Die von Fabian Döbber erstellte Masterarbeit untersucht datenschutz- und rechtsstaatskonforme Ansätze smarter Technologien und künstlicher Intelligenz für die Polizei. Sie verbindet aktuelle Literatur, Experteninterviews und Dokumentenanalysen zu einem fundierten Gesamtbild neuer technologischer Möglichkeiten. Besondere Stärken liegen in der systematischen Analyse, klaren Strukturierung und praxisnahen Handlungsempfehlungen, die einen wichtigen Beitrag zur digitalen Transformation der Polizeiarbeit leisten.

Hintergrund:
The Open Government Institute | TOGI ist an der Zeppelin Universität Friedrichshafen angesiedelt. Es setzt sich das Ziel, als Pionier wegweisende Ideen, Visionen, Strategien, Konzepte, Theorien, Modelle und Werkzeuge zum Einsatz moderner Informations- und Kommunikationstechnologien zu erarbeiten und diese mit Partnern zu realisieren.

Mit der vorliegenden Schriftenreihe des TOGI besteht ein interdisziplinärer Raum für Veröffentlichungen. Empirische Untersuchungen und Forschungsergebnisse sollen in Form von Monographien, Beiträgen, Vorträgen sowie Tagungs- und Konferenzergebnissen die Inhalte der Schriftenreihe sein und so direkt zum Wissenstransfer beitragen.

Informationen: https://togi.zu.de

ISSN 2193-8946
ISBN 978-3-819068-29-4

zeppelin universität

The
Open Government Institute |TOGI

ZU |TOGI

Datenschutz- und rechtsstaatskonforme Ansätze smarter Technologien und künstlicher Intelligenz für die Polizei

Monographie am
The Open Government Institute |TOGI
der Zeppelin Universität

Band 26 der Schriftenreihe des
The Open Government Institute |TOGI
der Zeppelin Universität Friedrichshafen

zeppelin universität

The Open Government Institute | TOGI

Fabian Döbber

Datenschutz- und rechtsstaatskonforme Ansätze smarter Technologien und künstlicher Intelligenz für die Polizei

Monographie am
The Open Government Institute |TOGI
der Zeppelin Universität

TOGI Schriftenreihe - Band 26

Schriftenreihe des
The Open Government Institute |TOGI
der Zeppelin Universität Friedrichshafen

The Open Government Institute | TOGI
TOGI Schriftenreihe

Band 26

Herausgeber von Band 26

Univ.-Prof. Dr. Jörn von Lucke
TOGI | Zeppelin Universität, Friedrichshafen
joern.vonlucke@zu.de

Herausgeber der TOGI Schriftenreihe

Univ.-Prof. Dr. Jörn von Lucke
TICC | Zeppelin Universität, Friedrichshafen
joern.vonlucke@zu.de

Impressum

Druck und Verlag: Neopubli GmbH, Berlin, http://www.epubli.de
Verlagsgruppe Holtzbrinck
ISBN 978-3-819068-29-4
ISSN 2193-8946

Vorwort

Band 26 der TOGI Schriftenreihe widmet sich einem hochaktuellen und zugleich äußerst sensiblen Thema: der Nutzung smarter Technologien und künstlicher Intelligenz in der Polizeiarbeit, unter besonderer Berücksichtigung von Datenschutz und rechtsstaatlichen Anforderungen. Die von Fabian Döbber angefertigte Masterthesis entstand im Herbst 2024 vor dem Hintergrund signifikanter Leistungssprünge bei generativer künstlicher Intelligenz, einer zunehmend datengetriebenen Sicherheitsarchitektur und wachsenden Diskussionen über die Vereinbarkeit technologischer Innovationen mit den Grundsätzen eines demokratischen Rechtsstaats sowie einer sich verändernden Sicherheitslage.

Diese Arbeit ist in zehn Kapitel aufgeteilt. Die inhaltliche Grundlage bildet eine Kombination aus systematischer Literaturrecherche, Experteninterviews und Dokumentenanalyse. Diese methodische Triangulation ermöglicht es dem Autor, bestehende, neuartige sowie künftige Anwendungsfelder smarter Technologien für die Polizei präzise zu definieren, zu analysieren und kritisch zu reflektieren. Besonders hervorzuheben ist der Praxisbezug der Arbeit, der sich unter anderem in elf Experteninterviews zeigt, die Fabian Döbber im Herbst 2024 geführt hat. Die Interviews wurden mithilfe eines selbst entwickelten Leitfadens strukturiert, der im Anhang der Arbeit dokumentiert ist. Die Gespräche wurden transkribiert und flossen in die Analyse ein. Diese Interviews, ergänzt durch eine sorgfältige Dokumentenanalyse, bilden die Grundlage für die fünf Handlungsempfehlungen. Mein Dank geht an dieser Stelle an Herrn Dr. Moritz Huber für die Zweitbetreuung der Thesis sowie an die Experten, die sich die Zeit für die Interviews nahmen.

Fabian Döbber leistet mit dieser Masterarbeit einen wichtigen Beitrag zur Debatte über die digitale Transformation der Polizei. Aufbauend auf Arbeiten von Sebastian Fritz (Band 19, 2018-19) und Moritz Huber (Promotion, 2022), die sich bereits mit früheren Entwicklungsstufen smarter Polizeitechnologien befassten, erweitert er den Diskurs um aktuelle und künftige Technologien, insbesondere aus den Bereichen erweiterte und virtuelle Realität, generative KI und automatisierte Berichts- und Einsatzplanung.

Besonders hervorzuheben sind die praxisnahen Überlegungen und Szenarien, die der Autor entwickelt und die zum direkten Ausprobieren einladen, wie etwa die KI-gestützte Einsatzplanung bei Fußballspielen oder Großdemonstrationen, die Kostenkalkulation virtueller Tatortrekonstruktionen oder die Simulation von Bodycam-Einsätzen mit automatisierter Berichtserstellung. Diese Beispiele verdeutlichen, dass die disruptive Kraft neuer Technologien nicht nur in ihrer Funktionalität liegt, sondern auch in der

Geschwindigkeit, mit der sie Daten auswerten und Entscheidungsprozesse unterstützen können. Sie zeigen aber auch auf, warum es wichtig ist, dass die Polizei über eigene, vertrauenswürdige und sichere generative künstliche Intelligenz verfügen sollte.

Abschließend bleibt festzuhalten, dass diese Arbeit nicht nur analytisch überzeugt, sondern auch Impulse für die praktische Polizeiarbeit liefert. Die formulierten Handlungsempfehlungen, von rechtlichen Anpassungen über die Einrichtung von Test- und Experimentierfeldern bis hin zum Kompetenzaufbau in den Polizeibehörden, zeigen konkrete Wege auf, wie der Einsatz smarter Technologien rechtsstaatlich und sicher gestaltet werden kann.

In der Tradition von Ernst Benda, der betonte: „Den Polizei- und Überwachungsstaat wollen wir nicht. Aber wir wollen, dass der Staat seine Sicherheitsaufgaben angemessen erfüllt“, steht diese Masterarbeit exemplarisch für eine wissenschaftlich fundierte, kritisch reflektierte und zugleich praxisorientierte Auseinandersetzung mit der Digitalisierung der Polizei im 21. Jahrhundert.

Friedrichshafen, 04. März 2025

Jörn von Lucke

Zusammenfassung

Künstliche Intelligenz und smarte Technologien sind Schlüsseltechnologien, um die Polizeiarbeit effizienter und zielgerichteter zu gestalten. Ihr Einsatz ergibt sich jedoch eine ganze Reihe an Vorgaben, Herausforderungen und Risiken, welche es bei Implementierung zu beachten gilt. Diese Masterthesis untersucht auf Grundlage von leitfadengestützten Experteninterviews und vor dem Hintergrund der Häfler Definition des Smart Government und dem Real-Time Government-Ansatz eine Reihe an möglichen polizeilichen Anwendungsfällen für KI, smarte Technologien, AR und VR. Weiterhin werden die verschiedenen Herausforderungen und Risiken des Technologieeinsatzes betrachtet, wobei ein besonderer Fokus auf dem Datenschutz liegt. Im Ergebnis empfiehlt es sich, den initialen Fokus auf polizeiliche KI-Anwendungen ohne Grundrechtseingriffe zu legen. Zudem ist der Aufbau digitaler Souveränität und die Förderung von KI-Kompetenz innerhalb der Polizei essenziell, um die nötigen Grundlagen für den KI-Einsatz zu schaffen.

Abstract

Artificial intelligence and smart technologies are key technologies for making police work more efficient and targeted. However, their use results in a whole range of requirements, challenges and risks that need to be considered during implementation. Based on guided expert interviews and within the framework of the Häfler definition of smart government and the real-time government approach, this master's thesis examines a range of possible police use cases for AI, smart technologies, AR and VR. The various challenges and risks associated with the use of technology are also considered, with a particular focus on data privacy and protection. The findings suggest that the initial focus should be on AI applications in policing that do not interfere with fundamental rights. In addition, establishing digital sovereignty and the promotion of AI expertise within the police are essential to lay the necessary foundations for the use of AI.

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

Abkürzungsverzeichnis

AIP	American Institute of Physics
AR	Erweiterte Realität (engl. Augmented Reality)
ARCD	Auto- und Reiseclub Deutschland e.V.
BDK	Bund Deutscher Kriminalbeamter
BDSG	Bundesdatenschutzgesetz
BfDI	Bundesbeauftragte(r) für den Datenschutz und Informationsfreiheit
BKA	Bundeskriminalamt
BKAG	Bundeskriminalamtgesetz
BMI	Bundesministerium des Innern und für Heimat
BOS	Behörden und Organisationen mit Sicherheitsaufgaben
BSI	Bundesamt für Sicherheit in der Informationstechnik
BT	Bundestag
BT-Drs.	Bundestag Drucksache
BVerfG	Bundesverfassungsgericht
CDU	Christlich Demokratische Union
CILIP	Civil Liberties and Police (Fachzeitschrift)
CPS	Cyberphysische Systeme
CSU	Christlich Soziale Union
DOI	Digital object identifier
DSGVO	Datenschutzgrundverordnung
DSK	Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder
DuD	Datenschutz und Datensicherheit (Fachpublikation)
EU	Europäische Union
e.V.	Eingetragener Verein
FDP	Freie Demokratische Partei
FOCUS	Fraunhofer-Institut für Offene Kommunikationssysteme
GFF	Gesellschaft für Freiheitsrechte
GG	Grundgesetz
GKI	Generative Künstliche Intelligenz
GmbH	Gesellschaft mit beschränkter Haftung
HDM	Handbuch der maschinellen Datenverarbeitung

Hrsg.	Herausgeber
IGMR	Institut für Informations-, Gesundheits- und Medizinrecht
IM BW	Ministerium des Inneren, für Digitalisierung und Kommunen Baden-Württemberg
INPOL	Informationssystem der Polizei
IOSB	Fraunhofer-Institut für Optronik, Systemtechnik und Bildauswertung
IoS	Internet der Dienste (engl. Internet of Services)
IoT	Internet der Dinge (engl. Internet of Things)
IT	Informationstechnologie
IW	Institut der deutschen Wirtschaft
KfZ	Kraftfahrzeug
KI	Künstliche Intelligenz
KI-VO	Verordnung über künstliche Intelligenz
LKA	Landeskriminalamt
LKW	Lastkraftwagen
LLM	Large Language Model
MDR	Mitteldeutscher Rundfunk
NExT	Netzwerk: Experten für die digitale Transformation der Verwaltung
NGO	Nichtregierungsorganisation (engl. Non-Governmental Organization)
NRW	Nordrhein-Westfalen
OWiG	Gesetz über Ordnungswidrigkeiten
P20	Polizei 2020 (bundesweites Projekt zur Modernisierung und Standardisierung der polizeilichen IT-Verfahren und -Systeme)
PAG	Polizeiaufgabengesetz
PolG	Polizeigesetz
PwC	PricewaterhouseCoopers International
RAF	Rote-Armee-Fraktion
RAG	Retrieval Augmented Generation
RAND	Research and development corporation (Think Tank)
SPD	Sozialdemokratische Partei Deutschland
StPO	Strafprozessordnung
StVO	Straßenverkehrsordnung
SWR	Südwestrundfunk

SWOT	Strengths, Weaknesses, Opportunities, Threats (Analyseinstrument zum strategischen Management)
TatuP	Zeitschrift für Technikfolgenabschätzung in Theorie und Praxis
USA	Vereinigte Staaten von Amerika (engl. United States of America)
VeRA	Verfahrensübergreifendes Recherche und Analysesystem
VR	Virtuelle Realität (engl. Virtual Reality)
WD	Wissenschaftliche Dienste des Deutschen Bundestages
ZDF	Zweites Deutsches Fernsehen

Gender Hinweis

Zur besseren Lesbarkeit wird in dieser Publikation das generische Maskulinum verwendet. Die in dieser Arbeit verwendeten Personenbezeichnungen beziehen sich – sofern nicht anders kenntlich gemacht – auf alle Geschlechter.

1. Einleitung

1.1. Problemstellung und Relevanz des Themas

Künstliche Intelligenz (KI) erfährt spätestens seit der ersten Veröffentlichung von leistungsfähigen generativen KI-Programmen wie ChatGPT, Gemini und Midjourney ein reges Interesse. Die wachsende Bedeutung des Themas KI spiegelt sich auch in der Verordnung über künstliche Intelligenz (informell KI-Verordnung) der Europäischen Union (EU) wider, welche im August 2024 in Kraft trat und künftig die Entwicklung und den Einsatz von KI in der EU regulieren soll. Auch der öffentliche Sektor, allen voran die Polizei, ist von dieser Entwicklung betroffen. KI gilt hier als Schlüsseltechnologie bei der Abwehr von Gefahren, Bekämpfung von Kriminalität und Ermittlung von Straftaten. Damit wird KI zu einem zentralen Bestandteil der technologischen Unterstützung der Polizei im Sinne eines Smart und Real-Time Governments.

Erste Ansätze von KI finden sich bereits heute in der Polizei in Deutschland, wobei die Auswertung von großen Mengen an Bild- und Videodaten im Rahmen von Ermittlungen im Bereich sexueller Missbrauchsdarstellungen von Kindern das bekannteste Beispiel ist (Laude, Reinhardt & Bomert 2023, S. 1517ff). Angesichts der rasanten technologischen Entwicklung von KI-Systemen sind die Einsatzmöglichkeiten jedoch nicht allein auf diesen Bereich begrenzt und können künftig sogar Ansätze für eine Polizeiarbeit nahezu in Echtzeit beinhalten. Ein stärkerer Einsatz von KI in der Polizei zusammen mit anderen modernen und smarten Technologien ist insbesondere deswegen relevant, da auch aufseiten von Kriminellen eine zunehmende Technologisierung stattfindet, mit welcher die Polizei Schritt halten muss. Dies betonte auch der Präsident des Bundeskriminalamts (BKA) Holger Münch im Rahmen der 69. Herbsttagung des BKA (Mahnke 2024). Entsprechend lautet die erste Forschungsfrage dieser Arbeit:

> Welche neuen Ansätze für smarte Technologien und künstliche Intelligenz gibt es, um die Polizei in Deutschland im Sinne einer Polizei 4.0 und 5.0 bei ihrer Arbeit zu unterstützen?

Da die Cyberkriminalitätsbekämpfung ein hochspezialisierter und technisch anspruchsvoller Bereich ist, werden diesbezügliche Anwendungen in dieser Arbeit ausgeklammert. Der Fokus liegt stattdessen auf Anwendungsfällen für die allgemeine Polizeiarbeit der Polizeibehörden von Bund und Ländern, welche im Rahmen einer ersten Recherche als besonders vielversprechend eingestuft und basierend auf den Ergebnissen der vorgenommenen Experteninterviews weiter konkretisiert wurden.

Daneben ist ein polizeilicher Einsatz von KI und smarten Technologien allerdings auch mit einer ganzen Reihe an Anforderungen, Herausforderungen und Risiken verbunden, nicht zuletzt für die Freiheit der betroffenen Bürger durch übermäßige staatliche Überwachungsmaßnahmen. Aus diesem Grund lautet die zweite Forschungsfrage:

> Welche konkreten Anforderungen, Probleme und Risiken ergeben sich im Zusammenhang mit diesen Technologien beim Einsatz durch die Polizei?

