneinander, sondern bauen stellenweise aufeinander auf.

Ein solches Anliegen begegnet jedoch einigen Hürden: Einerseits soll mit der Polizei eine institutionelle Organisation erforscht werden, die in polizeiwissenschaftlichen Kreisen als nur schwer zugänglich gilt.[1483] Darüber hinaus ist mit der Datenverarbeitung ein sensibles Thema angesprochen. Die Sammlung, Speicherung und Auswertung von Daten, kurz das informationelle Handeln der Polizei, ist heute mehr denn je conditio sine qua non für fast jegliche polizeiliche Aktivität. Ein externer Zugriff auf das in polizeilichen Informationssystemen vorgehaltene Wissen ist damit aus der Innenperspektive der Polizei immer sehr genau darauf zu prüfen, ob er in irgendeiner Weise problematisch für die Aufgabenerfüllung oder Außenwirkung der Polizei sein könnte – selbst wenn es sich nur um einen impliziten wissenschaftlichen Zugriff handelt. Trotz dieser grundsätzlichen Hindernisse erschien es sinnvoll, die vorliegende Untersuchung über den Wandel des polizeilichen Informationswesens mit weiteren, selbst generierten empirischen Erkenntnissen zu komplementieren, gerade auch weil diese Wirklichkeit der Rechtsdogmatik zu lange als Anknüpfungspunkt für sinnvolle normative Steuerungskonzepte verborgen war. Auch wenn die Rechtsrealität polizeilichen Informationshandelns bereits seit einiger Zeit immer öfter Gegenstand wissenschaftlicher Arbeiten wird,[1484] bleibt das Urteil des fehlenden empirischen Wissens über polizeiliche Datenverarbeitung aktuell. Vor allem mit Blick auf die durchgreifenden strukturellen Umwälzungen der digitalen Transformation der Gesellschaft, welche die Polizei innengerichtet als Behörde und gleichzeitig als Institution der Sozialkontrolle außengerichtet in Form von neuen Unordnungsphänomenen zu bewältigen hat, ist ohnehin fraglich, ob es auf kurze Sicht möglich sein wird, ein empirisch treffendes Bild polizeilichen Informationshandelns zu erfassen.[1485] Jedenfalls bleibt es aufgrund der Geschwindigkeit der Entwicklungen eine Momentaufnahme. Nichtsdestotrotz muss weiter der Versuch unternommen werden, die nach wie vor gesellschaftlich zentrale Institution der Polizei in ihren tatsächlichen Wirkweisen besser verstehen zu lernen,

1483 Vgl. etwa *Mokros,* Polizeiwissenschaft, S. 33 ff. et passim.

1484 Zu instruktiven empirischen Vorarbeiten siehe bereits oben S. 20 f.

1485 So bspw. *Brayne,* Predict and surveil, S. 4, die deshalb davon ausgeht, dass der wissenschaftliche, wie gesellschaftliche Diskurs insgesamt stark im Spekulativen verbleibt.

nicht zuletzt auch um polizeiliches Handeln demokratisch weiterhin regulieren zu können.

Die aus dieser Motivation in Form von Expert:inneninterviews mit polizeilichen Datenschutzbeauftragten durchgeführte empirische Untersuchung polizeilichen Informationshandelns soll nun im Folgenden in ihrem methodischen Zuschnitt erläutert und reflektiert werden.

I. Expert:inneninterviews als indizierte Methode

Expert:inneninterviews haben mitunter den Ruf, wissenschaftliche Informationsgewinnungsprozesse auf bequeme Weise abzukürzen. Forschungsökonomisch kann auf Expert:innen als „Kristallisationspunkte" relevanten Wissens zugegriffen werden, um so eigene, aufwändigere Datenerhebungsprozesse zu umgehen.[1486] Auch wenn forschungsökonomische Erwägungen nie ganz irrelevant sind, sollten sie die Methodenwahl nicht in erster Linie bestimmen, sodass die Frage nach der Indikation einer Methode für einen Forschungsgegenstand aufkommt. Hierbei muss, so beispielsweise *Steinke*, darauf geachtet werden, ob „mit den Methoden und deren Umsetzung den Äußerungen und Bedeutungssetzungen des Untersuchten hinsichtlich des Untersuchungsgegenstandes ausreichend Spielraum eingeräumt" wurde.[1487] Insofern ist es nötig, die Methode des Expert:inneninterviews und den Untersuchungsgegenstand – das polizeiliche Informationswesen – weiter zu konkretisieren.

Als Expert:in gilt generell eine Person, die „in irgendeiner Weise Verantwortung trägt für den Entwurf, die Implementierung oder die Kontrolle einer Problemlösung oder wer über einen privilegierten Zugang zu Informationen über Personengruppen oder Entscheidungsprozesse verfügt".[1488] Aufgrund der Durchsetzung der Gesellschaft mit Expert:innen – immer wieder macht die Rede von der Expertokratie die Runde – sind sie wissenschaftlich interessant, weil angenommen werden kann, dass ihr Wissen und ihre Handlungslogiken konstitutiv für den Ablauf moderner Gesellschaften sind.[1489] Insofern erhalten komplexe gesellschaftliche Felder, zu denen auch

1486 *Bogner/Littig/Menz,* Interviews mit Experten, S. 2.
1487 *Steinke* in Kuckartz/Grunenberg/Dresing (Hrsg.), Qualitative Datenanalyse: computergestützt, 176 (181).
1488 *Meuser/Nagel* in Bogner/Littig/Menz (Hrsg.), Das Experteninterview, 71 (73).
1489 *Bogner/Littig/Menz,* Interviews mit Experten, S. 4.

das der Polizei[1490] oder spezieller: der polizeilichen Informationsverarbeitung gehört, ihr jeweiliges Gepräge maßgeblich durch die in ihnen wirkenden, spezialisierten Akteur:innen.

Mit Blick auf das Volumen von Massendaten und die Technizität vieler Prozesse rund um polizeilichen Datenumgang ließe sich einwenden, eine quantitative Herangehensweise zur genauen Aufschlüsselung der Informationsbestände und der damit einhergehenden Abläufe sei adäquater, um Erkenntnisse über das polizeiliche Informationswesen zu gewinnen. Dem ist zuzugestehen, dass ein rein qualitativer Zugriff auf Dauer blinde Flecken aufweisen wird, die durch ergänzende quantitative Forschungsansätze beleuchtet werden müssen. Allerdings sind informationelles Handeln der Polizei und die an ihm Beteiligten und Betroffenen in einen gesellschaftlichen Diskurs eingebettet, der sich einem rein quantitativen Zugang nicht eröffnet. So ist etwa Datenschutz vor allem zunächst ein ideelles Konzept, das unterschiedlichen interpretativen Ansätzen zugänglich ist und erst dann praktisch umgesetzt werden kann. Expert:innen verfügen in diesem Diskurs über „institutionalisierte Kompetenz zur Konstruktion von Wirklichkeit"[1491] und bestimmen damit darüber, „aus welcher Perspektive und mithilfe welcher Begrifflichkeiten in der Gesellschaft über bestimmte Probleme nachgedacht wird."[1492] Um zu eruieren, in welchem Maße gesetzlich vorgeschriebene Konzepte von Datenschutz tatsächlich in die Rechtswirklichkeit transformiert werden, ist es also unabdingbar, die Perspektiven relevanter Akteur:innen in der Rechtsanwendung zu untersuchen.

Darüber hinaus fungieren die Apparaturen, die das polizeiliche Informationswesen technisch ausmachen, als sozio-technische Systeme, mit denen im Kontext der Organisation Polizei interagiert wird. Um die Integration von Informationstechnologien in polizeiliche Abläufe zu verstehen, müssen deshalb organisationale und auch kulturelle Strukturen der polizeilichen Institutionen untersucht werden.[1493] Auch diese Ebene lässt sich gut über Expert:innen erschließen, die mit einer „gewisse[n] Intersubjektivität […] Beurteilungen von Situationen, Positionen und Geschehnissen" vornehmen können.[1494]

1490 Zur Polizei als Feld bzw. Akteur in einem Feld im Bourdieuschen Sinne siehe *Brayne,* Predict and surveil, S. 139.

1491 *Hitzler/Honer/Maeder* (Hrsg.), Expertenwissen.

1492 *Bogner/Littig/Menz,* Interviews mit Experten, S. 15.

1493 So *Egbert/Leese,* Criminal futures, S. 3 für den speziellen, informationstechnologischen Fall des Predictive Policing.

1494 *Kaiser,* Qualitative Experteninterviews, S. 38.

Optimal wäre zugegebenermaßen ein noch breiteres qualitatives Vorgehen, wie es die wegweisenden Studien von *Brayne*[1495] für den US-amerikanischen Kontext oder auch von *Egbert und Leese*[1496] für den deutschen und schweizerischen Kontext vorgemacht haben: Dort wurden neben Interviews auch ethnografische Feldaufenthalte und Dokumentenanalysen in einem triangulierten Design zusammengebracht. Insbesondere die Feldforschung war in der vorliegenden Arbeit leider nicht möglich. Einerseits lag dies an der seit März 2020 andauernden Covid-Pandemie, die persönliche Kontakte von Angesicht zu Angesicht mit der Polizei, abgesehen von Videoanrufen, unmöglich machte. Darüber hinaus hätte aber auch der zeitliche Aufwand ein solches Vorhaben nicht erlaubt. Daneben wurden in der vorliegenden Untersuchung selbstverständlich auch Dokumente herangezogen. Ihre Auswertung und wissenschaftliche Nutzung erfolgte jedoch weniger systematisch als etwa bei *Egbert und Leese*, die auch die herangezogenen Dokumente qualitativ auswerteten. Für die vorliegende Arbeit wurden die Dokumente insbesondere zur thematischen Annäherung vor den Interviews, zur Strukturierung des Interviewleitfadens sowie teilweise zur Validierung von Interviewinhalten genutzt und sind insofern mit in die Anmerkungen eingeflossen.

II. Behördliche Datenschutzbeauftragte der Polizeien als Expert:innen

Als zu befragende Gruppe wurden die gesetzlich vorgeschriebenen behördlichen Datenschutzbeauftragten der Polizeien ausgewählt. Dies hatte mehrere Gründe.

Zunächst gab es forschungspragmatische Erwägungen: Behördliche Datenschutzbeauftragte werden im Rahmen der behördlichen Internetpräsenz mit Adressdaten und E-Mail-Adresse gesondert neben dem Präsidium genannt, welches als datenschutzrechtlich verantwortliche Stelle aufgeführt ist, wodurch die Kontaktaufnahme erleichtert wird, da von vornherein Ansprechpersonen vorhanden sind. Darüber hinaus üben behördliche Datenschutzbeauftragte einen Beruf aus, der prinzipiell einen erheblichen kommunikativen Teil beinhaltet, denn sie sind sowohl für Bürger:innen als auch für verschiedene polizeiliche und nicht-polizeiliche Akteure, wie die Aufsichtsbehörden, Kontaktpersonen. Zwar kann eine gewisse kommu-

1495 *Brayne,* Predict and surveil, S. 7 ff.
1496 *Egbert/Leese,* Criminal futures, S. 8 f.

nikative Versiertheit auch hinderlich für Expert:inneninterviews sein, aber für die vorliegende Untersuchung wurde die Zugänglichkeit der polizeilichen Datenschutzbeauftragten als Möglichkeit gesehen, den Feldzugang zu polizeilichen Organisationen zu erleichtern.

Der eben erwähnte Kontakt polizeilicher Datenschutzbeauftragter mit verschiedensten Beteiligten an und auch mit Betroffenen von polizeilichem Informationshandeln deutet zugleich auch auf den zentralen inhaltlichen Grund für ihre Auswahl als Interview-Partner:innen hin: Sie sind aufgrund ihrer gesetzlichen vorgeschriebenen Stellung Schlüsselfiguren im komplexen polizeilichen Informationswesen.[1497] Datenschutzbeauftragte müssen neben einer entsprechenden Qualifikation vor allem „Fachwissen […] auf dem Gebiet des Datenschutzrechts und der Datenschutzpraxis" besitzen. Zudem verlangt das Aufgabespektrum, wie es in Art. 34 JI-Richtlinie festgelegt ist, von ihnen eine sehr breite, interdisziplinäre Auseinandersetzung mit dem polizeilichen Informationswesen in seiner Gänze. Neben der Unterrichtung und Beratung des Verantwortlichen und der Beschäftigten, die Verarbeitungen durchführen, hinsichtlich ihrer datenschutzrechtlichen Pflichten und der Zusammenarbeit mit der Aufsichtsbehörde sind polizeiliche Datenschutzbeauftrage vor allem über ihre Konsultation bei erforderlichen Datenschutz-Folgeabschätzungen und ihre Überwachungsfunktion sehr stark in organisatorische Strukturen und Prozesse involviert, die maßgeblich über die Ausrichtung polizeilichen Informationshandelns mitbestimmen, wie beispielsweise auch in der Möglichkeit zur „Zuweisung von Zuständigkeiten" zum Ausdruck kommt (Art. 34 b) JI-Richtlinie). Schließlich ermöglicht diese Tätigkeit am Querschnitt des polizeilichen Informationswesens den behördlichen Datenschutzbeauftragten auch einen tiefgehenden Einblick in die Berufskultur, denn die Beauftragten müssen auch die ihnen anheimfallende Aufgabe der „Sensibilisierung und Schulung der an Verarbeitungsvorgängen beteiligten Mitarbeiter" (Art. 34 b) JI-Richtlinie) erfüllen.[1498]

1497 Siehe dazu und zum Folgenden bereits oben S. 362 ff.

1498 Hier wird die JI-Richtlinie zitiert, weil in ihr das normative Programm der behördlichen Datenschutzbeauftragten bei den Polizeien prägnant und zusammenhängend beschrieben wird. Auf eine Zitierung der jeweils in den Polizei- bzw. Datenschutzgesetzen festgelegten Aufgaben der Datenschutzbeauftragten wurde aus Gründen der Übersichtlichkeit verzichtet, wenngleich es hier Diskrepanzen zur JI-Richtlinie geben mag.

Insofern sind die polizeilichen Datenschutzbeauftragten als Teil der – beim Präsidium angesiedelten – polizeilichen „Funktionselite“[1499] aufgrund ihres Mitsprachrechts konstitutiv für das Funktionieren der modernen Gesellschaft im Bereich der Polizei, deren Tätigkeit zunehmend datenvermittelt erfolgt.[1500] Die Datenschutzbeauftragten bei den Polizeien sind auf diese Weise an der konkreten Ausformung und Aushandlung des gesellschaftlichen Werts und verfassungsrechtlichen Grundrechts der informationellen Selbstbestimmung beteiligt. Über ihre epistemische[1501] Beteiligung beeinflussen sie letztlich das (informationelle) Handeln der Polizei selbst und damit – für diese Untersuchung von Interesse – auch den Möglichkeitsraum der Polizei als gesellschaftliche Institution zur Produktion und Erhaltung von sozialer Ordnung sowie zur Ausübung von Sozialkontrolle.

III. Interviewkonzeption und Leitfadenkonstruktion

In einem nächsten Schritt mussten sodann die Interviews konzeptioniert und ein daran anknüpfender Leitfaden erstellt werden. Mit Blick auf die drei teilweise aufeinander aufbauenden Erkenntnisziele der weiteren Exploration des Informationshandelns und Informationswesens der Polizei, des organisations- und prozesssoziologischen Wissens über digitale Wandlungsprozesse innerhalb der Polizei sowie der Rechtswirklichkeit des polizeilichen Datenschutzrechts musste zunächst festgelegt werden, welche Wissenstypen im Rahmen des jeweiligen Ziels relevant sein würden.

Dafür wird vorliegend der Typologie von *Bogner et al.* gefolgt,[1502] die zwischen technischem Wissen („Daten, Fakten, „sachdienliche Informationen“, Tatsachen), Prozesswissen („Einsichten in Handlungsabläufe, Interaktionen, organisationale Konstellationen Ereignisse, usw., in die die Befragten involviert sind“) und Deutungswissen („subjektive Relevanzen,

1499 *Meuser/Nagel* in Hitzler/Honer/Maeder (Hrsg.), Expertenwissen, 180 (181).

1500 Instruktiv dazu die Analyse von *Egbert* in Hunold/Ruch (Hrsg.), Polizeiarbeit zwischen Praxishandeln und Rechtsordnung, 77.

1501 Zum Epistemischen und seiner Bedeutung für Realitätsproduktionen siehe *Knorr Cetina* in Kalthoff (Hrsg.), Theoretische Empirie, 35 (51 f., 59).

1502 Eine andere Typologie findet sich – eher für den politikwissenschaftlichen Kontext – bspw. bei *Kaiser,* Qualitative Experteninterviews, S. 44. Die dortige Einteilung ist jedoch für die vorliegende Untersuchung unpassend, da die beiden Typen des Betriebs- und Kontextwissens sich m.E. überschneiden und sie den mit der Kategorie des technischen Wissens beschriebenen Aspekten nicht hinreichend konzeptionellen Raum gibt.

Sichtweisen, Interpretationen, Deutungen, Sinnentwürfe und Erklärungsmuster der [Expert:innen]") unterscheidet.[1503] Im Rahmen des explorativen Erkenntnisziels lag der Fokus dabei auf technischem Wissen rund um die faktischen Aspekte des polizeilichen Informationswesens, wobei auch Prozesswissen von Interesse war, da auch über die Arbeitsabläufe von Datenschutzbeauftragten und ihre organisationale Einbindung in der Polizei quasi kaum Wissen vorliegt. Zur Generierung von organisations- und prozesssoziologischem Wissen über digitale Wandlungsprozesse innerhalb der Polizei war hingegen in erster Linie Prozesswissen sachdienlich. Aber auch Deutungswissen hinsichtlich der Bewertung der Befragten bezüglich der bestehenden und der sich wandelnden Prozesse sollte hier abgefragt werden, da Datenschutzbeauftragte, so die Annahme, als relevante Akteur:innen maßgeblich in derartige Prozesse in den Organisationen eingebunden sind. Zur Beleuchtung der Rechtswirklichkeit polizeilichen Datenschutzrechts war schließlich ebenfalls Deutungswissen von Interesse, da Rechtsanwendung immer auch ein Interpretations- und Deutungsprozess ist. Darüber hinaus war aber in diesem Rahmen auch technisches Wissen in Form von Tatsachen – beispielsweise: (wie) wird das Recht in bestimmten Fällen überhaupt angewendet? – und Prozesswissen – beispielsweise: in welchen Handlungsabläufen werden Normen in die Rechtswirklichkeit übersetzt? – bedeutend.

Dieser Interviewzuschnitt ist also nicht auf die Erhebung von einem Wissenstyp fokussiert und lässt sich damit nicht in Typologien einfügen, die sich in der Literatur finden, sondern ist zwischen den klassischen Formen von Expert:inneninterviews (explorativ oder fundierend, informatorisch oder deutungswissensorientiert) situiert und nimmt je nach Erkenntnisziel Anleihen bei den Strukturen dieser typischen Interviewformen.[1504]

Um alle relevanten Aspekte mit Fragen abzudecken, wurde eine Teil-Strukturierung der Gespräche mittels Interviewleitfaden vorgenommen. Dementsprechend enthält der Interviewleitfaden unterschiedliche Fragetypen, um die verschiedenen Wissenstypen und Felder abzudecken, und ist nach folgenden Bereichen gegliedert:[1505] Nach den beiden Einleitungsfragen zu beruflichem Werdegang und typisch anfallenden Aufgaben ging es im zweiten Fragenkomplex um die Stellung der jeweils befragten Datenschutzbeauftragten in ihrer Behörde sowie um ihre Beziehung mit polizeili-

1503 *Bogner/Littig/Menz,* Interviews mit Experten, S. 17 ff.
1504 Vgl. dazu die Einteilung bei *Bogner/Littig/Menz,* Interviews mit Experten, S. 23.
1505 Der Leitfaden findet sich im Anhang.

chen aber auch nicht-polizeilichen Akteur:innen[1506] in ihrem Tätigkeitsbereich. Hier sollte vor allem Prozesswissen, aber auch technisches Wissen freigelegt werden. Der dritte Fragekomplex war demgegenüber stärker auf die inhaltliche Arbeit der polizeilichen Datenschutzbeauftragten gerichtet, auch hier waren technisches Wissen und Prozesswissen von Interesse. Mit einem Fokus auf die Anwendung von Rechtsnormen sollte allerdings auch Deutungswissen angesprochen werden. Im vierten und letzten Fragekomplex ging es um Chancen und Risiken im polizeilichen Informationswesen, insbesondere aus datenschutzrechtlicher Perspektive. Hier ging es vorrangig um Deutungswissen, da vor allem laufende Entwicklungen mit offenen Fragen thematisiert wurden. Die vorherige Strukturierung durch einen Leitfaden sollte zudem die bessere Vergleichbarkeit der Interviews in der späteren Auswertung ermöglichen. Gleichzeitig sollte aber dem qualitativen Forschungsideal entsprechend auch die Offenheit der Gesprächssituationen gewahrt bleiben, was neben offenen Erzählaufforderungen zu bestimmten thematischen Aspekten auch durch nicht im Leitfaden enthaltene, öffnende Nachfragen aus den jeweiligen Gesprächssituationen heraus erzielt werden sollte. Auf einen Pretest wurde aufgrund der Erwartung einer nicht allzu großen Sample-Größe verzichtet. Der Leitfaden wurde aber hinsichtlich Struktur und Konsistenz durch Dritte kritisch geprüft.

Die Erkenntnisziele wurden in den Fragekomplexen verschiedentlich betont: Während der offene Charakter vieler Fragen dem Ziel der Exploration in der gesamten Interviewkonzeption viel Raum gibt, ging es vor allem im zweiten und vierten Fragekomplex um die Generierung von organisations- und prozesssoziologischem Wissen über Wandlungsprozesse anlässlich der Digitalisierung der Polizei. Die Rechtswirklichkeit polizeilichen Datenschutzes sollte daneben vor allem mittels der Fragekomplexe drei und ebenfalls vier vermessen werden.

IV. Rahmenbedingungen der Interviews

Die Interviews wurden größtenteils parallel zur Ausarbeitung der übrigen Teile der vorliegenden Untersuchung durchgeführt, im Zeitraum von März 2020 bis Ende 2021. Zur Akquise der Interviewpartner:innen wurden behördliche Datenschutzbeauftragte in allen Bundesländern über die zu-

1506 Hier wurde explizit nur nach der Beziehung zur jeweiligen Aufsichtsbehörde, d.h. den Landesdatenschutzbeauftragten, gefragt.

meist auf dem Internetauftritt der jeweiligen Polizeibehörde verfügbaren E-Mail-Adressen kontaktiert. Insgesamt wurden 15 Interviews mit behördlichen Datenschutzbeauftragten aus 10 Bundesländern durchgeführt. Mit Datenschutzbeauftragten aus Polizeibehörden der Bundesebene wurde ein Interview durchgeführt. Einige Male war es zur Herstellung der Gesprächsbereitschaft der Interviewpartner:innen nötig, vorab den Leitfaden zur Durchsicht zuzusenden, was eine gewisse Vorbereitung der Interviewten im Vorfeld der Interviews nahelegt. Lediglich einmal ist es jedoch zu einem Interview gekommen, in dem vorbereitete Antworten auf die jeweiligen Fragen vorgetragen wurden. Auch in diesem Fall wurde die Gesprächssituation jedoch mittels nicht im Leitfaden aufgeführter Fragen in ein natürlicheres Gespräch überführt.

Die Interviews wurden – vor allem der erwähnten Pandemie-Situation geschuldet – telefonisch durchgeführt. Vereinbart waren stets einstündige Interviews, die jedoch im Schnitt etwa anderthalb Stunden dauerten. Gesprochen wurde unter Vereinbarung von Anonymität, wozu die Interviews an Stellen mit zu starkem Personenbezug – etwa im Rahmen des beruflichen Werdegangs – abgeändert wurden. Die Interviews wurden aufgezeichnet und im Anschluss eigenhändig transkribiert. Die Transkription erfolgte dabei wortwörtlich, ohne jedoch Dialekte oder Fülllaute oder ähnliches in das Transkript zu übernehmen.[1507] Nach der Fertigstellung der Transkripte wurden diese zur Einhaltung eines angemessenen Anonymisierungsniveaus zur Durchsicht an die Interviewten gesendet. In diesem Rahmen wurden auch im Rahmen der Transkription aufgekommene Nachfragen in Form von Kommentaren im jeweiligen Dokument formuliert. Bei der Durchsicht der Transkripte durch die Interviewpartmer:innen wurden von diesen vereinzelt inhaltliche Korrekturen an Stellen angemerkt, an denen sich die Partner:innen missverstanden fühlten. Diese Anmerkungen wurden ins Transkript unter entsprechender Kennzeichnung aufgenommen.

V. Auswertung der Interviews

Die Interviews wurden computergestützt unter Zuhilfenahme der MAXQDA-Software ausgewertet.[1508] Dies war notwendig, da im Rahmen der

1507 Es wurde sich im Wesentlichen an den Regeln von *Rädiker/Kuckartz,* Analyse qualitativer Daten mit MAXQDA, S. 44 f. orientiert.

1508 *Rädiker/Kuckartz,* Analyse qualitativer Daten mit MAXQDA.

Expert:inneninterviews durch die Offenheit im Rahmen der Leitfadenstruktur zunächst erwartungsgemäß viel Datenmaterial angefallen war, das relativ unstrukturiert war. Nichtsdestotrotz wurde die Codierung nicht vollständig im Sinne des klassischen Grounded Theory-Ansatzes ad hoc aus dem Datenmaterial entwickelt,[1509] denn aufgrund der vorangegangenen Teil-Strukturierung der Interviews auf Grundlage der theoretischen und rechtswissenschaftlichen Vorarbeiten waren einige Codes für die qualitative Auswertung bis zu einem gewissen Grad naheliegenderweise anzuwenden. Insofern erfolgte methodologisch eine Anlehnung an die qualitative Inhaltsanalyse nach Mayring in Form der Strukturierung.[1510] Vor allem der explorative Gehalt des Untersuchungsdesigns hatte jedoch auch Aussagen in den Interviews produziert, die sich nicht in die bereits zuvor lose durchgeführte Kategorienbildung einfügen ließen. Deshalb erfolgte eine Ergänzung und Verfeinerung der Code-Struktur unter dem Einfluss der induktiven Grounded Theory-Methodologie.[1511] Auch diese iterativen Ausdifferenzierungen der Code-Struktur waren jedoch nicht völlig von theoretischen und rechtswissenschaftlichen Vorarbeiten und -überlegungen abgekoppelt. Mit *Strübing* wird also das Theorie-Empirie-Verhältnis im Rahmen der Grounded Theory nicht „in einem Konkurrenz-, sondern in einem Komplementärverhältnis" stehend gesehen,[1512] womit eine Absage an ein rein induktivistisches Vorgehen verbunden ist.

Auf diese Weise wurde ein in 17 Codes differenziertes Kategoriensystem geschaffen, innerhalb dessen zwei Codes noch Untercodes (einmal vier Untercodes, einmal zwei Untercodes) haben. Insgesamt wurden 1308 Textsegmente im Datenmaterial codiert. Zusätzlich wurden viele Codesegmente zur weiteren Kontextualisierung, Einordnung und Anreicherung mit Memos versehen. Nach Abschluss der Codierung des Datenmaterials erfolgte eine je codespezifische Zusammenschau der jeweils mit einem Code versehenen Elemente. Im Rahmen dieser codespezifischen Sichtung wurden die so zusammengestellten Elemente zunächst theoriegeleitet und konzeptuell geordnet. Sodann wurden die einzelnen Codes thematischen Kapiteln für die schriftliche Ausarbeitung der Auswertung zugeordnet. Es folgte die Anordnung der Kapitel und die schriftliche Ausarbeitung, in deren Rahmen

1509 Vgl. etwa *Kelle* in Kuckartz/Grunenberg/Dresing (Hrsg.), Qualitative Datenanalyse: computergestützt, 32 (40).

1510 *Mayring,* Qualitative Inhaltsanalyse.

1511 *Glaser/Strauss,* The discovery of grounded theory; *Strauss/Corbin,* Basics of qualitative research.

1512 *Strübing* in Kalthoff (Hrsg.), Theoretische Empirie, 282 (308).

eine weitere Anreicherung und weitere Abgleiche mit themenverwandten Studien und theoretischen Überlegungen durchgeführt wurden.

VI. Reflexionen

Da die „Qualität qualitativer Forschung jenseits dessen liegt, was in eindeutige Kriterien gefasst werden kann",[1513] soll neben der vorstehenden Dokumentation des methodischen Vorgehens in einem abschließenden Schritt über potentielle Schwächen des Forschungsdesigns reflektiert werden.[1514]

Zunächst lässt sich im Nachhinein über die gewählte Methode der Expert:inneninterviews nachdenken. Während diese Methode durchaus verbreitet in der Sozialforschung zu polizeilicher Informationsverarbeitung ist, zeigt ein Blick auf jüngere Studien, dass auch Feldaufenthalte in Form von teilnehmenden bzw. ethnografischen Beobachtungen einen großen Erkenntnisgewinn in Gestalt von wertvollen Einblicken in die tatsächliche Informationsarbeit verschiedener Rollenträger:innen in den Polizeien geben können.[1515] Zwar sind die zitierten Studien in ihrem primären Erkenntnisinteresse und Hintergrund vorrangig soziologischer Natur. Aber neben dem Umstand, dass auch die vorliegende Arbeit keineswegs ein rein rechtswissenschaftliches Interesse verfolgt, ist auch von großem rechtlichem Interesse, wie mit polizeilichen Datenverarbeitungstechnologien in Aktion umgegangen wird. Dies konnte indessen nur implizit aus einigen Aussagen der Interviewpartner:innen gefiltert werden. Insofern traf die eingesetzte Methode das Erkenntnisziel partiell nicht in optimaler Weise. Im Rahmen des vorliegenden (nicht drittmittelfinanzierten) Projekts, das zudem polizeiliche Kontakte erst aufbauen musste, war eine solche tiefgehende empirische Untersuchung – auch neben den anderen Bearbeitungsaspekten – allerdings nicht zu leisten.

Denkbar wäre es zudem gewesen, insgesamt eine größere Varietät von polizeilichen Akteur:innen mit ins Forschungsdesign einzubeziehen. Auch hier war die Akquise von Gesprächspartner:innen allerdings ohne vorheri-

1513 *Flick* in Kuckartz/Grunenberg/Dresing (Hrsg.), Qualitative Datenanalyse: computergestützt, 188 (204).

1514 *Grunenberg* in Kuckartz/Grunenberg/Dresing (Hrsg.), Qualitative Datenanalyse: computergestützt, 210 (219 f.).

1515 *Brayne,* Predict and surveil; *Egbert/Leese,* Criminal futures.

ge Kontakte nicht leicht.[1516] Zudem wird dieses Manko dadurch relativiert, dass die befragten Datenschutzbeauftragten alle zuvor in anderen Verwendungen in den Polizeien tätig waren, sodass insoweit auch auf selbst erlebte oder bekannte Rollendynamiken außerhalb der Position von behördlichen Datenschutzbeauftragten zugegriffen werden konnte.

Die Akquise der Interviewpartner:innen ist insgesamt recht zufriedenstellend verlaufen. Nichtsdestotrotz hätte die Anzahl der letztlich interviewten Datenschutzbeauftragten idealerweise höher sein können. Dies wurde allerdings durch die Absage einiger Bundesländer in Gänze sowie durch teilweise interne Koordinierung einiger Länderpolizeien mit der Bestimmung einer zentralen Ansprechperson für das Interview im Land verunmöglicht. Es wurden alle Länderpolizeien und Bundespolizeibehörden angefragt, sodass insoweit eine Ausschöpfung der Möglichkeiten erfolgt ist.

Da sich im Laufe der Interviewdurchführung zeigte, dass einige Fragen keinen weiteren Erkenntnisgewinn mehr mit sich brachten, wurden einige Fragen im Leitfaden modifiziert, ohne jedoch die übergeordnete Gliederung der Fragekomplexe und deren grundlegende thematische Ausrichtung aufzugeben. Wenn Besonderheiten des polizeilichen Informationswesens im Zuständigkeitsbereich einer zu befragenden Polizeibehörde bekannt waren, wurden zudem gesonderte Fragen zu diesen Aspekten eingefügt. Diese Schritte geht sicherlich etwas zu Lasten der Vergleichbarkeit der durchgeführten Interviews, schienen aber dennoch methodisch sinnvoll, einerseits um nicht zu viel redundantes Wissen zu generieren und andererseits um der partiell explorativen, induktiven Vorgehensweise gerecht zu werden, indem aufbauend auf neuen Erkenntnissen weitere Aspekte von Interesse ins Forschungsdesign mit eingeschlossen wurden.

Trotz aller Bemühungen, sich der polizeilichen Informationsverarbeitung empirisch zu nähern, sie zu vermessen und vielleicht sogar zu erfassen, sind die soziologische Forschung insgesamt kaum und einzelne Untersuchungen umso weniger in der Lage, ein vollständiges Bild der

1516 Zu einem fortgeschrittenen Zeitpunkt der Interviewdurchführung konnte über Kontakte mit einem interviewten Datenschutzbeauftragten zudem eine Person für ein Interview gewonnen werden, die im Rahmen der technischen Verwirklichung polizeilicher Informationsverarbeitung bei einem Landeskriminalamt in zentraler Stellung beschäftigt war. Diese Art der sekundären Akquise von Interviewpartner:innen wäre für das oben angesprochene breitere Forschungsdesign passend gewesen, konnte jedoch aus zeitlichen Gründen nicht umfassend durchgeführt werden.

(Rechts)Wirklichkeit des polizeilichen Informationswesens zu liefern. *Brayne* fasst es – für den US-amerikanischen Kontext – so zusammen:

> „No matter how quickly empirical research emerges, the technological capacities for data-intensive surveillance far outpace scholarship. Consequently, much discourse on the topic is speculative, focusing on the possibilities, good and bad, of new forms of data-based surveillance. We know very little about how big data is actually used by police in practice – and to what consequence."[1517]

So ist dann auch Vieles der vorliegenden Studie „nur" eine Interpretation von Aussagen aus den deutschen Polizeien auf Grundlage vertiefter Kenntnisse des akademischen Wissensstandes. Eine weitere und vor allem stetige Aufhellung der polizeilichen Informationsverarbeitung ist vor diesem Hintergrund aber jedenfalls geboten. Auch wenn die folgenden Darstellungen nur ein bruchstückhaftes Mosaikbild des polizeilichen Informationswesens und der in ihm stattfindenden Prozesse und Informationspraktiken rekonstruieren kann, ist es hoffentlich dennoch geeignet, einige Schattierungen und Undurchsichtigkeiten im Verständnis des untersuchten Feldes aufzuhellen.

B. Rekonstruktion des polizeilichen Informationswesens

I. Die Datenschutzbeauftragten der deutschen Polizeien: Werdegänge, Situationen, Selbstverständnisse

Obwohl die Berufsbezeichnung des behördlichen Datenschutzbeauftragten bei der Polizei ein homogenes Berufsbild vermuten lässt, wird die Position mitunter von Organisationstyp (also etwa Landeskriminalamt, Polizeipräsidium, Polizeidirektion, usw.) zu Organisationstyp und von Land zu Land sehr unterschiedlich ausgestaltet. Neben den unterschiedlichen Anforderungen, die unterschiedliche polizeiliche Organisationstypen an die Gestaltung des Datenschutzes bei sich im Hause haben, liegt ein wesentlicher Grund dafür in der Stellung der Datenschutzbeauftragten selbst. Anders als viele Verwendungen in der Polizei ist die Position weniger mit den herkömmlichen Laufbahnen verknüpft und wird kaum als

1517 *Brayne,* Predict and surveil, S. 4.

Karriereziel anvisiert.[1518] Im Wesentlichen scheint dies darauf zurückzugehen, dass der Position der polizeilichen Datenschutzbeauftragten erst seit der EU-Datenschutzreform von 2016 eine Bedeutung zukommt, die sich auch stärker in der Organisationsstruktur der Polizei materialisiert. Zwar gab es bereits zuvor Datenschutzbeauftragte bei den Polizeien, meistens allerdings handelte es sich dabei um eine Teilzeittätigkeit im Nebenamt oder um eine Teilaufgabe des Justiziariats. Trotz der Aufwertung durch die europäischen Rechtsakte ist die Herausbildung eines klaren Berufsbildes noch im Fluss – insbesondere in seiner polizeibehördlichen Ausformung, was sich in erster Linie in der Heterogenität der Werdegänge zeigt: Während sich diese noch grob in polizeiliche (etwas mehr als die Hälfte der Befragten[1519]), juristische (etwas weniger als ein Drittel der Befragten[1520]) und sonstige Laufbahnen[1521] einteilen lässt, ist eine feinere Systematisierung kaum möglich, zu unterschiedlich sind die vorherigen Bildungs- und Tätigkeitsbiografien, die von Kriminologie[1522] über Ingenieursinformatik[1523] bis hin zur Leitung eines großstädtischen Spezialdezernats[1524] reichen. Drei der 15 interviewten Personen waren Frauen. Kaum eine befragte Person war von vornherein oder kurz nach Beginn ihrer Karriere mit Datenschutzfragen beschäftigt.[1525] Die Mehrheit der Datenschutzbeauftragten bei den deutschen Polizeien hat vor ihrer Ernennung vielmehr jahrelang in anderen, häufig auch stark wechselnden Verwendungen gearbeitet. Allen Befragten gemein war indessen ihre berufliche Verbundenheit mit der Polizei. Nur eine Person – mit verwaltungsjuristischem Hintergrund – kam ohne längere Beschäftigung bei einer Polizei zum behördlichen Datenschutz.[1526] Aber auch die Verwendungen bei den Polizeien unterscheiden sich mitun-

1518 In keinem der geführten Interviews wurde davon berichtet, dass die Position der/des Datenschutzbeauftragte/n schon in einem früheren Karrierestadium als Karriereziel oder -station ins Auge gefasst wurde, was eine solche Karriereplanung indessen auch nicht ausschließt; sie scheint aber zumindest ungewöhnlich zu sein.

1519 Interview 1, Pos. 24; Interview 3, Pos. 6; Interview 4; Pos. 6-7; Interview 8, Pos. 7; Interview 9, Pos. 6, 24; Interview 10, Pos. 6; Interview 11, Pos. 9, 11.

1520 Interview 2, Pos. 30; Interview 5, Pos. 6; Interview 7, Pos. 8; Interview 12, Pos. 6; Interview 15.

1521 Interview 13, Pos. 6; Interview 14, Pos. 6.

1522 Interview 1, Pos. 24.

1523 Interview 4, Pos. 6.

1524 Interview 9, Pos. 6.

1525 Lediglich der in Interview 5 Befragte war nach einer kurzen Station in der Justiz beim Landesdatschutzbeauftragten und danach bei der Polizei mit Datenschutzsachen beschäftigt.

1526 Interview 2, Pos. 30.

ter stark, und bilden eher die Breite polizeilicher Aufgabenfelder ab, als dass hier eine bestimmte Beschäftigtenklasse der Polizei klar herausstechen würde. Mit Blick auf die wenigen Gemeinsamkeiten scheint es für behördliche Datenschutzbeauftragte bei den deutschen Polizeien bezüglich ihres Werdegangs also vor allem auf einen Faktor anzukommen:

> „Das Wort, das ich mir hier zu ihrer Frage [zum Werdegang] notiert habe, lautet: Zufall!"[1527]

Auch nach Ernennung scheint es bisher wenig, an einem klaren Berufsbild orientierte Regeln über den weiteren Werdegang der polizeilichen Datenschutzbeauftragten zu geben. Während einige Male auch von einem Wechsel in eine anschließend andere Funktion berichtet wurde[1528] – etwa ins Innenministerium des Landes[1529] oder in eine andere Verwendung innerhalb der Polizei[1530] – scheint ein nicht unerheblicher Teil die Stelle der oder des Datenschutzbeauftragten bis zum Ruhestand oder zumindest ohne klares weiteres Karriereziel auszuführen. Diese etwas wenig institutionalisierte Einbindung der Stellung spiegelt sich auch im berufsinternen Möglichkeitsfeld bezogen auf Qualifizierungs- und Weiterbildungsmaßnahmen der Datenschutzbeauftragten wider. So wird etwa von Schwierigkeiten betreffend die weitere Qualifizierung nach Berufung als Datenschutzbeauftragte:r berichtet:

> „Das ist relativ schwierig im internen Bereich sowas zu bekommen. Das sind häufig dann Dinge, also ich habe meine Fortbildung, die mache ich meistens extern. Also da schaue ich auf dem Markt der Fortbildungen, da schaue ich, was es dort gibt. Gerade für den, ich sag mal, für behördliche Datenschutzbeauftragte ist das Angebot eher klein der sonstigen Anbieter für Fortbildungen. Da richten sich viele an die betrieblichen Datenschutzbeauftragten. Also was die materiellen Rechtmäßigkeitsanforderungen angeht. Wobei die da mit der DSGVO auch mittlerweile ziemlich einheitlich sind, zumindest in Teilen. Für die JI-Richtlinie gibt es wenig. Und was die Technik angeht, da muss man tatsächlich auf dem Markt draußen eher schauen."[1531]

1527 Interview 9, Pos. 6.
1528 Berichtet wurde dies über diejenigen Personen, die jeweils die Stelle vor den Interviewten innehatten.
1529 Interview 4, Pos. 6.
1530 Interview 2, Pos. 30.
1531 Interview 1, Pos. 47.

Allerdings handelt es sich dabei nicht um einen universellen Zustand im polizeilichen Datenschutz. In einigen Ländern gibt es beispielsweise bereits polizei- oder zumindest landesverwaltungsinterne Fortbildungsangebote, die eine weitere Institutionalisierung der Position des Datenschutzbeauftragten vorantreiben.[1532] Darüber hinaus gibt es mitunter auch Anbindungen an den wissenschaftlichen Hochschulbetrieb zur Weiterbildung und Qualifizierung,[1533] was in einem auch stark rechtsdogmatisch geprägten Bereich wie dem Datenschutzrecht angemessen erscheint. Nichtsdestotrotz bleibt es für nicht juristisch ausgebildete Datenschutzbeauftragte nicht aus, einen gewissen Teil des benötigten Fachwissens über das autodidaktische Studium der Rechtsmaterie zu erlernen.[1534]

In diesen unterschiedlichen Ausgangsvoraussetzungen der polizeilichen Datenschutzbeauftragten zeigt sich auch einmal mehr ein für die deutsche Polizeilandschaft generell bezeichnendes Charakteristikum: Die vor allem durch den Föderalismus bedingte strukturelle Divergenz der deutschen Polizeien, die sich grundsätzlich in vielen Landesverwaltungszweigen bemerkbar macht, aber vor allem über das jeweils landeseigene Polizeirecht und die damit verbundenen historisch gewachsenen Besonderheiten der einzelnen Polizeien besonders sichtbar hervortritt. So verwundert es dann auch wenig, dass die beruflichen Selbstverständnisse der polizeilichen Datenschutzbeauftragten eher heterogen ausfallen.

Wie es dem gesetzlichen Leitbild entspricht, haben sich in den Interviews die Beratungs- und die Überwachungsfunktion als zentrale Bausteine des professionellen Selbstbildnisses der Datenschutzbeauftragten herausgestellt. So wird etwa betont, die „Idealvorstellung" sei jemand, „der wirklich weisungsfrei seine Aufgaben wahrnimmt, mit dem Schwerpunkt auf einer Überwachungsaufgabe."[1535] Vor allem für diejenigen Datenschutzbeauftragten, die zuvor in genuin polizeilichen Bereichen gearbeitet haben, kann sich aus dieser Überwachungsaufgabe ein Dilemma ergeben, weil datenschutzrechtliche Belange mit der eigenen Vorstellung von Notwendigkeiten der Polizeiarbeit konfligieren können.[1536] Zwar wird häufig der prinzipielle Wert von einem überwachendem Datenschutz gesehen, aber es schwingt durchaus auch eine Sorge für eine weiterhin effektive polizeiliche

1532 Interview 7, Pos. 8.
1533 Interview 11, Pos. 9.
1534 Interview 9, Pos. 26.
1535 Interview 1, Pos. 28.
1536 Interview 3, Pos. 56.

Aufgabenerfüllung mit, wenn etwa die Anwendung der für Bürger:innen verfügbaren Instrumente des Datenschutzes als missbräuchlich empfunden wird.[1537] Dennoch wird die Überwachungsfunktion von denjenigen, die sie als eine ihrer zentralen Aufgaben ansehen, durchaus in offensiver Weise praktiziert, was auch Konfliktpotenzial mit sich bringt:

> „Der Datenschützer ist der, der mittags alleine in der Kantine sitzt, also so diese Reaktionen, die hatte ich auch schon. Vor denen darf man natürlich in dem Job keine Angst haben."[1538]

Eher entfernt von dem Bild der Überwachung der Polizei durch Datenschutzbeauftragte ist hingegen ein Verständnis von Datenschutz, in dem es vorrangig um den rechtlich reibungslosen Ablauf der Datenverarbeitung geht und Irregularitäten eher durch Bürgerbeschwerden an die Polizei herangetragen werden.[1539] Nichtsdestotrotz hat auch ein solches Selbstverständnis von polizeilichem Datenschutz, in dem die Funktion als „beratende[s] Organ"[1540] stärker in den Vordergrund gerückt wird, letztlich eine Grundlage im Gesetz. Zudem ist es sicherlich für die Aufgabenerfüllung der Datenschutzbeauftragten bei den Polizeien nicht unerheblich, zumindest auch „Ansprechpartner und Berater [zu] sein und nicht als Feind im eigenen Nest betrachtet [zu] werden",[1541] wenngleich diese Formulierung auch bereits auf Problemzonen des Verhältnisses der Polizei zum Konzept und der Praxis des Datenschutzes hindeutet.[1542] Auch bei denjenigen, die sich hauptsächlich in einer die polizeiliche Informationsverarbeitung überwachenden Funktion sehen, gibt es eine gleichzeitige Betonung der Beratungsfunktion, da man „ja immer nur die Möglichkeit [habe, …] Vorschläge zu machen oder auch auf Risiken hinzuweisen."[1543] Die Beratungsfunktion spielt vor allem auch dort eine Rolle, wo es den Datenschutzbeauftragten in erster Linie darum geht, die Praxis mit den datenschutzrechtlichen Vorgaben zusammenzubringen, also nicht nur konfrontativ zu überwachen, sondern über ein kooperatives Verhältnis zu den operativ arbeitenden Poli-

1537 Interview 4, Pos. 24, 49. Es ging hierbei um eine wohl systematische und flächendeckende Nutzung von Auskunftsanfragen bei einer Landespolizei.
1538 Interview 9, Pos. 18
1539 Interview 7, Pos. 46.
1540 Interview 10, Pos. 26.
1541 Interview 12, Pos. 18.
1542 Siehe näher dazu unten S. 424 ff.
1543 Interview 1, Pos. 28.

zeieinheiten zu einer sinnvollen Verbindung von Datenschutz und polizeilicher Praxis zu kommen.[1544]

Unabhängig von der konkreten Ausprägung, also ob eher überwachend oder eher beratend, ist die Position der oder des Datenschutzbeauftragten im Verständnis der Befragten vor allem auch eine interdisziplinär anspruchsvolle Querschnittstätigkeit – sie ist „sehr mannigfaltig und erstreckt sich auf die unterschiedlichsten Aufgabengebiete."[1545] Zwar gibt es abhängig vor allem von der Ebene, auf der die jeweils von den Datenschutzbeauftragten zu überwachende oder zu beratende Polizeiorganisation angesiedelt ist, unterschiedliche Bedürfnisgrade für die strategische Weitsicht, die für die jeweils zu erledigenden Aufgaben erforderlich ist.[1546] Allerdings müssen die Datenschutzbeauftragten auf allen Ebenen stets rechtliche Vorgaben, technische Gegebenheiten und Pläne sowie polizeiliche Fachlichkeit in Einklang bringen. Insofern ist auch das Selbstverständnis als vermittelnde Instanz präsent, die komplexe polizeiliche Prozesse und Informationstechnik nach normativen Vorgaben miteinander verzahnen muss.[1547]

II. Die Aufgaben der Datenschutzbeauftragten in ihrer Selbstbeschreibung

Diese Verzahnung, die im Idealfall die normativen Vorgaben des Datenschutzrechts Rechtswirklichkeit werden lässt, hängt in der datenschutzrechtlichen Praxis ganz wesentlich davon ab, wie die Datenschutzbeauftragten und die Polizeiorganisation, in der sie tätig sind, ihren Aufgabenbereich sehen und organisiert haben. In den Interviews zur Sprache gekommen sind insbesondere die bereits erwähnten Aufgabenbereiche der Beratung, der Überwachung bzw. Kontrolle sowie der Schulung und Sensibilisierung. Alle Bereiche unterscheiden sich in ihrer konkreten Ausgestaltung merklich voneinander.

1544 Interview 9, Pos. 40, 72.
1545 Interview 10, Pos. 20.
1546 So ist etwa in einigen Polizeien die Tätigkeit der Befragten auf konkrete, eher abgegrenzte Rechtsfälle und -fragen begrenzt, ohne dabei ein wirklich vorausschauendes, ein größeres Bild im Blick habendes strategisch-planerisches Moment zu enthalten, Interview 13, Pos. 105; Interview 7, Pos. 56.
1547 Interview 4, Pos. 7; Interview 9, Pos. 72; Interview 12, Pos. 26; Interview 14, Pos. 14, 92.

1. Beratung

Zentrale Hauptaufgabe für alle Befragten war die Beratung der polizeilichen Organisationseinheiten in allen aufkommenden datenschutzrechtlichen Fragen.[1548] Die Datenschutzbeauftragten sind „dabei im Wesentlichen eine zentrale Servicestelle."[1549] Je nach Zuständigkeit wird auch überregional beraten,[1550] immer besteht aber im jeweiligen Zuständigkeitsbereich Beratungsverantwortlichkeit für die jeweiligen datenschutzrelevanten Ausprägungen des polizeilichen Informationswesens, wozu spezielle Anwendungen, wie auch immer organisierte Datenbestände und alle sonstigen Datenverarbeitungsvorgänge gehören.[1551] Im Kontakt der Datenschutzbeauftragten mit den operativ arbeitenden Polizeiorganisationsteilen ist die Beratung grundsätzlich der Ausgangspunkt, denn „Kontrolle steht ja ganz am Ende von allem."[1552]

Die Beratung erfolgt dabei zumeist in konkreten und teilweise eher speziellen rechtlichen Fragestellungen zur Strafverfolgung und Gefahrenabwehr.[1553] Themen sind beispielsweise die Weitergabe von Daten an nichtpolizeiliche Stellen bei Unsicherheit der Beamt:innen,[1554] die Nutzung von Corona-Listen zu Strafverfolgungszwecken,[1555] die Regelung von datenschutzrechtlichen Verhältnissen zwischen den einzelnen Polizeibehörden, etwa einem Landeskriminalamt und dem Bundeskriminalamt,[1556] oder auch der Einsatz von auf künstlicher Intelligenz basierenden Datenverarbeitungsverfahren in der jeweiligen Polizeibehörde.[1557] Neben diesen konkreten Fragestellungen müssen die Datenschutzbeauftragten aber auch stärker konzeptuell ausgerichtete Aufgaben umsetzen. Ein Thema, das in diesem Zusammenhang alle Befragten in den letzten Jahren und bis in die Gegenwart hinein beschäftigt hat, ist zum Beispiel die Umsetzung von neuen Landesdatenschutz- und Landespolizeigesetzen, also die Einarbeitung der Vorgaben auf allen Ebenen der polizeilichen Arbeitsabläufe.[1558] Dane-

1548 Interview 2, Pos. 44, Interview 10, Pos. 14; Interview 11, Pos. 15.
1549 Interview 8, Pos. 9.
1550 Interview 5, Pos. 8.
1551 Interview 9, Pos. 64.
1552 Interview 7, Pos. 14.
1553 Interview 1, Pos. 33.
1554 Interview 3, Pos. 26.
1555 Interview 4, Pos. 13.
1556 Interview 9, Pos. 10.
1557 Interview 11, Pos. 17.
1558 Interview 8, Pos. 9; Interview 11, Pos. 15.

ben geht es bei solchen stärker strategisch ausgerichteten Beratungsleistungen gegenwärtig vor allem auch um das IT-Großprojekt Polizei 2020.[1559]

Die Beratung bezieht sich aber auch auf eher strukturelle Komponenten und Vorhaben der Polizeien, etwa die Begleitung von Vorhaben wie der Kennzeichnungspflicht, wo es im Gegensatz zur repressiven oder präventiven Datenverarbeitung vor allem um die rechtmäßige Verarbeitung von Beschäftigtendaten geht.[1560] An der Schnittstelle zwischen strukturellen Komponenten des polizeilichen Informationswesens und konkreten Datenverarbeitungen zu Zwecken der Strafverfolgung und Gefahrenabwehr liegt die Beratung von Projekten, die sich um Dateien und Dateisysteme, insbesondere auch auf Verbundebene drehen.[1561]

Im Mittelpunkt der Beratungstätigkeiten der Datenschutzbeauftragten steht dabei häufig das Instrument der Datenschutz-Folgenabschätzung.[1562] Als prospektive Folgenbewertung dient es der Beratung, indem die Einschätzung von neuen Verarbeitungstätigkeiten formalisiert und damit vereinfacht werden soll.[1563] Voraussetzung für die Folgenabschätzung ist aber ein voraussichtlich hohes Risiko, das zunächst in einem vorgelagerten Prüfschritt ermittelt werden muss, was häufig in Form einer sogenannten Schwellenwertanalyse geschieht, mittels derer ermittelt wird, wie hoch die Gefahr ist, dass die Persönlichkeitsrechte einer Person betroffen sind.[1564] Durchgeführt werden Schwellenwertanalyse und Datenschutz-Folgenabschätzung recht breit für jede Datei, die neu erstellt wird, oder auch für die Einführung neuer informationstechnologischer Systeme, die personenbezogene Daten verarbeiten.[1565] Diese Risikoeinschätzungen verursachen sehr hohe Arbeitsaufwände,[1566] was nicht zuletzt daran liegen wird, dass häufig rechtliche Konkretisierungen für eine ordentliche Durchführung der Folgenabschätzung fehlen.[1567] Grundsätzlich gehört zu einer Folgenabschätzung zum Beispiel die Festlegung, wie Daten zu verarbeiten und übertragen

1559 Interview 14, Pos. 8; s. näher zum Projekt bereits oben S. 271 ff. und nochmal unten S. 465 ff.
1560 Interview 1, Pos. 33, Interview 11, Pos. 15.
1561 Interview 1, Pos. 31.
1562 Siehe dazu bereits oben S. 371 f.
1563 Interview 1, Pos. 29; Interview 10, Pos. 20; Interview 13, Pos.12.
1564 Interview 4, Pos. 11; Interview 11, Pos. 15.
1565 Interview 4, Pos. 11; Interview 11, Pos. 15.
1566 Interview 14, Pos. 8.
1567 Interview 1, Pos. 64; Interview 11, Pos. 54; siehe zu weiteren Problemen des polizeilichen Datenschutzrechts unten S. 453 ff.

sind und ob die technisch-organisatorischen Maßnahmen zum Schutz der Daten vorliegen, also etwa Zugriffskontrollen, die über ein Rollen- und Berechtigungskonzept gesteuert werden, sowie Protokollierung.[1568] Allerdings haben sich als Konsequenz der nur rudimentären rechtlichen Konkretisierung uneinheitliche Verständnisse des Instruments herausgebildet, sodass beispielsweise mancherorts noch das alte, dem deutschen polizeilichen Datenschutzrecht entspringende Instrument der Errichtungsanordnungen als konkretisierendes Papier bei der Betreibung von automatisierten Dateien verwendet wird, während die Datenschutz-Folgenabschätzung „einen größeren Weitblick hinsichtlich der Gefährdungen des Persönlichkeitsrechts wagen muss."[1569] Andernorts wird demgegenüber eine Kongruenz zwischen Folgenabschätzung und Errichtungsanordnung gesehen[1570] oder stattdessen das Verzeichnis von Verarbeitungstätigkeiten verwendet, in das jeweils „eine Art Kurzprüfung für eine Datenschutz-Folgenabschätzung" integriert wird.[1571] Teilweise gehen die Errichtungsanordnungen auch in den Verzeichnissen von Verarbeitungstätigkeiten auf.[1572] Dort, wo Errichtungsanordnungen noch verwendet werden, sollen sie ganz generell als „dienststelleninterne Papiere zum Ablauf von den automatisierten Dateien" den Aufsichtsbehörden als Kontrollgrundlage dienen, erfordern dabei aber Spezialwissen, das zumeist nur von Techniker:innen geliefert werden kann.[1573] Die Heterogenität der Praktiken deutet darauf hin, dass die konkrete Form der Beratung durch die Datenschutzbeauftragten trotz des unionsrechtlichen Vereinheitlichungsimpulses nach wie vor von außerrechtlichen Faktoren abzuhängen scheint, was die Anwendungspraxis beeinflusst und damit die Effektivität wichtiger Instrumente wie das der Datenschutz-Folgenabschätzung beeinträchtigen kann.

Die Beratungstätigkeit der Datenschutzbeauftragten fordert aber jedenfalls häufig Verständnis von bzw. Vermittlung oder Übersetzung zwischen Recht, Polizeifachlichkeit und der Informationstechnik, wobei es im Rahmen dieser Transmissionsleistung unterschiedliche Komplexitätsanforderungen gibt, die sich je nach Art der Polizeibehörde richten; beispielsweise

1568 Interview 4, Pos. 21.
1569 Interview 5, Pos. 11, 25; siehe zu Uneinheitlichkeiten im polizeilichen Datenschutzrecht unten S. 398.
1570 Interview 4, Pos. 21.
1571 Interview 9, Pos. 62.
1572 Interview 11, Pos. 54.
1573 Interview 5, Pos. 23.

ist dies in höherem Maße in Landeskriminalämtern oder den in vielen Ländern bestehenden technisch spezialisierten Polizeipräsidien der Fall.[1574]

2. Überwachung und Kontrolle

Etwas weniger stark im Mittelpunkt der Aufgabenbeschreibungen aber dennoch wesentlich ist zudem die Überwachungs- und Kontrolltätigkeit der Datenschutzbeauftragten. Die Freiheitsgrade bei der Ausübung dieser Tätigkeit unterscheiden sich jedoch sehr deutlich. So wurde nur einmal von tatsächlich prinzipiell freier Kontrolltätigkeit berichtet:

> „Da ist es tatsächlich so, dass ich mir überlege, was möchte ich zum Beispiel überwachen. Das ist das eine, dass ich mir tatsächlich überlege, das kann man… also Ausgangspunkt sind da häufig parlamentarische Anfragen, Presseberichte. Hinweise tatsächlich von extern und intern. Dann überlege ich mir, was für Bereiche, was für Themen möchte ich mir mal anschauen? Dann schaue ich mir die vor Ort an, führe eine Kontrolle durch, führe ein internes Audit durch."[1575]

In den meisten Polizeibehörden ist diese Aufgabe hingegen nicht so frei organisiert, wofür als Grund etwa das Fehlen von Kapazitäten für eigene Überprüfungen angegeben wurde.[1576] Teilweise liegen Überwachungs- und Kontrolltätigkeiten durch die Datenschutzbeauftragten auch im Wesentlichen brach, sind bis auf Weiteres aufgrund von Personalkapazitäten und Organisationsstrukturen auch nicht herstellbar und werden dann auf anderen Organisationseinheiten oder auch die Aufsichtsbehörde ausgelagert.[1577]

Die Instrumente, die für die Umsetzung von Überwachung und Kontrolle des polizeilichen Informationswesens eingesetzt werden, sind divers. Als eher niedrigschwelliges Kontrollinstrument dienen die eben erwähnten Datenschutz-Folgenabschätzungen und sonstige von den Fachabteilungen selbst oder in Zusammenarbeit mit den Datenschutzbeauftragten erstellten Datenschutzkonzepte, indem über sie für die Datenschutzbeauftragten sichtbar wird, was in den einzelnen Fachabteilungen an Datenverarbeitungen durchgeführt wird.[1578]

1574 Interview 14, Pos. 28.
1575 Interview 1, Pos. 28.
1576 Interview 2, Pos. 55-58, 48.
1577 Interview 15, Pos. 10, 26; Interview 5, Pos. 29, 15.
1578 Interview 15, Pos. 26.

Daneben existieren aber zusätzliche und weitergehende Instrumente der Überwachung und Kontrolle. Ein zentraler Baustein sind dabei die verdachts- und anlassunabhängigen sowie auch verdachts- und anlassbezogenen[1579] Datenschutzkontrollen, die sich wiederum in ihrer Durchführungsform und -intensität je nach Behörde signifikant voneinander unterscheiden. So wird beispielsweise bei einer der befragten Länderpolizeien lediglich einmal im Jahr pro Dienststelle eine Überprüfung der Protokolldaten in der Form vorgenommen, dass für eine halbe Stunde Abfragen im Informationssystem herausgezogen werden und die Protokolle überprüft werden, wobei diese Kontrolle nur vonseiten des Datenschutzes veranlasst wird und die eigentliche Überprüfung von Informationssicherheitsverantwortlichen ausgeführt wird.[1580] In einer anderen Landespolizeibehörde werden die Protokolldaten demgegenüber zwei mal pro Jahr anlassunabhängig geprüft und es können weitere, anlassbezogene Prüfungen anfallen.[1581] Neben Protokolldatenüberprüfungen gibt es auch weitere Datenschutzkontrollen, etwa durch eine Überprüfung einzelner Dienststellen. So berichtet ein Datenschutzbeauftragter beispielsweise, zwei Dienststellen im Monat auf Einhaltung datenschutzrechtlicher Vorschriften zu überprüfen,[1582] was konkret die Begehung vor Ort, die Inspektion der Anlagen, der Verzeichnisse von Verarbeitungstätigkeiten sowie den Datenumgang der Mitarbeiter:innen vor Ort und die Überprüfung, ob die geführten Dateien im landeseigenen Meldesystem angemeldet sind, beinhalten kann.[1583] Auch die Überwachung der Einhaltung der Rechte der Beschäftigten gehört dabei grundsätzlich in den Aufgabenbereich der Datenschutzbeauftragten.[1584]

Ein weiteres wichtiges Werkzeug, auch wenn es nicht direkt die Überwachung durch die Datenschutzbeauftragten bedeutet, aber weitergehende Überwachungs- und Kontrolluntersuchungen initiieren kann, ist das polizeiliche Auskunftswesen zur Bearbeitung der Anfragen von Bürger:innen. Neben der rechtlichen Beurteilung der Anfragen[1585] ist mitunter auch die tatsächliche Bearbeitung der Anfragen bei den Datenschutzbeauftragten angesiedelt, die dann bei den nachgeordneten Dienststellen im Land die gegebenenfalls verfügbaren personenbezogenen Daten zur anfragenden

1579 Interview 4, Pos. 15, Interview 11, Pos. 15.
1580 Interview 2, Pos. 48.
1581 Interview 4, Pos. 15.
1582 Interview 10, Pos. 13.
1583 Interview 3, Pos. 25.
1584 Interview 7, Pos. 12.
1585 Interview 12, Pos. 12.

Person ermitteln müssen. Dies wird als sehr aufwändig beschrieben und nimmt mancherorts in etwa einen halben Tag pro Anfrage in Anspruch, weil einerseits die Dienststellen abgefragt werden müssen und bei Vorhandensein von Daten noch rechtlich geprüft werden muss, ob bzw. welche Daten herausgegeben werden dürfen.[1586] Der Anteil dieser Bearbeitung am Arbeitspensum scheint stellenweise sehr groß zu sein[1587] und wird auch als sonstige Arbeiten behindernd beschrieben.[1588] Nicht in allen Polizeien ist dies allerdings eine Aufgabe der Datenschutzbeauftragten, sondern wird teilweise ausgelagert.[1589]

Ein letztes verbreitetes Überwachungs- und Kontrollinstrument oder zumindest Hilfsinstrument sind die sogenannten Verzeichnisse von Verarbeitungstätigkeiten. Diese dienen als Index für alle von einer Behörde durchgeführten Verarbeitungstätigkeiten, der laufend aktualisiert werden muss.[1590] Die Verzeichnisse verschaffen den Datenschutzbeauftragten einen Überblick über die verschiedenen, in einer Behörde durchgeführten Verarbeitungstätigkeiten und ermöglichen so überhaupt erst eine systematische Überwachungstätigkeit. Über dieses Hilfsmittel kann die Kontrolltätigkeit angeleitet werden, indem etwa an Lösch- und Aussonderungspflichten erinnert wird, sofern diese nicht automatisiert erfüllt werden.[1591] Aufgrund der Bedeutung und Vielfalt der Informationsverarbeitung bei der Polizei ist auch dieser Aufgabenteil in der Regel mit erheblichen Aufwänden verbunden.[1592] Dort, wo die Verzeichnisse die Errichtungsanordnung abgelöst haben, wird aber mitunter von einem inhaltlichen Substanzabfall der Verzeichnisse gegenüber den Errichtungsanordnungen, die den Datenumgang im Rahmen einer Datei normativ näher konkretisieren und damit steuern, berichtet.[1593]

Insgesamt gibt es deutliche Divergenzen in der Überwachungs- und Kontrollintensität, was einerseits vor allem dort, wo nur niedrige Intensitäten bestehen, bedenklich ist. Andererseits ist dies mit Blick auf die Einheitlichkeit des polizeilichen Informationswesens problematisch, das zwar durch den Föderalismus (rechtlich) durchaus divers und heterogen ist,

1586 Interview 3, Pos. 13-18, ähnlich auch Interview 8, Pos. 9; Interview 13, Pos. 20.
1587 Interview 4, Pos. 9; Interview 13, Pos. 10.
1588 Interview 13, Pos. 10.
1589 Interview 2, Pos. 154.
1590 Interview 14, Pos. 8.
1591 Interview 4, Pos. 19.
1592 Interview 10, Pos. 13.
1593 Interview 11, Pos. 58.

aber dennoch umfassend vom Impetus nach möglichst vollständigen Daten zu untersuchtem deviantem Verhalten geprägt ist, sodass Unterschiede im Datenschutzniveau kritisch zu sehen sind.[1594]

3. Schulungen und Sensibilisierung

Als ebenfalls wichtiger Teil des Aufgabentableaus der Datenschutzbeauftragten ist die Schulung und Sensibilisierung der Mitarbeiter:innen anzusehen, die mit personenbezogenen Daten umgehen müssen. Dazu werden häufig Vorträge und Schulungen innerhalb der Polizei gehalten,[1595] sofern dies nicht wegen fehlender Ressourcen ebenfalls aus dem Aufgabenspektrum der Beauftragten entfallen muss.[1596] Konkret werden etwa Fortbildungsveranstaltungen für alle Neuzugänge im Präsidium und einmal jährlich stattfindende Informationsveranstaltung für die vorgesetzten Ebenen über neue datenschutzrechtliche Erkenntnisse abgehalten.[1597] Zudem finden Beschulungen der Polizist:innen bei der Einführung neuer Technologien statt[1598] und auch an den Polizeihochschulen sensibilisieren manche Datenschutzbeauftragte in Ausbildungsfeldern wie Führung oder Kriminalitätsbekämpfung.[1599]

4. Sonstige Aufgabenbeschreibungen

Weitere Aufgaben, die in den Befragungen berichtet wurden, sind beispielsweise die Vertretung der Behörde vor Gericht in Datenschutzverfahren, was kritisch mit Blick auf die eigene Unabhängigkeit in puncto Datenschutz gesehen wird,[1600] die Bearbeitung von Anfragen nach dem IFG, was als sehr zeitaufwändig beschrieben wird, eigentlich keine Aufgabe der Datenschutzbeauftragten ist und vor diesem Hintergrund ebenfalls kritisiert wird[1601] sowie die Pflichten nach der DSGVO, betreffend alle Datenverarbeitungen,

1594 Siehe näher zum Verwirklichungsgrad des Datenschutzes in den deutschen Polizeien unten S. 453 ff.
1595 Interview 1, Pos. 37.
1596 Interview 2, Pos. 48.
1597 Interview 3, Pos. 88.
1598 Interview 10, Pos. 13.
1599 Interview 11, Pos. 15.
1600 Interview 2, Pos. 82-86, Interview 8, Pos. 9.
1601 Interview 2, Pos. 44.

die nicht die originären Polizeiaufgaben betreffen und damit nicht der JI-Richtlinie unterfallen.[1602]

5. Stellungnahme zu den Aufgaben der Datenschutzbeauftragten

Vor dem Hintergrund der Funktion der Datenschutzbeauftragten, das polizeiliche Datenschutzrecht Rechtswirklichkeit werden zu lassen, indem Recht, Fachlichkeit und Technik der polizeilichen Informationsverarbeitung miteinander verzahnt werden, ist es vor allem die Beratung durch die Datenschutzbeauftragten, die hier den größten Beitrag leisten kann, da sie – wenn die entsprechenden Ressourcen und organisatorischen Gegebenheiten es erlauben – einen Raum für das Zusammentreffen und den disziplinenübergreifenden Dialog der drei Komponenten polizeilicher Informationsverarbeitung erlaubt, wodurch ein Einklang der unterschiedlichen rechtlichen, fachlichen und technischen Anforderungen gelingen kann.[1603] Auch die sonstigen Aufgaben sind für das polizeiliche Informationswesen in seiner Gesamtheit wichtig, aber unterstützen eher die Beratung, indem im Wege der Überwachung Rechtswidrigkeiten Anlass für weitere Beratungen geben und Sensibilisierung der Mitarbeiter:innen über Schulungen ein stetig mitlaufendes Bewusstsein für datenschutzrechtliche Belange kreieren. Damit aber das Informationswesen über normative Vorgaben steuerbar bleibt, müssen auch immer Kapazitäten für die Unterbindung von rechtswidrigen Datenverarbeitungen durch entsprechende Überwachungs- und Kontrollbemühungen vorhanden sein.

III. Organisation und Strukturen des polizeilichen Datenschutzes

Die Potenziale der Arbeit der Datenschutzbeauftragten hängen zu einem großen Teil von der Organisation des Datenschutzes bei den jeweiligen Behörden und daneben bestehenden Strukturen ab, in die die Datenschutzbeauftragten bei der Erfüllung ihrer Aufgaben eingebettet sind.

1602 Interview 5, Pos. 11.

1603 Diese Funktion der Mediation zwischen den verschiedenen, für das polizeiliche Informationswesen relevanten Bereichen beobachten bspw. auch *Egbert/Leese,* Criminal futures, S. 55 im Rahmen ihrer Studie.

