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 l, 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 l, Pos. 119.
1654 Interview l, 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.