Der folgende Abschnitt gibt zuerst einen Überblick über ausgewählte Veröffentlichungen, welche sich dem Einsatz smarter Technologien, Big Data und KI durch die Polizei widmen. Im Anschluss daran folgt ein Gesamtüberblick über den Aufbau dieser Arbeit.

1.2. Literaturüberblick und Stand der Forschung

Im Hinblick auf smarte Polizeiarbeit im Sinne der Häfler Smart Government Definition baut diese Arbeit auf früheren Arbeiten zu diesem Thema auf. Fritz (2020) untersuchte hierzu im Rahmen seiner Masterarbeit Chancen, Risiken und Herausforderungen sowie den Status Quo smarter Polizeiarbeit in Deutschland. Hierbei überwiegen beim Status Quo die identifizierten Schwächen die Stärken, während die Chancen die potenziellen Risiken überwiegen. Diesbezüglich handelt es sich um eine „Strategie des Aufholens". (Fritz 2020, S. 97). Die von Fritz interviewten Experten sehen den Einsatz von KI-Systemen perspektivisch vor allem in unterstützenden Funktionen (ebd., S. 75). Gleichzeitig befand sich KI als Technologie laut einem der interviewten Experten zu diesem Zeitpunkt gerade erst am Anfang ihres Einsatzes in der Polizei (ebd., S. 76). Unter Bezugnahme auf die Arbeit von Fritz wirft von Lucke (2020) einen kritischen Blick auf die disruptive Wirkung smarter Technologien auf die Polizeiarbeit in einem demokratischen Rechtsstaat und die damit verbundene Gefahr übermäßiger staatlicher Eingriffe in die Privatsphäre seiner Bürger. Hierzu verweist er auf bereits im Einsatz befindliche smarte Technologien und wie diese insbesondere in Asien zur Überwachung von Bürgern genutzt werden. Gleichzeitig nennt er eine Reihe an Voraussetzungen, um die Potenziale smarter Polizeiarbeit in Deutschland ausschöpfen zu können, ohne dass es zu flächendeckenden Überwachungsmaßnahmen kommt, welche die offene und freie Gesellschaft gefährden (von Lucke 2020, S. 121f). Beispiele für datenschutzkonforme und ethisch vertretbare Ansätze smarter Polizeiarbeit präsentiert Huber (2022), welcher im Rahmen seiner Dissertation am Beispiel der Stadt Ulm Potenziale einer urbanen Sicherheitsarchitektur 4.0 erforscht. Von den neun entwickelten Anwendungskonzepten können vier ohne weiteres weiterentwickelt und implementiert werden, während dies für zwei Konzepte im Rahmen enger Grenzen pilothaft möglich ist (Huber 2022, S. 253). Weiterhin geht Huber

ausführlich auf mögliche Gefahren im Bereich smarter Sicherheitslösungen, sowie mögliche Gegenmaßnahmen ein und schließt mit einer Reihe an Handlungsempfehlungen für die Stadt Ulm.

Insbesondere vorausschauende Polizeiarbeit (Englisch Predictive Policing) und algorithmenbasierte Videoüberwachung sind vieldiskutierte Beispiele für bereits im Einsatz befindliche Ansätze smarter Polizeiarbeit. Bezüglich Predictive Policing können an dieser Stelle die Arbeiten von Perry, McInnis, Price, Smith und Hollywood (2013) sowie Knobloch (2018) hervorgehoben werden. Beide zielen darauf ab, politischen Entscheidungsträgern und Behörden in den Vereinigten Staaten (USA) und Deutschland Orientierungshilfen und Verbesserungsvorschläge für den Einsatz von Predictive Policing zu geben (Knobloch 2018, S. 4; Perry et al. 2013, S. xiii). Hinsichtlich intelligenter Videoüberwachung diskutieren Apelt und Möllers (2011) auf Basis früherer Forschungsarbeiten zentrale Problemfelder dieser Technologie und leiten hieraus Empfehlungen für eine interdisziplinäre Herangehensweise an ein geplantes Projekt ab (Apelt & Möllers 2011, S. 591). Golda, Cormier und Beyerer (2023) stellen in ihrer Arbeit das gemeinsame Pilotprojekt des Fraunhofer-Instituts für Optronik, Systemtechnik und Bildauswertung (IOSB), des Landes Baden-Württemberg und des Polizeipräsidiums Mannheim als datenschutzkonformes Beispiel für eine algorithmenbasierte Videoüberwachung vor.

Stock (2023) widmet sich in seinem Kapitel aus dem „Handbuch Polizeimanagement" den Herausforderungen des polizeilichen Auftragsverständnis im Zuge der Digitalisierung. Hierbei geht er unter anderem auf einen aus Sicht der Polizei herrschenden Widerspruch ein, dass dieser im Gegensatz zu Unternehmen bestimmte Befugnisse zur Datenspeicherung fehlen beziehungsweise stark reglementiert sind. Dies schränke widerum die Fähigkeit der Polizei zur Bekämpfung von Cyberkriminalität ein, beispielsweise durch fehlende Rechte zur Mindestspeicherung von Verbindungsdaten (Stock 2023, S. 1454f). Weiterhin gibt der Autor Ratschläge zur Implementierung und zum Einsatz von Cloudtechnologien und KI. Laude, Reinhardt und Bomert (2023) beschreiben in einem weiteren Kapitel drei aktuelle Anwendungsbeispiele für den Einsatz von KI, Data Science und Big Data zur Auswertung von Massendaten in der Polizei Niedersachsens. Ein Beispiel ist hier die bereits eingangs erwähnte Unterstützung bei Ermittlungen im Bereich sexueller Missbrauchsdarstellungen von Kindern (Laude, Reinhardt & Bomert 2023, S. 1517ff).

Bereits im Jahr 2017 haben sich Gerrit Hornung und Stephan Schindler mit den rechtlichen Voraussetzungen und Grenzen für eine algorithmenbasierten Auswertung biometrischer Daten in Bild- und Videoaufnahmen auseinandergesetzt. Zum Zeitpunkt der Veröffentlichung fehlte es laut den Autoren an expliziten gesetzlichen Regelungen für den Einsatz dieser

Technologie (Hornung & Schindler 2017, S. 206). Obwohl nicht jede Maßnahme in diesem Zusammenhang von vornherein als verfassungswidrig einzustufen ist, betonen die Autoren, dass besonders intensive Maßnahmen klare Ermächtigungsgrundlagen mit hohen Eingriffsschwellen benötigen bis hin zum Verbot bestimmter Maßnahmen (ebd., S. 205f, 208). Farthofer (2022) wiederum beschäftigt sich mit der rechtlichen Vereinbarkeit von KI-Systemen zum Predictive Policing. Laut der Autorin ist hierbei vor allem die Art der verwendeten Daten sowie die Datenqualität von entscheidender Bedeutung, was klare gesetzliche Standards zur Datensammlung erfordere (Farthofer 2022, S. 20). Jedoch mangelt es laut der Autorin weiterhin an geeigneten gesetzlichen Grundlagen, weshalb diesbezüglich ein großer Nachholbedarf bestehe (ebd., S. 16, 20). Um vonseiten des Gesetzgebers der Herausforderung zu begegnen, dass die gesetzlichen Eingriffsgrundlagen des Polizeirechts mit dem technischen Fortschritt von KI-Systemen nur schwer schritthalten können, empfiehlt Golla (2020) das Konzept eines „lernfähigen Polizeirechts". Wie komplex eine Regulierung von Technologien ist, verdeutlicht er am Beispiel des Versuchs von Bund und Ländern, Rechtsgrundlagen für eine KI-gestützte Videoüberwachung und automatisierte Datenauswertung zu schaffen (Golla 2020, S. 155-159).

1.3. Aufbau der Arbeit

Einleitend wurden bereits die Problemstellung und die Relevanz des Themas erläutert sowie ein Überblick über bestehende Literatur und den aktuellen Forschungsstand gegeben, auf der diese Arbeit aufbaut und anknüpft. Im zweiten Kapitel wird nun die Methode des leitfadengestützten Experteninterviews vorgestellt, welche als zentrale Grundlage zur Beantwortung der Forschungsfragen aus Abschnitt 1.1. dient. Daraufhin werden im dritten Kapitel die zentralen theoretischen und konzeptionellen Grundlagen der Arbeit behandelt. Im Anschluss folgt in Kapitel vier eine Betrachtung des thematischen Hintergrunds, welche den Begriff der „Sicherheit", die Organisation der Polizei auf Ebene des Bundes und der Länder sowie die unterschiedlichen Arten polizeilicher Maßnahmen beinhaltet. In Kapitel fünf werden anhand der Kategorien „Information und Analyse" und „Automation und Steuerung" ausgewählte smarte Technologien beleuchtet, die bereits heute bei der Polizei in Deutschland im Einsatz sind. In Kapitel sechs werden ausgewählte neue Anwendungsfälle von KI und smarten Technologien für die Bereiche Einsatzmanagement, operative Prozesse und polizeiliche Kernaufgaben präsentiert. Ergänzend werden mit der Polizei-Cloud, polizeilichen Datenplattformen und dem Polizei-Datenraum zentrale Grundlagen für den Austausch und das Management von Big-Data vorgestellt. Im Anschluss werden in Kapitel sieben verschiedene technische, rechtliche, gesellschaftlich-politische und polizeiinterne Herausforderungen und Vorgaben erörtert, welche es bei der Einführung von KI und neuen smarten Technologien in der Polizei allgemein zu beachten gilt. Ein besonderer Fokus

liegt hierbei auf dem Datenschutz. Auf Grundlage dieser Befunde wird in Kapitel acht ein Zielbild für den Polizeieinsatz formuliert und eine SWOT-Analyse durchgeführt, welche die Stärken, Schwächen, Chancen und Risiken des Einsatzes smarter Technologien und KI durch die Polizei beleuchtet. Hieraus werden in Kapitel neun Handlungsempfehlungen abgeleitet. Abschließend wird in Kapitel zehn ein Fazit gezogen sowie ein Ausblick auf weiteren Forschungsbedarf gegeben.

2. Methodik

Methodisch wurde für diese Arbeit in Anlehnung an Fritz (2020, S. 48) ein qualitatives Forschungsdesign mit leitfadengestützten Experteninterviews gewählt, da das Thema fortschrittlicher KI in der Polizei sehr aktuell und entsprechend wissenschaftlich noch relativ unerforscht ist. Beim qualitativen Experteninterview handelt es sich um ein „systematisches und theoriegeleitetes Verfahren der Datenerhebung in Form der Befragung von Personen, die über ein exklusives Wissen […] verfügen" (Kaiser 2021, S. 9). Als Methode zielt das Experteninterview darauf ab, am speziellen Wissen des Experten teil zu haben und neue Erkenntnisse zu gewinnen, welche über die in der Literatur verfügbaren hinausgehen (Bogner, Littig & Menz 2009, S. 65). Die Interviews orientieren sich an einem standardisierten Leitfaden, um die Vergleichbarkeit der Ergebnisse zu gewährleisten. Bei besonders aufschlussreichen Antworten besteht jedoch die Möglichkeit, zur Vertiefung bestimmter Aspekte ergänzende Fragen zu stellen (Gläser & Laudel 2010, S. 42).

Die Auswahl der jeweiligen Experten erfolgte einerseits aufgrund ihrer Position, andererseits aufgrund ihres relevanten Funktionswissens zum Thema (Kaiser 2021, S. 44f). Hinsichtlich der Position lag der Fokus vor allem auf behördeninternen Verantwortlichen für die Digitalisierung, einer Beteiligung des jeweiligen Experten an einem Digitalisierungsprojekt der Polizei oder der Zugehörigkeit zu einer bestimmten Institution. Hinsichtlich des Funktionswissens wurden die Experten aufgrund früherer Veröffentlichungen zum Thema KI und Digitalisierung der deutschen Polizei ausgewählt. Die Auswahl der Experten erfolgte aus den Bereichen der „Wissenschaft", „Recht", „IT-Wirtschaft", „Zivilgesellschaft" und „Polizei" und „Verwaltung". Auf Experten aus dem Bereich der „Politik" wurde bewusst verzichtet, da das Thema des polizeilichen Technologieeinsatzes parteipolitisch weitgehend neutral behandelt werden soll und für das Erkenntnisinteresse dieser Arbeit nachrangig ist. Zudem wäre es schwierig gewesen, im Rahmen dieser Arbeit das gesamte Feld an unterschiedlichen parteipolitischen Positionen abzudecken. Stattdessen wurde der Fokus auf die rechtlichen, technischen und gesellschaftlichen Rahmenbedingungen gelegt. Weiterhin sollte geprüft werden, welche Anwendungsfälle aus einer polizeifachlichen Sicht sinnvoll sind.

Vorab wurde mit dem Betreuer dieser Arbeit als Zielgröße zehn Experteninterviews vereinbart, um einen möglichst breiten Input für die spätere Auswertung zu erhalten. Insgesamt wurden 16 Experten direkt oder indirekt über eine Anfrage an ihre jeweilige Institution per E-Mail kontaktiert. Hiervon antworteten 15 der Angefragten. In vier Fällen erfolgte eine Absage, in drei

Fällen wurde das Interview mit einem Stellvertreter[1] des ursprünglich angefragten Experten geführt. Insgesamt wurden 11 Interviews geführt. In einem Fall wurde einer Sprachaufzeichnung nicht zugestimmt, weshalb dieses Interview lediglich als Hintergrundgespräch für weitere Recherchen genutzt wurde. Tabelle 1 enthält eine anonymisierte Übersicht über die durchgeführten Experteninterviews.[2] [3]

Kürzel	Position	Bereich/Sektor
E1	Professor für Öffentliches Recht	Wissenschaft/Recht
E2	Mitarbeiter in einem IT-Dienstleistungsunternehmen	Wirtschaft
E3	Vertriebsleiter eines IT-Dienstleistungsunternehmens, ehemaliger Polizeibeamter	Wirtschaft
E4	KI-Wissenschaftler in einem deutschen Forschungsinstitut	Wissenschaft
E5	Projektleiter in einem IT-Dienstleistungsunternehmen	Wirtschaft
E6	Wissenschaftlicher Leiter eines Cybersicherheitsunternehmens	Wissenschaft/ Wirtschaft
E7	Jurist in einer Nichtregierungsorganisation (NGO) für Grund- und Menschenrechte	Zivilgesellschaft/ Recht
E8	Professor für Strafrecht	Wissenschaft/Recht
E9	Externer Berater des Bundesinnenministeriums	Wirtschaft
E10	Führungskraft in einem Polizeipräsidium (Landespolizei)	Polizei

Tabelle 1: Übersicht Experteninterviews inklusive Funktion und Expertenbereich

Die Erstellung des Interviewleitfadens orientierte sich an der Gliederung dieser Arbeit und erfolgte in Abstimmung mit dem Betreuer. Der finale Interviewleitladen[4] beinhaltet insgesamt 31 Fragen, welche in vier Teile aufgeteilt wurden: „Einstieg", „Neue Einsatzfelder", „Anforderungen, Herausforderungen und Risiken" und „Abschluss und Blick in die Zukunft". Der

[1] Grund hierfür ist unter anderem, dass die Experten zum Teil Führungspositionen innehaben und entweder aus Zeitmangel nicht verfügbar waren oder ihre Stellvertreter aufgrund eigener Expertise besser geeignet sind.
[2] Eine ausführliche Übersicht findet sich in Anhang I.
[3] Zur vollständigen Anonymisierung wird im Folgenden in Bezug auf die befragten Expertinnen und Experten ausschließlich die männliche grammatikalische Form verwendet.
[4] Eine Übersicht über den Interviewleitfaden findet sich in Anhang II.