1. Organisation

Die Datenschutzbeauftragten bei den deutschen Polizeien sind in der Regel bei der Behördenleitung angesiedelt[1604] und weisungsfrei,[1605] die Ansiedelung bei der Leitung ist also rein organisatorischer Natur. Es wird sich bemüht, eine Unabhängigkeit von sonstigen behördlichen Verfahren, in denen häufig personenbezogene Daten verarbeitet werden, sicherzustellen, um Interessenkonflikte zu vermeiden.[1606]

Weniger einheitlich ist hingegen der Anstellungsstatus: Berichtet wird davon, dass Datenschutzbeauftragte Angestellte, Verwaltungsbeamte, Kriminalbeamte oder Schutzpolizeibeamte sind.[1607] Häufig handelt es sich aber zumindest um Vollzeitstellen,[1608] wobei durchaus auch von auch Teilzeitstellen berichtet wird.[1609] Letztere finden sich insbesondere in einigen Ländern in nachgeordneten Dienststellen, also etwa in den Inspektionen, wo es Datenschutzbeauftragte im Nebenamt gibt,[1610] die mehr als Ansprechperson für die hauptamtlichen Datenschutzbeauftragten fungieren,[1611] etwa wenn Verzeichnisse von Verarbeitungstätigkeiten dezentral in den Untereinheiten geführt werden.[1612] Es existieren Richtwerte für Vollzeitstellen, die von einer Datenschutzbeauftragten-Stelle pro 700-900 Mitarbeiter:innen ausgehen,[1613] wovon einige deutsche Polizeibehörden recht weit entfernt sein dürften. Die Divergenzen setzen sich in der personellen Organisation fort: Teilweise sind die Befragten allein, als „Einzelkämpferin“[1614], für ihren Datenschutzbereich zuständig, teilweise erfolgt eine Ausstattung mit Mitarbeiter:innen.[1615] Dennoch wird die Ausstattung mit Ressourcen, vor dem Hintergrund der generell eher angespannten Personallage im öffentlichen Dienst, überwiegend als ausreichend beschrieben.[1616]

1604 Interview 1, Pos. 41; Interview 2, Pos. 54; Interview 4, Pos. 26; Interview 5, Pos. 30; Interview 5, Pos. 21; Interview 8, Pos. 18-21.
1605 Interview 3, Pos. 42.
1606 Interview 10, Pos. 38.
1607 Interview 3, Pos. 109.
1608 Interview 5, Pos. 34.
1609 Interview 10, Rn. 36.
1610 Interview 13, Pos. 23.
1611 Interview 3, Pos. 20; Interview 5, Pos. 8.
1612 Interview 11, Pos. 26.
1613 Interview 12, Pos. 12.
1614 Interview 9, Pos. 16.
1615 Interview 5, Pos. 34.
1616 Interview 8, Pos. 34-37.

Wie bereits im Rahmen der Aufgabenbeschreibung angeklungen, unterscheiden sich auch die Zuständigkeitsbereiche stark. So sind die Datenschutzbeauftragten je nach Land mal für die gesamte Polizeiorganisation und mal nur für eine einzelne Behörde zuständig – etwa für ein Landeskriminalamt, ein Präsidium oder eine Direktion, wobei dann prinzipiell Zuständigkeiten nach der Größe und dem damit einhergehenden Bedarf vergeben werden.[1617] Der Zuschnitt des Zuständigkeitsbereichs hat auch Auswirkungen auf die Ausrichtung der Arbeit, sodass etwa keine Überwachung, sondern nur eine juristische Beratung geleistet werden kann, diese dann aber flächendeckend für das ganze Land.[1618] Die Ausrichtungen der Aufgabenzuständigkeit kann man grundsätzlich idealtypisch in operativen Datenschutz, also beispielsweise Protokolldatenauswertung oder das polizeiliche Auskunftswesen, und strategischen Datenschutz, also Beratungen und Überwachung bei komplexeren Systemen und Verfahren, unterteilen. Strategischer Datenschutz wird tendenziell bei höhergestellten Organisationstypen wie den Landeskriminalämtern angesiedelt,[1619] während operativer Datenschutz eher bei regional für bestimmte Landesteile zuständigen Behörden durchgeführt wird. Diese – keineswegs universelle – Aufteilung kann allerdings beispielsweise wegen Personalknappheiten nicht immer ganz durchgehalten werden.[1620] Neben diesen sachbezogenen Mustern gibt es zusätzlich noch organisatorische Besonderheiten, je nach intern gewachsener Organisationsstruktur, sodass etwa das Auskunftswesen kein Teil der Tätigkeit mancher Datenschutzbeauftragten ist.[1621] Die mancherorts praktizierte, eben erwähnte, Ausstattung von Dienststellen mit datenschutzrechtlichen Ansprechpersonen ist Ausdruck der insgesamt für die Polizei (und Verwaltung) typischen Hierarchisierung auch in der Organisation des polizeilichen Datenschutzes.[1622] Ganz generell werden aber die Datenschutz-Komponenten von Projekten, die mehr als eine eigenständigen Behördeneinheit im Land betreffen, nachvollziehbarerweise stark bei den hauptamtlichen Datenschutzbeauftragten mit strategischer Ausrichtung zentralisiert. Trotz der beschriebenen Unterschiede scheint sich die Organisationslage im polizeilichen Datenschutz zunehmend zu

1617 Interview 1, Pos. 57; Interview 11, Pos. 34.
1618 Interview 5, Pos. 18-19.
1619 Interview 9, Pos. 28.
1620 Interview 13, Pos. 10.
1621 Interview 2, Pos. 158; Interview 9, Pos. 14.
1622 Interview 3, Pos. 14.

vereinheitlichen, denn vor 2018[1623] soll es noch größere Abweichungen gegeben haben. Teilweise gab es keine Datenschutzbeauftragten oder Datenschutz war lediglich Nebenaufgabe.[1624] Auch gab es Lösungen, die etwa den oder die Leiter:in des Rechtsreferats automatisch in die Position der oder des Datenschutzbeauftragten hoben.[1625] Insgesamt ist die Position der Datenschutzbeauftragten durch die organisatorischen Zusammenhänge entweder mit einem deutlichen rechtlichen Fokus ausgestaltet[1626] oder weist etwa unter Einbezug technischer Elemente eine stärkere Interdisziplinarität auf. Damit wird die Tätigkeit der polizeilichen Datenschutzbeauftragten, die grundsätzlich durch den rechtlichen Hintergrund der JI-Richtlinie und der sie umsetzenden nationalen Gesetze bestimmte Merkmale aufweisen soll, in nicht unerheblicher Weise durch die Organisation der jeweiligen Polizeibehörde beeinflusst. Die Ausrichtung der Tätigkeit am gesetzlichen Leitbild konfligiert somit mit einer organisationalen Determinierung der Tätigkeit. Am deutlichsten zeigt sich das daran, dass – wie es bereits im Rahmen der Aufgabenbeschreibungen zur Sprache gekommen ist – eine gewisse Freiheit der Datenschutzbeauftragten bei ihrer Aufgabenausübung insbesondere im Bereich der Überwachung und Kontrolle sehr selten ist.[1627] Beobachten lassen sich tendenziell eher verschiedene Grade von organisationaler Determiniertheit,[1628] was konkret etwa dazu führt, dass Kontrollprozesse reaktiv gehandhabt werden, das heißt etwa von einer konkreten Anfrage einer Behörde um Protokolldatenauswertung beim Landeskriminalamt abhängen,[1629] dass Beratung und Überwachung als Aufgaben personell getrennt werden[1630] oder dass die Kontrolldimension im Wesentlichen an die Aufsichtsbehörde ausgelagert wird.[1631]

1623 In diesem Jahr musste die JI-Richtlinie vollständig in nationales Recht umgesetzt sein.
1624 Interview 8, Pos. 25; weit vor 2018 lag der Datenschutz anscheinend stellenweise „völlig brach", Interview 8, Pos. 45.
1625 Interview 10, Pos. 6.
1626 Interview 7, Pos. 18.
1627 Interview 1, Pos. 28.
1628 Interview 2, Pos. 88-92.
1629 Interview 4, Pos. 10.
1630 Interview 5, Pos. 17.
1631 Interview 15, Pos. 26.

2. Strukturen

Neben der organisatorischen Seite wird die Tätigkeit der Datenschutzbeauftragten zudem durch weitere Strukturen bestimmt, die mal mehr, mal weniger institutionalisiert sind.

Eine dieser Strukturen sind die vielfältigen fachlichen Netzwerke der polizeilichen Datenschutzbeauftragten in Deutschland. Besonders wirkmächtig ist das überregionale Netzwerk, das aus den Datenschutzbeauftragten der Landeskriminalämter besteht,[1632] vom Bundeskriminalamt koordiniert wird und schon einen gewissen Institutionalisierungsgrad erreicht hat.[1633] Hier besteht auch reger Kontakt abseits von festgelegten Treffen zu aufkommenden datenschutzrechtlichen Fragen.[1634] Daneben gibt es analog dazu Netzwerke der polizeilichen Datenschutzbeauftragten in den Ländern, zumeist unter Koordination des jeweiligen Landeskriminalamtes.[1635]

Auch innerhalb der Organisationseinheit, für die die Datenschutzbeauftragten zuständig sind, gibt es zahlreiche Vernetzungs- und Kontaktpunkte, die eine gewisse strukturelle Verfestigung aufweisen. So sind Datenschutzbeauftragte nicht die einzigen, die an der Verwirklichung von Datenschutz beteiligt sind. Stets erforderlich ist etwa die Beteiligung der technischen Abteilungen, mit denen folglich zusammengearbeitet werden muss.[1636] Da Datenschutz aber auch im Übrigen eine „Querschnittsaufgabe der Behörde und somit Aufgabe aller Organisationseinheiten und aller Mitarbeiter" ist,[1637] gibt es vielfältige Verbindungen zur Fachlichkeit, wobei allerdings die Arbeit der Datenschutzbeauftragten als koordinierendes Zentrum der Bemühungen fungiert,[1638] da ja auch gerade durch die zentrale Bearbeitung von Datenschutzthemen die restliche Organisation in diesen Fragen entlastet werden soll.[1639] So wird dann etwa bei den Landeskriminalämtern oder bei auf technische Verfahren spezialisierten Polizeibehörden die Da-

1632 Interview 1 Pos. 51, 57; Interview 9, Pos. 30.
1633 Interview 1, Pos. 55; Interview 5, Pos. 29.
1634 Interview 2, Pos. 74, 76.
1635 Interview 3, Pos. 40; Interview 4, Pos. 33; Interview 5, Pos. 29; Interview 7, Pos. 20; Interview 10, Pos. 26.
1636 Interview 2, Pos. 100; Interview 12, Pos. 26.
1637 Interview 11, Pos. 26.
1638 Interview 14, Pos. 40; es wurde aber auch von nur begrenzten Einbindungen in die Fachlichkeiten berichtet, was im Wesentlichen davon abhängt, ob die Ausrichtung der Datenschutzbeauftragten rein rechtlich oder eher interdisziplinär ist, Interview 15, Pos. 10.
1639 Interview 3, Pos. 52.

tenschutz-Folgenabschätzung zentral für ein System und Verfahren durchgeführt.[1640] Koordinierungs- und Kommunikationsbedarf ergeben sich für die Datenschutzbeauftragten demgegenüber wieder häufig, wenn konkret Daten, etwa anlässlich einer Anfrage, überprüft werden, da die dafür einzusehenden Daten oftmals nur dezentral verfügbar sind, sodass die Datenschutzbeauftragten sie erst zusammentragen müssen.[1641]

Strukturelle Vernetzungen bestehen aber auch über die jeweiligen Polizeibehörden hinaus, etwa zur ministerialen Ebene[1642] und mitunter auch zu anderen Länderpolizeien, wenn beispielsweise aufgrund geographischer Gegebenheiten eine enge Kooperation besteht.[1643] Ansonsten sind länderübergreifende Kontakte bei fehlender Bekanntschaft eher unüblich ist.[1644] Darüber hinaus gibt es natürlich auch Kontakte zu den Polizeibehörden im eigenen Land, wenn bspw. besonders sensible Auskunftsanfragen gebündelt vom Landeskriminalamt beantwortet werden sollen.[1645]

Besonders wichtig sind zudem noch die Kontaktstrukturen mit den Aufsichtsbehörden, also den Landes- und dem Bundesdatenschutzbeauftragten. Diese werden aufgrund der politischen Ausrichtung mancher Landesdatenschutzbeauftragten teilweise als schwierig bezeichnet, was sich in Konflikten mit der Polizei äußern kann.[1646] Überwiegend wird das Verhältnis indessen nicht als problematisch beschrieben,[1647] vielmehr wird sogar von einem „Schulterschluss" mit der Aufsichtsbehörde berichtet, um mit ähnlicher Ausrichtung zu operieren.[1648] Recht üblich sind auch Hospitationen von designierten Datenschutzbeauftragten bei den jeweiligen Aufsichtsbehörden.[1649] Teilweise wird auch der oder die Landesdatenschutzbeauftragte in das landeseigene datenschutzrechtliche Expert:innennetzwerk

1640 Interview 4, Pos. 11; Interview 8, Pos. 57; Interview 14, Pos. 8.
1641 Interview 4, Pos. 32; teilweise sind die Daten auch direkt über das Informationssystem für die Datenschutzbeauftragten einsehbar, Interview 8, Pos. 13; siehe zu Zentralität und Dezentralität in der polizeilichen Informationsverarbeitung unten S. 439 ff.
1642 Interview 3, Pos. 48.
1643 Interview 3, Pos. 40; Interview 11, Pos. 36.
1644 Interview 3, Pos. 40
1645 Interview 3, Pos. 22.
1646 Interview 2, 63-66; Interview 15, Pos. 32.
1647 Interview 3, Pos. 32; Interview 4, Pos. 34; Interview 7, Pos. 24.
1648 Interview 5, Pos. 30.
1649 Interview 8, Pos. 27; Interview 9, Pos. 32; Interview 10, Pos. 34; Interview 13, Pos. 58.

involviert, um schon in frühen Projektstadien miteinander konzeptuell zusammenzuarbeiten und Konflikte gar nicht erst aufkommen zu lassen.[1650]

Während die Faktoren der Organisation die Tätigkeit der Datenschutzbeauftragten teilweise hemmen, ist die Wirkung der sonst bestehenden Strukturen, in die das Handeln der Beauftragten eingebettet ist, eher unterstützend, indem gegenseitige Unterstützung etwa in den fachspezifischen Netzwerken oder durch Zuarbeiten anderer am Datenschutz beteiligter Stellen gewährleistet wird. Das gilt bis auf wenige Ausnahmen auch für die Kommunikation und Kooperation mit den Landes- und dem Bundesdatenschutzbeauftragten.

IV. Das Recht des polizeilichen Datenschutzes

Das polizeiliche Datenschutzrecht strukturiert das polizeiliche Informationswesen und Informationshandeln. Dabei sind die polizeilichen Datenschutzbeauftragten personelle Punkte der Materialisierung normativer Vorgaben. Wenngleich Technik und polizeiliche Fachlichkeit ebenfalls bestimmende Momente für Informationswesen und Informationshandeln sind, ist es das Recht, ausgestattet mit einer ihm eigenen Verbindlichkeit, das der Ausgangspunkt aller Gestaltungsmaßnahmen der Datenschutzbeauftragten ist. Insofern ist es für eine weitere Annäherung an die Rechtwirklichkeit der polizeilichen Datenverarbeitung von nicht zu unterschätzender Bedeutung, zu ergründen, wie die Datenschutzbeauftragten als Rechtsanwender:innen das polizeilichen Datenschutzrecht als strukturierendes Element und Instrument wahrnehmen und damit arbeiten.

Auf das polizeiliche Datenschutzrecht angesprochen bemängelten die Befragten – dem Ergebnis der rechtswissenschaftlichen Ausführungen entsprechend[1651] – mitunter substanzielle Defizite der gegenwärtigen Rechtslage, deren Ursprünge in erster Linie bei den verschiedenen Gesetzgebern verortet werden. Insbesondere das Fehlen von Grundsatzarbeit, die das Rechtsgebiet klarer strukturiert, wird kritisiert. Eine immer nur punktuelle und vor allem maßnahmenbezogene Regelung von polizeilicher Datenverarbeitung wird dabei als unzureichend wahrgenommen[1652] und auch bei dieser punktuellen gesetzgeberischen Aktivität wird Nachbesserungsbedarf angemahnt:

1650 Interview 8, Pos. 25.
1651 Siehe dazu bereits oben S. 358 ff.
1652 Interview 1, Pos. 124.

> „Warum haben wir zum Beispiel nicht vernünftige Normen, die Ermittlungen im Internet richtig abbilden? Wenn ich jetzt zum Beispiel anfange, im Internet zu ermitteln, im Darknet, was ist denn das? Stütze ich das auf Generalklausel? Das ist so der Punkt. Aus meiner Sicht ist das so eine Herausforderung, da ist der Gesetzgeber gefordert, dass die Dinge letztendlich durch saubere Normen, die einen sauberen Tatbestand haben und Voraussetzungen haben und Folgen haben, sauber abzubilden und nicht vieles einfach so laufen zu lassen. Und am Ende die Sicherheitsbehörden vor die Herausforderung zu stellen, dass sie es irgendwie umsetzen und möglich machen sollen und dann am Ende auf Generalklauseln zurückfallen, das kann es nicht sein. Das empfinde ich als unbefriedigend."[1653]

Bemängelt wird weiterhin die gesetzgeberische Regelungstechnik. Da die Judikatur des Bundesverfassungsgerichts im Bereich sicherheitsbehördlichen Informationshandelns über die Jahre recht umfangreich geworden ist, sind die Gesetzgeber häufig dazu übergegangen, die Verfassungsrechtsprechung wortwörtlich zu übernehmen. Geschehen ist dies etwa bei § 12 BKAG, was von der Datenschutzpraxis mitunter als unbefriedigend und verwirrend empfunden wird.[1654] Diese gesetzgeberische Praxis ist nicht neu und ist aus rechtswissenschaftlicher Sicht insbesondere mit Blick auf Sicherheitsgesetzgebung kritisiert worden, da an den Gesetzgeber adressierte Vorgaben an die Ebene der Rechtsanwendung durchgereicht werden, wodurch Schwierigkeiten für diese entstehen.[1655] Ebenfalls in diesem Zusammenhang wird kritisiert, dass klare Vorgaben für zentrale Komponenten des polizeilichen Informationswesens fehlen. Beispielsweise gibt es keine rechtlichen Grundlagen für Vorgangsbearbeitungssysteme, sodass in der Praxis solche Systeme auf die Normen für Vorgangsverwaltung gestützt werden. Da Vorgangsbearbeitung jedoch unter Zweckgesichtspunkten der Erfüllung der originären Polizeiaufgaben dient, während Vorgangsverwaltung administrativen Charakter hat und Zwecksperren enthält, die es grundsätzlich verbieten die dort vorgehaltenen Daten zur Aufgabenerfüllung zu nutzen,[1656] ist das Fehlen konkreter Vorgaben für informationstechnische Systeme der Vorgangsbearbeitung mit Blick auf den Eingriffs-

1653 Interview 1, Pos. 119.
1654 Interview 1, Pos. 94, 96.
1655 Siehe zu diesem Problem etwa bereits *Aulehner,* Polizeiliche Gefahren- und Informationsvorsorge, S. 8.
1656 Siehe dazu bereits oben S. 254 ff.

charakter von Datenverarbeitungen – vor allem diejenigen, die weitere polizeiliche oder sonst staatliche Maßnahmen nach sich ziehen können – problematisch und wird auch so wahrgenommen.[1657] Die Problematik einer mangelhaften Konturierung durch das Recht ist grundsätzlich bei fast allen polizeilichen Informationssystemen bzw. Datenverarbeitungssystemen akut,[1658] was eine einheitliche Datenschutz-Praxis und damit eine einheitliche Regulierung des polizeilichen Informationswesens und der darin stattfindenden Informationshandlungen enorm erschwert und so die datenschutzrechtliche Rechtsanwendung und -durchsetzung gefährdet.[1659] Während es sich bei diesen Versäumnissen um bereits seit langem nicht adressierte Missstände handelt, wird von den Gesetzgebern auch eine zukunftsgerichtete Proaktivität verlangt, um „modernen Massenüberwachungssystemen" die notwendige Regulierung zukommen zu lassen.[1660] Neben solchen Handlungs- und Reformbedürfnissen wird vonseiten der Datenschutzbeauftragten jedoch auch die Notwendigkeit der Konsolidierung der durch die EU-Datenschutzreform und das Karlsruher BKAG-Urteil ausgelösten Rechtsänderungen beschrieben, damit die Polizeien die angestoßenen Veränderungen organisatorisch absorbieren, verarbeiten und ihre informationelle Praxis anpassen können.[1661] Zusätzlich zu den durch rechtliche Entwicklungen ausgelösten Gesetzesänderungen[1662] fordert das ständige Fortschreiten der Möglichkeiten polizeilicher Informationstechnologie laufende Anpassungsleistungen von den verschiedenen Gesetzgebern, um dem institutionellen Interesse an effektiver Polizeiarbeit gerecht zu werden.[1663]

Die Kritik gegenüber datenschutzrechtlichen Gesetzen richtet sich auch gegen den unionalen Gesetzgeber, dessen JI-Richtlinie als nicht hinreichend konkret wahrgenommen wird. Hierin wird eine zusätzliche Quelle der Verunsicherung gesehen, etwa was den Umgang mit dem – wie

1657 Interview 14, Pos. 130, 132.
1658 Eine Ausnahme bildet das INPOL-System, das im BKAG eine begrenzte Normierung erfahren hat, siehe dazu bereits oben S. 230 ff.
1659 Interview 14, Pos. 76, 80, 121 ff.
1660 Interview 14, Pos. 110.
1661 Interview 12, Pos. 53.
1662 Auch diese rechtlichen Entwicklungen reagieren häufig auf technische Entwicklungen, sind allerdings – anders als neue Technologien wie die Bodycam oder die sog. automatisierte Datenanalyse – weniger punktuell in ihrer gesetzgeberischen Reichweite.
1663 Interview 10, Pos. 56.

dargestellt – zentralen Instrument der Datenschutz-Folgenabschätzung angeht.[1664] Auch hier wird die mangelhafte gesetzgeberische Umsetzungsleistung kritisiert, wenn etwa die besondere Kategorien personenbezogener Daten in der JI-Richtlinie nur wortwörtlich und ohne Konkretisierung übernommen wurden, sodass Unklarheit über die Rechtsfolge dieser normativen Vorgabe herrscht.[1665] Daneben wird aus datenschutzrechtlicher Sicht moniert, dass der Gesetzgeber, insbesondere auf Bundesebene, versucht habe, die JI-Richtlinie aufzuweichen.[1666] Dennoch wird von einer merklichen Wirkung der JI-Richtlinie auf die polizeiliche Praxis berichtet,[1667] wenngleich das deutsche Datenschutz-Niveau bei der Polizei auch schon vor der JI-Richtlinie als hoch beschrieben wird.[1668] Positive Wirkungen auf das Recht der polizeilichen Datenverarbeitung und seine Anwendung werden der vereinheitlichenden[1669] und sensibilisierenden[1670] Wirkung zugeschrieben.

Trotz dieser monierten gesetzgeberischen Versäumnisse bzw. im Gegensatz zu dieser Deutung wird die Regelungslage teilweise auch als eher von gesetzgeberischer Überaktivität gekennzeichnet gesehen:

> „Also wenn man sich den Datenschutz mal vor 10 Jahren anschaut und wenn man jetzt sieht: Die DS-GVO, die JI-Richtlinie, die daraus resultierenden Bundesdatenschutzgesetze und Landesdatenschutzgesetze und auch bei uns das neue Polizeigesetz, das sind ja immer mehr Regeln, die den Datenschutz betreffen, das heißt, das Korsett der polizeilichen Arbeiten wird eigentlich immer enger geschnürt. Das heißt, der Datenschutz nimmt immer eine wesentlich stärkere Rolle ein“[1671]

Neben dem Rückzug des Rechts und nicht wahrgenommener gesetzgeberischer Regelungsverantwortung wird also auch eine Erhöhung der Regelungsdichte gesehen.[1672] Allerdings ist anzumerken, dass über die Frage

1664 Interview 1, Pos. 64; Interview 11, Pos. 54; allerdings sollte die JI-Richtlinie auch nicht maßgeblich für die Datenschutzbeauftragten sein, da sie sich als Richtlinie an die Gesetzgeber im Bundesstaat richtet, die eine hinreichende Praktikabilität der Regelungen sicherzustellen haben.
1665 Interview 1, Pos. 70.
1666 Interview 1, Pos. 68.
1667 Interview 3, Pos. 42ff., 52, 82.
1668 Interview 5, Pos. 42.
1669 Interview 9, Pos. 42.
1670 Interview 11, Pos. 48; Interview 15, Pos. 103.
1671 Interview 4, Pos. 42.
1672 Interview 5, Pos. 38; Interview 6, Pos. 54.

nach substanziellen Fortschritten in der (dogmatischen) Entwicklung des polizeilichen Informationsrechts mit dem Befund der zunehmenden Regelungsdichte natürlich noch nichts gesagt ist. Die dogmatische Durchdringung ist ebenfalls ein Aspekt, der als unzureichend wahrgenommen wird, wenn etwa gesetzlichen Kernregelungen wie den §§ 12 ff. BKAG unter explizitem Verweis auf die wenigen dogmatischen Überlegungen, die es dazu vorrangig von *Bäcker* gibt, die Konsistenz abgesprochen wird.[1673] Dogmatische Leerstellen solcher Art führen in der Folge zu einer nur rudimentär angeleiteten Auslegung durch die Datenschutzbeauftragten und andere Rechtsanwender:innen.[1674] Dass es zudem nur wenig nicht-verfassungsrechtliche Rechtsprechung zur polizeilichen Datenverarbeitung abseits von Erhebungsmaßnahmen gibt,[1675] trägt in der Deutung einiger Befragter zu dieser Stagnation bei. Im polizeilichen Datenschutzrecht selbst ist auch immer der Unterschied zwischen prozessualen Datenschutzvorgaben und materiell-rechtlichen Grenzen der polizeilichen Informationsverarbeitung zu bedenken; letztere werden, abseits des Grundsatzes der hypothetischen Datenneuerhebung, als kaum ausgeprägt wahrgenommen.[1676]

Bemerkenswert ist in diesem Zusammenhang weiter, dass der Zweckbindungsgrundsatz als wichtiges normatives Strukturmerkmal der polizeilichen Datenverarbeitung in der polizeilichen Informationspraxis, wie angenommen, tatsächlich nur noch begrenzt Steuerungswirkung zu entfalten scheint:

> „Die Zweckbindung existiert nicht. Gefahrenabwehr und Strafverfolgung sind eigentlich nicht wirklich getrennt. […] Das kann man ganz schwierig finden und ich finde das aus einer grundrechtlichen Perspektive auch ganz schwierig, es ist nun aber mal so."[1677]

Allerdings wäre ein auf diese Aussage gestützter Eindruck falsch, der Zweckbindungsgrundsatz spiele keine Rolle für die polizeilichen Informationspraktiken, denn in einem anderen Interview wird der Umgang mit den Zweckbindungen im polizeilichen Alltag generalisierend wie folgt beschrieben:

1673 Interview 1, Pos. 96 ff.
1674 Interview 5, Pos. 60, 62.
1675 Interview 11, Pos. 45, 47; Interview 13, Pos. 72.
1676 Interview 1, Pos. 45; ähnlich auch schon *Aulehner,* Polizeiliche Gefahren- und Informationsvorsorge, S. 8 f.
1677 Interview 1, Pos. 126, 45.

> „Für eine Zweckänderung müsste auch eine neue Akte erschaffen werden. Beispielsweise führen Erkenntnisse aus einer rein polizeilichen Maßnahme in ein Strafverfahren. Dann wird eine neue Akte für das Strafverfahren eröffnet, für die neue Speicherfristen gelten. Die polizeiliche Maßnahme bleibt im sogenannten Vorkommnis und wird automatisiert nach einem Jahr gelöscht. Die benötigten Daten müssen somit rechtzeitig aus dem einen Verfahren entnommen und in das Strafverfahren übernommen werden."[1678]

Inwieweit aber eine rechtliche Prüfung der Zulässigkeit der zweckändernden Nutzung bei diesem Vorgang vorgenommen wird, kann allgemein nicht gesagt werden. Die jeweiligen Sachbearbeiter:innen müssen „bei der Zweckänderung prüfen, ob die „neue Datenerhebung" nach der Zweckänderung anderen Speicherfristen unterliegt" und „ob die Datenerhebung nach der Zweckänderung noch gerechtfertigt ist" – wird dies bejaht, können die Daten weiterverwendet werden.[1679] Darüber entscheiden die jeweilig mit den Daten arbeitenden Sachbearbeiter:innen „vor Ort für sich."[1680] Da bereits einige Datenschutzbeauftragte von Schwierigkeiten mit der Auslegung des polizeilichen Datenschutzrechtes berichten, kann es als zweifelhaft gelten, ob oder inwieweit die nicht aufs polizeiliche Datenschutzrecht spezialisierten Polizeibeamt:innen sich mit den Einzelheiten von Zweckbindung und -änderung auskennen. In der Praxis wird eine schlichte Erforderlichkeitsprüfung der Daten, die den jeweiligen Beamt:innen aufgrund ihrer individuellen Zugriffsberechtigung zur Verfügung stehen,[1681] vermutlich die höchste Schwelle in einem Großteil aller Datenverarbeitungen sein. Eine Chance zur Verbesserung dieser Praxis ist vor allem technisch denkbar, indem rechtliche Vorgaben in die technischen Prozesse eingearbeitet werden:

> „Das Programm sagt dem Sachbearbeiter: „Wenn ich jetzt die Daten brauche, dann aus vorgegebenen Gründen." Wenn man solche Sachen hinterlegt, dann habe ich es einfach präsenter. Egal, um welche Uhrzeit (Nachtdienst) die Sachbearbeitung stattfindet."[1682]

1678 Interview 10, Pos. 87.
1679 Interview 10, Pos. 84.
1680 Interview 10, Pos. 86.
1681 Interview 10, Pos. 52 ff.
1682 Interview 10, Pos. 82.

Damit würde dann zumindest eine Erforderlichkeitsprüfung konsistenter und flächendeckender; inwieweit man dies auch zur Sicherstellung der Zweckbindung nutzen könnte,[1683] scheint aufgrund der weitgehenden Freigabe der Zweckänderung im polizeilichen Datenschutzrecht dagegen eher eine Frage von rechtlicher Nachbesserung und weniger von polizeilicher Informationsverarbeitungspraxis zu sein.

Weitere strukturelle Schwächen werden in der mangelnden Anpassung der unterschiedlichen Rechtsmaterien der polizeilichen Informationsverarbeitung gesehen. Insbesondere die Strafprozessordnung hinke in ihrer Anpassung dem mittlerweile schon detaillierteren Polizeirecht hinterher. Gerade Grundsätzliches wie Zweckbindung, Löschung und Ähnliches werden als für die Datenschutz-Praxis unzureichend geregelt beschrieben.[1684] Allerdings arbeiten ohnehin viele Datenschutzbeauftragten vorrangig mit dem Polizeirecht und dem jeweiligen Datenschutzrecht,[1685] sodass das einschlägige Strafprozessrecht teilweise kaum bekannt ist.[1686] Dieser Zustand hat seinen Ursprung aber auch nicht zuletzt darin, dass fast alle polizeilichen Datenbestände Mischdateien sind und somit gem. § 483 Abs. 3 StPO vorrangig das jeweilige Landespolizeirecht gilt.[1687]

Als spürbar und teilweise störend werden daneben auch die Divergenzen empfunden, die sich aus den unterschiedlichen polizeirechtlichen Gesetzesmaterien ergeben.[1688] Dabei handelt es sich allerdings um keine universelle Wahrnehmung, so wird von anderer Seite auch eine große Kongruenz zwischen den Ländern (wohl intuitiv: weit über 90 % Übereinstimmung) gesehen,[1689] wobei nichtsdestotrotz auch von diesen Befragten eine größere Vereinheitlichung in Form eines Musterpolizeigesetzes begrüßt würde.[1690] Die Rechtszersplitterung wird einerseits als Hindernis für technologische Innovationen in der polizeilichen Informationsverarbeitung wahrgenom-

1683 In diese Richtung auch etwa *Löffelmann* Zeitschrift für das Gesamte Sicherheitsrecht 2 (2019), 16 (22), der eine technikgestützte Farbvisualisierung von Schutzwürdigkeitsstufen in Zweckänderungskontexten vorschlägt.

1684 Interview 1, Pos. 127.

1685 Interview 2, Pos. 105 ff.

1686 Interview 13, Pos. 75 ff.

1687 Interview 14, Pos. 34.

1688 Interview 3, Pos. 96, 102; Interview 7, Pos. 40, 42.

1689 Interview 5, Pos. 40; Interview 15, Pos. 76; interessanterweise sind die beiden interviewten Personen in diesen beiden Fällen stark juristisch arbeitende Datenschutzbeauftragte.

1690 Interview 5, Pos. 40; Interview 14, Pos. 68.

men, innerhalb derer es viele länderspezifische Techniklösungen gibt[1691] und behindert andererseits auch eine einheitliche(re) Datenschutz-Praxis,[1692] wie bereits oben für die Instrumente von Datenschutz-Folgenabschätzung, Errichtungsanordnung und Verzeichnis von Verarbeitungstätigkeiten beispielhaft beschrieben wurde. Neben dieser länderübergreifenden Kritik wird auch das jeweilige polizeiliche Datenschutzrecht der Länder kritisiert, etwa bezüglich der umständlichen Systematik der Gesetze.[1693] Auch in diesem Zusammenhang wird ganz grundsätzlich eine unzureichende dogmatische Durchdringung der polizeilichen Datenverarbeitung als Problem gesehen.[1694]

Im Grunde wird das polizeiliche Informationshandeln aber auch nur mittelbar vom polizeilichen Datenschutzrecht reguliert, da zwischen beiden Ebenen noch die organisationseigenen Normen in Form der polizeilichen Dienstvorschriften (PDV) und der Richtlinien über Kriminalpolizeiliche personenbezogene Sammlungen (KPS-Richtlinien) als vermittelnde Instanz fungieren.[1695] Die Aufwände zur Abstimmung der internen Vorschriftenlage an die Gesetzeslage werden als groß aber bewältigbar beschrieben.[1696] Nichtsdestotrotz werden die Probleme der Regulierung polizeilicher Informationsverarbeitung zu einem wesentlichen Teil hier verortet:

> „Die Polizei arbeitet nach Vorschrift […] und zwar nach der Polizei-Dienstvorschrift, PDV, und so sind auch die gesamten Systeme ausgelegt. Das Problem ist aber, die PDV ist keine Rechtsgrundlage. Die Dinge, die in der PDV festgeschrieben sind, die spiegeln sich nicht im Gesetz wieder. Das heißt, da hat der Gesetzgeber noch einiges vor sich. Entweder ändert er die PDV ab oder lässt sie abändern oder er ändert die Gesetze ab. Eins von zwei. Das ist jetzt auch hier gemeint, das heißt die Polizei… also PDV gilt ja hauptsächlich für die Schutzpolizei. Ansonsten sind wir ja in den kriminalpolizeilichen Personendatensammlung, in der KPS-Richtlinie, drin. Das geht prinzipiell so nicht, d.h. also Sie versuchen verzweifelt für einen Sachverhalt eine Rechtsgrundlage zu finden und dann wird es schon schwierig da eine zu finden. Nach PDV ist das

1691 Interview 3, Pos. 94.
1692 Interview 3, Pos. 40.
1693 Interview 9, Pos. 42; Interview 12, Pos. 38; Interview 14, Pos. 136.
1694 Interview 15, Pos. 96.
1695 Interview 12, Pos. 40.
1696 Interview 12, Pos. 40.

> alles ganz klar, die Polizisten machen das 40 Jahren so. Jetzt könnte man sagen: „Nur weil man es immer so gemacht hat, heißt es nicht, dass man es weiter so machen muss." Aber das Schlechte daran ist, dass es in der Vorschrift genau so drin steht, wie die das machen. Die arbeiten da nicht im luftleeren Raum, die arbeiten nach Vorschrift. Nur passt halt eben die Vorschrift weder auf die Gesetzeslage noch auf das Datenschutzgesetz. Das heißt also, hier hat die Polizei in Gesamtdeutschland nochmal ein großes Stück Arbeit vor sich."[1697]

Da also die Arbeitsprozesse sich eher an diesen nicht-gesetzlichen Normen orientieren und die Informationstechnologie für die polizeiliche Praxis diese Arbeitsprozesse als Anknüpfungspunkt nimmt, entsteht ein polizeiliches Informationswesen, das zwar an polizeifachlichen Bedürfnissen ausgerichtet ist, aber an der Gesetzeslage vorbeisteuert.[1698] Vor diesem Hintergrund wäre es für den Gesetzgeber erforderlich, sich über die Datenverarbeitungsprozesse der Polizei zu informieren und auf dieser Grundlage sein Regulierungsmodell weiter auszubauen.[1699] Allerdings scheinen selbst der Polizei diese Arbeitsprozesse in ihrer Gänze nur unzureichend bekannt zu sein:

> „Dann hat auch noch nie jemand die gesamte Datenverarbeitung der Polizei insgesamt betrachtet, das heißt also einen kompletten Workflow von der Straße oder vom Ladendiebstahl bis hinten nach Schengen betrachtet. Das heißt, die gesamten Geschäftsprozesse in der Polizei sind eigentlich unklar und würden die Geschäftsprozesse mal klar dargelegt werden, was eine Voraussetzung ist, um eine einheitliche und klare Gesetzgebung zu ermöglichen, dann wären wir da schon mal einen riesigen Schritt weiter."[1700]

Die Verstrickungen des polizeilichen Datenverarbeitungsrechts erschweren anscheinend auch einigen Datenschutzbeauftragten die Orientierung, sodass teilweise nur eine begrenzte Rezeption zentraler Entwicklungen vollzogen wird, wie wenn etwa der Grundsatz der hypothetischen Datenneuerhebung als für die eigene Praxis nicht relevante Teilfrage von Polizei

1697 Interview 14, Pos. 32.
1698 Interview 14, Pos. 81 ff.
1699 Interview 14, Pos. 30; kritisch zur Uninformiertheit des Gesetzgebers bei der Normierung von Informationsverarbeitungstechnologien auch die Befragten bei *Egbert/Leese,* Criminal futures, S. 166.
1700 Interview 14, Pos. 80.

2020 gesehen wird[1701] oder als Stichwort nicht wirklich bekannt ist.[1702] Verstärkt wird die rechtliche Orientierungslosigkeit, wie bereits angedeutet, durch ein als unbefriedigend empfundenes Angebot dogmatischer Aufbereitung des polizeilichen Datenschutzrechts.[1703] Neben den Problemen der Gesetzeslage kommt dabei als erschwerender Faktor zudem hinzu, „dass derjenige, der guten Gewissens das Recht anwendet, gar nicht mehr weiß, wo er ansetzen soll, weil es technisch unüberschaubar ist."[1704]

Perspektivisch scheinen weitere Herausforderungen auf die Regulierung des polizeilichen Informationswesens zuzukommen. Wird auch das Prinzip der automatisierten Datenanalyse, wie sie in § 25a HSOG, (dem nunmehr nicht mehr geltenden) § 49 HmbPolDVG oder auch § 23 Abs. 6 PolG NRW vorgesehen ist, als „gefühlt, nicht schlimm" bezeichnet, da es nur um die Auswertung der eigenen Daten geht,[1705] so wird doch auch die Einschätzung geäußert, dass die normgemäße Ausgestaltung neuer polizeilicher Informationstechnologien und der datafizierten Polizeiarbeit, deren Kern die Zusammenführung von Daten zur Generierung weiterführender Informationen ist, nicht nur oder überwiegend rechtlich adressiert werden kann, sondern besonders stark technisch eingehegt werden muss.[1706] Dabei dürfe aber auch das Recht als Fundament etwa zugunsten reiner technischer Lösungen nicht aufgegeben werden.[1707] Die in diesem Kontext geforderte Normenklarheit[1708] tritt dabei in das bekannte Spannungsverhältnis, das bei der Regulierung schnell voranschreitender Technik gleichzeitig ein gewisses Abstraktionsniveau erforderlich macht.[1709] Moderne Datenanalyseinstrumente wie Anwendungen von „Predictive Policing" werden insofern als „sehr große Herausforderung" für das polizeiliche Datenschutzrecht gesehen.[1710] Die interdisziplinäre Natur der Regelungsgegenstandes macht es zudem erforderlich, dass auch die Perspektive der Techniker:innen berücksichtigt wird, die eigene Prozesse haben und eigenen Zwängen ausgesetzt

1701 Interview 2, Pos. 134.
1702 Interview 10, Pos. 81 f.
1703 Interview 3, Pos. 109.
1704 Interview 5, Pos. 52.
1705 Interview 1, Pos. 138.
1706 Interview 1, Pos. 136.
1707 Interview 4, Pos. 42.
1708 Interview 1, Pos. 122.
1709 Interview 5, Pos. 36.
1710 Interview 10, Pos. 49.

sind,[1711] wobei die technologisch fundierten Informationspraktiken der Polizei andererseits auch wieder vor Gericht bestehen müssen, um einsetzbar zu sein.[1712] Zusammengefasst ergibt sich ein Bild vom polizeilichen Datenschutzrecht als äußerst lebendige Rechtsmaterie,[1713] die aber aufgrund ihrer komplexen Zielsetzung, das informationstechnologisch fundierte und historisch gewachsene Informationshandeln der Polizei mit verfassungsrechtlichen Vorgaben übereinzubringen, in ihrer Ausgestaltung und Anwendung durchaus stark problembehaftet ist und deshalb nur begrenzt die von ihr erwartete normative Steuerungsleistung erbringen kann.

V. Technische Aspekte des polizeilichen Datenschutzes

Wie bereits mehrmals angeklungen, ist Datenschutz oder vielmehr die polizeiliche Informationsverarbeitung, die durch datenschutzrechtliche Bestimmungen dem Versuch der Normierung und Begrenzung unterzogen wird, ein im Grunde dreigeteiltes Feld, das neben Recht durch polizeiliche Fachlichkeit und die Technizität der Informationsverarbeitungsverfahren bestimmt wird. Um letzteres, also die technischen Aspekte polizeilichen Datenschutzes soll es nun im Folgenden gehen.

Da mit der rechtlichen Ebene eine normative Orientierungsfunktion verbunden ist, wird der grundsätzliche Zusammenhang von Recht und Technik in der polizeilichen Informationsverarbeitung in einem einseitigen Beeinflussungsverhältnis verortet: Die Technik muss durch das Recht eingehegt werden.[1714] Das ist umso mehr der Fall, weil „Sicherheitsbehörden [...] fast alles [dürfen], materiell-rechtlich", und ihre Befugnisse zudem immer weiter ausgedehnt würden,[1715] was im Umkehrschluss bedeutet, dass es vor allem die formell-rechtlichen Elemente des Datenschutzes sind, die in der Technik wirksam werden müssen. Dieses Bewusstsein für die

1711 Interview 6, Pos. 68; beispielsweise haben auch Techniker:innen rechtliche Bedürfnisse, etwa Vorschriften, die das Testen von Systemen erlauben, was gegenwärtig nur in sehr begrenztem Umfang möglich ist, für eine datafizierte Polizei aber rechtssicher möglich sein muss, Interview 14, Pos. 138.

1712 Interview 6, Pos. 54; wobei gerade derartige technologische Innovationen bei der Polizei eine wissenschaftliche Aura haben, die auch Objektivität ausstrahlt, wie man es etwa von der Technologie der DNA-Identifizierung her kennt, vgl. *Lynch/Cole/McNally* ua, Truth Machine.

1713 Interview 12, Pos. 38.

1714 Interview 1, Pos. 122.

1715 Interview 1, Pos. 45.

techniksteuernden Impulse des Rechts gibt es auch in den technischen Organisationseinheiten, in denen die anlässlich der JI-Richtlinie novellierten Polizeigesetze etwa zu Analysen, welche Anforderungen die Novellierungen konkret für die polizeilichen Systeme bedeuten, und darauf bezogenen Anpassungsbemühungen geführt haben.[1716] Gleichzeitig – und weniger im Bewusstsein der Befragten – deutet dies auf ein Primat der Technik in dem Sinne hin, dass rechtliche Vorgaben im Informationswesen eigentlich nur noch technisch umgesetzt werden können und daher entscheidend von der Konfiguration der Technik abhängt, inwieweit das Datenschutzrecht wirksam bzw. die polizeiliche Informationsverarbeitung an die gesetzlichen Vorgaben angepasst wird.[1717] Insofern bestimmen die Programmcodes des polizeilichen Informationswesens die Gesetzesumsetzung zu einem wesentlichen Teil mit[1718] und wenn sich das Recht ändert, ist die Wirklichkeit polizeilicher Informationsverarbeitung zunächst immer weiter durch die technischen Gegebenheiten determiniert. Oft muss dann zur erneuten Anpassung ans Recht wieder eine Änderung der technischen Strukturen vorgenommen werden. Dennoch besteht bei den Datenschutzbeauftragten der Anspruch, die Technik mit dem Recht zu steuern,[1719] wobei die Implementierung datenschutzrechtlicher Belange in die technischen Strukturen nicht immer einfach ist:

> „Gerade bei so einer IT-Abteilung besteht die große Gefahr, dass wenn man die zu sehr autark arbeiten lässt, dass die sich dann verselbstständigen und wichtige Aspekte des Datenschutzes vielleicht dann nicht so Berücksichtigung finden, als wenn man da eng dran wäre und eben sich lieber mal Sachen nochmal erklären lässt, obwohl man sie vielleicht weiß, und dann aber nochmal beim Gegenüber ein gewisser Erinnerungs- oder Lerneffekt nochmal greift."[1720]

Dafür ist technisches Grundwissen Voraussetzung für Datenschutzbeauftragte.[1721] Das eigene technische Wissen der Beauftragten hängt ganz we-

1716 Interview 6, Pos. 38.
1717 Interview 6, Pos. 38.
1718 Grundlegend und viel zitiert im Kontext dieser Idee der normierenden Kraft von *Lessig*, Code.
1719 Interview 7, Pos. 32.
1720 Interview 11, Pos. 32.
1721 Interview 12, Pos. 26: „Also als behördlicher Datenschutzbeauftragter muss man meines Erachtens entweder juristisch vorgebildet sein und ein Interesse für IT-Technik haben oder man sollte letztlich IT-mäßig vorgebildet sein und ein recht-

sentlich vom jeweiligen Werdegang ab und auch, wenn es nicht der einzig erforderliche Wissenstypus ist, so handelt es sich schon um einen wesentlichen Faktor für die Aufgabenerfüllung der Datenschutzbeauftragten im Rahmen des internen Datenschutzkontrollregimes.[1722] Entsprechendes Wissen wird auch als zunehmend wichtiger wahrgenommen, weil Datenbanken und Datenverarbeitung immer stärker digitalisiert werden.[1723] Wo das eigene Wissen nicht ausreicht, wird es regelmäßig ergänzt durch tiefergehende Expertise, die mittels dann notwendiger Konsultation der eher technisch ausgerichteten Stellen innerhalb der eigenen Behörde gewonnen werden kann[1724] oder in selteneren Fällen etwa auch durch Schulungen beispielsweise zu Vorgangsbearbeitungs- oder Fallbearbeitungssystemen als eigenes Wissen erworben werden kann.[1725] Als „oftmals nicht ganz optimal" wurde von einer Person vor diesem Hintergrund auch der Umstand bezeichnet, dass Datenschutzbeauftragte überwiegend Jurist:innen seien.[1726] So verwundert es vor diesem Hintergrund auch nicht, dass recht häufig auch von nur begrenztem Wissen über technische Abläufe der polizeilichen Informationsverarbeitung berichtet wird.[1727] Demgegenüber gut aufgestellt sind die vereinzelten Datenschutzbeauftragten, die ein Informatikstudium oder ähnliche technische Ausbildungen durchlaufen haben, wodurch sie wertvolles Wissen in die Steuerung polizeilicher Informationsverarbeitung einbringen,[1728] beispielsweise wie man als Polizist:in Kontrollmechanismen in den polizeilichen Informationssystemen umgehen könnte.[1729]

Andere technische Fragen, die wichtig für die Tätigkeit der Datenschutzbeauftragten sind und den datenschutzrechtlichen Vorgaben zur Wirksamkeit verhelfen können, sind etwa, welche Daten überhaupt verarbeitet werden, wie hoch das Schutzbedürfnis ist und wie diesem durch technisch-organisatorische Maßnahmen entsprochen werden kann, welche Algorithmen eingesetzt werden, wie Schnittstellen zwischen Datenbanken gestaltet

---

liches Interesse haben. Irgendwie beides braucht man, man muss da eine Art Symbiose haben."

1722 Interview 1, Pos. 45.

1723 Interview 4, Pos. 7.

1724 Interview 1, Pos. 51; Interview 2, Pos.100; Interview 5, Pos. 23, 52, 68; Interview 8, Pos. 23; Interview 9, Pos. 22; Interview 10, Pos. 28.

1725 Interview 4, Pos. 30.

1726 Interview 1, Pos. 45.

1727 Interview 3, Pos. 36; Interview 7, Pos. 18; Interview 13, Pos. 105; Interview 15, Pos. 30.

1728 Interview 4, Pos. 40.

1729 Interview 4, Pos. 28.

sind oder welche Anwendungen generell in der polizeilichen Informationsverarbeitung genutzt werden.[1730] Bei diesem Informationsbedürfnis verwundet es nicht, dass die Techniker:innen innerhalb der Polizei mitunter eher als Berater:innen des Datenschutzes fungieren als umgekehrt.[1731] Zudem obliegt die faktische Umsetzung der datenschutzrechtlichen Vorgaben eben den Organisationseinheiten, die sich um die technische Seite des Informationswesens kümmern.[1732]

Die Techniker:innen der Polizeien sind wiederum damit konfrontiert, dass die praktischen Anforderungen polizeilicher Informationsverarbeitung nach Innovationen bei den technischen Datenverarbeitungstechnologien verlangen. Projekte, wie etwa Polizei 2020, das als zentrale Komponente die Abschaffung bzw. Transzendierung der Datei als Rahmengröße für die polizeilichen Informationsverarbeitungsprozesse beabsichtigt, haben komplexe datenschutzrechtliche Implikationen, die eine ebenso komplexe technische Seite mit sich bringen.[1733] Durch die geplante Umstrukturierung von Datenbeständen sind für einzelne personenbezogene Datensätze in den technischen Strukturen des Systems die verschiedenen gesetzlichen Grundlagen der Länder und des Bundes umzusetzen:

> „Sie haben halt einen Datensatz und da haben Sie normalerweise dann Tags oder Marker für Löschen oder für die Kennzeichnung dran. Und jetzt haben Sie 20 unterschiedliche Löschfristen und dann müssen Sie das Berechtigungsmanagement noch so schalten, dass das nach 20 unterschiedlichen gesetzlichen Vorschriften geht. Das heißt also, das alles in einen Datensatz und eine Datenbank zu integrieren, ist auch nicht gerade vergnügungssteuerpflichtig. Da rauchen schon ganz schön die Köpfe. Das muss ja auch funktionieren am Schluss. […] Also extremer Aufwand in den Datensätzen."[1734]

Darüber hinaus muss der Grundsatz der hypothetischen Datenneuerhebung in diesem „Datenhaus"[1735] eingehalten werden, was ebenfalls über das Setzen von Kennezeichnungen (§ 14 BKAG) in Form von Markern oder Tags (technisch) unterstützt werden muss, weil eine Verwirklichung der

1730 Interview 1, Pos. 45; Interview 4, Pos. 45; Interview 14, Pos. 18.
1731 Interview 6, Pos. 38.
1732 Interview 6, Pos. 18.
1733 Interview 1, Pos. 116.
1734 Interview 14, Pos. 64.
1735 *Bundesministerium des Innern*, Polizei 2020.

verfassungsrechtlichen Vorgaben anders nicht möglich ist.[1736] Neben solchen Großprojekten gibt es auch konkretere rechtlich angedachte Technikstrukturen, deren Umsetzung große Aufwände erforderlich machen würde, wie etwa die Unterscheidung der JI-Richtlinie zwischen Tatsachen und Einschätzungen, also personenbezogene Daten, die auf Tatsachen beruhen und solchen, die auf Einschätzungen beruhen.[1737] Insgesamt befindet sich vor allem die Entwicklungsphase von informationstechnologischen Projekten bei der Polizei in einem Zwiespalt zwischen dem Bedürfnis der Informatiker:innen nach größtmöglicher Freiheit beim Programmieren und den festgeschriebenen rechtlichen Vorgaben.[1738]

Neben der Umsetzung von datenschutzrechtlichen Vorgaben zum Schutz der Betroffenen ist ein signifikanter Teil des technischen Datenschutzes auch Daten- bzw. Informationssicherheit, denn

> „für die Polizei geht es natürlich nicht nur darum, die Daten Externer, Betroffener zu schützen, sondern auch die eigenen Prozesse zu schützen, geheim zu halten oder sicher zu halten."[1739]

Die notwendige technische Ausgestaltung des Datenschutzes wurde in seiner Bedeutung auch im Recht erkannt, wo dies durch die bereits erläuterten technisch-organisatorischen Maßnahmen ins normative Programm des Datenschutzes aufgenommen wurde.[1740] Darunter fällt allen voran das Zugriffsmanagement, das mittels Kennung und zugehöriger Berechtigung Zugriff auf bestimmte Systeme gewährt oder verweigert. Mit diesem sogenannten Rollen- und Berechtigungskonzept kann dann beispielsweise deliktsübergreifend arbeitenden Polizeieinheiten, die mehrere Phänomenbereiche einsehen können müssen,[1741] ein adäquater Datenzugriff gewährt werden. Wichtig ist daneben die Automatisierung von Löschpflichten,[1742] die sich händisch gar nicht mehr bewältigen lassen, sodass bereits bei Erhebung bestenfalls Löschfristen eingetragen werden, die dann auf allen möglichen Ablageservern der erhobenen Daten immer synchronisiert wer-

1736 Interview 14, Pos. 58.
1737 Interview 1, Pos. 70, es wird nach Angaben der befragten Person gegenwärtig allerdings nicht geplant, diese Unterscheidung technisch umzusetzen, u.a. weil auch die Unterscheidung als rechtsfolgenlos gesehen wird.
1738 Interview 14, Pos. 92.
1739 Interview 1, Pos. 53.
1740 Siehe dazu bereits oben S. 366 ff.
1741 Interview 4, Pos. 45, 47.
1742 Interview 10, Pos. 70.

den (müssen).[1743] Das gilt insbesondere auch zwischen staatsanwaltschaftlichen Sachständen und polizeilichen Datenbeständen, sodass hier eine technische Automatisierung der Löschung strafverfahrensrechtlich nicht mehr benötigter Daten den Rechten Betroffener zur Verwirklichung verhelfen kann.[1744] Immer wichtiger werden zum Beispiel auch technische Sicherungen gegen Fehlidentifizierungen von Personen über die Auswertung von Datensätzen, die innerhalb der datafizierten Polizeiarbeit nur noch durch technisch-organisatorische Maßnahmen eingezogen werden können.[1745]

Insgesamt ist eine Kooperation, eine „Symbiose"[1746] zwischen juristischem und technischem Wissen notwendig, damit ein zufriedenstellendes Wirksamkeitsniveau der datenschutzrechtlichen Vorgaben weiter sichergestellt werden kann.[1747] Dabei muss, wie erwähnt, aber stets auch die Polizeifachlichkeit mit in diese Symbiose involviert werden. Für diese Prozesse ist es wichtig, diese Trias von Faktoren von Anfang an zusammenzudenken, damit etwa die Informationssysteme, wie eingangs betont, technisch die datenschutzrechtlichen Vorgaben von vornherein umsetzen und auch in der Zukunft eine Anpassung an sich wandelnde Gesetzeslagen möglich bleibt.[1748] Perspektivisch wurde vor diesem Hintergrund eine Steigerung technischer Expertise bei Datenschutzbeauftragten ohne technischen Werdegang verlangt.[1749]

VI. Das Verhältnis der Polizei zum Datenschutz

Die Arbeit der Datenschutzbeauftragten steht in einem direkten Einflussverhältnis zur fachlichen Polizeiarbeit, egal ob schutz- oder kriminalpolizeilich. Da polizeiliches Handeln heutzutage im Wesentlichen informationelles Handeln ist, wirkt sich das polizeiliche Datenschutzrecht, das im Grunde nichts anderes als die Regulierung dieses informationellen Han-

1743 Interview 4, Pos. 43
1744 Interview 13, Pos. 47, wo davon berichtet wird, dass „mit Übermittlung der eMAV [elektronische Mitteilung über den Ausgang des Verfahrens, FB] und endgültigen Erledigungsmitteilung über eine Schnittstelle von der Staatsanwaltschaft in das System „ComVor" […] der Vorgang abgeschlossen [ist]."
1745 Interview 14, Pos. 76.
1746 Interview 11, Pos. 41.
1747 Interview 5, Pos. 52; Interview 12, Pos. 18.
1748 Interview 14, Pos. 92.
1749 Interview 14, Pos. 14.

delns ist, direkt auf polizeiliche Tätigkeiten aller Art aus. Mit Blick auf die Ausrichtung des polizeilichen Datenschutzrechts, die vorrangig den Grundrechtsschutz von Betroffenen der polizeilichen Datenverarbeitung bezweckt, verwundert es nicht, dass das Recht und die daran geknüpfte Tätigkeit der Datenschutzbeauftragten als die polizeiliche Praxis bremsend wahrgenommen wird.[1750] So wird davon berichtet, dass gesetzliche Regelungen der Polizei in manchen Ermittlungsverfahren die Hände binden, etwa im Bereich der Cyberkriminalität.[1751] Das „Korsett" polizeilichen Informationshandelns würde immer enger geschnürt,[1752] sodass auf den Ermittlungserfolg fokussierte Polizeiarbeit und datenschutzrechtliche Belange manchmal nur schwer übereingebracht werden können.[1753] Polizeilicher Datenschutz ist in dieser – auf Ermittlungen fokussierten – Wahrnehmung unnötige Verwaltung, es sei denn, es geht um den Schutz der polizeilichen Daten vor äußeren Gefahren,[1754] was wiederum mittelbar der Absicherung des Ermittlungserfolges dient. Störungen der polizeilichen Arbeitsabläufe ergeben sich auch durch die vielfältig erforderlichen datenschutzrechtlichen Anpassungs- und Lernerfordernisse der polizeilichen Organisationen,[1755] was laufend Mehraufwände für die Polizist:innen produziert.[1756] Gleichzeitig beseht ein Bewusstsein dafür, dass nicht alles, was technisch möglich wäre, auch rechtlich erlaubt ist,[1757] die Polizei also aufgrund rechtlicher Vorschriften teilweise hinter ihren (technologischen) Möglichkeiten zurückbleibt. Vor diesem Hintergrund verwundert es dann auch nicht, dass Datenschutzbeauftragte als „Spielverderber"[1758] oder „Störfaktor[en]"[1759] wahrgenommen werden und als „Sonderlinge" im eigenen Haus[1760] und „Einzelkämpfer" gelten, denen auch Ablehnung entgegenschlägt.[1761] Datenschutz werde „natürlich […] als etwas Nervendes empfunden".[1762]

1750 Interview 1, Pos. 37.
1751 Interview 4, Pos. 53.
1752 Interview 4, Pos. 42.
1753 Interview 12, Pos. 18.
1754 Interview 14, Pos. 12.
1755 Interview 12, Pos. 12, 16.
1756 Interview 8, Pos. 11.
1757 Interview 6, Pos. 27 f.
1758 Interview 1, Pos. 37, wobei das als universelle Zuschreibung an „den" Datenschutz überall gesehen wird.
1759 Interview 6, Pos. 14.
1760 Interview 1, Pos. 59.
1761 Interview 9, Pos. 16, 18
1762 Interview 15, Pos. 50.

Neben den verursachten Mehraufwänden und scheinbaren oder tatsächlichen Beeinträchtigungen der polizeilichen Effektivität liegt dies wohl auch daran, dass der Mehrwert des Datenschutzes von Polizeibeamt:innen häufig nicht erkannt wird, sodass die Vorschriften eher als lästig empfunden werden:

> „Denn es geht am Ende ja doch um die Aufrechterhaltung einer Idee. Der Konformität. Denn gerade im öffentlichen Bereich haben wir im Gegensatz zum nicht-öffentlichen Bereich ein kaum vorhandenes Sanktionsregime."[1763]

Ferner wird das Verhältnis der Polizei zum Datenschutz mitunter durch die Überwachungs- und Kontrollfunktion der Datenschutzbeauftragten strapaziert:

> „Man hat das Gefühl, beobachtet und kontrolliert zu werden. Das schätzen die meisten Leute natürlich nicht, niemand wird gerne kontrolliert."[1764]

Gerade das ist allerdings ein intentionaler Teilaspekt polizeilichen Datenschutzes: Die Polizist:innen sollen auch abgeschreckt werden, etwa durch die bereits dargestellten Protokollierungen.[1765] Kommt es in diesem nicht ganz unkomplizierten Verhältnis zu Konflikten, hat sich nach Aussage einer befragten Person die die Ansiedelung der Datenschutzbeauftragten bei der Behördenleitung bewährt, da datenschutzrechtliche Belange so eine innerorganisationale Legitimierung erfahren.[1766]

Trotz dieses Konfliktpotenzials wird aber bei den meisten Polizeibeamt:innen ein Wille zur Umsetzung der für sie geltenden Normen beobachtet,[1767] was einerseits auf das Wesen der Beschäftigten und andererseits auf das Legitimationsbedürfnis gegenüber der Gesellschaft zurückgeführt wird, das erfordert, dass sich die Polizei stark am Ideal der Regelkonformität ausrichtet.[1768] Täte sie dies im Bereich des Datenschutzes nicht, könnte die polizeiliche Tätigkeit in Verruf geraten.[1769] Polizist:innen bekommen

1763 Interview 1, Pos. 39.
1764 Interview 1, Pos. 39.
1765 Interview 4, Pos. 24.
1766 Interview 11, Pos. 24.
1767 Interview 13, Pos. 28.
1768 Interview 1, Pos. 37.
1769 Interview 12, Pos. 18.

Datenschutz zudem auch von Anfang an beigebracht,[1770] was nicht verwundert, da das polizeiliche Datenschutzrecht im Grunde schlicht die negative normative Formulierung und Rahmung einer der zentralen polizeilichen Tätigkeiten, der Informationsverarbeitung, ist. Nichtsdestotrotz sind juristische Expert:innendiskurse den Polizeibeamt:innen nur begrenzt vermittelbar,[1771] was eine Synthese zwischen Datenschutz und polizeilicher Praxis mit Blick auf die beschriebenen Komplexitäten des Rechts der polizeilichen Informationsverarbeitung erschwert.[1772]

So wächst beispielsweise die Akzeptanz für die Speicherfristzyklen und Löschungspflichten und die daraus folgende limitierte Verfügbarkeit von Daten,[1773] gleichzeitig wird aber auch noch davon berichtet, dass Daten nach wie vor gesammelt werden und die Polizei nur sehr ungern Wissen aufgibt, also Daten löscht.[1774] Auch gibt es, wie hinreichend aus medialer Berichterstattung bekannt ist,[1775] weiterhin Fälle von (intentionalen) Datenschutzverstößen, die aber etwa im Bereich des Datenmissbrauchs eher als Einzelfälle gesehen werden („Schwarzes Schaf"[1776]).

Die damit angesprochene Sensibilisierung scheint gegenwärtig noch zu divergieren. Berichtet wird von hoher oder vielleicht sogar Über-Sensibilisierung, wenn Polizeibeamt:innen aufgrund von Datenschutzbedenken ihre gesetzlichen Aufgaben teilweise zögerlicher als zuvor erfüllen.[1777] Teilweise wird aber auch von einer noch nicht ganz adäquaten Sensibilität gesprochen, wobei diese sich aber entwickle.[1778] Vor dem Hintergrund zunehmender Empfänglichkeit[1779] für die dem Datenschutz zugrundeliegenden normativen Konzepte in der Gesellschaft wundert es auch nicht, dass Polizist:innen ebenfalls wollen, dass die zu ihnen verfügbaren personenbezogenen Daten, etwa Protokolldaten, bei ihrer Behörde datenschutzkonform verwendet werden.[1780]

1770 Interview 10, Pos. 89.
1771 Interview 12, Pos. 38.
1772 Interview 13, Pos. 70.
1773 Interview 10, Pos. 74.
1774 Interview 13, Pos. 72.
1775 Siehe dazu bereits Fn. 730.
1776 Interview 3, Pos. 58; Interview 4, Pos. 24.
1777 Interview 3, Pos. 86; Interview 12, Pos. 12, 16.
1778 Interview 14, Pos. 76.
1779 Interview 10, Pos. 46.
1780 Interview 9, Pos. 68; Interview 10, Pos. 47 ff.; Interview 15, Pos. 16 ff.

Alles in allem wird zwischen Polizei und Datenschutz insgesamt von einem guten Zusammenarbeitsverhältnis berichtet,[1781] in dem die Datenschutzbeauftragten kooperativ und beratend mit der polizeilichen Fachlichkeit zusammenarbeiten, wobei dies, wie bereits zuvor dargelegt, auch maßgeblich vom Zuschnitt der Position der Datenschutzbeauftragten abhängt: Ist der Datenschutz eher reaktiv organisiert, dann gibt es auch weniger konfrontatives Potenzial.[1782] Daneben wird die Herkunft von Datenschutzbeauftragten aus dem Polizeivollzugsdienst als Faktor für ein kooperatives Verhältnis gesehen.[1783] Beratungen durch die Beauftragten werden von der Polizeifachlichkeit angenommen,[1784] was aber auch daran liegt, dass die Polizei, vor allem für ihre informationstechnologischen Projekte, auf die Datenschutzbeauftragten angewiesen ist („Die wissen ganz genau, ohne den Datenschützer geht gar nichts und sind natürlich deshalb ausgesprochen höflich und freundlich").[1785] Mitunter wünschen sich Fachabteilungen auch konkrete Vorgaben durch die Datenschutzbeauftragten, weil die Orientierung im Geflecht des polizeilichen Datenschutzes, wie beschrieben, schwerfällt.[1786] Ein vertrauensvolles Verhältnis müsse aber erarbeitet werden[1787] und kann daher wohl nicht als Selbstverständlichkeit gelten.

Trotz der teilweise schwer vereinbaren Zielrichtungen der dem Datenschutz zugrundeliegenden normativen Ideen und der operativen Polizeiarbeit, ist polizeiliches Datenschutzrecht als Normierung polizeilichen Informationshandelns unabdingbar. Datenschutz muss daher, damit er von der polizeilichen Fachlichkeit wahrgenommen wird, bestenfalls direkt und frühzeitig in die fachlichen Konzepte einfließen und sollte nicht als unverbundenes Etwas daneben stehen.[1788] Insofern hängt der Datenschutz aber auch ganz maßgeblich von der Mitwirkung der polizeilichen Fachlichkeit ab, da die gesetzlichen Vorgaben ansonsten nicht mit Leben gefüllt werden können.[1789] Auch darf nicht übersehen werden, dass der Datenschutz als

1781 Interview 1, Pos. 37; Interview 4, Pos. 24; Interview 7, Pos. 16; Interview 9, Pos. 16; Interview 10, Pos. 24; Interview 11, Pos. 22; Interview 13, Pos. 29; dabei ist das natürlich vorrangig die Sicht der Datenschutzbeauftragten.
1782 Interview 2, Pos. 52; Interview 7, Pos. 14.
1783 Interview 8, Pos. 16.
1784 Interview 5, Pos. 32.
1785 Interview 9, Pos. 16.
1786 Interview 15, Pos. 22.
1787 Interview 3, Pos. 30.
1788 Interview 9, Pos. 34, 66.
1789 Interview 11, Pos. 26.

etwas „Nervendes“ empfunden werden muss, um ins Bewusstsein der Polizeibeamt:innen zu dringen und Sensibilisierungswirkungen auslösen zu können.[1790]

VII. Organisation der polizeilichen Informationsverarbeitung

Das polizeiliche Informationswesen ist wie dargelegt bereits seit weit vor dem Volkszählungsurteil entstanden,[1791] sodass es neben den verschiedenen Ausprägungen des Datenschutzes und den ihn ausgestaltenden Datenschutzbeauftragten auch von im Wesentlichen technisch und polizeifachlich geprägten organisatorischen Eigendynamiken geformt wurde und wird. Diese zusätzlich zum polizeilichen Datenschutz zu beleuchten, ist für ein Verständnis des polizeilichen Informationswesens unerlässlich.

Staatliche und damit auch polizeiliche Informationsverarbeitung ist ressortspezifisch organisiert. Dabei wird die – auch rechtliche bestehende – Unterteilung in Ressorts technisch seit den Anfängen der Digitalisierung durch Datenmodelle und Datenaustauschformate verwirklicht, sodass innerhalb eines abgegrenzten Bereichs miteinander kommuniziert werden kann. Lange Zeit gab es indessen auch innerhalb des Polizeiressorts nur begrenzt interoperable Datenmodelle, was mit dem Informationsmodell XPolizei geändert wurde. Auf diese Weise werden Datenflüsse zwischen den Polizeien vereinfacht. Zu anderen Ressorts gibt es hingegen dadurch zunächst nur eine begrenzte Austauschbarkeit, was etwa im Falle der Justiz, die XJustiz nutzt, problematisch ist. Um auch hier eine Austauschbarkeit herzustellen, müssen die Standards ständig mitlaufend harmonisiert werden, was die Kommunikation mit gewissen Widerständen versieht. Gegenwärtig laufen darüber hinaus Planungen zu einem verwaltungsübergreifenden Datenmodell, genannt X-ÖV[1792], das externe Kompatibilität des XPolizei-Modells mit den Informationssystemen der öffentlichen Verwaltung sicherstellen soll und perspektivisch ist eine „Abbildung behördenübergreifender und internationaler Prozesse Bestandteil des Harmonisierungsprojektes.“[1793]

1790 Interview 15, Pos. 50.
1791 Siehe dazu bereits oben S. 101 ff.
1792 Interview 6, Pos. 64.
1793 https://www.xoev.de/die-standards/uebersicht-aller-xoev-standards/xpolizei-11268 (Stand: 01.10.2023).

Die Beschreibung dieser vielfältigen Vernetzungsstrukturen von Informationen bei der Organisation[1794] in entsprechenden Systemen deutet schon in den Grundlagen auf einen – schon zur Sprache gekommenen – zentralen Befund hin: Das polizeiliche Informationswesen und seine Teilkomponenten sind „höchstkomplex".[1795] Aufgrund technischer, aber auch rechtlicher und polizeifachlicher Faktoren unterliegt die polizeiliche Informationstechnik einem stetigen Weiterentwicklungsprozess, wobei immer eine Abstimmung der vielfältigen und unterschiedlichen Verästelungen des Informationswesens erfolgen muss, wenn sich neue Anforderungen ergeben und diese in befriedigender Weise eingearbeitet werden sollen. Da die Systeme „dicht miteinander verwoben sind", gibt es Kaskadeneffekte, die bei Veränderungen einer Komponente auf die anderen Teile übergreifen. Um die dafür erforderlichen organisatorischen Abstimmungen durchzuführen hat sich eine Gremienstruktur etabliert.[1796] Fragen, die bei allen Änderungen geklärt werden müssen, sind etwa: Ist die Änderung technisch möglich? Ist sie sinnvoll? Ist die geplante Änderung im Informationswesen bereits hinreichend optimiert? Können die Beamt:innen damit arbeiten? Ist die Umstrukturierung rechtmäßig?[1797] Zudem ist das polizeiliche Informationswesen auf einer speziellen, informationstechnologischen Sicherheitsstandards genügenden Infrastruktur errichtet und alle Neuerungen müssen sich auch unter diesem Gesichtspunkt implementieren lassen.[1798]

Dabei ist polizeiliche Informationsverarbeitung, wie aus den vorstehenden Fragen ersichtlich wird, auch aus dieser eher technischen Perspektive stark interdisziplinär: Laufend muss zwischen den Techniker:innen, zwischen den Jurist:innen und zwischen der Polizeifachlichkeit vermittelt werden, wofür entsprechende Stellen benötigt werden, die zwischen diesen verschiedenen Fachkulturen hin- und herwandern können.[1799] Gleichzeitig macht eine solche Querschnittskompetenz wegen des Zugriffs auf unterschiedliche Bereiche eine hohe Verortung in der Organisationshierarchie notwendig.[1800]

1794 Siehe dazu auch *Heinrich,* Innere Sicherheit und neue Informations- und Kommunikationstechnologien, S. 276 ff.
1795 Interview 14, Pos. 14.
1796 Interview 6, Pos. 44; Interview 12, Pos. 45.
1797 Interview 6, Pos. 40.
1798 Interview 14, Pos. 102.
1799 Interview 6, Pos. 38.
1800 Interview 6, Pos. 18.