Einstiegsteil dient dazu, den Experten an das Thema heranzuführen, während der zweite Teil der Operationalisierung der ersten Forschungsfrage diente und Fragen zum Big-Data Management und technischen Einsatzmöglichkeiten sowie eine Beurteilung der Stärken, Chancen und Schwächen der Technologien für die abschließende SWOT-Analyse der Arbeit beinhaltet. Die Fragen zu den Einsatzmöglichkeiten sind bewusst offen gestaltet, um mögliche weitere Ansätze zu ermitteln. Der dritte Teil des Leitfadens diente der Operationalisierung der zweiten Forschungsfrage. Im vierten Teil sollten abschließend positive sowie negative Eindrücke hinsichtlich eines zukünftigen Technologieeinsatzes gewonnen und damit zusammenhängend Handlungsempfehlungen der verschiedenen Experten gesammelt werden. Den Experten wurde im Falle einer Zusage angeboten, vorab den Interviewleitfaden zugeschickt zu bekommen. Aufgrund einer aktuellen Entwicklung im Laufe der Bearbeitungsphase wurde Frage 18 angepasst.[5] Die meisten Interviews dauerten im Schnitt zwischen 60 und 70 Minuten. Eine Ausnahme bildete hier das Interview drei, für welches aufgrund des Umfangs seitens des Experten um ein längeres Gespräch gebeten wurde. Da es sich hierbei um einen ehemaligen Polizeibeamten handelte und das Interview vergleichsweise früh während des Forschungs- und Bearbeitungsprozesses stattfand, wurde es zusätzlich dazu genutzt mehr über die Hintergründe der polizeilichen Arbeit zu erfahren. Alle Interviews wurden online durchgeführt und in diesem Rahmen auch aufgezeichnet und im Anschluss automatisch transkribiert. Während der Interviews wurde ein Precoding-Bogen genutzt, um die spätere Auswertung der Interviews zu erleichtern.

Die Auswertung der Transkripte erfolgte mithilfe des Programms „Atlas.ti", welches den übersichtlichen Vergleich, die Kommentierung sowie Kodierung von relevanten Textstellen innerhalb der Transkripte ermöglicht. Die Kodierung orientierte sich dabei am Precoding-Bogen. Ergänzend zu den Interviews wurden außerdem verfügbare Dokumente analysiert, um die Datenbasis zu erweitern, Aussagen aus den Interviews bei Bedarf zu kontextualisieren und zusätzliche Perspektiven einfließen zu lassen (Gläser & Laudel 2010, S. 105; Kaiser 2021, S. 129f).

[5] Diese Anpassung betraf eine Anpassung der Einleitung der Frage aufgrund der Verabschiedung des Sicherheitspaketes durch den Bundestag. In Anhang II befindet sich der Leitfaden in seiner finalen Version.

3. Theoretischer Hintergrund

In Kapitel drei werden die wichtigsten theoretischen und konzeptionellen Hintergründe für den Einsatz smarter Technologien und künstlicher Intelligenz durch die Polizei erläutert. Hierzu wird im Folgenden näher auf das Internet der Dinge und Internet der Dienste das Smart und Real-Time Government, Big Data sowie den Begriff und verschiedene Ansätze von künstlicher Intelligenz eingegangen. In diesem Zusammenhang werden auch bereits erste allgemeine Risiken dargestellt, welche für das Thema dieser Arbeit bedeutsam sind.

3.1. Internet der Dinge und Internet der Dienste

Das „Internet der Dinge“ (Englisch Internet of Things - IoT) bezeichnet ein Netzwerk physischer Objekte, welche mit Sensoren, Aktoren und Funkchips zur Informationsübermittlung ausgestattet sind. Durch Vernetzung erhalten diese Objekte eine eigene virtuelle Identität, welche eine Kommunikation zwischen Mensch und Objekt sowie den Objekten untereinander ermöglicht (von Lucke 2016, S. 173, 175). Man spricht hierbei auch von „intelligent vernetzten“ Objekten (ders. 2015, S. 1).

Mithilfe der Sensoren können intelligent vernetzte Objekte Daten zu ihrer Umgebung sammeln, während die Aktoren zur datenbasierten Steuerung bestimmter Aktionen dienen. Im Ergebnis erhalten diese Objekte so eine erweiterte Funktionalität, wodurch sie in IT-Systeme und komplexere cyberphysische Systeme (CPS) eingebettet werden können, welche eine Vielzahl intelligent-vernetzter Objekte zur Erledigung bestimmter Aufgaben miteinander verbinden (ebd., S. 14). Die Verbindung der Objekte und darauf aufbauender CPS erfolgt mittels der IP-Protokolle, wodurch diese über ihre IP-Adresse eindeutig identifizierbar sind (ders. 2016, S. 175). Personen und andere vernetzte Objekte können so mittels Apps, Programmen und Diensten die eingebetteten Objekte und CPS kontaktieren, nutzen und gegebenenfalls auch steuern (ebd., S. 175). Einerseits können sie Menschen so durch die gesammelten Daten und deren Analysen unterstützen, andererseits können sie aber auch mittels Automation und Steuerung selbstständig Aufgaben übernehmen (ebd., S. 173). Neben dem Einsatz in der Industrie (Industrial IoT) spielen intelligent-vernetzte Objekte und das Internet der Dinge inzwischen in Form von „Smartphones“, „Smart TVs“, „Smart Homes“ und vernetzten Autos eine zentrale Rolle im alltäglichen Leben (Consumer IoT) (Flügge & Fromm 2016, S. 5ff).

Das Internet der Dinge ist eng verbunden mit dem Internet der Dienste (Englisch Internet of Services - IoS). Dies beruht darauf, dass eine Vielzahl realer Dinge mit vergleichbarer Funktionalität auch in webbasierte Dienste überführen und sich durch neue, praktische Funktionen erweitern lassen

(von Lucke 2015, S. 19). Im Internet der Dienste werden diese Dienste und bestimmte Funktionalitäten primär als feingranulare Softwarekomponenten abgebildet und von Providern auf Anforderung über das Internet zur Verfügung gestellt (ebd., S. 19). Ermöglicht wird dies über Web-Services, Cloud-Computing und standardisierte Schnittstellen (ebd., S. 19). Praktische Beispiele für das Internet der Dienste sind Plattformdienste und Software-as-a-Service, welche Software ohne lokale Installation über das Internet zur Verfügung stellt.

Das Internet der Dinge und das Internet der Dienste bieten zahlreiche Möglichkeiten zur Optimierung von Prozessen und Fachverfahren durch effizientere Abläufe, Automatisierungen und Vermeidung von Medienbrüchen. Gleichzeitig ergeben sich mit diesen neuen Technologien eine Reihe an Herausforderungen und Risiken. Zu nennen wären hier die Interoperabilität der vernetzten Objekte und Dienste, Cybersicherheit, sowie die Verfügbarkeit drahtloser Kommunikationsnetze mit ausreichend hoher Bandbreite (Flügge & Fromm 2016, S. 17f). Des Weiteren ist auf den Datenschutz zu verweisen, insbesondere wenn personenbezogene Daten durch intelligent-vernetzte Objekte erhoben und verarbeitet werden. Mit Blick auf die Möglichkeiten der Prozess- und Verfahrensautomatisierung stellt sich außerdem die kritische Frage, welche Prozesse und Verfahren für eine Automatisierung geeignet sind und wie abhängig man in Zukunft von bestimmten Technologien sein möchte (von Lucke 2015, S. 20f).

Web 5.0	Taktiles Internet	Netzwerkkommunikation nahezu in Echtzeit	Real-Time Government
Web 4.0	Internet der Dinge & Internet der Dienste	Smarte Objekte, Cyberphysische Systeme	Smart Government
Web 3.0	Internet der Daten Semantisches Web	Linked Data, Open Data, Big Data, Big Data Analytics	Open Government Data
Web 2.0	Internet der Menschen Internet zum Mitmachen	Netzwerkkommunikation über Social Media	Open Government
Web 1.0	Internet der Systeme World Wide Web	Netzwerkkommunikation über das World Wide Web	Electronic Government

Abbildung 1: Häfler Stufenmodell für die weitere Entwicklung des Internet und des World Wide Webs (von Lucke 2016, S. 175)

Mit Blick auf die Entwicklungsgeschichte des Internets und des World Wide Web bilden das Internet der Dinge und das Internet der Dienste die vierte Generation (Web 4.0). Die einzelnen Entwicklungsschritte des Internet und des World Wide Webs werden im „Häfler Stufenmodell" aufgezeigt (siehe Abbildung 1). Hierbei ist die jeweilige Entwicklungsstufe mit einer bestimmten Form des Verwaltungshandelns verbunden, welche von der jeweiligen Entwicklungsstufe des Internets geprägt ist. Im Falle des Web 4.0 und des darauf aufbauenden Web 5.0 sind dies das „Smart" und das „Real-Time Government", auf welches im folgenden Abschnitt eingegangen wird.

3.2. Smart Government und Real-Time-Government

Für den Begriff „smart" beziehungsweise „Smartness" gibt es keine einheitliche Definition. Entsprechend gibt es vielseitige Assoziationen mit diesen Begriffen. Im Deutschen wird dieser Begriff des Öfteren mit „clever", „gewitzt" oder auch als „von modischer und auffallend erlesener Eleganz" übersetzt (Dudenredaktion o.J.). Vor dem Hintergrund des Themas dieser Arbeit und dem in Abschnitt 3.1 bereits erläuterten Internet der Dinge soll smart gleichbedeutend sein mit „intelligent-vernetzt". Dies rührt daher, dass man den vernetzten Objekten eine gewisse eigene „Intelligenz" zuspricht, wenn diese im Internet der Dinge mit Menschen oder anderen vernetzten Objekten interagieren, auch wenn eine „Intelligenz" im Sinne von Denkvermögen und Weisheit nicht vorliegt (von Lucke 2015, S. 2).

Ähnlich wie für den Begriff smart existiert keine einheitliche Definition für Smart Government. Einerseits finden sich hier Ansätze, welche unter Smart Government den vermehrten Einsatz innovativer und datenbasierter Technologien durch Regierungsbehörden zur verbesserten staatlichen Leistungserbringung verstehen. Andererseits finden sich aber auch Definitionen, welche den Begriff smart in seiner ursprünglichen Weise als „cleveres", „geschicktes" oder „gewitztes" Regierungs- und Verwaltungshandeln verstehen (ebd., S. 3f). Diese Arbeit folgt hierbei dem ersteren Ansatz und bezieht sich wie Fritz (2020) und Huber (2022) hierzu auf die umfassende „Häfler Definition von Smart Government":

> *„Unter **Smart Government** soll die Abwicklung geschäftlicher Prozesse im Zusammenhang mit dem Regieren und Verwalten (Government) mit Hilfe von intelligent vernetzten Informations- und Kommunikationstechniken verstanden werden. Ein **intelligent vernetztes Regierungs- und Verwaltungshandeln** nutzt die Möglichkeiten intelligent vernetzter Objekte und cyberphysischer Systeme zur effizienten wie effektiven Erfüllung öffentlicher Aufgaben. Dies schließt das Leistungsportfolio von E-Government und Open Government einschließlich Big Data und Open Data mit ein. Im Kern geht es um ein nachhaltiges Regierungs- und Verwaltungshandeln im Zeitalter des Internets der Dinge und des Internets der Dienste, die technisch auf dem Internet der Systeme, dem Internet der Menschen und dem Internet der Daten aufsetzen."* (von Lucke 2015, S. 4)

Die Häfler Definition bezieht sich hierbei auf das intelligent vernetzte Regierungs- und Verwaltungshandeln des gesamten öffentlichen Sektors, was neben den drei Bereichen der Staatsgewalt Legislative, Exekutive und Jurisdiktion auch öffentliche Unternehmen mit einschließt (ebd., S. 4).

Smart Government bietet zahlreiche Chancen für ein effizienteres und effektiveres Regierungs- und Verwaltungshandeln. Beispielsweise können mithilfe der eingesetzten Sensoren in umfassender und qualitativ hochwertiger Weise Daten erhoben und ausgewertet werden, so auch bei großen Flächen und an entfernt liegenden Orten (Djeffal 2017, S. 810). Bürgern können verbesserte und innovative Verwaltungsleistungen schneller, günstiger und individueller zur Verfügung gestellt werden (von Lucke 2015, S. 24). Des Weiteren können Verwaltungsmitarbeiter durch die unterstützenden Funktionen der verwendeten Technologien und Dienste entlastet werden (ebd., S. 24). Neben diesen Vorteilen ergeben sich jedoch auch Herausforderungen und Risiken, beispielsweise die Gefahr schwerwiegender technischen Fehlfunktionen, die Cybersicherheit der Systeme und die Folgen von Hackerangriffen (Djeffal 2017, S. 810). Weiterhin ist auf gesetzliche Vorgaben zum Regierungs- und Verwaltungshandeln zu verweisen, welche dem Einsatz smarter Technologien rechtliche Grenzen setzen. Hervorzuheben sind hier insbesondere der Bereich Datenschutz und Verarbeitung personenbezogener Daten (ebd., S. 811f).

Aufbauend auf dem Internet der Dinge und dem Internet der Dienste stellt das taktile Internet die nächste Stufe des Internets (Web 5.0) dar, welches eine Netzwerkkommunikation nahezu in Echtzeit ermöglicht (siehe hierzu erneut Abbildung 1 auf Seite 26). Ermöglicht wird dies durch ein zunehmend verfügbares Gigabit-Glasfasernetzwerk, Mobilfunknetzwerke der fünften Generation (5G) sowie leistungsstarke Rechner und Algorithmen (von Lucke 2018, S. 12). Im öffentlichen Sektor bietet das Web 5.0 die Möglichkeit für ein sogenanntes „Real-Time-Government", wobei Verwaltungsentscheidungen auf Basis von Sensordaten nahezu in Echtzeit stattfinden. So ließen sich in der Verwaltung autonome Echtzeit-Entscheidungssysteme aufbauen, welche Verwaltungsprozesse enorm beschleunigen können (ebd., S. 12). Gleichzeitig birgt Real-Time-Government aber auch das Potenzial zum Aufbau umfangreicher und smarter Echtzeit-Überwachungsmaßnahmen, welche die Freiheit der betroffenen Bürger in erheblichem Maße einschränken (ebd., S. 12f).

Eine wichtige Grundlage für die Anwendungen und Verfahren von Smart und Real-Time Government ist „Big Data", weshalb dies zusammen mit Open Data in der Häfler Definition explizite Erwähnung findet. Im nächsten Abschnitt wird daher das Thema Big Data näher beleuchtet.

3.3. Big Data

Der Begriff „Big Data“ beschreibt im Allgemeinen die im Zuge der Digitalisierung entstehende Menge an Massendaten. Wie schon bei Smart Government fehlt es allerdings auch bei Big Data an einer allgemein gültigen Begriffsdefinition. Dies liegt unter anderem daran, dass je nach Definition der Fokus auf unterschiedlichen Aspekten von Big Data liegt. De Mauro, Greco und Grimaldi (2015, S. 103) versuchen deshalb eine neutrale Definition von Big Data zu formulieren, indem sie den Fokus auf den Wert der Informationen (Information Assets) legen:

> *“Big Data represents the Information assets characterized by such a High Volume, Velocity and Variety to require specific Technology and Analytical Methods for its transformation into Value.”*

Die Datenmenge („Volume“), Datenvielfalt („Variety“) und die Geschwindigkeit der zu verarbeitenden Daten („Velocity“) sind dabei zentrale Charakteristika von Big Data. Volume bezieht sich hierbei auf die Menge an Massendaten, welche teilweise im Bereich von Peta- und Exabytes liegt, was für besondere Anforderungen an die Datenübertragung, -verarbeitung und -speicherung sorgt (Alt 2018). Diese Daten stammen aus den unterschiedlichsten Quellen, wozu im Besonderen auch Sensoren von smarten IoT-Geräten gehören. Variety bezeichnet die Heterogenität der Daten in strukturierter sowie unstrukturierter Form (ebd.). Bei strukturierten Daten ist die Form der zu verarbeitenden Daten vorab bekannt und im zu verarbeitenden Datensatz üblicherweise konstant, wodurch diese Daten meist ohne größere Probleme automatisch verarbeitet werden können (Laude et al. 2023, S. 1510). Im Gegensatz dazu ist bei unstrukturierten Daten (z.B. Audio- und Videodaten) abseits des Dateiformats vorab nichts Weiteres zu den Inhalten der Daten bekannt (ebd., S. 1511). Um unstrukturierte Daten zu verarbeiten, müssen diese zuerst und teils mit erheblichem Aufwand aufbereitet werden (Alt 2018). Die Dritte Kategorie Velocitiy beschreibt die hohe Geschwindigkeit, mit der Daten erhoben und verarbeitet werden (ebd.). Je nach Publikation werden diese drei Vs um weitere Eigenschaften wie beispielsweise den Wert („Value“) und die Echtheit von Daten („Veracity“) ergänzt. Ersteres bezieht sich auf den Mehrwert der ausgewerteten Massendaten, häufig im Sinne eines ökonomischen Mehrwertes, während letzteres die Verlässlichkeit, Richtigkeit und Aussagekraft der Daten hinsichtlich ihres Informationsgehalts und der Datenqualität beschreibt (De Mauro, Greco & Grimaldi 2015, S. 103; Fritz 2020, S. 20).

Neben den oben genannten Charakteristika spielen spezifische Technologien und Analysemethoden eine weitere zentrale Rolle für das Verständnis von Big Data. In technischer Hinsicht liegt der Fokus dabei vor allem auf der Schaffung der notwendigen Rechen- und Speicherkapazitäten, um die

Mengen an Massendaten erheben und auswerten zu können (De Mauro, Greco & Grimaldi 2015, S. 101f). Die Analyse von Big Data (Big Data Analysis) wiederum beschreibt eine Vielzahl unterschiedlicher Methoden, Verfahren und Werkzeuge zur Konfiguration und Modellierung von Analyseprozessen zu vergangenheits-, gegenwarts- und zukunftsorientierten Fragestellungen auf Basis von Massendaten (Alt 2018). Aus einer organisatorischen Perspektive ist dabei wichtig, relevante Ergebnisse mit den vorhandenen Abläufen zu verknüpfen und eine Verbindung zur Organisationsstruktur und übergeordneten Strategie herzustellen (ebd.). Dies kann beispielsweise durch die Zusammenführung von Kompetenzen oder die Entwicklung datenbasierter Modelle umgesetzt werden.

Potenziale, welche sich durch den Einsatz von Big Data im öffentlichen Sektor ergeben, sind beispielsweise bessere Entscheidungsgrundlagen für Verwaltungsentscheidungen, Kosteneinsparungen, die Senkung von Risiken durch das frühzeitige Erkennen von Fehlern, mehr Transparenz sowie die bereits in 3.2. erwähnten individuelleren und verbesserten Dienstleistungen für Bürger (Eckert et al. 2014, S. 12; Plazek 2016, S. 9).

Während durch den Einsatz von Big Data-Analysen auf der einen Seite Risiken gesenkt werden können, ergeben sich auf der anderen Seite neue Herausforderungen und Risiken, welche es bei Big Data-Analysen zu beachten gilt. Zu nennen wäre hier einerseits die Qualität der Daten, da hiervon die Genauigkeit der Analyseergebnisse abhängt. Unvollständige, fehlerhafte oder manipulierte Datenbestände beeinflussen die Ergebnisse der Datenanalyse und so auch die darauf aufbauenden Entscheidungen negativ. Eine weitere Herausforderung ist ein Mangel an Experten mit Kenntnissen über die technischen und fachlichen Grundlagen von Big Data, insbesondere im öffentlichen Sektor (Eckert et al. 2014, S. 14). Nicht zuletzt ergibt sich bei der massenhaften Erhebung, Auswertung und Speicherung personenbezogener Daten das bereits in Abschnitt 3.2. erwähnte Risiko des „gläsernen Bürgers“. Insbesondere deshalb ist es essenziell, dass bei Big Data-Analysen die rechtlichen Vorgaben des Datenschutzes eingehalten und datenethische Grundsätze beachtet werden (ebd., S. 13). Plazek verweist zudem darauf, dass Big Data-Analysen im öffentlichen Sektor das Ziel eines gesellschaftlichen Mehrwerts verfolgen müssen (Plazek 2016, S. 7).

Big Data ist eng verbunden mit KI, indem Massendaten einerseits die Arbeitsgrundlage für KI-Systeme bilden, andererseits KI zur Analyse von Big Data eingesetzt wird. Der folgende Abschnitt erläutert deshalb zum Abschluss des theoretischen Hintergrunds das Thema der Künstlichen Intelligenz.

3.4. Künstliche Intelligenz

Der Begriff der „Künstlichen Intelligenz" beschreibt eine Reihe verschiedener Technologien, Systemarchitekturen und Ansätze, welche computerbasiert versuchen, Fähigkeiten menschlicher Intelligenz nachzubilden, um bestimmte Aufgaben eigenständig oder auf Befehl zu übernehmen (von Lucke 2024, S. 8). In ihrem Aufbau basieren KI-Systeme einerseits auf einer leistungsfähigen Hardware für die Rechenoperationen, andererseits auf der bereits im vorherigen Abschnitt skizzierten Big Data sowie Algorithmen, um die Datenmengen zu analysieren. Diese drei Komponenten werden umgangssprachlich als KI-Befähiger (englisch Enabler) bezeichnet und sorgen durch immer größere Rechen- und Speicherkapazitäten und Datenmengen, Vernetzung und maßgeschneiderte Algorithmen für eine beschleunigte Dynamik bei der KI-Entwicklung (BSP Business School Berlin 2021, S. 13).

Hinsichtlich der Fähigkeit von KI-Systemen, menschliche Intelligenz nachzubilden, wird meist zwischen schwacher und starker KI sowie der Superintelligenz unterschieden. Erstere wird für spezifische Anwendungen eingesetzt, wie beispielsweise Experten- oder Navigationssysteme (Etscheid et al. 2020, S. 8). Als solche sind schwache KIs bereits heute vielfach im Einsatz. Starke KIs hingegen sind in der Lage, selbstständig logisch denken, planen, lernen und Entscheidungen unter Unsicherheit zu treffen (ebd., S. 8). Eine weitere Steigerung der starken KI wäre die Superintelligenz, welche dem Menschen in Intelligenz überlegen ist und aktuell sowie auf absehbare Zukunft ein theoretisches Konzept bleibt (ebd., S. 8). Für die öffentliche Wahrnehmung von KI und (häufig dystopische) Science-Fiction ist dieses Konzept jedoch sehr prägend.

Aufgrund der Vielfalt an möglichen Ansätzen für die technische Abgrenzung von KI (beispielsweise anhand der verwendeten Lernmethoden) soll an dieser Stelle auf die Differenzierung von KI-Systemen anhand ihrer Grundfähigkeiten (Basistechnologien) eingegangen werden. Zu Beginn ist die KI-basierte Musterkennung zu nennen, wobei Daten auf Regelmäßigkeiten, Wiederholungen, Ähnlichkeiten oder Gesetzmäßigkeiten untersucht werden, um so relevante Zusammenhänge aufzuzeigen (Etscheid et al. 2020, S. 9). Insbesondere für die Analyse von Big Data ist diese Basistechnologie essenziell. Weiterhin sind die KI-basierte Text- und Tonerkennung zu nennen, mithilfe derer unstrukturierte Daten aus Texten für technische Systeme verarbeitbar gemacht sowie akustische Signale und Tonfolgen erkannt und bestimmten Ereignissen oder Verursachern zugeordnet werden können (ebd., S. 10). Auf Basis von Text- und Tonerkennung kann KI auch dazu eingesetzt werden, menschliche Sprache und Texte in maschinenlesbaren Text und in Fremd-, leichte, Zeichen- oder Amtssprache zu übersetzten (ebd., S. 10). Zudem kann KI dazu eingesetzt werden, sowohl zwei- als auch dreidimensionale Objekte in Bildern und Räumen zu identifi-

zieren und zu analysieren (ebd., S. 10). Ein Sonderfall hiervon ist die KI-basierte Erkennung von Gesichtern, Gesten und Bewegungsmustern (ebd., S. 10f). Im Verlauf dieser Arbeit wird sich mit dieser KI-Basistechnologie als Anwendung für die Polizei noch näher und kritisch auseinandergesetzt.

Die KI-Basistechnologien lassen sich wiederum für verschiedenste KI-Basisanwendungen nutzen. Diese reichen von der KI-basierten Wahrnehmung und Benachrichtigung, über Empfehlungen, Vorhersagen und Prognosen, Vorsorge, bis zu selbstständigen Entscheidungen der KI und Echtzeit-Situationswahrnehmung (ebd., S. 11f). Speziell für die öffentliche Verwaltung gibt es sowohl für das Front- (beispielsweise Chatbots für Bürgerkontakte), als auch das Backoffice (beispielsweise beim Workflow- und Personalmanagement) verschiedene Ansätze für den KI-Einsatz (ebd., S. 22-32). Des Weiteren kann KI im öffentlichen Dienst zur Entscheidungsunterstützung und Beratung sowie zur Automatisierung einfacher Verwaltungsverfahren genutzt werden (ebd., S. 33-41). Im Bereich des Real-Time-Governments sorgen fortschrittliche KI-Systeme für eine beschleunigte Datenverarbeitung und -auswertung, wodurch diese in bestimmten Situationen für automatisierte Entscheidungen nahezu in Echtzeit eingesetzt werden können (ebd., S. 42-45). Dabei gilt es jedoch darauf zu achten, dass der jeweilige KI-Einsatz immer mit den rechtlichen und ethischen Vorgaben in Einklang steht (von Lucke 2024, S. 10).

In den letzten Jahren gab es mit der generativen KI (GKI) eine weitere bedeutende Entwicklung. Im Gegensatz zu den zuvor vorgestellten KI-Basistechnologien analysieren GKIs nicht nur große Datenmengen mittels maschinellem Lernen, sondern sind darüber hinaus auch in der Lage, auf Grundlage des Erlernten neue Artefakte zu generieren (Büchel & Engler 2024, S. 5; von Lucke 2024, S. 10). Am bekanntesten dürften hierbei sogenannte Large Language Models (LLM) wie ChatGPT und Co-Pilot sein, welche menschenähnlich Texte generieren können. GKIs sind außerdem dazu in der Lage, Bilder, Videos, Ton- und Sprachsequenzen und Programmcodes in Teils sehr hoher Qualität zu generieren. Hierdurch ergeben sich zahlreiche Anwendungsmöglichkeiten für Wissenschaft, Forschung, Wirtschaft und den öffentlichen Sektor. Trotz dieser Potenziale verfügen generative KIs immer noch über eine Reihe von Schwächen, da sie wie alle KI-Systeme von ihren Trainingsdaten abhängig und nur in begrenztem Maße zu kritischem Denken fähig sind. Ein bekanntes Beispiel aus LLMs ist hier das Phänomen, dass die GKI Fakten erfindet („Halluzinieren"), was mit der technischen Funktionsweise von LLMs zusammenhängt (ebd., S. 6; ebd., S. 10). Aus diesem Grund ist es erforderlich, die Ergebnisse von LLMs immer kritisch zu hinterfragen, insbesondere wenn man diese in der öffentlichen Verwaltung einsetzt.

Ähnlich wie die in den vorherigen Abschnitten erläuterten Technologien und Konzepte beinhaltet auch KI Potenziale für eine datenbasierte, effizientere, und leistungsfähigere Verwaltung. Bereits heute spielt KI in vielen Bereichen eine zentrale Rolle und mit Blick auf das disruptive Potenzial dieser Technologie wird KI in Zukunft für große Veränderungen in Wirtschaft, Gesellschaft und Verwaltung sorgen. Obwohl die häufig geäußerte Befürchtung, dass der Mensch irgendwann von einer KI-Superintelligenz ersetzt wird, angesichts des aktuellen Entwicklungsstands der KI unrealistisch erscheint, hat KI dennoch bereits heute Einfluss auf den Menschen und sein Verhalten. Aus diesem Grund gilt es Risiken, welche mit den Einsatz bestimmter KI-Anwendungen einhergehen, zu regulieren und wenn nötig, bestimmte KI-Anwendungen auch zu verbieten. Einen Orientierungsansatz hierzu bietet die Kritikalitätspyramide der Datenethikkommission der Bundesregierung, welche algorithmische Systeme nach ihrem Schädigungspotenzial einteilt (siehe Abbildung 2).

Im Falle eines eheblichen Schädigungspotenzials verbindet dies den Einsatz einer Anwendung mit umfangreichen Kontroll- und Transparenzpflichten, während ein unvertretbares Schädigungspotenzial ein vollständiges oder teilweises Verbot zur Folge hat (beispielsweise bei autonomen Waffensystemen) (Datenethikkommission 2019, S. 179f). Einen vergleichbaren Ansatz folgt die EU mit der KI-Verordnung, welche die Anwendbarkeit bestimmter KI-Systeme vom potenziellen Risiko eines Schadens für die Gesellschaft abhängig macht (Rat der Europäischen Union 2024).

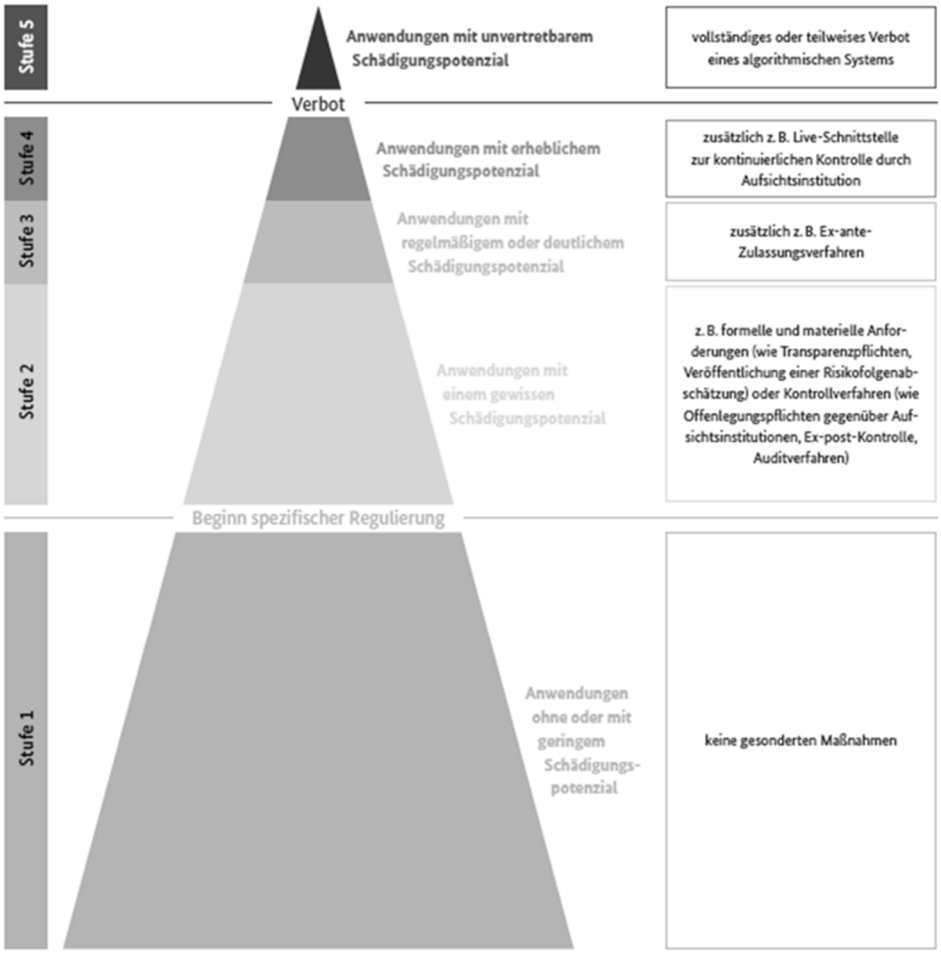

Abbildung 2: Kritikalitätspyramide und risikoadaptiertes Regulierungssystem für den Einsatz algorithmischer Systeme (Datenethikkommission 2019, S. 177)

4. Thematischer Hintergrund

Nachdem Kapitel drei bereits der theoretische und konzeptionelle Hintergrund dieser Arbeit erläutert wurde, widmet sich Kapitel vier im Folgenden dem thematischen Hintergrund dieser Arbeit. Hierzu wird einleitend auf die zentralen Begriffe der Inneren und öffentlichen Sicherheit eingegangen und diese von anderen Arten der Sicherheit abgegrenzt. Daran anschließend widmet sich Abschnitt 4.2. die der Polizei in Deutschland als eine der Behörden, welche maßgeblich für die Innere und öffentliche Sicherheit verantwortlich ist. Abschnitt 4.3. wiederum beschreibt verschiedene Maßnahmen, welche die Polizei zur Gewährleistung der Inneren und öffentlichen Sicherheit ergreift und so Grundlage für mögliche Anwendungsfälle smarter Technologie und künstlicher Intelligenz bilden.