So gibt es etwa eine „INPOL-Fachlichkeit"-Kommission, in der sich Vertreter:innen der Länder- und Bundespolizeibehörden auf fachlicher Ebene zu Fragestellungen der informationstechnologischen Weiterentwicklung in den deutschen Polizeien verständigen.[1801] Ähnliche informationelle Vernetzungen – die als charakteristisches Merkmal moderner Polizeien beschrieben werden[1802] – gibt es auch zu „den zivilen Behörden" wie dem „Kraftfahrbundesamt, [der] Ausländerzentrale [und dem] Bundesverwaltungsamt" und auch zu der für das polizeiliche Informationshandeln besonders wichtigen Staatsanwaltschaft. Überall dort wird über Fragen, die sich aus gesetzlichen Neuregelungen oder Urteilen ergeben, beraten:

> „Dort bereitet man die fachliche Abstimmung vor, um dann die IT-mäßigen Änderungen machen zu können. Da gibt es ein unheimliches Netz an Informations- oder Abstimmungsverfahren und auch Netzwerken, die informell entstanden sind, in denen man sich permanent Erfahrung holt oder Wissen holt oder abstimmt, wie man es am besten macht."[1803]

Innerhalb der Länder wird die informationstechnologische Infrastruktur häufig von darauf spezialisierten Organisationeinheiten der Polizei, etwa in Form von Präsidien für Technik[1804] oder auch von den Landeskriminalämtern, zentral verantwortet.[1805] Dort sind dann beispielsweise die großen zentralen Datenbanken, auf denen praktisch die Mehrzahl der landesweiten Datenverarbeitungen stattfinden, auf entsprechenden Servern angesiedelt.[1806] Von einer Zentralisierung wird auch hinsichtlich der Entwicklung von neuen Programmen und Komponenten berichtet,[1807] wenngleich informationstechnologische Innovationen auch polyzentrisch im polizeilichen Austausch der deutschen Polizeien zu entstehen scheinen, wonach sie dann über die Führungsebenen in die Organisation eingebracht und einer zentralen Umsetzung zugeführt werden.[1808]

Auch das polizeiliche Informationswesen innerhalb der Länder ist durch Vernetzungen geprägt, die mitunter zu Unübersichtlichkeiten in den Verarbeitungsprozessen führen können:

1801 Interview 8, Pos. 67.
1802 *Sheptycki* Global Crime 18 (2017), 286.
1803 Interview 6, Pos. 42.
1804 Interview 8, Pos. 53.
1805 Interview 12, Pos. 26.
1806 Interview 10, Pos. 28.
1807 Interview 10, Pos. 28.
1808 Interview 9, Pos. 34.

> „Besonderheit ist vielleicht, dass das LKA im Land die Zentrale der Kriminalitätsbekämpfung ist, das heißt wir haben sehr viele Spezialanwendungen, die wir den Polizeipräsidien im Land zur Verfügung stellen, also als eine Art Auftragsverarbeiter agieren. Wir wissen oft nicht, welche Daten die schicken oder zu welchem Ermittlungsverfahren die gehören oder ob das jetzt Daten vom Beschuldigten, vom Zeugen oder Ähnliches sind."[1809]

Aufgabe aller informationstechnologischen Planer:innen bei den Polizeien ist es, die polizeilichen Datenströme konzeptuell zu steuern. Damit das Informationswesen möglichst reibungslos funktioniert, ist dafür nötig, die wie auch immer erhobenen und generierten Daten in die polizeilichen Informationssysteme zu schleusen und sie dann von dort aus verschiedentlich je nach Bedarf in „dahinterliegende Systeme", etwa in die staatsanwaltschaftliche elektronische Akte oder auch Predictive Policing-Anwendungen,[1810] weiter zu kanalisieren:

> „Die Quelle ist also der Polizist und Sie müssen sich einen Kopf machen, was er denn da an Sachverhalten aufnimmt, was da an Informationen entstehen. Wo diese Informationen alle gebraucht werden. Wie müssen die angepasst werden? Gegebenenfalls manipuliert werden, also manipuliert im positiven Sinne, also verändert werden, damit sie qualitätsgerecht bei dem jeweiligen Adressaten auch ankommen. Das macht die Sache so unheimlich komplex."[1811]

Dabei sollten die informationstechnologischen Entwicklungsprojekte immer in die organisatorischen Abstimmungsprozesse eingebunden bleiben, damit sich die informationstechnischen Abteilungen nicht zu sehr verselbstständigen und dann bei ihren technischen Ausführungen rechtliche Vorgaben nicht oder nicht ausreichend beachten.[1812] So wirkt die informationstechnologische Infrastruktur im Idealfall entlastend und fügt sich in die polizeilichen Arbeitsabläufe ein[1813]:

1809 Interview 9, Pos. 10.
1810 *Egbert/Leese,* Criminal futures, S. 70.
1811 Interview 6, Pos. 30.
1812 Interview 11, Pos. 32.
1813 Interview 6, Pos. 34; vgl. etwa auch *Ackroyd/Harper/Hughes* ua, New technology and practical police work, S. 26: "Devising information systems that can serve as instruments of police work requires some conception about the nature of that work, how it is organized day-to-day, what tacit understandigs are built into this

> „Das, was wir hier zu tun haben, als unser Sachgebiet, dass wir die Fachlichkeit in die IT einbringen, dass er mit seinem Fachwissen sich dort wiederfindet und das auch versteht, die Abläufe, die auf der Oberfläche sind. Wenn er eben eine Strafanzeige macht, dann muss er eben die Begriffe wiederfinden: „Verletzte Rechtsnorm", „Tatort", „Tatzeit" und solche Begriffe. Die bringen wir dann schon fachlich auf die Präsentationsebene, sodass er damit arbeiten kann. Wenn er diese Schritte abarbeitet, sollte er im Wesentlichen auch alles drin haben. Da entlasten wir ihn auch. Auch in der Prüfung auf Plausibilitäten, Vollständigkeit und Weitergabe der Daten."[1814]

Informationstechnologische Planung erfordert also auch die konzeptuelle Umsetzung der Nutzung, etwa in Form der Konzeption und Umsetzung von Interaktionsformen der Nutzer:innen mit dem System oder von Zugriffsberechtigungen und Kontrollen.[1815]

Angesprochen auf den Zustand des polizeilichen Informationswesens wird der föderalen Polizeistruktur nach wie vor eine hemmende Wirkung auf die Vereinheitlichung der zugrundeliegenden technischen Infrastruktur zugeschrieben, weil die in Teilen abweichenden innenpolitischen Interessen zu anderen Prioritäten und unterschiedlichen Ausprägungen in den Informationssystemen führen.[1816] Vom Zentralismus der 1970er Jahre ist man insofern – auch durch den Datenschutzdiskurs – zu „Insellösungen" gekommen, um dann wiederum in den 1990ern zentrale(re) Datenbanken mit zentrale(re)n Anwendungen zu konstruieren, woraus die heutigen Vorgangsbearbeitungssysteme der Länder und des Bundes entstanden sind.[1817] Allerdings bleiben das polizeiliche Informationswesen und seine Datenbanken fragmentiert. So wird etwa im Bereich der in Kriminalakten gespeicherten Daten nach wie vor nur das beschriebene Kriminalaktennachweissystem im INPOL-System geführt, sodass dort zwar der zu Beschuldigten angelegte Nachweis in einem übergreifenden Index recherchierbar ist, dann aber bei der aktenbesitzenden Kriminalpolizeidienststelle weitere Daten angefragt werden müssen.[1818] Eine nur begrenzte Integration von Datenbe-

---

organization, its situatedness within a network of other organizational arrangements, and so on.".

1814 Interview 6, Pos. 38.
1815 Interview 6, Pos. 18.
1816 Interview 6, Pos. 62.
1817 Interview 6, Pos. 24; siehe dazu auch bereits oben S. 119 ff.
1818 Interview 13, Pos. 94; siehe dazu auch bereits oben S. 240 ff.

ständen zeigt sich auch bei Löschungen aus manchen INPOL-Land-Systemen. Sollen hier Löschungen vorgenommen werden, so muss eine entsprechende Meldung der Dienststelle an die zentrale datenverwaltende Stelle im Land, etwa das Landeskriminalamt, gehen, das dann bestimmte Vorgänge löschen kann.[1819] Ferner sind die Systeme untereinander getrennt. So sind beispielsweise Vorgangsbearbeitungssysteme mitunter nicht mit INPOL verknüpft, womit Speicherungen und Löschungen in einem System ohne Auswirkung auf die Bestände des anderen Systems bleiben. Übertragungen, etwa von Daten zu strafprozessualen Zwecken durch die KAN-Stellen nach INPOL oder Löschungen in INPOL zu Zwecken der Gefahrenabwehr, können dann nur einzelfallbezogen vorgenommen werden.[1820] Inhaltlich findet allerdings insgesamt scheinbar keine große Trennung von strafprozessual und polizeirechtlich erhobenen Daten statt, da die meisten Systeme als Mischdateien im Sinne des § 483 Abs. 3 StPO zu klassifizieren sind.[1821] Es gibt in den Systemen jedoch immer stärkere Automatisierungsbemühungen: So werden Löschungen in Vorgangbearbeitungssystemen zunehmend automatisiert, etwa im Verhältnis zur Staatsanwaltschaft, die über eine Schnittstelle eine elektronische Erledigungsmitteilung (eMAV: elektronische Mitteilung über den Ausgang des Verfahrens) schicken kann, womit der Vorgang im Vorgangsbearbeitungssystem geschlossen und automatisch gelöscht wird.[1822]

Eine mangelnde Integration von Datenbeständen scheint es aber nicht nur im Land-Land- oder Land-Bund-Verhältnis zu geben, sondern auch innerhalb der jeweiligen Länder, wo Datenschutzbeauftragte berichten, dass Dienststellen ihre eigenen Datenbestände vorhalten und verwalten, die im Fall von Auskunftsersuchen beispielsweise individuell abgefragt werden müssen.[1823] Dieses sehr breite Tableau an polizeilichen Datenbeständen und daran anknüpfenden Datenverarbeitungsprozessen hat zu einem auch gegenwärtig noch beklagten „Wildwuchs an Schnittstellen" geführt."[1824] Zwar gibt es innerhalb der föderalen Struktur zur Adressierung dieser Problematik etwa länderübergreifende IT-Kooperationen, beispielsweise das IPCC (INPOL-Land-POLAS-Competence-Center) in Hamburg, das

1819 Interview 13, Pos. 51.
1820 Interview 13, Pos. 49.
1821 Interview 14, Pos. 34 ff.
1822 Interview 13, Pos. 47.
1823 Interview 13, Pos. 10.
1824 Interview 14, Pos. 68.

für mehrere Länder zentral die informationstechnologischen Prozesse verwaltet. Die dortigen Koordinierungs- und Anpassungsprozesse sind jedoch langwierig, da sich dort die Komplexitäten, die man bereits landesintern hat, noch einmal potenzieren.[1825]

Insgesamt hat man es in der polizeilichen Datenverarbeitung überwiegend mit sogenannten Legacy-Systemen[1826] zu tun, die, weil sie historisch gewachsen sind, nur mit großen Aufwänden gepflegt und weiterentwickelt werden können und sich in diesem Punkt stark von moderneren Datenbanklösungen unterscheiden:[1827]

> „[W]ir [haben] auch viele alte Systeme […], die sich nicht einfach so umstellen lassen in technischer Hinsicht. Es sind also nicht immer moderne Datenbanken drunter gelegt, wo man mal schnell ein paar Haken setzen kann, und dann ist gut."[1828]

Diese Trägheit der Systeme überträgt sich auch auf die Schwierigkeit der Änderung von Arbeitskultur und Workflows in den polizeilichen Informationspraktiken, etwa wenn Vorgangsverwaltung und -bearbeitung stärker getrennt werden sollen, aber im Rahmen der technischen Infrastruktur immer stark miteinander verbunden waren.[1829]

Trotz aller Problemlagen wird allerdings berichtet, dass man „Kernprozesse in der polizeilichen Arbeit und im Informationsaustausch hingekriegt [habe], sodass sie einigermaßen stabil laufen und auch tatsächlich eine Unterstützung für die Polizei darstell[en]",[1830] was aufgrund des basistechnologischen Charakters von Informationsverarbeitung[1831] („Jeder, der in der Polizei arbeitet, hat heute mit IT zu tun."[1832]) für die Polizei essenziell ist. Mit Blick auf die gegenwärtigen medialen Umbruchsdynamiken der

1825 Interview 14, Pos. 22, 24.
1826 Legacy-Systeme sind historische gewachsene informationstechnologische Systeme, auch Altsysteme genannt, die jeweils zu unterschiedlichen Zeiten eingeführt wurden, von verschiedenen Personen in unterschiedlichen Organisationseinheiten genutzt werden und oft nicht miteinander kompatibel sind und somit nicht von einem System zum anderen kommunizieren können.
1827 Interview 14, Pos. 22.
1828 Interview 14, Pos. 20.
1829 Interview 15, Pos. 34, 36.
1830 Interview 6, Pos. 20.
1831 So auch schon *Manning* Crime and Justice 15 (1992), 349 (352); *Reiss* Crime and Justice 15 (1992), 51 (82).
1832 Interview 6, Pos. 20.

Digitalisierung ist dieser gegenwärtig stabile Zustand aber wohl ständig in Gefahr, wieder instabiler zu werden.

Vor diesem Hintergrund soll aus der Not des polizeilichen Informationssystems nun eine Tugend gemacht werden, indem die föderale Struktur arbeitsteilig zur Innovation polizeilicher Informationstechnologien genutzt werden soll, wie es als Strukturmerkmal des Projekts Polizei 2020[1833] angedacht ist: Nach stärkerer Integration der polizeilichen Datenbestände zu einem gemeinsamen „Datenhaus" sollen in diesem Rahmen technologische Verfahren nach der Konzeption von Polizei 2020 in einem Land entworfen und dann in das ganze Bundesgebiet ausgerollt werden (können).[1834]

Die Fragmentierung des polizeilichen Informationssystems wird neben infrastrukturellen Überarbeitungen im Rahmen von Polizei 2020 seit Kurzem auch durch die Einführung der automatisierten Datenanalyse in einigen Ländern[1835] adressiert. Diese stellt über eine virtuelle Ebene datenbankübergreifenden Zugriff auf die Datenbestände, die bei den jeweiligen Länderpolizeien verfügbar sind,[1836] her und soll so die Abschottung der Datenbestände überwinden, um eine reibungslosere Suche in den Daten mit anschließender analytischer Nutzung zu ermöglichen.[1837]

Im Kontext der Organisation polizeilicher Informationsverarbeitung ebenfalls beachtenswert ist der Umstand, dass die Polizei für den Ausbau und die Pflege ihres Informationswesens viel technisches Personal braucht, also Informatiker:innen, Ingenieur:innen und Projektant:innen und um diese Leute mit Privatunternehmen konkurriert, sodass die Überlegung im Raum steht, die Fachkompetenz in der informationstechnologischen Entwicklung ganz aufzugeben und an Private auszulagern,[1838] was wiederum

1833 Siehe dazu oben S. 271 ff. sowie unten S. 465 ff.

1834 Interview 9, Pos. 50.

1835 Siehe dazu und zur rechtlichen Einordnung bereits oben S. 281 ff.

1836 Interview 14, Pos. 52.

1837 So auch ein Befragter in der Studie von *Egbert/Leese,* Criminal futures, S. 218; ebenso bei *Brayne,* Predict and surveil, S. 32: "The Palantir platform helps overcome this fragmentation by integrating previously disparate data sources into a single search. A query takes mere seconds. As the captain explained, before Palantir, his data were "a mile wide but only an inch deep." Now, in Palantir's terminology, he can "drill down" much deeper on any one individual, address, car, or entity by accessing more data points collected from more disparate sources, all searchable in relation to one another. Seeing the data all together is its own kind of data.".

1838 Interview 6, Pos. 46; siehe dazu näher unten S. 476 ff.

eine gute Strukturierung des Vergabeprozesses erfordert.[1839] Schon jetzt gibt es auch externe Private, die in der polizeilichen Informationsverarbeitung arbeiten. Sie müssen eine Sicherheitsprüfung durchlaufen und bei ihrer Arbeit von hausinternen Techniker:innen beaufsichtigt werden.[1840]

Gleichzeitig zeichnet sich eine Änderung der Struktur des polizeilichen Informationswesens als abgeschotteter Datenspeicher der polizeilichen Daten auch insofern ab, als durch Schnittstellen zu akkumulierten Datenbeständen privater Unternehmen eine Integration von polizei-externen Informationsquellen erfolgen soll. Dies wird etwa im Rahmen der Anwendungen der automatisierten Datenanalyse beschrieben, wo Schnittstellen zu sozialen Medien wie Facebook angelegt sind, die Daten, die sonst für Marketing oder Werbezwecke gedacht sind, einzelfallbezogen abgreifen und in die Analyse miteinbeziehen können sollen.[1841]

VIII. Verhältnis der Polizei zur Informationstechnik

Die operativ arbeitenden Teile der polizeilichen Fachlichkeit stehen - wie auch schon mit dem Feld des Datenschutzes – in einem ständigen gegenseitigen Beeinflussungsverhältnis mit der für ihre Tätigkeit so zentralen Informationstechnik und denen, die sie verwalten.

Dabei nehmen die Polizeien (und auch Staatsanwaltschaften[1842]) die hauseigenen Verantwortlichen für die informationstechnologische Infrastruktur stark als Dienstleister wahr.[1843] Nicht selten scheinen insofern aber die Leistungsfähigkeit derjenigen, die die Systeme konstruieren, und der Systeme selbst überschätzt oder die rechtlichen Möglichkeitsspielräume verkannt zu werden.[1844] Dass sich diese hohen Erwartungshaltungen gegenüber Informationstechnik abschwächen werden, scheint eher unwahrscheinlich, sind sie doch nachvollziehbarerweise geprägt durch die digitalen Umgebungen im „Privaten", wo beispielsweise Suchmaschinen, mit denen auf Datenbanken zugegriffen und Wissen geordnet extrahiert werden kann, den Umgang mit Informationen prägen. Ganz besonders wird dies bei der heranwachsenden Polizist:innen-Generation beobachtet:

1839 Interview 14, Pos. 8.
1840 Interview 3, Po. 38
1841 Interview 14, Pos. 74; siehe zu diesem Trend auch *Brayne,* Predict and surveil, S. 24.
1842 Interview 6, Pos. 68.
1843 Interview 6, Pos. 20; so auch bei *Brayne,* Predict and surveil, S. 93.
1844 Interview 6, Pos. 20, 26; Interview 14, Pos. 12.

> „Die jetzige Generation, die heranwächst, die Handy-Generation, die permanent in der Lage sind, auf Informationssysteme zuzugreifen, egal welcher Art und zumindest im privaten Bereich, kann sich das gar nicht vorstellen, dass man das früher alles nur mit Karteikarten und Papier und Lochkarten gemacht hat und sowas und Stöpseln – und man hat trotzdem Erfolge gehabt. Das fällt denen ein stückweit schwer und da sind auch die Erwartungshaltungen da, dass die Polizei so etwas Modernes in jedem Fall zur Verfügung hat, ohne zu wissen, was das kostet in der Entwicklung, im Betrieb und ob das alles auch gesetzlich zulässig ist. Das verstehen viele nicht. Und dann kommen natürlich auch die Philosophien hinzu. Bei Google gebe ich ein Stichwort ein, ich finde etwas und das war es dann. Das funktioniert in der Polizei natürlich nicht ganz so. Da muss man immer gegensteuern und immer erklären, dass wir die IT im für die Aufgabenerfüllung erforderlichen Umfang machen und nicht, damit es elegant und schön aussieht. Wenn man beides miteinander vereinigen kann, ist das ok. Ist aber selten der Fall."[1845]

Zusätzlich fungiert die Informationstechnik in ihrer Gesamtheit auch als Projektionsfläche für akute Problemlagen in den verschiedenen polizeilichen Tätigkeitsbereichen, für die sich eine technologische Lösung erhofft wird oder bei denen technische Fehler als Ursache vermutet werden, wobei die Technik nicht immer eine Lösung bereithält und selten tatsächlich der Grund für die Problemlage ist.[1846]

Wie bereits mehrere Male dargelegt, ist allerdings die aus Informationstechnologie und polizeilicher Fachlichkeit (und dem Datenschutz) insgesamt zusammengesetzte polizeiliche Datenverarbeitung nicht durch einseitige Verhältnisse geprägt. Die polizeilichen Fachabteilungen wirken dementsprechend nicht schlicht mit ihren Erwartungen auf die technische Ausgestaltung des polizeilichen Informationswesens ein. Vielmehr wird das informationelle Handeln von Polizist:innen sehr stark durch die jeweiligen, in einer Behörde geschaffenen informationstechnologischen Konfigurationen angeleitet und damit zugleich auch strukturiert. So wird etwa durch das Design der Technik bis zu einem gewissen Grad bestimmt, was aufzunehmen ist und wie es aufgenommen werden muss, womit sich die Qualität polizeilicher Arbeit auch an den Interaktionsfähigkeiten mit der Technik

1845 Interview 6, Pos. 24.
1846 Interview 6, Pos. 22.

bemisst und die Technik die polizeiliche Tätigkeit in einem gewissen Umfang Zwängen unterwirft.[1847]

Andererseits hängt auch die Qualität der polizeilichen Datenbestände zu einem nicht unerheblichen Teil von dieser Fähigkeit ab, denn die Polizist:innen sind neben ihrer Rolle als Nutzer:innen auch für die Erfassung von Informationen verantwortlich und müssen als solche auch prinzipiell in der Lage sein, adäquate Informationen zu liefern.[1848] Dabei kann die Informationstechnik das originär polizeiliche Handwerk nicht ersetzen, das trotz aller technischen Innovationen beherrscht werden muss, egal ob in der Kriminal- oder Schutzpolizei.[1849] Allerdings haben etwa *Chan et al.* gezeigt, dass polizeiliche Arbeitsweisen sich nur begrenzt intentional durch technologische Innovationen beeinflussen lassen.[1850]

IX. Polizeiliche Informationspraktiken

Auf Grundlage der zuvor beschriebenen Dimensionen polizeilicher Informationsverarbeitung soll nun – soweit dies auf Grundlage der Interviews möglich ist – ein Blick auf die tatsächlichen Informationspraktiken geworfen werden. Dabei ist zunächst wichtig, dass es nicht *die* Informationspraxis der Polizei gibt. Vielmehr gibt es verschiedene polizeiliche Aufgabenprofile, die im Arbeitsalltag zu unterschiedlichen Situationen führen, in denen wiederum unterschiedliches Informationshandeln erforderlich ist. Etwa muss im Streifenwagen, wo sich dynamische Situationen ergeben, ein schematisches Programm an (informationellen) Handlungen abgespult werden. Geht es vielleicht an kriminalpolizeilichen Tatorten dagegen etwas statischer zu, ist auch dort im Endeffekt ein routinisiertes Programm an Informationsmaßnahmen durchzuführen, das aber regelmäßig andere Schwerpunkte hat.[1851] Kurzum: es gibt eine Mannigfaltigkeit polizeilicher Dateien und Datenverarbeitungspraktiken, die aber auch gemeinsame Fixpunkte im polizeilichen Informationswesen haben:

1847 Interview 6, Pos. 34, 36, 72.
1848 Interview 6, Pos. 30.
1849 Interview 6, Pos. 28; Interview 9, Pos. 40.
1850 *Chan/Brereton/Legosz* ua, E-policing: The Impact of Information Technology on Police Practices.
1851 Interview 6, Pos. 30.

> „Wenn man die Praxis anschaut, jeder Beamte, das fängt beim Streifendienst an und geht dann über alle Bereiche bis in die Kriminalpolizei, die alle verarbeiten ja Daten. Die alle haben ihr INPOL-Land, ihr INPOL-Zentralsystem." [1852]

Je nach Aufgaben haben aber auch alle „ihre spezialisierten Dateien".[1853] Der Zugriff hierauf wird gesteuert, indem jede:r Polizist:in eine Kennung hat, mit der je nach Berechtigung auf die unterschiedlichen in einer Polizei zur Verfügung stehenden Systeme zugegriffen werden kann.[1854] Die Berechtigungen richten sich wiederum nach der Verwendung in der Behörde:

> „[N]icht jeder Polizeibeamte darf ja alle Daten sehen, es gibt bestimmte Phänomenbereiche und wenn ich in Phänomenbereich A arbeite, darf ich den Phänomenbereich B eigentlich nicht sehen. Und es gibt dann natürlich Personen, die in deliktsübergreifenden Einheiten arbeiten, die müssen sogar mehrere Bereiche sehen und aus dem Grund gibt es das Rollen- und Berechtigungskonzept, das ist da ganz, ganz wichtig, das wird dann natürlich da aufgenommen. Da muss man sich schon gut mit der Anwendung auskennen, d.h. man muss tief reinschauen: Wer darf was? Also dieses Rollen- und Berechtigungskonzept: Wer darf welche Daten sehen? Das gewinnt zunehmend an Bedeutung in dem Bereich."[1855]

Das Rollen- und Berechtigungskonzept ist hierarchisch strukturiert und dünnt sich nach oben aus:

> „Wir haben ja bestimmte Anwendungen, auf die kann grundsätzlich mal jeder zugreifen und auch die fachspezifischeren Anwendungen… also wir haben die üblichen Auskunftssysteme, da hat nahezu jeder Zugang, der das operativ braucht. Und speziellere Anwendungen, wir haben zum Beispiel die Anwendung Lagebild, die auf unser Vorgangsverwaltungssystem ComVor aufsetzt, da arbeiten wir sehr stark mit einem Berechtigungskonzept, das nach oben hin natürlich immer dünner wird. Wo es dann um sehr breite Daten geht, zum Beispiel die oberste Stufe hat relativ lang Zugang zu bestimmten Opferdaten, während die unterste Stufe dann

1852 Interview 1, Pos. 157.
1853 Interview 1, Pos. 157.
1854 Interview 4, Pos. 47.
1855 Interview 4, Pos. 45.

eher die Grundsätzlichkeit, also die Delikte in einem bestimmten Bezirk mitgeteilt bekommt"[1856]

Diese Hierarchisierung zeigt sich etwa auch im Rahmen der Nutzung von invasiven informationellen Maßnahmen wie der automatisierten Datenanalyse, die bisher nur sehr eingeschränkten Nutzer:innenkreisen offensteht.[1857] Auch die polizeiinternen Reflexionsniveaus über das eigene informationelle Handeln staffeln sich je nach Verwendung: So haben Streifenbeamt:innen normalerweise in ihrem Arbeitsalltag nachvollziehbarerweise wenig Raum und Gelegenheit sich über die Implikationen ihres Informationshandelns Gedanken zu machen.[1858] Wie bereits angeklungen kann durch entsprechende Systeme, die die Zugangsdaten erfassen, nachvollzogen werden, „wer sich wann wo eingebucht hat".[1859] Interessant ist, dass es trotz dieser bekannten Protokollierungspflichten und Kontrollen dennoch immer mal wieder zu Unregelmäßigkeiten und Datenschutzverstößen[1860] kommt. Um dies zu verhindern, müsse polizeilichen „Anwendern [...] ein klarer und einheitlicher rechtlicher Rahmen für Datenspeicherung und Löschung et cetera aufgezeigt werden."[1861]

Die Informationspraktiken sind mitunter recht deutlich durch die Technik vorgeformt,[1862] wenn etwa an einem Tatort bestimmte Informationsfelder ausgefüllt oder Checklisten abgearbeitet werden müssen,[1863] wobei dabei auch immer Spielraum für eigene Interpretationen und Entfaltung polizeilicher Fertigkeiten besteht.[1864] Grundsätzlich soll (gegenwärtig) ein Grundverständnis bei den polizeilichen Sachbearbeiter:innen für die technischen Anforderungen der polizeilichen Datenverarbeitung ausreichen.

1856 Interview 9, Pos. 56.
1857 Interview 14, Pos. 44.
1858 Interview 12, Pos. 20.
1859 Interview 8, Pos. 43.
1860 Interview 8, Pos. 43; Interview 12, Pos. 12
1861 Interview 13, Pos. 72.
1862 Code im Sinne einer programmatischen Informationsinfrastruktur ist insofern auch Recht („Law) im Sinne einer normativ wirkenden Struktur im Bereich polizeilicher Informationssysteme; siehe dazu grundlegend, wenn auch in anderem Kontext *Lessig,* Code, wobei sich neue informationstechnologische Instrumente natürlich regelmäßig an den vormaligen Informationspraktiken orientieren, vgl. dazu bereits die historischen Ausführungen zuvor S. 101 ff.
1863 Interview 6, Pos. 36; Interview 3, Pos. 52.
1864 Interview 6, Pos. 36; siehe dazu auch *Egbert/Leese,* Criminal futures, S. 79 f., die von Problemen bei der Standardisierung von Datenerhebungsprozessen bei der Polizei im Kontext von Predictive Policing berichten.

Als mindestens ebenso wichtig wird die Beherrschung originär polizeilicher Fertigkeiten, etwa im Bereich kriminalpolizeilicher Ermittlungen, angesehen[1865]: „Das ist der Anspruch der Systeme: Wer Ahnung hat, Fachwissen hat, der sollte mit den Systemen weitgehend klarkommen."[1866]

Es gibt allerdings einige informationspraktische Divergenzen was die technologischen Niveaus angeht[1867]: So wird etwa in der intra-behördlichen Kommunikation bei erhöhten Datenschutz-Niveaus noch von Brief-Kommunikation,[1868] von Anrufen und händischem Heraussuchen von Daten anstatt automatisierten Abrufen[1869] und von (noch bestehenden) aufwändigen Verwaltungssystemen für Papierakten berichtet,[1870] was wohl vor allem auch für Kriminalakten gilt.[1871] In absehbarer Zeit sollen Akten aber ausschließlich elektronisch geführt werden.[1872] Deutlicher werden die Diskrepanzen aber in den Hoch-Technologie-Bereichen wie den Spielarten der automatisierten Datenanalyse oder von (raumbezogenem) Predictive Policing, die in manchen Bundesländern noch nicht einmal geplant sind, während es sie anderswo schon gibt.[1873] Insgesamt gibt es aber bereits schon jetzt eine hohe Durchdringung der unterschiedlichen polizeilichen Arbeitsalltage mit informationstechnologischen Systemen und darauf bezogener Tätigkeit:

> „Man merkt, wenn so ein System mal ausfällt, was da eigentlich passiert und wie weit die Kollegen schon an diese Arbeit gewöhnt sind. Ich sage immer, ich habe noch gelernt mit einem Kugelschreiber zu schreiben, das fällt den heutigen Kollegen schon bisschen schwerer."[1874]

Vor allem im Zuge der Digitalisierung nimmt die Dichte an informationstechnologischen Instrumenten bei der Polizei weiter zu. Während dies zu einer Effizienzsteigerung auf verschiedenen Ebenen führt, bedeutet es gleichzeitig aber auch eine hohe informationelle Vernetztheit der Polizei-

1865 Interview 6, Pos. 28.
1866 Interview 6, Pos. 34.
1867 Siehe dazu für die deutschen Polizeien auch *Egbert/Leese,* Criminal futures, S. 76.
1868 Interview 3, Pos. 78.
1869 Interview 4, Pos. 65.
1870 Interview 10, Pos. 78.
1871 Interview 13, Pos. 93.
1872 Interview 10, Pos. 70.
1873 Interview 12. Pos. 49; *Egbert/Leese,* Criminal futures, S. 169, berichten in diesem Zusammenhang von "ripple effects", d.h. einer nachahmenden Technologie-Adaption durch die anderen Landespolizeibehörden, um die Rückstände aufzuholen.
1874 Interview 6, Pos. 24.

einsätze, wodurch eine direkte Speicherung vieler lebensweltlicher Daten in den polizeilichen Datenbeständen ermöglicht wird, von denen die Daten dann in den polizeilichen Systemen nach Bedarf weitergeleitet werden können:

> „Wenn Sie jetzt einen einfach schutzpolizeilichen Einsatz haben mit einem Streifenwagen, die sind heutzutage ausgerüstet mit Handys, die dienstlich zur Verfügung gestellt werden, die haben Laptops mit im Einsatz. Insofern alles das, was die da irgendwo machen, müssen sie dokumentieren. Vollzugspolizeiliches Handeln ist nun mal dokumentationspflichtig, dabei entstehen Informationen. Wenn sie einen Verkehrsunfall haben, haben sie auf jeden Fall zwei Betroffene, einen Verursacher, den Geschädigten, dann haben sie die KFZ dazu, dann kriegen sie Daten dazu, ob der Alkohol getrunken hat oder nicht. Sie müssen den Unfall aufnehmen, sie müssen mit dokumentieren und solche Dinge stehen dann natürlich in der Vorgangsbearbeitung elektronisch zur Verfügung."[1875]
>
> „Der [Polizist, FB] arbeitet im Vorgangsbearbeitungssystem vor Ort. Der hat einen Laptop, wo er die Oberfläche des Vorgangsbearbeitungssystems hat, in die er mobil die Daten erfasst, die entstehen und gegebenenfalls Ausdrucke erzeugen kann, um dem Bürger bestimmte Dokumente mitzugeben und wir speichern. Diese Speicherung des Vorgangs, die er hat, ziehen wir auf die zentralen Datenbanken hoch und steuern diese Information an die notwendigen Stellen an, die sie dann brauchen. Das ist soweit mit der Informationsverarbeitung heute schon durchkonzipiert bis hin zur Fahndungsausschreibung und weiß der Teufel was."[1876]

Damit findet eine weitere Mobilisierung und in Teilen auch Dezentralisierung von polizeilicher Datenverarbeitung statt, was das polizeiliche Informationswesen dynamischer macht, indem jetzt Daten (nahezu) in Echtzeit[1877] gesammelt „von der Straße" in die Informationssysteme gelangen, die Informationen aus den Systemen aber auch jederzeit vor Ort zur Verfügung stehen:

> „Mit den neuen Handys kann auf Datenbanken der Polizei zurückgegriffen werden und Datenabfragen eigenständig vor Ort erfolgen. Die Polizei

1875 Interview 6, Pos. 30.
1876 Interview 6, Pos. 32.
1877 Zu diesem Ideal bereits *Bratton/Malinowski* Policing 2 (2008), 259 (264 f.).

> nutzt die Poliphones während des Dienstes auf Streife und geben die danach wieder ab. Alle unterwegs erfassten Daten werden in bestehende EDV-Systeme überspielt und anschließend auf dem Handy wieder gelöscht. Beispielsweise werden im Einsatz personenbezogene Daten, meist Personalien, erfasst und anschließend ins EDV-System der Polizei zur weiteren Verarbeitung übertragen."[1878]

Dasselbe gilt auch für strafprozessuale Datenverarbeitungsprozesse:

> „Und bei Straftaten haben sie das halt auch. Sie haben einen Tatort, der muss aufgenommen werden, da müssen die Beweise gesichert werden – fotografisch, da sind wir bei Digitalkameras, die sie haben. Sie haben den Tatort als solchen, da sind sie bei Georeferenzierungen, sie haben gegebenenfalls einen Beschuldigten – Personaldaten – sie haben einen Geschädigten, sie haben geklaute Gegenstände, die in das Fahndungssystem reinsollen. Also überall entstehen Daten bei der Bearbeitung, die an anderen Stellen logischerweise benötigt werden, was man früher über Papierwege gemacht hat, was jetzt elektronisch alles funktioniert. Diese Vielfältigkeit der Nachnutzung und Mehrfachnutzung ist ein Problem, das die Komplexität der Informationsverarbeitung ausmacht."[1879]

Diese anforderungsreiche Dynamik der Datengenerierung bzw. -erhebung kann Erkenntnissen aus der Studie von *Egbert und Leese* zufolge durchaus zu einem Qualitätsdefizit der Daten führen, die ins Vorgangsbearbeitungssystem gelangen, gegenüber denjenigen Daten, die dann später in Fallbearbeitungssysteme für kriminalpolizeiliche Zwecke übertragen werden.[1880]

Insgesamt wird das Arbeitsumfeld der Polizist:innen damit immer stärker mit Schnittstellen zu den Informationssystemen und den in ihnen vorgehaltenen digitalen Daten durchsetzt, was neben den möglichen polizeilichen Effektivitätssteigerungen auch aus rechtlicher Warte interessant ist, da so auch normative Vorgaben in Form von elektronischen Prozessen in den Workflows hinterlegt werden können, die den Sachberarbeiter:innen dann noch einmal etwa an Erforderlichkeit und Zweckbindung erinnern können,[1881] womit die Informationspraktiken der Beamt:innen graduell besser gesteuert werden könnten.

1878 Interview 10, Pos. 16.
1879 Interview 6, Pos. 30.
1880 *Egbert/Leese,* Criminal futures, S. 83.
1881 Interview 10, Pos. 70.

Allerdings sind die unterschiedlichen Informationspraktiken innerhalb der Polizei durch unterschiedliche informationelle Bedürfnisse geprägt, sodass es hier zusätzlicher Koordinierungsleistungen zur möglichst breiten und effektiven Nutzbarkeit von Daten innerhalb der Polizei bedarf:

> „Aber dazwischen sitzen immer wieder Kollegen, die gucken müssen: Sind die Informationen so, wie wir sie brauchen? Denn das, was der Polizist vor Ort macht, macht er unter seinen Gesichtspunkten und das ist das Schwierige: Der denkt dann eben nicht daran, dass irgendwo noch eine Datenbank steht, die die Informationen auch benötigt. Und die Jungs, die mit der Datenbank arbeiten, die sagen: Wieso hat er da nicht daran gedacht. Das ist das Problem Einmalerfassung/Mehrfachnutzung unter verschiedenen Zwecken. Da gibt es Konflikte, die letzten Endes in irgendwelchen Kompromissen enden, wo man versucht, zwischen dem, der da unten alles erfasst oder aus seiner Sicht im Rahmen einer Vorgangsbearbeitung bearbeitet, ohne dass er es merkt, dass die Information trotzdem die Qualität erreicht, die der andere an anderer Stelle benötigt."[1882]

Insofern agieren etwa Streifenbeamt:innen als datensammelnde Instanz für weitere Organisationseinheiten[1883] – letztere sind mit der anspruchsvollen Aufgabe der möglichst effektiven Umwandlung der Daten in handlungsleitendes Wissen betraut.[1884] Dazu sind allerdings auch die datenerhebenden Polizeibeamt:innen gefordert. Sie müssen die stets mehrdeutigen Realitäten und Phänomene, auf die sie bei ihrer Arbeit treffen, in die eher schematische Kategorien der Informationssysteme überführen, was zu im Zitat beschriebenen Meinungsverschiedenheiten über die Datenqualität führen kann.[1885] Erschwert wird dies zusätzlich durch die Vielfältigkeit der verschiedenen Arten der Weiterverwendung durch unterschiedlich spe-

1882 Interview 6, Pos. 32.

1883 Betont wird der Datenfluss von Polizist:innen "auf der Straße" hinein in die polizeilichen Informationssysteme auch in der Studie von *Brayne,* Predict and surveil, S. 64 f.

1884 *Egbert/Leese,* Criminal futures, S. 73, 75 f..

1885 Siehe zur polizeilichen Datengenerierung und ihren Problemen auch *Haggerty,* Making crime count, 64 ff; *Maltz*, Bridging Gaps in Police Crime Data, A Discussion Paper from the BJS Fellows Program, 1999; grundlegend dazu *Hand,* Dark data.

zialisierte Stellen in der Polizei.[1886] Beispielhaft werden sie etwa wie folgt beschrieben:

> „Also wir haben bei Verkehrsunfällen die Unfallstatistik, von der man möchte, dass die weitaus automatisiert die Daten aus solchen Unfallaufnahmen hat. Der Staatsanwalt wünscht eine elektronische Akte, das muss dokumentiert sein. Das muss an den weitergegeben werden. Die haben bestimmte Spuren, wo sie die kriminaltechnischen Institute haben, die das auch nicht abtippen wollen, die wollen diese Informationen auch haben. Die Quelle ist also der Polizist und Sie müssen sich einen Kopf machen, was er denn da an Sachverhalten aufnimmt, was da an Informationen entstehen."[1887]

Ohnehin besteht ein generelles polizeiliches Bedürfnis nach möglichst vielen Informationen:

> „Es ist natürlich so, dass es sinnvoll ist, und auch gerade aus so einer Ermittlerperspektive, möglichst viele Daten zur Verfügung zu haben. Das ist sinnvoll. Das wollen da bestimmt auch alle und das ist sicher hier auch eine Vorstellung, die die Politik möchte."[1888]
>
> „Es ist in der Tat manchmal so, dass Daten „gesammelt" werden, aber man gibt sehr ungern Wissen auf, das heißt, man löscht ungern Daten."[1889]

Zwar müssen Polizist:innen durch die zunehmende Digitalisierung von Datenbeständen und der damit verbundenen Automatisierung von Datenlöschungen auch stärker lernen, mit der Zeitlichkeit der Datenaggregationen, die für sie zur Verfügung stehen, zu arbeiten.[1890] Jedoch gibt es auch hier gewisse entgegenwirkende Beharrungskräfte. So gibt es noch immer die sogenannten „Mitziehautomatiken", die bei mehrfach bekannt gewordenen Straftaten, wie bei Wiederholungstätern üblich, dazu führt, dass neu verzeichnete Straftaten (oder Verdachte) – prinzipiell gleich welchen

1886 Siehe dazu auch *Egbert/Leese,* Criminal futures, S. 77, die einen Befragten (übersetzt) wie folgt zitieren: The patrol officer just doesn't want the same thing as the analyst. The officer wants to get rid of the case as quickly as possible, and the analyst wants good data. So we have to explain to the patrol officer why we need good data. And that's not easy.'.

1887 Interview 6, Pos. 30.

1888 Interview 1, Pos. 86.

1889 Interview 13, Pos. 72.

1890 Interview 10, Pos. 84.

Gewichts – zu einer Zurückstellung der Löschung aller auf diese Person bezogenen Daten führen.[1891] Damit soll verhindert werden, dass „Einzelfalllöschungen" zu einer „polizeilichen Erkenntnislücke" führen, wobei die Polizei dies begründen muss, aber dabei eben auch die Definitionsmacht bezüglich zu vermeidender Erkenntnislücken innehat.[1892] Darüber hinaus werden Daten teilweise auch über den eigentlichen Zeitraum des Bearbeitungszwecks vorgehalten, wobei scheinbar aber auch stellenweise nachgebessert wird:

> „Daten aus dem Vorgangsbearbeitungssystem „ComVor" werden in der Tat noch für einen weiteren Zeitraum vorgehalten. Bei Straftaten erfolgt die weitere Speicherung für maximal 24 Monate zur Abwicklung von noch offenen Geschäftsvorfällen (z.B. von zivil- oder verwaltungsrechtlichen Ansprüchen). Nach dieser Frist erfolgt auch hier die endgültige Löschung der Datensätze/des Vorgangs im ComVor. Die weitere Speicherung der Daten wurde auch von unserer Aufsichtsbehörde kritisiert. Aufgrund dessen haben sich die Kolleginnen und Kollegen das Verfahren vor Ort angesehen und erklären lassen. Inzwischen besteht jedoch die Möglichkeit, nicht mehr benötigte Datensätze vor Ablauf der Aussonderungsprüffrist zu löschen. Jedoch erfolgt diese Prozedur nicht automatisch und wird einzelfallbezogen manuell umgesetzt."[1893]

Damit ist erneut der bereits zuvor erwähnte, nicht klar geregelte Unterschied zwischen Vorgangsbearbeitung und Vorgangsverwaltung angesprochen.[1894] Dieser führt dann, wie im Zitat beschrieben, zur Verfügbarkeit von Daten, die zur Vorgangsbearbeitung nicht mehr zur Verfügung stehen sollten, aber trotzdem weiter einsehbar sind. Hierin drückt sich wiederum das bereits beschriebene Problem aus, dass die polizeilichen Informationspraktiken nur unzureichend im Recht abgebildet sind, weil sie den gesetzgebenden und -ausarbeitenden Organen auch nur unzureichend bekannt

1891 Siehe dazu etwa *Arzt* in *Möstl/Kugelmann* (Hrsg.), Beck'scher Online-Kommentar Polizei- und Ordnungsrecht Nordrhein-Westfalen, § 22 Rn. 53.

1892 Interview 13, Pos. 56.

1893 Interview 13, Pos. 54 f.

1894 Interview 14, Ps. 132, Interview 15, Pos. 34; siehe dazu bereits oben S.254 ff.; interessant ist auch, dass bspw. *Egbert/Leese,* Criminal futures, S. 83 in Beschreibung der polizeilichen Informationssystemtypen bei "process management databases" nicht weiter unterscheiden, sondern im Wesentlichen von einem Typus auszugehen scheinen, von dem dann nur Fallbearbeitungssysteme für kriminalpolizeiliche Zwecke zu unterscheiden sind. .

sind.[1895] Gleichzeitig haben die Polizist:innen nicht das Gefühl, „im luftleeren Raum" zu arbeiten, denn sie halten sich an die internen Vorschriften (PDV oder KPS-Richtlinie) zur Datenverarbeitung,[1896] die vermutlich in der Regel „historisch gewachsene Nutzungen" abbilden.[1897] Das macht polizeiliche Informationspraktiken bis zu einem gewissen Grad widerstandsfähig gegen Änderungen des Rechts. Eine Änderung dieses Zustandes wird für möglich gehalten, gleichzeitig aber auch als aufwändig und zeitintensiv beschrieben.[1898]

Historisch gewachsen ist auch die Vielfältigkeit der Dateien und Systeme – es gibt zentrale Systeme im Land und solche, die dezentral nur von einzelnen untergeordneten Polizeibehörden im Land verantwortet werden[1899] – die anscheinend zu etlichen redundanten Doppelverarbeitungen führt, was Arbeitsaufwände und Fehleranfälligkeit erhöht.[1900] So kann es beispielsweise sein, dass die einzelnen Dienststellen als Untereinheiten im Land nicht miteinander synchronisierte Daten zu ein und derselben Person führen,[1901] wobei auch darauf aufbauende Verfahren über die Dienststelle hinaus unbekannt sein können.[1902] Insofern lässt sich bei der Polizei gegenwärtig eher (noch) von einer fragmentierten Datenbankkultur und -praxis sprechen, die sich erst in letzterer Zeit wieder stärker zu integrieren versucht[1903]:

> „[W]ir [haben] ja verschiedene Datenspeicher. Jedes Land, weil Polizei ja Ländersache ist, hat eigene Speicher- und Auswerteprogramme entworfen. Das ist in der heutigen Zeit nicht sehr produktiv. Also wenn man schon Daten abfragen darf, dann müsste man das auch bundesweit machen können […]"[1904]
>
> „Ich sage mal, das ist die Vorgangsbearbeitung an sich in einer Leitstelle, wo Daten erfasst werden und Vorgänge generiert werden. Die Vorgangsbearbeitung in… ich sage mal, alles was man unter „elektronische Akte"

1895 Interview 14, Pos. 80.
1896 Interview 14, Pos. 32.
1897 Interview 15, Pos. 36.
1898 Interview 15, Pos. 34.
1899 Interview 14, Pos. 9.
1900 Interview 1, Pos. 86.
1901 Interview 3, Pos. 14; Interview 4, Pos. 9; Interview 5, Pos. 9.
1902 Interview 4, Pos. 9.
1903 Interview 6, Pos. 24; Interview 9, Pos. 40.
1904 Interview 10, Pos. 66.

verstehen kann – das muss funktionieren, miteinander funktionieren. Schön wäre es, wenn es länderübergreifend funktioniert."[1905]

Allerdings gibt es durchaus zentrale Auskunftssysteme, die zumindest weitere mögliche Speicherorte von Daten anzeigen können.[1906] Nichtsdestotrotz bleiben Asynchronitäten in den Datenspeicherungen bestehen:

„Das ist aber separat, INPOL ist separat, ComVor, das polizeiliche Informationssystem, ist separat. Aber das heißt eben, dass wenn ich im polizeilichen Informationssystem lösche, dann ist es noch im INPOL drin, das muss dann im INPOL auch separat gelöscht werden."[1907]

Trotz dieser Heterogenität in den Datenbeständen haben alle Polizeien in Deutschland ähnliche Funktionalitäten ausgebildet. Eine weitere Vereinheitlichung wird aber durch die unterschiedlichen Polizeigesetze erschwert,[1908] womit auch eine gleichmäßige Regulierung der polizeilichen Informationspraktiken wohl nicht erleichtert wird.

Abseits rechtlicher Fragen ändern sich auch die fachlichen Grundlagen für polizeiliches Informationshandeln. Bestimmte Phänomenbereiche erfordern eine zunehmende Kompetenz im Umgang mit digitalen Prozessen und Praktiken, was sich etwa am Beispiel der Kinderpornographie illustrieren lässt:

„Es ist im Moment noch ein bisschen wenig intelligent. Das heißt Sie können schon automatisiert Daten filtern, Sie können sich zum Beispiel alle JPEGs raussuchen oder auch wenn JPEGs umbenannt werden, dass das automatisiert über die Metadaten erkannt wird, dass das ein Bild ist. Das können Sie filtern lassen. Sie können sich auch den Hautfarbenanteil von so einem Bild anzeigen lassen, dass Sie nur Bilder mit einem Hautfarbenanteil nach oben bekommen. Sie haben natürlich auch Hashwerte von Bildern, die bekannt sind, die automatisiert rausgefiltert werden. Das heißt der Beschuldigte A hat zehn Bilder, die verdächtig sind, davon können Sie einen Hashwert bilden und aus keine Ahnung wie vielen Millionen Bildern können Sie genau die zehn Bilder auf Knopfdruck rausfiltern. Das geht."[1909]

1905 Interview 12, Pos. 59.
1906 Interview 8, Pos. 13.
1907 Interview 13, Pos. 49.
1908 Interview 8, Pos. 69.
1909 Interview 4, Pos. 71.

Neben diesen neuen Informationspraktiken muss gleichzeitig weiter traditionelle Ermittlungstätigkeit geleistet und gekonnt werden, wobei aber auch hier die Entwicklung hin zu technologisch innovativen Hilfsinstrumenten geht, deren Einsatz von kriminalpolizeilichem Fachwissen angeleitet werden muss:

> „Aber es geht ja um die – gerade in KiPo-Verfahren – die Sie noch nicht erkannt haben und die müssen Sie irgendwie detektieren und da hilft ihnen manchmal der Hautfarbenanteil auch nicht weiter, denn wenn es einfach nur darum geht, ob der Beschuldigte das Kind gekannt hat, dann kann der das ja auch auf einem Urlaubsbild gekannt haben. Dann ist das Kind, ist jetzt kein verdächtiges Bild im Bereich Kinderpornographie, aber es ist wichtig zu wissen, dass der dieses Kind gekannt hat, auf einer Urlaubsreise oder sonst irgendwas. Und um die Bilder… die können Sie halt noch nicht so richtig rausfiltern, da brauchen Sie eine Bildmustererkennung, da muss einfach das Gesicht oder die Person muss man detektieren und muss die mit einem Bildmuster mit anderen Bildern, wenn Sie anders schaut und nicht genau gleich ist, herausfinden. Und das läuft im Prinzip auf eine KI hinaus und diese KI ist nichts anderes als ein neuronales Netz, das Sie trainieren können und sowas muss man halt auch bauen."[1910]

Vor allem im „IuK[1911]-Forensik"-Bereich braucht es zunehmend „Tools", wie die hier beispielhaft angeführte Gesichts- oder Objekterkennung,[1912] die mit den Datenmengen umgehen können, sodass der Wandel polizeilicher Informationspraktiken immer stärker hin zu dem, was als Datafizierung beschrieben wurde, als (zumindest in Teilen) unausweichlich gesehen wird[1913]: „Also brauchen wir irgendwelche Daten-Mining-System, die dort eine automatisierte Verarbeitung zulassen, das heißt wir brauchen KI-Systeme."[1914]

Auch die polizeirechtliche Maßnahme der automatisierten Datenanalyse wird als erforderlich beschrieben: „Es ist definitiv erforderlich in der heuti-

1910 Interview 4, Pos. 71.
1911 Informations- und Kommunikationstechnik.
1912 Interview 14, Pos. 76.
1913 Interview 4, Pos. 69.
1914 Interview 4, Pos. 67

gen Zeit, d.h. wir arbeiten nicht mehr auf Papier, wir haben eine Masse an Datenquellen, die zusammengeführt werden müssen".[1915]

Das führt auch zu einem Wandel der Berufsanforderungen für Polizist:innen: „[D]er künftige Polizist wird sehr viel von IT verstehen müssen, wenn er denn erfolgreich sein will."[1916] Dabei spielen auch die Erwartungen, die man heutzutage an Informationstechnologie aus dem privaten Bereich mitbringt, eine Rolle.[1917] Darauf antwortet auch der Trend zur Plattformisierung der Polizeiarbeit, mit dem – quasi wie in einem Anwendungsstore auf mobilen Endgeräten – informationstechnologische Anwendungen zentral entwickelt und dann in größerem Stil distribuiert werden sollen,[1918] wobei es dezidiert auf nutzer:innenfreundliches Design der Anwendungen ankommt.[1919]

Gleichzeitig bedeutet die Zunahme der Datafizierung der Polizeiarbeit neben der Steigerung der technischen Anforderungen auch eine Erhöhung der datenschutzrechtlichen Anforderungen.[1920] Im Rahmen von bestimmten polizeilichen Informationspraktiken, bei denen es um eine möglichst schnelle und breite Erfassung und Auswertung von Informationen geht, etwa bei der Suche nach Personen mittels einer an einen Hubschrauber angebrachten (Infrarot)-Kamera, wird berichtet, dass sich datenschutzrechtliche Vorgaben, wie die Benachrichtigung von Betroffenen, nur noch eingeschränkt umsetzen lassen.[1921] Auch bei weniger umfassenden informationellen Maßnahmen spüren Polizist:innen den Datenschutz, etwa wenn bei Observationen erfasste Nichtverdächtige protokolliert werden müssen.[1922] Die laufenden Rechtsänderungen der letzten Jahre haben sich dementsprechend in einer ständig anzupassenden internen Vorschriftenlage hinsichtlich erlaubtem Informationshandeln ausgedrückt,[1923] was mit Blick auf die Volatilität des Rechtsbereichs[1924] vermutlich nicht abreißen wird. Da-

1915 Interview 14, Pos. 40.
1916 Interview 6, Pos. 28.
1917 Interview 6, Pos. 24.
1918 Interview 10, Pos. 64.
1919 *Bundesministerium des Innern*, Polizei 2020; *Münch* Kriminalistik 73 (2019), 11 (15).
1920 Interview 11, Pos. 48.
1921 Interview 3, Pos. 84.
1922 Interview 3, Pos. 52.
1923 Interview 12, Pos. 40.
1924 So sind gegen das geänderte BKAG wieder Verfassungsbeschwerden anhängig, https://freiheitsrechte.org/themen/freiheit-im-digitalen/bka-gesetz (Stand: 01.10.2023).

neben müssen auch stets angepasste Schutzmaßnahmen gegen Fehlidentifizierungen und -kategorisierungen in komplexen Datenanalysen, etwa wenn jemand in der beschriebenen Bildauswertung in Kinderpornographie-Verfahren aus nicht-delinquenten Gründen in den Bildern auftaucht, geschaffen und weiterentwickelt werden,[1925] um die – auch von Befragten gesehene – Gefahr eines Automation Bias, also das blinde Vertrauen in automatisierte Ergebnisse,[1926] abzuwenden.[1927]

Zusätzlich kommt es durch technologische Innovationen wie der Bodycam und durch die Gestattung ihres Einsatzes in Wohnungen zu einer bemerkenswerten Erweiterung des polizeilichen Maßnahmenspektrums um polizeiliche Informationspraktiken,[1928] die zunehmend multimediale Daten aus der Breite der polizeilichen Alltagspraxis erheben und für die weitere polizeiliche Informationsverarbeitung verfügbar machen können, wobei wiederum Sicherungsmaßnahmen, wie das zunächst abgegrenzte Speichern der Daten,[1929] ergriffen werden, bevor über ihre weitere Verarbeitung entschieden wird.

Multimediale Daten können zudem auch über sog. open source intelligence (OSINT)-Datenerhebungen in die Datenbestände der Polizei gelangen. Wie bereits angesprochen gibt es Systeme mit Schnittstellen zu Social-Media-Plattformen wie Facebook („Und dann gibt es in Teilen auch Facebook-Schnittstellen, die diese Daten absaugen können. Gegen geringes Entgelt natürlich."[1930]). Allerdings können auch schlicht über „Online-Streifen"[1931] Screenshots oder Bildschirmaufnahmen auf verschiedenen Seiten, etwa auf Twitter während Demonstrationen, gesammelt und (im Schnitt drei Jahre) gespeichert werden.[1932] Diese virtuellen Informationspraktiken stellen zudem grundsätzlich andere Formen des Informationsumgangs dar, als sie bisher bekannt waren, wobei die Implikationen sich gegenwärtig noch nicht abschätzen lassen.[1933]

1925 Interview 14, Pos. 76.
1926 Für eine umfassende und aktuelle Analyse, siehe *Strauß* BDCC 5 (2021), 18.
1927 Interview 15, Pos. 94.
1928 Interview 8, Pos. 51.
1929 Interview 10, Pos. 40.
1930 Interview 14, Pos. 72.
1931 Siehe dazu bereits oben S. 314 ff.
1932 Interview 14, Pos. 74.
1933 Siehe dazu bereits oben S. 71 ff.

X. Verwirklichungsgrade des Datenschutzes bei der Polizei

Nach den vorangegangenen Darstellungen der einzelnen Einflussfaktoren und Komponenten des polizeilichen Informationswesens und der darin stattfindenden Informationshandlungen soll nun der gegenwärtige Verwirklichungsgrad des polizeilichen Datenschutzes, wie er aus den Gesprächen offenbar geworden ist, dargestellt werden, womit auch die Normgemäßheit polizeilicher Informationspraktiken angesprochen ist.

Als normatives Konzept und einem Ziel unter mehreren in der Polizei hängt die Umsetzung des Datenschutzes zunächst wesentlich von innerorganisationaler Legitimation durch die Behördenleitung ab,[1934] wobei allerdings in keinem Interview von Problemen, sondern vielmehr von „große[m] Rückhalt" berichtet wurde.[1935]

Allerdings ist dies lediglich der Ausgangspunkt für die Verwirklichung des polizeilichen Datenschutzes und insgesamt gibt es durchaus Probleme bei der Umsetzung der rechtlichen Vorgaben. Bereits angesprochen wurden Probleme der Rechtslage, die eine Rechtsanwendung erschweren. So wird dann auch über fehlende Vorgaben für die Handhabung der JI-Richtlinie geklagt, wenn etwa besondere Formen der Datenverarbeitung wie besondere Kategorien von personenbezogenen Daten oder der Unterschied zwischen Daten, die auf Tatsachen beruhen, und Daten, die auf Einschätzungen beruhen, aufgrund der in diesen Punkten anscheinend mangelhaften deutschen Umsetzungsgesetze in der deutschen Polizeipraxis nicht in einem befriedigenden Maße berücksichtigt werden können.[1936] Diese unzureichende Umsetzung oder auch Aufweichung der Datenschutzstandards durch den deutschen Gesetzgeber[1937] und ebenso die fehlenden Konkretisierungen der JI-Richtlinie durch den Unionsgesetzgeber werden als hinderlich empfunden.[1938] Ähnliches gilt auch für den Umstand, dass durch die föderalistische Struktur Synergieeffekte zwischen den Ländern bei der Verwirklichung des Datenschutzes nur begrenzt genutzt werden können.[1939] So ist es dann auch nicht verwunderlich, dass teilweise noch keine vollständige Umsetzung in den Behörden stattgefunden hat,[1940] wenngleich

1934 Interview 1, Pos. 41-43; Interview 11, Pos. 24.
1935 Interview 9, Pos. 36.
1936 Interview 1, Pos. 70.
1937 Interview 1, Pos. 68.
1938 Interview 1, Pos. 64.
1939 Interview 3, Pos. 100.
1940 Interview 13, Pos. 28.

den Rechtsänderungen der jüngeren Vergangenheit eine Verbesserung des Datenschutzes durch Sensibilisierung der Polizist:innen zugeschrieben wird.[1941] Ein höherer Verwirklichungsgrad wird gegenwärtig auch durch beschriebene dogmatische Fehlstände, etwa die fehlende Kategorisierung der polizeilichen Informationssysteme, blockiert.[1942]

Die normative Struktur des Datenschutz wird grundsätzlich als kongruent zum den Polizist:innen zugeschriebenen Wesen gesehen, das auf Normbefolgung gepolt sei.[1943] Auch die gesetzlich vorgeschriebene und zunehmend technisch umgesetzte Vergesslichkeit des polizeilichen Informationsgedächtnisses scheint sich durchaus zu etablieren.[1944] Gleichzeitig bestehen immer noch auf die originäre Polizeiarbeit gerichtete Datensammelbestrebungen bei Polizist:innen.[1945] Inwieweit hier datenschutzrechtliche Grenzen ernst genommen und damit datenschutzrechtliche Normen befolgt werden, ist auch von der Eingebundenheit der Datenschutzbeauftragten und der ihnen entgegengebrachten Akzeptanz abhängig.[1946] Daneben wird auch der politischen Relevanz des Datenschutzes in einem Land oder im Bund eine Rolle zugemessen.[1947]

Als positiv werden die Auswirkungen der Zusammenarbeit mit den Aufsichtsbehörden auf die Verwirklichung des Datenschutzes beschrieben, insbesondere wenn ein enges Kooperationsverhältnis besteht.[1948] Eine frühzeitige Einbindung, wie etwa eine Prüfmöglichkeit der Landesdatenschutzbeauftragten bezüglich der Verwendung von invasiven Bodycam-Daten, kann dabei helfen, datenschutzrechtlichen Fehlentwicklungen vorzubeugen.[1949] Nicht überall wird aber von einem einfachen Verhältnis zwischen Aufsicht und Beaufsichtigten berichtet.[1950] Außerdem wurde in diesem Zusammenhang eine fehlende Ausstattung der Aufsichtsbehörden als Problem gesehen, die durch intensivere Tätigkeit verbindlichere Normen zur Verbes-

1941 Interview 15, Pos. 103.
1942 Interview 14, Pos. 76.
1943 Interview 1, Pos. 37; Interview 11, Pos. 24.
1944 Interview 10, Pos. 80.
1945 Interview 13, Pos. 72.
1946 Interview 3, Pos. 30.
1947 Interview 1, Pos. 37.
1948 Interview 9, Pos. 32; Interview 13, Pos. 58.
1949 Interview 10, Pos. 40.
1950 Interview 15, Pos. 32.

serung der datenschutzrechtlichen Orientierung für die Polizeien schaffen könnten, was noch immer als unzureichend wahrgenommen wird.[1951]

Unter Personalknappheit leidet aber – wie der Rest der Polizei – auch der polizeiliche Datenschutz.[1952] Die Personalausstattung verunmöglicht mitunter eine Erhöhung oder überhaupt erst eine Etablierung eigener Kontrollbemühungen,[1953] wie sie das Gesetz vorschreibt. Was die übrige, individuelle Ausstattung und Stellung vieler Datenschutzbeauftragten angeht, besteht aber ansonsten Zufriedenheit mit Blick auf die Aufgabenerfüllung.[1954] Nichtdestotrotz führt vor allem eine mangelnde Personalausstattung dazu, dass zu erledigende Aufgaben stärker auflaufen, als sie sollten.[1955] Erschwert kann dies zusätzlich durch die Ausgestaltung der Position als Teilzeitstelle werden, wie nicht selten beschrieben.[1956]

Wie bereits zuvor beschrieben, kommt die Realität dem Idealbild der Datenschutzbeauftragten als beratende und überwachende Instanz nur selten nahe.[1957] Datenschutzbeauftragte können so in vielen Fällen die ihnen auferlegten Aufgaben nur im Rahmen der Beratung verwirklichen, etwa indem mahnend auf Missstände hingewiesen wird.[1958] Daraus ergibt sich im Wesentlichen das Bild eines reaktiven polizeilichen Datenschutzes, in dessen Rahmen in erster Linie diejenigen Probleme behandelt werden, die an die Beauftragten herangetragen werden[1959]:

> „Aber es ist praktisch eher so, dass wir die Probleme, die eben auf uns einstürzen, versuchen zu lösen, als dass wir uns selber auf den Weg machen. Da fehlt ehrlich gesagt einfach die Muße für."[1960]
>
> „Da gibt es viel Luft nach oben an Aufgaben, die man wahrnehmen kann, so würde ich das mal umschreiben."[1961]

1951 Interview 1, Pos. 120.
1952 Interview 2, Pos. 60; Interview 4, Pos. 38; Interview 14, Pos. 26.
1953 Interview 2, Pos. 55-56.
1954 Interview 3, Pos. 42; Interview 11, Pos. 39; Interview 12, Pos. 30.
1955 Interview 9, Pos. 64; Interview 12, Pos. 14.
1956 Interview 1, Pos. 28; Interview 5, Pos. 52; Interview 10, Pos. 36.
1957 Interview 1, Pos. 28; Interview 2, Pos. 88-92, berichtet von nur einem Bundesland, in dem die Position „wirklich völlig frei" sei.
1958 Interview 2, Pos. 52.
1959 Interview 2, Pos. 52; Interview 7, Pos. 28; Interview 15, Pos. 10.
1960 Interview 2, Pos. 48.
1961 Interview 12, Pos. 12.

Trotz aller Problemlagen werden teilweise auch eher positive Bilder der Datenschutzverwirklichung gezeichnet[1962]: Man sei auf einem sehr guten Weg und die Befugnisse der Polizei würden mit den Bedürfnissen der Bürger:innen in ein ausgewogenes Verhältnis gebracht.[1963] Auch der Informationsfluss zu und die Sensibilisierung von Polizist:innen bezüglich polizeilicher Datenschutzbelange wird dabei als gut beschrieben:[1964]

> „Früher schwamm das [der Datenschutz, FB] irgendwie mit. Jetzt ist der Fokus viel stärker drauf."[1965]
>
> „Der Datenschutz hat eine so große Präsenz erlangt auch im Hinblick auf die wachsenden Risiken der Digitalisierung, dass eine personelle Erweiterung in diesem Bereich unbedingt erforderlich ist."[1966]

Umgekehrt werden, vor allem mit Blick auf schon spürbare Zukunftstendenzen der polizeilichen Informationsverarbeitung, ein Auseinanderklaffen von normativem Anspruch und den faktischen Zwängen des Polizeialltags gesehen, bei denen komplexe datenschutzrechtliche Vorgaben nicht mehr befriedigend umgesetzt werden können,[1967] was als zunehmendes Problem in der automatisierten Datenverarbeitung gesehen wird:

> „Denn diese Unübersichtlichkeit der automatisierten Datenverarbeitung geht so weit, dass derjenige, der guten Gewissens das Recht anwendet, gar nicht mehr weiß, wo er ansetzen soll, weil es technisch unüberschaubar ist."[1968]

Um solchen Tendenzen entgegenzuwirken, bemühen sich Aufsichtsbehörden um eine sehr enge Prüfung von invasiven Maßnahmen wie etwa der automatisierten Datenanalyse.[1969]

Allerdings braucht es bereits in den Polizeibehörden entsprechend befähigte Personen als Datenschutzbeauftragte, damit die bereits zuvor beschriebenen erforderlichen Übersetzungsaufgaben angemessen durchge-

1962 Interview 7, Pos. 32.
1963 Interview 3, Pos. 106.
1964 Interview 3, Pos. 88; Interview 11, Pos. 48; Interview 11, Pos. 26.
1965 Interview 12, Pos. 12.
1966 Interview 13, Pos. 21.
1967 Interview 3, Pos. 84; beispielhaft hierfür ist der mit einer (Infrarot-)Kamera ausgestattete Polizeihubschrauber aus dem vorangegangenen Unterkapitel, der eine Vielzahl an Menschen erfasst.
1968 Interview 5, Pos. 52.
1969 Interview 13, Pos. 40.

führt werden können.[1970] Dazu gehört auch die Einstellung der behördlichen Datenschutzbeauftragten zum Datenschutz selbst, die vereinzelt nicht ganz unproblematisch zum Ausdruck kam, etwa wenn bezüglich der Rechte Betroffener geäußert wird, dass „ein normaler Bürger […] solche Anfragen auch gar nicht stellen [würde]".[1971] Nicht unproblematisch scheint auch die dem Einfluss der Datenschutzbeauftragten entzogene Trennung zwischen operativem Datenschutz, also beispielsweise Bürger:innen-Anfragen und Protokolldatenauswertungen, und dem strategischen Datenschutz,[1972] da so ein stückweit die Kenntnis über die Realität der Datenschutzverwirklichung in einer Behörde von der Steuerung der Datenschutzverwirklichung entkoppelt wird.

Schwerwiegend sind auch die Defizite der datenschutzrechtlichen Kontrollarchitektur, etwa was ihr Sanktionsregime, auch im Vergleich zum privaten Bereich, angeht.[1973] In diesem Kontext wird auch von der Unterbesetzung von Auskunftsstellen für Betroffene berichtet.[1974] Direkt damit verbunden sind die Aufwände, die teilweise dezentral vorgehaltenen Daten bei den einzelnen Dienststellen zu lokalisieren und abzufragen.[1975] Auch eine tragende Säule des datenschutzrechtlichen Kontrollregimes, die Protokolldatenüberprüfung, ist nicht überall befriedigend ausgestaltet. So wird etwa davon berichtet, dass nur einmal im Jahr eine halbstündige Abfragenüberprüfung pro Dienststelle erfolgt,[1976] was bei der Bedeutung der Informationssysteme und der Menge der Abfragen unzureichend erscheint. Effektiver scheint dagegen die Praxis, jede 50ste Abfrage landesweit für eine Überprüfung herauszuziehen.[1977] Insgesamt besteht durch die Protokollierung eine mächtige, wenn auch in Teilen Deutschlands ausbaufähige Möglichkeit, bei Verdachtsfällen retrospektiv Informationspraktiken auszuleuchten[1978] und polizeilichen Datenumgang umfassend zu überwachen. Dabei ist theoretisch über die technische Zugangslösung mit Nutzer:innen-Kennung und Passwort eine gute, weil individuelle, Zuordnung mög-

1970 Interview 9, Pos. 72.
1971 Interview 4, Pos. 49.
1972 Interview 9, Pos. 16.
1973 Interview 1, Pos. 39.
1974 Interview 2, Pos. 154-156.
1975 Siehe dazu bereits oben S. 400 f.
1976 Interview 2, Pos. 48.
1977 Interview 14, Pos. 48.
1978 Interview 8, Pos. 40-43.

lich,[1979] sofern auch das Benutzer- und Rechtekonzept, also ob die Zugriffsrechte zur jeweiligen Rolle in der Polizeiorganisation passen, zusätzlich kritisch überprüft wird.[1980] Wie bereits angeklungen sind dennoch aber unberechtigte Datenabfrage ein Phänomen, das immer wieder auftaucht.[1981] Vor diesem Hintergrund wird es von den Datenschutzbeauftragten auch für angemessen gehalten, dass die Polizei wohl am intensivsten datenschutzrechtlich in der deutschen Behördenlandschaft kontrolliert wird.[1982]

Bezeichnend für das Spannungsverhältnis bei der Verwirklichung des polizeilichen Datenschutzes bleibt insgesamt, dass davon berichtet wird, dass zwar zunehmend automatisiert gelöscht wird, wodurch es auch versehentlich mal zu Erkenntnislücken kommen kann, gleichzeitig aber mancherorts eine Art Sicherheitsnetz besteht, sodass auch gelöschte Daten nicht gleich unwiederbringlich verloren sind,[1983] womit auf die schon beschriebene Problematik rund um Vorgangsbearbeitungs- und -verwaltungssysteme angespielt wird. Hieran lässt sich im Wesentlichen ablesen, dass die Verwirklichungszeiträume des polizeilichen Datenschutzes aufgrund polizeilicher Arbeitskultur, träger technischer Strukturen und Komplexität der Rechtslage sehr lang sind,[1984] sodass es naheliegt, schon heute robuste Regelungsstrukturen für die bereits laufenden technologischen Wandlungsprozesse zu schaffen und so einem Steuerungsverlust über das polizeiliche Informationswesen vorzubeugen. Inwieweit das angesichts der sichtbaren Verselbstständigungstendenzen des polizeilichen Informationswesens gelingen kann, ist dabei indessen eine offene Frage.[1985]

XI. Technologische Wandlungsprozesse

Nachdem nun die Gegenwart der polizeilichen Informationsverarbeitung so rekonstruiert wurde, wie sie sich in den Interviews präsentiert hat, soll nun ausgehend von diesem gegenwärtigen Standpunkt der Blick nach vorne gerichtet werden auf das, was sich für die Zukunft bereits aus den schon

1979 Interview 10, Pos. 52.
1980 Interview 14, Pos. 44.
1981 Interview 12, Pos. 12.
1982 Interview 11, Pos. 70.
1983 Interview 10, Pos. 70.
1984 Interview 15, Pos. 34.
1985 *Heinrich,* Innere Sicherheit und neue Informations- und Kommunikationstechnologien, S. 381.

laufenden, in erster Linie technologischen Wandlungsprozessen ablesen lässt.