4.1. Sicherheit

„Sicherheit" ist ein sehr breiter Begriff, welcher jedoch im Kern immer die Abwesenheit von Gefahr und Sorge beschreibt (Frevel 2018, S. 2). Hierbei kann wiederum zwischen der „subjektiven", also der gefühlten Abwesenheit einer Gefahr und damit verbundener Sorglosigkeit und der „objektiven" Sicherheit unterschieden werden, der tatsächlichen Abwesenheit von Gefahr und Bedrohung (Hummelsheim-Doss 2017). Eine eingehende Betrachtung der unterschiedlichen Facetten von Sicherheit würde über den vorgesehenen Rahmen für diese Arbeit hinausgehen, weshalb an dieser Stelle der Fokus auf die in Deutschland übliche Einteilung von innerer, äußerer und öffentlicher Sicherheit gelegt wird. Daneben umfasst Sicherheit unter anderem auch die Bereiche Betriebssicherheit und soziale und wirtschaftliche Sicherheit, auf welche mit Blick auf das Thema dieser Arbeit jedoch nicht weiter eingegangen wird.

Der politische Begriff der Inneren Sicherheit kam im Laufe der 1960er und 1970er Jahre auf und wird in Debatten unterschiedlich breit und teils kritisch aufgefasst (Frevel 2018, S. 4-7). Eine mit Blick auf das Thema dieser Arbeit hilfreiche Definition liefert Frevel (2018, S. 11), welcher die Innere Sicherheit wie folgt beschreibt:

> *„... Als (angestrebter) Zustand der Angriffssicherheit (security) von Individuen, Staat und Gesellschaft (Referenz) auf der lokalen bis nationalen Ebene (Raum) vor Bedrohungen (Gefahrendimension) mit kriminellem, extremistischen oder terroristischen Hintergrund (Sachdimension).*"

Im Gegenzug richtet sich die Äußere Sicherheit gegen externe Bedrohungen durch andere Staaten oder staatsähnliche Gebilde, welche durch militärische Maßnahmen, Bündnisse und Diplomatie adressiert werden

(ebd., S. 5f). Jedoch können Bedrohungen für die Innere Sicherheit auch einen externen Ursprung haben, wie beispielsweise internationaler Terrorismus und grenzüberschreitende organisierte Kriminalität, wodurch die Linie zwischen Innerer und Äußerer Sicherheit nicht immer trennscharf gezogen werden kann (ebd., S. 11f).

Im Gegensatz zum politischen Begriff der Inneren Sicherheit ist die öffentliche Sicherheit ein Rechtsbegriff, welcher regelmäßig in den deutschen Polizeigesetzten verwendet wird. Allgemein wird unter der öffentlichen Sicherheit der Schutz der geschriebenen Rechtsordnung (Gesetze und sonstigen Rechtsvorschriften) und seiner Institutionen und der individuellen Rechtsgüter der Bürger (beispielsweise Leben, Eigentum, Gesundheit, Freiheit) verstanden (Alexy et al. 2023). Meist wird die öffentlichen Sicherheit zusammen mit der öffentlichen Ordnung erwähnt, welche die Gesamtheit der ungeschriebenen Regeln umfasst, die nach allgemeinem Verständnis für ein geordnetes gesellschaftliches Zusammenleben relevant sind (ebd.).

Die Gewährleistung von Sicherheit ist eine der Kernaufgaben eines modernen Rechts- und Verfassungsstaates, genauso wie die Gewährleistung der Freiheit seiner Bürger, jedoch besteht zwischen Sicherheit und Freiheit ein Spannungsverhältnis (Papier 2011, S. 2). Während Sicherheit einerseits eine Grundvoraussetzung dafür ist, dass Bürger frei leben können, können übermäßige staatliche Sicherheitsmaßnehmen gleichzeitig auch die Freiheit der Bürger einschränken. Wie genau das Spannungsverhältnis zwischen Freiheit und Sicherheit in einer Gesellschaft genau ausgestaltet sein soll, ist eine politische Frage und sollte idealerweise im Rahmen der demokratischen Entscheidungsfindung festgelegt werden (Volkmann 2022).

Für die Gewährleistung der Inneren Sicherheit im Sinne der oben genannten Definition sind in Deutschland neben den Verfassungsschutzämtern in erster Linie die Polizeibehörden von Bund und Ländern verantwortlich. Im folgenden Abschnitt wird deshalb die Organisation der Polizei in Deutschland näher beleuchtet, bevor im Anschluss auf die unterschiedlichen Maßnahmen der Polizeiarbeit eingegangen wird.

4.2. Die Polizei in Deutschland

4.2.1. Länder

Die grundsätzliche Zuständigkeit der Bundesländer für die Polizei ergibt sich aus Art. 30 des Grundgesetztes (GG), welcher die Ausübung staatlicher Befugnisse und Erfüllung staatlicher Aufgaben in erster Linie den Bundesländern zuweist. Die 16 Landespolizeibehörden unterstehen dabei der Aufsicht des jeweiligen Landesinnenministeriums. Ihre Organisation, Aufgaben und Befugnisse sind in den jeweiligen Landespolizeigesetzen (PolG) und zum Teil in einem separaten Polizeiorganisationsgesetz (beispielsweise in Bayern) geregelt. Hierbei unterscheiden sich die Aufgaben und Befugnisse zwischen den einzelnen Bundesländern teils erheblich. Die als zentrales Koordinationsorgan zuständige Innenministerkonferenz hat zwar in der Vergangenheit versucht, einen einheitlichen Rechtsrahmen für die Polizeibehörden der Länder zu schaffen (Groß 2012). Jedoch gibt es bis heute weiterhin Unterschiede bei der Regelung (oder Nicht-Regelung) polizeilicher Maßnahmen zwischen den einzelnen Bundesländern (Wissenschaftliche Dienste des Deutschen Bundestages (WD) 2017). Bundeseinheitliche Rechtsgrundlagen für die polizeiliche Arbeit sind indessen die Strafprozessordnung (StPO), die Straßenverkehrsordnung (StVO) und das Gesetz über Ordnungswidrigkeiten (OWiG). Weiterhin unterscheiden sich die Landespolizeien auch hinsichtlich ihrer Organisation und der Ausbildung und Laufbahn ihrer Beamten.

Wesentliche Gemeinsamkeit aller Landespolizeien ist der Polizeivollzugsdienst, welcher in jedem Bundesland eine uniformierte und für die Gefahrenabwehr zuständige Schutzpolizei sowie eine für Strafverfolgung zuständige Kriminalpolizei beinhaltet. Die genauen Aufgaben und die weitere Unterteilung der Schutzpolizei unterscheiden sich jedoch erneut von Bundesland zu Bundesland (beispielsweise in der Zugehörigkeit der Verkehrspolizei zur Schutzpolizei). Weiterhin verfügt jede Landespolizei über eine kasernierte Bereitschaftspolizei, welche vor allem zur Bewältigung polizeilicher Großlagen wie Demonstrationen eingesetzt wird, häufig auch länderübergreifend. Aufgrund der bereits erwähnten Unterschiede in den Landespolizeigesetzen führt dies oftmals zu Problemen, wobei in der Praxis das Landespolizeirecht des jeweiligen Einsatzortes gilt (Groß 2012). Zudem verfügt jedes Bundesland über ein eigenes Landeskriminalamt (LKA), welches in zentraler Funktion für die Bekämpfung schwerer Kriminalität auf Landesebene zuständig ist, örtliche Polizeidienststellen bei Ermittlungen unterstützt und die polizeiliche Zusammenarbeit zwischen einzelnen Bundesländern koordiniert.

4.2.2. Bund

Auf Bundesebene gibt es mit der Bundespolizei und dem Bundeskriminalamt (BKA) zwei Polizeibehörden in der Zuständigkeit des Bundesministeriums des Innern und für Heimat (BMI).

Die Bundespolizei (bis 2005 Bundesgrenzschutz) ist hauptsächlich zuständig für den polizeilichen Grenzschutz, die Sicherheit an Bahnhöfen und in Zügen (Bahnpolizei), an Flughäfen und im Luftverkehr sowie den Schutz von Bundesorganen (BMI o.D.). Des Weiteren unterstützt die Bundespolizei auf Anforderung die Landespolizeien (meist bei Großeinsätzen), weshalb sie auch über eigene Bereitschaftspolizeieinheiten verfügt (ebd.). Zahlenmäßig ist die Bundespolizei mit rund 45.000 Polizeivollzugsbeamtinnen und -beamten die größte Polizeibehörde in Deutschland (ebd.). Primäre Rechtsgrundlage für die Arbeit der Bundespolizei ist das Bundespolizeigesetz.

Das BKA ist die Zentralstelle der deutschen Kriminalpolizei. Als solches koordiniert es zusammen mit den LKAs die Kriminalitätsbekämpfung in Deutschland und unterstützt die Kriminalpolizei der Länder mit zentralen kriminalistischen Informationssammlungen und Know-How (Frevel 2018, S. 84; Groß 2012). Im Bereich schwerer und internationaler Straftaten wie Terrorismus, illegalem Waffen- und Drogenhandel und der organisierten Kriminalität führt das BKA selbständig Ermittlungen durch. Weiterhin fungiert das BKA auf internationaler Ebene als Verbindungsstelle für ausländische Polizeien, Europol und Interpol. Außerdem ist das BKA zuständig für den Schutz von Mitgliedern der Verfassungsorgane (Bundespräsident, Bundeskanzler und Bundesminister) (Groß 2012). Rechtsgrundlage für die Arbeit des BKA ist das BKA-Gesetz.

4.3. Polizeiliche Maßnahmen

Polizeiliche Maßnahmen in Deutschland sind in erster Linie präventiv und repressiv. Daneben gibt es im Polizeialltag aber auch Situationen, in welchen sich diese Maßnahmen nicht trennscharf voneinander abgrenzen lassen, weshalb man hier von doppelfunktionalen Maßnahmen spricht. Alle drei Arten von polizeilichen Maßnahmen bieten wiederum Ansätze für Anwendungen von smarter Technologie und KI, welche später im sechsten Kapitel vorgestellt werden.

4.3.1. Präventive Maßnahmen

Präventive polizeiliche Maßnahmen zielen auf die Abwehr von Gefahren für die öffentliche Sicherheit und Ordnung ab und sind als solche in den jeweiligen Polizeigesetzen von Bund und Ländern geregelt. Eine besondere Rolle spielen hierbei die sogenannten polizeilichen Generalklauseln, welche der Polizei auch ohne eine ausdrückliche rechtliche Ermächtigungsgrundlage ermöglichen, Maßnahmen zur Gefahrenabwehr vorzunehmen (im Falle Baden-Württembergs exemplarisch §§ 1, 3 PolG). Innerhalb der gesetzlichen Schranken wird Polizeibeamten so ein pflichtgemäßer Ermessensspielraum eingeräumt, um notwendige Maßnahmen zur Gefahrenabwehr vorzunehmen (das sogenannte „Opportunitätsprinzip") (Kugelmann 2012, S. 10). Polizeiliche Maßnahmen, welche sich aus den Generalklauseln ergeben, müssen darüber hinaus verhältnismäßig sein und können im Zweifel gerichtlich nachgeprüft werden. In der Praxis werden präventive polizeiliche Maßnahmen in erster Linie von der uniformierten Schutzpolizei wahrgenommen. Ein klassisches Beispiel hierfür ist der tägliche Streifendienst, um durch eine polizeiliche Präsenz im öffentlichen Raum und bei Großveranstaltungen das subjektive Sicherheitsgefühl der Bürger zu stärken und potenzielle Straftäter abzuschrecken. Des Weiteren gehören Personenkontrollen, Gefährderansprachen und kriminalpräventive Beratungen für Bürger zu präventiven Maßnahmen der Polizei. Sensordaten und Big Data Analysen können der Polizei beispielsweise dabei helfen, frühzeitig Gefahren an Kriminalitätsschwerpunkte zu erkennen und einschreiten zu können.

Prävention beziehungsweise Kriminalprävention haben seit den 1990er Jahren zunehmend an Bedeutung gewonnen, wobei sich neben der Polizei auch zahlreiche weitere Akteure aus Justiz und Gesellschaft einbringen (Kerner 2018; Steffen 2015, S. 72ff). Auch Fritz und Huber weisen auf die wachsende Bedeutung präventiver Maßnahmen hin (Fritz 2020, S. 29; Huber 2022, S. 93f). Gleichzeitig verweisen beide Autoren auf das Risiko von Freiheitseinschränkungen, welche sich aus dem Einsatz smarter Technologien zu Präventionszwecken ergeben können (ebd., S. 81ff; ebd., S. 95ff).

4.3.2. Repressive Maßnahmen

Repressive Maßnahmen der Polizei zielen auf die Strafverfolgung und Ermittlung der verantwortlichen Täter ab. Rechtsgrundlage hierfür bildet die StPO. Vor allem Big Data Analysen spielen bereits heutzutage bei polizeilichen Ermittlungen eine zentrale Rolle, worauf auch in den Experteninterviews von Fritz hingewiesen wird (Fritz 2020, S. 69). Weiterhin können smarte und digitale Anwendungen zur Sammlung und Aufnahme von Zeugenaussagen und Beweisen genutzt werden (ebd., S. 69).

In der Praxis übernimmt vor allem die Kriminalpolizei repressive Maßnahmen. Dies beinhaltet die Suche und Sicherung von Spuren am Tatort, Vernehmungen, operative Maßnahmen wie Durchsuchungen und Überwachungen und schließlich die Festnahme von Verdächtigen. Im Gegensatz zum Opportunitätsprinzip gilt bei repressiven Maßnahmen das sogenannte „Legalitätsprinzip". So sind die Polizei und die laut Gesetz für Ermittlungen zuständige Staatsanwaltschaft nach § 152 StPO dazu verpflichtet, Ermittlungen aufzunehmen, sobald sie Kenntnis von einer begangenen Straftat erhalten (beispielsweise mittels Strafanzeige). Angehörige der Kriminalpolizei agieren hierbei im Sinne des § 163 StPO als Ermittlungspersonen der Staatsanwaltschaft, wobei die Kriminalpolizei über eigene und weitreichende Ermittlungsbefugnisse verfügt (Koppers & Weidling 2021, S. 77). Die Unterrichtung der Staatsanwaltschaft seitens der Kriminalpolizei über ihre Ermittlungsarbeit ist somit ebenfalls eine repressive Maßnahme (Pansa 2023).

4.3.3. Doppelfunktionale Maßnahmen

In der Praxis ist eine klare Trennung zwischen präventiven und repressiven Maßnahmen der Polizei nicht immer möglich, da sich oft Situationen ergeben, in welchen polizeiliche Maßnahmen sowohl der Gefahrenabwehr als auch der Strafverfolgung dienen. In diesen Fällen spricht man von doppelfunktionalen Maßnahmen (Schoch 2013, S. 1116).

Häufig finden doppelfunktionale Maßnahmen im Rahmen von Gemengelagen wie Großdemonstrationen statt (ebd., S. 117). Ein weiteres Beispiel, welches im Verlauf dieser Arbeit noch genauer betrachtet wird, sind Videoüberwachungsmaßnahmen. Einerseits können die so gewonnen Videoaufzeichnungen als Beweismittel zur Aufklärung von Straftraten dienen, andererseits sollen weitere Straftaten verhindert werden, indem die Videoüberwachung als Abschreckung dienen soll (ebd., S. 1115f). Die Frage, ob es sich bei einer polizeilichen Maßnahme um eine doppelfunktionale Maßnahme handelt, ist insbesondere aus zwei Gründen relevant: Einerseits, für die ausführenden Polizeibeamten, um Klarheit über die Rechtsgrundlage ihres Handelns zu haben, andererseits für die Betroffenen der polizeilichen Maßnahme, da sich je nach Maßnahme unterschiedliche Rechtswege gegen das polizeiliche Handeln eröffnen (ebd., S. 115f, S. 1121ff).