Generell unterliegen Wandlungsprozesse bei der Polizei – ganz im Sinne der beschriebenen Sozio-Technizität polizeilicher Informationstechnologie[1986] – häufig schwer vorherzusehenden Verläufen und vollziehen sich mitunter als reflexhafte Reaktionen[1987]:

> „Viele Dinge geschehen oft sehr schnell und geschehen im Anschluss an bestimmte Ereignisse und aus meiner Sicht kann man manchmal das Gefühl bekommen, dass manche Dinge nicht ganz zu Ende gedacht werden, sondern dass es dann vielmehr unter einem gewissen Handlungsdruck geschieht. Das ist erstmal riskant."[1988]

Dennoch sind technologische Wandlungsprozesse kein lediglich spontanes und vereinzeltes Phänomen im organisationalen Kontext der Polizei, sondern zentral und sehr präsent. Der digitale Wandel wird als unausweichlich und unaufhaltsam wahrgenommen, sodass die Polizei diese Entwicklung spiegeln muss, etwa um sogenannte Hate Crimes in sozialen Netzwerken als Phänomen der vernetzten Informationsgesellschaft technisch bewältigen können.[1989] Daraus wird eine Notwendigkeit für die Polizei abgeleitet, sich an den technologischen Wandel anzupassen,[1990] um nicht ins Hintertreffen zu geraten[1991]:

> „Ohne IT, ohne die Leute, die diese Technik bedienen können, werden wir irgendwann in die Steinzeit zurückgebeamt werden. Wenn wir da nicht mithalten, da wird der Abstand der anderen zu uns so groß, auch zu den Straftätern wird der so groß werden, dass wir da nicht mehr mitkommen. Die blockieren dann unsere Systeme."[1992]

In einigen Wahrnehmung steht man kurz vor einem Entgleiten der Handlungsfähigkeit, die nur über eine technologische Adaption verhindert werden kann[1993]:

1986 Siehe dazu bereits oben S. 68 f.
1987 Interview 8, Pos. 39; Interview 12, Pos. 45.
1988 Interview 1, Pos. 118.
1989 Interview 1, Pos. 75.
1990 Interview 1, Pos. 74; Interview 9, Pos. 48; Interview 12, Pos. 59.
1991 Interview 8, Pos. 53.
1992 Interview 3, Pos. 104.
1993 Ähnliches wurde auch in anderen empirischen Untersuchungen berichtet, siehe etwa bereits vor knapp 20 Jahren *Chan/Brereton/Legosz* ua, E-policing: The Impact

> „Es geht schon nicht mehr. Es ist im Moment noch gerade so händelbar, aber die Technologie schreitet immer weiter voran, die Festplatten werden immer größer, der Cloud-Speicher wird immer größer, der Cloud-Speicher wird ausgelagert in andere Länder, wo Sie im Prinzip gar keinen Zugriff mehr drauf haben und wir müssen immer mehr auf automatisierte Verfahren zugreifen."[1994]

Die dabei zum Ausdruck kommende technologische Rückständigkeit der Polizei wird als „ewiger Kreislauf" konzeptualisiert.[1995] Bemerkenswert ist auch, dass die Polizei im Stand ihrer technischen Entwicklung mitunter 15 Jahre hinter dem Level der Gegenwart verortet wird.[1996]

Damit spiegelt sich im Selbstverständnis die kriminalitätsbezogene Extensionstheorie: Kriminogene Technologie-Extensionen müssen mit kriminalpräventiven Technologie-Extensionen aufgewogen und bestenfalls – auch wenn das als kaum erreichbar angesehen wird – überwältigt werden.[1997]

Als „das größte Problem der Zukunft der Polizei" wird vor allem die Bewältigung von Massendaten gesehen.[1998] Insgesamt erscheint aber auch die fortschreitende Technologisierung per se eher als Nachteil denn als Vorteil für polizeiliches Arbeiten, da sich in der Innensicht der Polizei die Waffengleichheit zugunsten der Täter:innen verschiebt[1999] und für die eigenen Organisationen vorrangig eher neue Zwänge und Widersprüchlichkeiten entstehen, etwa wenn die Polizei über die neuen Verarbeitungsverfahren auch Personalknappheit ausgleichen soll,[2000] eine technologische Weiterentwicklung polizeilichen Informationshandelns gleichzeitig aber (beispielsweise finanzielle) Ressourcen[2001] braucht und wiederum Personalressourcen benötigt, um die Wissensgewinne durch datafizierte Polizeiarbeit dann auch an den jeweiligen Stellen wirksam werden zu lassen:

---

of Information Technology on Police Practices, S. 17: „Policing knowledge, which used to be carried inside police officers' heads, has now become synonymous with data that are too complex and voluminous for the human brain to cope with."; ähnlich auch bei *Egbert/Leese,* Criminal futures, S. 94.

1994 Interview 4, Pos. 69.
1995 Interview 6, Pos. 28.
1996 Interview 14, Pos. 76.
1997 Siehe dazu bereits oben S. 67 ff.
1998 Interview 4, Pos. 67; Interview 15, Pos. 64.
1999 Interview 4, Pos. 53.
2000 Interview 4, Pos. 43.
2001 Interview 6, Pos. 70.

> „Ich muss natürlich die Organisation der Polizei mit entsprechenden Kräften dann auch vorhalten, um bei solchen Prognosen dann auch polizeilich mitzuwirken. Wenn ich keine Kräfte habe, dann nützt mir die beste Prognose nichts."[2002]

Im Rahmen des Massendatenphänomens wird wiederum der Cyberkriminalität eine zentrale Rolle als Impulsgeber der technologischen Wandlungsprozesse bei der Polizei zugeschrieben.[2003] Aber auch herkömmlichere oder bagatellhafte Kriminalität und ihre Bearbeitung durch die Polizei werden von technologischen Wandlungsprozessen erfasst. Dabei wird die schnellere, weil digitale Erfassung und Erledigung von Anzeigen aber auch als Chance gesehen.[2004] Die Online-Wachen[2005] werden so zusätzliche, zentralisierte Informationsquellen und Interaktionspunkte für die Polizeien. Diese neuen Schnittstellen mit der Gesellschaft, über die lebensweltliche Daten quasi unmittelbar über mobile Endgeräte von Bürger:innen in das polizeiliche Informationswesen gespeist werden können, sind dabei ein wesentliches Instrument. So hat sich etwa in Nordrhein-Westfalen die Zahl der über die Online-Wache eingegangenen Vorgänge zwischen 2019 und 2021 mehr als verdoppelt.[2006]

Tendenziell werden immer mehr polizeiliche Informationspraktiken digitalisiert und automatisiert, etwa wenn Beamt:innen direkt aus dem Streifenwagen oder mit dem Smartphone Daten in die Informationssysteme eingeben, von wo sie dann auf die zentralen Datenbanken gezogen und im Anschluss an die notwendigen Stellen gesteuert werden können.[2007] Auch werden invasivere Maßnahmen wie die Bodycam-Verwendung in Wohnungen, die mal „undenkbar" war, im Zuge des technologischen Fortschritts möglich.[2008] Damit entstehen zudem lauter mobile Schnittstellen des polizeilichen Informationswesens, über die Daten über (potenziell abweichendes) Verhalten in die Datenbestände der Polizei gelangen, was ein generelles Anwachsen der polizeilichen Datenbasis erwarten lässt.

2002 Interview 6, Pos. 50.
2003 Interview 2, Pos. 120; Interview 7, Pos. 46; Interview 14, Pos. 76.
2004 Interview 1, Pos. 74.
2005 Interview 11, Pos. 50.
2006 *Ministerium des Innern des Landes Nordrhein-Westfalen*, Neues Portal „Internetwache" der nordrhein-westfälischen Polizei freigeschaltet, https://www.im.nrw/neues-portal-internetwache-der-nordrhein-westfaelischen-polizei-freigeschaltet (Stand: 01.10.2023).
2007 Interview 6, Pos. 32.
2008 Interview 8, Pos. 51.

Als technologiebedingten Einschnitt lässt sich auch die Einführung von KI-Verfahren in die allgemeinen Arbeitsprozesse der Polizei deuten, etwa im Rahmen der informationellen Qualitätskontrolle der eigenen Daten, um diese konsistenter und schneller für anschließende Verarbeitung verfügbar zu haben.[2009] In eine ähnliche Richtung bewegt sich auch die nach innen gerichtete informationelle Durchdringung und Aufschlüsselung der Polizeiorganisationen selbst, etwa wenn die operativ relevanten organisatorischen Komponenten in modernen Einsatzleit- und -führungssystemen analysiert und strukturiert werden, mittels derer präziser auf Lagen mit den richtigen Ressourcen reagiert werden kann,[2010] um so in einer Welt, die durch die Wahrnehmung von mehr und mehr Daten komplexer geworden ist, Überblick und Handlungsfähigkeit zu behalten. Diesem Anliegen dienen letztlich auch Verfahren wie die automatisierte Datenanalyse, die im Kontext des technologischen Wandels und insbesondere der Massendaten als unausweichlich beschrieben werden.[2011] In der Folge ist Informationstechnologie längst eine nicht mehr wegzudenkende Basis für polizeiliches Handeln und durchzieht jeden polizeilichen Arbeitsalltag.[2012] Eine umfassende Datafizierung der polizeilichen Arbeit lässt sich also auf ganzer Breite im polizeilichen Informationswesen beobachten.[2013]

Die Bewältigung dieser Entwicklungen macht eine neue Datenliterarität der künftigen Polizist:innen notwendig[2014]: „Man muss mit diesen Daten umgehen können, diese Daten auswerten können."[2015] Aber nicht nur auf der Ebene der jeweiligen Polizist:innen ist eine Anpassung diesbezüglich gefordert. Vielmehr werden auch organisationale Lernprozesse für einen Umgang mit datafiziertem Wissen gefordert. So müssten die polizeilichen Führungsebenen lernen, besser mit Unschärfen und der latenten Fehleranfälligkeit von Trendberechnungen und Prognosen, die als notwendig für eine bessere strategische Ausrichtung der Polizei gesehen werden, umzugehen.[2016] Zudem entstehen durch die starke Technologisierung, insbesonde-

2009 Interview 11, Pos. 19 f.
2010 Interview 14, Pos. 90.
2011 Interview 14, Pos. 40.
2012 Interview 6, Pos. 18, 20.
2013 Siehe zum Begriff und Dynamiken der Datafizierung bereits oben S. 46 ff.
2014 Interview 4, Pos. 28; Interview 6, Pos. 28; in diese Richtung bereits *Wilz/Reichertz* in Lange/Ohly (Hrsg.), Auf der Suche nach neuer Sicherheit, 221 (226 f.).
2015 Interview 1, Pos. 75.
2016 Interview 6, Pos. 50, 52.

re auch mit vernetzten Informationsmedien, neue Vulnerabilitäten für die Polizei als Organisation selbst.[2017]

Technologischer Wandel bei der Polizei wird aber durch polizeiliche Organisationsstrukturen, die eher starr sind, gehemmt.[2018] Solche Hemmnisse entstehen zudem durch Pfadabhängigkeit vieler zentraler informationstechnologischer Strukturen, die in großen Teilen durch den Föderalismus bedingt sind.[2019] Infolge dieser unterschiedlichen Voraussetzungen gibt es zwischen den Länder- und Bundespolizeien auch unterschiedliche Adaptionsgrade,[2020] etwa im Bereich des Predictive Policing[2021] oder auch hinsichtlich der Einführung der E-Akte,[2022] weshalb in das Projekt Polizei 2020 große Hoffnungen als übergreifendes Restrukturierungs- und Integrationsprogramm für das polizeiliche Informationswesen in seiner Gänze gesetzt werden.[2023]

Aber auch hier bestehen die vielen, bereits zuvor angesprochenen Probleme bezüglich der Durchführung von Projekten, die den technologischen Wandel adressieren sollen, weil die Planung Komplexitäten nicht hinreichend oder technologisch induzierte Zwänge nur begrenzt berücksichtigt:[2024]

> „Mittlerweile ist die Informationsverarbeitung so weit vernetzt über Schnittstellen mit allen möglichen Sachen, dass die Chance, dass man an den Knöpfen dreht… relativ schwierig ist, dass man ganz große Entwürfe macht. Man kann also maximal gegensteuern und bestimmte Dinge neu entwickeln, aber man muss dann eben gucken, wo das einschlägt, wenn man da was ändert, weil die Abhängigkeit der Systeme mittlerweile sehr groß geworden ist."[2025]

Zum Ausdruck kommt hier die zentrale Bedeutung infrastruktureller Konfigurationen, wie sie bereits für andere sozio-technische Systeme beschrie-

2017 Interview 12, Pos. 12.
2018 Interview 14, Pos. 96, 98.
2019 Interview 3, Pos. 98; Interview 5, Pos. 40.
2020 Interview 13, Pos. 93.
2021 Interview 12, Pos. 49.
2022 Interview 13, Pos. 91.
2023 Interview 11, Pos. 62.
2024 Interview 6, Pos. 46, 68.
2025 Interview 6, Pos. 16.

ben wurde.[2026] Im polizeilichen Informationswesen wirken sich die beschriebenen (infra)strukturellen Fehlentwicklungen nun innovationshemmend aus. Trotz dieser Schwierigkeiten in der Weiterentwicklung des polizeilichen Informationswesens erscheint vielen der informationstechnologische Wandel als Versprechung – zumindest grundsätzlich: „das wird alles immer mehr digitalisiert, also das wird einfacher werden – angeblich."[2027] Dieser Charakter von neuen informationstechnischen Lösungen als Projektionsfläche, die man gleichzeitig kritisch hinterfragen muss, äußert sich beispielsweise auch im Kontext der automatisierten Datenanalyse:

> „Es ist eine neue Technologie, der man eine Chance geben sollte, um sie auszuprobieren. Aber man darf dabei bei allem Enthusiasmus nicht vergessen, einen kühlen Kopf zu bewahren und zu sagen: Aufwand-Nutzen-Verhältnis und wo sind die rechtlichen Grenzen, wo sind die fachlichen Grenzen, was bringt es und was nicht?"[2028]

Das erfordert eine Fehlerkultur und Offenheit bezogen auf technologische Wandlungsprozesse, die gegenwärtig als nicht in befriedigendem Maße vorhanden beschrieben wird.[2029] Ähnliches gilt auch für Anwendungen von Predictive Policing:

> „Wir hatten hier so einen Prototyp und ich bin jetzt mal vorsichtig, weil es noch nicht 100% abgeschlossen ist, aber das klingt immer so schön: Ich nehme die Daten, kippe sie in ein System rein und der Rechner sagt mir per Prognose, wann der Täter das nächste Mal einbricht. Das funktioniert nicht."[2030]

In diesem Zusammenhang wird auch die Ersetzung von traditioneller Polizeiarbeit durch technologische Lösungen eher kritisch gesehen.[2031]

Mit Blick auf technologische Wandlungsprozesse spielt der Datenschutz oder die Regulierung von polizeilicher Informationsverarbeitung wieder

---

2026 *Star* American Behavioral Scientist 43 (1999), 377; ähnlich auch *Hughes* in Bijker (Hrsg.), The Social Construction of Technological Systems. New Directions in the Sociology and History of Technology, 51.

2027 Interview 3, Pos. 54.

2028 Interview 6, Pos. 56.

2029 Interview 6, Pos. 54.

2030 Interview 6, Pos. 50.

2031 Interview 6, Pos 54. Siehe dazu auch *Egbert/Leese,* Criminal futures, S. 108, die ebenfalls davon berichten, dass die polizeiliche Entscheidungsträger:innen Analyseverfahren wie Predictive Policing als Hilfsinstrument sehen, dessen Einfluss man nicht überschätzen solle.

eine ambivalente Rolle: Polizeiliches Handeln soll nicht (noch weiter) durch das Recht gelähmt werden,[2032] wobei aber durch den technologischen Fortschritt die Befürchtung entsteht, das Persönlichkeitsrecht könnte auf der Strecke bleiben,[2033] sodass Regulierung geradezu lähmen muss: „Wir müssen mit dem Recht der Technik sagen, was sie zu machen hat."[2034] In dieser Schlichtheit bleibt diese einseitige Kausalitätsvorstellung, wie dargelegt, mit Blick auf die Wechselwirkungen der Regulierung allerdings unterkomplex, denn es sind vor allem auch die bereits angesprochenen technischen Aspekte des Datenschutzes, von denen eine gelingende Regulierung polizeilicher Datenverarbeitung ganz maßgeblich abhängt.[2035]

XII. Zukünftige Entwicklungspfade der polizeilichen Informationsverarbeitung

Anknüpfend an die beschriebenen technologischen Wandlungsprozesse ließen sich in den Interviews weitere Entwicklungspfade und aufkommende Phänomene im Bereich der polizeilichen Informationsverarbeitung ausmachen.

1. Das Projekt „Polizei 2020"

Die deutlichste Linie ist dabei wohl das Projekt „Polizei 2020",[2036] das als konkrete, polizeiübergreifende Entwicklung große Aufmerksamkeit innerhalb wie außerhalb der Polizeien generiert. Die befragten Datenschutzbeauftragten sind auch hier als Berater:innen eingesetzt, wobei allerdings nur diejenigen von ihnen größere Berührungsflächen mit dem Projekt haben, die an neuralgischen Punkten des polizeilichen Informationswesens positioniert sind.[2037] Das wirkt sich dementsprechend auch auf die Kenntnisgrade aus, die sich bei den Befragten über das Projekt auftaten.[2038]

2032 Interview 4, Pos. 45.
2033 Interview 5, Pos. 52.
2034 Interview 7, Pos. 32.
2035 Siehe dazu bereits oben S. 366 ff.
2036 Siehe zum konzeptuellen Inhalt des Programms bereits oben S. 271 ff.
2037 Interview 1, Pos. 76-81; Interview 10, Pos. 66.
2038 Interview 2, Pos. 132, 134; Interview 3, Pos. 104; Interview 5, Pos. 50; Interview 15, Pos. 74.

Den Äußerungen der Befragten zufolge ist das Projekt strukturell stark beim Bundeskriminalamt verwurzelt und bezieht daneben auch die Landeskriminalämter mit in die Planung und Umsetzung ein, teilweise auch in Kooperation mit den technischen Polizeiorganisationen in einem Land, die dann ländereigene Projektgruppen ausbilden.[2039] Insgesamt handelt es sich aber um ein „autarkes Programm", das wenig in die eigentlichen Polizeistrukturen eingebunden zu sein scheint,[2040] sondern sich ein stückweit verselbstständigt hat,[2041] sodass auch mitunter nicht genau bekannt ist, ob neue Projekte auf das Programm zurückgehen oder hauseigene Vorhaben sind.[2042] Im Rahmen von Polizei 2020 gibt es dann regelmäßig Programmleiter-Tagungen mit zwei untergeordneten Gremien mit Vertreter:innen aus Bund und Ländern (Steuerungskreis Technik und Steuerungskreis Fachlichkeit).[2043]

Das Projekt wird tendenziell positiv bewertet und in seinem Konzept begrüßt.[2044] Auch die Einschätzung der Notwendigkeit des Projekts als technologischen Innovationsimpuls für alle Polizeien in Deutschland wird geteilt.[2045] Erhofft werden sich Effektivitäts- und Effizienzgewinne,[2046] insbesondere durch den Aufbau einheitlicher Datenbanken mit einheitlichen Abfragemodalitäten sowie die Bereitstellung neuer Anwendungen als Arbeitsplattformen für regionale Polizeiorganisationen.[2047] Gleichzeitig wird sich auch ein besser strukturierter Datenschutz vom Projekt versprochen.[2048] Trotz der positiven Aspekte wird auch die politische Natur des Projekts und bestimmter Ambitionen, gesehen, da Polizei 2020 seinen Ursprung in der „Innenministerkonferenz" hat.[2049]

Dreh- und Angelpunkt der Vereinheitlichung ist, wie bereits angesprochen, das einheitliche Datenformat. Den vormals bestehenden Wildwuchs

2039 Interview 4, Pos. 57; Interview 5, Pos. 48, 50; Interview 10, Pos. 64; Interview 12, Pos. 59.
2040 Interview 4, Pos. 64.
2041 Interview 15, Pos. 66 ff.
2042 Interview 9, Pos. 50.
2043 Interview 6, Pos. 58.
2044 Interview 2, Pos. 134; Interview 7, Pos. 52; Interview 9, Pos. 52; Interview 10, Pos. 68; Interview 11, Pos. 62; Interview 12, Pos. 59; Interview 15, Pos. 78.
2045 Interview 3, Pos. 104; ebenso etliche Befragte bei *Egbert/Leese,* Criminal futures, S. 213.
2046 Interview 4, Pos. 65; Interview 12, Pos. 59.
2047 Interview 10, Pos. 64, 68.
2048 Interview 4, Pos. 57; Interview 13, Pos. 96.
2049 Interview 5, Pos. 50.

an polizeilichen Datenmodellen hat man bereits vor Polizei 2020 immer weiter konsolidiert und in ein „Polizei 2020-XPolizei-Datenmodell" kanalisiert, mit dem nun eine gemeinsame Datenbank erstellt werden soll.[2050] Dabei müssen allerdings alle rechtlichen Rahmenbedingungen aller deutschen Polizeien berücksichtigt werden,[2051] was die erheblichen Aufwände des Projekts verursacht.[2052] Insbesondere ergeben sich aus dem Berechtigungskonzept komplexe Anforderungen, vor allem, um auch die Rechtsprechung des Bundesverfassungsgerichts zur sicherheitsbehördlichen Datenverarbeitung, wie sie sich etwa in § 12 Abs. 1 und 2 BKAG niedergeschlagen hat, umzusetzen und in der Technik abzubilden.[2053] Alle Daten müssen technisch mit entsprechenden Tags und Markern für die jeweiligen Löschungsfristen oder Kennzeichnungen – etwa wegen der Herkunft der Daten aus invasiven Maßnahmen – versehen werden, damit der Zugriff auf die Daten durch die einzelnen Polizeibeamt:innen je nach den unterschiedlichen landes- und bundespolizeirechtlichen Rahmenbedingungen freigeschaltet werden kann. Dieses – zentrale – Vorhaben von Polizei 2020 wird als äußerst aufwändig beschrieben.[2054]

Nicht nur anlässlich dieser Schwierigkeiten wird das Projekt aber auch kritisch gesehen:

> „Bei Zentralsystemen geht schnell Innovation verloren. Das ist so meine Befürchtung: Wir haben einen Haufen Pläne, Entwicklungen überall, die immer wieder hochsprießen, die hochinnovativ sind. Da müssen sich die Zentralstellen dann durchsetzen und das mitnehmen, damit es dann landesweit gilt. Wie das in diesem System bei einer kompletten Software funktionieren soll, habe ich so meine Zweifel. Und wenn da eine Firma mitspielt, sagt die: Nur wenn ich Geld verdiene, macht Innovation Sinn. Mal gucken wohin das geht."[2055]

Neben diesen befürchteten Innovationseinbußen, die konträr zum expliziten Ziel der Innovationsförderung durch die geplante Vernetzung der Polizeien liegt,[2056] wird auch die föderale Ausgangslage als problematisch für die Umsetzbarkeit des Konzepts gesehen:

2050 Interview 14, Pos. 62.
2051 Interview 14, Pos. 62.
2052 Interview 4, Pos. 17.
2053 Interview 1, Pos. 114.
2054 Interview 14, Pos. 64.
2055 Interview 6, Pos. 62.
2056 Siehe dazu bereits oben S. 271 ff.

> „16 Bundesländer, mit 16 verschiedenen Interessen und wer da alles mitwirkt. Das ist schwierig… ich sage immer: In der IT gibt es ein bisschen schwanger nicht. Aber der Kompromiss besteht dann immer bei irgendwas darin, das so zu formulieren: „Das bedarf der länderspezifischen Ausprägung." Das heißt, das was man eigentlich will, ein gesamtdeutsches, einheitliches System für die Informationsverarbeitung, wird an der Stelle schon wieder ausgehebelt, weil ländermäßig darf ich das nachher so konfigurieren wie ich es will, wie es brauche, wie ich es muss. Das heißt, alles das, was dazu geführt hat, dass die Länder unterschiedliche Systeme haben, wird nicht geändert. Das heißt, die Rechtsgrundlagen bleiben so, die Organisationsfragen innerhalb der Polizei bleiben so. Die strategische Ausrichtung bleibt länderbezogen. Genau das schlägt in solchen Systemen ein. Ich glaube nicht, dass das funktionieren wird. Insofern habe ich sehr viel Skepsis auch aufgrund der Mitspieler, die da alle dabei sind, dass es so wie es jetzt aussieht, dass das nicht funktioniert. Der Grundsatz ja, bin ich dafür. Aber die Art und Weise, wie es umgesetzt wird und die Rahmenbedingungen, die sie dafür geschaffen haben, lassen aus meinen Erfahrungen von solchen Großprojekten sagen: Ihr seid auf einem ganz dünnen Eis, das kann schnell schiefgehen. Und das sieht wohl auch so aus, dass ich Recht behalten muss."[2057]

Insgesamt besteht allerdings scheinbar nur wenig Klarheit über den Umsetzungsstand und sonstige Aspekte, wie etwa die technischen Grundlagen des Projekts: So soll es eine BKA-Cloud-Anwendung geben, die wohl als Grundlage für das im Rahmen von Polizei 2020 zentral geplante Data-Warehouse, also die einheitliche, auf einem Datenmodell basierende Datenbank, dienen soll.[2058] Diese Undurchsichtigkeit und mangelnde Kommunikation des Projekts mit den Datenschutzbeauftragten wird auch offen moniert.[2059] Insofern müssen die Belange des Datenschutzes offensiv vertreten werden, denn das Zusammenlegen der Datenbestände und die Kooperationen im informationstechnologischen Bereich machen eine datenschutzrechtliche „Gratwanderung" erforderlich. [2060] Allerdings wird es für Betroffene auch als datenschutzrechtlich sinnvoll beschrieben, dass das „Denken in Dateien […] als Relikt aus dem alten Datenschutzrecht auf[ge]geben"

2057 Interview 6, Pos. 58.
2058 Interview 11, Pos. 66.
2059 Interview 14, Pos. 84.
2060 Interview 11, Pos. 62.

wird und man so einen datenschutzrechtlichen Blick auf Verarbeitungsverfahren in ihrer Breite und Vernetzung ermöglicht.[2061] Daneben können wohl auch Redundanzen in den Datenbeständen abgebaut werden,[2062] damit Personen nicht mehr in „fünf Dateien gleichzeitig sind."[2063] Allerdings darf nicht darüber hinweggesehen werden, dass sich aus der verschiedentlichen Schaltung der Zugriffe auf die Datenbestände je nach polizeilicher Rolle letztlich wiederum „sowas wie eine Dateistruktur" ergibt,[2064] nur eben virtuell und flexibel freischaltbar.

Will man die Umsetzbarkeit des Projekts abschließend mit einer Prognose versehen, so könnten die Kriterien, die *Chan et al.* für die Implementierung technologischer Innovationsprojekte bei polizeilichen Organisationen vorschlagen, eine systematischere Beurteilung erlauben. Die Kriterien sind die Technologie selbst und ihr Design (1), die Art und Weise der Implementierung, der Grad möglicher Konflikte zwischen den technologischen Vorstellungen der Entwickler und den praktischen Bedürfnissen der Nutzer (3), der Grad der daraus möglicherweise resultierende Verschiebungen der Machtverhältnisse und Verantwortlichkeiten innerhalb der Organisation (4) und daraus resultierende zusätzliche Formen der Öffnung der Polizei gegenüber externen Einflüssen der Öffentlichkeit (5).[2065] Vor allem die beschriebenen Komplexitäten des Technologiekonzepts selbst und seiner Implementierung stehen einer allzu positiven Prognose insofern im Wege. Auch Unterschiede in den technologischen Vorstellungen bezüglich der Umsetzbarkeit scheint es innerhalb der Organisationen zu geben und die zuweilen begrenzte Involvierung von durchaus wichtigen Akteur:innen im Feld der polizeilichen Informationsverarbeitung deutet darüber hinaus auch auf innerorganisatorische Verschiebungen zumindest der Verantwortlichkeiten hin, sodass ein Verlauf wie geplant und eine zielgenaue Beendigung des Projekts wohl als unsicher gelten dürften.

2061 Interview 1, Pos. 116.
2062 Interview 1, Pos. 114.
2063 Interview 1, Pos. 86.
2064 Interview 1, Pos. 86.
2065 *Chan/Brereton/Legosz* ua, E-policing: The Impact of Information Technology on Police Practices, S. 13.

2. Emergente Kriminalitätsphänomene

Immer wieder wurde in den Gesprächen auch auf emergente Kriminalitätsphänomene Bezug genommen. Das verwundert nicht, bedenkt man, dass technologische Entwicklungen vor allem unter legitimatorischen Gesichtspunkten untrennbar mit dem Aufkommen neuer und auch veränderter Wahrnehmung bestehender Kriminalitätsphänomene verbunden sind, da es für die Polizei im Rahmen des technologischen Wandels direkt oder indirekt darum geht, dem delinquenten Einsatz von technologischen Innovationen Waffengleiches entgegenzuhalten oder neue technologische Lösungen als Antwort auf Kriminalitätsbereiche zu formulieren, die bereits bekannt sind, sich aber teilweise – in der Wahrnehmung durch die Polizei oder tatsächlich – ändern.[2066]

Als größte Herausforderung wird dabei eine Art sich immer weitere professionalisierende oder bereits professionalisierte Cyberkriminalität wahrgenommen. Daraus leitet sich ein Zugzwang für die Polizei ab, sich ebenfalls weiter in den je einschlägigen informationstechnologischen Bereichen weiterzuentwickeln.[2067] Daneben besteht in diesem Zusammenhang ein Problem mit der Internationalisierung vor allem dieser Kriminalitätsform.[2068]

Allerdings wird im Zusammenhang mit jeglicher Form von Kriminalität, die über das Auswerten von Informationen ermittelt wird, die sich im Einflussbereich der Täter:innen befinden – von Kinderpornographie über Betäubungsmittelkriminalität bis hin zu Betrug – ein problematischer Umstand bemerkt: Die zunehmenden technischen Fähigkeiten der Täter:innen bzw. das Absinken der Lernkosten, die für den Gebrauch von kriminalitätsermöglichender oder -unterstützender Technik investiert werden müssen[2069]:

> „Also es ist schwierig. Wenn Sie einen Täter haben, der sich in der Technik gut auskennt, der Krypto-Handys verwendet, der verschlüsselt kommuniziert, der nur TOR-Browser verwendet, wie wollen Sie da Beweise finden? […] Stellen Sie sich vor: Sie sind auf einer Durchsuchung und haben dort die Rechner des Beschuldigten sichergestellt und der hat alles

2066 Interview 8, Pos. 39; siehe zu dieser Dynamik bereits oben S. 69.
2067 Interview 1, Pos. 131; Interview 2, Pos. 120; Interview 3, Pos. 104; Interview 6, Pos. 28; Interview 7, Pos. 54; Interview 14, Pos. 76.
2068 Interview 10, Pos. 56, 58.
2069 Interview 4, Pos. 55.

> nur in der Cloud-Anwendung gemacht, sie haben keinen Hinweis, der hat nichts gespeichert, keine Cookies, hat einen PC-Cleaner drauf, Sie haben einen komplett blanken Rechner. Wenn Sie einen guten Beschuldigten haben, haben Sie gar nichts. Der kann KiPo vertreiben, wie er möchte, wenn er das richtig macht, dann kriegen Sie den erstmal nicht. Dann haben Sie eine Überwachung von ihm, Telefonüberwachung oder sonst was. Der holt sich irgendwo im nächsten Urlaub – jetzt mit Corona ist schwierig – in Marokko irgendwelche SIM-Karten und telefoniert dann, oder Lyca-Mobile, da wechselt die IMSI, wie er gerade möchte und versuchen Sie, den mal zu überwachen. Wenn Sie einen haben, der sich mit der Technik auskennt, haben Sie wenig Chancen."[2070]

Neben neuen Schwierigkeiten ergeben sich für die Polizeien durch die informationstechnologischen Entwicklungen aber auch Chancen der besseren Ressourcenallokation durch eine organisationale Selbstregulation,[2071] indem Phänomene und die Reaktion der Polizei auf diese informationell analysierbar gemacht werden, um so im Wege von selbstreflexiven Informationsschleifen die polizeiliche Herangehensweise an emergente oder sich wandelnde Kriminalitätsbereiche zu effektivieren,[2072] wobei aufgrund beschränkter Ressourcen trotzdem eine Priorisierung notwendig bleibt.[2073]

3. Technologische Innovationen

Die verschiedenen technologischen Innovationspfade, auf denen die Polizeien Lösungen für die von ihnen wahrgenommenen Probleme suchen, sind alle bereits mehr oder weniger deutlich im Rahmen dieser Auswertung der Gespräche angeklungen, sollen an dieser Stelle allerdings noch einmal kondensiert dargestellt werden.

Stark im Wandel ist die basale informationelle Infrastruktur der Polizei. Mobile Endgeräte[2074] samt Anwendungen in App-Format[2075] werden für die verschiedenen Dienstgebräuche ausgerollt und Vereinheitlichung von Grundstandards wie dem Datenmodell[2076] sollen in einem kohärenten,

2070 Interview 4, Pos. 53.
2071 *Mastrofski/Willis* Crime and Justice 39 (2010), 55 (57, 90).
2072 Interview 10, Pos. 9.
2073 Interview 12, Pos. 45.
2074 Interview 11, Pos. 50.
2075 Interview 10, Pos. 15 ff.
2076 Interview 6, Pos. 60; Interview 14, Pos. 62.

konsolidierten polizeiliches Informationswesen münden. Dabei bleibt eine Aufteilung in Grundsysteme und Spezialsysteme bestehen,[2077] nur sollen die jeweiligen Systeme auf eine gemeinsame Datenbank zugreifen können, was über die vergrößerte Datenbasis zu einer höheren informationellen Durchdringung von Sachverhalten führen würde. Weitere grundlegende Veränderungen der polizeilichen Informationsarchitektur sind mit dem Einsatz von Cloud-Systemen[2078] geplant, etwa zur Entgegennahme großer Bild- und Videodatenmengen aus der Bevölkerung.[2079]

Daneben kommt es zur Digitalisierung von bereits Bestehendem: Der Kontakt zu den Bürger:innen kann zusätzlich über Online-Wachen abgewickelt werden,[2080] womit sich für die Polizei eine besonders niedrigschwellige Informationsquelle über möglicherweise abweichendes Verhalten auftut. Auch die traditionellen Arbeitsweisen sind davon betroffen, wenn die bereits begonnene Digitalisierung der Aktenhaltung flächendeckend in der E-Akte gemündet ist.[2081] Neben den damit verbundenen Risiken[2082] ermöglichen digitalisierte Fachverfahren auch eine Beeinflussung von Informationspraktiken der Polizist:innen, etwa durch Erforderlichkeits- oder Zweckbindungserinnerungen[2083] und automatisierte Einhaltung von anderen datenschutzrechtlichen Bestimmungen wie Löschpflichten.[2084]

Nicht nur die Arbeitsweise, auch die zu erfassenden Informationspunkte sollen an die zunehmende Digitalität unserer Lebenswelten angepasst werden, indem vor allem OSINT-Techniken, aber auch Techniken wie das Data Scraping[2085] als lohnenswerte Ergänzung für polizeiliches Arbeiten gesehen werden („wenn das Private dürfen, ist es dann nicht irre, wenn der Staat das nicht darf und dadurch möglicherweise ein Anschlag nicht

2077 Interview 9, Pos. 56; Interview 14, Pos. 76.
2078 Interview 11, Pos. 64.
2079 Bundeskriminalamt, Abteilung „Digitale Services und Innovation" (DI), https://www.bka.de/DE/DasBKA/OrganisationAufbau/Fachabteilungen/Informationstechnik/informationstechniknode.html (Stand: 01.10.2023).
2080 Interview 11, Pos. 50; Interview 13, Pos. 59.
2081 Interview 3, Pos. 54; Interview 12, Pos. 91.
2082 Siehe dazu bereits oben S. 310 ff.
2083 Interview 10, Pos. 70 ff.
2084 Interview 10, Pos. 70; so bereits *Mastrofski/Willis* Crime and Justice 39 (2010), 55 (89).
2085 Data Scraping ist eine Technik, bei der automatisiert Daten aus der von Menschen lesbaren Ausgabe eines anderen Programms, insbesondere auch von Webseiten, extrahiert und in eine Datenbank übertragen werden.

verhindert werden kann").[2086] Vom Einsatz von OSINT-Techniken, etwa in sozialen Netzwerken, wird dementsprechend bereits berichtet.[2087] Die Anreicherung der polizeilichen Wahrnehmung durch Ausbau der Datenerhebungskapazitäten beschränkt sich allerdings nicht auf digitale Räume, sondern ist auch in der analogen Lebenswelt zu verzeichnen.[2088]

Die durch diese vielfältigen Praktiken gefüllten Datenbestände der Polizei sind in der Informationsgesellschaft indessen bei weitem nicht die einzigen oder umfangreichsten Informationssammlungen. Insofern liegt eine Verknüpfung der polizeilichen Informationsbestände mit den externen, „latenten" Datenbanken anderer gesellschaftlicher, vor allem aber privater Akteure vor. Dazu scheint es im Rahmen von automatisierten Datenanalysen eine – in Reichweite und Zeitlichkeit beschränkte – Möglichkeit zu geben.[2089]

Die automatisierte Datenanalyse ist als flexibles und mit Erwartungen beladenes Instrument ein wichtiger Baustein in der polizeilichen Strategie zur Bewältigung von Massendaten,[2090] auch wenn es in seiner gegenwärtigen Form als polizeirechtliche Maßnahme „nur" zur Gefahrenabwehr, zur Ausleuchtung des Gefahrenvorfelds und zur vorbeugenden Straftatenbekämpfung genutzt werden darf.[2091] Daneben dient die automatisierte Datenanalyse auch als Tool zur Überbrückung der Fragmentierung polizeilicher Datenbestände, wie es auch bei PIAV – dort aber überregional – der Fall ist,[2092] indem eine Art virtuelle Datenbank simuliert wird. Auch für dieses Instrument wird aber technisch bezüglich der Leistungsfähigkeit und rechtlich bezüglich der Vereinbarkeit mit den Prinzipien des Datenschutzes Skepsis geäußert.[2093] Gemäß ihrer polizeirechtlichen Anbindung hat die automatisierte Datenanalyse nur Zugriff auf polizeiliche Systeme. Da aber diese überwiegend Mischdateien sind, also auch strafverfahrensrechtliche Daten enthalten, hat das Instrument auch Zugriff auf Daten aus Strafver-

2086 Interview 1, Pos. 139.
2087 Interview 14, Pos. 72.
2088 Interview 14, Pos. 108; Siehe dazu bereits oben etwa S. 312 ff.
2089 Interview 1, Pos. 139; Interview 14, Pos. 74; siehe dazu auch *Brayne,* Predict and surveil, S. 5, die von ähnlichem Gebrauch privater Plattformen in den Vereinigten Staaten berichtet.
2090 Interview 1, Pos. 132 ff.; Interview 14, Pos. 40.
2091 Interview 14, Pos. 60.
2092 Interview 8, Pos. 69.
2093 Interview 6, Pos. 56; Interview 15, Pos. 88; einen ähnlichen Befund stellen auch *Egbert/Leese,* Criminal futures, S. 52 vor, die von einer medial vermittelten Furcht vor dystopischen Szenarien auch bei Polizeibeamt:innen berichten.

fahren, die sich in den polizeilichen Informationssystemen finden. Darüber hinaus können auch Daten aus anderen Ländern erfasst werden, sofern diese zuvor über dafür bestehende informationelle Übermittlungskanäle in die Systeme derjenigen Länder mit automatisierter Datenanalyse gelangt sind.[2094] Über die konkrete Funktionsweise dieses Instruments bei den deutschen Polizeien ist kaum etwas bekannt. Auch im Rahmen der Interviewdurchführung konnten nur begrenzt Informationen dazu generiert werden. Allerdings ist die Funktionsweise der automatisierten Datenanalyse bei *Brayne* beschrieben. Zwar ist es eine Beschreibung im US-amerikanischen Polizeikontext, die sich allerdings auf die Software Palantir Gotham bezieht, die unter anderem auch hessenDATA (§ 25a HSOG) zugrunde liegt, sodass die Beschreibung zumindest als Ausgangspunkt für ein Verständnis dieser neuen Form der Datenverarbeitung genommen werden kann:

> „So now, imagine a robbery detective who says, „Hey, you know what, I have a male, average build, black 4-door sedan." Like, they would [previously be able to] do nothing with that, right? So, we can do that. Let's go take a look at vehicles that are in the system. Here is vehicles. So, I change my focus to vehicles… Now, we're going to go look at color… There are 140 million records in this system… we know it's a Toyota, maybe a Hyundai, right? Or a Lexus… So let's say we think it's one of those types of vehicles, right? And that got us then to 2 million [vehicles]. And if we were to go look at, say, a color. We are going to lose about 100,000 records just by choosing a color immediately, just because certain records just don't have that information. And so, we know it was black. Maybe it was blue, 'cause it could have been blue. It could be dark green… And we know it was a 4-door. Do you see what's happening over here? In five hops, they're able to get down to 160,000. Now they're still not going to look at 160,000 vehicles. We didn't get into model and year, but we could do that, and we could chart it, which makes it easy. Now this is just one of the cool advantages of „object explorer" and being able to look at all your data… So now I could say, I think it was between 2002 to 2005, drill down, now we're 23,000. Now it gets pretty manageable. So now let's flip over and let's look at the people that are connected to these vehicles. And I know I'm looking for a male. And I'll just do one of them. And I know that like let's say he was pretty short. And he was on the

2094 Interview 14, Pos. 49-58.

> heavier side. Brick house. We just got down to 13 objects, 13 people. And you could say, „Okay, well, now let me take a look at – all 13 have driver's license numbers." So now we've narrowed it down to 13 potential people and they could take these 13 objects and go to the DMV and pull their DMV photos and go to the witness or victim and say, „Here you go." In less than a minute, using partial information, Doug was able to narrow a search from 140,000,000 records to 13."[2095]

Neben solchen extrem verbesserten Recherchen in großen Datenspeichern ermöglicht die automatisierte Datenanalyse zudem auch die Visualisierung von sozialen Netzwerken in den polizeilichen Datenbeständen, wie sie durch Verbindungen zwischen Personen (Verurteilte, Beschuldigte, Verdächtige, Kontakt- und Begleitpersonen, Anlasspersonen, Zeugen, Opfer), Objekten, Orten und Ereignissen in den Datensätzen der Polizeien abgebildet sind.[2096] Auf diese Weise werden die Beziehungen rund um Normabweichungen – ganz gleich, ob sie stattgefunden haben oder vermutet werden – durchsichtiger für die Polizist:innen.

Neben diesem speziellen Massendatenverarbeitungsverfahren werden auch zunehmend KI-Verfahren als generelle Hilfstools zur Identifizierung von Mustern in den anschwellenden Datenbeständen eingesetzt.[2097] Damit sollen auch Prognose- und Trendberechnungen zur besseren strategischen Ausrichtung der Polizeien auf Grundlage ihrer Informationsbestände ermöglicht werden.[2098] Ein prominentes Beispiel sind die verschiedenen Spielarten von ortsbasiertem Predictive Policing[2099], wobei aber ebenfalls Zweifel an der Wirksamkeit bestehen[2100] und Probleme im Hinblick auf die datenschutzrechtliche Einhegung geäußert werden.[2101]

Diese technologischen Entwicklungen bringen auch häufig Fragen nach der Verortung menschlichen Ermessens bei polizeilichen Entscheidungen mit sich. Grundsätzlich unterliegen gänzlich automatisierte Entscheidungen engen Grenzen (vgl. etwa § 54 BDSG). Allerdings wird Ermessen durch datenangereicherte Umgebungen und datengetriebene Entscheidungspro-

2095 *Brayne,* Predict and surveil, S. 37 ff.
2096 *Brayne,* Predict and surveil, S. 111.
2097 Interview 4, Pos. 67, 69, 71; Interview 11, Pos. 18 ff.
2098 Interview 6, Pos. 52.
2099 Siehe dazu bereits oben S. 279 ff.
2100 Interview 6, Pos. 50; ähnlich auch die Befragten in der Studie von *Brayne,* Predict and surveil, S. 86.
2101 Interview 12, Pos. 49.

zesse regelmäßig nicht vollständig ersetzt, sondern verlagert, an einen anderen, der eigentlichen Handlungssituation vorgelagerten Zeitpunkt, zu dem es von einer anderen Person unter eventueller Zuhilfenahme von informationstechnologischen Instrumenten in einem sozio-technischen System zukunftsgerichtet ausgeübt wird.[2102] Inwiefern sich dies auf die Beamt:innen auswirken wird, ist informationspraxis- und informationstechnologiespezifisch zu erforschen.

4. Organisationale Wandlungsprozesse

Wie anhand der Interviews herausgearbeitet wurde, ist die technologisch fundierte Informationsverarbeitung mittlerweile ein absolut integraler Teil der polizeilichen Organisation selbst,[2103] da der polizeiliche Arbeitsalltag durchzogen von informationstechnologischen Geräten und daran anknüpfenden Prozessen ist und die daraus entstehenden Datenflüsse strukturiert werden müssen,[2104] wodurch polizeiliches Handeln überhaupt erst ermöglicht wird. Trotz dieser Bedeutung ist die organisatorische Zusammenarbeit von Jurist:innen und Informatiker:innen in der Polizei nicht überall ausreichend institutionalisiert, um Recht und Technik miteinander in Einklang zu bringen. Stattdessen werden informationstechnologische Abteilungen innerhalb der Polizeien als organisationale Dienstleister wahrgenommen:

> „Die IT ist noch nicht als gleichberechtigter und notwendiger Abstimmungspartner bei solchen Dingen akzeptiert worden. Das muss passieren. Bisher ist es immer so: Die IT wird nach wie vor als Dienstleister verstanden."[2105]

Eine solche Wahrnehmung steht deutlich in Kontrast zu der zunehmenden Bedeutung informationstechnologischer Expertise für die Polizeien. So kommt es beispielsweise – neben der bereits dargestellten Bedeutung von technischen Expert:innen für das polizeiliche Informationswesen im Allgemeinen – zunehmend zur Spezialisierung der polizeilichen Berufsbilder, um die durch den digitalen Wandel ausgelösten Problemlagen[2106] zu adressieren. Dafür müssen Laufbahnen geschaffen werden, wie etwa als

2102 *Brayne,* Predict and surveil, S. 139.
2103 Interview 3, Pos. 104; Interview 6, Pos. 24, 28.
2104 Interview 6, Pos. 32.
2105 Interview 6, Pos. 68.
2106 Interview 7, Pos. 54.

„Cyberfahnder", „die […] für andere dann auch Daten aufbereiten, denn die Komplexität wird ja immer höher."[2107] Die neuen Spezialisierung zeichnen sich aber durchaus auch durch ein breites, interdisziplinäres Tableau an erforderlichen Fähigkeiten aus.[2108] Gleichzeitig kommen mit den nachrückenden Polizist:innen-Generationen auch zunehmend „digital natives" zur Polizei, die technikaffin sind,[2109] dabei aber auch gewisse Anforderungen an den technologischen Entwicklungsstand der Organisation haben.[2110] Insgesamt deuten diese Beschreibungen auf eine Aufwertung von Kenntnissen und Fähigkeiten, die auf technischer Expertise basieren, innerhalb der Organisation hin. Auch in anderen Studien ist diese stärkere Betonung von Fähigkeiten, die sich als Verwissenschaftlichung der polizeilichen Tätigkeiten beschreiben lassen, zum Nachteil des traditionellen Polizeihandwerks festgestellt worden,[2111] sodass stets eine Integration von erfahrungsbasierter Polizeiarbeit und ihrem technisch-wissenschaftlichen Überbau angestrebt werden sollte, um eine Separierung beider Fachkulturen zu verhindern und so synergetische Potenziale ungenutzt zu lassen.[2112]

Diese neuen technischen Fertigkeiten erfordern zudem teilweise entsprechende organisatorische Einbettungen. So muss vor allem bei automatisierten Verknüpfungs- und Analyseverfahren auch durch eine entsprechende Organisation der Prozesse gesichert sein, dass weiterhin eine menschliche Bewertung am Ende von Auswertungsverfahren steht.[2113] Ferner müssen die Polizeien als Organisationen lernen, damit umzugehen, dass die Wissensbasis, auf der sie ihr Handeln aufbauen, zwar breiter, aber dadurch mitunter unschärfer und auch fehleranfälliger wird, was durch eine Organisations-

2107 Interview 1, Pos. 122 ff., 131.
2108 So *Egbert/Leese,* Criminal futures, S. 102.
2109 Interview 10, Pos. 56.
2110 Interview 12, Pos. 47.
2111 Vgl. etwa *Willis*, Improving police: What's craft got to do with it?, https://www.policefoundation.org/publication/improving-police-whats-craft-got-to-do-with-it/ (Stand: 01.10.2023); vgl. auch *Brayne,* Predict and surveil, S. 75, die in diesem Kontext die generelle Hierarchisierung und Machtasymmetrie von Polizeimanagement und den Polizei-"Arbeiter:innen" als organisationale Problemstelle sieht; zu den Problemen die sich aus abweichend spezialisierten Professionalitätskulturen ergeben können siehe etwa *Egbert/Leese,* Criminal futures, S. 81.
2112 *Willis/Mastrofski* Policing and Society 28 (2018), 27.
2113 Interview 4, Pos. 67; Interview 15, Pos. 94; siehe beispielhaft zu der organisationalen Umsetzung im Falle des ortsbezogenen Predictive Policing *Egbert/Leese,* Criminal futures, S. 109 ff.

struktur und -kultur aufgefangen werden muss, die Fehler eingestehen und mit ihnen operieren kann.[2114]

Allerdings ist eine Perspektive, die nur die inneren Abläufe der Polizei in den Blick nimmt, verkürzt, denn die Polizeien operieren in einem größeren informationstechnologischen Ökosystem. In diesem besteht eine zugespitzte Konkurrenzsituation mit der freien Wirtschaft beim Werben um qualifizierte Polizist:innen, die zu einem Verlust an Expertise in den Polizeiorganisationen führt:[2115]

> „Das hängt einfach damit zusammen, dass der Bedarf an Informatikern, an Ingenieuren und an Projektanten bundesweit extrem hoch gegangen ist. Wer alles überall über Informatiker verfügen will – das ist der Kampf um die guten Köpfe. Da muss die Polizei sich überlegen, wie sie dieses Fachwissen für die Polizei in der Breite verfügbar macht, aber auch, wie sie Spitzenleute gewinnt, in welcher Weise auch immer. Da sind neue Lösungen gefragt. Das ist nicht ganz trivial, diese Geschichte. Ansonsten würde das bedeuten, dass die Polizei ihre Fachkompetenz in der IT-Entwicklung aufgibt und an die Wirtschaft abgibt. Ob das gut ist, sei mal dahingestellt."[2116]

So wird dann auch berichtet, dass die hauseigene Technologie-Entwicklung zurückgefahren wird und es stattdessen je nach Bedarf zu einer Einbindung externer Expertise über private Unternehmen,[2117] etwa bei KI-Anwendungen,[2118] kommt. Zwar wird auch der Polizei eine solide Technologiekenntnis zugeschrieben,[2119] allerdings kann diese Expertise teilweise nur über Beschäftigung von nicht-verbeamteten Mitarbeiter:innen hergestellt werden,[2120] die lediglich lose an die Polizeien gebunden sind. Die Einbindung von privaten Unternehmen kann zwar risikoärmer sein, weil die Verantwortung für die Finalisierung des Projekts ausgelagert wird. Hauptgrund für eine Auslagerung sind jedoch häufig die faktischen Gegebenheiten:

2114 Interview 6, Pos. 52, 54 zum Umgang der Polizei mit nicht optimaler Datengrundlage im Bereich des ortsbasierten Predictive Policing für Fälle des Wohnungseinbruchsdiebstahls siehe *Egbert/Leese,* Criminal futures, S. 81.

2115 Interview 4, Pos. 38; Interview 14, Pos. 106, siehe auch *Egbert/Leese,* Criminal futures, S. 49.

2116 Interview 6, Pos. 46.

2117 Interview 2, Pos. 128.

2118 Interview 11, Pos. 15.

2119 Interview 4, Pos. 73.

2120 Interview 4, Pos. 23.

> „Ich sehe das in München, die haben das Problem. Weil da irgendeine große Firma wieder aufgemacht hat, die alles an Informatikern aufkaufen kann mit hervorragenden Stellen und Jahresgehältern, bei denen der öffentliche Dienst in keinem Maße mithalten kann. Da bist du dann manchmal gar nicht mehr in der Lage, selbst zu entscheiden, sondern kannst nur noch in Form solcher Werksverträge arbeiten, weil es sonst perspektivisch nicht durchzuhalten ist. Geld lässt sich immer auftreiben, aber Personal auszubilden, zu halten, zu motivieren und die Leute glücklich zu machen, in jeglicher Hinsicht, das ist dann schon ein deutlich schwierigeres Thema."[2121]

Daneben zwingen auch die teils enormen Aufwände, die technologische Neuerungen verursachen können, die Polizeiorganisationen häufig dazu, Projekte auszulagern. Das vorhandene Personal reicht gerade so aus, um von Externen gelieferte Technologien zu testen.[2122] Mit diesen Kooperationen erhöhen sich die Vulnerabilitäten der Polizeien, weil mitunter sensible Daten durch Private verarbeitet werden.[2123]

Dass sich diese Tendenzen des gegenwärtigen Zustandes kurz- und mittelfristig verstärken, erscheint nicht unwahrscheinlich: Die Aufwände zur Anpassung an die technologische Entwicklung nehmen zu, sodass die polizeilichen Organisationen hier „einigermaßen intelligente Lösungen" finden müssen, um mitzuhalten.[2124] Inwiefern sie das aus eigener Kraft schaffen werden, wird sich zeigen. Gut vorstellbar ist vor dem Hintergrund der beschriebenen Probleme bei der organisatorischen Integration informationstechnologischer Expertise allerdings, dass den Polizeien ihre eigene technische Expertise zunehmend erodiert und dann nur schwerlich wieder aufgebaut werden kann. Die Folge könnte eine abnehmende Fähigkeit sein, das polizeiliche Informationssystem durch organisationsinterne Impulse zu kontrollieren und zu steuern, was wiederum ein rein staatlich gesteuertes polizeiliches Kontrollsystem ein stückweit verhindern würde.[2125]

Trotz dieser Kooperationen mit privaten Unternehmen bleibt die Reaktion der Polizeien als Organisationen auf den digitalen Wandel aufgrund ihrer Größe, der Interdisziplinarität der Informationstechnologie und

2121 Interview 6, Pos. 48.
2122 Interview 14, Pos. 96.
2123 Interview 9, Pos. 12.
2124 Interview 6, Pos. 28.
2125 Siehe dazu *Heinrich,* Innere Sicherheit und neue Informations- und Kommunikationstechnologien, S. 380 f.

der wenig flexiblen rechtlichen Vorgaben zudem weiterhin eher träge,[2126] was ein Befund für polizeiliche Organisationen im Allgemeinen zu sein scheint.[2127]

XIII. Das mosaikhafte Gesamtbild des polizeilichen Informationswesens

Das auf Grundlage der Interviewstudie rekonstruierte, mosaikhafte Gesamtbild der Polizei ist eines, das eine Institution unter Spannung zeigt. Die Polizei ist eine Organisation, die – wie der Rest der Gesellschaft – „beständig ins Bodenlose fällt"[2128] und sich nur durch ständige interne wie externe Koordinationsleistungen Halt verschaffen kann. Die Polizeien erscheinen insofern fragil und müssen stets versuchen, Dysfunktionalitäten in ihrer Informationsverarbeitung vorzubeugen, indem stetig mitlaufende Anpassungsleistungen zwischen den verschiedenen Aspekten des polizeilichen Informationswesens erbracht werden. Die gesellschaftsstrukturellen Umwälzungen, die durch die Möglichkeiten der Produktion und Nutzung von Massendaten ausgelöst wurden und werden, fordern die Polizei auf rechtlicher, technischer und organisationaler Ebene heraus und legen an bestimmten Punkten Bruchstellen frei.

Diese Herausforderungen führen die Polizeiorganisationen in ständige Prozesse des Wandels und der Anpassung, um Potenziale als auch Risiken der Massendatenverarbeitung zu adressieren. Prioritäten sind dabei die Weiterentwicklung der technologischen Infrastruktur des polizeilichen Informationswesens, die Erhöhung der informationstechnologischen Expertise und Datenliterarität bei den Polizeibeamt:innen sowie der Ausbau von Massendatenverarbeitungsverfahren – alles bei gleichzeitiger Einhaltung der rechtlichen Rahmenbedingungen bzw. Bemühung um eine adaptive Reform des Rechts, damit die Realitäten der polizeilichen Informationsver-

2126 Interview 12, Pos. 45.

2127 Vgl. etwa aus dem angloamerikanischen Diskurs *Braga/Weisburd* in Weisburd/Braga (Hrsg.), Police Innovation, 544.

2128 Die Metapher des Bodenlosen stammt in ihrem gesellschaftlichen Bezug in dieser Form von *Luhmann,* Die Gesellschaft der Gesellschaft, S. 998; die konkrete Formulierung an dieser Stelle findet sich bei *Vesting*, Kein Anfang und kein Ende, https://www.jura.uni-frankfurt.de/43748222/kein-anfang-und-kein-ende.pdf (Stand: 01.10.2023).

arbeitung besser mit den normativen Steuerungsvorgaben verzahnt werden können.[2129]

Das polizeiliche Informationswesen hat sich im Rahmen der Befragung als voraussetzungsvolles, schwer zu steuerndes System gezeigt. Gleichzeitig hat es gemeinsam mit dem informationellen Polizeihandeln, das vom Informationswesen ermöglicht wird, einen großen Einfluss auf das Verhältnis der Polizei zur Gesellschaft, das rechtlich durch knapp 40 Jahre (Verfassungs-)Rechtsprechung und Gesetzgebung (meist in dieser kausal bedingten Reihenfolge) seiner Bedeutung entsprechend fein austariert worden ist. Die gegenwärtige Evolution informationstechnologischer Möglichkeiten verändert dieses komplexe Interaktionsverhältnis zwischen Polizei und Gesellschaft auf nachhaltige Weise, weil sich die Art und Weise der Wahrnehmung der Wirklichkeit und anschließenden Produktion von handlungsleitendem Wissen durch die Polizei verändert. Polizei und (Informations-)Technologie stehen dabei in einem komplexen Wechselwirkungsverhältnis, in dem sich beide gegenseitig beeinflussen und formen. Neben den Interaktionsverhältnissen mit der Gesellschaft rekonfigurieren die informationstechnologischen Neuerungen zugleich die organisationalen Arrangements, polizeilichen Arbeitsalltage[2130] und – wenn auch in schwächerer Weise – auch das Institutionengefüge, in dem – trotz unbestrittenem Fortbestand des Föderalismus – zentralisierende Effekte etwa durch das Projekt Polizei 2020 auftreten. Ähnlich ist dies auch für die regionale Verteilung organisatorischer Macht innerhalb der Länderpolizeien zu konstatieren.

Wie bereits *Ericson und Haggerty* vor mehr als 20 Jahren gezeigt haben, deuten auch Beobachtungen in den Interviews darauf hin, dass das Berufsbild der Polizist:innen sich weiter in Richtung von Wissensarbeit[2131] verschiebt.[2132] Das gilt nicht nur für hochspezialisierte Cyberkrimminalitätsexpert:innen, die wie beschrieben mithilfe von KI-Verfahren digitalen Mustern nachspüren, sondern durch die zunehmende Anreicherung des polizeilichen Arbeitsumfeldes mit Informationstechnologie auch für weniger spezialisierte Beamt:innen, die aus den zur Verfügung stehenden

2129 Ähnlich auch *Egbert/Leese,* Criminal futures, S. 11.
2130 *Egbert/Leese,* Criminal futures, S. 44.
2131 Grundlegend zum Konzept der "knowledge work" *Drucker* Modern Office Procedures 24 (1979), 12; siehe auch *Blackler* Organization Studies 16 (1995), 1021; *Pyöriä* Journal of Knowledge Management 9 (2005), 116.
2132 *Ericson/Haggerty,* Policing the risk society.

Daten Sinn für ihre Arbeit ableiten müssen. Neben der Qualifizierung für entsprechende Informationspraktiken müssen in diesen mit Informationen saturierten Arbeitswelten auch schädliche Effekte durch zu viel neue Information oder zu häufige Aktualisierung derselben verhindert werden.[2133] Eine starke informationstechnologische Vernetzung der Polizist:innen scheint aber bereits zu bestehen und wird wohl vor dem Hintergrund gegenwärtiger Entwicklungstendenzen in Zukunft weiter zunehmen. Ob eine stärkere Interaktion der Beamt:innen mit digitalen Informationssystemen sich nachteilig auf den Polizeikontakt von Bürger:innen auswirken wird und welche Effekte dies für das generelle Verhältnis der Polizei zur Gesellschaft mit sich bringen könnte, sind dabei offene, aber unbedingt weiter zu erforschende Fragestellungen.[2134] Ebenso bleibt fraglich, inwieweit das zunehmende Stützen von Entscheidungsprozessen auf digitale Daten das Erfahrungswissen des traditionellen Polizeihandwerks devaluieren wird.[2135] Die (scheinbare) Rationalität von datengestützten Erkenntnis- und Entscheidungsprozessen führt jedenfalls eher zu einer Aufwertung der höheren Führungsebenen. In einer häufig als „managerialism" bezeichneten Entwicklung wird zunehmend eine Tendenz zu Rationalisierung und Optimierung der zur Verfügung stehenden Ressourcen beobachtet.[2136] In diesem Kontext wurde etwa eine stärkere von oben erfolgende Kontrolle des Verhaltens von Streifenbeamt:innen in Bezug auf die Umsetzung von Predictive Policing-Analysen beschrieben.[2137]

Die Vernetzung des polizeilichen Informationswesens bis hin zur Streife oder zum Tatort fügt sich zudem in die Vision von einer Polizei ein, die immer näher an der zeitlichen Grenze operiert, an der sich Zukunftsmöglichkeiten als Gegenwart realisieren. Hinstrebend zum Ideal echtzeitlicher Reaktionsfähigkeit wird zusätzlich dazu das polizeiliche Wahrnehmungsfeld – etwa durch OSINT-Verfahren – ausgeweitet und die Informationsverarbeitung beschleunigt. Abweichendes Verhalten wird in dieser Idealvor-

2133 *Egbert/Leese,* Criminal futures, S. 89, 103 f., 123.

2134 *Mastrofski/Willis* Crime and Justice 39 (2010), 55 (89): „Over time systematic observation of police can tell us the extent to which street-level officers, like the general public, are investing more time in their computer screens and less in face-to-face contact with people. Perhaps more important, these studies can tell us how such a trend is affecting the way the police and public conceive the police mission and how decision making is altered.".

2135 *Brayne,* Predict and surveil, S. 78.

2136 *Egbert/Leese,* Criminal futures, S. 3.

2137 *Egbert/Leese,* Criminal futures, S. 153.

stellung schnellstmöglich registriert und von einer nahtlosen polizeilichen Gegenreaktion aufgefangen.[2138] Echtzeit bedeutet allerdings regelmäßig ein Operieren auf (sehr) unsicherer Tatsachengrundlage, was „durch das Versprechen der Aktualität des Echtzeitbetriebs systematisch verdeckt wird."[2139] Aber auch abseits dieses Strebens nach echtzeitlicher Kriminalitätskontrolle, die eher mit der Algorithmisierung der Polizei in enger Verbindung steht, kann man bereits der Ausweitung des polizeilichen Wahrnehmungsfelds mit Blick auf die polizeiliche Sozialkontrolle Bedeutung zumessen, da über die Vervielfältigung der Schnittstellen des polizeilichen Informationswesens eine breitere informationelle Erfassung von (abweichendem) Verhalten möglich wird. Nimmt man die Leistungssteigerungen der Datenverarbeitungsprozesse hinzu, entsteht so zunehmend eine sozio-technische Struktur, die in größerem Umfang als bisher Informationen über soziale Konflikte ins Hellfeld trägt, wo sie dann auch effektiver polizeilich bearbeitet werden können.

Auch die konkreten Instrumente der datafizierten Polizei treiben die Ausweitung des polizeilichen Wissens voran. Derartige Expansionen beschreiben etwa *Egbert und Leese* für das (raumbezogene) Predictive Policing hinsichtlich der Reichweite der Maßnahme, also etwa welche Kriminalitätsformen davon erfasst werden,[2140] hinsichtlich der Daten, das heißt es werden mehr Daten aus verschiedenen Datenquellen erfasst,[2141] hinsichtlich der Funktionalitäten, also etwa neue Analysefunktionalitäten[2142] oder Darstellungsweisen, sowie hinsichtlich der technischen Architektur.[2143] Diese strukturellen und funktionalen Expansionsdynamiken sind dabei nichts Neues für informationstechnologische Überwachungs- und Kontrollinstrumente. In der kritischen Sicherheits- und Überwachungsforschung wird

2138 *D. Wilson* SS 17 (2019), 69; bzgl. der dazu ebenfalls wichtigen Integration von OSINT-Daten siehe auch *Mackey/Courtney* in Bain (Hrsg.), Law Enforcement and Technology, 27 (31).

2139 *Burkhardt,* Digitale Datenbanken, S. 247.

2140 Etwa neben Wohnungseinbruchsdiebstahl auch Ladendiebstahl, Raub, Handtaschendiebstahl, Sachbeschädigung, KFZ-Diebstahl bzw. Diebstahl aus KFZ sowie Sexualstraftaten.

2141 Etwa soziodemografische Daten, Wetterdaten oder Daten über Mobilitätsinfrastruktur.

2142 Etwa die Analyse von Freitext-Feldern, die es in den polizeilichen Informationssystemen an verschiedenen Stellen gibt.

2143 Siehe dazu *Egbert/Leese,* Criminal futures, S. 214 ff.

generell von „surveillance“[2144] oder „function creep“[2145] gesprochen. Dass diese Dynamiken etwa auch im Rahmen der automatisierten Datenanalyse Wirkungen entfalten werden, erscheint insofern recht wahrscheinlich, zumal die breite Analyse von Datenaggregationen zu polizeilichen Informationszwecken gerade emblematisch für die Arbeit der datafizierten Polizei ist. Auch wurden diese Ausweitungstendenzen bereits von *Brayne* für den US-amerikanischen Kontext für Palantir Gotham – die auch hessenDATA zugrundeliegende Software – beschrieben.[2146] Solche extensiven Tendenzen sollten indessen nicht überraschen, da sie strukturell durch positive Rückkopplungsschleifen in den technologischen Logiken angelegt sind: Mehr Daten ermöglichen bessere Datenverarbeitungsinstrumente, die wiederum mehr Daten brauchen und dadurch wieder qualitativ verbessert werden können und so weiter. Insofern ist *Andrejevic und Gates* zuzustimmen, wenn sie schreiben: „The point is that so-called „function creep" is not ancillary to the data collection process, it is built into it—the function is the creep."[2147] Das führt letztlich zu dem prononcierten Spannungsverhältnis des gegenwärtigen polizeilichen Datenschutzschutzrechts – mit seinen normativen Postulaten der Datenminimierung und -sparsamkeit – und den Informationspraktiken einer datafizierten Polizei.

Aus einer Globalperspektive präsentiert sich das polizeiliche Informationswesen als sozio-technisches Großsystem. Die Sozialität dieses Systems ist zweifacher Natur. Einerseits ist das System in seinem Kern auf eine soziale Komponente, also seine Bedienung durch Polizeibeamt:innen angewiesen. Die Interaktion von Menschen mit dem technischen System dient als Kondensationspunkt, an dem datenförmig vorgehaltene Information in handlungsleitendes Wissen umgewandelt werden kann. Andererseits ist das polizeiliche Informationswesen auf Sozialität in Form von zunehmenden Schnittstellen mit den sozialen Prozessen der Gesellschaft angewiesen. Ohne als Daten aufbereitete Informationen über die soziale Lebenswelt wäre das Informationswesen nur eine leere technische Infrastruktur, die ihre Funktionslogik nicht erfüllen könnte und dadurch überflüssig würde. Die Expansion des polizeilichen Informationswesens bzw. seine zunehmende Durchdringung der Gesellschaft entwickelt sich zu einer eigenwilligen Rationalität, die von internen und externen Kontrollbemühungen nur noch

2144 *Marx,* Undercover, S. 2.
2145 *Andrejevic/Gates* SS 12 (2014), 185 (189).
2146 *Brayne,* Predict and surveil, S. 37 ff.
2147 *Andrejevic/Gates* SS 12 (2014), 185 (189).

bedingt eingehegt werden kann. Stattdessen kommt es zunehmend zu einer Selbststeuerung des Funktionssystems Polizei oder konkreter: des polizeilichen Informationswesens. Aufgrund des wachsenden Umfangs wird das sozio-technische System komplexer, vielschichtiger und damit für Steuerungsversuche sowohl von gesetzgeberischer als auch behördeninterner Seite schwerer zu erfassen und zu lenken. Mit dieser Lösung von politischen und insbesondere auch rechtlichen Vorgaben droht also zunehmend die immer weniger zu kontrollierende Verselbstständigung eines sozio-technischen Systems, dessen Hauptfunktion in der Ausübung von sozialer Kontrolle und Produktion von sozialer Ordnung liegt. Das Bedrohungspotenzial, das diesem Apparat innewohnt ist dabei nicht in erster Linie das eines hochtechnisierten, polizeilichen Überwachungsstaats oder -apparats, sondern die inkrementelle und schleichende Erfassung pluralistischer gesellschaftlicher Felder und die damit verbundene Schaffung von Anknüpfungspunkten für eine – wie dann auch immer genau modulierte[2148] – polizeiliche Sozialkontrolle. Dabei wären die Wirkungen der dadurch angestoßenen Ordnungsproduktionen immer weniger zu kontrollieren, was auch die dortig praktizierten Lebensweisen und die für sie zentralen Freiheitspraktiken einem kaum demokratisch legitimierten Anpassungsdruck unterwerfen könnte.[2149] Auf diese Weise – das haben schon *Steinmüller et al.* in ihrem wegweisenden Datenschutz-Gutachten 1971 festgestellt – treten entsprechende freiheitsbeschränkende Effekte ein,

> „ohne daß auch nur im geringsten die Verwaltung oder einer ihrer Beamten entfernt totalitäre Absichten hätte! Das System als solches entfaltet diese Wirkungen (werden sie nicht durch geeignete Maßnahmen verhindert), die der Beobachter von außen nicht von den Auswirkungen totalitärer Systeme unterscheiden kann."[2150]

Aber auch eine solche Globalperspektive auf das sozio-technische Großsystem des polizeilichen Informationswesens ist weiterhin mit erheblichen Schattierungen und blinden Flecken konfrontiert. Wer welche Systeme ganz konkret in welcher Funktion nutzt lässt sich gegenwärtig kaum näher

2148 Siehe dazu bereits oben S. 87 ff.

2149 Dieser Abschnitt lehnt sich an die insofern sehr instruktiven und weitsichtigen Überlegungen bei *Heinrich,* Innere Sicherheit und neue Informations- und Kommunikationstechnologien, S. 376 ff. an.