5. Bestehende Ansätze smarter Polizeiarbeit

Smarte Polizeiarbeit wird von Fritz (2020, S. 35) in Anlehnung an die bereits in Abschnitt 3.2. genannte Häfler Definition von Smart Government wie folgt definiert:

> *„Unter Smarter Polizeiarbeit sollen Prozesse im Zusammenhang mit dem polizeilichen Handeln und der Aufgabenbewältigung mit Hilfe von intelligent vernetzten Informations- und Kommunikationstechnologien sowie der Analyse großer (hieraus entstehender) Datenmengen verstanden werden. Eine intelligent vernetzte Polizeiarbeit nutzt die Möglichkeiten smarter Objekte sowie cyber-physischer Systeme zur effizienten wie effektiven Erfüllung ihrer Aufgaben und der Gewährleistung der Öffentlichen Sicherheit und Ordnung. Im Kern geht es um das polizeiliche Handeln im Internet der Dinge und der Dienste. Gleichzeitig schließt die Smarte Polizeiarbeit auch das polizeiliche Leistungsportfolio im Internet der Systeme (E-Government), Internet der Menschen (Open Government und Social Media) sowie insbesondere im Internet der Daten (Big und Open Data) mit ein. Im Vordergrund der Smarten Polizeiarbeit steht neben der Repression und Prävention von Straftaten die Dienstleistungsfunktion gegenüber der Bevölkerung sowie der Schutz der Freiheits- und Grundrechte. Eine Smarte Polizeiarbeit soll zu einer Effizienzsteigerung des polizeilichen Handelns, einer Erhöhung der Transparenz sowie zu verbesserten Serviceleistungen für den Bürger führen.“*

Mit Blick auf die in dieser Arbeit untersuchten neuen Einsatzmöglichkeiten smarter Technik, Big Data und fortgeschrittener KI kann diese Definition um das *„Taktile Internet“* ergänzt werden, um in Zukunft eine Aufgabenerfüllung (nahezu) in Echtzeit zu ermöglichen.

Bevor im Folgenden Teil auf neue Einsatzmöglichkeiten eingegangen wird, soll einleitend ein kurzer Überblick über ausgewählte Ansätze smarter Polizeiarbeit gegeben werden, die sich bereits in Deutschland im Einsatz befinden und die Grundlage für neue Anwendungsfälle bilden. Entsprechend finden sie sich auch in den Anwendungsfällen aus Kapitel wieder, wobei KI hier Ansätze zur Ergänzung und Optimierung bietet. Eine zentrale Funktion bei der Digitalisierung der Polizei in Deutschland nimmt das Programm „Polizei 2020“ (P20)[6] ein, mit welchem eine Modernisierung und Standardisierung der polizeilichen IT-Verfahren und -Systeme angestrebt wird (BMI 2018, S. 8).

[6] Für einen ausführlichen Überblick über die Ziele und Inhalte von P20: Holger Gadorosi und Susanne Matthey (2023): „Auf dem Weg zu einer digitalen und vernetzten Polizei – P20“.

5.1. Information und Analyse

Smarte Technologien im Sinne eines Smart Governments lassen sich zur Information und Analyse mithilfe smarter Objekte und CPS nutzen. In diesem Zusammenhang bereits bestehende Ansätze smarter Polizeiarbeit in Deutschland sind Bodycams, die algorithmenbasierte Videoüberwachung, mobile Polizeiarbeit mittels Apps und das Predictive Policing, welche im Folgenden jeweils näher beleuchtet werden.

5.1.1. Bodycams

Bodycams (Englisch für „Körperkameras", wobei im Deutschen allgemein der englische Begriff verwendet wird), sind kleine Kameras, welche von Einsatzkräften der Polizei auf der Schulter oder an der Brust (meist der Einsatzweste) getragen werden (Seckelmann 2017, S. 292). Abhängig von den jeweiligen Polizeigesetze können Bodycams nur für Bildaufnahmen, für Bild- und Ton-Aufnahmen und zum Pre-Recording eingesetzt werden. Dies ermöglicht es, kurze Zeiträume vor Aktivierung der Aufnahme vorübergehend und bei Bedarf dauerhaft zu speichern, sobald die Funktion (beispielsweise per Knopfdruck) aktiviert wird (ebd., S. 292). Als polizeiliche Maßnahme wird Bodycams sowohl eine präventive als auch repressive Funktion zugeschrieben: Präventiv, da die Videoaufzeichnung vor möglichen Übergriffen auf Polizeikräfte abschrecken soll und repressiv, da im Falle eines Übergriffs Videoaufnahmen zur Aufklärung der Tat gewonnen werden können (ebd., S. 291f). Gleichzeitig wird auch argumentiert, dass der Einsatz von Bodycams Bürger schützen soll, da ungerechtfertigte Übergriffe durch die Polizei ebenfalls dokumentiert werden, was die Transparenz des polizeilichen Handelns fördert (Fritz 2020, S. 37; Seckelmann 2017, S. 293). Deutschlandweit finden Bodycams inzwischen weite Verbreitung bei der Polizei von Bund und Ländern (Adams, van den Heuvel, Yan & Korz 2019). Auf die Frage, welche Beispiele für smarte Technologien bereits heute bei der Polizei in Deutschland im Einsatz sei, wurde auch die Bodycam von vier Experten als Beispiel genannt[7] (E5 2024, 04:28; E6 2024, 04:40; E7 2024, 06:29; E10 2024, 6:37).

Ein Hauptkritikpunkt beim Einsatz von Bodycams ist, dass diese einen Eingriff in die Grundrechte der informationellen Selbstbestimmung und Handlungsfreiheit als allgemeine Persönlichkeitsrechte nach Art. 2 Abs. 1 GG darstellen (Kipker 2017, S. 166). Auch der Jurist der NGO für Menschen und Grundrechte äußert sich diesbezüglich kritisch zum Einsatz (E7 2024, 08:03). Demensprechend muss der Gebrauch von Bodycams mit klaren Rechtsgrundlagen zum Einsatzzweck und -umfang sowie Transparenzanforde-

[7] Der Wissenschaftliche Leiter des Cybersicherheitsunternehmens äußert hier jedoch Skepsis hinsichtlich der Smartness von Bodycams, da der „Feedback-Loop" fehle (E6, 2024, 06:18).

rungen an die Aufzeichnung, Speicherung und Auswertung der Videoaufnahmen verbunden sein (Kipker 2017, S. 167ff).

5.1.2. Algorithmenbasierte Videoüberwachung

Die herkömmliche stationäre Kameraüberwachung in Teilen des öffentlichen Raumes ist inzwischen weit verbreitet, vor allem an sogenannten „Kriminalitätsschwerpunkten" (Fritz 2020, S. 38). Jedoch besteht hier die Herausforderung, aus den großen Mengen an Videomaterial verdächtiges und für polizeiliche Ermittlungen relevantes Material zu identifizieren. KI-Systeme im Sinne einer algorithmenbasierten Datenauswertung können dabei helfen, die Auswertung der Videoüberwachungsdaten effizienter zu gestalten.

Ein diesbezüglicher Ansatz stammt von Fraunhofer IOSB, welches hierzu gemeinsam mit dem Polizeipräsidium Mannheim 2018 ein Pilotprojekt[8] gestartet hat, das kürzlich bis 2026 verlängert wurde (Kessel 2023). Die Führungskraft im Polizeipräsidium erwähnt ebenfalls das Projekt aus Mannheim (E10 2024, 7:00). Im Rahmen dieses Projekts werden Kameras mit KI-basierter Software von Fraunhofer IOSB an fünf Kriminalitätsschwerpunkten in Mannheim eingesetzt, wobei Verhaltensmuster automatisch auf sicherheitskritische Bewegungen hin untersucht werden (Ministerium des Inneren, für Digitalisierung und Kommunen Baden-Württemberg (IM BW) 2023). Hierzu werden Personen im Erfassungsbereich der Kameras „digital zu skelettiert" und ihre Verhaltensmuster auf Basis der digitalen Stichfiguren analysiert (Golda et al. 2023, S. 1488). Ein wesentlicher Vorteil, auch gegenüber der herkömmlichen Videoüberwachung, ist, dass die anonymisierten Strichfiguren ein hohes Maß an Datenschutz bieten (ebd., S. 1488). Das System aus Mannheim dient als Assistenzsystem: Wird ein auffälliges Verhalten erkannt, wird automatisch ein menschlicher Entscheidungsträger im Polizeipräsidium Mannheim informiert, welcher nach Begutachtung der Bilder und bei Feststellung eines Notfalls weitere Maßnahmen einleitet. Hierdurch bietet der Ansatz aus Mannheim ein größeres präventives Potenzial, verglichen mit der eher repressiv ausgerichteten herkömmlichen Videoüberwachung (ebd., S. 1488f). Technische Probleme in der Anfangsphase waren vor allem häufige Fehlalarme, da das System harmlose Verhaltensweisen wie Umarmungen als bedrohlich einstufte (Susanka 2023). Nach Mannheim hat auch Hamburg im vergangenen Jahr ein eigenes Pilotprojekt in Zusammenarbeit mit Fraunhofer IOSB gestartet (Fengler 2023).

[8] Einen Überblick über das Pilotprojekt in Mannheim bieten Thomas Golda, Mickael Cormier und Jürgen Beyerer (2023): „Intelligente Bild- und Videoauswertung für die Sicherheit".

5.1.3. Polizei-Apps

Ein in den Interviews häufig genanntes Beispiel für bestehende Ansätze smarter Polizeiarbeit sind speziell für die Arbeit der Polizei entwickelte Apps. Hintergrund ist eine zunehmende Ausstattung der Polizei mit Tablets und Smartphones zur mobilen Polizeiarbeit. Beispielhaft sei hier auf die Polizei in Nordrhein-Westfalen (NRW) verwiesen, welche im Jahr 2019 seine operativ arbeitenden Einsatzkräfte flächendeckend mit 20.000 Smartphones ausstattete (Tack 2019). Die möglichen Einsatzbereiche sind vielfältig. In den Interviews werden Apps für Datenauskünfte genannt, verbunden mit der Möglichkeit zum Scan von Ausweisdokumenten und Führerscheinen sowie Apps, mit welchen Polizeibeamte mobil Strafanzeigen aufnehmen können (E2 2024, 04:40; E3 2024, 07:52). Weiterhin wird auf die App „iVe" des Herstellers Berla verwiesen, mit welcher man Daten aus Infotainmentsystemen zur Aufklärung von Straftaten oder Unfällen auslesen kann (E6 2024, 07:42, Polster & Labudde 2022, S. 276, 284). In präventiver Hinsicht kann diese App außerdem Informationen zur Verhinderung von Fahrzeugdiebstählen liefern (E6 2024, 08:00). Als weitere Anwendungsmöglichkeit werden Apps zum Ausrüstungsmanagement und zur Navigation im Einsatz genannt (E8 2024, 08:20).

Vorteile, welche sich aus der mobilen Polizeiarbeit mit Smartphone, Tablet und Apps ergeben, sind eine schnellere und einmalige Datenerfassung sowie eine verbesserte Kommunikation und Informationsvermittlung (Fritz 2020, S. 41). Zudem stehen nicht nur Apps für die Polizei zur Verfügung, sondern umgekehrt werden auch Bürgern Apps zur Verfügung gestellt, welche beispielsweise beim Finden von Polizeidienststellen helfen, bei der Kriminalprävention beraten und vor Gefahren warnen (ebd., S. 41f). Hinsichtlich der Anforderungen an die Apps gilt es vor allem auf Cybersicherheit und Datenschutz zu achten, wenn mit sensiblen und personenbezogenen Daten gearbeitet wird (Polizei Hessen 2022).

5.1.4. Predictive Policing

Als sehr bekanntes Beispiel präventivpolizeilicher Big Data Analyse wird Predictive Policing in mehreren der Interviews erwähnt (E1 2024, 2:40; E5 2024, 5:20; E6 2024; 21:09; E7 2024, 21:13; E9 2024, 4:37). Auch Fritz (2020) geht in seiner Arbeit auf das Predictive Policing ein (S. 43f).

In der Praxis wird hierbei zwischen einem orts- und einem personenbezogenen Predictive Policing unterschieden. Letzteres findet beispielsweise in den USA und in der Schweiz Anwendung, wobei versucht wird, auf Basis vorhandener Daten vermeintliche Gefährder zu identifizieren und diese anschließend einem Bedrohungsmanagement zu unterziehen, um mögliche Straftaten zu verhindern (Fichter & Wüstholz 2020; Perry et al. 2013, S. 81).

Weiterhin werden personenbezogene Ansätze in den USA auch dazu verwendet, das Risiko einer zukünftigen Straffälligkeit zu bewerten, um mögliche Straftaten vorzubeugen und Rückfallquoten zu senken (Perry et al. 2013, S. 81). Da in den USA übermäßig viele Afro- und Lateinamerikaner in der Datenbasis vertreten waren, kam es in der Vergangenheit vermehrt zu Diskriminierungen dieser Bevölkerungsgruppen (Knobloch 2018, S. 12). Neben dem erheblichen Diskriminierungsrisiko ist ein weiteres Problem, das personenbezogenes Predictive Policing verglichen mit anderen Ansätzen technisch deutlich weniger ausgereift ist (Perry et al. 2013, S. 93f).

In Deutschland findet bislang nur das ortsbezogene Predictive Policing Anwendung. Hierbei wird mittels eines Algorithmus die Wahrscheinlichkeit für das Auftreten von Straftaten (meist Einbrüche) an bestimmten Orten und zu bestimmten Zeiten berechnet, um im Anschluss die Polizeipräsenz vor Ort zu erhöhen und die Effizienz bei der Kriminalprävention zu steigern (Knobloch 2018, S. 8ff). In Deutschland wurde bislang eine Reihe an Systemen getestet oder befindet sich bereits im Einsatz. Hierzu gehören Eigenentwicklungen (NRW und Berlin), kommerzielle Systeme (Bayern und Baden-Württemberg) oder auf kommerzieller Software basierende Systeme, die für den Eigenbedarf weiterentwickelt wurden (Hessen und Niedersachsen) (ebd., S. 13). Grundlage hierfür ist meist die Near-Repeat-Theorie. Diese geht davon aus, dass nach einem Einbruch in einem bestimmten Gebiet die Wahrscheinlichkeit für weitere Einbrüche in unmittelbarer Nähe und innerhalb eines kurzen Zeitraums erhöht ist, da die Täter Einbrüche gezielt in räumlicher und zeitlicher Nähe begehen (ebd., S. 16).

Obwohl ortsbezogenes Predictive Policing hinsichtlich Datenschutz und dem Schutz der bürgerlichen Freiheitsrechte deutlich weniger invasiv ist als personenbezogenes, verweist der Jurist der NGO für Grund- und Menschenrechte darauf, dass der ortsbezogene Ansatz immer auch an soziale Faktoren in verschiedenen Stadtgebieten anknüpfe und so ebenfalls eine diskriminierende Komponente habe (E7 2024, 21:18). Ein weiteres, vielfach geäußertes Problem ist eine mangelnde Messbarkeit der Wirkung von ortsbezogenem Predictive Policing. Hierauf wird auch in zwei Interviews hingewiesen, wobei das Messbarkeitsproblem eines Rückgangs von Einbrüchen durch verstärkte Polizeipräsenz kritisch als „Self-Fulfilling Prophecy“ bezeichnet wird (E1 2024, 3:13; E6 2024, 21:47). Weiterhin benötigt Predictive Policing als Big Data-Anwendung eine ausreichend große Datengrundlage, um verwertbare Ergebnisse zu erzeugen. Der Wegfall dieser Datengrundlage führte beispielsweise dazu, dass in Bayern 2021 der Testlauf des Systems PRECOBS eingestellt werden musste, da bedingt durch die Corona-Pandemie keine ausreichende Datenmenge mehr verfügbar war (Hub 2021).

5.2. Automation und Steuerung

Über die zuvor vorgestellten Ansätze der Information und Analyse hinaus können smarte Technologien und CPS außerdem selbstständig Automation und Steuerung übernehmen. Bekannte Beispiele aus der smarten Polizeiarbeit sind Polizeiroboter und Drohnen, auf welche im Folgenden näher eingegangen wird.

5.2.1. Roboter

Roboter sind als CPS dazu in der Lage, autonom oder teilautonom bestimmte Aufgaben zu erfüllen und so Aufgaben zu übernehmen, welche für Menschen physisch zu anfordernd oder zu gefährlich sind (von Lucke 2015, S. 14f). Als Beispiel für smarte Technologie im Polizeieinsatz werden Roboter in drei Interviews erwähnt (E4 2024, 29:23; E5 2024, 28:30; E10 2024, 6:45).

Besonders für den Einsatz in besonders gefährlichen Situationen ergeben sich Anwendungsszenarien für die Polizei. So kam beispielsweise der hundeähnliche Laufroboter „Spot" der Polizei NRW erstmals 2022 zu Einsatz, um eine einsturzgefährdete Brandruine in Essen zu erkunden und Bilder für die Brandursachenermittlung aufzunehmen (Hegemann 2022). Nach NRW hat Baden-Württemberg 2023 ebenfalls einen der Roboter beschafft, dessen Modell von der US-amerikanischen Firma Boston Dynamics stammt (Landesregierung Baden-Württemberg 2023a). Technisch ist der Roboter mit einer dreidimensionalen Hinderniserkennung und Greifarm ausgestattet, der eine halbautonome Öffnung von Türen ermöglicht, ohne dass Einsatzkräfte durch mögliche Sprengfallen gefährdet werden (ebd.). Ein weiterer Vorteil des Laufroboters ist, dass dieser sich schneller fortbewegen kann als Roboter auf Rädern oder Ketten, was Einsätze im schwierigen Gelände und eine spurenschonende Beweisaufnahme an Tatorten ermöglicht (ebd.). Abseits von „Spot" sind in Deutschland bislang vor allem Roboter speziell für die Sprengstoffentschärfung im Einsatz (Bendel 2023). Im Gegensatz dazu sind andernorts wie beispielsweise in Dubai und Singapur bereits humanoide Roboter bei der Polizei im Einsatz (ebd.).

Der polizeiliche Einsatz von Robotern ist mit einer ganzen Reihe an soziologischen, ethischen und rechtlichen Fragen verbunden. Hierzu gehört einerseits die Akzeptanz durch die Bevölkerung, andererseits aber auch die Akzeptanz innerhalb der Polizei, da durch den Einsatz mit Robotern der zwischenmenschliche Kontakt beeinflusst wird, welcher bei der Polizeiarbeit von zentraler Bedeutung ist (ebd.). Sind Roboter mit Kameras ausgestattet, stellen sich hier ähnliche Fragen und Herausforderungen hinsichtlich des Datenschutz wie beim bereits behandelten Einsatz von Bodycams. Besonders schwerwiegend wären Einsätze im privaten Raum, da hier die Unverletzlichkeit der Wohnung (Art. 13 Abs.1 GG) betroffen wäre (ebd.). Vor

dem Hintergrund ähnlicher Debatten aus dem militärischen Bereich könnte sich in Zukunft auch die kritische Frage ergeben, ob man Roboter bewaffnet, um mit diesen unter bestimmten Umständen Gewalttäter ausschalten zu können, wie dies bereits in den USA der Fall ist (Dampz 2022).

5.2.2. Drohnen

Unbemannte Luftfahrzeuge (Drohnen) sind ein weiteres CPS, welches inzwischen bei den Polizeien in Deutschland vermehrt zum Einsatz kommt[9]. Als Beispiel für bestehende smarte Anwendungen werden Drohnen in drei der Interviews genannt (E4 2024, 9:44; E5 2024, 4:44, E10 2024, 6:50). Drohnen werden hierbei entweder von einem Controller am Boden gesteuert oder operieren gänzlich autonom (Gusy 2014). Mithilfe der verbauten Kamerasysteme, Sensoren und Radarsysteme werden Drohnen beispielsweise dazu eingesetzt, Tatorte und Unfallstellen millimetergenau zu vermessen und nach flüchtigen Straftätern oder vermissten Personen zu fahnden (Benöhr-Laqueur 2018, S.14; E11 2024, 6:50). Weiterhin können Drohnen zur Verkehrsüberwachung und Luftaufklärung bei Versammlungen und Veranstaltungen genutzt werden (Gusy 2014; Kirchner, 2022). Bei Letzteren verweist der Projektleiter des IT-Dienstleisters allerdings auf sicherheitsbedingte Einschränkungen beim Überflug von Menschengruppen, damit im Falle eines Absturzes niemand zu Schaden käme (E5 2024, 7:23). Vorteile von Drohnen sind eine größere Effizienz und Flexibilität bei Einsätzen. So sind Drohnen beispielsweise in der Anschaffung und im Unterhalt deutlich günstiger als Polizeihelikopter und können vielfach unabhängig von der Wetterlage eingesetzt werden (Arndt 2018; Glaser 2023). Dadurch, dass moderne Drohnen sehr geräuscharm und nicht so einfach wahrnehmbar sind, ergeben sich außerdem Vorteile bei der polizeilichen Observationen (Dieckert 2017, S. 34f).

Herausforderungen und Risiken des polizeilichen Drohneneinsatz betreffen im Besonderen die Überwachung von Personen. Ähnlich wie auch beim Einsatz von Bodycams und Kameraüberwachung handelt es sich um einem Grundrechtseingriff, wenn die Polizei Drohnen zur Bild- und Videoüberwachung von Personen nutzt (Recht auf informationelle Selbstbestimmung nach Art. 2 Abs. 1 GG). Werden Drohnen zur Überwachung von Versammlungen und Demonstrationen eingesetzt, ist zudem das Grundrecht auf Versammlungsfreiheit betroffen, weshalb ein Einsatz hier nur im Falle einer konkreten Gefahr zulässig wäre (WD 2021, S. 8). Des Weiteren wird für solche Einsätze eine eigene Rechtsgrundlage vorausgesetzt, was in der Praxis jedoch häufig problembehaftet ist, wie beispielsweise Art. 47 des Bayeri-

[9] Fritz (2020) erwähnt in seiner Arbeit den Einsatz oder Pilotprojekte bei der Bundespolizei und zwölf Landespolizeien (S. 39). Inzwischen haben auch die verbleibenden Bundesländer Baden-Württemberg, Bremen, Hamburg und Thüringen Drohnen für ihre Polizei beschafft (MDR Thüringen 2023; Michel 2024; Schönfelder 2023; Zand-Vakili 2020).

schen Polizeiaufgabengesetztes (PAG) zeigt (WD 2021, S. 8; Benöhr-Laqueur 2018, S. 16f). Ein weiteres umstrittenes Beispiel aus der jüngeren Vergangenheit sind Drohneneinsätze während der Coronapandemie zur Überwachung von Kontaktverboten, welche ebenfalls als nicht rechtmäßig angesehen werden (Irnich 2021).

6. Neue Einsatzmöglichkeiten smarter Technik, Big Data und fortgeschrittener KI bei der Polizei

Bevor auf die ausgewählten Anwendungsfälle aus den Bereichen „Unterstützung beim Einsatzmanagement und operativen Prozessen“ und „Unterstützung bei polizeilichen Kernaufgaben“ eingegangen wird, soll zuerst ein kurzer Blick auf die IT-technischen Grundlagen zum Austausch und Management der benötigten Daten geworfen werden.

6.1. Plattformen und Datenmanagement

6.1.1. Polizei-Cloud

Als Lösung für Herausforderungen des polizeilichen Big Data Managements wird von mehreren der Experten einerseits auf den Bedarf an zusätzlichen Rechenzentren verwiesen, andererseits Cloud-Computing im Sinne des IoS genannt. Letzteres wird hierbei als die bevorzugte Lösung angesehen, da die vorhandenen Rechenzentren bereits heute mit den verfügbaren Speicherkapazitäten an ihre Grenzen kommen (E2 2024, 8:30; E3 2024, 16:48; E5 2024,18:18). Weiterhin wird der Vorteil einer Skalierbarkeit von Cloud-Lösungen betont, um diese flexibel dem eigenen Bedarf anpassen zu können (E2 2024, 9:58). Zudem sorgt die Dezentralität einer Cloud-Infrastruktur dafür, dass diese unempfindlicher gegen Stromausfälle, Cyberangriffe und physische Angriffe auf einzelne Rechenzentren ist (E4 2024, 17:47; E6 2024, 12:50).

Die größte Herausforderung ist die bestehende Abhängigkeit von US-amerikanischen Hyperscalern und die hiermit verbundene Notwendigkeit einer souveränen Cloud-Infrastruktur (E2 2024, 10:22; E5 2024; 19:04; E6 2024, 13:11). Derzeit wird auf europäischer Ebene angestrebt, eine souveräne Cloud-Infrastruktur im Rahmen des Gaia-X-Projekts aufzubauen (E2 2024, 13:54). Der wissenschaftliche Leiter des Cybersicherheitsunternehmens wirft an dieser Stelle auch die Frage auf, wie die Souveränität hier im Detail aussehen soll und ob sich diese auf den Standort der Server, die Cloudbetreiber oder die im Einsatz befindliche Software bezieht (E6 2024, 13:46). Als Ergänzung zur Cloud äußert er zudem den Wunsch, dass mehr Datenauswertung mittels Edge Computing auf dem jeweiligen Endgerät stattfinden solle (ebd., 14:23).

Auch Stock (2023, S. 1463f) empfiehlt aufgrund der benötigten Rechenressourcen und Skalierbarkeit den Einsatz von Cloudsystemen zur Speicherung und Verarbeitung großer Datenmengen. Kernanforderungen an eine polizeiliche Cloud-Infrastruktur betreffen neben dem Datenschutz, der Cybersicherheit und der polizeilicher Vorgangsbearbeitung auch die Mög-

lichkeit eigener Softwareentwicklungen innerhalb der Cloud (ebd., S. 1463f). Aufgrund der Bedeutung von Cloud-Lösungen für die polizeiliche IT-Infrastruktur sollten bundesweite Anforderungen und technische Standards künftig im Rahmen von P20 abgestimmt werden (ebd., S. 1464).

6.1.2. Polizei-Datenplattformen

Aufbauend auf der Cloud-Infrastruktur bilden Datenplattformen eine weitere zentrale Komponente beim polizeilichen Datenmanagement. Hierbei handelt es sich um eine Softwarelösung, welche zentral zur Speicherung, Aufbereitung, Analyse und Ausgabe von Daten aus verschiedensten Quellen genutzt wird (Stock 2023, S. 1463). Im polizeilichen Kontext existieren solche Datenplattformen beispielsweise bereits in Form des polizeilichen Informationsverbundes als gemeinsame Plattform zum Datenaustausch der Polizeien von Bund und Ländern. Dieser war erst kürzlich Gegenstand eines Urteils des Bundesverfassungsgerichts (BVerfG), welches einzelne gesetzliche Befugnisse des BKA zur Datenerhebung und -speicherung im Rahmen des Informationsverbundes für verfassungswidrig erklärte (BVerfG 2024). Stock empfiehlt außerdem die Einrichtung einer Beweismittelplattform für Polizei und Justiz, um zunächst große unstrukturierte Datenmengen zu analysieren (2023, S. 1463).

Im Rahmen der Interviews kommen Datenplattformen als solche bei der Frage zum polizeilichen Big Data-Management nur vereinzelt zur Sprache. Auf Nachfrage verweist der externe Berater der BMI darauf, dass Plattformlösungen vor allem auf Ebene der einzelnen Bundesländer entwickelt werden, um den individuellen Bedürfnissen der Landespolizeien zu entsprechen und verweist als Beispiel auf das Land Hessen (E9 2024, 9:59). Die polizeiliche Führungskraft wiederum hebt die Vorteile einer übersichtlichen Aufbereitung und Visualisierung der Datenbestände mittels Dashboards hervor, um Polizeikräfte bei Entscheidungsprozessen zu unterstützen (E10 2024, 9:50).

In mehreren Interviews werden allerdings Anwendungen zur automatisierten Recherche- und Analyse erwähnt, welche oft ein Kernbestandteil von polizeilichen Datenplattformen sind und dem Erkennen von Zusammenhängen dienen (E3 2024, 12:05; E4 2024, 10:05; E5 2024, 13:10; E7 2024, 7:50). Unklar ist, inwiefern es sich hierbei bereits um KI-Systeme handelt (E6 2024, 10:16). Aufgrund sehr umfangreicher Datenverarbeitung sind insbesondere Recherche- und Analyse-Systeme des US-amerikanischen Herstellers Palantir, welche bereits in NRW, Hessen und Bayern im Einsatz sind, stark umstritten (Kurz 2024a). Auch der Jurist der NGO für Grund- und Menschenrechte unterstreicht die Gefahr der Diskriminierung Unbeteiligter bei einer umfassenden automatisierten Datenverarbeitung (E7 2024, 25:04). Vor diesem Hintergrund hatte das BVerfG in einem Urteil von 2023 der auto-

matisierten Massendatenauswertung durch die Polizei hinsichtlich der Umsetzung und verwendeten Datenquellen klare Grenzen gesetzt (Kurz 2023).

6.1.3. Polizei-Datenräume

In ihrer Mitteilung vom 19.2.2020 zur Europäischen Datenstrategie nennt die Europäische Kommission ausdrücklich die Erleichterung von Strafverfolgung als Ziel gemeinsamer europäischer Datenräume für die öffentliche Verwaltung (Europäische Kommission 2020, S. 27). Sogenannte Datenräume sind dabei laut der Definition des Gaia-X Hub Deutschland „eine föderierte, offene Infrastruktur für souveränen Datenaustausch, die auf gemeinsamen Vereinbarungen, Regeln und Standards beruht" (Reiberg, Niebel & Kraemer 2022, S. 11). Diese Definition wurde aufgrund ihrer Übersichtlichkeit in Frage acht des Interviewleitfadens verwendet, welche sich auf das Verhältnis zwischen dem im Aufbau befindlichen zentralen Datenhaus von P20 und dem dezentralen Konzept der Datenräume bezieht. Da das Thema der Datenräume ein sehr umfangreiches Thema ist, soll an dieser Stelle nur ein kurzer Überblick über die wesentlichen Ergebnisse aus den Interviews gegeben werden.[10]

Datenräume zielen darauf ab, vorhandene Datensilos aufzubrechen und so den Austausch zwischen unterschiedlichen Teilnehmern des Datenraumes zu ermöglichen, zu erleichtern und zu steuern, allen voran Empfängern und Bereitstellern von Daten (ebd., S. 12f). Dies sind im vorliegenden Fall in allererster Linie die Polizeibehörden von Bund und Ländern. Die diesbezügliche Frage, welche räumliche Ausdehnung ein Verbund unterschiedlicher Polizei-Datenräumen sinnvollerweise haben sollte (bezogenen auf einen bundesweiten BKA-, Europol- oder Interpol-Datenraum), wird in den Interviews sehr unterschiedlich beantwortet. Das allgemeine Stimmungsbild unter den Experten tendiert jedoch zu einem Verbund auf europäischer Ebene. Als Voraussetzungen für den Datenaustausch innerhalb eines Interpol-Datenraum werden völkerrechtrechtliche Kooperationsabkommen zur Sicherstellung eines ausreichenden Datenschutzes sowie ein klarer Sinn und Zweck eines Austausches auf internationaler Ebene genannt (E1 2024, 14:55; E3 2024, 25:15, E4 2024, 16:40). Je nach Situation können auch nicht-polizeiliche Behörden an Polizeidatenräumen beteiligt werden (beispielsweise Justiz und Ausländerbehörden), welche mit der Polizei zusammenarbeiten. Auch wäre eine Beteiligung von Unternehmen und Dienstleistern aus dem IT-Sektor im Rahmen von Digitalisierungsprojekten vorstellbar, wobei hier besonders die Voraussetzungen des Datenschutz und der Cybersicherheit hervorzuheben sind (E5 2024, 12:38).

[10] Einen umfassenden Überblick über Datenräume im Kontext urbaner Sicherheit bietet Huber (2022, S.114-141), wobei hier auch auf die Rolle der Polizei eingegangen wird.

Ähnlich unterschiedlich wie die räumliche Ausdehnung sind die Einschätzung zu den Datenarten, welche sinnvollerweise zur Verfügung gestellt und ausgetauscht werden. Neben einer Vielfalt an polizeilichen Daten wie Vorgangsdaten, Falldaten und Daten aus operativen Maßnahmen wird hier auch auf andere behördliche Daten wie Justiz-, Visa- und Schengen-Daten verwiesen (E1 2024, 11:46; E2 2024, 12:04; E6 2024, 19:17). Da es sich hierbei um behördeninterne und besonders sensible Daten handelt, wird in mehreren der Interviews die Notwendigkeit klarer Zugriffregelungen betont (E2 2024; 13:37; E3 2024, 17:28; E5 2024, 17:13, E6 2024, 19:40; E7 2024, 16:11). Diese sind auch Voraussetzung für die „Souveränität" beim Austausch in Datenräumen, weshalb technische und organisatorische Vorkehrungen bereits bei der Konzeption von Datenräumen getroffen werden müssen, um unbefugte Zugriffe auf sensible Daten zu vermeiden (Huber 2022, S. 138; Reiberg, Niebel & Kraemer 2022, S. 5f). Des Weiteren nennt der externe Berater des BMI Trainingsdaten für KI-Systeme und Schulungsdaten als Beispiele für im engeren Sinne nicht-behördliche Daten, welche in einem Datenraum getauscht und bereitgestellt werden können (E9 2024, 12:56). In technischer Hinsicht setzt der Austausch und die anschließende Datenhaltung und -verarbeitung eine entsprechend ausgebaute und interoperable IT-Infrastruktur voraus, wobei die zuvor bereits erläuterten Cloud-Lösungen und Datenplattformen hier eine zentrale Funktion einnehmen (E2 2024, 13:20; Huber 2022, S. 125-129).