2150 *W. Steinmüller/Lutterbeck/Mallmann* ua, Grundfragen des Datenschutzes, Gutachten im Auftrag des Bundesministeriums des Innern, BT-Drs. 6/3826, 1971, S. 88.

bestimmen,[2151] was einerseits daran liegt, dass viele Aspekte des Informationswesens als Verschlusssache eingestuft sind und andererseits noch immer eine zu große Heterogenität zwischen den Ländern und anscheinend auch innerhalb der Länder besteht.[2152] „Die" Polizei ist somit voll von nicht erforschter (technologischer und handlungspraktischer) Heterogenität, was allerdings auch eine wissenschaftliche Chance sein kann, indem verschiedene Grade der Adaption von Technologie in den unterschiedlichen Polizeiorganisationen auf ihre je unterschiedliche Wirkung hin untersucht werden können.[2153]

2151 So auch *Arzt* in *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch des Polizeirechts, G. Rn. 1129.

2152 Ähnlich auch *Brayne,* Predict and surveil, S. 33 für den US-amerikanischen Kontext.

2153 So auch *Brayne,* Predict and surveil, S. 8, für die noch fragmentiertere informationstechnologische Infrastruktur der US-amerikanischen Polizei.

Kapitel V. Zukünfte der Polizei: Zwischen einer Polizei der Zukünfte und einer Zukunft ohne Polizei

Wie sich im Rahmen der bisherigen Untersuchung gezeigt hat, ist die Polizei als zentrale Akteurin der formellen Sozialkontrolle aufs Engste mit dem informationstechnologischen Wandel verwoben. Der Grad und die Weise ihrer organisationalen und technischen Adaption an die Dynamiken und Logiken des Massendatenparadigmas wird maßgeblich mit über ihre weitere Entwicklung als Institution bestimmen. Damit wird ihr technologischer Entwicklungsgrad von zentralem Einfluss darauf sein, welche Rolle die Polizei in Deutschland im gesamtgesellschaftlichen Gefüge einnehmen wird und inwiefern sie in diesem Kontext soziale Kontrolle ausüben kann.

Dabei sind der Modus der Produktion sozialer Ordnung und die Ausübung sozialer Kontrolle in einer Gesellschaft keine schlichten Funktionen technologischer Möglichkeiten, sie sind, mit anderen Worten, nicht technologisch determiniert. So ist Massenüberwachung keinesfalls das „natürliche" oder zwangsläufige Ergebnis der gesellschaftlichen Massendatenproduktion und -verarbeitung, sondern eine Entwicklung die durch – intentionale wie nicht-intentionale – menschliche Handlungen und Entscheidungen aus den unterschiedlichen gesellschaftlichen Feldern beeinflusst wird, die mit dem Massendatenphänomen verschränkt sind. Getragen werden diese Aktivitäten immer von wertegeleiteten Annahmen, wie man etwa an der zutiefst normativen Natur der Verknüpfung von Risikozuschreibungen mit massendatenbasierten Korrelationen ablesen kann. So heißt es bei *Završnik* zutreffend: „[A]scribing weight to past correlations in the form of oscillating between the past and present is an inherently political/value-based process."[2154] Aber nicht nur die Zuschreibung von Risiken wird im sicherheitspolitischen Diskurs unter dem Eindruck verschiedener Prämissen, Zielvorstellungen oder Zweckmäßigkeitserwägungen verhandelt. Vielmehr steht das ganze polizeiliche Informationswesen mit seinen unterschiedlichen technischen Ausprägungen in einer diskursiven Sphäre, in der Wechselwirkungen zwischen den spezifischen sozialen, kulturellen, politischen und wirtschaftlichen Zwängen einer Gesellschaft darüber entscheiden, ob

2154 *Završnik* in Završnik (Hrsg.), Big Data, Crime, and Social Control, 3 (13).

und inwiefern bestimmte Technologien sich im gesellschaftlichen Geflecht entfalten können.[2155] Soll es umfassende biometrische Gesichtserkennung zu Fahndungszwecken oder intelligente Videoüberwachung zur Identifizierung gefährlichen Verhaltens geben? Soll die Polizei unter Nutzung privater Datensammlungen einen umfassenderen Datenbestand zur Verhinderung von Kriminalität errichten können? Sollen polizeiliche Daten umfassend durch erkenntnisversprechende Datenverarbeitungsverfahren ausgewertet werden dürfen, um die polizeiliche Aufgabenerfüllung insgesamt zu effektivieren? Solche und weitere Fragen liegen den gesellschaftlichen Aushandlungsprozessen rund um das polizeiliche Informationswesen zugrunde.

Soll das polizeiliche Informationswesen, der Modus polizeilicher Informationsverarbeitung und damit auch die polizeiliche Sozialkontrolle gesellschaftlich regulierbar bleiben, erscheint zunächst nicht in erster Linie relevant, *wie* man Fragen wie die vorstehenden konkret beantwortet. Vielmehr – dem gleichsam vorgelagert – kann man die Frage stellen, ob technologische Entwicklungen von etwas, also von einem Faktor, beeinflusst werden können, der die disparaten und miteinander in manchmal unüberschaubarer Weise interagierenden Einflussgrößen von gesellschaftlicher Technologie-Entwicklung durchdringt, formiert und steuert. Vor dem Hintergrund der dargestellten Heterogenität und Komplexität des polizeilichen Informationswesens scheint es zunächst schwierig, klare Verlaufslinien oder sogar eine konzeptuelle übergeordnete Einflussgröße zu identifizieren, mit denen sich Entwicklungstendenzen dieses sozio-technischen Großsystems aufzeigen lassen.[2156]

Gegen die theoretische Sprachlosigkeit, die in diesen Schwierigkeiten bis zu einem gewissen Grad zum Ausdruck kommt, wenden sich *Jasanoff und Kim* mit ihrem Konzept der „sociotechnical imaginaries".[2157] Die Idee von sozio-technischen Imaginationen steht auf dem theoretischen Fundament des Menschen als narrativem Wesen. Eines oder sogar das wesentliche Alleinstellungsmerkmal ist danach die Fähigkeit, Narrative gesellschaftlich zu stabilisieren und über die so etablierten kollektiven Vorstellungsbilder gesellschaftliche Prozesse steuerbar zu machen.[2158] An diesen Gedanken

2155 *Završnik* in Završnik (Hrsg.), Big Data, Crime, and Social Control, 3 (18).
2156 In diese Richtung etwa *Heinrich,* Innere Sicherheit und neue Informations- und Kommunikationstechnologien, S. 378.
2157 *Jasanoff/Kim* (Hrsg.), Dreamscapes of modernity.
2158 Siehe dazu etwa *Paumier Jones* The Georgia Review 50 (1996), 649; *Gottschall,* The storytelling animal; stark popularisiert auch durch *Harari,* Sapiens.

anknüpfend gehen *Jasanoff und Kim* davon aus, dass technologische Entwicklungen von impliziten Vorstellungen darüber durchdrungen sind, was in der sozialen Welt wünschenswert ist, und „collective visions of the good society" in die soziale Struktur einschreiben.[2159] Damit verbunden sind zwei weitere Überlegungen: Erstens beeinflussen kollektive Werte, die sich gesellschaftlich entsprechend durchsetzen können, die Gestaltung technologischer Systeme. Und zweitens lassen sich an technologischen Projekten normative Entscheidungen hinsichtlich sozialer Ordnung ablesen, worüber spezifische Vorstellungen einer Gesellschaft sichtbar werden können.[2160] Sozio-technische Imaginationen spielen also bei gesellschaftsbeeinflussenden Technologieprojekten, wozu auch der Ausbau des polizeilichen Informationswesens gehört, eine zentrale Rolle: Einerseits stellen sie Leitsterne für die am technologischen Fortschritt beteiligten gesellschaftlichen Systemen dar, nach denen sich die Koordinierung und Mobilisierung von Ressourcen zur Umsetzung der Imagination ausrichten kann. Andererseits reflektieren sozio-technischen Imaginationen gesellschaftliche Selbststeuerungsimpulse, Richtungsentscheidungen und Ordnungswünsche. So wird der sozio-technische Wandel und sein Wertefundament sichtbar, kritisierbar und mit imaginativen Gegendarstellungen kontrastierbar.

Aufbauend auf dem Konzept der sozio-technischen Imaginationen sollen die herausgearbeiteten Entwicklungstendenzen des polizeilichen Informationswesens daher zu möglichen Zukunftsszenarien verdichtet werden. Damit soll der werteabhängige Verlauf des informationstechnologischen Wandels bei den deutschen Polizeien und dessen Auswirkungen auf die polizeiliche Sozialkontrolle greifbarer gemacht werden. Nach einer näheren Aufschlüsselung des Konzepts der sozio-technischen Imaginationen (A.) und einigen Bemerkungen zum Szenarien-Design (B.), sollen sodann aus den gegenwärtigen Wandlungsprozessen, wie sie sich insbesondere in den Expert:inneninterviews ausmachen ließen, zwei Szenarien destilliert werden (C. und D.). Beides sind Zukünfte, die von der Warte der grundgesetzlich verfassten Gesellschaft nicht zu befürworten sind. Orientiert wird sich dabei an der Szenarienerstellung von *Gerhold und Brandes*, die dasselbe bereits für Sicherheitstechnologien und ihre Wirkung auf den gesamten Sektor der öffentlichen Sicherheit und damit auch auf das gesellschaftliche

2159 *Jasanoff/Kim* Minerva 47 (2009), 119 (123).
2160 *Chateau/Devine-Wright/Wills* Energy Research & Social Science 80 (2021) (3).

Leben instruktiv vorgemacht haben.[2161] Allerdings sind die hier vorgestellten sozio-technischen Zukünfte gegenüber den Szenarien von *Gerhold und Brandes* zweifach enger gefasst: Es geht erstens nur um einen Ausschnitt des Sektors der öffentlichen Sicherheit und zweitens nur um eine bestimmte – wenn auch fundamentale – Auswirkung auf das gesellschaftliche Leben, die soziale Kontrolle. Kontrastiert werden beide Szenarien sodann mit einem positiven Entwurf für eine weitere Entwicklung des polizeilichen Informationswesens unter dem Eindruck des Massendatenphänomens (E.).

Insgesamt sind die folgenden Ausführungen auch als Synthese der Erkenntnisse und Ergebnisse der Arbeit zu lesen. Die Potenzialität, die aus der Methode des Szenariendesigns spricht, d.h. die vielgestaltigen Möglichkeiten der weiteren Entwicklung polizeilicher Sozialkontrolle, ist dabei eine Folge ihrer multikausalen Bedingtheit. Hier nur eine einzige, definitive Version des Wandels polizeilicher Sozialkontrolle auf der Grundlage der Vorarbeiten zu entwerfen würde sich in unredlicher Weise vor den unterschiedlichen aufscheinenden Entwicklungspfaden verschließen. Gleichzeitig ist das Szenariendesign aber keine exakte Wissenschaft, sodass im Folgenden auch nicht alle denkbaren Wechselwirkungsverhältnis durchgespielt wurden. Gerade mit Blick auf den qualitativen Aspekt der vorliegenden Untersuchung fügt sich der qualitative Charakter des Szenariendesigns aber in die Vorarbeiten ein. Das gilt umso mehr, als dass die weitere Entwicklung des polizeilichen Informationswesens vor allem auch von menschlichen Entscheidungen abhängt und nicht nach naturwissenschaftlichen Gesetzmäßigkeiten verläuft. Insofern geht es auch nicht um die Akkuratheit der Szenarien im Sinne einer möglichst zutreffenden Vorhersage, sondern um das Aufzeigen von in gegenwärtige Entscheidungen mit einzubeziehende Entwicklungsmöglichkeiten:

> „Whether or not a given hypothesized future will actually manifest is not the essential matter. Rather, the aim is to shed light on possible development paths in order to facilitate present-day decisions that will lay the groundwork for a desired future to occur."[2162]

2161 *Gerhold/Brandes* Eur J Futures Res 9 (2021), wobei auch bei ihnen die Polizei eine zentrale Rolle einnimmt. Interessanterweise sind einige Überlegungen zur Polizei im Rahmen des von ihnen als Rückschritt betrachteten Szenarios schon gegenwärtige Polizeipraxis.

2162 *Gerhold/Brandes* Eur J Futures Res 9 (2021) (2).

Das gilt umso mehr, als technologische Entwicklungen stets auch unbeabsichtigte Nebeneffekte zeitigen können, die in der modernen Gesellschaft, die sich vor allem durch komplexe Wechselwirkungsverhältnisse auszeichnet, nur schwer nachzuvollziehen sind. Einmal eingeführt sind Technologien aber beharrend.[2163] Daraus ergibt sich eine prekäre Situation für die Regulierung von risikobehafteten Technologien: Die tatsächlichen Wirkungen technologischer Innovationen zeigen sich erst, wenn sie in die soziale Struktur eingewoben sind, aber die dann wirkenden Beharrungskräfte machen es erforderlich, möglichst zuvor schon problembehaftete Aspekte der Technologie regulativ zu adressieren.[2164] Auf Grundlage des positiven sozio-technischen Zukunftsszenarios sollen abschließend Regulierungspfade aufgezeigt werden (F.).

A. Sozio-technische Imaginationen der (Spät-)Moderne

Sozio-technische Imaginationen entstammen, wie das bereits erwähnte Konzept der Sozio-Technizität technologischer Artefakte, den Science & Technology Studies.[2165] Während die Idee der Sozio-Technizität vor allem darauf abzielt, die soziale Bedingtheit von Technologien, also auch ihre Nicht-Determiniertheit, zu ergründen, beschäftigen sich die Science & Technology Studies auch mit der umgekehrten Perspektive, das heißt, wie Technologien auf das soziale Gefüge in all seinen Ausprägungen zurückwirken können. Dabei erteilt diese wissenschaftliche Strömung der Idee eines einseitigen Beeinflussungsverhältnisses eine Absage.[2166] Vielmehr hat sich mit dem Konzept der Koproduktion („co-production") die Idee eines gegenseitigen, hin-und-herschaukelnden Wechselwirkungsverhältnisses entwickelt. Technologien bedingen sozialen Wandel, aber sozialer Wandel bedingt umgekehrt auch die technologische Entwicklungen.[2167] Oder in den Worten *Jasanoffs*:

2163 Das gilt *Bailey/Barley* Information and Organization 30 (2020) zufolge insb. für "intelligente" Informationstechnologien; siehe dazu auch *Collingridge,* The social control of technology, 47 ff.

2164 *Lutz,* Das Ende des Technikdeterminismus und die Folgen: soziologische Technikforschung vor neuen Aufgaben und neuen Problemen, S. 38 f.

2165 Siehe dazu bereits oben S. 68 f.

2166 *Jasanoff* in Jasanoff/Kim (Hrsg.), Dreamscapes of modernity, 1 (2).

2167 *Gerhold/Brandes* Eur J Futures Res 9 (2021) (1).

> „Briefly stated, co-production is shorthand for the proposition that the ways in which we know and represent the world (both nature and society) are inseparable from the ways in which we choose to live in it. Knowledge and its material embodiments are at once products of social work and constitutive of forms of social life; society cannot function without knowledge any more than knowledge can exist without appropriate social supports. Scientific knowledge, in particular, is not a transcendent mirror of reality. It both embeds and is embedded in social practices, identities, norms, conventions, discourses, instruments, and institutions – In short, in all the building blocks of what we term the social. The same can be said even more forcefully of technology."[2168]

Allerdings lässt sich mit dem Konzept der Koproduktion mehr verstehen als erklären. Warum es etwa zur Ausformung spezifischer technologischer Entwicklungen bei ähnlichen sozialen Bedingungen kommt, lässt sich damit nur begrenzt beleuchten.[2169] Diese theoretische Sprachlosigkeit konzeptuell zu überwinden versucht die Idee der sozio-technische Imagination. Ursprünglich für die nationalstaatliche Ebene entwickelt,[2170] hat sich das Konzept davon mittlerweile gelöst und lässt sich durch eine variablere gesellschaftliche Verortung – auf kleinere Kollektive oder sogar Individuen – erkenntnisgewinnbringender als theoretische Ressource nutzen. So können mehrere Imaginationen innerhalb einer Gesellschaft koexistieren, sowohl in Spannung als auch in einem produktiven Verhältnis zueinander. Ob oder inwiefern sich derartige Imaginationen zukünftiger technologischer Konfigurationen gegenüber anderen durchsetzen, hängt vor allem von gesellschaftlichen Machtverhältnissen ab. So obliegt es oft dem Gesetzgeber, den Gerichten, den Medien oder anderen Institutionen mit gesellschaftlicher Macht, bestimmte Zukunftsvorstellungen über andere zu stellen und sie so im politischen Prozess voranzubringen. Insofern kommen *Jasanoff und Kim* zu folgender Definition sozio-technischer Imaginationen:

> „Taking these complexities into account, we redefne sociotechnical imaginaries in this book as collectively held, institutionally stabilized, and publicly performed visions of desirable futures, animated by shared un-

2168 *Jasanoff* (Hrsg.), States of knowledge, 2 f.
2169 *Jasanoff* in Jasanoff/Kim (Hrsg.), Dreamscapes of modernity, 1 (3)
2170 *Jasanoff/Kim* Minerva 47 (2009), 119.

derstandings of forms of social life and social order attainable through, and supportive of, advances in science and technology"[2171]

Besondere Betonung erfährt dabei das Wort „desirable", weil Projekte, die sozio-technische Zukünfte verwirklichen wollen, regelmäßig auf Visionen aufbauen, die sozialen Fortschritt technologisch erreichen wollen. Damit ist – auf der Kehrseite – stets auch das Gegenteil, also unerwünschte Zukünfte, Teil von sozio-technischen Imaginationen, als Angst vor den gesellschaftlichen Folgen, die bei Durchführung des technologischen Innovationsprozesses eintreten oder aber beim Unterlassen der Innovation. Sozio-technische Imaginationen oszillieren also zwischen den Utopien technologischer Verheißungen und den Dystopien technologischer Abgründe.[2172]

Während sozio-technische Imaginationen häufig auf einzelne als visionär angesehene Personen zurückgehen, brauchen sie den intersubjektiven Halt vieler Mitglieder einer sozialen Gemeinschaft, um in der gesellschaftlichen Struktur wirksam werden zu können.[2173] So war etwa *Horst Herold* als Visionär eines kybernetischen Informationswesens der Polizei zur Steuerung gesellschaftlicher Prozesse im Zusammenhang mit Devianz zwar der Anstoß für viele Projekte der Elektronisierung innerhalb der deutschen Polizei in den 1970er Jahren. Dabei war er jedoch stark auf eine verbreitete Technikeuphorie im polizeilich-sicherheitspolitischen Feld angewiesen, wie sie generell bezeichnend für das sozialliberale Fortschrittsjahrzehnt und den historischen Endpunkt der *trente glorieuses* war. *Herolds* visionäre Kraft verblasste und verlor ihre Wirkkraft dann auch im Angesicht des heraufziehenden Datenschutz-Paradigmas und der Ablehnung eines zu sehr zentralisierten polizeilichen Informationswesens, was sich in einer sozio-technischen Imagination verdichtete, in deren Zentrum die gesellschaftliche Angst vor einem zu mächtigen polizeilichen Überwachungs- und Kontrollapparat stand.[2174]

Dieses Beispiel zeigt auch, dass sozio-technische Imaginationen ein gesellschaftliches Handlungsfeld (geworden) sind, in dem verschiedene Akteur:innen – mal mehr, mal weniger intentional – über die Vorzüge und Nachteile konkreter Vorstellungen verhandeln. Individuen und Kollektive stecken auf diese Weise Gebiete in großen sozio-technischen Möglichkeits-

2171 *Jasanoff* in Jasanoff/Kim (Hrsg.), Dreamscapes of modernity, 1 (4).
2172 *Jasanoff* in Jasanoff/Kim (Hrsg.), Dreamscapes of modernity, 1 (4 f.).
2173 *Jasanoff* in Jasanoff/Kim (Hrsg.), Dreamscapes of modernity, 1 (6).
2174 Siehe zu dieser Entwicklung bereits oben S. 130 f.

räumen ab und schaffen damit handlungsleitende Pfadabhängigkeiten.[2175] So wird etwa im sicherheitspolitischen Diskurs von Seiten der Befürworter:innen die Einführung bestimmter technologischer Strukturen zur Terrorismusbekämpfung gefordert, wobei die Angst vor einer technologischen Rückständigkeit der Polizei und der davon ausgehenden Gefahr für die dann vor Terror ungeschützte Gesellschaft als sozio-technische Imagination katalysierend auf Entscheidungsträger:innen wirkt. Umgekehrt bringen Kritiker:innen dagegen die Angst vor einem polizeilich gestützten Überwachungsstaat und vor der Erosion bürgerlicher Freiheiten als Folge technischer Aufrüstung der Sicherheitsbehörden in Stellung.

Der Möglichkeitsraum sozio-technischer Imaginationen ist dabei äußerst weit, aber wohl auch in großen Teilen unsichtbar. Denn die Blicke der Gesellschaft für das, was möglich ist, sind durch die eingeübte soziale Ordnung – bei einigen mehr als bei anderen – konditioniert. Soziale Ordnung ist auf einer grundlegenden Ebene nichts anderes als eine kulturell konditionierte Wahrnehmung der Realität.[2176] Eine Durchbrechung dieser Konditionierung durch neue Vorstellungen davon, was ist und sein sollte, kann also eine soziale Umordnung bewirken – sowohl mit positiven als auch mit negativen gesellschaftlichen Auswirkungen.[2177] Insofern sind sozio-technische Imaginationen auch immer mit der Frage nach gesellschaftlicher Macht verbunden.[2178] Die Imaginationen konkurrieren um eine Hegemonialstellung, auch wenn in der technischen Materialisierung eines Projekts verschiedene gegenläufige Vorstellungen wirksam werden können. Kompromisse zwischen Effektivierung und Begrenzung polizeilicher Sozialkontrolle werden etwa an der datenschutzrechtlichen Sicherung im Rahmen der Einführung neuer Technologien bei der Polizei sichtbar. Technologische Innovationsprojekte sind insofern aber immer ideologisch und politisch.[2179]

Der politische Diskurs verlangt dafür, dass eine Imagination überhaupt anschlussfähig werden und bleiben kann, eine kontinuierliche Anstrengung von Befürworter:innen, mittels derer sich das sozio-technische Imaginativ stabilisieren und in technischen und anderen sozialen Strukturen ein-

2175 *Jasanoff* in Jasanoff/Kim (Hrsg.), Dreamscapes of modernity, 1 (8).
2176 *Jasanoff* in Jasanoff/Kim (Hrsg.), Dreamscapes of modernity, 1 (14).
2177 Dabei wäre natürlich die Perspektive, aus der die Bewertung „positiv" und „negativ" vorgenommen wird, näher zu charakterisieren. Hier geht es jedoch nur um die abstrakte Ebene dieser Dynamik.
2178 *Jasanoff* in Jasanoff/Kim (Hrsg.), Dreamscapes of modernity, 1 (18).
2179 *Jasanoff* in Jasanoff/Kim (Hrsg.), Dreamscapes of modernity, 1 (19).

schreiben kann, worüber dann auch wiederum gesellschaftliche Ordnungs gestützt werden können: „An imaginary is neither cause nor effect in a conventional sense but rather a continually rearticulated awareness of order in social life […] and a resulting commitment to that order's coherence and continuity."[2180]

Wie bereits eben angedeutet, spiegelt sich diese sozio-technisch beeinflusste Ordnung in besonderer Weise im Recht, wo die jeweiligen Praktiken und Ordnungsentwürfe unterschiedlicher sozio-technischer Imaginationen aufeinanderprallen. Hier ist es dann an den Richter:innen und Gesetzgebern, auf Grundlage der vorgebrachten Argumente die hegemoniale Stellung bestimmter Vorstellungen auszubauen oder zu schwächen.[2181] Für den vorliegenden Kontext dürfte das Volkszählungsurteil als Grundsatzentscheidung in der Frage nach dem Ausmaß eines datengestützten staatlichen Steuerungsanspruches gelten. Im Urteil stärkten die Richter:innen Ende 1983 eine sozio-technische Imagination, die in der unbeherrschten Datenverarbeitung durch moderne Informationstechnik ein unkalkulierbares Risiko für eine freiheitliche Gesellschaft sah. Verdichtet wurde diese unerwünschte Vorstellung im Bild des informationell selbstbestimmten Individuums, das seither Grundstein für die sich entfaltenden Datenschutzdogmatik ist, welche die Imagination rechtlich operationalisiert und ihr damit gesellschaftliche Wirksamkeit verleihen möchte. Immer wieder wurden aber seitdem auch sicherheitspolitische Technologieprojekte der konkurrierenden Imagination vorgebracht. In der als zunehmend unübersichtlich und ordnungslos wahrgenommenen Gesellschaft der Spätmoderne soll eine Expansion der polizeilichen Datenverarbeitungsfähigkeiten und -kompetenzen die polizeiliche Handlungsfähigkeit und damit die Produktion sozialer Ordnung durch die Polizei aufrechterhalten. Die vielen verfassungsrechtlichen Auseinandersetzungen über den Stellenwert der jeweiligen Imagination haben das Ideal informationeller Selbstbestimmung mittlerweile stark relativiert und das polizeiliche Datenschutzrecht ausgehöhlt. Hat der Datenschutz auch neuen Auftrieb durch die EU-Datenschutzreform von 2016 erfahren, so bleibt die Ausgestaltung des Verhältnisses beider Imaginationen ein „Kampf ums Recht".[2182] Dabei kann aber gerade die Konkurrenz zweier Imaginationen die Schaffung neuer Vorstellungen stimulieren.[2183]

2180 *Jasanoff* in Jasanoff/Kim (Hrsg.), Dreamscapes of modernity, 1 (26).
2181 *Jasanoff* in Jasanoff/Kim (Hrsg.), Dreamscapes of modernity, 1 (26).
2182 *Jhering,* Der Kampf ums Recht.
2183 *Jasanoff* in Jasanoff/Kim (Hrsg.), Dreamscapes of modernity, 321 (337).

Sozio-technische Imaginationen der Ausgestaltung polizeilicher Sozialkontrolle im Zeitalter der Massendaten bleiben insofern ein Vehikel für die Neugestaltung und Neukalibrierung der gesellschaftlichen und menschlichen Zukunft.[2184] Eine Analyse der sozio-technischen Imaginationen ermöglicht insofern eine tiefgreifende Reflexion über die Perspektiven einer Gesellschaft auf ihre Zukunft und auch über dabei bestehende blinden Flecken. Damit sollte – im besten Fall – das schöpferische Potenzial des Technologie-Einsatzes im Namen der Gesellschaft freigelegt und eingängig betrachtet werden, um die sozio-technische Machbarkeit vielfältiger gesellschaftlicher Welten sicht- und praktizierbar zu machen.[2185]

B. Szenarien-Design

Bevor die benannten Szenarien breiter dargestellt werden, muss noch über das Szenarien-Design, das eine Methode der Zukunftsforschung ist, gesprochen werden. Wie bereits erwähnt, wird für die folgenden Entwicklungspfade der Polizei als Institution der formellen Sozialkontrolle eine Arbeit von *Gerhold und Brandes* als Ausgangspunkt genommen.[2186] Deren Szenarien-Entwicklung für die Zukunft des Technologie-Einsatzes im öffentlichen Sicherheitssektor in den nächsten 10 bis 15 Jahren und die daraus folgenden Auswirkungen für das gesellschaftliche Leben haben bereits zwei kondensierte Verlaufspfade hervorgebracht. Da die Polizei als wichtigste einzelne Institution im Feld öffentlicher Sicherheit gelten dürfte, weisen beide Szenarien bereits eine hohe Dichte an Überlegungen und fundierten Spekulationen, gewissermaßen „educated guesses", auch zur Polizei auf. Mit den in der vorliegenden Studie herausgearbeiteten theoretischen, rechtswissenschaftlichen und empirischen Aspekten sollen die von *Gerhold und Brandes* konstruierten Entwicklungslinien der Polizei ergänzt oder aber auch korrigiert werden. Vor allem die qualitative Natur der Szenarien-Methode ermöglicht eine Zusammenführung mit den erarbeiteten Erkenntnissen der Interviewstudie.

Das Konstruieren von Szenarien zielt dabei zunächst einmal darauf ab, Elemente, die als einflussreich für zukünftige Entwicklungen identifiziert worden sind, im Rahmen eines systemischen Vorgehens in konsistente,

2184 *Jasanoff* in Jasanoff/Kim (Hrsg.), Dreamscapes of modernity, 1 (27).
2185 *Jasanoff* in Jasanoff/Kim (Hrsg.), Dreamscapes of modernity, 321 (339).
2186 *Gerhold/Brandes* Eur J Futures Res 9 (2021).

plausible und leicht zugängliche Bilder möglicher Zukünfte zu übersetzen.[2187] Szenarien sind also „logical, plausible and realistic situations based on today's knowledge, therefore giving an approximate idea of how the future may look."[2188] Ob eine solche Zukunft tatsächlich eintritt, ist hingegen immer ungewiss,[2189] sodass im Folgenden auch keine Aussagen über die Wahrscheinlichkeit des einen oder anderen Szenarios getroffen werden. Wie bei *Gerhold und Brandes* ist das Ziel der Szenarien-Entwicklung greifbare Bilder der Zukunft zu entwerfen, „which allows the reflection of current debates about security technologies and can inform which actions in the present are best-suited to bringing about desired future states."[2190] Insofern wird der Wert der Szenarien vorliegend vor allem auch in der Unterstützung beim Finden einer sinnvollen Regulierungsrichtung für das polizeiliche Informationswesen gesehen.

Für die Konstruktion der Szenarien werden in erster Linie die gegenwärtigen technologischen Entwicklungen im polizeilichen Informationswesen herangezogen. Eine zentrale Rolle spielt dabei aber nicht nur die eingesetzte oder auch nicht eingesetzte Technik an sich, sondern auch der organisatorische Umgang der Polizei mit technologischen Innovationen und den Herausforderungen, die sich daraus für die Institution und das polizeiliche Arbeitsfeld stellen. Daneben ist vor allem der rechtliche Rahmen relevant, da normative Rahmenbedingungen Technikentwicklung anleiten, konkret also begrenzen oder freisetzen können. Inwiefern die Polizei in ihren Aufgaben und Befugnissen durch das Recht eingehegt ist, wird eine zentrale Stellschraube für die Form ihrer weiteren informationellen Technisierung sein.[2191] In Bezug auf den bereits begonnenen oder geplanten Technologie-Einsatz sollen explizit auch unerwünschte, nicht bezweckte Effekte der informationstechnologischen Evolution[2192] bei den Polizeien miteinbezogen werden, auch wenn deren Identifizierung sich sachgemäß als schwierig ge-

2187 So *Gerhold/Brandes* Eur J Futures Res 9 (2021) (7); siehe auch *K. Steinmüller* in Popp (Hrsg.), Zukunft und Wissenschaft, 101; *Lindgren/Bandhold,* Scenario planning.

2188 *Gerhold/Brandes* Eur J Futures Res 9 (2021) (4).

2189 *Gerhold/K. Steinmüller* in Peperhove/K. Steinmüller/Dienel (Hrsg.), Envisioning Uncertain Futures, 69 (71).

2190 *Gerhold/Brandes* Eur J Futures Res 9 (2021) (4); siehe auch *Grishakova/Gramigna/Sorokin* Frontiers of Narrative Studies 5 (2019), 112; *Neuhaus* in Gerhold/Holtmannspötter/Neuhaus ua (Hrsg.), Standards und Gütekriterien der Zukunftsforschung, 21.

2191 Ähnlich *Gerhold/Brandes* Eur J Futures Res 9 (2021) (6).

2192 *Rammert,* Technik - Handeln - Wissen, 109 et passim.

staltet.[2193] Allerdings müssen auch Technologie-Entwicklung und -Einsatz in der Gesellschaft sozialer Kontrolle unterworfen werden und bleiben,[2194] sodass der verantwortungsbewusste Umgang mit Technik eine möglichst frühzeitige Reflexion über Technikfolgen erforderlich macht.[2195]

Auch bei ausgeprägten Bemühungen um eine möglichst anschlussfähige intersubjektive Objektivität bleibt beim Szenarien-Design, das vorliegend im Sinne seiner qualitativen Ausprägung durchgeführt wird, die forschende, konstruierende Person in den konkreten Prognosen präsent. Wie auch im Rahmen der durchgeführten Interviews sind Entscheidungen während des Forschungsprozesses immer von einem Vorverständnis abhängig, das generell jedes wissenschaftliche Vorhaben – aber qualitative Studien in besonders expliziter Weise – durchdringt und beeinflusst. Diesem unüberwindbaren Fakt lässt sich nur mit Transparenz begegnen. Diese wurde einerseits bereits im Rahmen der Interviewstudie, die ja maßgeblich in die folgenden Szenarien einfließt, durch Offenlegung von Prozess und Reflexionen gewährleistet. Darüber hinaus wurde mit der Darlegung der Vorgehens bei der Konstruktion auch die Transparenz der Szenarien sichergestellt.[2196] Diese Transparenz stellt zwar keine Objektivität her, macht auch die vorgestellten Szenarien weder richtig, aber auch nicht falsch, sondern vor allem diskutabel, was ohnehin ihr eigentlicher Zweck ist. Sie sollen als Debattenimpuls und Diskussionsgrundlage dienen und gerade kritisiert werden. Die Unvollständigkeit und Kritisierbarkeit der Szenarien ist mithin eine ihrer zentralen und intendierten Eigenschaften:

> „While the scenarios we have described intend to enable negotiative processes, a scenario development approach can never be suitable for arriving at a final or conclusive assessment of a subject matter. In this way, far from seeking to adopt a specific polemic tact, we aim instead […] to provide impetus to debates about our collective future."[2197]

2193 *Gerhold/Brandes* Eur J Futures Res 9 (2021) (3).
2194 Grundlegend dazu *Collingridge,* The social control of technology.
2195 *Gerhold/Brandes* Eur J Futures Res 9 (2021) (3).
2196 Siehe zu den methodischen Reflexionen zu den referenzierten Szenarien *Gerhold/Brandes* Eur J Futures Res 9 (2021) (17).
2197 *Gerhold/Brandes* Eur J Futures Res 9 (2021) (17 f.).

C. Erstes Szenario: Die datenmächtige Polizei der Zukünfte

Das erste hier konstruierte Szenario ist das einer datenmächtigen Polizei, die über die Beherrschung der in den datenmäßigen Repräsentationen liegenden Unwägbarkeiten des prospektiven Realitätsverlaufs den Zufall „gezähmt" hat[2198] – oder das zumindest auf Grundlage einiger Anhaltspunkte für die Effektivitätssteigerung polizeilicher Sozialkontrolle glaubt.[2199] Dafür sind zwei Faktoren, die sich gegenseitig bedingen und durchdringen, also im erwähnten Sinne koproduzieren,[2200] ausschlaggebend: Die technische und organisatorische Bewältigung des Massendatenphänomens, womit auch die Anpassung der Bewältigungsleistungen ans Recht verbunden ist, sowie eine gesellschaftliche Sicherheitskultur,[2201] die der datenmächtigen Polizei im Wesentlichen befürwortend gegenüber steht. Als Sicherheitskultur wird hier in Anlehnung an *Daase* „die Summe der Überzeugungen, Werte und Praktiken von Institutionen und Individuen verstanden werden, die darüber entscheiden, was als eine Gefahr anzusehen ist und wie und mit welchen Mitteln dieser Gefahr begegnet werden soll" angesehen.[2202] Es besteht insofern ein recht enger Zusammenhang zwischen Sicherheitskultur und sozio-technischen Imaginationen.

I. Sicherheitskultur

Die Sicherheitskultur ist in diesem Entwicklungsverlauf vor allem durch das häufig beschriebene spätmoderne Unsicherheitsempfinden geprägt.[2203] Die pointiert von *Beck* beschriebene Bewusstwerdung der Gesellschaft über ihre vielfältigen Risiken[2204] hat – das ist mittlerweile hinlänglich beschrieben worden – einen sich selbst verstärkenden Kreislauf in Gang gesetzt, der technisch immer neue Risiken produziert oder auch entdeckt, um dann wiederum mit vor allem technischen Innovationen darauf zu reagieren,

2198 *Hacking,* The Taming of Chance.
2199 Dieses Szenario knüpft an das Szenario „To Be Ahead" von *Gerhold/Brandes* Eur J Futures Res 9 (2021) (8 ff.) an.
2200 Siehe dazu bereits oben S. 491.
2201 Zu diesem Konzept siehe *Gerhold/Brandes* Eur J Futures Res 9 (2021) (4); *Daase* Aus Politik und Zeitgeschichte 2010, 9.
2202 *Daase* Aus Politik und Zeitgeschichte 2010, 9 (9).
2203 Siehe dazu bereits Fn. 6.
2204 *Beck,* Risikogesellschaft.

was aufgrund technischer Risiken häufig wieder zum Beginn des Kreislaufs führt. Die dadurch entstandene Risikowahrnehmung wird dabei immer sensibler und weitet sich auf immer neue Risikophänomene aus – unter anderem auch auf alle möglichen Formen der Devianz.[2205] Der Modus der Sicherheitsproduktion wird zunehmend technisch[2206] und etabliert damit Stück für Stück technische Systeme mit dem Zweck der Überwachung und Kontrolle verschiedener Risiken.[2207] Getragen wird dieser gesellschaftliche Komplex von einer sozio-technischen Imagination der Beherrschbarkeit risikoreicher Zukünfte durch exzessiven und expansiven Technologie-Einsatz.[2208] Beabsichtigte Folge dieses sozio-technischen Sicherheitskomplexes, der seine zentrale staatliche Ausprägung im polizeilichen Informationswesen findet, ist also die zunehmende Sammlung von Daten – Informationen – über Risiken mit der Absicht, sie technisierten Überwachungs- und Kontroll- oder auch: Lösungsstrategien zuzuführen.

Diese Sicherheitskultur spiegelt sich auch im Modus, den die Gesellschaft zur rechtlichen Einhegung von neuen Sicherheitstechnologien an den Tag legt. *Gerhold und Brandes* gehen davon aus, dass Gesetzgeber und sonstige Regulierungsinstanzen nicht in der Lage sind, mit der Geschwindigkeit und Vielfalt der neuen technischen Regulationsobjekte Schritt zu halten.[2209] Schon jetzt sind solche Effekte in den Interviews zur Sprache gekommen. Fehlende oder fehlerhafte Gesetzgebungsaktivitäten erschweren die Tätigkeit der polizeilichen Datenschutzbeauftragten, was den Verselbstständigungstendenzen der informationstechnologischen Infrastruktur und der mit dieser interagierenden Informationspraktiken des polizeilichen Informationswesens Vorschub leistet. Fehlende Regelungskonzepte,[2210] ein nur unzureichend lernfähiges Recht[2211] sowie die Komplexität der bisherigen Rechtslage und föderale Ordnung der Regulierungsinstanzen verhindern in diesem Szenario eine konsistente und vor allem auch verfassungsgemäß einhegende Regulierung des polizeilichen Informationswesens, dass sich deshalb immer weiter aus seinem Regelungsrahmen löst. Die Gesetz-

2205 *Miller* in *Jasanoff/Kim* (Hrsg.), Dreamscapes of modernity, 277 (278 f.).
2206 *Gerhold/Brandes* Eur J Futures Res 9 (2021) (3), sprechen insoweit von einer "technization of security".
2207 *Miller* in Jasanoff/Kim (Hrsg.), Dreamscapes of modernity, 277 (278 f.)
2208 Ähnlich auch *Miller* in Jasanoff/Kim (Hrsg.), Dreamscapes of modernity, 277 (278); siehe auch *Gerhold/Brandes* Eur J Futures Res 9 (2021) (2).
2209 *Gerhold/Brandes* Eur J Futures Res 9 (2021) (8).
2210 *Bäcker,* A-Drs. 18(4)806 D, S. 2, 10.
2211 Zur Lernfähigkeit bereits *Roßnagel* Zeitschrift für Rechtspolitik 1991 (25), 55 (57); *Golla* Kriminologisches Journal 52 (2020), 149.

gebung beschränkt sich – wie schon jetzt teilweise zu konstatieren ist – zunehmend auf die reine Legitimierung polizeilicher Informationstechnologien und der damit einhergehenden Informationspraktiken. Kriminalitätsrisiken wird von der Sicherheitskultur aber ein größerer Stellenwert zugestanden als abstrakte Risiken für schleichende Freiheitsverluste.

II. Technologische Entwicklung des Informationswesens

Die Technisierung polizeilicher Sozialkontrolle wird von einer insofern affirmativen Sicherheitskultur getragen. Gleichzeitig wird diese Kultur kaum durch ein normatives Element der Zurückhaltung eingeschränkt, sodass die Grenzen des technisch Möglichen zunehmend die Grenzen des Faktischen im polizeilichen Informationswesens bestimmen.[2212]

Zunächst gelingt den deutschen Polizeien daher der im Rahmen des Projekts Polizei 2020 geplante Umbau des polizeilichen Informationswesens, was die Datenhaltung stark effektiviert. Daten müssen nun regelmäßig nur noch einmal erfasst werden und können dann über entsprechende Programmierungen an die Anwendungen, für die sie jeweils gebraucht werden, gesteuert werden. Die Schaffung eines zentralen Datenbestandes ermöglicht auch einen erkenntnisgewinnbringenderen Einsatz von algorithmengestützten Massendatenverarbeitungsverfahren. Im Zuge des Prozesses, der oben bereits als Datafizierung beschrieben wurde,[2213] meistern die deutschen Polizeien die „zunehmende Nutzung korrelativ fundierter, statistischer Datenanalysen […], [also] die auf Entscheidungsfindung ausgerichtete und algorithmisch vermittelte (Massen-)Analyse von Daten […], deren Resultate entsprechend umgesetzt werden und somit die polizeilichen Praktiken nachhaltig prägen."[2214] Dabei erhält das polizeiliche Informationswesen Unterstützung durch einen großen polizeilich-sicherheitswirtschaftlichen Komplex, der stetig neue Innovationen für verlässliche Abnehmer hervorbringt. Auf einer basalen Ebene effektivieren die verbesserte Datenhaltung und die steigende Kompetenz in der datengestützten Produktion von handlungsleitendem Wissen die polizeiliche Informations-

2212 Skeptisch hinsichtlich einer solchen polizeilichen Entwicklung etwa *Krahmer* in Rüdiger/Bayerl (Hrsg.), Digitale Polizeiarbeit, 215.

2213 Siehe dazu bereits oben S. 46 ff.

2214 *Egbert* in Hunold/Ruch (Hrsg.), Polizeiarbeit zwischen Praxishandeln und Rechtsordnung, 77 (78).

arbeit nachhaltig und eröffnen der polizeilichen Sozialkontrolle damit neue Potenziale.

Gleichzeitig vervielfältigen sich die Kontaktpunkte, die das polizeiliche Informationswesen mit gesellschaftlichen Feldern hat, indem mehr informationstechnische Schnittstellen geschaffen werden, über die lebensweltliche Daten über soziale Konflikte und abweichendes Verhalten direkt in die polizeilichen Datenbestände gelangen können.

Einerseits sind Smartphones alltägliches Einsatzgerät bei der datenmächtigen Polizei. Jeder Einsatz, ob mit vorrangig präventiver oder repressiver Stoßrichtung, wird umfassend und – nach Möglichkeit – granular erfasst und an die polizeilichen Informationssysteme übertragen, von wo dann eine automatisierte Weiterleitung an Stellen und Anwendungen erfolgt, an denen die Daten benötigt werden. Zudem nimmt der Einsatz von automatischen Kennzeichenlesesystemen, Bodycams – auch zu generellen Einsatzdokumentationszwecken – und anderen Formen mobiler und stationäre Videoüberwachung zu. Videoüberwachungssysteme dienen generell als Plattform für Software, etwa zur Verhaltenserkennung und biometrischen Identifikation, sodass sich die informationelle Durchdringung der von den Kameras erfassten Lebenswelt noch einmal erhöht.[2215]

Andererseits erlauben Online-Wachen es den Bürger:innen, über ihre (mobilen) Endgeräte wie Smartphones und Laptops direkt Informationen an die Polizei zu senden. Eine Weiterentwicklung dieser Kommunikationsart ermöglicht das Melden einer Straftat über einen speziellen Kanal, etwa über eine App, woraufhin die Polizei augenblicklich Einsatzkräfte entsenden kann, die sich zuvor über mitgesendete Daten beispielsweise in Form von Videos ein Vorabbild der Lage am Einsatzort machen können.[2216] Daneben werden in großem Maße OSINT-Verfahren und Online-Streifen durchgeführt, mit denen virtuelle Räume zum einen präventiv nach Auffälligkeiten durchsucht werden, zum anderen aber auch digitale Hinweise auf Devianz sowohl im Virtuellen als auch im Analogen registriert werden. Neben den allgemeinen Online-Wachen bestehen institutionalisierte Meldeverfahren für als besonders gesellschaftsschädlich geltendes abweichendes Verhalten im digitalen Raum – „Hate Speech"-Verdachtsfälle etwa werden nach Meldung automatisiert zur Auswertung an die dafür

2215 Es wird etwa bereits davon berichtet, dass Bodycams in einigen Ländern mit Gesichtserkennungssoftware ausgestattet werden, siehe dazu *Cheslow* Times of Israel v. 22. Januar 2022.

2216 *Gerhold/Brandes* Eur J Futures Res 9 (2021) (8 f.).

vorgesehene Stelle beim Bundeskriminalamt geleitet, wo Algorithmen die massendatenförmige Online-Kommunikation der Gesellschaft vorfiltern und dann an menschliche Bearbeiter:innen weiterleiten. In einem an dieser Stelle zugespitzten Szenario wäre auch das automatisierte Versenden von Strafbefehlen nach algorithmengestützter Entscheidung über die strafrechtliche Relevanz einer Äußerung ähnlich dem automatisierten Mahnverfahren denkbar.

Neben diesen Dynamiken, welche die Expansion der polizeieigenen Datensammlung betreffen, können die deutschen Polizeien auch zunehmend auf die in der Gesellschaft an anderer Stelle aggregierten Datenakkumulationen zugreifen. Einerseits sind staatliche Daten weitestgehend über einheitliche Datenformate harmonisiert und somit schnell je nach Bedarf austausch- und integrierbar. Daneben besteht zudem die Möglichkeit des bedarfsmäßigen Zugriffs auf die Bestände privater Akteure wie Social Media-Betreiber, Data Broker und sonstige Digitalunternehmen. Dieser Kontakt ist über Schnittstellen technisch verfestigt worden, sodass die Polizei gesellschaftliche Realitäten im Bedarfsfall über die kontextbezogene Integration verschiedener Datenquellen rekonstruieren und darüber Anzeichen für erwartetes oder bereits geschehenes abweichendes Verhalten identifizieren und entsprechend adressieren kann.[2217] In ähnlicher Weise können etwa Smart Home-Geräte und die sonstigen Sensoren der „Onlife"-Welt[2218] ausgewertet und vergangene Lebenssituationen auf diese Weise besser für Zwecke der Strafverfolgung rekonstruiert werden.

Neben diesen Tendenzen der Extensivierung und Effektivierung der technologischen Infrastruktur des polizeilichen Informationswesens verändert sich auch die Interaktion der Polizist:innen mit diesem sozio-technischen Großsystem fundamental. Vor allem anderen macht sich dies in der mobilen Verfügbarkeit der Datenmacht des Informationswesens in den verschiedenen Einsatzkonstellationen bemerkbar, die den Beamt:innen einen starken informationsbasierten Rückhalt und damit einen Wissensvorsprung vor ihrem Gegenüber gewährt. Wie eine solche Zukunft der engmaschigen Integration polizeilicher Einsätze in datenangereicherte Handlungsabläufe aussehen könnte, haben *Bain et al.* beschrieben:[2219]

2217 *Gerhold/Brandes* Eur J Futures Res 9 (2021) (10).

2218 Zum Begriff des „Onlife" bereits oben Fn. 1272.

2219 Siehe zum Folgenden *Bain/Carsone/Conser* ua in Bain (Hrsg.), Law Enforcement and Technology, 115 (126 ff.).

Zwei Polizeibeamt:innen werden zu einem Fall häuslicher Gewalt geschickt. Ein Sprachassistent gibt über einen auf der Schulter angebrachten Miniatur-Lautsprecher bisher bekannte Informationen zum Einsatzgeschehen durch, die Anfahrt wird durch die auf dem Fahrzeugbildschirm dargestellten GPS-Informationen geleitet. Das Kamerasystem des Fahrzeugs und die Bodycams werden automatisch zu Eigensicherungs- und Dokumentationszwecken aktiviert und ein Live-Video-Feed wird an die Einsatzleitzentrale übertragen. Vor Eintreffen am Einsatzort erfahren die Beamt:innen, dass ein offensichtlich betrunkener Ehemann seine Frau anschreit und bedroht, dass zwei kleine Kinder in der Wohnung leben, dass der Ehemann in der Vergangenheit wegen häuslicher Gewalt verhaftet wurde und dass eine weitere Einheit entsandt wird. Fotos von allen Bewohner:innen der Wohnung und Kennzeicheninformationen für die auf Ehemann und Ehefrau zugelassenen Fahrzeuge werden an den Computer des Streifenwagens gesendet. Sofort bei Ankunft am Ort des Geschehens scannt das Videosystem des Polizeifahrzeuges die Nummernschilder der vor dem Haus geparkten Fahrzeuge. Ein Fahrzeug gehört der Familie, ein weiteres vor dem Haus abgestelltes Fahrzeug ist auf eine andere Person zugelassen. Name und Bild dieser Person werden an den Bordcomputer des Streifenwagens gesendet. Die Beamt:innen steigen aus und schieben sich ihre Visiere über die Augen, woraufhin das in die Visiere integrierte Heads-up-Display aktiviert wird. Die Displays stellen den Beamt:innen die zuvor an den Bordcomputer gesendeten Informationen zu den Fahrzeugen bereit. Beide Polizist:innen nähern sich der Eingangstür, aus der gerade eine männliche Person auf die Veranda tritt. Auf Ansprache hin äußert der Mann, dass die Polizei nicht gebraucht werde, es sei nur ein herkömmlicher, mittlerweile geklärter Familienstreit gewesen. Die Bodycams tasten Gesicht und Augen der Person ab und übertragen die biometrischen Daten an das polizeiliche Informationswesen, wo sie verarbeitet werden. In Sekundenschnelle wird die Identität der männlichen Person mit einer Wahrscheinlichkeit von 95 % durch einen Datenbankabgleich festgestellt. Ein Bild der identifizierten männlichen Person wird an den Bordcomputer des Einsatzfahrzeugs gesendet und dann wieder an das Display der Visiere übertragen, wo sie das Ergebnis und die Wahrscheinlichkeitsschätzung sichtbar werden. Die Beamt:innen akzeptieren das Ergebnis als korrekt, es ist der Halter des familienfremden Fahrzeugs. Im Hintergrund werden weitere Daten abgeglichen, vorherige Polizeikontakte der Person werden gesucht. Währenddessen haben die Bodycams das Verhalten der familienfremden Person erfasst und analysiert. In der Ecke der polizeilichen Displays beginnt eine rote LED zu blinken. Zwei

Warnungen werden eingeblendet. Einerseits zeigt die Person eine Körpersprache, die auf einen bevorstehenden körperlichen Angriff schließen lässt. Zudem sei aufgrund unbewusster Gesichts- und Körperbewegungen zu erkennen, dass die Person wahrscheinlich lügt. Die Beamt:innen bitten die Person, auf die Straße zu gehen und mit den anderen Polizist:innen zu sprechen, die – worüber mittels des Schulterlautsprechers informiert wird – innerhalb weniger Sekunden eintreffen würden. Die Person leistet der Aufforderung folge, wird aber bei ihren Bewegungen von den Bodycams erfasst, sodass bei verdächtigem Verhalten wie dem Abweichen vom Kurs eine Alarmmeldung erfolgen kann. Während ein Beamter vor dem Haus verbleibt, betritt seine Kollegin die Wohnung und spricht mit dem Mann und der Frau. Während der Interaktion zwischen (mutmaßlichem) Täter und Opfer bleiben die am Körper getragenen Überwachungssysteme der Beamtin zur Beobachtung der Situation eingeschaltet. Der Ehemann wird wegen Körperverletzung festgenommen, noch am Ort werden Daten an zu beteiligende (staatliche) Stellen wie dem Jugendamt, dem Opferhilfebüro und dem zuständigen Gericht wegen eines Aufenthaltsverbots übertragen. Der festgenommene Ehemann wird vor Ort biometrisch vermessen und die Daten werden samt einer DNA-Probe an das polizeiliche Informationswesen übertragen. Ein eingesprochener Bericht wird automatisiert in Text umgewandelt und mit allen anderen Daten, die beim Einsatz angefallen sind, an das polizeiliche Vorgangsbearbeitungssystem übertragen, von wo die Daten dann an die entsprechenden Anwendungen gesteuert werden. Abschließend wenden sich die Beamt:innen noch an die Social-Media-Seite ihrer Polizeibehörde und informieren so die örtliche Gemeinschaft über den Vorfall und den Ausgang des Einsatzes.

Die anhand dieses hypothetischen Fallbeispiels beschriebenen Potenziale des polizeilichen Technologie-Einsatzes zeichnen sich vor allem durch die Eigenschaften der Kombination und Synergie aus. Die Möglichkeiten, die sich daraus ergeben, sind vielfältig und in ihren Kontrolleffekten tiefgehend. So ist etwa auch denkbar, dass über mobile Endgeräte flächendeckend über Apps auf die automatisierte Datenanalyse zugegriffen werden kann, womit die informationelle Macht der Polizei bei Kontakt mit Personen massiv gesteigert würde – die Implikationen werden bereits im geschilderten Beispiel deutlich: Ein Objekt – das familienfremde Fahrzeug – wird in seiner Verknüpfung zu einer Person angezeigt, über die wiederum Erkenntnisse zu vorheriger Delinquenz zur Verfügung gestellt werden können. Auch der Streifenwagen wird bei der datenmächtigen Polizei zu einer

Plattform für weitere Technologien: Die installierten Kameras könnten schlicht dauerhaft Kennzeichen lesen und bei Trefferfällen eine Benachrichtigung an die Besatzung des Wagens senden – samt entsprechend verfügbarer Datenverknüpfungen zum in Frage stehenden Kennzeichen bzw. Fahrzeug. *Brayne* beschreibt diesen Wandel von einer auf aktives Suchen und Identifizieren gerichteten hin zu einer von automatisierten Alarmen geleiteten Polizeiarbeit bereits konkret für das Los Angeles Police Department und sieht darin eine emblematische Entwicklung der massendatengestützen Polizeiarbeit.[2220]

Im Szenario der datenmächtigen Polizei verschränken sich also menschliches und maschinelles Wahrnehmen, zu einer Hybridform, was vor allem die Frage nach der menschlichen Handlungsmacht aufwirft. Was soll passieren, wenn die Verhaltenserkennung einen erheblichen Angriff detektiert? Denkbar wäre es, dass – wenn die angreifende Person auch auf Aufforderung nicht ablässt und weitere Gefahrenparameter überschritten werden – eine automatisierte Verteidigungshandlung von der insoweit „intelligenten" Ausrüstung der Beamt:innen ausgeführt wird, etwa in Form eines Elektroschocks oder Pfeffersprays. Die Bediensteten der datenmächtigen Polizei wären in einem solchen Fall keineswegs auch datenmächtige Polizist:innen, sondern vielmehr instrumentelle Ausformungen des sozio-technischen Informationswesens.[2221]

Mit der zumindest graduellen Übersteuerung des individuellen Polizist:innenverhaltens würde polizeiliches Handeln in der Breite zunehmend homogenisiert. Divergierende Interpretationen anlässlich des Verhaltens von Personen würden mehr und mehr einer durch technische Instrumente programmierten Reaktion auf abweichendes Verhalten weichen,[2222] wobei dies aufgrund der potenziellen Diskriminierungsanfälligkeit von algorithmengestützten (Massen-)Datenverarbeitungsverfahren nicht zwangsläufig einen Gerechtigkeitszuwachs bedeuten würde.

Allerdings schafft die Datafizierung mit ihrer Durchdringung des polizeilichen Arbeitsalltags auch neue Potenziale für eine öffentliche Kontrolle, etwa durch die Veröffentlichung von Videomaterial aus Polizeieinsätzen zur Ansicht durch die Bürger:innen. Auch die einsatzgestaltenden Entschei-

2220 *Brayne,* Predict and surveil, S. 45 f.
2221 *Bain/Carsone/Conser* ua in Bain (Hrsg.), Law Enforcement and Technology, 115 (121 f.).
2222 *Bain/Carsone/Conser* ua in Bain (Hrsg.), Law Enforcement and Technology, 115 (123).

dungen selbst sind durch die starke technische Rahmung detaillierter nachvollzieh- und damit überprüfbar.[2223] Allerdings setzt eine solche Kontrolle voraus, dass es noch einen hinreichend konkreten normativen Rahmen gibt, der ein solches Kontrollregime überhaupt fordert und der Kontrolle inhaltliche Anhaltspunkte liefert. Denkbar wäre vor allem eine organisatorische Absicherung der informationellen Maßnahmen der datenmächtigen Polizei durch human in the loop-Verfahren, um möglichst viele Fehlidentifizierungen und damit verbundene unrechtmäßige Persönlichkeitsbeeinträchtigungen zu vermeiden[2224] sowie um die Legitimität der technikgestützten Sozialkontrolle nicht allzu stark erodieren zu lassen.

III. Polizeiliche Sozialkontrolle

Die Datenmacht der Polizei übersetzt sich im hier beschriebenen Entwicklungspfad in eine gegenüber der heutigen Situation intensivierten Sozialkontrolle. Dabei wären die Wandlungsprozesse der polizeilichen Sozialkontrolle wohl nicht auf eine der vier oben beschriebenen Dynamiken (totaler oder umfassender, selektiver, sanfter, härter) beschränkt,[2225] da es nach wie vor sehr heterogene Kontexte gibt, in denen die Polizei über ihr Handeln soziale Ordnung wiederherstellt oder aufrechterhält.

Durch ihre verbesserten Fähigkeiten in Datengenerierung, Datenhaltung und Datenverarbeitung dürfte die polizeiliche Sozialkontrolle in erster Linie umfassender werden. Wenn durch das Anwachsen entsprechender Schnittstellen mehr Informationen über soziale Konflikte und abweichendes Verhalten in das polizeiliche Hellfeld gelangen, wo sie dann auch effektiver verarbeitet werden können, steigt die Zahl der bekanntgewordenen Fälle abweichenden Verhaltens sowie die entsprechende Verhinderung oder Sanktionierung dieses Verhaltens. Durch die generelle Anwendung von algorithmengestützten Massendatenverarbeitungsverfahren innerhalb der Polizei kann nach datenförmigen Mustern von Devianz in den informationellen Repräsentationen von lebensweltlichen Phänomenen gesucht werden. Sowohl retrospektiv als auch proaktiv können zunehmend Kriminalitätsmuster in den aus verschiedenen Quellen zusammengeführten Datensätzen identifiziert werden. Die Polizei wird damit in die Lage

2223 *Gerhold/Brandes* Eur J Futures Res 9 (2021) (11).
2224 *Gerhold/Brandes* Eur J Futures Res 9 (2021) (10).
2225 Siehe dazu bereits oben unter S. 87 ff.

versetzt, aggregiertes gesellschaftliches Verhalten auf Irregularitäten und Abweichungen hin zu untersuchen, Kriminalitätsursachen zu ergründen und – im „Idealfall" – neue Kriminalitätsphänomene bei ihrer Entstehung zu beobachten. Diese polizeiliche Form der Massendatenproduktion und -verarbeitung macht es quasi unmöglich, sich dauerhaft dem staatlichen Blick zu entziehen, da die Teilhabe an der Gesellschaft und ihren Einrichtungen das Hinterlassen digitaler Spuren erforderlich macht.[2226] Zwar gibt es weiterhin solche, die mit technologischen Mitteln ihrer Identifizierung und Dingfestmachung entgehen können, aufgrund der dafür erforderlichen Expertise trifft dies allerdings nur auf einen geringen Teil der Delinquenten und auf einen noch geringeren Teil der Gesamtgesellschaft zu. Vermisste Personen gehören der Vergangenheit an, gesuchte Personen werden zumeist umgehend verhaftet.[2227] Damit einher geht zudem eine ausgeweitete Zuständigkeit der Polizei für abweichendes Verhalten, da sie die entsprechenden technischen „Lösungen" dafür in Form des stark ausgeweiteten Informationswesens zur Hand hat.[2228] Die Polizei ist (weiterhin) der zentrale Knotenpunkt im Netzwerk staatlicher Sozialkontrolle. Insgesamt schwingt in dieser zunehmend umfassender werdenden Sozialkontrolle die implizite Grundphilosophie der uneingeschränkten Befürworter:innen des Massendatenparadigmas mit: Wenn nur genug Daten gesammelt sind, wird handlungsleitendes Wissen über bisher unverstandene oder gänzlich unbekannte gesellschaftliche Prozesse generiert werden können,[2229] was sich in eine sozio-technische Vision der datengestützten Steuerung und Neutralisierung von Verhaltensdivergenzen übersetzt. In der so imaginierten Gesellschaft wird es weiterhin bestimmte Kriminalitätsphänomene geben, diese sind aber durch massendatenbasierte Wissensproduktion und darauf aufbauende Kriminalitätskontrollmechanismen sehr viel stärker eingehegt als dies gegenwärtig der Fall ist.[2230] Aufgrund der Ubiquität von als Kriminalität etikettiertem abweichendem Verhalten in der Gesellschaft[2231] bedeutet die Ausweitung des polizeilichen Blickes zugleich die zunehmende Erfassung und datenförmige Repräsentation von Gesellschaftsmitgliedern in den poli-

2226 *Gerhold/Brandes* Eur J Futures Res 9 (2021) (9).
2227 *Gerhold/Brandes* Eur J Futures Res 9 (2021) (10).
2228 *Gerhold/Brandes* Eur J Futures Res 9 (2021) (9).
2229 *Mayer-Schönberger/Cukier,* Big Data; *Anderson*, The end of theory: The data deluge makes the scientific method obsolete.
2230 *Egbert/Leese,* Criminal futures, S. 56.
2231 *Farrall/Karstedt,* Respectable citizens - shady practices.

zeilichen und strafjustiziellen Informationssammlungen, wie es sich in den Vereinigten Staaten bereits abzeichnet.[2232]

Innerhalb dieser engmaschigen polizeilichen Sozialkontrolle wird die Polizei voraussichtlich – trotz affirmativer Sicherheitskultur – mit Ressourcenengpässen zu kämpfen haben, sodass eine Priorisierung des Ressourceneinsatzes nach wie vor geboten sein wird. Aufgrund der umfassenden Datenbasis des Informationswesens und der darauf aufbauenden leistungsstarken Algorithmen der massendatengestützten Wissensproduktion kann die Polizei allerdings im Wege des personen- und raumbezogenen Predictive Policing besonders gefährliche Individuen und Orte effektiver identifizieren und kontrollieren.[2233] Insofern wird die polizeiliche Sozialkontrolle gleichzeitig – und scheinbar paradoxerweise – totaler und selektiver. Erst durch eine Ausweitung des polizeilichen Hellfeldes, das heißt der für die Wissensproduktion benötigten Datenbasis, kann die Polizei jedoch überhaupt mit größerer Sicherheit Prognosen darüber treffen, ob eine Person oder ein Ort im Vergleich besonders gefährlich ist oder nicht. Die Selektivität massendatenvermittelter Sozialkontrolle durch die Polizei baut mithin auf einer umfassenderen Datenerfassung und -verarbeitung auf.[2234]

Zudem gibt es im Szenario der datenmächtigen Polizei auch Anhaltspunkte dafür, dass die ausgeübte polizeiliche Sozialkontrolle – zumindest auf den ersten Blick und in der Breite – sanfter werden könnte. Einerseits kann die Massendatenverarbeitung schon frühzeitig Muster gerade beginnender oder zu erwartender Kriminalität identifizieren, was der Polizei – etwa durch Gefährderansprachen und Ähnliches[2235] – ein gleichsam frühzeitiges, aber dafür weniger invasives Eingreifen und Gegensteuern ermöglicht, um entsprechende Kriminalitätsrisiken im Keim zu ersticken oder gar nicht erst aufkommen zu lassen. Zudem ermöglicht auch die Anreicherung der Lebenswelt mit Sensoren frühzeitige(re) oder echtzeitige Interventionen der Polizei in bevorstehenden oder akuten Gefahrensituationen, indem etwa visuelle Sensoren, also Kameras, verdächtiges Verhalten erkennen, softwarebasiert klassifizieren und dann Alarm auslösen können,[2236]

2232 Siehe dazu etwa *Brayne,* Predict and surveil, S. 2.

2233 *Gerhold/Brandes* Eur J Futures Res 9 (2021) (10).

2234 In diese Richtung für den gesamtgesellschaftlichen Zusammenhang auch *Chriss,* Social Control, S. 211 ff.

2235 Solche – nach deutscher Terminologie – Gefährderansprachen wurden beispielsweise im Rahmen der sogenannten Strategic Subject List („Heat List") in Chicago praktiziert, siehe dazu etwa *Ferguson,* The rise of big data policing, S. 37 ff.

2236 *Gerhold/Brandes* Eur J Futures Res 9 (2021) (10).

wodurch auch hier zunächst mit möglichst niedrigschwelligen Maßnahmen der Versuch einer Gefahrauflösung unternommen werden kann.

Allerdings ist bedenkenswert, ob die datenmächtige Polizei nicht auch punktuell Formen härterer Sozialkontrolle hervorbringt. Das ist in zweierlei Hinsicht möglich. Einerseits werden, wie beschrieben, im Rahmen der Selektivierung der massendatenbasierten Sozialkontrolle besonders gefährliche Personen und Orte identifiziert. Da es sich dabei um Individuen und Räume handelt, die – in der relativen Logik des Vergleichs der zur Verfügung stehenden Daten – als die nach jeweils aktuellem Kenntnisstand die *gefährlichsten* für die soziale Ordnung angesehen werden müssen, liegt es nahe, dass die polizeiliche Reaktion hier einigermaßen hart ausfällt, um das wahrgenommene Risiko möglichst effektiv zu eliminieren. Zwar ist damit noch nicht unbedingt eine unterwerfende Sozialkontrolle im Sinne *Beydouns*[2237] beschrieben. Andererseits ist, gewissermaßen an die Unterseite der sanften Sozialkontrolle angeheftet, eine Entwicklung denkbar, die sich gegenüber Teilen der Gesellschaft als strengere Sozialkontrolle äußert:

> „The control in this algorithmic world is not a control that guides you against some presumed, autonomous will. Instead it's a control that frames your world. It conditions the possibilities available for you to live your life as a user - as well as a member of a category."[2238]

In einer Gesellschaft, in der Teilhabe am Gemeinwesen über die Preisgabe von Daten vermittelt wird, in der die soziale Ordnung zunehmend über Algorithmen der Risikoidentifizierung und -kategorisierung hergestellt wird, werden diejenigen, die sich davor fürchten, dass ihr abweichendes und eventuell auch strafrechtlich relevantes Verhalten bekannt wird und zu Nachteilen für sie führt, weniger am gesellschaftlichen Leben teilhaben können.[2239] Die Massendatenüberwachung wirkt so gesamtgesellschaftlich gesehen negativ auf die ohnehin schon ungleiche Verteilung von Lebenschancen im Digitalzeitalter.[2240] Vermeidendes Verhalten und Verdrängungseffekte schaffen so eine Klasse von digital von der Gesellschaft Ausgegrenzten. Zugespitzt formuliert könnte man darin eine Form der digital vermit-

2237 Siehe dazu bereits oben unter S. 98 f.
2238 *Cheney-Lippold,* We are data, S. 148.
2239 *Haggerty/Ericson* Br J Sociol 51 (2000), 605 (619); *Brayne* Am Sociol Rev 79 (2014), 367.
2240 *Brayne,* Predict and surveil, S. 148.

telten Verbannung oder Internierung sprechen.[2241] Auch ist zu bedenken, dass eine Intensivierung der polizeilichen Sozialkontrolle die Polizei nicht zu einer Institution macht, die plötzlich die Ursachen von Kriminalität wirksam beheben kann. Zu erwarten bleibt vielmehr, dass auch die datenmächtige Polizei weiterhin nur die Konsequenzen sozialer Probleme in Form von Kriminalität und Unordnung bekämpft, ohne den Versuch zu unternehmen, Ihnen das Substrat zu entziehen und wirksame sozialpolitische Interventionen zu betreiben.[2242]

Insgesamt könnte diese gewandelte polizeiliche Sozialkontrolle auch über die beschriebenen Effekte hinaus gesamtgesellschaftliche und wohl ungewollte Nebenwirkungen auslösen. So meint *Moore*, „[i]f we reduced crime, but did so by relying on more intrusive investigative techniques, or patrol techniques that were both more assertive and viewed as biased, then the increased use of authority would have to be viewed as a loss to be put against the gain."[2243] Auch sind vor diesem Hintergrund sich aufschaukelnde Auswirkungen auf gesellschaftliche Interaktionen rund um die soziale Ordnung denkbar: Führt etwa eine als zu eng empfundene Sozialkontrolle zu einem zunehmenden Verlust der Legitimation der Polizei, könnte es als Reaktion auf diesen Legitimationsverlust zu stärkeren sozialen Unordnungsphänomenen kommen, die dann wiederum eine Intensivierung der (polizeilichen) Sozialkontrolle hervorrufen. Überhaupt wäre fraglich, was für eine Subjektkultur[2244] eine Gesellschaft ausformen würde, in der die Polizei in der beschriebene Art und Weise soziale Ordnung produziert. Während einerseits die umfassende Sozialkontrolle ein stark diszipliniertes, fremdgesteuertes und normbefolgendes Subjekt plausibel erschienen ließe, wie es noch recht typisch für die 1950er und 1960er Jahre war,[2245] ist mit Blick auf *Popitz* Konzept der Präventivwirkung des Nichtwissens[2246] auch die gegenteilige Tendenz denkbar. Dadurch, dass sich das Subjekt der vielfältigen gesellschaftlichen Normübertretungen gewahr wird, die aufgrund der engmaschigen polizeilichen Sozialkontrolle aufgedeckt sowie dann verhindert oder sanktioniert (oder beides) werden, normalisiert sich

2241 So etwa *Leman-Langlois* in Deflem (Hrsg.), The Handbook of Social Control, 347 (359); siehe genereller zu dieser Dynamik der Ausgrenzung auch *Singelnstein/Kunz,* Kriminologie, S. 407 ff.
2242 *Lyon* Big Data & Society 1 (2014), 1-13 (7).
2243 Mark H. Moore, zitiert nach *Brayne,* Predict and surveil, S. 143.
2244 Zum Begriff siehe etwa *Reckwitz,* Das hybride Subjekt.
2245 *Reckwitz,* Das Ende der Illusionen, S. 207 f.
2246 *Popitz,* Über die Präventivwirkung des Nichtwissens.

einerseits die gesellschaftliche (Straf-)Sanktion bis zu einem gewissen Grad und andererseits verblasst das Vertrauen des Subjekts in das gesellschaftliche Normsystem zunehmend. Die soziale Normordnung wäre also paradoxerweise geschwächt. Gleichzeitig wäre aber auch sozialer Wandel, der sich *Durkheim* zufolge im Wesentlichen über die Weiterentwicklung des Normbestandes durch Übertretung der Normen materialisiert, gehemmt.[2247]

D. Zweites Szenario: Die überforderte Polizei – Zukunft ohne Polizei

Das zweite Szenario konstruiert eine Zukunft, in der die Polizei weitgehend überfordert mit dem digitalen Wandel und den gesellschaftlichen Auswirkungen des Massendatenphänomens ist.[2248] Es ist, pointiert formuliert, eine Zukunft ohne Polizei, weniger zugespitzt könnte man auch sagen: mit einer in ihrer gesellschaftlichen Rolle stark herabgestuften Polizei. In diesem Szenario haben sich die gegenwärtigen Entwicklungspotenziale zu einer im Kern vor allem kritischen Sicherheitskultur in der Gesellschaft verdichtet. Die Polizei hat die technisch-organisatorische Anpassung an die neuen gesellschaftlichen und medialen Konfiguration nicht bewältigen können, was zu einer Verkümmerung der polizeilichen Sozialkontrolle in wichtigen Bereichen und einem institutionellen Bedeutungsverlust geführt hat.

I. Sicherheitskultur

Die bereits heute im Diskurs präsenten Datenschutz-Befürworter:innen sind tonangebend geworden. Bei den deutschen Polizeien ist es immer wieder zu unrechtmäßigen Datenverarbeitungen gekommen: Es wurden polizeiliche Daten zu privaten Zwecken abgerufen und im Rahmen von strafrechtlichen Ermittlungen wurden verbotene Datenverarbeitungsmethoden angewendet. Ohne dass zuvor Rechtsgrundlagen geschaffen worden waren, hatten einzelne Behörden zudem mit neuen, eingriffsintensiven Technologien experimentiert[2249] und damit in für die Betroffenen spürbarer Wei-

2247 *Durkheim* in Sack/König (Hrsg.), Kriminalsoziologie, 3 (7 f.).

2248 *Gerhold/Brandes* Eur J Futures Res 9 (2021) (8), nennen ihr Szenario "Turning back the clock", wobei nicht ganz klar wird, zu welchem Zustand hier zurückgekehrt wird.

2249 So ist es auch bei hessenDATA schon der Fall gewesen, siehe HessLT-Drs. 19/6864 Teil B, S. 6 f.

se Persönlichkeitsrechte verletzt. Die nunmehr hegemoniale Position im sicherheitspolitischen Diskurs befürwortet eine stärkere Begrenzung von Massendatenüberwachung.[2250] Dabei ist die Kriminalitätsfurcht nicht homogen niedrig ausgeprägt. Zwar gibt es diejenigen, die von der relativen Sicherheit der Gesellschaft ausgehen oder eine höhere Unsicherheitstoleranz aufweisen. Daneben sind aber auch Einstellungen vorhanden, die sich durch eine relativ hohe Kriminalitätsfurcht und damit auch durch ein ausgeprägtes Unsicherheitsempfinden auszeichnen. Allerdings wird der Polizei und den mit ihr im Strafjustizsystem verknüpften Instanzen der staatlichen Sozialkontrolle einerseits eine wirksame Kriminalitätsbekämpfung nicht zugetraut und andererseits wird ein zu extensives polizeiliches Informationswesen klar als zum Unsicherheitsempfinden beitragender Faktor angesehen, sodass entsprechenden Ausweitungstendenzen mit politischer Ablehnung und Kritik begegnet wird. Bezüglich des Einsatzes überwachender und kontrollierende Informationstechnologie durch die Polizei ist im gesellschaftlichen Diskurs eine kritisch-dystopische sozio-technische Imagination eines hochtechnisierten polizeilichen Kontrollapparats hegemonial und entfaltet als mahnende Vision einer zu stark überwachten Gesellschaft hemmende Wirkungen auf informationstechnologische Innovationen. Affirmative Positionen, wie sie im Szenario 1 vorherrschend sind, haben kaum Diskursmacht.

II. Technologische Entwicklung des Informationswesens

Die Technologisierung des polizeilichen Informationswesens hat massiv an Schwungkraft verloren und befindet sich an vielen Stellen in einer Sackgasse. Verglichen mit vergleichbaren Technologien des Privatsektors ist der technologische Standard der Polizei rückständig und gerät immer weiter ins Hintertreffen.

Ein zentrales Hindernis der informationstechnologischen Weiterentwicklung des polizeilichen Informationswesens ist die insofern blockierende rechtliche Struktur der Gesellschaft. Das liegt zum einen daran, dass grundrechtsinvasive Technologien vor ihrer Implementierung zunächst von unabhängigen Gutachter:innen eingehend geprüft werden müssen. Vor dem Einsatz müssen zudem noch umfassende Datenschutz-Folgenabschät-

2250 *Gerhold/Brandes* Eur J Futures Res 9 (2021) (8).

zungen durchgeführt werden. Der Prozess ist langwierig und kostspielig, was insgesamt zu einer Verlangsamung des Innovationstempos führt.[2251] Diese Vorgaben für den Technologie-Einsatz in der polizeilichen Informationsverarbeitung erschwert die Entwicklung und Einführung von Massendatenverarbeitungsverfahren sowohl durch den Privatsektor als auch durch die Polizei selbst. Eine polizeiliche Sicherheitsindustrie kann sich nicht in Deutschland etablieren.[2252] Hinzu kommt eine für die Polizeien selbst schwer zu überschauende Regelungslage, die gepaart mit strengster Aufsicht durch die Landes- und Bundesdatenschutzbeauftragten den organisatorischen Ressourcenaufwand so gesteigert hat, dass nur sehr ausgewählte und dringende informationstechnologische Entwicklungsprojekte betrieben werden.

Zudem haben sich auch die träge Organisationsstruktur und bestimmte Organisationskulturen als wandlungsresistenter erwiesen, als einmal angenommen. Die Fachkulturen zwischen Polizeipraxis, Informationstechnologie und Verwaltung, wozu auch der interne Datenschutz zu zählen ist, sind mit den Komplexitäten der Integration von Polizeipraxis, technischer Infrastruktur und rechtlichen Vorgaben zunehmend überfordert und finden keine gemeinsame Sprache. Die hauseigene Entwicklung von neuen technischen Verfahren versandet häufig und auch der Einkauf von Software scheitert an organisatorischen Koordinations- und Integrationsproblemen, etwa weil Projekt-Spezifikationen nicht passen, sodass die technische Infrastruktur immer weiter veraltet und laufend Dysfunktionalitäten produziert. Informatiker:innen und sonstiges technisches Personal wandert zunehmend in die Privatwirtschaft ab. Aufgrund der Mängel des Informationswesens wird die Verwendung von technischen Verfahren von einer überwiegenden Mehrheit der operativ arbeitenden Polizist:innen abgelehnt. Ohnehin bestehen starke Widerstände gegenüber der Digitalisierung und Datafizierung der Polizeiarbeit, da ein Verlust der organisationsinternen Macht zugunsten der Führungsebenen befürchtet wird.[2253] Das „traditionelle Polizeihandwerk" von Schutz- und Kriminalpolizei erfährt vor diesem Hintergrund eine Aufwertung gegenüber technisierten Formen der Polizeiarbeit.

2251 *Gerhold/Brandes* Eur J Futures Res 9 (2021) (8).
2252 *Gerhold/Brandes* Eur J Futures Res 9 (2021) (9).
2253 Siehe zu diesem Konflikt etwa *Vera/Jablonowski* in Stierle/Wehe/Siller (Hrsg.), Handbuch Polizeimanagement, 475; *Reuss-Ianni,* Two cultures of policing.

Das Projekt Polizei 2020 ist an der überbordenden Komplexität des heterogenen polizeilichen Informationswesens gescheitert. Es bestehen weiterhin Divergenzen zwischen den unterschiedlichen Länder- und Bundessystemen, Schnittstellen bleiben ein Problem. Datenübertragungen zu anderen Verwaltungszweigen sind ebenfalls nur bedingt möglich. Die informationstechnologische Infrastruktur erlaubt nur noch begrenzte Grundfunktionen wie den Datenaustausch, der aber – durch datenschutzrechtliche Vorgaben und technische Mängel bedingt – verlangsamt ist. Zudem übersteigt die Masse der Daten die Verarbeitungskapazitäten des Informationswesens und „verschmutzt" die Datenspeicher. Datenabfragen produzieren nur noch begrenzt handlungsleitendes Wissen, da häufig zu viele widersprüchliche und falsche Daten in den Datenbanken abgelegt worden sind. Erkenntnisgewinnbringende Daten sind knapp. Daten sind, mit anderen Worten, zum Problem geworden.[2254] Einigen Länderpolizeien gelingt es besser als anderen die Funktionalitäten ihrer eigenen Systeme aufrechtzuerhalten, aber generell ist das polizeiliche Informationswesen immer weniger in der Lage, die zu seinem Erhalt und zu seinem Betrieb erforderlichen Aufwände durch entsprechende positive Effekte auf die polizeiliche Arbeit zu rechtfertigen.

Die technologische Diskrepanz der Polizei zu den übrigen Teilen der Gesellschaft produziert Folgeprobleme für die Polizei. Auf der einen Seite geraten die polizeilichen Systeme selbst immer wieder in den Fokus von Kriminellen, die mithilfe von technisch überlegenen Cyberangriffen sensible Daten aus den polizeilichen Datenbeständen zu Polizist:innen selbst, verdächtigen Personen, aber auch unter besonderem Polizeischutz stehenden Personen, wie hochrangigen Politiker:innen, erbeuten und diese schädigend nutzen: Betroffene werden mit der Veröffentlichung von persönlichen Daten erpresst, immer wieder kommt es zu Drohungen und weitergehenden Repressalien gegenüber denjenigen, deren Daten publik gemacht worden sind.[2255]

Vor allem macht sich die technologische Superiorität professionalisierter krimineller Felder aber darin bemerkbar, dass der polizeiliche Blick in bestimmten Kriminalitätsbereichen nur noch sehr oberflächlich Strukturen aufhellen kann. Vor allem in Bereichen, in denen es verfestigte Strukturen mit professionellen Täter:innen gibt, die ihre Kommunikations- und sonstige Technik stetig an fortschreitende Standards anpassen – also insbeson-

2254 *Gugerli* in Gugerli/Hagner/Hampe ua (Hrsg.), Nach Feierabend, 7 (7).
2255 *Gerhold/Brandes* Eur J Futures Res 9 (2021) (11 f.).

dere die organisierte Kriminalität, terroristische Täter:innen und Cyberkriminalität – gelingen der Polizei kaum noch Ermittlungserfolge. Terroristische Anschläge werden von der Sicherheitskultur mit einer gewissen „Gelassenheit" (*Münkler*)[2256] hingenommen, lassen sich aber regelmäßig nur während ihrer situativen Entfaltung bekämpfen. Die organisierte Kriminalität agiert größtenteils von der rechtstreuen Gesellschaft unerkannt. Ab und an kommt es zu partiellen Aufdeckungen durch Medien oder seltene Ermittlungserfolge. Cyberkriminalität und Kriminalität, die in datenvermittelten Kontexten wie Umgebungen der sogenannten Smart City begangen wird, kann von der Polizei ebenfalls nur sehr begrenzt erkannt und dementsprechend kaum behandelt werden. Auch Kriminalität im Wirtschaftsleben, das hochtechnisiert und stark um Datenverarbeitungsprozesse herum organisiert ist, lässt sich kaum aufklären.

Polizeiliche Überwachungs- und Kontrolltätigkeiten sind in erster Linie auf die traditionellen (und analogen) Räume beschränkt. Die von der Polizei eingesetzte Informationstechnologie dient vor allem der Abkürzung von Arbeitsabläufen, etwa durch automatische Sprache-zu-Text-Umwandlung, oder zur Erleichterung der Kommunikation zwischen Beamt:innen im Einsatz. Es gibt allerdings kaum größere Integrationsverbünde von technischen Komponenten. Das polizeiliche Instrumentarium ist ansonsten auf hergebrachte „Werkzeuge" wie Schusswaffen und sonstigen Verteidigungsmittel, Handschellen und einsatzunterstützende Hilfsmittel beschränkt.

III. Polizeiliche Sozialkontrolle

Die vom Massendatenphänomen überforderte Polizei hat ihre einst zentrale Position im System der gesellschaftlichen Sozialkontrolle verloren. Damit geht ein genereller Bedeutungsverlust der staatlichen Sozialkontrolle in der zunehmend datafizierten Welt einher, da die Polizei als diejenige Institution wegfällt, die allen voran Devianz identifiziert und filtert.

Die beschriebenen Probleme der Wissensgenerierung der Polizei in der zunehmend digitalisierten Lebenswelt der Gesellschaft begrenzen den polizeilichen Wirkungsradius. Die Polizei ist primär im analogen öffentlichen Raum präsent und agiert dort als Produzentin sozialer Ordnung, etwa

2256 *Münkler* in Hucho/Nida-Rümelin/Julian, Sperling, Karl ua (Hrsg.), Berichte und Abandlungen der Band Berlin-Brandenburgischen Akademie der Wissenschaften, 101 (112).

im Kontext von gewalttätigen Auseinandersetzungen. Auch die kriminalpolizeiliche Tätigkeit ist im Wesentlichen auf die retrospektive Aufklärung klassischer Fälle beschränkt: Kapitaldelikte, Sexualstraftaten oder auch die abnehmenden Formen von Vermögensdelikten, die sich noch rein im analogen Raum begehen lassen. Polizeiarbeit findet also (wieder) vor allem auf „der Straße" statt. Damit ergeben sich einerseits Potenziale für eine nahbare, gemeinschaftsbezogene Form der Polizeiarbeit (community policing[2257]).[2258] Gleichzeitig führt der Fokus auf „Straßenkriminalität" jedoch weiterhin zu einer starken Überrepräsentierung von gesellschaftlichen Minderheiten und ohnehin bereits Ausgegrenzten im polizeilichen Fokus. Diese Selektivität hält Konfliktpotenzial für das Verhältnis zwischen Polizei und „Polizierten" bereit. Dort, wo ein positives Verhältnis zur Gemeinschaft nicht hergestellt oder aufrechterhalten werden kann, kommt es zu Legitimationsverlusten, die Widerständen gegenüber den polizeilichen Einsatzkräften hervorrufen, worauf die Sicherheitspolitik mitunter mit einer – informationstechnologisch anspruchslosen – Militarisierung[2259] der Polizeitechnik reagiert.

Die Einschränkung des aufklärenden Blickes der Polizei führt auch dazu, dass sich Strukturen organisierter Kriminalität stärker ausbreiten und verfestigen können. Diese Strukturen fordern den staatlichen Ordnungsanspruch heraus und produzieren parallele Ordnungen in bestimmten Gebieten, in denen sie dann zwangsläufig auch (informelle) Sozialkontrolle an der Polizei bzw. des Staates statt ausüben.[2260] Damit ist keinesfalls eine nur fatalistisch rezipierbare Entwicklung eingeleitet, denn wie *Eisenstadt* bereits feststellte: „collapse, far from being an anomaly, both in the real world and in social evolutionary theory, presents in dramatic form not the end of social institutions, but almost always the beginning of new ones."[2261] Insofern kommt es zu einer Pluralisierung der Akteure. So wird die bereits für die

2257 *Cordner* in Reisig/Kane/Bradford (Hrsg.), The Oxford handbook of police and policing, 148.

2258 *Gerhold/Brandes* Eur J Futures Res 9 (2021) (9).

2259 Siehe zu diesem vorrangig aus dem US-amerikanischen Diskursraum stammenden Phänomen *Bieler* PIJPSM 39 (2016), 586; zur deutschen Situation siehe *Naplava* in Hunold/Ruch (Hrsg.), Polizeiarbeit zwischen Praxishandeln und Rechtsordnung, 165.

2260 Siehe zu dieser Dynamik der Konkurrenz von Ordnungen und Regimen sozialer Kontrolle etwa *Timothy Raeymaekers*, Collapse or Order? Questioning State Collapse in Africa, Nr. 10, 2005, S. 11 f.

2261 *Eisenstadt* in Yoffee (Hrsg.), The collapse of ancient states and civilizations, 236 (243). Zwar ist der Kontext ein entwicklungsgeschichtlich anderer, aber diese

Spätmoderne beschriebene Privatisierung der Sozialkontrolle beispielsweise stark intensiviert.[2262] Mit der Verkümmerung staatlicher Sozialkontrolle und Ordnungsproduktion einher gehen Strategien der Responsibilisierung der Individuen für ihre persönliche Sicherheit und die Kommodifizierung der je eigenen Sicherheitsbedürfnisse.[2263] In der Folge kommt es zu einer räumlichen Multiplikation sozialer Ordnungen. In Städten etwa bilden sich in Vierteln mit besserem sozioökonomischem Status deutlich abgeschottete Gemeinschaften heraus. Die verschiedenen Formen und Grade sozialer Ordnungen bringen zudem stark abweichend ausgeprägte Subjektkulturen hervor. Diese verteilen sich sicherheitskulturell auf der eingangs beschriebenen Achse zwischen denjenigen, die gelassener mit Unsicherheit umgehen und denjenigen, die Unsicherheit als Bedrohung wahrnehmen, aber keinen produktiven Umgang damit finden. Mit der multipolaren Ordnungstopografie, in der die Polizei nur eine Ordnungsproduzentin von vielen ist, geht auch ein Wandel des gesamtgesellschaftlichen Normgefüges einher. Den Institutionen der staatlichen Sozialkontrolle gelingt es mit Trübung des polizeilichen Blicks immer weniger, eine minimale normative Integration der Gesellschaft zu leisten. In der Folge kommt es zu einer stärkeren Fragmentierung bzw. Pluralisierung der normativen Grundlagen der Gesellschaft.

E. Drittes Szenario: Die Polizei als spezialisiertes Konfliktlösungsinstrument

Die beiden vorstehenden Szenarien sind aus der Perspektive des grundgesetzlichen Wertefundaments der hiesigen Gesellschaft nicht erstrebenswert. Im Szenario der datenmächtigen Polizei ist es vor allem die faktische und umfassende Aushöhlung des Rechts auf informationelle Selbstbestimmung, die den normativen Leitvorstellungen des Grundgesetzes widerspricht. Die Möglichkeiten des polizeilichen Informationswesens auf Daten in der Gesellschaft zuzugreifen und darüber Wissen über Personen – etwa in Form von Persönlichkeitsbildern im Rahmen von Risikoprognosen – und Gruppen zu generieren sind unter den Aspekten der Streubreite und des Informationsgehalts von Daten, die bereits jetzt als dogmatische Kriterien zur

grundlegende Dynamik sozialer Evolution dürfte als einigermaßen universell gelten.

2262 *Shearing/Stenning* Social Problems 30 (1983), 493.

2263 Siehe dazu etwa *Singelnstein/Kunz,* Kriminologie, S. 411 ff.

Bestimmung der Eingriffsintensität einzelner Maßnahmen dienen, kaum mit dem Verhältnismäßigkeitsgrundsatz in Einklang zu bringen. Auch das Szenario der überforderten Polizei kann nicht als vor dem Hintergrund des Grundgesetz erstrebenswerte gesellschaftliche Zukunft gelten. Ganz gleich, wie man sie konzeptualisiert – ob als Grundrecht auf Sicherheit[2264] oder als objektiv-rechtliche Schutzpflicht des Staates[2265] – ist die Sicherheitsgewährleistung eine dem Staat zentrale und ihn als verfasste Friedens- und Ordnungsmacht auch im Angesicht der Pluralisierung der Gesellschaft charakterisierende Aufgabe. Bestehen auch unterschiedliche Auffassungen darüber, wie die normativen Gehalte des Sicherheitsbegriffs auszugestalten sind und wie viel dann von der so oder anders verstandenen Sicherheit zu gewährleisten ist, so ist doch ein gewisses Maß an Sicherheit in Form einer fundamentalen sozialen Ordnung, die gleichsam die Gesellschaft bis zu einem gewissen Grad normativ zu integrieren vermag, eine anerkannte Grundvoraussetzung menschlicher Vergesellschaftung.

Vor diesem Hintergrund soll nun im Folgenden ein drittes Szenario entworfen werden, das einen vermittelnden Pfad zwischen den beiden wenig erstrebenswerten Zukünften der datenmächtigen bzw. überforderten Polizei aufzeigen möchte. Damit soll ein Beitrag zur Reflexion über die Bedeutung wachsenden Wissens und technologischer Beherrschung von sozialen Prozessen im Rahmen polizeilicher Sozialkontrolle für die heutige Gesellschaft geleistet werden. Ziel ist es dabei, den technologie-induzierten Risiken des polizeilichen Informationswesens mit regulativer Voraussicht zu begegnen und in Auseinandersetzung mit diesen Risiken eine produktive sozio-technische Imagination informationstechnisch fundierter Sozialkontrolle durch die Polizei zu entwickeln. Das folgende Szenario ist das der Polizei als ein spezialisiertes Konfliktlösungsinstrument der Gesellschaft.

2264 *Isensee,* Das Grundrecht auf Sicherheit.

2265 Siehe dazu etwa *Aulehner,* Polizeiliche Gefahren- und Informationsvorsorge, S. 431 ff; grundlegend zu Schutzpflichten *Unruh,* Zur Dogmatik der grundrechtlichen Schutzpflichten.

I. Sicherheitskultur

Der Sicherheitsdiskurs ist – wie immer wieder gefordert – tatsächlich evidenzbasierter[2266] geworden, was eine prinzipiell rationale Sicherheitskultur in der breiten Bevölkerung befördert hat. Die Kriminalitätsfurcht ist einigermaßen kongruent mit den jeweiligen Kriminalitätsrisiken der Betroffenen. Kriminalpolitischer Populismus vermag kaum mehr als überschaubare Teile der Wahlbevölkerung zu mobilisieren. Die Straf- und Sicherheitsgesetzgebung haben sich dementsprechend gewandelt. Legislative Projekte rezipieren in hohem Maße Erkenntnisse der kriminologischen Forschung, die als Fundament für kriminalpolitische Richtungsentscheidungen gelten. Dabei bedeutet eine rationale Sicherheitskultur hingegen nicht, dass es keine problematischen Kriminalitätsrisiken gibt. Vielmehr ist im sicherheitspolitischen Diskurs präsent, dass die globalisierte, digitalisierte und datafizierte Gesellschaft neue Phänomene sozialer Unordnung mit sich bringt, die einen stellenweise geänderten Überwachungs- und Kontrollmodus erforderlich machen. Die hochtechnisierte Gesellschaft hat vielfältige Vulnerabilitäten, etwa an den neuralgischen Punkten ihrer kritischen Infrastrukturen, in neuen virtuellen Räumen oder aufgrund ihrer grundsätzlich offenen Struktur. Tatsächlich bestehende Bedrohungen durch terroristische Täter:innen, Cyberkriminelle oder konkrete Formen nachgewiesener organisierter Kriminalität sind die neuen Schwerpunkte des Sicherheitsdiskurses und damit auch der Polizei.

II. Technologische Entwicklung des polizeilichen Informationswesens

Die Entwicklung und der Einsatz von informationstechnologischen Verfahren zur Massendatenverarbeitung verlaufen innerhalb der polizeilichen Organisationen nach zwei getrennten und weitgehend entkoppelten Dynamiken.

Ein Teil der Polizei ist wieder vorrangig auf Streife im öffentlichen Raum. Die Polizeibeamt:innen sind mehrheitlich zu Fuß unterwegs und versuchen, ansprechbar zu sein und gleichzeitig Verbindungen zur örtlichen Gemeinschaft zu knüpfen, wodurch an ein traditionelles Modell der Polizeiarbeit angeknüpft wird. Diese Form der gemeinschaftsbezogenen

2266 Siehe zum Ideal der Evidenzbasiertheit aus jüngerer Zeit etwa *B.-D. Meier* Kriminalpolitische Zeitschrift 5 (2020), 1; *M. Walsh* NK 32 (2020), 24.

Polizeiarbeit wird durch die Einstellung von mehr Beamt:innen und die Investition in bessere Ausrüstung flankiert. Informationstechnologische Geräte und Verfahren werden zwar von der Polizei eingesetzt, dienen aber in erster Linie dazu, die Effizienz der internen Abläufe und der Kommunikation mit der Öffentlichkeit zu steigern.[2267] Zudem wurden die Beamt:innen hinsichtlich ihrer technischen Ausrüstung weniger letal ausgestattet. Nur sporadisch werden Schusswaffen getragen. Es werden deeskalierende Taktiken und möglichst wenig beeinträchtigende Angriffs- und Verteidigungstechniken gelehrt. Zudem sind die Polizeikräfte nur ein Akteur im System der Produktion und Gewährleistung sozialer Ordnung in der Öffentlichkeit. Neben den Streifenbeamt:innen existiert ein breiteres Tableau von Akteur:innen in Form von zivile Konfliktlösungsteams zu diesem Zweck. Die Polizeikräfte der gemeinschaftsbezogenen Polizei dienen in diesem pluralen System der Sicherheitsproduktion vor allem als Reserve für Situationen und Konflikte, die sich ohne eine institutionalisierte Zurschaustellung von staatlicher Macht und erforderlichenfalls auch durch die Anwendung von verhältnismäßiger Gewalt nicht lösen lassen. Dafür ist eine datenmäßige Erfassung von Sachverhalten nur sehr selten vonnöten. Intervenieren diese Polizeibeamt:innen und registrieren strafrechtlich relevantes Verhalten, werden die Daten auch nur begrenzt von der Polizei verarbeitet, sondern vor allem direkt an die anzulegende elektronische Strafakte der Staatsanwaltschaft übertragen, die so wieder stärker ihre Rolle als Herrin des Ermittlungsverfahrens im Bereich der herkömmlichen Kriminalität im öffentlichen Raum erlangt hat. Insgesamt ist der Grad des informationstechnologisch fundierten Überwachungs- und Kontrollpotenzials bei diesem Teil der Polizei eher gering. Eine vollständige oder auch nur möglichst umfassende polizeiliche Durchdringung des öffentlichen Raumes zum Zweck der sozialen Kontrolle ist allerdings auch nicht das Ziel dieser institutionell abgegrenzten gemeinschaftsbezogenen Polizeiorganisation.

Dem gegenüber steht der zweite, ebenfalls institutionell abgegrenzte Teil der Polizei, der auf die Aufklärung und Verfolgung bestimmter hochschädlicher Kriminalitätsfelder fokussiert ist. Dazu gehören vor allem die drei großen Kriminalitätsphänomene der globalisierten und digitalisierten Gesellschaft: Terrorismus, (tatsächlich bestehende[2268]) organisierte Krimina-

2267 *Gerhold/Brandes* Eur J Futures Res 9 (2021) (9).

2268 Für eine kritische Reflexion hinsichtlich des vom medial-politischen Diskurs mitunter etwas schnell verwendeten und nicht immer durch tatsächliche Erkenntnisse

lität und Cyberkriminalität. Es sind Formen der Devianz, die ohne staatliche bzw. polizeiliche Überwachung und Kontrolle das ihren schweren Formen innewohnende Schädigungspotenzial realisieren und gesellschaftliche Strukturen damit real und nachhaltig bedrohen können, sodass eine spezialisierte Bekämpfung dieser Straftaten durch eine spezialisierte Institution geboten ist. Auch bestimmte Formen der (organisierten) hochrangigen Wirtschaftskriminalität[2269] ließen sich dazu zählen. Dieser Teil der Polizei ist mithin ein spezialisiertes Instrument für die Bearbeitung originärer Unordnungsphänomene der spätmodernen Gesellschaft.[2270]

Dazu ist ein effektives, aber gleichsam beschränktes und darin kontrolliertes polizeiliches Informationswesen erforderlich. Hierfür haben diese spezialisierten Polizeikräfte ein breites informationstechnologisches Instrumentarium, das von invasiven und streubreiten Erhebungsmethoden über interoperable und gut strukturierte Datenspeicher bis hin zu leistungsstarken Datenanalyseverfahren reicht. Allerdings ist das darin liegende Überwachungs- und Kontrollpotenzial ständigen Einhegungsbemühungen unterworfen, die vom Recht initiiert sind. Neben materiellen Begrenzungen auf bestimmbare Personenkreise und konkretere Eingriffsschwellen auch im Vorfeld findet vor allem eine prozedurale Beschränkung des Informationswesens statt. Zur Kontrolle der polizeilichen Sozialkontrolle hat sich ein robustes und handlungsfähiges internes Datenschutzkontrollregime in den Polizeiorganisationen etabliert, das durch eine enge Aufsicht der Bundes- und Landesdatenschutzbeauftragten ergänzt wird. Das interne System zeichnet sich allerdings bereits durch eine hohe Überwachungs- und Kontrolldichte bezüglich der polizeilichen Datenverarbeitung aus, sodass die Aufsichtsbehörden regelmäßig keine akuten Missstände feststellen, sondern eher strategische Ausrichtungsentscheidungen des polizeilichen Überwachungs- und Kontrollapparats im sicherheitspolitischen Diskurs mitbeeinflussen. Gewährleistet wird dies zunächst durch eine präsente und starke Stellung der behördlichen Datenschutzbeauftragten. Da diese aber die massenhafte Erhebung und Verarbeitung der Daten nicht alleine auf ihre Rechtmäßigkeit überprüfen können, ist eine automatisierte techni-

---

fundierten Konzepts der organisierten Kriminalität siehe etwa *Paoli/Vander Beken* in Paoli (Hrsg.), The Oxford handbook of organized crime, 13.

2269 *Liebl* (Hrsg.), Wirtschafts- und Organisierte Kriminalität.

2270 Angelehnt an *Derin/Singelnstein,* Die Polizei: Helfer, Gegner, Staatsgewalt, S. 362, die ebenfalls für die Polizei als "abgesteckte Ausnahmebehörde mit wenigen spezifischen Kompetenzen" plädieren, die also ein Konfliktlösungsmechanismus unter vielen ist.

sche Datenschutzkontrollarchitektur implementiert worden, die aus zwei wesentlichen Elementen besteht: Einerseits ist ein umfassendes Protokollierungssystem geschaffen worden, das lückenlos jede Datenerhebung und daran anschließende Verarbeitung bis zur Löschung dokumentiert. Die dabei anfallenden Protokolldaten über das aggregierte Informationshandeln der Polizei werden algorithmengestützt und gleichfalls automatisiert nach Mustern durchsucht, die auf einen rechtswidrigen Datenumgang hindeuten, wonach Verdachtsfälle dann durch die behördlichen Datenschutzbeauftragten gesondert geprüft werden. Andererseits ist das polizeiliche Informationswesen bezüglich seiner Löschungsvorgaben, also hinsichtlich des Rechts auf Vergessen im polizeilichen Kontext, automatisiert. Daten werden also bei ihrer Erhebung anhand ihrer personenbezogenen Klassifikation einem automatisiertem Löschregime unterstellt, das nur in Ausnahmefällen nach Konsultation der behördlichen Datenschutzbeauftragten in wichtigen Ermittlungskomplexen suspendiert werden kann. Geschieht dies nicht, „vergisst" das polizeiliche Informationswesen automatisiert nach entsprechend festgelegten Zeiträumen personenbezogene Daten unwiederbringlich, wodurch die polizeilichen Datenbestände laufend verjüngt werden.

Die Fokussierung dieses Teils der Polizei auf bestimmte Kriminalitätsfelder macht es zudem leichter, informationstechnologische Infrastrukturen und Verfahren zur Massendatenverarbeitung zu entwickeln und zu implementieren, da die informationellen Bedürfnisse, die miteinander harmonisiert werden müssen, nicht mehr so stark divergieren, wie in der vorherigen organisationalen Struktur. Gleichzeitig kann durch diese graduelle Senkung des Komplexitätsniveaus des polizeilichen Informationswesens ein größerer Fokus auf die Rechtmäßigkeitskontrolle von Technologie-Entwicklung und -einsatz gelegt werden. Es gibt genug zeitliche und sonstige Ressourcen, um eine Anpassung von Technologien an die Regulierungsstrukturen zu vollziehen, um Sicherheitslücken zu identifizieren und zu schließen und um die Polizeibeamt:innen im rechtmäßigen Umgang mit den technologischen Verfahren zu schulen.[2271] Damit aber diese datenmächtigen Polizeikräfte auch von möglichen Devianzphänomenen erfahren, die ihrem Zuständigkeitsbereich unterfallen, aber im Blickfeld der gemeinschaftsbezogenen Polizeikräfte auftauchen, bestehen eng umgrenzte Datenübermittlungspflichten anlässlich bestimmter Verdachts- oder Erkenntnismerkmale. Neben einem operativen Apparat für die Durchführung von polizeilichen

2271 *Gerhold/Brandes* Eur J Futures Res 9 (2021) (9).

Maßnahmen von Datenerhebungen bis zu Festnahmen besteht zudem eine grundsätzliche, wenn auch selten akute Notwendigkeit für die auf hochschädliche Kriminalitätsfelder spezialisierte Polizei einzugreifen, wenn sich etwa terroristische Risikopotenziale im öffentlichen Raum zu materialisieren drohen oder materialisiert haben. Dazu sind, wie schon heute, entsprechende Eingreifteams eingerichtet. Im Gegensatz zur gemeinschaftsbezogenen Polizei sind diese Beamt:innen durchgehend mit letalen Waffen ausgestattet und können je nach Einsatzszenario auch mit entsprechenden informationstechnologischen Instrumenten ausgestattet werden – etwa mit mobilen Videosysteme wie Bodycams zur biometrischen Identifizierung von Zielpersonen oder zur Erkennung verdächtigen Verhaltens sowie mit weiteren bereits oben nach *Bain et al.*[2272] beschriebenen Geräte und Verfahren.[2273]

III. Polizeiliche Sozialkontrolle

Die polizeiliche Sozialkontrolle im Szenario der Polizei als spezialisiertes Konfliktlösungsinstrument lässt sich vor allem als modular beschreiben: Der Einfluss der gemeinschaftsbezogenen Polizei auf die Produktion sozialer Ordnung ist relativiert und von eher abnehmender Tendenz. Die Pluralisierung der Akteuren zur Bearbeitung von verbreiteter und gewöhnlicher Devianz bzw. zur – effektiveren – Bearbeitung der damit verbundenen sozialen Missstände und Konflikte verdrängt die Polizei ein stückweit aus diesen Feldern. Zwar ist auch die Polizei weiterhin an sozialer Kontrolle etwa im öffentlichen Raum beteiligt, aber hauptsächlich gewährleistet sie einen Rahmen, innerhalb dessen vielfältige Konfliktlösungsteams den Versuch eines sanfteren Umgangs mit Devianz unternehmen und durch ihren höheren Professionalisierungsgrad – beispielsweise im Bereich der Drogenprävention und -arbeit – auf eine nachhaltigere Adressierung von deviantem Verhalten zugrundeliegenden Konfliktpotenzialen hinarbeiten. Damit einher geht eine gewisse Akzeptanz spätmoderner Ordnungsphänomene, die in einer Welt des „eskalierenden Wandels“[2274] multiple Normgefüge nebeneinander hervorbringt. Im Gegensatz dazu versucht die auf

2272 Siehe zum Folgenden *Bain/Carsone/Conser* ua in Bain (Hrsg.), Law Enforcement and Technology, 115 (126 ff.).
2273 Siehe dazu bereits oben S. 503 f.
2274 *Sheptycki* Global Crime 18 (2017), 286 (296).

hochschädliche Kriminalitätsfelder fokussierte Polizei über ihre begrenzte Datenmacht eine möglichst umfassende und – wegen immer nur begrenzt vorhandenen Ressourcen – selektive, also möglichst auf die „gefährlichsten" Individuen und Strukturen gerichtete, Sozialkontrolle zu etablieren. Die informationelle Durchdringung bestimmter gesellschaftlicher Felder ermöglicht es den begrenzt datenmächtigen Polizeikräften zudem, neue Kriminalitätsphänomene zu identifizieren und darauf zu reagieren. Die Modularität der polizeilichen Sozialkontrolle bedeutet also auch eine Flexibilisierung der Ausrichtung des polizeilichen Fokus, womit auch bisher „underpoliced" Bereiche wie etwa hochrangige Wirtschaftskriminalität erschlossen und polizeilicher Sozialkontrolle zugeführt werden können.[2275] Die Fragmentierung sozialer Ordnungen in der spätmodernen Gesellschaft bringt also eine zunehmend plurale, mehrebene und netzwerkartige Sozialkontrolle hervor, in der die Polizei – auf den niedrigeren Ebenen Netzwerke von pluralen Akteuren der Bearbeitung von Devianz unterstützt, während sie auf den höheren Ebenen zu einem spezialisierten Instrument der Ausübung durchgreifender Sozialkontrolle gegenüber hochschädlichen Kriminalitätsfeldern wird.[2276]

F. Regulierung: Kollektive Handlungsfähigkeit gegenüber dem soziotechnischen Großsystem des polizeilichen Informationswesens

Dem französischen Technikphilosophen *Ellul* wird manchmal vorgeworfen, er zeichne ein hoffnungsloses Bild einer von der Technik besessenen und letztlich gefesselten Gesellschaft. Gleichzeitig bietet sein Werk aber stets auch Anknüpfungspunkte, um einem deterministischen Verhältnis von Technologie und gesellschaftlicher Entwicklung zu entkommen:

> „[I]f man – If each one of us – abdicates his responsibilities with regard to values; if each of us limits himself to leading a trivial existence in a technological civilization, with greater adaptation and increasing success as his sole objectives; if we do not even consider the possibility of making a stand against these determinants, then everything will happen as I have described it, and the determinants will be transformed into inevitabili-

2275 Ähnlich etwa *Brayne,* Predict and surveil, S. 144.

2276 So auch – aber mit kritischem beziehungsweise skeptischem Unterton – *Sheptycki* Global Crime 18 (2017), 286 (296).

> ties. […] We must not think of the problem in terms of a choice between being determined and being free. We must look at it dialectically, and say that man is indeed determined, but that it is open to him to overcome necessity, and that this act is freedom. Freedom is not static but dynamic; not a vested interest, but a prize continually to be won. The moment man stops and resigns himself, he becomes subject to determinism. He is most enslaved when he thinks he is comfortably settled in freedom."[2277]

Wie also lässt sich eine (kollektive) gesellschaftliche Handlungsfähigkeit herstellen oder erhalten, um im stetigen Ringen um Freiheit im Angesicht zunehmender informationstechnologischer Überwachungs- und Kontrollmöglichkeiten nicht in einen genügsamen, aber unfreien Stillstand zu geraten? Diese Frage führt zunächst zurück zum Ausgangspunkt dieses Kapitels, zu den sozio-technischen Imaginationen. Als kollektiv geteilte, institutionell stabilisierte und öffentlich praktizierte Vorstellungen einer wünschenswerten Zukunft, die durch eine normativ bedingte Technologie-Entwicklung beeinflusst wird, ermöglichen es sozio-technische Imaginationen Anstrengungen gebündelt auf die Erreichung eines gemeinsamen Ziels auszurichten.[2278] Für die Frage, wie sich eine Imagination gegenüber anderen durchsetzen kann, eignet sich das bereits eingeführte Konzept der Sicherheitskultur als Antwortansatz. In ihrem Rahmen finden gesellschaftliche Aushandlungsprozesse statt, mit denen die verschiedenen Akteur:innen darüber entscheiden, was als Gefahr anzusehen ist und wie dieser Gefahr – etwa mit technischen Mitteln – begegnet werden muss.[2279] Insofern ist die hegemoniale Sicherheitskultur untrennbar mit dem Aufstieg und Fall bestimmter sozio-technischer Imaginationen im Kontext gesellschaftlicher Sicherheitsbedürfnisse verbunden.[2280]

Die genauen Verlaufspfade der gegenwärtigen Sicherheitskultur lassen sich nur erahnen, aber ihre derzeitigen Eigenschaften und Dynamiken enthalten durchaus Potenziale für die Realisierung eines der beiden unerwünschten Szenarien. *Daase* zufolge ließe sich bereits jetzt „zeigen, dass der Wandel der Sicherheitskultur nicht nur zu institutionellen Veränderun-

2277 *Ellul,* The Technological Society, xxix, xxxiii. Dieser Zusammenhang der beiden Fundstellen ist übernommen von *Sacasas*, What Is To Be Done? — Fragments, https://theconvivialsociety.substack.com/p/what-is-to-be-done-fragments (Stand: 01.10.2023).
2278 *Gerhold/Brandes* Eur J Futures Res 9 (2021) (3).
2279 *Daase* Aus Politik und Zeitgeschichte 2010, 9 (9).
2280 *Gerhold/Brandes* Eur J Futures Res 9 (2021) (4).

gen und rechtlichen Verwerfungen in der Sicherheitspolitik führt, sondern generell staatliche Sicherheitsorgane und internationale Sicherheitsinstitutionen zu überfordern beginnt."[2281] Der mittlerweile von überall aus der Gesellschaft schallende Anspruch auf staatliche Sicherheitsgewährleistung provoziert einen reflexhaft gewordenen staatlichen Legitimierungsimpetus- und -zwang – Sicherheitsgewährleistung für all jene (mit gesellschaftlichem Einfluss) im staatlichen Herrschaftsbereich – und trifft gleichzeitig auf begrenzte staatliche Ressourcen zur Produktion und Aufrechterhaltung von Sicherheit.[2282] Bezogen auf die Polizei als zentrale Akteurin staatlicher Sozialkontrolle und Sicherheitsgewährleistung lässt sich insofern ein Spannungsfeld ausmachen. Im Rahmen dieser Spannung drängt eine Dynamik – Sicherheitsansprüche und staatliche Legitimierungsbedürfnisse – in Richtung der datenmächtigen Polizei, die hoch technologisiert möglichst umfassende Sicherheit gewährleisten soll. Dem entgegen wirkt paradoxerweise die stetige Übernahme neuer Sicherheitsaufgaben und -versprechen durch den Staat und damit auch durch die Polizei. Denn die zunehmende Inanspruchnahme der begrenzten polizeilichen Ressourcen produziert laufend Potenziale für eine im Wesentlichen überforderte Polizei.

Insofern erscheint eine Neutralisierung dieser dysfunktionalen Tendenzen geboten, die ihren Ausgangspunkt in einer sukzessiven Umstellung des der Sicherheitskultur zugrundeliegenden normativen Gefüges nehmen muss. Eine rationalere Sicherheitskultur würde es sodann ermöglichen, nachhaltige sozio-technische Imaginationen der gesellschaftlichen Verwendung von informationellen Überwachungs- und Kontrolltechnologien zu entwickeln, die eine grundgesetzadäquate Sozialordnung auch in der spätmodernen Gesellschaft und darüber hinaus gewährleisten kann. Im Kern einer solchen Sicherheitskultur sollte vor allem ein Verständnis für die unhintergehbare *conditio humana* stehen. *Sacasas* schreibt in diesem Zusammenhang:

> I would add, too, that because many of the problems we face are functions of the human condition, we cannot solve them, exactly—we can just find better ways of abiding them. Indeed, it may be that some of the problems we face stem precisely from the temptation to relate to the

2281 *Daase* Aus Politik und Zeitgeschichte 2010, 9 (16).
2282 *Daase* Aus Politik und Zeitgeschichte 2010, 9 (9).

> human condition as one would to a technical problem in need of an engineered solution.[2283]

So sind den auch die vielfältigen Probleme, die die Gesellschaft mit deviantem Verhalten erfährt, zumeist Ausdruck sozialer Missstände und menschlicher Fehlbarkeiten, für die eine technologische Lösung selten oder nur unter stetiger Erhöhung des Drucks auf die menschliche Natur Abhilfe schaffen kann. Diese Idee ist auch dem gegenwärtigen System staatlicher Sozialkontrolle und der Polizei natürlich nicht völlig fremd. Damit sie aber zu einem robusten Kern einer neuen Sicherheitskultur werden kann, scheint eine rechtliche Programmierung der Sicherheitskultur, die ohnehin in ihren Strukturen stark normativ geprägt ist, erstrebenswert. Nun lässt sich *die* Sicherheitskultur nicht einfach durch *das* Recht umgestalten. Aber die Zukunft des polizeilichen Informationswesens wird entscheidend von gesetzgeberischen und gerichtlichen Entscheidungen abhängen.[2284] Um einem ausufernden technischen Solutionismus[2285] im allgegenwärtigen gesellschaftlichen Streben nach Sicherheit entgegenzutreten, gibt es also regulative Möglichkeiten, die freilich nicht ohne Weiteres generell auf die gesellschaftliche Produktion von Sicherheit angewendet werden können, sondern bereichsspezifischer Anpassung bedürfen.

Ein solcher – für die Sicherheitsproduktion zentraler – Bereich ist das vorliegend behandelte polizeiliche Informationswesen. Auch hier ist die Beförderung einer neuen Sicherheitskultur durch normative Programmierung keine von zentraler Stelle aus zu leistende Möglichkeit. Das Recht ist vielmehr ein Aushandlungsort, an dem die mit den drei Szenarien verbundenen sozio-technischen Imaginationen darum kämpfen, normativ festgeschrieben zu werden. Um (in einem systemtheoretischen Sinne) Anschlussfähigkeit im Recht zu erzeugen, müssen die Imaginationen dafür in dogmatische Konzepte überführt werden, sodass sie vom Rechtssystem prozessiert werden können.[2286]

Bestrebungen, das dritte hier gezeichnete Szenario normativ abzusichern, scheinen insofern besonders aussichtsreich, als es in besonderer Weise am Verhältnismäßigkeitsgrundsatz orientiert ist, der die gesamte grundgesetzliche Ordnung und damit auch die Sicherheitsverfassung rahmt. Insofern

2283 *Sacasas*, What Is To Be Done? — Fragments, https://theconvivialsociety.substack.com/p/what-is-to-be-done-fragments (Stand: 01.10.2023).
2284 *Gerhold/Brandes* Eur J Futures Res 9 (2021) (17).
2285 *Morozov,* To save everything, click here.
2286 *Luhmann,* Das Recht der Gesellschaft, S. 275.

ist das Szenario für alle jene Akteur:innen erstrebenswert, die sich einer verhältnismäßigen polizeilichen Informationsverarbeitung verpflichtet fühlen. Zudem sind ein Großteil der informationellen Erhebungsbefugnisse der Polizei – zumindest *de iure* – in ihrer grundsätzlichen Struktur vor allem Ausdruck dieses für die Verfassungsordnung grundlegenden Prinzips. Die Dogmatik des polizeilichen Informationswesen ist jedoch nicht angemessen entwickelt, wie *Bäcker* zutreffend sowohl für die rechtliche Regulierung der infrastrukturellen Aspekte wie den einheitlichen Informationsbestand im Sinne des Polizei 2020-Projekts, als auch für die Ebene des praktischen Datenumgangs im Informationswesen in Form vieler (neuer) Formen der Datenanalyse feststellt.[2287] Für beide Säulen des Informationswesens entwickeln sich zunehmend dogmatische Ressourcen für eine angemessenere Regulierung. Hervorzuheben sind etwa *Bäckers* Überlegungen zur rechtlichen Strukturierung von sogenannten verfahrensexternen Datensammlungen bei der Polizei, die einen Großteil des polizeilichen Informationswesens ausmachen. Das nach verfahrensübergreifenden und verfahrensunabhängigen sowie verfahrensinternen und verfahrensvorbereitenden unterscheidende Konzept erlaubt eine verhältnismäßige Strukturierung und Verwendung von polizeilichen Datensammlungen und sollte daher expliziter gesetzgeberisch rezipiert werden.[2288] Auf der Ebene des Datenumgangs, die immer mehr durch den Einsatz von Anwendungen künstlicher Intelligenz geprägt wird, gibt es bereits seit einiger Zeit dogmatische Bemühungen, regulative Konzepte zu entwickeln.[2289] Die neuartigen Formen der Datenauswertung etwa im Kontext des bereits bestehenden Datenabgleichs oder der neuen Anwendungen zur automatisierten Datenanalyse harren jedoch noch ihrer befriedigenden Bearbeitung.[2290] Mit Blick auf die Geschwindigkeit informationstechnologischer Innovation muss die dogmatische Auseinandersetzung um passende Konzepte für das polizeiliche Informationswesen zudem mehr als herkömmliche Rechtsdogmatik als stetiger Prozess verstanden werden, in dem es keinen Endpunkt, son-

2287 Zum ersten Aspekt siehe *Bäcker*, A-Drs. 18(4)806 D, S. 2, zum zweiten Aspekt *Bäcker* in Hoffmann-Riem (Hrsg.), Big Data - Regulative Herausforderungen, 167 (169 ff.).

2288 Siehe dazu *Bäcker,* Kriminalpräventionsrecht, S. 494 ff.

2289 Grundlegend zur Regulierung etwa *Martini,* Blackbox Algorithmus – Grundfragen einer Regulierung Künstlicher Intelligenz; für ein spezifisches Verfahren im polizeilichen Bereich siehe etwa die Empfehlungen von *Sommerer,* Personenbezogenes Predictive Policing.

2290 *Golla* Kriminologisches Journal 52 (2020), 149 (156 ff.).

dern nur aktuell mehr oder weniger gut an den gegenwärtigen Entwicklungsstand adaptierte Konzepte geben kann. Insofern ist *Gollas* Plädoyer für ein lernfähiges Recht der polizeilichen Informationsverarbeitung, das technologische Wandlungsprozesse laufend beobachtet und den rechtlichen Rahmen bedarfsweise korrigiert, unumwunden beizupflichten.[2291]

Dafür müssen der dogmatischen Diskussion ausreichend Material und Gelegenheiten zum Lernen gegeben werden. Zudem ist essenziell, dass das Gelernte auch Anwendung finden kann und nicht bereits durch die faktische Fortentwicklung des polizeilichen Informationswesens überholt worden ist.

Neben von *Golla* befürworteten Evaluationspflichten, parlamentarischen Unterrichtungen, Auslaufklauseln und besonderen Begründungserfordernissen bezüglich einzelner technischer Verfahren[2292] erscheint es auf Grundlage der vorliegend dargestellten Dynamiken des polizeilichen Informationswesens zudem notwendig, dessen technischen und organisationalen Schranken rechtlich zu verstärken bzw. wo erforderlich auch neu zu schaffen, um den bedenklichen Tendenzen polizeilicher Informationsverarbeitung zu begegnen. Zu verhindern ist vor allem, dass sich das sozio-technische Großsystem des polizeilichen Informationswesens zu einem verselbstständigten, nicht mehr kontrollierbaren Ensemble für (polizeiliche) Sozialkontrolle entwickelt,[2293] das die Freiheitssphären gesellschaftlicher Felder schleichend aushöhlt.[2294] Auf eine kurze Formel gebracht geht es also in erster Linie um die Überwachung und Kontrolle eines technischen Überwachungs- und Kontrollsystems. Neben dem demokratischen und rechtsstaatlichen Wert einer darüber herstellbaren Transparenz des polizeilichen Informationswesens wäre damit zudem der dogmatischen

2291 Siehe dazu *Golla* Kriminologisches Journal 52 (2020), 149.

2292 *Golla* Kriminologisches Journal 52 (2020), 149 (160).

2293 Siehe zu diesem theoretischen Konzept der "control without control" bereits *Thacker*, Networks, Swarms, Multitudes (Part Two), https://journals.uvic.ca/index.php/ctheory/article/view/14541/5388 (Stand: 01.10.2023): "The political fantasy that is a by-product of these contradiction is that of a "control without control," the best of both worlds: a totally distributed, self-organizing, flexible and robust model of group organization, that can be directed towards certain ends, that is able to mobilize in a particular way, and that is able to express purpose or intention on a global scale.".

2294 Siehe dazu bereits oben S. 484 f.

Entwicklung gedient, die mit klarerem Blick passgenauere Normstrukturen entwickeln könnte.[2295]

I. Überwachung des aggregierten Überwachungs- und Kontrollverhaltens der Polizei: Überwachungsbarometer

Wie bereits weiter oben angesprochen ist die individualrechtsschützende Struktur des Grundgesetzes im Kontext des Massendatenphänomens nicht unproblematisch.[2296] In diese Richtung wendet es auch *Cheney-Lippold*:

> "Privacy as an atomizing, isolating phenomenon is a privacy not worth fighting for. Privacy as intersubjective, social, and associative is a privacy worth thinking through and resuscitating."[2297]

Insofern kann sich eine Überwachung des polizeilichen Informationswesens nicht auf Einzelfälle beschränken, sondern muss eine globale Perspektive einnehmen, mit der die unterschiedlichen Ausprägungen polizeilicher Überwachung und Kontrolle möglichst in ihrer Aggregation in den Blick genommen werden können. Das gilt vor allem, weil das polizeiliche Informationswesen ständig evolviert, wodurch sich die Eingriffsintensität von Datenumgang und Datenbeständen laufend wandeln kann.[2298] Insofern sind die für die Polizeien zuständigen Gesetzgeber gehalten, das polizeiliche Informationswesen als technologische Struktur in seinen unterschiedlichen Ausprägungen auf potenziell neue grundrechtliche Gefährdungslagen hin zu überprüfen und entsprechend ihrer parlamentarischen Regelungspflichten neu zu justieren.[2299] Zudem können die Gesetzgeber natürlich auch über diese Minimalverpflichtung hinausgehen und die polizeiliche Datenverarbeitung aktiv sicherheitspolitisch gestalten. Dafür muss allerdings auch eine proaktivere Auseinandersetzung mit Zustand und Wandlungsprozessen des polizeilichen Informationswesens aus einer Globalper-

2295 Ähnlich *Poscher/Kilchling/Landerer*, Überwachungsbarometer für Deutschland, Ein Modellkonzept, 2022, S. 12.

2296 Siehe dazu bereits oben S. 358 ff.

2297 *Cheney-Lippold,* We are data, S. 244.

2298 *Golla* Kriminologisches Journal 52 (2020), 149 (151); *Poscher/Kilchling*, Entwicklung eines periodischen Überwachungsbarometers für Deutschland, 2021, S. 4.

2299 Diesen Grundsatz hat das Bundesverfassungsgericht in seiner ersten Kalkar-Entscheidung für das technische Sicherheitsrecht formuliert, vgl. BVerfGE 49, 89 (130) – Kalkar I.

spektive erfolgen. Die Gesetzgeber müssen, so *Golla*, „verstärkt Instrumente und Verfahren einsetzen, um ihre ‚Produkte' und ihre Anwendung kritisch zu überprüfen."[2300] Insofern muss ein adäquates Transparenzniveau hinsichtlich polizeilicher Datenbestände und Datenumgangsformen geschaffen werden.

Um dies in dem vorliegend vorgeschlagenen Umfang zu ermöglichen, erscheint in erster Linie das bereits in seinen Grundzügen dargestellte,[2301] bisher beispiellose und vor allem ebenfalls globalperspektivisch strukturierte Überwachungsbarometer für Deutschland von *Poscher, Kilching und Landerer* geeignet. Ziel dieses Instruments ist die verstetigte und periodische[2302] Darstellung der staatlichen Überwachungslast in ihren unterschiedlichen Erscheinungsformen. So soll aufgezeigt werden, „wo reale Schwerpunkte der Überwachung liegen und wie diese sich insgesamt entwickelt", um etwa je nach Bundesland oder Datenverarbeitungsverfahren differenziert Aussagen über Überwachungsintensität zu ermöglichen.[2303] In seiner gegenwärtigen modellhaften Fassung ist das Instrument auf die wesentlichen staatlichen Zugriffsrechte auf private Datenbestände gerichtet, was auch proaktive Berichtspflichten von Seiten der privaten Bestandsinhaber einschließt.[2304]

Allerdings wird das polizeiliche Informationswesen, wie es vorliegend als Verschränkung von informationstechnologischen Infrastrukturen und polizeilichen Informationspraktiken dargestellt wurde, nur sehr begrenzt erfasst. Vorliegend wird vor diesem insoweit beschränkten Umfang des Überwachungsbarometers für eine Ausweitung auf polizeiliche Datenbestände und polizeiliche Datenumgangsformen plädiert. Anders als *Poscher et al.* wird nämlich davon ausgegangen, dass das polizeiliche Informationswesen durch sein zu erwartendes Anwachsen unter dem Eindruck des Massendatenphänomens zumindest partiell den Charakter einer Massendatensammlung und – hier stimmen auch *Poscher et al.* zu – (behördlichen)

2300 *Golla* Kriminologisches Journal 52 (2020), 149 (160).
2301 Siehe dazu bereits oben unter S. 172 ff.
2302 *Poscher/Kilchling*, Entwicklung eines periodischen Überwachungsbarometers für Deutschland, 2021, S. 4.
2303 *Poscher/Kilchling/Landerer*, Überwachungsbarometer für Deutschland, Ein Modellkonzept, 2022, S. 7.
2304 *Poscher/Kilchling/Landerer*, Überwachungsbarometer für Deutschland, Ein Modellkonzept, 2022, S. 10.

Vorratsdatenspeicherung aufweisen kann.[2305] Zudem ist aus hier vertretener Perspektive vor allem die Koppelung der sich aus dem polizeilichen Informationswesen ergebenden Datenmacht an die Institution der Polizei, die einen regen internen Datenaustausch pflegt, besonders relevant im Kontext staatlicher Überwachung und Kontrolle. *Poscher et al.* erfassen zwar den maßnahmenbezogenen Umfang staatlicher Massendatenüberwachung in ihrer Breite, ermöglichen aber nur bedingt eine Abschätzung institutioneller Machtakkumulation im Kontext staatlicher Überwachung und Kontrolle. Hinzukommt, dass polizeiliche Datenmacht – anders als etwa die von Nachrichtendiensten – wegen der polizeilichen Exekutivbefugnisse und ihrer Bedeutung im System strafrechtlicher Sozialkontrolle besonders folgenreich für einen größeren Teil der Bevölkerung sein kann. Zu erfassen wären für das polizeiliche Informationswesen der Umfang und die Intensitätsgrade informationeller Durchdringung durch polizeiliche Datenbestände und Informationspraktiken. Eine umfassende Erfassung des polizeilichen Informationswesens nach diesen Parametern müsste sodann auch eine sektorale Aufschlüsselung – etwa nach einer bestimmten Datenumgangsform (automatisierte Datenanalyse, Datenabgleiche, et cetera) – ermöglichen, um für bestimmte Ausprägungen dieses sozio-technischen Großsystems empirisch fundierter Intensitätsgrade hinsichtlich polizeilicher Überwachung und Kontrolle festzustellen.[2306]

Voraussetzung für eine solche Erfassung des Informationswesens durch das Überwachungsbarometer wäre – neben der Dokumentation der von *Poscher et al.* in den Blick genommenen Überwachungsmaßnahmen – die Erfassung und Zusammenführung der Informationen über polizeiliche Datenbeständen und tatsächlich anfallende Datenumgänge. Da ein Großteil des polizeilichen Datenumgangs im Informationswesen als Eingriffe von geringer Intensität gelten dürfte, ließe sich eine Dokumentationspflicht nicht aus der Verfassung ableiten,[2307] sondern wäre Ausdruck einer gestaltenden Sicherheitspolitik. Allerdings werden Datenabrufe in den polizeilichen Informationssystemen ohnehin bereits protokolliert. Zudem werden durch die Digitalisierung der polizeilichen Informationspraktiken – etwa

2305 *Poscher/Kilchling*, Entwicklung eines periodischen Überwachungsbarometers für Deutschland, 2021, S. 6.

2306 So *Poscher/Kilchling/Landerer*, Überwachungsbarometer für Deutschland, Ein Modellkonzept, 2022, 13 für das Überwachungsbarometer insgesamt.

2307 *Poscher/Kilchling*, Entwicklung eines periodischen Überwachungsbarometers für Deutschland, 2021, S. 6.

in Form der Verwendung von Smartphones zum Datenabgleich im Einsatz –immer mehr Formen des polizeilichen Datenumgangs datenmäßig abbildbar, sodass das polizeiliche Informationswesen zunehmend Anknüpfungspunkte für die Etablierung einer reflexiven Überwachungspraxis bietet, die sich sodann auch ins Überwachungsbarometer einspeisen ließen. Im Idealfall wäre eine – vor allem durch das polizeiinterne Datenschutzkontrollregime[2308] ermöglichte – Nachverfolgung der Verarbeitungshistorie eines Datums von der Erhebung bis zur Löschung möglich. Dies wäre indessen ein notwendiger Zwischenschritt, um die Überwachungslast durch das polizeiliche Informationswesen in abstrakteren Größenordnungen aggregiert darzustellen. So ließen sich etwa Aussagen darüber treffen, welcher Anteil der Bevölkerung datenförmig in den polizeilichen Datenbeständen zu einem bestimmten Zeitpunkt abgebildet ist. Denkbar wäre es auch, zu ermitteln, welches Datenvolumen und welche Datenqualität in bestimmten Bereichen zu einem bestimmten Zeitpunkt erreicht ist, was Rückschlüsse auf den Intensitätsgrad der informationellen Aufschlüsselung bestimmter Phänomenbereiche und Personencluster geben könnte. Dabei sollten die Daten so aggregiert werden, dass sie auch wieder auf bestimmte Regionen, Behörden oder Datenbestände und Datenumgangsformen heruntergebrochen werden können und so ein granulares Bild des polizeilichen Informationswesens ermöglichen können. Inwieweit in diesen Aggregationen persönliche Merkmale zu den betroffenen Personenkreisen und sonstige Informationen zu individuellen Umständen der Datenverarbeitung rekonstruierbar sein sollten, lässt sich hier nicht abschließend diskutieren. *Poscher et al.* halten dies aus forschungsökonomischen Gründen für zu aufwendig und aus datenschutzrechtlicher Perspektive für nicht wünschenswert.[2309] Allerdings würde man insoweit auch eine Möglichkeit verspielen, diskriminierende Tendenzen und Dynamiken im polizeilichen Informationswesen zu identifizieren, was zu einer gerechteren polizeilichen Sozialkontrolle und rationaleren Sicherheitskultur beitragen könnte.

Die Realisierung eines solchen Überwachungsbarometers ist – vor allem in seiner periodischen Verstetigung – mit Schwierigkeiten behaftet. Bereits der einem institutionalisierten Instrument notwendigerweise vorausgehende Forschungsaufwand ist immens und braucht dementsprechend eine institutionelle Absicherung, was neben finanziellen Ressourcen vor allem

2308 Dazu sogleich im Anschluss an diesen Abschnitt.

2309 *Poscher/Kilchling/Landerer*, Überwachungsbarometer für Deutschland, Ein Modellkonzept, 2022, S. 15.

auch die Unterstützung der entsprechenden staatlichen Stellen erfordert.[2310] Diese Schwierigkeiten würden durch die vorliegend für sinnvoll gehaltene Ergänzung des Barometers in der soeben beschriebenen Weise noch einmal potenziert. Erschwert wird eine solche Ergänzung zudem durch die Heterogenität des Informationswesens, wobei allerdings das Polizei 2020-Projekt mit seinem Ziel der Homogenisierung polizeilicher Datenhaltung und -verarbeitung auch als Chance für ein erweitertes Überwachungsbarometer verstanden werden muss. Hinzu kommen zu erwartende Widerstände polizeilicher Interessenvertretungen, die sich gegen eine Überwachung der Polizei und einen „Generalverdacht" gegenüber Polizist:innen wenden. Diese Schwierigkeiten werden aber durch den potenziellen Nutzen eines solchen, um die beschriebene Erfassung des polizeilichen Informationswesens erweiterten Instruments nach hier vertretener Ansicht deutlich ausgeglichen. Zusammen mit den Datengrundlagen zu Kriminalität, die bereits bestehen und stetig ausgebaut werden, könne ein Überwachungsbarometer, das evidenzbasiert Auskunft über die staatliche bzw. polizeiliche Überwachungs- und Kontrolltätigkeit gibt, zu einer rationaleren Sicherheitskultur im oben beschriebenen Sinne[2311] beitragen. Eine insofern empirisch fundierte Rechtspolitik könnte besser über die Sinnhaftigkeit bestimmter polizeilicher Datenverarbeitungsformen diskutieren. Zudem könnten sich – da eine zu intensive Überwachung in individueller[2312] wie kollektiver[2313] Hinsicht die grundgesetzliche Verfassungsidentität berührt – neue rechtliche Grenzen für den Ausbau des polizeilichen Informationswesens ergeben.[2314]

Vor diesem Hintergrund ließe sich trotz aller Schwierigkeiten und gegen zu erwartende Widerstände von einem der Verfassungsidentität wegen gebotenem Projekt sprechen. Mit dem Überwachungsbarometer unter Einschluss des polizeilichen Informationswesen könnte ein wichtiger Akzent für eine Neujustierung der Sicherheitskultur gesetzt werden, die sich nach wie vor insbesondere durch eine Intensivierung von informationstechnologisch fundierter Überwachung und Kontrolle auszeichnet. Um das Barometer als Instrument zu institutionalisieren wäre, auch eine rechtliche Absicherung geboten. Dazu müsste ein adäquates Transparenzniveau sicher-

2310 *Poscher/Kilchling*, Entwicklung eines periodischen Überwachungsbarometers für Deutschland, 2021, S. 8.
2311 Siehe dazu oben unter S. 520.
2312 BVerfGE 156, 63 (123) – Elektronische Aufenthaltsüberwachung.
2313 BVerfGE 125, 260 (324) – Vorratsdatenspeicherung.
2314 *Poscher/Kilchling/Landerer*, Überwachungsbarometer für Deutschland, Ein Modellkonzept, 2022, S. 7 f.

heitsbehördlicher Datenbestände und Datenumgangsformen gewährleistet werden. Für das polizeiliche Informationswesen bedeutet das insbesondere die Pflicht, grundlegende Informationen über ihre Datensammlungen in öffentlich zugänglicher Form zur Verfügung zu stellen, damit besser abgeschätzt werden kann, wie Datenbestände durch welche Datenumgangsformen in der Praxis genutzt werden.[2315] Daneben könnte die Integration des polizeilichen Informationswesens in das Überwachungsbarometer wie bereits angedeutet auf das polizeiinterne Datenschutzkontrollregime zurückgreifen, das zudem unabhängig von einem Überwachungsbarometer zu intensivieren ist.

II. Ausbau des polizeiinternen Datenschutzkontrollregimes

Ob ein „umfassendes, polizeiliches Kontrollsystem" in der Gesellschaft wahrscheinlich ist, kann vor dem Hintergrund der hohen technischen Komplexität des polizeilichen Informationswesens und seiner vielfältigen gegenläufigen Entwicklungsdynamiken bezweifelt werden.[2316] Nichtsdestotrotz zeigt die Nutzung der informationstechnologischen Möglichkeiten in anderen Ländern, dass die von der digitalen Gesellschaft produzierten „Kontrollüberschüsse"[2317] durchaus zur Etablierung invasiverer Überwachungs- und Kontrollpraktiken durch insbesondere staatliche Akteure genutzt werden können.[2318] Insofern muss eine Polizei, die tatbestandlich ein immer größeres Tableau an informationellen Befugnissen hat[2319] und deren technischen Möglichkeiten sich stetig fortentwickeln,[2320] hinsichtlich der von ihr ausgeübten Sozialkontrolle in besonderer Weise ihrerseits kontrolliert werden. Das gilt umso mehr, als dass neuere informationelle Pra-

2315 So schon (ohne Bezug zum Überwachunsbarometer) *Bäcker* in T. Dreier/V. Fischer/van Raay ua (Hrsg.), Informationen der öffentlichen Hand - Zugang und Nutzung, 229 (246 f.), der aber bereits fordert, dass die "erforderlichen Änderungen und Neuregelungen auf einem Gesamtkonzept beruhen [müssen], das die einzelnen transparenzgewährleistenden Regelungsbausteine zueinander ins Verhältnis setzt".

2316 *Heinrich,* Innere Sicherheit und neue Informations- und Kommunikationstechnologien, S. 381.

2317 *Baecker,* Studien zur nächsten Gesellschaft, S. 169; *Nassehi,* Muster, S. 43.

2318 Für die Nutzung der Informationstechnologie zu Überwachungs- und Kontrollzwecken in autoritären wie demokratischen Kontexten siehe bereits oben S. 17 f.

2319 Interview 8, Pos. 39.

2320 Interview 14, Pos. 44.

xen wie die automatisierte Anwendung zur Datenanalyse oder Formen des Predictive Policing sich regelmäßig durch eine gewisse technische Opazität auszeichnen. Um hier weiterhin eine Überprüfbarkeit von Ergebnissen dieser technischen Erkenntnisinstrumente sicherzustellen, ist eine Verstärkung der Verfahrenssicherungen notwendig, die im Wechselspiel mit der technologischen Entwicklung evolvieren müssen. Im Sicherheitsdiskurs erfolgt die Entscheidung für die Einführung neuer Technologien häufig nach der Prämisse, dass alles, was technisch möglich ist, auch praktisch umgesetzt und rechtlich zugelassen werden sollte. Es scheint nur konsequent, dies nicht nur für technische Verfahren zu fordern, mit denen polizeiliche Sozialkontrolle effektiviert werden kann, sondern auch zur Verbesserung der Kontrolle der polizeilichen Sozialkontrolle. Das bereits zuvor beschriebene interne Datenschutzkontrollregime der Polizeien[2321] sollte also als rechtsstaatlich und demokratisch gebotene Erweiterung und Intensivierung der Kontrolle des polizeilichen Informationswesens begriffen und ausgebaut werden, um dessen Potenzialen für Missstände, Verselbstständigung und Dysfunktionalitäten etwas entgegenzusetzen. Für eine umfassende Kontrolle des polizeilichen Informationswesens erscheinen vor allem Strukturen relevant, die eine systematische und auf das aggregierte polizeiliche Informationshandeln in seiner Gesamtheit gerichtete Kontrolle ermöglichen. Damit soll individuellen Kontroll- und Rechtsschutzmöglichkeiten wie datenschutzrechtlichen Auskunftsrechten nicht ihre Zweckmäßigkeit abgesprochen werden. Aber eine umfassende Überwachung und Kontrolle der polizeilichen Informationsverarbeitung bezüglich ihrer Rechtmäßigkeit kann über eine solche sehr punktuelle Überprüfung, die zudem von der Geltendmachung durch individuelle Rechtsträger:innen abhängt, nicht gewährleistet werden. Um das kollektive Risikopotenzial von polizeilicher Datenverarbeitung zu adressieren und perspektivisch auch die Einbindung des polizeilichen Informationswesens in ein periodisches Überwachungsbarometer zu unterstützen, erscheint vor allem eine Intensivierung der Protokollierung polizeilichen Informationshandelns und die Stärkung der Position der Datenschutzbeauftragten geboten. Zudem sollte das Recht auf Vergessenwerden im Kontext polizeilicher Datensammlungen gesellschaftlich neu verhandelt werden.

Im Zentrum des polizeiinternen Datenschutzkontrollregimes muss die Protokollierung stehen. Schon jetzt sind in vielen polizeilichen Systemen

2321 Siehe dazu bereits oben S. 361 ff.

auch immer Verwaltungsdaten gespeichert, zu denen auch ID-Nummern, Speicher- und Änderungsdaten sowie Besitzdaten eines Datensatzes gehören. Damit ist es grundsätzlich möglich, „jede Änderung und Löschung, aber auch jede Einsicht mitsamt dem Anfrageanlass" zu dokumentieren.[2322] Die Protokollierungspraktiken in den deutschen Polizeibehörden sind zurzeit nicht einheitlich.[2323] Idealerweise sollte – wo technisch möglich – jeder Datenumgang durch Polizist:innen so protokolliert werden, dass eine vollständige Rekonstruktion und Überprüfung des Umgangs erfolgen kann. In vielen polizeilichen Informationssystemen scheint dies – dem vorstehenden Zitat von *Kathke* nach – bereits zumindest technisch möglich zu sein. Zudem sollten neue Potenziale zur Protokollierung polizeilichen Informationshandelns – etwa in Form des Datenabgleiches im Einsatz über Smartphones und ähnliches – ebenfalls genutzt werden, um die Interaktionen von Beamt:innen mit dem polizeilichen Informationswesen möglichst zu dokumentieren und damit einer Kontrolle zugänglich zu machen.[2324] Dafür müssen jedoch auch ausreichende Ressourcen zur Verfügung gestellt werden.

Eine Kontrolle der so massenhaft anfallenden Protokolldaten lässt sich händisch auch auszugsweise kaum mehr bewerkstelligen, sodass auch hier über die Nutzung technischer Verfahren nachgedacht werden sollte. Die Verarbeitung von Massendaten mit dem Ziel über mustererkennende Algorithmen bestimmte Verhaltensformen zu identifizieren, lässt sich nicht nur auf abweichendes Verhalten in bestimmten Kriminalitätsfeldern, sondern theoretisch auch auf das aggregierte polizeiliche Informationshandeln anwenden. Insofern erscheint die Entwicklung von KI-gestützten Auswertungsverfahren zur Detektierung von rechtswidrigen oder in einem weiteren Sinne schädlichen Informationspraktiken im Informationswesen der Polizei denkbar. Damit könnten nicht nur missbräuchliche Informationspraktiken wie die immer wieder medial bekannt werdenden intentionalen Datenmissbräuche illuminiert werden.[2325] Vielmehr wäre damit auch die Möglichkeit einer laufenden systematischen Überprüfung eines Großteils polizeilicher Handlungen eröffnet, mit der Defizite und Fehlentwicklun-

2322 *Kathke*, Überlieferungsbildung aus, Fachverfahren Überlegungen zu POLAS BW der Polizei Baden-Württemberg, 2015, S. 16.
2323 Siehe dazu bereits oben S. 400.
2324 Siehe zur möglichen praktischen Umsetzung eines solchen Kontrollrahmens etwa *Fährmann* MultiMedia und Recht 24 (2021), 775 (778).
2325 Siehe dazu bereits Fn. 730.

gen identifiziert ausgeglichen werden könnten. Ein naheliegendes Anwendungsfeld wäre die Identifizierung von eventuell (unintentional) diskriminierenden Polizeipraktiken. Zumindest ließe sich ermitteln, in welchem Umfang und Verhältnis etwa Daten von Personen aus bestimmten sozioökonomischen Schichten vorhanden sind und verarbeitet werden. Mit der algorithmengestützten Überprüfung des eigenen Informationshandelns könnte die Polizei zudem versuchen, ihre blinden Flecken aufzuhellen und stereotype Wahrnehmung durch das Füllen von lückenhaften Datenbeständen zu korrigieren; das würde aber vor allem voraussetzen, dass Daten nicht nur aus denjenigen soziodemografischen Schichten erhoben werden, über die die Polizei ohnehin schon zahlreiche Datenpunkte besitzt, sondern auch dort, wo der polizeiliche Blick bisher nur oberflächlich schaut.[2326] Damit könnte ein wichtiger Schritt in Richtung einer polizeilichen Sozialkontrolle gegangen werden, die in der pluralen Gesellschaft der Spätmoderne mit ihren vielfältigen normativen Ordnungen weniger starke Verzerrungen – wie die überdurchschnittliche Erfassung von insbesondere ausländischen Minderheiten durch staatliche Sozialkontrolle – erzeugt.

Neben die Protokollierung sollte auch eine starke interne Kontrolle durch die behördlichen Datenschutzbeauftragten der Polizeien treten. Teilweise sind die Datenschutzbeauftragten schon in einer wirkmächtigen Position und können dem gesetzlichen Leitbild entsprechend beraten und vor allem auch recht frei kontrollieren. Allerdings scheint es durchaus auch Bedarf an einer (weiteren) Stärkung der Position beziehungswiese Aufstockung der zur Verfügung stehenden Ressourcen, etwa in Form von Personal zu geben, um eine adäquate Aufgabenerfüllung zu gewährleisten. Denn für eine dem gesetzlichen Leitbild entsprechende Beratung und Kontrolle ist ein umfassender Einblick in das polizeiliche Informationswesen in seinen spezifischen Ausformungen und Wirkweisen im jeweiligen Zuständigkeitsbereich vonnöten. Nur dann ist die erforderliche Einbindung in informationstechnologische Verfahren und Entwicklungsprozesse und damit eine optimale Nutzung von Beratungs- und Kontrollkapazitäten möglich. Vor allem auch die fortlaufende Entwicklung der Datenverarbeitungstechnologie gebietet eine stetige Anpassung der Handlungsmöglichkeiten der polizeilichen Datenschutzbeauftragten. Mit Blick auf die Fachkulturen der Technik, des Rechts und der Polizeifachlichkeit, die dem polizeilichen Informationswesen sein Gepräge geben, erscheint es zudem geboten, die dafür erforderliche Expertise im polizeiinternen Datenschutzkontrollregime

2326 In diese Richtung beispielsweise *Brayne,* Predict and surveil, S. 106.

entsprechend abzubilden, wobei hier sowohl die personelle Aufstockung, also die Einrichtung einer Datenschutzabteilung, als auch die personelle Weiterbildung, also die weitere Professionalisierung der einzelnen Datenschutzbeauftragten, als gangbare Wege erscheinen.

Die Polizei mag diese Forderungen nach engerer Überwachung und Kontrolle ihres informationellen Handelns durch Ausweitung der Protokollierung und Intensivierung der internen Überprüfung durch die behördlichen Datenschutzbeauftragten als Misstrauen wahrnehmen. Gerade über solche Überwachungs- und Kontrollmechanismen wird aber das in einem demokratischen Rechtsstaat so essenzielle Vertrauen in die staatliche Handlungsmacht überhaupt erst möglich. Vor diesem Hintergrund sollte auch der bisweilen von polizeilichen Interessensvertretungen kritisierte „Generalverdacht", unter den man Polizei und Polizist:innen zu Unrecht gestellt sieht, in positivem Sinne umgedeutet werden. Anstatt das gesellschaftliche Verlangen nach einer rechenschafspflichtigen Polizei abzuwerten, sollte das Stehen unter „Generalverdacht" vielmehr Teil des polizeilichen Selbstverständnisses werden, denn: eine demokratische Polizei ist eine kontrollierte Polizei.[2327]

Ein letzter, aus hier vertretener Sicht zentraler Aspekt des internen Datenschutzkontrollregimes muss das Recht auf Vergessenwerden i.S.d. Art. 17 DS-GVO im Kontext des polizeilichen Informationswesens sein, in gesetzlichem Duktus häufig etwas weniger verfassungssprachlich als Löschungsverpflichtung und (dieser Verpflichtung vorgelagert) Aussonderungsprüffristen gefasst. Während die gesellschaftliche Medienentwicklung über Jahrtausende darauf bedacht war, das Erinnern und Aufbewahren von Informationen zu optimieren, dreht sich die Notwendigkeit von Vergessen und Erinnern im digitalen Zeitalter um.[2328] *Mayer-Schönberger* argumentiert, dass Vergessen in der massendatenbasierten Informationsgesellschaft nützlich und notwendig ist.[2329] Das gilt auch für das polizeiliche Informationswesen, dass als je nach Datenlage als mehr oder weniger detailliertes Kriminalitätsgedächtnis der Gesellschaft konzeptualisiert werden kann. Insofern müssen Strategien und Technologien des digitalen Vergessens für die polizeilichen Datenbestände entwickelt werden.[2330] Dabei müssen neben

2327 *Derin/Singelnstein,* Die Polizei: Helfer, Gegner, Staatsgewalt, S. 350.
2328 *Mayer-Schönberger* in Reiter/Wittmann-Tiwald (Hrsg.), Goodbye privacy - Grundrechte in der digitalen Welt, 9 (9).
2329 *Mayer-Schönberger,* Delete.
2330 *Burkhardt,* Digitale Datenbanken, S. 339.

der dem Massendatenphänomen inhärenten Problem eines nicht mehr zu bewältigenden Datenvolumens für die Polizei vor allem auch Erwägungen bezüglich einer zu intensiven Sozialkontrolle, wie sie etwa Ausdruck in *Popitz* These von der Präventivwirkung des Nichtwissens (man könnte vorliegend auch ergänzen: des Vergessens) gefunden haben, eine wesentliche Rolle für die Ausgestaltung von organisationalen Vergessensprozessen spielen. Denn die Digitalisierung von gesellschaftlichen Prozessen lässt immer mehr Datenströme entstehen, die durch die informationstechnologische Entwicklung der Polizeien erfasst werden können. Einmal ins polizeilichen Informationswesen aufgenommen, können lange Aussonderungsprüffristen (bei Straftäter:innen regelmäßig zehn Jahre, siehe etwa § 77 BKGA) und rechtlich abgesicherte Dynamiken wie die Mitziehautomatik[2331] sedimenthafte Datenakkumulationen entstehen lassen: In einer Gesellschaft, die soziale Prozesse zunehmend über digitale Daten erfasst und festhält, werden mit dieser rechtlich-technischen Struktur auf lange Sicht mehr neue Daten gesammelt und „erinnert", als dass sie „vergessen" werden. Der Entwicklungsstand von Technologien zur Datenhaltung und Datenauswertung wird dann letztlich darüber entscheiden, ob die Polizei diese Datenansammlung zur Effektivierung ihrer Sozialkontrolle wird nutzen können oder ob sie orientierungslos auf der dadurch bewirkten Datenflut umhertreiben wird. Eine Auseinandersetzung mit einem zweckmäßigen Verhältnis von Erinnern und Vergessen im Kontext polizeilicher Informationsverarbeitung erfordert sicherlich einerseits eine tiefergehende Auseinandersetzung mit gegenwärtigen Speicherpraktiken, die bisher eher selten und dann auch nur schlaglichtartig durch Tätigkeitsberichte von Bundes- oder Landesdatenschutzbeauftragten beleuchtet wurde. Hier wäre eine systematischere Durchdringung der polizeilichen Datenbestände geboten, wozu auch der beschriebene Ausbau des polizeiinternen Datenschutzkontrollregimes beitragen könnte. Andererseits ist aber auch ein gesellschaftlicher Aushandlungsprozess mit dem Recht auf Vergessenwerden im Rahmen des polizeilichen Informationswesens verbunden. Letztlich ist es eine demokratische Wertentscheidung, was kollektiv über abweichendes Verhalten erinnert und was vergessen werden soll. Die für eine Entscheidung anzustellende Abwägung ist keine leichte, denn die Funktionsfähigkeit des polizeilichen Informationswesens und damit der Polizei selbst liegt mit in der Waagschale. Insofern geht es um (berechtigte) Sicherheitsbedürfnisse

2331 Siehe dazu bereits oben S. 258 f.

der Gesellschaft. Gleichzeitig gebietet das Grundgesetz die Resozialisierung von Rechtsbrecher:innen,[2332] wozu auch ein Verblassen von Stigma und Vorwurf im kollektiven Gedächtnis gehören muss. Insofern lässt sich eine (annähernd) totale Sozialkontrolle durch die Polizei und weitere staatliche Akteure, die ein entsprechend umfassendes Erinnern als Grundvoraussetzung hat, nicht mit dem Grundgesetz vereinbaren. Die insoweit komplexen, multipolaren Abwägungsfragen werden sich nicht pauschal für *die* Kriminalität treffen lassen, sondern erfordern eine fortgesetzte und tiefgehende Auseinandersetzung mit dem polizeilichen Informationswesen und von ihm registrierten Devianzformen mitsamt ihrer Akteursfelder. Gerade diese Schwierigkeiten machen die Entscheidung über Vergessen oder Erinnern von abweichendem Verhalten aber zu einer zentralen und bisher ungelösten Herausforderung der spätmodernen Sicherheitskultur.

2332 *Di Fabio* in *Dürig/Herzog/R. Scholz,* Grundgesetz, Art. 2 Rn. 216 f.

Epilog

Was wird die Zukunft der Polizei im Zeitalter der Massendaten sein? Wie schon im Rahmen des Szenariendesigns[2333] angeklungen, lässt sich das vom gegenwärtigen Standpunkt aus kaum abschätzen. Das Phänomen der Massendaten und die es umgebenden Technologien sind größtenteils noch jung und entwickeln sich schnell. Laufend kommen neue Verfahren und Anwendungsmöglichkeiten auf, sodass sich schon in ein, zwei oder fünf Jahren ein völlig anderes Bild als das hier gezeichnete zeigen kann. Im Gegensatz zu diesen Unwägbarkeiten von polizeilicher Technologie-Entwicklung und der davon beeinflussten Sozialkontrolle lässt sich mit Sicherheit sagen, dass die Zukunft des Verhältnisses von Polizei und Informationstechnologie maßgeblich davon abhängt, wie die Gesellschaft beide Aspekte wahrnimmt und erlebt.[2334] Deshalb – es sei hier noch einmal betont – sind die sozio-technischen Imaginationen, die sich die Gesellschaft von ihrer Zukunft macht, so relevant – sowohl in ihrer stabilisierenden als auch in ihrer disruptiven Wirkung:

> „Imaginaries operate as both glue and solvent, able – when widely disseminated and effectively performed – to preserve continuity across the sharpest ruptures of innovation or, in reverse, to upend firm worlds and make them anew."[2335]

Wie schon zuvor mit den drei kondensierten Szenarien gezeigt, existieren dabei verschiedene affirmative und kritische Vorstellungen von technologisch vermittelten Zukünften nebeneinander. Sie beeinflussen einander, streiten miteinander, einige verblassen, andere erstarken. Gerade diese evolutive Fluktuation macht dabei auf ein zentrales und wichtiges Merkmal sozio-technischer Imaginationen aufmerksam: Sie verweisen auf die Handlungsfähigkeit sozialer Gruppen und Individuen, Technologie aktiv zu gestalten, anstatt von ihr determiniert zu werden.[2336] Damit werden Un-

2333 Siehe oben unter S. 496 ff.
2334 *Chan* in McDaniel/Pease (Hrsg.), Predictive policing and artificial intelligence, 41 (41).
2335 *Jasanoff* in Jasanoff/Kim (Hrsg.), Dreamscapes of modernity, 1 (29).
2336 *Chan* in McDaniel/Pease (Hrsg.), Predictive policing and artificial intelligence, 41 (50).

bestimmtheit, Kontingenz, Sprunghaftigkeit und Kreativität menschlicher und gesellschaftlicher Entwicklung gegen die Determiniertheit einer starr auf technologischen Fortschritt fixierten Erzählung in Stellung gebracht.[2337]

Dabei fällt es allzu leicht, den sozio-technischen Wandel, wie er sich etwa im polizeilichen Informationswesen darstellt, zu ignorieren, so lange er sich als im Wesentlichen konsequenzlos für das eigene Leben erweist. Eine solche Position kann sich die Gesellschaft, anders als das einzelne Individuum jedoch nicht leisten.[2338] Insoweit ist sie aber auf Akteur:innen angewiesen, die die von *Jasanoff* betonte politische Natur von Imaginationen über und die eigentliche Entwicklung und Implementierung von Technologie anerkennen und danach handeln.[2339] Technologie und die Zukünfte, die sie ermöglicht, sind – um noch einmal zu *Kranzbergs* Eingangszitat zurückzukehren weder gut, noch schlecht, aber eben auch nicht neutral. Auf jeden Fall sind sie jedoch – wie *Jasanoff* auch für die dazugehörigen Imaginationen feststellt – politisch. Daraus ergeben sich Gestaltungsmöglichkeiten, aber auch Gestaltungsbedarfe. Um letztere wahrnehmen zu können, braucht es vor allem nach wie vor eine solide Wissensbasis über polizeiliche Informationsverarbeitung unter dem Eindruck des Massendatenphänomens. Neben fortgesetzter Forschung sollte diese, wie dargelegt, auch durch ein Überwachungsbarometer und das polizeiinterne Datenschutzkontrollregime ermöglicht werden. Auf dieser Grundlage kann dann eine gesellschaftliche und zu Regulierungszwecken vor allem auch rechtswissenschaftliche Auseinandersetzung mit den technologischen Möglichkeitsräumen erfolgen und die Wünschbarkeit ihrer Materialisierung angeleitet durch widerstreitende sozio-technische Imaginationen auf sachlicherer Grundlage verhandelt werden. Denn ebenso wie wir nicht übermäßig optimistischen Visionen anhängen sollten, die potenziell problematische Auswirkungen des technologischen Wandels ignorieren oder beschönigen,[2340] sind auch überzogene dystopische Imaginationen, die informationstechnologisch vermittelte Sozialkontrolle per se ausschließlich mit Unterdrückung und Unfreiheit gleichsetzen, wenig hilfreich.

2337 *Jasanoff* in Jasanoff/Kim (Hrsg.), Dreamscapes of modernity, 1 (23).
2338 *Chan* in McDaniel/Pease (Hrsg.), Predictive policing and artificial intelligence, 41 (55).
2339 *Jasanoff* in Jasanoff/Kim (Hrsg.), Dreamscapes of modernity, 321 (335).
2340 *Chan* in McDaniel/Pease (Hrsg.), Predictive policing and artificial intelligence, 41 (55 f.).

Letztlich muss es darum gehen, auch unter den Bedingungen der technologischen Gesellschaft, die eine technologisch vermittelte Sozialkontrolle ebenso wie eine technologisch vermittelte Kriminalität beinhaltet, laufend nach einem verhältnismäßigen und gesellschaftlich verträglichen Ausgleich zu suchen: Einerseits muss der Normalität und sogar Nützlichkeit von abweichendem Verhalten und als Kriminalität etikettierter Devianz im Kontext eines gesellschaftlichen Normbestandes[2341] Raum verbleiben; andererseits darf dies nicht zulasten einer nachdrücklichen und effektiven Adressierung von schädlichen Ausläufern krimineller Verhaltensweisen gehen.

Unabhängig von der Frage, ob die technologische Entwicklung einen „Homo digitalis" hervorbringen wird, der weitaus schlauer als wir Homo sapiens ist,[2342] werden wir eine Handlungsmacht aufbauen, deren Fundierung „both in our brains and in the larger digital space" uns wie nie zuvor die Möglichkeit geben wird, eine Welt zu schaffen, die schön, gerecht und gut oder aber von Ungleichheit, Ungerechtigkeit und Leid geprägt sein wird.[2343] Wichtig scheint vor diesem Hintergrund vor allem, in einer sich pluralisierenden Sozialordnung eine gewisse Toleranz gegenüber harmlosen Formen der Devianz zu entwickeln bzw. beizubehalten und zu fördern, ohne dabei in eine Gleichgültigkeit bezüglich negativer Auswirkungen von abweichendem Verhalten auf das soziale Geflecht zu verfallen. Damit einhergehen muss auch eine gewisse Gelassenheit in der Sicherheitskultur, freilich ohne Sicherheitsbedrohungen nur noch apathisch zu begegnen. Denn mit zunehmender Datafizierung aller oder der meisten gesellschaftlichen Felder entstehen Informationsüberschüsse, mit denen – wie es schon jetzt nach Terroranschlägen oder Amokläufen regelmäßig der Fall ist – sich das Geschehene hätte vorhersagen lassen können, hätte man nur besser gesucht, registriert und analysiert. Allerdings sind auch die besseren Verarbeitungsverfahren zur Suche, Registrierung und Analyse von abweichenden Mustern in Massendaten und damit zur Identifizierung von deviantem Verhalten immer nur aus Menschenhand und damit einerseits grundsätzlich fehlbar und andererseits in ihren Möglichkeiten durch unsere limitierte Wahrnehmung – die sich in eine begrenzte Funktionslogik von datenverarbeitenden Algorithmen übersetzt – beschränkt.[2344] An dieser Stelle ist

2341 *Durkheim* in Sack/König (Hrsg.), Kriminalsoziologie, 3 (5 f., 7 f.).
2342 *T. Walsh,* 2062, S. 21.
2343 *T. Walsh,* 2062, 21 f.
2344 *Burkhardt,* Digitale Datenbanken, S. 313 f.

erneut zu betonen, was bereits unzählige Male geschrieben und gesagt worden ist: Sicherheit ist ein letztlich unerreichbarer Zustand. So tragisch jeder Tod, jede Beeinträchtigung durch unsichere Zustände und Entitäten ist: Das getriebene Verlangen nach mehr und lückenloser Sicherheit braucht klare Limitierungen. Das gilt umso mehr, als etwa von *Barabas et al.* vorgeschlagen wird,[2345] den polizeilichen Blick mittels datengetriebener Erkenntnisverfahren auf gesamtgesellschaftliche Fehlentwicklungen auszuweiten, um diagnostisch die sozialen Ursachen von Kriminalität zu ergründen und zu beheben. Den damit verbundenen Ausweitungstendenzen polizeilicher Macht ist eine entschiedene Absage zu erteilen. Mag die Idee auch im Ursprung gut gemeint sein – die beste Kriminalpolitik ist wohl nach wie vor eine gute Sozialpolitik (*von Liszt*) – muss das gesamtgesellschaftliche Phänomen der Kriminalität auch gesamtgesellschaftlich bearbeitet werden. Es ist Aufgabe einer praxisbezogenen und gleichzeitig hinterfragenden Kriminologie, in Kooperation mit den zivilgesellschaftlichen Akteuren der verschiedenen gesellschaftlichen Felder notwendigen Handlungsbedarf aufzuzeigen und über den kriminalpolitischen Diskurs Reformen anzustoßen.

2345 *Barabas/Virza/Dinakar* ua in Friedler/C. Wilson (Hrsg.), Proceedings of the 1st Conference on Fairness, Accountability and Transparency, 62.

Thesenhafte Zusammenfassung der Arbeit

Prolog

Ordnungsproduktion in der Spätmoderne – als Ergebnis sozialer Kontrolle – ist einem Wandel unterworfen, der einerseits durch die vielfältigen sozialen Umbruchsprozesse und Spannungen, andererseits aber auch durch die damit verwobenen Fortschritte insbesondere in der Informationstechnologie bedingt wird. Als wichtigste Akteurin im System staatlicher Sozialkontrolle ist die Polizei von diesem Wandel in erheblichem Maße betroffen. Wie sich staatliche und polizeiliche Sozialkontrolle in den nächsten Jahren entwickeln, wird die Grundbedingungen gesellschaftlichen Zusammenlebens im weiteren Verlauf des 21. Jahrhunderts maßgeblich prägen.

1. Theoretische Grundannahmen und Konzepte

1.1 Daten sind Repräsentationen (häufig nur technisch) wahrnehmbarer Reize und stehen vor allem mit maschineller Verarbeitung in Verbindung. Dabei hängt die „Form" der Daten ganz wesentlich von Erhebungs- und Aufzeichnungssensoren ab, es gibt also keine absolut objektiven Daten („raw data is an oxymoron").

1.2 Information ist begrifflich stärker mit menschlicher Wahrnehmung verbunden. Sie ist ggü. Daten höher strukturiert und hat ein semantisches Potenzial (Bedeutung); daher ist sie zentral für menschliches Verhalten, für Gesellschaft und mithin auch für die Polizei.

1.3 Massendaten meint die rasante und hochvoluminöse Produktion vielfältiger Daten. In der Folge sind wir immer abhängiger von technischen Datenverarbeitungsverfahren. Zentral hierfür sind Algorithmen, d.h Prozesse mit denen - häufig mittels KI - automatisiert große Datenmassen verarbeitet und bestimmte Ergebnisse produziert werden. Die konkrete Wahl der Datenverarbeitungstechnologien bestimmt unser Weltbild.

1.4 Da Daten in ihrer Erscheinungsweise von den zu ihrer Erhebung und Aufbereitung eingesetzten Technologien abhängen, sind sie immer durch die Wahl der entsprechenden Apparaturen konstruiert (Konstruiertheit von Daten). Gleichzeitig folgt aus der Bedeutung von Daten für die (menschliche) Informationsgewinnung, dass die konkrete

Wahl der Datenverarbeitungstechnologien unser Weltbild bestimmt (Konstruktion durch Daten).

1.5 Dieses konstruktivistische Element setzt sich auch in der datenförmigen Erfassung von Menschen durch: Die dabei entstehenden, datenbasierten Repräsentationen lassen sich als Datendoubles bezeichnen, was das aus persönlichen Datenfragmenten zusammengestellte, digitale Profil einer lebenden Person meint, auf dessen Grundlage Bewertungen und Urteile in verschiedenen Zusammenhängen getroffen werden können. Ein solches Datendouble bleibt jedoch immer fragmentarisch, einseitig und vor allem auch instabil, da Bedeutungszusammenhänge durch einen Wandel der zur Verfügung stehenden Daten und Verarbeitungstechniken stetig umgeformt werden. Die Gleichsetzung von Datendouble mit einem real zu verdächtigendem Datensubjekt begegnet insofern Bedenken.

1.6 Die mediale Evolution, die eine Anreicherung unserer Lebenswelt mit Daten in verschiedensten Formationen mit sich bringt, hat insofern profunde Auswirkung auf die menschliche Weltwahrnehmung und unsere Fähigkeit, der Welt Sinn und Bedeutung abzuringen. Die Wahrnehmung einer zunehmend datenvermittelten Welt – im Rahmen der Arbeit als Datenwahrnehmung bezeichnet - hat neben epistemischen Folgen auch materielle Auswirkung, indem im Wege der Neuroplastizität die Neurobiologie menschlicher Gehirne betroffen ist. Als Phänomen scheint dies Vor- und Nachteile mit sich zu bringen. Jedenfalls aber müssen Menschen stärker lernen, mit Daten umzugehen (Datenliterarität), um die Potenziale und Risiken von aus - hauptsächlich über technische Verfahren - Daten gewonnenen Informationen identifizieren zu können.

1.7 Für das Verständnis des Technologie-Begriffes in der vorliegenden Arbeit ist auf die Extensionstheorie *McLuhans* sowie – in stärkerem Maße – auf das grundlegende Technologie-Verständnis der Science and Technology-Studies zurückgegriffen. Technologie wird also als Erweiterung des menschlichen Körpers und Geistes begriffen, die in ihrer konkreten Ausformung aber kontingent ist und von den Besonderheiten ihrer sozialen Umgebung abhängig ist, von der sie wesentlich mit produziert wird (Sozio-Technizität).

1.7.1 Als erster von drei näher beschriebenen Informationstechnologie-Typen gelten die Datenbanken als paradigmatische Medieninfrastruktur der Gegenwart. Jedoch verbergen sich hinter dem Begriff – ganz im Sinne der Sozio-Technität von Technologie –

ganz verschiedene und vielfältige konkrete Ausgestaltungen von Daten- bzw. Informationssammlungen. Nach *Burkhardt* sind die konkreten medientechnischen Verfahren der Versammlung, Verwaltung und Verarbeitung digitaler Daten maßgeblich für eine treffende Auseinandersetzung mit Datenbanken, um zu verhindern, dass „die heterogene Vielgestaltigkeit der digitalen Datenbankkultur hinter der vermeintlichen Einheit der Datenbank als symbolischer Form" verschwindet. Wichtig ist im Rahmen der Datenbank-Technologie einmal mehr deren konstruktivistisches Potenzial: Datenbanken stellen konstruierte Wissensordnungen dar, die Daten nach vorformulierten Kategorien und Konzepten versammeln und somit niemals die Wirklichkeit in Gänze, sondern immer nur in einer mehr oder weniger starken Begrenztheit darstellen können.

1.7.2 Daneben sind die bereits genannten Algorithmen eine zentrale Technologie für die Polizei im Massendaten. Technisch ist darunter zunächst eine bestimmte Abfolge von logischen Operationen zur Erfüllung einer spezifischen Aufgabe gemeint. Im Kontext der Datenbank werden Algorithmen dazu eingesetzt, Dateninputs, wie etwa eine Suchanfrage, in einen Output zu verwandeln, der dann informationell für Menschen nutzbar ist. Im Massendatendiskurs hat sich für Algorithmen ein darüber hinausreichendes Verständnis etabliert, das – regelmäßig verbunden mit dem Überbegriff der künstlichen Intelligenz – Algorithmen zunehmend als Techniken der Entscheidungsunterstützung und -findung begreift und ihnen dabei Handlungsmacht zuschreibt. Nichtsdestotrotz bleiben Algorithmen menschengemachte und auf von Menschen produzierten Daten trainierte Instrumente, welche die soziostrukturellen Eigenheiten unserer Gesellschaft(en) abbilden und reproduzieren.

1.7.3 Schließlich spielen Informationssysteme eine zentrale Rolle bei der Betrachtung des polizeilichen Informationswesens, da sie die technische Materialisierung der Interaktionsmöglichkeiten des Menschen mit Datenbanken darstellen. Insofern ist das Design von Informationssystemen folgenreich für (polizeiliche) Informationsverarbeitung, da hier ebenfalls wichtige Entscheidungen darüber getroffen werden, welche Informationen zu welchen Zwecken wie genutzt werden. Dieser Umstand macht Informationssysteme auch aus regulatorischer Perspektive interessant,

da sich an dieser Stelle grundlegende Weichen für polizeiliches Informationshandeln stellen lassen.

1.8 Soziale Kontrolle meint die Verhinderung devianten und die Beförderung normbefolgenden Verhaltens (*Durkheim*). Jede soziale Ordnung übt soziale Kontrolle aus; gleichzeitig ist Normabweichung eine gesellschaftliche Konstante und in Teilen sogar notwendig, um Normbestände zu erneuern. Eine totale Aufklärung von Devianz ist zudem nicht wünschenswert, wenn Normen in der Breite der Gesellschaft ihre Wirkung behalten sollen (Präventivwirkung des Nichtwissens nach *Popitz*). Mit einer zunehmenden staatlichen Datenbasis, die sich sowohl aus eigenen Datensammlungen als auch aus dem Zugriff auf Sammlungen nicht-staatlicher Akteure zusammensetzen kann, wandelt sich polizeiliche Sozialkontrolle fundamental: Sie wird totaler, also umfassender, teilweise „sanfter", paradoxerweise aber gleichzeitig auch selektiver und mitunter „härter" im Sinne einer zunehmend brutal-unterwerfenden Sozialkontrolle.

2. Historisches

2.1 Betrachtet man die Geschichte der Polizei so ist diese vor allem auch als institutionelle Entfaltung und Weiterentwicklung von organisationsbezogener Informationstechnologie zu begreifen. Von Entstehung der modernen deutschen Polizei in der zweiten Hälfte des 19. Jahrhunderts an bestimmt der Umgang mit dem Informationsüberschuss der modernen Gesellschaft in großen Teilen die Polizeiarbeit. Dabei bleiben die epistemischen Grundlagen kriminalistischer Konzepte trotz des Wandels der Technologien stabil: Stets geht es darum, auf Grundlage rationalen oder zumindest rational scheinenden Vorgehens kriminelle Typen in den angesammelten Daten zu identifizieren.

2.2 Diese Typisierungen reichen vom den „Verbrecheralben" des Kaiserreichs bis zu den gegenwärtigen Hinweissystemen in den Informationssystemen der Polizei. Welchen Verbrechen ein entgrenztes polizeiliches Informationswesen Diener sein kann zeigen die Erfahrungen des Dritten Reiches. Gegenwärtig befindet sich die polizeiliche Informationsverarbeitung in der Entwicklungsstufe, die in Anlehnung an Egbert als Datafizierung bezeichnet wird. Sie ist charakterisiert durch die Umwandlung aller der Polizei zur Verfügung stehenden Informationen in frei kombinierbare, digitale Daten und durch die algorithmisch mediatisierten Datenanalyse als neuem Modus der Wissensgenerierung. Unter diesem Begriff sind eine Vielzahl von Verarbeitungsverfahren

versammelt, die auf einen fundamentalen Wandel polizeilicher Informationsverarbeitung hindeuten, was das polizeiliche Handel generell und die Polizei als Organisation grundlegend verändert.

3. Normative Rahmenbedingungen

3.1 Wichtigstes Grundrecht im Kontext polizeilicher Informationsverarbeitung im Anschluss an Datenerhebungen ist das Grundrecht auf informationelle Selbstbestimmung. Zentral für eine grundrechtskonforme Regulierung war und ist insofern der Grundsatz der Zweckbindung, der eine Verarbeitung personenbezogener Daten grundsätzlich nur zum Erhebungszweck zulässt und eine zweckändernde Weiterverarbeitung an weitere Voraussetzungen knüpft. Zwar besteht dieses Grundmodell verfassungsrechtlich weiterhin, mit der Rechtsprechung zur zweckwahrenden Weiternutzung und dem Grundsatz der hypothetischen Datenneuerhebung, die auch eine praktikable Anpassung polizeilicher Datenverarbeitung an die Dynamiken des Massendatenzeitalters ermöglichen sollte, hat das Bundesverfassungsgericht den Zweckbindungsgrundsatzes jedoch ein stückweit aufgeweicht.

3.2 Mit dem individuenbezogenen Grundrechteschutz des Grundgesetzes fällt es schwer, Informationshandeln zu adressieren, dass auch durch die Aggregation von Daten über Viele freiheitsgefährdend wirkt. Erste Versuche der dogmatischen Operationalisierung dieser staatlichen Freiheitsgefährdung sind die Überwachungsgesamtrechnung und das auf ihr fußende Periodische Überwachungsbarometer, die als Ansätze zur Quantifizierung der durch sicherheitsbehördliches Informationshandeln ausgehenden Freiheitsgefahr ausdrücklich zu begrüßen sind.

3.3 Die spätmoderne Sensibilität für Risiken hat zu einer Ausweitung des polizeilichen Blicks in das gefahrenabwehr- und strafrechtliche Vorfeld geführt, die sich auch schon länger in der diesbezüglichen verfassungsrechtlichen Ausgestaltung niederschlägt. Das polizeiliche Vorfeld ist dabei ein wesentlicher Motor für das Anwachsen polizeilicher Datenbestände und damit für die Datafizierung der Polizeiarbeit.

3.4 Maßgeblich für die normative Analyse des polizeilichen Informationswesens ist auch die sog. JI-Richtlinie, die im Zuge der Datenschutzreform der Europäischen Union polizeiliche Datenverarbeitung unional überformt hat. Dabei wird der Harmonisierungsprozess zwischen nationalem Recht und EU-Datenschutzrecht, auch wenn die JI-Richtlinie von allen dazu aufgerufenen Gesetzgebern im Wesentlichen umgesetzt ist, noch Zeit in Anspruch nehmen. Wichtigste Neuerung für die deut-

sche Polizei dürfte die Starkmachung prozeduralen Grundrechteschutzes durch die Reform sein.

3.5 Gegenwärtig ist das als polizeiliches Informationssystem INPOL bekannte Verbundsystem, das zentral für das Informationswesen der deutschen Polizei ist, noch in Dateien, d.h. grundsätzlich abgegrenzten Datensilos organisiert. Aufgrund des Wunsches nach besserer Interoperabilität der polizeilichen Daten, also letztlich qualitativ besserer Datenvernetzung und damit -verarbeitung, wurde jedoch 2016 mit dem Projekt Polizei 2020 ein großer, bereits in der Vergangenheit erfolglos gebliebener Überarbeitungsversuch der polizeilichen Informationsarchitektur angestoßen. Eines der zentralen Ziele von Polizei 2020 ist eine verbesserte Datenhaltung – im Kern ein großer Datenspeicher mit unterschiedlich ausgestalteten Zugriffsrechten – um auf dieser Grundlage insbesondere auch mit Massendatenverarbeitungsverfahren mehr Informationen aus den verfügbaren Daten gewinnen zu können.

3.6 In der gegenwärtigen Überarbeitung des polizeilichen Informationswesens wird das für die polizeiliche Informationsverarbeitung generell problematische Verhältnis von Normativität und Faktizität besonders deutlich. Die rechtliche Steuerung polizeilichen Informationsumgangs funktioniert nur bedingt, was vor allem an einer häufig nur auf Polizeipraxis reagierenden bzw. sie abbildenden Gesetzgebung liegt. So hat noch immer keine Anpassung der die näheren Dateninhalte regelnden BKADV stattgefunden und auch die Regelung des § 91 BKAG zeugt von einem gesetzgeberischen Regelungsverständnis, das die normative Kraft des Faktischen akzeptiert anstatt die Rechtswirklichkeit proaktiv durch informierte Normierung zu gestalten versucht.

3.7 Die Regulierungsherausforderungen für die Polizeigesetzgeber sind jedoch groß: So ergeben sich etwa durch Datenbestände, die von privaten Akteuren akkumuliert werden und als latente Datenquelle der Polizei dienen können, oder auch durch die zunehmend zum Einsatz kommenden Analysesysteme (etwa § 25a HSOG) anspruchsvolle Regelungsfelder. So ist etwa für Analysesysteme mit dem hierzu jüngst ergangenen Bundesverfassungsgerichtsurteil den betroffenen Gesetzgebern einmal mehr eine unzureichende Regelungspraxis attestiert worden. Zwar ist ein dialogischer Aushandlungsprozess zwischen Verfassungsrechtsprechung und Gesetzgebung grundsätzlich normal; die gegenständlichen Regelungen waren jedoch bereits zuvor von großen Teilen der Literatur zutreffend als problematisch eingestuft worden. Die Neuregelung des § 25a HSOG zeigt insofern zwar erhöhte legislati-

ve Bemühungen. Ob damit aber auch tatsächlich regulierend auf die mit der Norm adressierte Datenverarbeitung eingewirkt wird, muss sich erst noch zeigen.

3.8 In der Zusammenschau der einfachgesetzlichen Rahmenbedingungen des polizeilichen Informationswesens zeigen sich trotz reger gesetzgeberischer Bemühungen seit 2016 strukturelle Defizite in der Regulierung. Emblematisch hierfür sind etwa die vor allem von *Bäcker* herausgearbeiteten legislativen Fehlleistungen im BKAG (i.e. das Verhältnis von §§ 12, 16, 18 und 19 BKAG zueinander), die einen integralen Teil des polizeilichen Informationsverbundes betreffen. Im Ergebnis zeigt sich, dass eine (insbesondere gesetzgeberische) Auseinandersetzung mit den internen Datenverarbeitungsprozessen bei der Polizei zu wenig stattgefunden hat; erforderlich erscheint vor dem Hintergrund des bisher häufig nur punktuellen Regelungsmodus eine systematische Überarbeitung der polizeilichen Informationsordnung.

3.9 Für das Verständnis polizeilichen Informationshandelns ist neben den klassischen Befugnisnormen und – so es sie denn, wie etwa im BKAG, gibt – den Regelungen zur Struktur der eingesetzten Datenbestände und Informationssysteme vor allem auch das Datenschutzkontrollregime integral. Dieses Regulativ mit seiner personellen (Datenschutzbeauftragte) und technisch-organisatorischen Komponente bestimmt maßgeblich mit, ob und wie die normativen Rahmenbedingungen in der Rechtswirklichkeit umgesetzt werden. Gerade diese Transformationsleistung macht das Datenschutzkontrollregime zu einem guten Ansatzpunkt für eine nähere Erforschung polizeilichen Informationshandelns.

4. Rekonstruktion

4.1 Das polizeiliche Informationswesen als Gesamtkomplex ist gekennzeichnet durch eine multikausale Bedingtheit, die durch die Trias aus Informationstechnik, Polizeipraktiken und Recht ausgemacht wird. Diese drei Aspekte stehen miteinander in Wechselwirkung und erfordern laufend Anpassungsleistungen aneinander, aber auch an die Umwelt, ermöglichen auf diese Weise aber auch erst ein Funktionieren des polizeilichen Informationswesens und seine Interaktion mit der Gesellschaft.

4.2 Polizeiliches Handeln wird (noch weiter) zunehmend zu Wissensarbeit, das polizeiliche Arbeitsumfeld wird immer stärker mit vielfältigen informationstechnologischen Instrumenten angereichert. Datenlitera-

rität und Datenwahrnehmung sind insofern Aspekte, die es in Zukunft bei der Aus- und Weiterbildung von Polizist:innen zu beachten gilt. Die „neuen" Instrumente ermöglichen prinzipiell eine bessere Kontrolle des polizeilichen Informationshandelns; gleichzeitig entstehen hierdurch neue Machtpotenziale, die immer mit Missbrauchsrisiken einhergehen.

4.3 Mit „Polizei 2020" sollen Datenquellen vereinheitlicht und vernetzt werden. Es ist das zentrale Datafizierungsprojekt und führt zu einer Intensivierung der Datennutzung, die Polizeiarbeit effektiver machen soll. Das Projekt ist aber nicht unumstritten und verläuft weniger reibungslos als geplant.

4.4 Die Datenbasis der Polizei nimmt im Umfang durch vielfältige Kontaktpunkte (Smartphone, Online-Wache, usw.) mit der Gesellschaft stark zu. Zusammen mit der – teilweise geplanten, teilweise bereits eingetretenen – Leistungssteigerung der Datenverarbeitungsprozesse entsteht so zunehmend eine sozio-technische Struktur, die in größerem Umfang als bisher Informationen über soziale Konflikte ins Hellfeld trägt, wo sie dann auch effektiver polizeilich bearbeitet werden können.

4.5 Neuere Datenverarbeitungsverfahren wie etwa die automatisierte Anwendung zur Datenanalyse (§ 25a HSOG) setzten für ihre informationelle Effektivität auf Massendatenlogiken, was strukturell und funktional Expansionsdynamiken von Datenbeständen und Datenverarbeitungsverfahren begünstigt. Damit setzen sich diese Verfahren in ein Spannungsverhältnis zu zentralen Prinzipien des europäischen und deutschen Datenschutzes.

4.6 Durch die wachsende technologische Abhängigkeit gerät die Polizei zugleich in eine neue Fragilität. Das polizeiliche Informationswesen wird immer anfälliger für Pannen, Angriffe und ausufernde Komplexität.

4.7 Aus einer Globalperspektive erscheint das polizeiliches Informationswesen als sozio-technisches Großsystem, das intern auf die Interaktion mit den Polizist:innen angewiesen ist, wobei die Interaktion als Kondensationspunkt für die Umwandlung von datenförmig vorgehaltener Information in handlungsleitendes Wissen dient. Zudem ist das Informationswesen auf Interaktion mit gesellschaftlichen Feldern angewiesen, damit es nach seiner Funktionslogik funktionieren kann. Mit steigender Komplexität verselbstständigt das Großsystem und lässt sich nur noch begrenzt erfassen und steuern. Mit zunehmender infor-

mationeller Durchdringung gesellschaftlicher Felder und dadurch in gesteigertem Maße möglicher polizeilicher Ordnungsproduktion drohen Freiheitssphären dysfunktional zu verkümmern – ohne dass dies intentional von den polizeilichen Akteur:innen im Informationswesen beabsichtigt sein muss.

5. Zukünfte der Polizei: Szenarien

5.1 Sozio-technische Imaginationen sind kollektiv getragene, institutionell stabilisierte und öffentlich vorgetragene Visionen einer wünschenswerten Zukunft, die durch ein gemeinsames Verständnis sozialen Lebens und sozialer Ordnung getragen werden und durch Fortschritte in Wissenschaft und Technologie erreichbar sind oder scheinen. Daraus folgt eine Gestaltbarkeit technologischen Fortschritts, die sich von Vorstellungen erwünschter, aber eben auch unerwünschter Zukünfte motivieren lassen muss. Die Arbeit entwickelt zwei aus Perspektive der grundgesetzlichen Ordnung unerwünschte Zukunftsszenarien und bringt dagegen eine erstrebenswertere Imagination in Stellung

5.2 Im Szenario der datenmächtigen Polizei der Zukünfte ist die Sicherheitskultur risikoavers und sicherheitsaffirmativ. Schutz vor Kriminalität wird ein stärkerer Stellenwert zugeschrieben als Freiheitsverlusten. Technologisch gelingt der Polizei die Transformation in eine Organisation, die Massendaten effektiv verarbeiten kann. Der Wandel der Sozialkontrolle erfolgt multidimensional, d.h. polizeiliche Sozialkontrolle wird selektiver, zugleich aber auch totaler, also umfassender, und auch sanfter. Denkbar ist auch, das ohnehin bereits marginalisierte Personen auch einer stärker disziplinierenden Kontrolle unterworfen werden.

5.3 Im Szenario der überforderten Polizei bzw. Zukunft ohne Polizei ist die Sicherheitskultur grundsätzlich nebensächlicher, den technologisch scheitert die Polizei an der Fragilität des Informationswesens, insbesondere an der ausufernden Komplexität. Der Wandel polizeilicher Sozialkontrolle lässt sich vor allem als Rückgang formeller Sozialkontrolle beschreiben. In der Folge kommt es zu einer Privatisierung und Kommodifizierung von Sicherheitsproduktion.

5.4 Im erstrebenswerteren Szenario der Polizei als spezialisiertes Konfliktlösungsinstrument ist die Sicherheitskultur rational. Technologisch funktioniert das polizeiliche Informationswesen nach einer dualen Dynamik. Auf der einen Seite existiert eine technisch wenig aufgerüstete, bürgernahe Alltagspolizei, auf der anderen Seite stehen informationstechnologisch mächtige Spezialpolizeibehörden zur Adressierung

gravierender Kriminalitätsrisiken der Spätmoderne. Der Wandel der polizeilichen Sozialkontrolle lässt sich mit dem Begriff der Modularität umschreiben. In der allgemeinen Ordnungsproduktion fungiert eine bürgernahe Polizei als eine Akteurin unter vielen. In gravierenden Konfliktsituationen agieren die Spezialbehörden mit dem Ziel engmaschiger Kontrolle in ihren Aufgabengebieten.

6. Rechtspolitische Stellungnahme

6.1 Das polizeilichen Informationswesen ist aufgrund der mangelhaften polizeilichen Informationsordnung rechtlich nur begrenzt steuerungsfähig, was an seiner Komplexität, aber auch an einer unzureichenden dogmatischen Durchdringung liegt.
6.2 Die Polizeigesetzgeber werden ihrer Steuerungsverantwortung nicht gerecht, da sie häufig polizeiliches Informationshandeln nicht aktiv gestalten, sondern reaktiv legitimieren.
6.3 Die dogmatische Bearbeitung sollte einen Fokus auf kollektive bzw. transsubjektive Freiheitsgefährdung legen; für Letztere ist etwa die sog. Überwachungsgesamtrechnung bzw. das periodische Überwachungsbarometer ein erster Ansatzpunkt
6.4 Vor allem eine robuste Kontrollarchitektur ist integral zur Steuerung des polizeilichen Informationswesens; dazu gehören die Stärkung des polizeilichen Datenschutzes, die Ausweitung von Protokolldatenprüfungen sowie ein Überdenken der Löschungsfristen von Daten insb. im Bereich alltäglicher Kriminalität

Epilog

Unter den Bedingungen der technologischen Gesellschaft, die eine technologisch vermittelte Sozialkontrolle ebenso wie eine technologisch vermittelte Kriminalität beinhaltet, muss laufend nach einem verhältnismäßigen und gesellschaftlich verträglichen Ausgleich gerungen werden. Dabei muss immer präsent bleiben: Sicherheit ist ein unerreichbarer Zustand. So tragisch jede Beeinträchtigung ist: Das Verlangen nach mehr und lückenloser Sicherheit braucht klare Limitierungen. Das gilt umso mehr, als immer wieder vorgeschlagen wird, der Polizei weitere Befugnisse und Aufgaben zu geben. Es gilt: Kriminalität kann als gesamtgesellschaftliches Phänomen nicht allein durch eine Institution bearbeitet werden. Es ist vor allem auch Aufgabe einer praxisbezogenen und gleichzeitig hinterfragenden Kriminologie, in Kooperation mit der Zivilgesellschaft notwendigen Handlungsbe-

darf aufzuzeigen und über den kriminalpolitischen Diskurs Reformen anzustoßen.

Literaturverzeichnis

92. Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder, Gemeinsame Prüfung der Falldatei Rauschgift deckt gravierende Mängel auf - Konsequenzen für polizeiliche Datenverarbeitung notwendig, 2016.

Aaron Loh/Kenneth Soo/Hui-lin Xing, Predicting Sexual Orientation based on Facebook Status, http://cs229.stanford.edu/proj2016/report/LohSooXing-PredictingSexualOrientationBasedOnFacebookStatusUpdates-report.pdf (Stand: 01.10.2023).

Abbühl, Anicee, Der Aufgabenwandel des Bundeskriminalamtes, Von der Zentralstelle zur multifunktionalen Intelligence-Behörde des Bundes, Stuttgart ua 2010 (Zugl.:Freiburg, Univ., Diss., 2009-10).

Abel, Ralf Bernd, Datenschutz in Anwaltschaft, Notariat und Justiz, H. 63 – Schriftenreihe der Neuen juristischen Wochenschrift, 2. Aufl., München 2003 (zitiert: *Abel*).

Ackoff, Russel L., From data to wisdom , Journal of Applied Systems Analysis 16 (1989), 3–9.

Ackroyd, Stephen/Harper, Richard/Hughes, John A. ua, New technology and practical police work, The social context of technical innovation, Buckingham 1992 (zitiert: *Ackroyd/Harper/Hughes/Shapiro/Soothill*).

Adam Crawford/Karen Evans, Crime Prevention and Community Safety, in: *Leibling, Alison/Maruna, Shadd/McAra, Lesley* (Hrsg.), The Oxford Handbook of Criminology, Oxford 2017.

Aden, Hartmut/Fährmann, Jan, Datenschutz-Folgenabschätzung und Transparenzdefizite der Techniknutzung Zeitschrift für Technikfolgenabschätzung in Theorie und Praxis 29 (2020), 24–29.

Aden, Hartmut/Fährmann, Jan, Defizite der Polizeirechtsentwicklung und Techniknutzung Zeitschrift für Rechtspolitik 2019, 175–178.

Aden, Hartmut/Fährmann, Jan, Wie lassen sich Informationseingrife der Polizei wirksam gesetzlich begrenzen?, Ein Ausblick am Beispiel der GPS-Ortung gestohlener Gegenstände vorgänge. Zeitschrift für Bürgerrechte und Gesellschaftspolitik 227 (2019), 95–106.

Ahlf, Ernst-Heinrich, Das Bundeskriminalamt als Zentralstelle, Wiesbaden 1985 (Zugl.: Speyer, Hochsch. für Verwaltungswiss., Diss., 1985).

Albers, Marion, Die Determination polizeilicher Tätigkeit in den Bereichen der Straftatenverhütung und der Verfolgungsvorsorge, Berlin 2001 (Zugl.: Bielefeld, Univ., Diss., 1999).

Albrecht, Peter-Alexis, Der Weg in die Sicherheitsgesellschaft, Auf der Suche nach staatskritischen Absolutheitsregeln, Berlin 2010 (zitiert: *P.-A. Albrecht*).

Aly, Götz/Roth, Karl Heinz, Die restlose Erfassung, Volkszählen, Identifizieren, Aussondern im Nationalsozialismus, Bd. 14767 – Fischer Die Zeit des Nationalsozialismus, 2. Aufl., Frankfurt am Main 2005 (zitiert: *Aly/K. Roth*).

Amoore, Louise, Security and the incalculable Security Dialogue 45 (2014), 423–439.

Amoore, Louise/Raley, Rita, Securing with algorithms: Knowledge, decision, sovereignty Security Dialogue 48 (2017), 3–10.

Anderson, Charles, The end of theory: The data deluge makes the scientific method obsolete.

Andrej, Stephan, Umgang des BKA mit Minderheiten unter besonderer Bercksichtigung der Minderheit der Sinti und Roma, in: *Bundeskriminalamt* (Hrsg.), Der Nationalsozialismus und die Geschichte des BKA. Spurensuche in eigener Sache; Ergebnisse - Diskussionen - Reaktionen; Dokumentation des Kolloquiums zum Forschungsbericht zur BKA-Historie vom 6. April 2011, Köln 2011, S. 37–44.

Andrejevic, Mark/Gates, Kelly, Big Data Surveillance: Introduction SS 12 (2014), 185–196.

Arzt, Clemens, Verbunddateien des Bundeskriminalamts – Zeitgerechte Flurbereinigung Neue Juristische Wochenschrift 2011, 352–354.

Assmann, Aleida/Assmann, Jan, Das Gestern im Heute. Medien und soziales Gedächtnis, in: *Merten, Klaus/Schmidt, Siegfried J./Weischenberg, Siegfried* (Hrsg.), Die Wirklichkeit der Medien, Wiesbaden 1994, S. 114–140.

August, Vincent, Technologisches Regieren, Der Aufstieg des Netzwerk-Denkens in der Krise der Moderne. Foucault, Luhmann und die Kybernetik, Bd. 8 – Edition transcript, Bielefeld 2021 (zitiert: *August*).

Aulehner, Josef, Polizeiliche Gefahren- und Informationsvorsorge, Grundlagen, Rechts- und Vollzugsstrukturen, dargestellt auch im Hinblick auf die deutsche Beteiligung an einem Europäischen Polizeiamt (EUROPOL), Berlin 1998 (Zugl.: Speyer, Hochsch. für Verwaltungswiss., Diss., 1995).

Awad, Elias M./Ghaziri, Hassan M., Knowledge management, Upper Saddle River, NJ 2004 (zitiert: *Awad/Ghaziri*).

Babuta, Alexander/Oswald, Marion, Machine learning predictive algorithms and the policing of future crimes, Governance and oversight, in: *McDaniel, John L. M./Pease, Ken* (Hrsg.), Predictive policing and artificial intelligence, London, New York 2021, S. 214–236.

Bäcker, Matthias, Big Data und Sicherheitsrecht, in: *Hoffmann-Riem, Wolfgang* (Hrsg.), Big Data - Regulative Herausforderungen, 2018, S. 167–172.

Bäcker, Matthias, Der Umsturz kommt zu früh: Anmerkungen zur polizeilichen Informationsordnung nach dem neuen BKA-Gesetz, https://verfassungsblog.de/der-umsturz-kommt-zu-frueh-anmerkungen-zur-polizeilichen-informationsordnung-nach-dem-neuen-bka-gesetz/ (Stand: 01.10.2023).

Bäcker, Matthias, Kriminalpräventionsrecht, Eine rechtsetzungsorientierte Studie zum Polizeirecht, zum Strafrecht und zum Strafverfahrensrecht, Tübingen 2015 (Zugl.: Hamburg, Univ., Habil-Schr., 2014/15).

Bäcker, Matthias, Terrorismusabwehr durch das Bundeskriminalamt, Bd. 1137 – Schriften zum öffentlichen Recht, 31. Aufl., Berlin 2009 (zitiert: *Bäcker*, Terrorismusabwehr).

Bäcker, Matthias, Transparenz von Datensammlungen der Sicherheitsbehörden, in: *Dreier, Thomas/Fischer, Veronika/van Raay, Anne ua* (Hrsg.), Informationen der öffentlichen Hand - Zugang und Nutzung, 2016, S. 229–248.

Bäcker, Matthias/Hornung, Gerrit, EU-Richtlinie für die Datenverarbeitung bei Polizei und Justiz in Europa, Einfluss des Kommissionsentwurfs auf das nationale Strafprozess- und Polizeirecht ZD 2012, 147–152.

Baecker, Dirk, Studien zur nächsten Gesellschaft, Bd. 1856 – Suhrkamp-Taschenbuch Wissenschaft, Frankfurt am Main 2007 (zitiert: *Baecker*).

Baeza-Yates, Ricardo/Ribeiro-Neto, Berthier, Modern information retrieval, The concepts and technology behind search, 2. Aufl., Harlow, England [etc.] 2011 (zitiert: *Baeza-Yates/Ribeiro-Neto*).

Bailey, Diane E./Barley, Stephen R., Beyond design and use: How scholars should study intelligent technologies Information and Organization 30 (2020).

Bain, Andy, Horses and Horsepower, Fingerprints and Forensics: The Development of Technology and Law Enforcement, in: *Bain, Andy* (Hrsg.), Law Enforcement and Technology, London 2016, S. 9–25.

Bain, Andy/Carsone, Louis P./Conser, James A. ua, Technology and the Future of Policing, in: *Bain, Andy* (Hrsg.), Law Enforcement and Technology, London 2016, S. 115–135.

Barabas, Chelsea/Virza, Madars/Dinakar, Karthik ua, Interventions over Predictions: Reframing the Ethical Debate for Actuarial Risk Assessment, in: *Friedler, Sorelle A./Wilson, Christo* (Hrsg.), Proceedings of the 1st Conference on Fairness, Accountability and Transparency, 2018, S. 62–76.

Barck, Die Erfahrung mit der Neuregelung des deutschen Fahndungswesens in Baden Kriminalistische Monatshefte 3 (1929), 170–171.

Barocas, Solon/Rosenblat, Alex/boyd, danah ua, Data & Civil Rights: Technology Primer SSRN Journal 2014.

Beck, Ulrich, Risikogesellschaft, Auf dem Weg in eine andere Moderne, Bd. 3326 – Edition Suhrkamp, Frankfurt am Main 1996 (zitiert: *Beck*).

Becker, Andreas, Schon wieder Datenmissbrauch bei der Polizei in MV Nordkurier v. 31.05.2022 (abrufbar unter https://www.nordkurier.de/mecklenburg-vorpommern/schon-wieder-datenmissbrauch-bei-der-polizei-in-mv-3148395805.html) (Stand: 01.10.2023).

Becker, Peter, Dem Täter auf der Spur, Eine Geschichte der Kriminalistik, EBL-Schweitzer, Darmstadt 2011 (zitiert: *P. Becker*).

Bellinger, Gene/Castro, Durval/Mills, Anthony, Data, Information, Knowledge, and Wisdom, http://www.systems-thinking.org/dikw/dikw.htm (Stand: 01.10.2023).

Bennett Moses, Lyria/Chan, Janet, Algorithmic prediction in policing: assumptions, evaluation, and accountability Policing and Society 28 (2018), 806–822.

Berger, Peter Ludwig/Luckmann, Thomas, The social construction of reality, A treatise in the sociology of knowledge, New York 1966 (zitiert: *Berger/Luckmann*).

Bergien, Rüdiger, »Big Data« als Vision., Computereinführung und Organisationswandel in BKA und Staatssicherheit (1967-1989) Zeithistorische Forschungen/Studies in Contemporary History 258-285 14 (2017), 258–285.

Beydoun, Khaled Ali, The New State of Surveillance: Societies of Subjugation Washington and Lee Law Review (Wash. & Lee L. Rev) 79 (2022), 769–845.

Bieler, Sam, Police militarization in the USA: the state of the field PIJPSM 39 (2016), 586–600.

Black, Donald J., Toward a General Theory of Social Control, Fundamentals, Saint Louis 2014 (zitiert: *Black*).

Blackler, Frank, Knowledge, Knowledge Work and Organizations: An Overview and Interpretation Organization Studies 16 (1995), 1021–1046.

Bloch-Wehba, Hannah, Automation in Moderation Cornell Int'l L.J. 53 (2020), 41–96.

Bloch-Wehba, Hannah, Content Moderation as Surveillance Law & Society: Private Law - Intellectual Property eJournal 2021, 102–144.

Boers, Klaus (Hrsg.), Kriminologische Perspektiven. Wissenschaftliches Symposium zum 70. Geburtstag von Klaus Sessar, 2012.

Bogner, Alexander/Littig, Beate/Menz, Wolfgang, Interviews mit Experten, Wiesbaden 2014 (zitiert: *Bogner/Littig/Menz*).

Bonin, Irina, Grundrechtsschutz durch verfahrensrechtliche Kompensation bei Maßnahmen der polizeilichen Informationsvorsorge, Schriften zum Recht der Inneren Sicherheit - Band 20, Stuttgart 2012 (zitiert: *Bonin*).

Borell, Anne/Schindler, Stephan, Polizei und Datenschutz Datenschutz und Datensicherheit 43 (2019), 767–773.

Borges, Jorge Luis, Die Bibliothek von Babel, Erzählungen, Nr. 9497 – Reclams Universal-Bibliothek, Stuttgart 2016 (zitiert: *Borges*).

Bowker, Geoffrey C., Memory practices in the sciences, Inside technology, Cambridge, Mass. 2005 (zitiert: *Bowker*).

Boyd, Danah Michele, It's complicated, The social lives of networked teens, New Haven 2014 (zitiert: *Boyd*).

boyd, danah/Crawford, Kate, CRITICAL QUESTIONS FOR BIG DATA Information, Communication & Society 15 (2012), 662–679.

Braga, Anthony A./Weisburd, David, Conclusion, in: *Weisburd, David/Braga, Anthony A.* (Hrsg.), Police Innovation, 2019, S. 544–563.

Bratton, W. J./Malinowski, S. W., Police Performance Management in Practice: Taking COMPSTAT to the Next Level Policing 2 (2008), 259–265.

Brayne, Sarah, Big Data Surveillance: The Case of Policing Am Sociol Rev 82 (2017), 977–1008.

Brayne, Sarah, Predict and surveil, Data, discretion, and the future of policing, New York, NY 2021 (zitiert: *Brayne*).

Brayne, Sarah, Surveillance and System Avoidance Am Sociol Rev 79 (2014), 367–391.

Brey, Philip, Theorizing technology and its role in crime and law enforcement, in: *McGuire, M. R./Holt, Thomas J.* (Hrsg.), The Routledge handbook of technology, crime and justice, London, New York 2020, S. 17–34.

Brey, Philip, Theorizing technology and its role in crime and law enforcement, in: *McGuire, Michael/Holt, Thomas J.* (Hrsg.), The Routledge handbook of technology, crime and justice, London, New York, N.Y 2017, S. 17–34.

Brink, Stefan/Wolff, Heinrich Amadeus, BeckOK Datenschutzrecht.

Britz, Gabriele, Freie Entfaltung durch Selbstdarstellung, Eine Rekonstruktion des allgemeinen Persönlichkeitsrechts aus Art. 2 I GG, Tübingen 2007 (zitiert: *Britz*).

Buckel, Sonja, Subjektivierung und Kohäsion, Zur Rekonstruktion einer materialistischen Theorie des Rechts, Weilerswist 2007 (Zugl.: Frankfurt (Main), Univ., Diss., 2005).

Buil-Gil, David/Medina, Juanjo/Shlomo, Natalie, Measuring the dark figure of crime in geographic areas: Small area estimation from the Crime Survey for England and Wales The British Journal of Criminology 61 (2021), 364–388.

Buil-Gil, David/Moretti, Angelo/Langton, Samuel H., The accuracy of crime statistics: assessing the impact of police data bias on geographic crime analysis J Exp Criminol 2021.

Bundesministerium des Innern, Polizei 2020, -White Paper-.

Burczyk, Dirk, Von der Kartei zum „Datenhaus“: Zur Geschichte polizeilicher Datenhaltung Bürgerrechte & Polizei (CILIP) 2020, 16–25.

Burkhardt, Marcus, Digitale Datenbanken, Eine Medientheorie im Zeitalter von Big Data, Bielefeld, Germany 2015 (zitiert: *Burkhardt*).

Busch, Heiner, INPOL-neu. Informatisierung des polizeilichen Alltags. Bürgerrechte & Polizei (CILIP) 25 (2003), 12–19.

Butz, Felix, Die Polizei und ihr Zugriff auf DNA-Daten: eine "genetische Inquisition"? NK 33 (2021), 316–332.

Butz, Felix/Christoph, Stephan/Sommerer, Lucia ua, Automatisierte Risikoprognosen im Kontext von Bewährungsentscheidungen Bewährungshilfe 68 (2021), 241–259.

Butz, Felix/Höffler, Katrin, Cyberbiokriminalität und Cyberbiosicherheit – Kriminologische Überlegungen im Angesicht von biotechnologischen Entwicklungen, in: *Rüdiger, Thomas-Gabriel/Bayerl, P. Saskia* (Hrsg.), Handbuch Cyberkriminologie 2, Wiesbaden 2023, S. 427–455.

Caliskan, Aylin/Bryson, Joanna J./Narayanan, Arvind, Semantics derived automatically from language corpora contain human-like biases Science 356 (2017), 183–186.

Capurro, Rafael/Hjørland, Birger, The concept of information Ann. Rev. Info. Sci. Tech. 37 (2003), 343–411.

Carr, Nicholas G., The shallows, What the internet is doing to our brains, London 2020 (zitiert: *Carr*).

Carter, A. F., The West German “Bundeskriminalamt” The Police Journal 49 (1976), 199–209.

Carvalho, Henrique, The preventive turn in criminal law, Oxford monographs on criminal law and justice, Oxford 2017 (zitiert: *Carvalho*).

Castells, Manuel, Der Aufstieg der Netzwerkgesellschaft, 2017 (zitiert: *Castells*).

Chan, Janet, The future of AI in policing, Exploring the sociotechnical imaginaries, in: *McDaniel, John L. M./Pease, Ken* (Hrsg.), Predictive policing and artificial intelligence, London, New York 2021, S. 41–57.

Chan, Janet, The Technological Game Criminal Justice 1 (2001), 139–159.

Chan, Janet/Brereton, David/Legosz, Margot ua, E-policing: The Impact of Information Technology on Police Practices, Brisbane 2001 (zitiert: *Chan/Brereton/Legosz/Doran*).

Chang, Brian, From Internet Referral Units to International Agreements; Censorship of the Internet by the UK and EU COLUM. HUM. RTS. L. REV. 49 (2018), 114–212.

Chateau, Zoé/Devine-Wright, Patrick/Wills, Jane, Integrating sociotechnical and spatial imaginaries in researching energy futures Energy Research & Social Science 80 (2021).

Cheney-Lippold, John, We are data, Algorithms and the making of our digital selves, New York 2017 (zitiert: *Cheney-Lippold*).

Cheslow, Danielle, Israeli firm develops body cams with facial recognition technology Times of Israel v. 22. Januar 2022 (abrufbar unter https://www.timesofisrael.com/israeli-firm-develops-body-cams-with-facial-recognition-technology).

Chriss, James J., Social Control, An introduction, [S.l.] 2022 (zitiert: *Chriss*).

Cios, Krzysztof J., Data Mining, A Knowledge Discovery Approach, Boston, MA 2007 (zitiert: *Cios*).

Clarke, Roger, Information technology and dataveillance Commun. ACM 31 (1988), 498–512.

Cohen, S., Visions of social control, Crime, punishment and classification, Cambridge 1985 (zitiert: *Cohen*).

Cole, Simon A., Suspect Identities, A History of Fingerprinting and Criminal Identification, Cambridge 2009 (zitiert: *Cole*).

Collingridge, David, The social control of technology, London 1982 (zitiert: *Collingridge*).

Cordner, Gary, Community Policing, in: *Reisig, Michael Dean/Kane, Robert J./Bradford, Ben* (Hrsg.), The Oxford handbook of police and policing, Oxford [etc.] op. 2014, S. 148–171.

Crary, Jonathan, Suspensions of perception, Attention, spectacle, and modern culture, October Books, Cambridge, Mass 1999 (zitiert: *Crary*).

Creemers, Rogier, China's Social Credit System: An Evolving Practice of Control SSRN Journal 2018.

Curtis, Graham/Cobham, David P., Business information systems, Analysis, design, and practice, 5. Aufl., Harlow, Munich 2005 (zitiert: *Curtis/Cobham*).

Daase, Christopher, Wandel der Sicherheitskultur Aus Politik und Zeitgeschichte 2010, 9–16 (abrufbar unter https://www.bpb.de/system/files/pdf/1EH2QT.pdf) (Stand: 01.10.2023).

Dachwitz, Ingo, Datenmissbrauch durch Polizeibeamte. Keine Einzelfälle Netzpolitik.org. (abrufbar unter https://netzpolitik.org/2020/datenmissbrauch-durch-polizeibeamte-keine-einzelfaelle-nsu20-hessen/) (Stand: 01.10.2023).

Dai, Xin, Toward a Reputation State: The Social Credit System Project of China SSRN Journal 2018.

d'Alessandro, Brian/O'Neil, Cathy/LaGatta, Tom, Conscientious Classification: A Data Scientist's Guide to Discrimination-Aware Classification Big Data 5 (2017), 120–134.

Daluege, Karl, Staatsanwaltschaft und Polizei in der Verbrechensbekämpfung Deutsche Justiz 97 (1935), 1846–1850.

Dangelmaier, Tamara/Brauer, Eva, Selektive Polizeiarbeit – Raumordnung und deren Einfluss auf das polizeiliche Handeln, in: *Hunold, Daniela/Ruch, Andreas* (Hrsg.), Polizeiarbeit zwischen Praxishandeln und Rechtsordnung, Wiesbaden 2020, S. 213–233.

Dee, D. P., Bias and data assimilation Q. J. R. Meteorol. Soc. 131 (2005), 3323–3343.

Deflem, Mathieu, Deviance and Social Control, in: *Goode, Erich* (Hrsg.), The Handbook of Deviance, Hoboken, NJ 2015, S. 30–44.

Deflem, Mathieu, Introduction, in: *Deflem, Mathieu* (Hrsg.), The Handbook of Social Control, Chichester, UK 2018, S. 1–6.

Derin, Benjamin/Singelnstein, Tobias, Die Polizei: Helfer, Gegner, Staatsgewalt, Inspektion einer mächtigen Organisation, Berlin 2022 (zitiert: *Derin/Singelnstein*).

Desrosières, Alain, The politics of large numbers, A history of statistical reasoning, 2011. Aufl., Cambridge, Mass. 2011 (zitiert: *Desrosières*).

Doidge, Norman, The brain that changes itself, Stories of personal triumph from the frontiers of brain science, New York 2014 (zitiert: *Doidge*).

Doorman, Sofie/Pali, Brunilda, Underneath the Promise of Safety and Security in a 'Smart City' JEA 5 (2021), 78–110.

Dreier, Horst, Grundgesetz, Kommentar, hrsg. v. Dreier, Horst, 3. Aufl., Tübingen 2018.

Drucker, Peter F., Managing the knowledge worker Modern Office Procedures 24 (1979), 12–16.

Dürig, Günter/Herzog, Roman/Scholz, Rupert, Grundgesetz, Kommentar, Beck-online Bücher, hrsg. v. Herdegen, Matthias/Herzog, Roman/Klein, Hans H./Scholz, Rupert, 97. Aufl., München 2022.

Durkheim, Emilé, Kriminalität als normales Phänomen, in: *Sack, Fritz/König, René* (Hrsg.), Kriminalsoziologie, Frankfurt am Main 1968, S. 3–8.

Egbert, Simon, Datafizierte Polizeiarbeit – (Wissens-)Praktische Implikationen und rechtliche Herausforderungen, in: *Hunold, Daniela/Ruch, Andreas* (Hrsg.), Polizeiarbeit zwischen Praxishandeln und Rechtsordnung, Wiesbaden 2020, S. 77–100.

Egbert, Simon/Krasmann, Susanne, Predictive Policing. Eine ethnographische Studie neuer Technologien zur Vorhersage von Straftaten und ihre Folgen für die polizeiliche Praxis., Projektabschlussbericht, 2019.

Egbert, Simon/Leese, Matthias, Criminal futures, Predictive policing and everyday police work, Routledge studies in policing and society, London, New York 2021 (zitiert: *Egbert/Leese*).

Ehmann, Eugen/Selmayr, Martin/Albrecht, Jan Philipp, DS-GVO, Datenschutz-Grundverordnung : Kommentar, Beck'sche Kurz-Kommentare, 2. Aufl., München 2018 (zitiert: *Ehmann/Selmayr/J. Albrecht*).

Eisenstadt, Shmuel N., Beyond Collapse, in: *Yoffee, Norman* (Hrsg.), The collapse of ancient states and civilizations, Tucson 1988, S. 236–243.

Ekblom, Paul, Crime, situational prevention and technology: the nature of opportunity and how it evolves, in: *McGuire, Michael/Holt, Thomas J.* (Hrsg.), The Routledge handbook of technology, crime and justice, London, New York, N.Y 2017, S. 353–374.

Eliot, T. S., The rock, A pageant play written for performance at Sadler's Wells Theatre, 28 May - 9 June 1934 on behalf of the Forty-Five Churches Fund of the Diocese London, 3. Aufl., London 1934 (zitiert: *Eliot*).

Ellul, Jacques, The Technological Society, Bd. 390 – A Vintage book V, New York 1964 (zitiert: *Ellul*).

Ericson, Richard Victor/Haggerty, Kevin D., Policing the risk society, Toronto 1997 (zitiert: *Ericson/Haggerty*).

Fährmann, Jan, Mehr Transparenz durch technische Innovationen?, Wie Technik polizeiliche Personenkontrollen effektiver und transparenter machen könnte MultiMedia und Recht 24 (2021), 775–779.

Farrall, Stephen/Karstedt, Susanne, Respectable citizens - shady practices, The economic morality of the middle classes, Clarendon studies in criminology, Oxford, New York, NY 2020 (zitiert: *Farrall/Karstedt*).

Ferguson, Andrew G., Big Data and Predictive Reasonable Suspicion U. Pa. L. Rev. 163 (2015), 327-410.

Ferguson, Andrew G., The rise of big data policing, Surveillance, race, and the future of law enforcement, New York 2017 (zitiert: *Ferguson*).

Finzen, Asmus, Schlechte Karten für psychisch Kranke Soziale Psychiatrie 2014, 40–43.

Fisher, Matthew/Goddu, Mariel K./Keil, Frank C., Searching for explanations: How the Internet inflates estimates of internal knowledge J Exp Psychol Gen 144 (2015), 674–687.

Flick, Uwe, Zur Qualität qualitativer Forschung — Diskurse und Ansätze, in: *Kuckartz, Udo/Grunenberg, Heiko/Dresing, Thorsten* (Hrsg.), Qualitative Datenanalyse: computergestützt, Wiesbaden 2007, S. 188–209.

Floridi, Luciano, Open Problems in the Philosophy of Information Metaphilosophy 35 (2004), 554–582.

Floridi, Luciano, Semantic Conceptions of Information, https://stanford.library.sydney.edu.au/archives/sum2010/entries/information-semantic/ (Stand: 01.10.2023).

Floridi, Luciano, The 4th revolution, How the infosphere is reshaping human reality, Oxford 2014 (zitiert: *Floridi*).

Floridi, Luciano, The philosophy of information, Oxford 2011 (zitiert: *Floridi*).

Floridi, Luciano, Two Approaches to the Philosophy of Information Minds and Machines 13 (2003), 459–469.

Folinus, Jeffery J./Madnick, Stuart E./Schutzman, Howard B., Virtual information in data-base systems SIGMOD Rec. 6 (1974), 1–15.

Foucault, Michel, Sicherheit, Territorium, Bevölkerung, Vorlesung am Collège de France, 1977 - 1978, Bd. 1 – Geschichte der Gouvernementalität / Michel Foucault. Hrsg. von Michel Sennelart, Frankfurt am Main 2004 (zitiert: *Foucault*).

Foucault, Michel, Überwachen und Strafen, Die Geburt des Gefängnisses, Bd. 184 – Suhrkamp-Taschenbuch Wissenschaft, 20. Aufl., Frankfurt am Main 2017 (zitiert: *Foucault*).

Fourcade, Marion/Gordon, Jeffrey, Learning Like a State: Statecraft in the Digital Age JLPE 1 (2020).

Frické, Martin, The knowledge pyramid: a critique of the DIKW hierarchy Journal of Information Science 35 (2009), 131–142.

Friedler, Sorelle A./Wilson, Christo (Hrsg.), Proceedings of the 1st Conference on Fairness, Accountability and Transparency, Proceedings of Machine Learning Research, 2018.

Frühauf, Ludwig/Schneider, Wolfgang/Schulz, Volker, Möglichkeiten des Einsatzes von wissensbasierten Systemen (Expertensystemen) zur Lösung polizeilicher Problemfelder, in: *Polizei-Führungsakademie* (Hrsg.), Thema heute: "Forschung und Entwicklung auf dem Gebiet der Polizeitechnik", Lübeck 1994, 9-26.

Funk, Albrecht, Die Entstehung der Exekutivpolizei im Kaiserreich, in: *Lange, Hans-Jürgen* (Hrsg.), Staat, Demokratie und Innere Sicherheit in Deutschland, Wiesbaden 2000, S. 11–27.

Gärditz, Klaus F., Sicherheitsrecht als Perspektive Zeitschrift für das Gesamte Sicherheitsrecht 2017, 1–6.

Geerdts, Torsten, Auf dem Weg zum Vorgangsbearbeitungssystem der Zukunft Moderne Polizei: Magazinreihe 2021, 6–7 (abrufbar unter https://www.behoerden-spiegel.de/wp-content/uploads/2021/04/Moderne_Polizei_1_2021.pdf) (Stand: 01.10.2023).

Gerhold, Lars/Brandes, Edda, Sociotechnical imaginaries of a secure future Eur J Futures Res 9 (2021).

Gerhold, Lars/Steinmüller, Karlheinz, Security 2025: Scenarios as an Instrument for Dialogue, in: *Peperhove, Roman/Steinmüller, Karlheinz/Dienel, Hans-Liudger* (Hrsg.), Envisioning Uncertain Futures, Wiesbaden 2018, S. 69–82.

Gerstner, Dominik, Predictive Policing als Instrument zur Prävention von Wohnungseinbruchdiebstahl, Evaluationsergebnisse zum Baden-Württembergischen Pilotprojekt P4, Bd. 50 – Forschung aktuell / Max-Planck-Institut für Ausländisches und Internationales Strafrecht, Freiburg im Breisgau 2017 (zitiert: *Gerstner*).

Gibbs, Jack P., A Theory About Control, 2019 (zitiert: *Gibbs*).

Gillespie, Tarleton, The Relevance of Algorithms, in: *Gillespie, Tarleton/Boczkowski, Pablo J./Foot, Kirsten A.* (Hrsg.), Media Technologies, 2014, S. 167–194.

Gitelman, Lisa/Jackson, Virginia, Introduction, in: *Gitelman, Lisa* (Hrsg.), "Raw data" is an oxymoron, Cambridge, Massachusetts 2013, S. 1–14.

Glaser, Barney G./Strauss, Anselm L., The discovery of grounded theory, Strategies for qualitative research, Observations, Chicago 1967 (zitiert: *Glaser/Strauss*).

Gluba, Alexander, Mehr offene Fragen als Antworten., Was für eine Bewertung des Nutzens von Predictive Policing noch zu klären ist Die Polizei 107 (2016), 53–57.

Goeschel, Albrecht/Heyer, Michael Anselm/Schmidbauer, Gertraud, Beiträge zu einer Soziologie der Polizei, Bd. 380 – Edition Suhrkamp, Frankfurt M. 1971 (zitiert: *Goeschel/Heyer/G. Schmidbauer*).

Gola, Peter/Heckmann, Dirk/Klug, Christoph ua, BDSG, Bundesdatenschutzgesetz, Gelbe Erläuterungsbücher, 13. Aufl., München 2019 (zitiert: *Gola/Heckmann/Klug/Körffer/Sandfuchs/Schmid/Schomerus/Starnecker*).

Golla, Sebastian J., Algorithmen, die nach Terroristen schürfen – „Data-Mining" zur Gefahrenabwehr und zur Strafverfolgung Neue Juristische Wochenschrift 74 (2021), 667–672.

Golla, Sebastian J., Der virtuelle Mr. Hyde, 2019.

Golla, Sebastian J., Lernfähige Systeme, lernfähiges Polizeirecht Kriminologisches Journal 52 (2020), 149–161.

Golla, Sebastian J., Missbrauch polizeilicher Informationssysteme: Neugier und Datenkriminalität Legal Tribune Online v. 16.08.2019 (abrufbar unter https://www.lto.de/persistent/a_id/37049/) (Stand: 01.10.2023).

Gorwa, Robert/Binns, Reuben/Katzenbach, Christian, Algorithmic content moderation: Technical and political challenges in the automation of platform governance Big Data & Society 7 (2020), 1-15.

Gottschall, Jonathan, The storytelling animal, How stories make us human, Boston, Mass. 2012 (zitiert: *Gottschall*).

Grace, Jamie, 'Algorithmic impropriety' in UK policing contexts, A developing narrative?, in: *McDaniel, John L. M./Pease, Ken* (Hrsg.), Predictive policing and artificial intelligence, London, New York 2021, S. 237–253.

Graf, Christoph/Hofer, Walther, Politische Polizei zwischen Demokratie und Diktatur, Die Entwicklung der preußischen Politischen Polizei vom Staatsschutzorgan der Weimarer Republik zum Geheimen Staatspolizeiamt des Dritten Reiches, Berlin 1983 (Zugl.: Bern, Univ., Habil.-Schr., 1980).

Graulich, Kurt, Die Zustimmungsbedürftigkeit der Aufhebung, Verlängerung und Änderung von Gesetzen und Rechtsverordnungen, @Frankfurt am Main, Univ., Diss., 1983, Darmstadt 1983 (zitiert: *Graulich*).

Gray, Jonathan/Gerlitz, Carolin/Bounegru, Liliana, Data infrastructure literacy Big Data & Society 5 (2018), 1-13.

Grimm, Dieter, Verfassungsrechtliche Anmerkungen zum Thema Prävention Kritische Vierteljahresschrift für Gesetzgebung und Rechtswissenschaft (KritV) 1 [69] (1986), 38–54.

Grishakova, Marina/Gramigna, Remo/Sorokin, Siim, Imaginary scenarios: On the use and misuse of fiction Frontiers of Narrative Studies 5 (2019), 112–129.

Growe, Nicolai/Gutfleisch, Ulf, Die Strafakte im Zeitalter ihrer digitalen Reproduzierbarkeit Neue Zeitschrift für Strafrecht 40 (2020), 633–639.

Grunenberg, Heiko, Empirische Befunde zur Qualität qualitativer Sozialforschung. Resultate einer Analyse von Zeitschriftenartikeln, in: *Kuckartz, Udo/Grunenberg, Heiko/Dresing, Thorsten* (Hrsg.), Qualitative Datenanalyse: computergestützt, Wiesbaden 2007, S. 210–226.

Gugerli, David, Editorial, in: *Gugerli, David/Hagner, Michael/Hampe, Michael ua* (Hrsg.), Nach Feierabend. Züricher Jahrbuch für Wissensgeschichte, Berlin 2007, S. 7–8.

Gusy, Christoph, Zukunft der Richtervorbehalte, in: *Barton, Stephan/Kölbel, Ralf/Lindemann, Michael* (Hrsg.), Wider die wildwüchsige Entwicklung des Ermittlungsverfahrens, 2015, S. 193–218.

Habermas, Jürgen, Faktizität und Geltung, Beiträge zur Diskurstheorie des Rechts und des demokratischen Rechtsstaats, Frankfurt am Main 1992 (zitiert: *Habermas*).

Hacking, Ian, The Taming of Chance, Ideas in context, Cambridge 1990 (zitiert: *Hacking*).

Hagemann, Otmar, „Ausländische Täter"als strukturelle „Opfer"?, in: *Boers, Klaus* (Hrsg.), Kriminologische Perspektiven. Wissenschaftliches Symposium zum 70. Geburtstag von Klaus Sessar, 2012, S. 139–161.

Haggerty, K. D./Ericson, R. V., The surveillant assemblage Br J Sociol 51 (2000), 605–622.

Haggerty, Kevin D., Making crime count, Toronto, Ont 2001 (zitiert: *Haggerty*).

Haigh, Thomas, "A veritable bucket of facts" origins of the data base management system SIGMOD Rec. 35 (2006), 33–49.

Hand, D. J., Dark data, Why what you don't know matters, Princeton, Oxford 2020 (zitiert: *Hand*).

Harari, Yuval Noah, Sapiens, A Brief History of Humankind, New York 2011 (zitiert: *Harari*).

Harnischmacher, Robert/Semerak, Arved, Deutsche Polizeigeschichte, Eine allgemeine Einführung in die Grundlagen, Stuttgart, Berlin [etc.] 1986 (zitiert: *Harnischmacher/Semerak*).

Härting, Niko, Zweckbindung und Zweckänderung im Datenschutzrecht Neue Juristische Wochenschrift 2015, 3284–3288.

Hebb, Donald O., The organization of behavior, A neuropsychological theory, New York, NY 1949 (zitiert: *Hebb*).

Heinrich, Stephan, Innere Sicherheit und neue Informations- und Kommunikationstechnologien, Veränderungen des Politikfeldes zwischen institutionellen Faktoren, Akteursorientierungen und technologischen Entwicklungen, Bd. 42 – Hamburger Studien zur Kriminologie und Kriminalpolitik, Berlin 2007 (zitiert: *Heinrich*).

Held, Cornelius, Intelligente Videoüberwachung, Verfassungsrechtliche Vorgaben für den polizeilichen Einsatz, Berlin 2014 (Zugl.: Würzburg, Univ., Diss., 2013-2014).

Herold, Horst, Künftige Einsatzformen der EDV und ihre Auswirkungen im Bereich der Polizei Kriminalistik Kriminalistik 28 (1974), 385–392.

Herold, Horst, Polizeiliche Informationsverarbeitung als Basis der Prävention, in: *Deutsche Kriminologische Gesellschaft* (Hrsg.), Praevention und Strafrecht. Tagungsberichte d. Dt. Kriminolog. Ges. vom 4. Dezember 1976; zur Verleihung der Beccaria-Medaille an Horst Herold, Heidelberg, Hamburg 1977, S. 23–35.

Hildebrandt, Mireille, Law As Computation in the Era of Artificial Legal Intelligence. Speaking Law to the Power of Statistics SSRN Journal 2017.

Hoehe, Margret R./Thibaut, Florence, Going digital: how technology use may influence human brains and behavior Dialogues Clin Neurosci 22 (2020), 93–97.

Hörath, Siegfried, Computer-Einsatz bei der Polizei Die Polizei 58 (1967), 129–134.

Hughes, John A., The Evolution of Large Technological Systems, in: *Bijker, Wiebe E.* (Hrsg.), The Social Construction of Technological Systems. New Directions in the Sociology and History of Technology, Cambridge, Mass. 1993, S. 51–82.

Hummer, Don/Byrne, James, Technology, innovation, and twenty-first-century policing, in: *McGuire, Michael/Holt, Thomas J.* (Hrsg.), The Routledge Handbook of Technology, Crime and Justice, London, New York, N.Y 2017, S. 375–389.

Igo, Sarah E., The Known Citizen, A History of Privacy in Modern America, Cambridge, MA 2018 (zitiert: *Igo*).

Innenministerkonferenz, Saarbrücker Agenda zur Informationsarchitektur der Polizei als Teil der Inneren Sicherheit, 2016.

Isensee, Josef, Das Grundrecht auf Sicherheit, Zu den Schutzpflichten des freiheitlichen Verfassungsstaates, Vortrag gehalten vor der Berliner Juristischen Gesellschaft am 24. November 1982, Bd. 79 – Schriftenreihe der Juristischen Gesellschaft zu Berlin, Berlin 1983 (zitiert: *Isensee*).

Janowitz, Morris, Sociological Theory and Social Control American Journal of Sociology 81 (1975), 82–108.

Jasanoff, Sheila, Future Imperfect: Science, Technology, and the Imaginations of Modernity, in: *Jasanoff, Sheila/Kim, Sang-Hyun* (Hrsg.), Dreamscapes of modernity. Sociotechnical imaginaries and the fabrication of power, Chicago, London 2015, S. 1–34.

Jasanoff, Sheila, Imagined and Invented Worlds, in: *Jasanoff, Sheila/Kim, Sang-Hyun* (Hrsg.), Dreamscapes of modernity. Sociotechnical imaginaries and the fabrication of power, Chicago, London 2015, S. 321–342.

Jasanoff, Sheila, Ordering Knowledge, Ordering Society, in: *Jasanoff, Sheila* (Hrsg.), States of knowledge. The co-production of science and social order, London, New York 2004, S. 13–45.

Jasanoff, Sheila/Kim, Sang-Hyun, Containing the Atom: Sociotechnical Imaginaries and Nuclear Power in the United States and South Korea Minerva 47 (2009), 119–146.

Jashapara, Ashok, Knowledge management, An integrated approach, Harlow 2004 (zitiert: *Jashapara*).

Jernigan, Carter/Mistree, Behram F.T., Gaydar: Facebook friendships expose sexual orientation FM 2009.

Jessup, Leonard M./Valacich, Joseph S., Information systems today, Upper Saddle River, N.J. 2003 (zitiert: *Jessup/Valacich*).

Jhering, Rudolf von, Der Kampf ums Recht, Wien 1872 (zitiert: *Jhering*).

Joh, Elizabeth E., The New Surveillance Discretion: Automated Suspicion, Big Data, and Policing Harvard Law & Policy Review Vol. 10 (2016), 15–42.

Jones, Trevor/Newburn, Tim, Private security and public policing, Clarendon studies in criminology, Oxford 1998 (zitiert: *Jones/Newburn*).

Jones, Trevor/Newburn, Tim/Reiner, Robert, 34. Policing and the police, in: *Jones, Trevor/Newburn, Tim/Reiner, Robert* (Hrsg.), The Oxford Handbook of Criminology, 2017.

Kaiser, Robert, Qualitative Experteninterviews, Wiesbaden 2014 (zitiert: *Kaiser*).

Kaminski, Margot E./Witnov, Shane, The Conforming Effect: First Amendment Implications of Surveillance, Beyond Chilling Speech University of Richmond Law Review 49 (2015), 465–518.

Kathke, Julia, Überlieferungsbildung aus, Fachverfahren Überlegungen zu POLAS BW der Polizei Baden-Württemberg, 2015.

Kehr, Thomas, Datei Gewalttäter Sport, Eine Untersuchung der Rechtsgrundlagen des BKAGs unter besonderer Berücksichtigung datenschutzrechtlicher und verfassungsrechtlicher Aspekte, Baden-Baden 2015 (Zugl.:Freiburg, Univ., Diss., 2014).

Kelle, Udo, Theoretisches Vorwissen und Kategorienbildung in der „Grounded Theory", in: *Kuckartz, Udo/Grunenberg, Heiko/Dresing, Thorsten* (Hrsg.), Qualitative Datenanalyse: computergestützt, Wiesbaden 2007, S. 32–49.

Kezer, Murat/Sevi, Barış/Cemalcilar, Zeynep ua, Age differences in privacy attitudes, literacy and privacy management on Facebook Cyberpsychology 10 (2016).

Kitchin, Rob, Big data and human geography Dialogues in Human Geography 3 (2013), 262–267.

Kitchin, Rob, Big Data, new epistemologies and paradigm shifts Big Data & Society 1 (2014), 1-12.

Kittler, Friedrich A., Grammophon, film, typewriter, Berlin op. 1986 (zitiert: *Kittler*).

Knierim, Antonie, Kumulation von Datensammlungen auf Vorrat, Vorratsspeicherung von TK- und Fluggastdaten und das Verbot umfassender Überwachung ZD 2011, 17–23.

Knöbl, Wolfgang, Polizei und Herrschaft im Modernisierungsprozeß, Staatsbildung und innere Sicherheit in Preußen, England und Amerika 1700 - 1914, Frankfurt/Main 1998 (Zugl.: Berlin, Freie Univ., Diss., 1995).

Knorr Cetina, Karin, Theoretischer Konstruktivismus, Über die Einnistung von Wissensstrukturen in sozialen Strukturen, in: *Kalthoff, Herbert* (Hrsg.), Theoretische Empirie. Zur Relevanz qualitativer Forschung, Frankfurt am Main 2008, S. 35–78.

Kollecker, Helmut, Gedanken zum kriminalpolizeilichen Meldedienst Kriminalistik 16 (1962), 49-53; 154-156.

Konferenz der Leiterinnen und Leiter der Archivverwaltungen des Bundes und der Länder, Bewertung von Fachverfahren der Polizeibehörden von Bund und Ländern, Abschlussbericht, (Version 1.1, 2020).

Kort, Yvonne de, Spotlight on aggression. ILI Magazine 2014, 10–11 (abrufbar unter https://www.win.tue.nl/~tozceleb/ILI%20magazine.pdf) (Stand: 01.10.2023).

Kowalczyk, Anneliese, Datenschutz im Polizeirecht, Reaktionen der Gesetzgeber auf das Volkszählungsgesetzurteil des Bundesverfassungsgerichts, Bd. 29 – Schriften zur öffentlichen Verwaltung, Köln 1989 (zitiert: *Kowalczyk*).

Krahmer, Florian, Mythos Überwachungsstaat – Über die alltägliche digitale Polizeiarbeit in Sachsen, in: *Rüdiger, Thomas-Gabriel/Bayerl, Petra Saskia* (Hrsg.), Digitale Polizeiarbeit, Wiesbaden 2018, S. 215–234.

Krajewski, Markus, In Formation: Aufstieg und Fall der Tabelle als Paradigma der Datenverarbeitung, in: *Gugerli, David/Hagner, Michael/Hampe, Michael ua* (Hrsg.), Nach Feierabend. Züricher Jahrbuch für Wissensgeschichte, Berlin 2007, S. 37–55.

Kranzberg, Melvin, Technology and History: "Kranzberg's Laws" Technology and Culture 27 (1986), 544–560.

Kretschmann, Andrea, Das Wuchern der Gefahr. Einige gesellschaftstheoretische Bemerkungen zur Novelle des Sicherheitspolizeigesetzes 2012 (2012), in: *Legnaro, Aldo/Klimke, Daniela* (Hrsg.), Kriminologische Diskussionstexte II, Wiesbaden 2022, S. 139–156.

Kucklick, Christoph, Die granulare Gesellschaft, Wie das Digitale unsere Wirklichkeit auflöst, Berlin 2014 (zitiert: *Kucklick*).

Kugelmann, Dieter/Dalby, Jakob, Die Neuregelung der Bestandsdatenauskunft gem. § 113 TKG und die Notwendigkeit des Grundrechtsschutzes durch Verfahren, in: *Busch, Dörte/Roggan, Fredrik* (Hrsg.), Das Recht in guter Verfassung?, 2013, S. 105–122.

Kühling, Jürgen/Buchner, Benedikt, Datenschutz-Grundverordnung, Bundesdatenschutzgesetz: DS-GVO / BDSG, [S.l.] 2020 (zitiert: *Kühling/Buchner*).

Kunz, Karl-Ludwig/Singelnstein, Tobias, Kriminologie, Eine Grundlegung, Bd. 1758 – UTB Recht, Soziologie, 7. Aufl., Bern 2016 (zitiert: *Kunz/Singelnstein*, Kriminologie).

Lageson, Sarah Esther, Digital Punishment, Privacy, Stigma, and the Harms of Data-Driven Criminal Justice, Oxford 2020 (zitiert: *Lageson*).

Lampe, Klaus von/*Knickmeier, Susanne*, Organisierte Kriminalität, Die aktuelle Forschung in Deutschland, Bd. 24 – Schriftenreihe Sicherheit, Berlin 2018 (zitiert: *Lampe/Knickmeier*).

Lana Merbach/Kai Seidensticker, Bitship Troopers - Big Data und informationsgeleitete Polizeiarbeit in Deutschland, 2019.

Laney, Douglas, 3D Data Management: Controlling Data Volume, Velocity, and Variety, 2001.

Latour, Bruno, Technology is Society Made Durable The Sociological Review 38 (1990), 103–131.

Laude, Thorsten/Reinhardt, Carsten/Bomert, Christian, Einsatz von künstlicher Intelligenz, Data Science und Big Data: Anwendungsbeispiele zur Bewältigung von Massendaten in der niedersächsischen Polizei, in: *Wehe, Dieter/Siller, Helmut* (Hrsg.), Handbuch Polizeimanagement, Wiesbaden 2022, S. 1–21.

Law, John, Introduction: Monsters, Machines and Sociotechnical Relations The Sociological Review 38 (1990), 1–23.

Lazer, David/Radford, Jason, Data ex Machina: Introduction to Big Data Annu. Rev. Sociol. 43 (2017), 19–39.

Lee, Claire Seungeun, Datafication, dataveillance, and the social credit system as China's new normal OIR 43 (2019), 952–970.

Legnaro, Aldo/Klimke, Daniela, Einleitung: Die Sekuritisierung des Lebens, in: *Legnaro, Aldo/Klimke, Daniela* (Hrsg.), Kriminologische Diskussionstexte II, Wiesbaden 2022, S. 89–102.

Lehmann, Lena, Stellungnahme Einsatz Bodycam in privaten Wohnräumen (SPolG), Gesetz zur Neuregelung der polizeilichen Datenverarbeitung im Saarland (Drucksache 16/1180), 2020.

Leman-Langlois, Stéphane, Technologies of Surveillance, in: *Deflem, Mathieu* (Hrsg.), The Handbook of Social Control, Chichester, UK 2018, S. 347–360.

Lessig, Lawrence, Code, And other laws of cyberspace, [New York, N.Y.] 1999 (zitiert: *Lessig*).

Lewinski, Kai von, Geschichte des Datenschutzrechts von 1600 bis 1977, in: *Arndt, Felix/Betz, Nicole/Farahat, Anuscheh ua* (Hrsg.), Freiheit - Sicherheit - Öffentlichkeit, 2009, S. 196–220.

Lindenau, Heinrich, Einführung, in: *Lindenau, Heinrich* (Hrsg.), Die Kriminalpolizei und ihre Hilfswissenschaften, Berlin 1908.

Lindgren, Mats/Bandhold, Hans, Scenario planning, Basingstoke 2009 (zitiert: *Lindgren/Bandhold*).

Löffelmann, Markus, Anmerkung zu BVerfG , Beschl. vom 27.5.2020 – 1 BvR 1873/13 und 1 BvR 2618/13 Zeitschrift für das Gesamte Sicherheitsrecht 3 (2020), 182–186.

Löffelmann, Markus, Die Umsetzung des Grundsatzes der hypothetischen Datenneuerhebung – Schema oder Struktur? Zeitschrift für das Gesamte Sicherheitsrecht 2 (2019), 16–22.

Lucia Zedner, Policing before and after the police - The historical antecedents of contemporary crime control British Journal of Criminology 46 (2006), 78–96.

Luhmann, Niklas, Das Recht der Gesellschaft, Frankfurt/Main 1993 (zitiert: *Luhmann*).

Luhmann, Niklas, Die Gesellschaft der Gesellschaft, Suhrkamp-Taschenbuch Wissenschaft, Frankfurt am Main 1998 (zitiert: *Luhmann*).

Luhmann, Niklas, Interpenetration – Zum Verhältnis personaler und sozialer Systeme / Interpenetration – On the relation between personal and social systems Zeitschrift für Soziologie 6 (1977), 62–76.

Luhmann, Niklas, Soziale Systeme, Grundriss einer allgemeinen Theorie, Bd. 666 – Suhrkamp-Taschenbuch Wissenschaft, 4. Aufl., Frankfurt am Main 1991 (zitiert: *Luhmann*).

Lutz, Burkart, Das Ende des Technikdeterminismus und die Folgen: soziologische Technikforschung vor neuen Aufgaben und neuen Problemen, Technik und sozialer Wandel: Verhandlungen des 23. Deutschen Soziologentages in Hamburg 1986, hrsg. v. Lutz, Burkart, Frankfurt am Main 1987.

Lynch, Michael/Cole, Simon A./McNally, Ruth ua, Truth Machine, The Contentious History of DNA Fingerprinting, Chicago, IL 2008 (zitiert: *Lynch/Cole/McNally/Jordan*).

Lyon, David, Facing the future: Seeking ethics for everyday surveillance. Ethics and Information Technology 3 (2001), 171–180.

Lyon, David, Globalizing Surveillance International Sociology 19 (2004), 135–149.

Lyon, David, Surveillance studies: an overview, Cambridge 2007 (zitiert: *Lyon*).

Lyon, David, Surveillance, Snowden, and Big Data: Capacities, consequences, critique Big Data & Society 1 (2014), 1-13.

Lyotard, Jean-François, The postmodern condition, A report on knowledge, Bd. 10 – Theory and history of literature, Manchester 1984 [1979] (zitiert: *Lyotard*).

Lyre, Holger, Der Begriff der Information: Was er leistet und was er nicht leistet, in: *Pietsch, Wolfgang/Wernecke, Jörg/Ott, Maximilian* (Hrsg.), Berechenbarkeit der Welt?, Wiesbaden 2017, S. 477–493.

Mackey, William J./Courtney, Brandon J., Advances in Technology and Policing: 21st Century America, in: *Bain, Andy* (Hrsg.), Law Enforcement and Technology, London 2016, S. 27–45.

Maguire, E. A./Gadian, D. G./Johnsrude, I. S. ua, Navigation-related structural change in the hippocampi of taxi drivers Proc Natl Acad Sci U S A 97 (2000), 4398–4403.

Maltz, Michael D., Bridging Gaps in Police Crime Data, A Discussion Paper from the BJS Fellows Program, 1999.

Mandinach, Ellen B./Gummer, Edith S., A Systemic View of Implementing Data Literacy in Educator Preparation Educational Researcher 42 (2013), 30–37.

Mangold, Hannes, Fahndung nach dem Raster, Dissertation 2017.

Manning, Peter K., Information Technologies and the Police Crime and Justice 15 (1992), 349–398.

Manning, Peter K., The technology of policing, Crime mapping, information technology, and the rationality of crime control, New perspectives in crime, deviance, and law series, New York 2008 (zitiert: *Manning*).

Manovich, Lev, Database as Symbolic Form Convergence 5 (1999), 80–99.

Marks, Amber/Bowling, Ben/Keenan, Colman, Automatic Justice? Technology, Crime and Social Control, in: *Brownsword, Roger/Scotford, Eloise/Yeung, Karen ua* (Hrsg.), The Oxford Handbook of Law, Regulation and Technology, 2017, S. 705–730.

Marthews, Alex/Tucker, Catherine E., Government Surveillance and Internet Search Behavior, 2017.

Martini, Mario, Blackbox Algorithmus – Grundfragen einer Regulierung Künstlicher Intelligenz, Berlin, Heidelberg 2019 (zitiert: *Martini*).

Marx, Gary T., Undercover, Police Surveillance in America, Berkeley 1988 (zitiert: *Marx*).

Mastrofski, Stephen D./Willis, James J., Police Organization Continuity and Change: Into the Twenty-first Century Crime and Justice 39 (2010), 55–144.

Matt, Holger/Renzikowski, Joachim, Strafgesetzbuch: StGB, 2. Aufl., 2020 (zitiert: *Matt/Renzikowski*).

Mayer, Verena, Berliner Polizei erhob rechtswidrig Daten von Sinti und Roma Süddeutsche Zeitung v. 17. Juni 2021 (abrufbar unter https://www.sueddeutsche.de/panorama/sinti-und-roma-polizei-racial-profiling-berlin-1.5176954) (Stand: 01.10.2023).

Mayer-Schönberger, Viktor, Delete, The virtue of forgetting in the digital age ; with a new afterword by the author, 4. Aufl., Princeton, NJ 2011 (zitiert: *Mayer-Schönberger*).

Mayer-Schönberger, Viktor, Nützliches Vergessen, in: *Reiter, Michael/Wittmann-Tiwald, Maria* (Hrsg.), Goodbye privacy - Grundrechte in der digitalen Welt. Internationales Symposium ; Dokumentation der Tagungsergebnisse vom 5.9.2007, Wien 2008, S. 9–15.

Mayer-Schönberger, Viktor/Cukier, Kenneth, Big Data, Die Revolution, die unser Leben verändern wird, 3. Aufl., München 2013 (zitiert: *Mayer-Schönberger/Cukier*).

Mayring, Philipp, Qualitative Inhaltsanalyse, Grundlagen und Techniken, Beltz Pädagogik, 12. Aufl., Weinheim 2015 (zitiert: *Mayring*).

McGee, W. C., Data Base Technology IBM J. Res. & Dev. 25 (1981), 505–519.

McGuire, Michael, Technology crime and technology control. Contexts and history, in: *McGuire, Michael/Holt, Thomas J.* (Hrsg.), The Routledge Handbook of Technology, Crime and Justice, London, New York, N.Y 2017, S. 35–60.

McLuhan, Marshall, The global village, 1989 (zitiert: *McLuhan*).

McLuhan, Marshall, The Gutenberg galaxy, The making of tyopographic man, [Toronto] 1962 (zitiert: *McLuhan*).

McLuhan, Marshall, Understanding media, The extensions of man, Bd. 2765 – Mentor books, 2. Aufl., New York, NY 1964 (zitiert: *McLuhan*).

McLuhan, Marshall, Understanding media, The extensions of man, Bd. 3039 – Signet books Q, New York 1964 (zitiert: *McLuhan*).

McLuhan, Marshall, Understanding media, The extensions of man, Media sociology, 9. Aufl., Cambridge, Mass. 2001 (zitiert: *McLuhan*).

Meier, Bernd-Dieter, Herausforderungen und Hindernisse einer evidenzbasierten Kriminalpolitik Kriminalpolitische Zeitschrift 5 (2020), 1–7 (abrufbar unter https://kripoz.de/wp-content/uploads/2020/01/kripoz-gesamtausgabe-1-2020.pdf) (Stand: 01.10.2023).

Meier, Robert F., Deviance, Social Control, and Criminalization, in: *Deflem, Mathieu* (Hrsg.), The Handbook of Social Control, Chichester, UK 2018, S. 23–35.

Mejias, Ulises A./Couldry, Nick, Datafication Internet Policy Review 8 (2019).

Merten, Klaus, Evolution der Kommunikation, in: *Merten, Klaus/Schmidt, Siegfried J./Weischenberg, Siegfried* (Hrsg.), Die Wirklichkeit der Medien, Wiesbaden 1994, S. 141–162.

Meuser, Michael/Nagel, Ulrike, Expertenwissen und Experteninterview, in: *Hitzler, Ronald/Honer, Anne/Maeder, Christoph* (Hrsg.), Expertenwissen. Die institutionalisierte Kompetenz zur Konstruktion von Wirklichkeit, Opladen 1994, S. 180–192.

Meuser, Michael/Nagel, Ulrike, ExpertInneninterviews — vielfach erprobt, wenig bedacht, in: *Bogner, Alexander/Littig, Beate/Menz, Wolfgang* (Hrsg.), Das Experteninterview, Wiesbaden 2002, S. 71–93.

Miller, Clark A., Globalizing Security: Science and the Transformation of Contemporary Political Imagination, in: *Jasanoff, Sheila/Kim, Sang-Hyun* (Hrsg.), Dreamscapes of modernity. Sociotechnical imaginaries and the fabrication of power, Chicago, London 2015, S. 277–299.

Ministerium des Innern des Landes Nordrhein-Westfalen, Neues Portal „Internetwache" der nordrhein-westfälischen Polizei freigeschaltet, https://www.im.nrw/neues-portal-internetwache-der-nordrhein-westfaelischen-polizei-freigeschaltet (Stand: 01.10.2023).

Mitterer, Andy, Die elektronische Akte im Strafverfahren: Chancen und Risiken, in: *Anders, Ralf Peter/Graalmann-Scheerer, Kirsten/Schady, Jan Henrik* (Hrsg.), Innovative Entwicklungen in den deutschen Staatsanwaltschaften, Wiesbaden 2021, S. 353–362.

Mokros, Reinhard, Polizeiwissenschaft und Polizeiforschung in Deutschland, Versuch einer kritischen Bestandsaufnahme, Bd. 2 – Kriminologisch-polizeiwissenschaftliche Arbeitspapiere der Ruhr-Universität Bochum, Holzkirchen/Obb 2011 (zitiert: *Mokros*, Polizeiwissenschaft).

Morozov, Evgeny, To save everything, click here, The folly of technological solutionism, New York 2013 (zitiert: *Morozov*).

Morris, Charles W., Grundlagen der Zeichentheorie, Bd. 35006 – Ullstein-Buch Ullstein-Materialien, Frankfurt/M, Berlin, Wien 1979 (zitiert: *Morris*).

Mulone, Massimiliano, History of Policing, in: *Deflem, Mathieu* (Hrsg.), The Handbook of Social Control, Chichester, UK 2018, S. 207–220.

Münch, Holger, Kriminalitätsbekämpfung weiterdenken. Kriminalistik 73 (2019), 11–16.

Münkler, Herfried, Die Strategie des Terrorismus und die Abwehrmöglichkeiten des demokratischen Rechtsstaats, Akademievorlesung am 1. Juni 2006, in: *Hucho, Ferdinand/Nida-Rümelin/Julian, Sperling, Karl ua* (Hrsg.), Berichte und Abandlungen der Band Berlin-Brandenburgischen Akademie der Wissenschaften, Berlin 2009, S. 101–112.

Murphy, Cullen, God's jury, The inquisition and the making of the modern world, London 2013 (zitiert: *Murphy*).

Naplava, Thomas, „Militarisierung" als Antwort auf „mangelnden Respekt"? Ein soziologischer Beitrag zur Diskussion um einen Paradigmenwechsel der Polizei in Deutschland, in: *Hunold, Daniela/Ruch, Andreas* (Hrsg.), Polizeiarbeit zwischen Praxishandeln und Rechtsordnung, Wiesbaden 2020, S. 165–183.

Nassehi, Armin, Muster, Theorie der digitalen Gesellschaft, München 2019 (zitiert: *Nassehi*).

Nassehi, Armin, Unbehagen, Theorie der überforderten Gesellschaft, München 2021 (zitiert: *Nassehi*).

Nelson, Ted, Geeks bearing gifts, How the computer world got this way, Sausalito, Calif. 2009 (zitiert: *Nelson*).

Neufeld, M. Lynne/Cornog, Martha, Database History: From Dinosaurs to Compact Discs J. Am. Soc. Inf. Sci. 37 (1986), 183–190.

Neuhaus, Christian, Prinzip Zukunfsbild, in: *Gerhold, Lars/Holtmannspötter, Dirk/Neuhaus, Christian ua* (Hrsg.), Standards und Gütekriterien der Zukunftsforschung, Wiesbaden 2015, S. 21–30.

Niceforo, Alfredo, Die Kriminalpolizei und ihre Hilfswissenschaften, Bd. 3 – Enzyklopädie der modernen Kriminalistik, hrsg. v. Lindenau, Heinrich, Berlin 1908.

Nikhil X. Bhattasali/Esha Maiti, Machine "Gaydar": Using Facebook Profiles to Predict Sexual Orientation, https://cs229.stanford.edu/proj2015/019_report.pdf (Stand: 01.10.2023).

Noble, Safiya Umoja, Algorithms of oppression, Data discrimination in the age of Google, New York 2018 (zitiert: *Noble*).

Nyíri, Kristóf, The networked mind Stud East Eur Thought 60 (2008), 149–158.

Oberwittler, Dietrich/Lukas, Tim, Schichtbezogene und ethnisierende Diskriminierung im Prozess der strafrechtlichen Sozialkontrolle, in: *Hormel, Ulrike/Scherr, Albert* (Hrsg.), Diskriminierung, Wiesbaden 2010, S. 221–254.

Oermann, Markus/Staben, Julian, Mittelbare Grundrechtseingriffe durch Abschreckung?, Zur grundrechtlichen Bewertung polizeilicher "Online-Streifen" und "Online-Ermittlungen" in sozialen Netzwerken Der Staat 52 (2013), 630–661.

Ogburn, William Fielding, Social change with respect to culture an original nature, London, New York 1923 (zitiert: *Ogburn*).

Olteanu, Alexandra/Castillo, Carlos/Diaz, Fernando ua, Social Data: Biases, Methodological Pitfalls, and Ethical Boundaries Front Big Data 2 (2019), 13.

O'Neil, Cathy, Weapons of math destruction, How big data increases inequality and threatens democracy, UK 2017 (zitiert: *O'Neil*).

Ott, Sascha, Information, Zur Genese und Anwendung eines Begriffs, Konstanz 2004 (zitiert: *S. Ott*).

Pangrazio, Luci/Sefton-Green, Julian, The social utility of 'data literacy' Learning, Media and Technology 45 (2020), 208–220.

Paoli, Letizia/Vander Beken, Tom, Organized Crime: A Contested Concept, in: *Paoli, Letizia* (Hrsg.), The Oxford handbook of organized crime, Oxford 2014, S. 13–31.

Pasquale, Frank, The Black Box Society, 2015 (zitiert: *Pasquale*).

Paumier Jones, Mary, The Storytelling Animal The Georgia Review 50 (1996), 649–666 (Stand: 2022-09-12).

Pearlson, Keri E./Saunders, Carol S./Galletta, Dennis F., Managing and using information systems, A strategic approach, 6. Aufl., Hoboken, NJ 2016 (zitiert: *Pearlson/Saunders/Galletta*).

Penney, Jonathon W., Chilling Effects: Online Surveillance and Wikipedia Use Berkeley Tech. L.J. 31 (2016), 117–182.

Perry, Walt L./McInnis, Brian/Price, Carter C. ua, Predictive policing, The role of crime forecasting in law enforcement operations, Santa Monica, CA 2013 (zitiert: *Perry/McInnis/Price/Smith/Hollywood*).

Peukert, Detlev, Die Weimarer Republik, Krisenjahre der Klassischen Moderne, 1282 = N.F., 282 – Neue historische Bibliothek, Frankfurt am Main 1987 (zitiert: *Peukert*).

Peukert, Detlev, Volksgenossen und Gemeinschaftsfremde, Anpassung, Ausmerze und Aufbegehren unter dem Nationalsozialismus, Köln 1982 (zitiert: *Peukert*).

Pitschas, Rainer, Europäisches Polizeirecht als Informationsrecht Zeitschrift für Rechtspolitik 26 (1993), 174–177.

Popitz, Heinrich, Über die Präventivwirkung des Nichtwissens, Dunkelziffer, Norm und Strafe, Bd. 350 – Recht und Staat in Geschichte und Gegenwart, Tübingen 1968 (zitiert: *Popitz*).

Poscher, Ralf, Konzept für ein periodisches Überwachungsbarometer, Deutscher Bundestag, Ausschussdrucksache 19(4)732 E, 2021.

Poscher, Ralf, Sicherheitsverfassungsrecht im Wandel, in: *Korioth, Stefan/Vesting, Thomas* (Hrsg.), Der Eigenwert des Verfassungsrechts, 2011, S. 245–262.

Poscher, Ralf/Kilchling, Michael, Entwicklung eines periodischen Überwachungsbarometers für Deutschland, 2021.

Poscher, Ralf/Kilchling, Michael/Landerer, Lukas, Ein Überwachungsbarometer für Deutschland, Entwicklung eines Konzeptes zur periodischen Erfassung staatlicher Überwachungsmaßnahmen Zeitschrift für das Gesamte Sicherheitsrecht (GSZ) 4 (2021), 225–232.

Poscher, Ralf/Kilchling, Michael/Landerer, Lukas, Überwachungsbarometer für Deutschland, Ein Modellkonzept, 2022.

Poster, Mark, The mode of information, Poststructuralism and social context, Cultural theory, intellectual history, Chicago 1990 (zitiert: *Poster*).

Pyöriä, Pasi, The concept of knowledge work revisited Journal of Knowledge Management 9 (2005), 116–127.

R+V Versicherung AG, Die Ängste der Deutschen, https://www.ruv.de/newsroom/themenspezial-die-aengste-der-deutschen/langzeitvergleich (Stand: 01.10.2023).

Rädiker, Stefan/Kuckartz, Udo, Analyse qualitativer Daten mit MAXQDA, Wiesbaden 2019 (zitiert: *Rädiker/Kuckartz*).

Raley, Rita, Dataveillance and Countervailance, in: *Gitelman, Lisa* (Hrsg.), "Raw data" is an oxymoron, Cambridge, Massachusetts 2013, S. 121–146.

Rammert, Werner, Technik - Handeln - Wissen, Wiesbaden 2016 (zitiert: *Rammert*).

Ratcliffe, Jerry H., Intelligence-Led Policing, 2016 (zitiert: *Ratcliffe*).

Reckwitz, Andreas, Das Ende der Illusionen, Politik, Ökonomie und Kultur in der Spätmoderne, Erscheinungsort nicht ermittelbar 2019 (zitiert: *Reckwitz*).

Reckwitz, Andreas, Das hybride Subjekt, Eine Theorie der Subjektkulturen von der bürgerlichen Moderne zur Postmoderne, Weilerswist 2006 (Zugl.: Hamburg, Univ., Habil.-Schr., 2005).

Reckwitz, Andreas, Die Gesellschaft der Singularitäten, Zum Strukturwandel der Moderne, Frankfurt am Main 2017 (zitiert: *Reckwitz*).

Reckwitz, Andreas, Risikopolitik, in: *Volkmer, Michael/Werner, Karin* (Hrsg.), Die Corona-Gesellschaft, Bielefeld, Germany 2020, S. 241–252.

Regener, Susanne, Ausgegrenzt, Die optische Inventarisierung des Menschen im Polizeiwesen und in der Psychiatrie Fotogeschichte 38 (1990) (1990).

Reiss, Albert J., Police Organization in the Twentieth Century Crime and Justice 15 (1992), 51–97.

Reuss-Ianni, Elizabeth, Two cultures of policing, 2017 (zitiert: *Reuss-Ianni*).

Reuter, Karl, Fahnden und Finden Die Polizei 56 (1965), 265–266.

Ribes, David/Jackson, Steven J., Data Bite Man: The Work of Sustaining a Long-Term Study, in: *Gitelman, Lisa* (Hrsg.), "Raw data" is an oxymoron, Cambridge, Massachusetts 2013, S. 147–166.

Ridgeway, Greg, Policing in the Era of Big Data Annu. Rev. Criminol. 1 (2018), 401–419.

Riegel, Reinhard, Nochmals: Das Bundeskriminalamtgesetz Neue Juristische Wochenschrift 50 (1997), 3408–3411.

Röhle, Theo, Der Google-Komplex, Über Macht im Zeitalter des Internets, Bielefeld 2010 (Zugl.: Hamburg, Univ., FB SLM I, Diss., WS 2009/10 u.d.T.: Röhle, Theo: Dispositiv Google : zur Analytik der Suchmaschinenmacht).

Ross, Edward Alsworth, Social Control. XX. The Vicissitudes of Social Control American Journal of Sociology 6 (1901), 550–562.

Roßnagel, Alexander, Die „Überwachungs-Gesamtrechnung" – Das BVerfG und die Vorratsdatenspeicherung Neue Juristische Wochenschrift 63 (2010), 1238–1242.

Roßnagel, Alexander, Die parlamentarische Verantwortung für den technischen Fortschritt Zeitschrift für Rechtspolitik 1991 (25), 55–60.

Roßnagel, Alexander, Verantwortung für Datenschutz Informatik Spektrum 28 (2005), 462–473.

Roth, Andreas, Kriminalitätsbekämpfung in deutschen Großstädten 1850 - 1914, Ein Beitrag zur Geschichte des strafrechtlichen Ermittlungsverfahrens, Berlin 1997 (Zugl.: Münster (Westfalen), Univ., Habil.-Schr., 1993).

Row, Michael/Muir, Rick, Big data policing, Governing the machines?, in: *McDaniel, John L. M./Pease, Ken* (Hrsg.), Predictive policing and artificial intelligence, London, New York 2021, S. 254–268.

Rowley, Jennifer, The wisdom hierarchy: representations of the DIKW hierarchy Journal of Information Science 33 (2007), 163–180.

Rowley, Jennifer, Where is the wisdom that we have lost in knowledge? Journal of Documentation 62 (2006), 251–270.

Ruch, Andreas/Feltes, Thomas, Gewalttäterdateien: Rechtliche Probleme und kriminologische Risiken NK 17 (2016), 62–77.

Russell, Stuart J./Norvig, Peter, Artificial Intelligence: A Modern Approach, Pearson Series in Artificial Intelligence, 4. Aufl., Upper Saddle River, N.J. 2020 (zitiert: *Russell/Norvig*).

Sacasas, Michael, Attending to the World, https://theconvivialsociety.substack.com/p/attending-to-the-world?utm_source=url (Stand: 01.10.2023).

Sacasas, Michael, What Is To Be Done? — Fragments, https://theconvivialsociety.substack.com/p/what-is-to-be-done-fragments (Stand: 01.10.2023).

Sanders, Carrie B./Sheptycki, James, Policing, crime and 'big data'; towards a critique of the moral economy of stochastic governance Crime Law Soc Change 68 (2017), 1–15.

Schantz, Peter/Wolff, Heinrich Amadeus, Das neue Datenschutzrecht, Datenschutz-Grundverordnung und Bundesdatenschutzgesetz in der Praxis, München 2017 (zitiert: *Schantz/H. Wolff*).

Schenke, Wolf-Rüdiger/Graulich, Kurt/Ruthig, Josef, Sicherheitsrecht des Bundes, Beck'sche Kurz-Kommentare, hrsg. v. Schenke, Wolf-Rüdiger/Graulich, Kurt/Ruthig, Josef, 2. Aufl., München 2019.

Schiepek, Günter, Von der Kybernetik erster zur Kybernetik zweiter Ordnung, in: *Schiepek, Günter* (Hrsg.), Systemtheorie der Klinischen Psychologie, Wiesbaden 1991, S. 307–342.

Schmidbauer, Wilhelm/Steiner, Udo, Polizeiaufgabengesetz, Polizeiorganisationsgesetz, Landesrecht Freistaat Bayern, 5. Aufl., München 2020 (zitiert: *W. Schmidbauer/Steiner*).

Schöch, Heinz, Kriminalprognose, in: *Schneider, Hans Joachim* (Hrsg.), Grundlagen der Kriminologie, 2007, S. 359–394.

Scholz, Leander, Rasterfahndung oder Wie wird Wachs gemacht, in: *Schröter, Jens/Böhnke, Alexander* (Hrsg.), Analog/Digital - Opposition oder Kontinuum?, 2004, S. 97–116.

Schuppert, Gunnar Folke, Governance und Rechtsetzung, 2011 (zitiert: *Schuppert*).

Schwabenbauer, Thomas, Heimliche Grundrechtseingriffe, Ein Beitrag zu den Möglichkeiten und Grenzen sicherheitsbehördlicher Ausforschung, Zugl, Band 15 – Studien und Beiträge zum öffentlichen Recht, Tübingen 2013 (zitiert: *Schwabenbauer*, Heimliche).

Schwan, Eggert, Datenschutz, Vorbehalt des Gesetzes und Freiheitsgrundrechte VerwArch 66 (1975), 120–151.

Scott, James C., Seeing like a state, How certain schemes to improve the human condition have failed, The Yale ISPS series, New Haven, Conn. 1998 (zitiert: *Scott*).

Selbst, Andrew D., Disparate Impact in Big Data Policing Georgia Law Review 52 (2018), 109–196.

Selwyn, Neil, Data entry: towards the critical study of digital data and education Learning, Media and Technology 40 (2015), 64–82.

Sennett, Richard, Together, The rituals, pleasures and politics of cooperation, London 2012 (zitiert: *Sennett*).

Seo, Sarah A., Policing the open road, How cars transformed American freedom, Cambridge, Massachusetts 2019 (zitiert: *Seo*).

Shannon, Claude Elwood/Weaver, Warren, The mathematical theory of communication, Urbana 1949 (zitiert: *Shannon/Weaver*).

Shearing, Clifford D./Johnston, Les, Governing Security, 2013 (zitiert: *Shearing/Johnston*).

Shearing, Clifford D./Stenning, Philip C., Private Security: Implications for Social Control Social Problems 30 (1983), 493–506.

Sheptycki, James, Liquid modernity and the police métier ; thinking about information flows in police organisation Global Crime 18 (2017), 286–302.

Shields, Milo, Information Literacy, Statistical Literacy, Data Literacy IQ 28 (2005), 6.

Sidhu, Dawinder S., The Chilling Effect of Government Surveillance Programs on the Use of the Internet by Muslim-Americans University of Maryland Law Journal of Race, Religion, Gender 7 (2007).

Siemann, Wolfram, »Deutschlands Ruhe, Sicherheit und Ordnung«, Die Anfänge der politischen Polizei 1806 - 1866, Bd. 14 – Studien und Texte zur Sozialgeschichte der Literatur, Berlin 1985 (zitiert: *Siemann*).

Singelnstein, Tobias, Digitalisierung, Big Data und das Strafverfahren., in: *Stein, Ulrich/Greco, Luís/Jäger, Christian ua* (Hrsg.), Systematik in Strafrechtswissenschaft und Gesetzgebung. Festschrift für Klaus Rogall zum 70. Geburtstag am 10. August 2018, Berlin 2018, S. 725–738.

Singelnstein, Tobias, Preventive Turn - Wie Gefahr und Risiko zum zentralen Gegenstand von Strafrecht und sozialer Kontrolle werden, in: *Fischer, Thomas/Hilgendorf, Eric* (Hrsg.), Gefahr, 2020, S. 95–112.

Singelnstein, Tobias/Kunz, Karl-Ludwig, Kriminologie, Eine Grundlegung, 1758. Recht/Soziologie – UTB, 8. Aufl., Bern 2021 (zitiert: *Singelnstein/Kunz*).

Singelnstein, Tobias/Stolle, Peer, Die Sicherheitsgesellschaft, Soziale Kontrolle im 21. Jahrhundert, 3. Aufl., Wiesbaden 2012 (zitiert: *Singelnstein/Stolle*, Sicherheitsgesellschaft).

Small, Gary W./Lee, Jooyeon/Kaufman, Aaron ua, Brain health consequences of digital technology use Dialogues Clin Neurosci 22 (2020), 179–187.

Solove, Daniel J., The digital person, Technology and privacy in the information age, Ex machina, New York 2004 (zitiert: *Solove*).

Sommerer, Lucia, Personenbezogenes Predictive Policing, Kriminalwissenschaftliche Untersuchung über die Automatisierung der Kriminalprognose, v.19 – Schriften zur Kriminologie, Baden-Baden 2020 (zitiert: *Sommerer*).

Spencer, Elaine Glovka, Police and the social order in German cities, The Düsseldorf district, 1848 - 1914, DeKalb, Ill. 1992 (zitiert: *Spencer*).

Spiecker gen. Döhmann, Indra, Bundesverfassungsgericht kippt BKA-Gesetz: Ein Pyrrhus-Sieg der Freiheitsrechte?, https://verfassungsblog.de/bundesverfassungsgericht-kippt-bka-gesetz-ein-pyrrhus-sieg-der-freiheitsrechte/ (Stand: 01.10.2023).

Spiecker gen. Döhmann, Indra/Kehr, Thomas, Die Entscheidung des Bundesverwaltungsgerichts vom 09.06.2010 - Datei Gewalttäter Sport Deutsches Verwaltungsblatt 2011, 930–936.

Star, Susan Leigh, The Ethnography of Infrastructure American Behavioral Scientist 43 (1999), 377–391.

Steinke, Ines, Qualitätssicherung in der qualitativen Forschung, in: *Kuckartz, Udo/Grunenberg, Heiko/Dresing, Thorsten* (Hrsg.), Qualitative Datenanalyse: computergestützt, Wiesbaden 2007, S. 176–187.

Steinmüller, Karlheinz, Szenarien – Ein Methodenkomplex zwischen wissenschaftlichem Anspruch und zeitgeistiger Bricolage, in: *Popp, Reinhold* (Hrsg.), Zukunft und Wissenschaft, Berlin, Heidelberg 2012, S. 101–137.

Steinmüller, W./Lutterbeck, B./Mallmann, C. ua, Grundfragen des Datenschutzes, Gutachten im Auftrag des Bundesministeriums des Innern, BT-Drs. 6/3826, 1971.

Stoll, Peter-Tobias, Sicherheit als Aufgabe von Staat und Gesellschaft, Verfassungsordnung, Umwelt- und Technikrecht im Umgang mit Unsicherheit und Risiko, Tübingen 2003 (Zugl.: Heidelberg, Univ., Habil.-Schr., 2001).

Strauss, Anselm L./Corbin, Juliet M., Basics of qualitative research, Grounded theory procedures and techniques, 3. Aufl., Newbury Park, Calif. 1991 (zitiert: *Strauss/Corbin*).

Strauß, Stefan, Deep Automation Bias: How to Tackle a Wicked Problem of AI? BDCC 5 (2021), 18.

Strübing, Jörg, Pragmatismus als epistemische Praxis, Der Beitrag der Grounded Theory zur Empirie-Theorie-Frage, in: *Kalthoff, Herbert* (Hrsg.), Theoretische Empirie. Zur Relevanz qualitativer Forschung, Frankfurt am Main 2008, S. 282–314.

Stümper, Alfred, Hat die Prävention eine Chance gegenüber der modernen Kriminalität? Kriminalistik 27 (1973), 193–201.

Tanneberger, Steffen, Die Sicherheitsverfassung, Eine systematische Darstellung der Rechtsprechung des Bundesverfassungsgerichts : zugleich ein Beitrag zu einer induktiven Methodenlehre, Band 11 – Freiburger rechtswissenschaftliche Abhandlungen, Tübingen 2014 (zitiert: *Steffen Tanneberger*).

Tetzlaff, Thilo, Gestaltungsspielräume für eine bundesweite Verbunddatei beim Bundeskriminalamt Verwaltungsrundschau (vr) 57 (2011), 403–408.

Thacker, Eugene, Networks, Swarms, Multitudes (Part Two), https://journals.uvic.ca/index.php/ctheory/article/view/14541/5388 (Stand: 01.10.2023).

Timothy Raeymaekers, Collapse or Order? Questioning State Collapse in Africa, Nr. 10, 2005.

Tooze, Adam, Defining polycrisis - from crisis pictures to the crisis matrix., https://adamtooze.substack.com/p/chartbook-130-defining-polycrisis (Stand: 01.10.2023).

Töpfer, Eric, (Dis-)Kontinuitäten antiziganistischen Profilings im Zusammenhang mit der Bekämpfung „reisender Täter", Forschungsbericht zur Vorlage bei der Unabhängigen Kommission Antiziganismus, 2020.

Townend, Judith, Freedom of Expression and the Chilling Effect, in: *Tumber, Howard/Waisbord, Silvio R.* (Hrsg.), The Routledge companion to media and human rights, London, New York 2017, S. 73–82.

Unruh, Peter, Zur Dogmatik der grundrechtlichen Schutzpflichten, Bd. 709 – Schriften zum öffentlichen Recht, Berlin 1996 (zitiert: *Unruh*).

Valverde, Mariana/Mopas, Michael, Insecurity and the dream of targeted governance Global governmentality: Governing international spaces 28 (2004), 233.

van Nimwegen, Christof, The paradox of the guided user: assistance can be counter-effective, Utrecht 2008 (zitiert: *van Nimwegen*).

Vera, Antonio/Jablonowski, Lara, Organisationskultur der Polizei, in: *Stierle, Jürgen/Wehe, Dieter/Siller, Helmut* (Hrsg.), Handbuch Polizeimanagement, Wiesbaden 2017, S. 475–491.

Vesting, Thomas, Die Medien des Rechts: Computernetzwerke, Weilerswist 2015 (zitiert: *Vesting*).

Vesting, Thomas, Kein Anfang und kein Ende, Die Systemtheorie des Rechts als Herausforderung für Rechtswissenschaft und Rechtsdogmatik, https://www.jura.uni-frankfurt.de/43748222/kein-anfang-und-kein-ende.pdf (Stand: 01.10.2023).

Völlinger, Veronika, 158 Verfahren gegen Polizisten wegen Daten-Missbrauch Zeit Online v. 1. November 2019 (abrufbar unter https://www.zeit.de/gesellschaft/zeitgeschehen/2019-11/datenschutz-polizisten-missbrauch-datenbanken-bussgeld-polizei) (Stand: 01.10.2023).

Wagner, Patrick, Prägungen, Anpassungen, Neuanfänge: Das Bundeskriminalamt und die nationalsozialistische Vergangenheit seiner Gründergeneration, Ansatz und Ergebnisse des Forschungsprojektes, in: *Bundeskriminalamt* (Hrsg.), Der Nationalsozialismus und die Geschichte des BKA. Spurensuche in eigener Sache; Ergebnisse - Diskussionen - Reaktionen; Dokumentation des Kolloquiums zum Forschungsbericht zur BKA-Historie vom 6. April 2011, Köln 2011, S. 21–35.

Wagner, Patrick, Volksgemeinschaft ohne Verbrecher, Konzeptionen und Praxis der Kriminalpolizei in der Zeit der Weimarer Republik und des Nationalsozialismus, 1996 (Zugl.: Hamburg, Univ., Diss., 1995 u.d.T.: Wagner, Patrick: Kommissar Sisyphus träumt vom letzten Fall).

Walsh, Maria, Evidenzorientierung in der deutschen Kriminalprävention und -politik. Entwicklung und Überlegungen zum Stand der Dinge NK 32 (2020), 24–34.

Walsh, Toby, 2062, The World That AI Made, Collingwood 2018 (zitiert: *T. Walsh*).

Walter, Joachim, Überrepräsentation von Minderheiten im Strafvollzug NK 19 (2007), 126–133.

Warren, Samuel D./Brandeis, Louis D., The Right to Privacy Harvard Law Review, pp. 193-220. Vol. 4 (1890).

Weaver, Warren, Ein aktueller Beitrag zur mathematischen Theorie der Kommunikation, in: *Shannon, Claude Elwood/Weaver, Warren* (Hrsg.), Mathematische Grundlagen der Informationstheorie, München 1976, S. 11–39.

Weber, Max, Gesammelte Aufsätze zur Wissenschaftslehre, Tübingen 1922 (zitiert: *Weber*).

Webster, Frank, Theories of the information society, International library of sociology, 4. Aufl., London 2014 (zitiert: *Webster*).

Weinberger, David, The Problem with the Data-Information-Knowledge-Wisdom Hierarchy, https://hbr.org/2010/02/data-is-to-info-as-info-is-not (Stand: 01.10.2023).

Weinhold, Robert/Johannes, Paul C., Europäischer Datenschutz in Strafverfolgung und Gefahrenabwehr - Die neue Datenschutz-Richtlinie im Bereich Polizei und Justiz sowie deren Konsequenzen für deutsche Gesetzgebung und Praxis Deutsches Verwaltungsblatt 131 (2016), 1501–1506.

Weiser, Mark, The Computer for the 21st Century Sci Am 265 (1991), 94–104.

Weizenbaum, Joseph, Computer power and human reason, From judgment to calculation, San Francisco 1976 (zitiert: *Weizenbaum*).

Werner, Paul, Aufbau und Aufgaben der Reichskriminalpolizei Zeitschrift für die gesamte Strafrechtswissenschaft 61 (1942), 465–470.

Weßlau, Edda, Vorfeldermittlungen, Probleme der Legalisierung "vorbeugender Verbrechensbekämpfung" aus strafprozeßrechtlicher Sicht, Berlin 1989 (Zugl.: Hamburg, Univ., Diss., 1988).

Westrope, Andrew, Wolfcom Embraces Body Cam Face Recognition Despite Concerns, https://www.govtech.com/biz/wolfcom-embraces-body-cam-face-recognition-despite-concerns.html (Stand: 01.10.2023).

Will, Rosemarie, Der automatisierte Datenaustausch zwischen Polizei und Nachrichtendiensten im Urt. des Bundesverfassungsgerichts zum Antiterrordateigesetz, in: *Nolte, Jakob/Poscher, Ralf/Wolter, Henner* (Hrsg.), Die Verfassung als Aufgabe von Wissenschaft, Praxis und Öffentlichkeit. Freundesgabe für Bernhard Schlink zum 70. Geburtstag, Heidelberg 2014, S. 429–445.

Willis, James J., Improving police: What's craft got to do with it?, https://www.policefoundation.org/publication/improving-police-whats-craft-got-to-do-with-it/ (Stand: 01.10.2023).

Willis, James J./Mastrofski, Stephen D., Improving policing by integrating craft and science: what can patrol officers teach us about good police work? Policing and Society 28 (2018), 27–44.

Wilson, Dean, Algorithmic patrol: the futures of predictive policing., in: *Završnik, Aleš* (Hrsg.), Big data, crime and social control, London, New York 2019, S. 108–127.

Wilson, Dean, Platform Policing and the Real-Time Cop SS 17 (2019), 69–75.

Wilz, Sylvia Marlene/Reichertz, Jo, polizei.de oder: Verändert das Internet die Praxis polizeilichen Arbeitens?, in: *Lange, Hans-Jürgen/Ohly, H. Peter* (Hrsg.), Auf der Suche nach neuer Sicherheit. Fakten, Theorien und Folgen, Wiesbaden 2008, S. 221–230.

Winkler, Hartmut, Docuverse, Zur Medientheorie der Computer, Regensburg 1997 (zitiert: *Winkler*).

Wittgenstein, Ludwig, Tractatus logico-philosophicus, International Library of psychology, philosophy and scientific method, London 1922 (zitiert: *Wittgenstein*).

Wolff, Annika/Gooch, Daniel/Cavero Montaner, Jose J. ua, Creating an Understanding of Data Literacy for a Data-driven Society The Journal of Community Informatics 12 (2016).

Wolff, Heinrich Amadeus, Das Urt. des Bundesverfassungsgerichts zum BKA-Gesetz ZG 31 (2016), 361–388.

Wolff, Heinrich Amadeus, Der EU-Richtlinienentwurf zum Datenschutz in Polizei und Justiz - Gehalt und Auswirkungen auf das Strafprozess- und Polizeirecht, in: *Kugelmann, Dieter/Rackow, Peter* (Hrsg.), Prävention und Repression im Raum der Freiheit, der Sicherheit und des Rechts. Belastbarkeit der Konzepte von Strafe und Gefahrenabwehr zwischen Staat und EU, Baden-Baden 2014, S. 61–94.

Würtenberger, Thomas/Tanneberger, Steffen B., Zum verfassungsrechtlichen Rahmen demokratischer Sicherheitspolitik: Die Sicherheitsverfassung des Bundesverfassungsgerichts, in: *Fischer, Susanne/Masala, Carlo* (Hrsg.), Innere Sicherheit nach 9/11, Wiesbaden 2016, S. 35–59.

Završnik, Aleš, Algorithmic justice: Algorithms and big data in criminal justice settings European Journal of Criminology 18 (2021), 623–642.

Završnik, Aleš, Big data. What it is and why does it matter for crime and social control?, in: *Završnik, Aleš* (Hrsg.), Big Data, Crime, and Social Control, [Place of publication not identified] 2019, S. 3–28.

Zimmermann, Michael, Rassenutopie und Genozid: Die nationalsozialistische "Lösung der Zigeunerfrage", Die nationalsozialistische Verfolgung Hamburger Roma und Sinti. Fünf Beiträge, Hamburg 2006, S. 9–28.

Zins, Chaim, Conceptual approaches for defining data, information, and knowledge J. Am. Soc. Inf. Sci. 58 (2007), 479–493.

Zöller, Mark A., Informationssysteme und Vorfeldmaßnahmen von Polizei, Staatsanwaltschaft und Nachrichtendiensten, Zur Vernetzung von Strafverfolgung und Kriminalitätsverhütung im Zeitalter von multimedialer Kommunikation und Persönlichkeitsschutz, Heidelberg 2002 (Zugl.: Mannheim, Univ., Diss., 2001/2002).

Zuboff, Shoshana, The age of surveillance capitalism, The fight for a human future at the new frontier of power, London 2019 (zitiert: *Zuboff*).

Anhang

Leitfaden: Interviews mit behördlichen Datenschutzbeauftragten der Polizeien des Bundes und der Länder

I. Einleitungsfragen

1. Beruflicher Werdegang: Datenschutzbeauftragte:r ist ein vergleichsweise junger Beruf. Könnten Sie mir kurz erläutern wie Sie zum Datenschutz gekommen sind und schließlich Datenschutzbeauftragte(r) geworden sind?
2. Was sind typische Aufgaben, die in ihrem Arbeitsalltag immer wieder anfallen?

II. Beziehung zw. DSB und Polizei

1. Wie würde Sie die grundsätzliche Zusammenarbeit von Datenschutz und Polizei beschreiben? Gibt es da eine? Sie stehen als behördlicher Datenschutzbeauftragter ja gewissermaßen "in der Mitte".
2. Würden Sie ihre Arbeit als behördliche/r Datenschutzbeauftragte/r eher als konfrontativ oder als kooperativ beschreiben? Warum eher konfrontativ / kooperativ?
3. Wie ist der Datenschutz bei ihrer Polizeibehörde intern organisiert?
4. Wie gut kennen Sie sich mit der den polizeilichen Datenbanken und der Datenverarbeitung zugrunde liegenden Technik aus? Und reicht ihr Wissen da aus oder müssen Sie auf externes Wissen von Kolleg:innen zurückgreifen?
5. Wie ist so die Zusammenarbeit mit anderen Datenschutzbeauftragten/-behörden – sowohl mit der jeweiligen Aufsichtsbehörde als auch andere behördliche DSB?

III. Verwirklichung des Datenschutzes im Rahmen polizeilicher Datenverarbeitung

1. Haben Sie den Eindruck, dass Ihnen ausreichend Ressourcen zur Verwirklichung des Datenschutzes in ihrem Zuständigkeitsbereich zur Verfügung stehen?
2. Wie bewerten Sie die EU-Datenschutzreform und insbesondere die für den vorliegenden Kontext relevante JI-Richtlinie?

3. Denken Sie, dass die Bedeutung technischer Datenschutzinstrumente mit Blick auf immer mehr anfallende Daten ausgebaut werden muss?
4. Spielen die strafprozessualen Bestimmungen zum Umgang mit Strafverfahrensdaten (insb. §§ 474 ff. StPO) für ihre Tätigkeit eine Rolle?

IV. Potentiale für Chancen und Risiken im Bereich der polizeilichen Datenverarbeitung

1. Gegenwärtig hat man ja das Gefühl, dass der gesellschaftliche technologische Wandel immer weiter anzieht. Ist die Polizei aus ihrer Sicht in der Lage, mitzuziehen? Was sind Problemfelder, die bereits bestehen oder voraussichtlich auf die Polizeiarbeit infolge des technologischen Wandels zukommen?
2. Das Programm Polizei 2020 und alle damit zusammenhängenden Umsetzungsbemühungen:
   Werden Sie durch das Programm gegenwärtig schon in ihrem Arbeitsalltag beeinflusst? Falls ja, wie?
   Halten Sie das Programm insgesamt für sinnvoll? Warum (nicht)?
   Denken Sie, es gäbe Alternativen bei der Anpassung der polizeilichen Datenbanken und Datenverarbeitung?
3. Macht sich die voraussichtlich zunehmende Nutzung von „smarten" Geräten im Alltag bereits bei Ihnen in der Behörde bemerkbar? Also werden solche Geräte bspw. in Ermittlungen ausgewertet?
4. Welche Chancen und Risiken sehen Sie in Zukunft im Bereich der polizeilichen Datenverarbeitung?