Im Rahmen der Interviews konnte nicht abschließend genau geklärt werden, wie das Verhältnis zwischen dezentralen Datenräumen der Polizei und dem zentralen Datenhaus von P20 einzuordnen ist. Einen Anhaltspunkt aus der Literatur bietet das häufig formulierte Zielbild eines „Datenhaus-Ökosystems" (Gadorosi & Matthey 2023, S. 1425). Reiberg, Niebel und Kraemer verweisen nämlich darauf, dass „Daten-Ökosysteme" durch den häufigen Bezug auf „Daten-Lebenszyklen" als eine dem Datenraum übergeordnete Einheit betrachtet werden können (2022, S. 16).

6.2. Unterstützung beim Einsatzmanagement und operativen Prozessen

Im Folgenden werden vier ausgewählte Ansätze vorgestellt, wie KI die Polizei beim Einsatzmanagement und operativen Prozessen unterstützen kann. Der Begriff des Einsatzmanagements soll hierbei die Planung von Großeinsätzen und Steuerung von Einsatzkräften während laufender Einsätze beschreiben. Operative Prozesse beschreiben wiederum die polizeiliche Aufgabenwahrnehmung während laufender Einsätze (oft in doppelfunktionaler Weise). Die hier vorgestellten Anwendungsfälle sollen dabei vor allem die Möglichkeit einer polizeilichen Aufgabenwahrnehmung in Echtzeit beziehungsweise nahezu in Echtzeit adressieren (Real-Time Government).

6.2.1. KI-unterstützte Einsatzplanung

Der erste Anwendungsfall zielt darauf ab, die Polizei mittels einer KI-Anwendung bei der Planung von Großeinsätzen wie Spielen der Fußballbundesliga oder regelmäßigen Großdemonstrationen wie am 1. Mai zu unterstützen. Hierbei handelt es sich somit vor allem um eine präventive Maßnahme zum Zwecke einer optimierten Gefahrenabwehr. Als Datengrundlage können Berichte zu früheren Einsätze dienen.

KI-Systeme zur Einsatzplanung können dazu genutzt werden, um den voraussichtlichen Bedarf an Einsatzkräften, Fahrzeugen und sonstigem Material, welches für den Einsatz benötigt wird, zu ermitteln. Praktische Mehrwerte dürften sich hierbei vor allem dadurch ergeben, da so eine optimierte polizeiliche Ressourcenplanung gewährleistet wird. Im Falle oben genannter Großeinsätze ist es üblich, dass Einheiten der Bereitschaftspolizei anderer Bundesländer und der Bundespolizei zur Unterstützung herangezogen werden, was mit Kosten und zusätzlichem logistischen Aufwand verbunden ist. Der KI-Wissenschaftler bejaht diesbezügliche Möglichkeiten zur Ressourcenoptimierung, merkt jedoch an, dass es hierzu nicht in jedem Falle einer fortschrittlichen KI bedarf (E4 2024, 23:18).

Weiterhin besteht die Möglichkeit, KI-gestützte Prognosen rund um den Einsatz zu machen, um (ähnlich wie beim ortsbezogenen Predictive Policing) Einsatzkräfte optimal im Einsatzgebiet zu positionieren und auf Basis früherer Einsatzerfahrungen Gefahrenschwerpunkte frühzeitig zu identifizieren (E3 2024, 30:39). Letzteres bietet sich insbesondere dann an, wenn Einsatzkräfte nicht aus dem gleichen Bundesland stammen und selbst nicht ortskundig sind. Auch der wissenschaftliche Leiter des Cybersicherheitsunternehmens sieht die Möglichkeit, KI bei der Einsatzplanung zur Identifizierung von Gefahrenhotspots einzusetzen. Gleichzeitig warnt er davor, die tatsächlichen Potenziale solcher Prognosen zu überschätzen, da es sich hierbei lediglich um statistische Verfahren handelt (E6 2024, 23:08). Der Jurist der NGO für Grund- und Menschenrechte knüpft den möglichen Einsatz solcher Prognosesysteme daran, ob hierbei personenbezogene Daten verarbeitet werden und welche Konsequenzen dies hätte (E7 2024, 21:43). Als Beispiel für Prognosen mit personenbezogenen Daten nennt der Professor für Strafrecht die Möglichkeit, Social-Media-Daten mit einfließen zu lassen, um das voraussichtliche Aufkommen von Demonstrationsteilnehmern zu ermitteln (E8 2024, 25:58). Ein solcher Einsatz bedarf jedoch einer expliziten Rechtsgrundlage, die es so noch nicht in Deutschland gibt und erst noch geschaffen werden müsste (ebd., 27:11).

6.2.2. KI-unterstütztes Echtzeit-Einsatzmanagement

Während im vorherigen Anwendungsfall die KI-basierte Einsatzplanung auf historischen Daten basiert, soll das KI-unterstützte Einsatzmanagement in diesem Falle mittels Echtzeitdaten vorgenommen werden. Auch hierbei geht es in erster Linie um präventivpolizeiliche Maßnahmen, je nach konkreter Situation kann dies auch doppelfunktionale Maßnahmen beinhalten. Entsprechende KI-Systeme sollen es der Polizei ermöglichen, vernetzt und nahezu in Echtzeit auf sich schnell verändernde Einsatzlagen und Bedrohungen zu reagieren.

Ein vergleichbarer Ansatz, welcher bereits heute Anwendung findet, ist das KI-basierte Alarmrouting (E3 2024, 28:57). Hierbei wird nach Eingang eines Alarms auf Basis von Geo- und Verkehrsdaten KI-basiert der schnellste verfügbare Weg zum Einsatzort ermittelt und die Einsatzkräfte dorthin navigiert. Weiterhin können KI-Systeme dazu genutzt werden, um komplexe Einsatzlagen laufend zu analysieren und zu bewerten. So können beispielsweise Gefahrstoffe, Fluchtbewegungen oder Schüssen frühzeitig erkannt werden (E2 2024, 16:48; E3 2024, 30:14). Die hierzu notwendigen Bild-, Video-, oder Audiodateiendaten können mittels Bodycams oder stationären Kameras, Drohnen und Sensoren sowie anderen CPS aufgezeichnet und in Echtzeit zur Auswertung übertragen werden. Auf Basis dieser Daten kann das KI-System für den Einsatzleiter so automatisch Entscheidungsvorlagen generieren (E5 2024, 26:42). Vor dem Hintergrund der bereits in den Abschnitt 5.1.1. und 5.1.2. geäußerten rechtlichen Grenzen ist allerdings auch in diesem Fall darauf zu achten, wofür diese Daten genau eingesetzt werden, insbesondere bei der Verwendung personenbezogener Daten.

Auch bei Huber findet sich mit der „Intelligenten Steuerung von Sicherheitskräften bei Großveranstaltungen“ ein Ansatz für ein Einsatzmanagement in Echtzeit. Dieser wurde jedoch im Verlauf seiner Dissertation nicht weiter in Betracht gezogen, da sich die Teilnehmenden der Fokusgruppeninterviews ablehnend geäußert haben (Huber 2022, S. 219-222). In technischer Hinsicht wirft der KI-Wissenschaftler zudem die Frage auf, ob verfügbare KI-Systeme ausreichend trainiert werden können, um diese in dynamischen Einsatzlagen einzusetzen (E4 2024, 32:44). Angesichts der Komplexität und möglicher rechtlicher Einschränkungen bei einer Echtzeitübertragung rechnet dieser nicht damit, dass Echtzeit-Einsatzmanagementsysteme in absehbarer Zeit Anwendung finden (ebd., 33:56).

6.2.3. Biometrische Fernidentifizierung in Echtzeit

In Abschnitt 5.1.2. wurde bereits ein Beispiel für algorithmenbasierte Videoüberwachung vorgestellt. Ein weiterer Ansatz, welcher mit Blick auf Datenschutz und staatliche Massenüberwachung äußerst kritisch gesehen wird, ist

die KI-basierte Fernidentifizierung mittels biometrischer Daten. Umgangssprachlich wird hierbei meist von „Gesichtserkennung" gesprochen, jedoch lassen sich Personen beispielsweise auch anhand ihres individuellen Bewegungsmusters identifizieren (von Lucke 2020, S. 118). Je nach Situation ergibt sich so eine präventive oder eine repressive Wirkung, indem man Personen von der Begehung einer Straftat abhalten will oder im Anschluss an eine solche zielgerichtet nach Verdächtigen fahndet.

Bislang gab es hierzu in Deutschland lediglich ein Pilotprojekt am Berliner Bahnhof Südkreuz (E1 2024, 4:15; Gruber 2018). Jüngst wurde dieses Thema auch im Rahmen der KI-Verordnung der EU aufgegriffen, welche in Art. 5 Abs. 1 h) die Verwendung biometrischer Echtzeit-Fernidentifizierungssysteme in öffentlich-zugänglichen Räumen zu Strafverfolgungszwecken nur in bestimmten Ausnahmefällen und engen Grenzen erlaubt. Dem war eine längere Debatte vorausgegangen, bei welcher das EU-Parlament ein allgemeines Verbot dieser Praktik gefordert hat, während eine Reihe an Mitgliedsstaaten einen Einsatz zum Zwecke der öffentlichen Sicherheit befürwortete (Weiz 2023). Künftig dürfen solche Systeme laut KI-Verordnung dafür eingesetzt werden, um gezielt nach Opfern und Verdächtigen besonders schwerer Straftaten (sogenannten „Katalogstraftaten") zu fahnden oder unmittelbare Gefahren wie Terroranschläge zu verhindern. Ein praktischer Einsatz innerhalb der Mitgliedsstaaten bedarf jedoch weiterhin einer eigenen nationalen Rechtsgrundlage (E1 2024, 58:04).

Trotz der Einschränkungen aus Art. 5 der KI-Verordnung werfen Kritiker ein, dass diese Regelungen zu weit gehen und damit zu rechnen sei, dass Mitgliedsstaaten die eingeräumten Ausnahmen bei der biometrischen Fernidentifizierung zur Gänze ausreizen werden (Krempl 2023). Weiterhin weist der Jurist der NGO für Grund- und Menschenrechte im Interview darauf hin, dass es angesichts der erheblichen Grundrechtsrelevanz dieser Maßnahme immer noch unklar ist, ob diese in ihrer Wirkung wirklich zu einer effizienteren Polizeiarbeit beiträgt (E7 2024, 8:02). Auch die polizeiliche Führungskraft äußert sich angesichts der rechtlichen Schranken sehr zurückhaltend zu einem möglichen Einsatz und betont, dass beim Thema biometrische Daten „ein Warnsignal hinten dran [sei]", wo unklar ist, wie man damit umgeht (E10 2024, 21:10).

6.2.4. Unterstützung bei der Vorgangs- und Sachbearbeitung

Ein wesentlicher Teil der polizeilichen Arbeit beinhaltet das Verfassen von Einsatzberichten, welche alle relevanten Angaben zu den Ereignissen, beteiligten Personen und polizeilichen Maßnahmen enthalten müssen. Hierbei dienen sie einerseits der Nachvollziehbarkeit des polizeilichen Handelns im Sinne des Rechtsstaats. Zum anderen können Einsatzberichte auch die

Grundlage für spätere Ermittlungen zu Straftaten bilden, was voraussetzt, dass diese vor Gericht als Beweismittel verwertbar sind.

In der Praxis besteht die Herausforderung darin, dass das Verfassen von Berichten zeitaufwendig ist und die verfassenden Polizeibeamten kognitiv beansprucht, welche dies aufgrund geringer Personalressourcen zudem oftmals allein tun müssen (E3 2024, 33:00). Hier bestehen Ansätze für GKI, um die polizeiliche Vorgangs- und Sachbearbeitung zu vereinfachen und diese parallel zum Einsatz vorzunehmen. LLMs können hierbei zum automatisierten Verfassen von Berichten und Zusammenfassungen genutzt werden, wodurch der verantwortliche Polizeibeamte zeitlich entlastet wird, um sich anderen Aufgaben zu widmen (E3 2024, 34:24). Diesbezüglich verweist der wissenschaftliche Leiter des Cybersicherheitsunternehmens auf eine von seinen Unternehmen entwickelte Anwendung zur automatisierten Aufnahme von Strafanzeigen (E6 2024, 24:33). Des Weiteren kann GKI nach Einschätzung des Vertriebsleiters und ehemaligen Polizeibeamten auch als eine Art „Sparring-Partner" fungieren und zusätzliche Hinweise und Einschätzungen zu einem Sachverhalt geben, welche für anschließende polizeiliche Maßnahmen von Relevanz sind (E3 2024, 33:43, 35:24).

Im Gegenzug äußert sich der KI-Wissenschaftler kritisch zum Ansatz des LLMs als „Sparring-Partner" und sieht den Einsatz von LLMs hier vordergründing im Zusammenfassen und Verfassen strukturierter Berichte (E4 2024, 27:25). Des Weiteren besteht hier das Problem der „Halluzinationen" von GKIs, dessen man sich einerseits bewusst sein muss, und die es andererseits technisch zu adressieren gilt (ebd., 30:29). Aus rechtlichen Gründen ist es zudem erforderlich, dass final im Sinne eines „Human-in-the-Loop" immer ein menschlicher Akteur die KI-generierten Berichte kontrolliert und freigibt (ebd., 28:05). Dies gilt vor allem dann, wenn diese später vor Gericht als Beweismittel Verwendung finden sollen (E7 2024, 23:20).

Entgegen der öffentlichen Prominenz von ChatGPT dürfen aus Gründen des Datenschutzes keine LLMs von kommerziellen Anbietern genutzt werden, da die Daten auf lokalen Servern der Polizei gespeichert werden müssen (E4 2024, 26:57). Hierzu verweist der KI-Wissenschaftler auf die Verfügbarkeit von Open Source LLMs, welche sich im Rahmen eines Fine Tunings relativ einfach für spezielle polizeiliche Anwendungen trainieren lassen (ebd., 29:16).

6.3. Unterstützung bei polizeilichen Kernaufgaben

Der Begriff der polizeilichen Kernaufgaben soll hier als ein allgemeiner Sammelbegriff dienen, welcher neben präventiven und repressiven polizeilichen Maßnahmen auch die Ausbildung und das Training von Einsatzkräften beinhaltet. Im Folgenden werden hierzu vier weitere ausgewählte

Anwendungsfälle vorgestellt, wobei neben KI hier auch die Technologien der virtuellen und erweiterten Realität Anwendung finden.

6.3.1. Spurensicherung und Forensik

Das Aufgabenfeld der Spurensicherung und Forensik beinhaltet das systematische Sichern und Sammeln sowie die wissenschaftliche Analyse von Spuren, um diese anschließend als Beweismitteln vor Gericht zu verwenden. Dementsprechend ist dieser Anwendungsfall der repressiven Polizeiarbeit zuzuordnen.

KI kann hier beispielsweise dazu verwendet werden, digital eingescannte Fußspuren zu analysieren und so den betreffenden Schuhtypen zu ermitteln oder herauszufinden, ob die betreffende Fußspur bereits an früheren Tatorten gefunden wurde (E5 2024, 27:13; E7 2024, 7:30). Weiterhin kann KI in der Forensik dazu genutzt werden, um Handschriften und bestimmte Sprachmuster zu identifizieren (E8 2024, 24:41).

Am weitaus häufigsten erwähnen die Experten Spurensicherung und Forensik im Zusammenhang mit den Technologien der erweiterten (Englisch Augmented Reality (AR)) und virtuellen Realität (Englisch Virtual Reality (VR)). AR bezeichnet die Erweiterung der menschlichen Realitätswahrnehmung mittels Brillen oder mobilen Geräten, wobei diese auf einzelne Personen, bestimmte Objekte oder ganze Umgebungen angewendet werden kann. (Knoll & Stieglitz 2022, S. 8). VR beschreibt die Darstellung und Wahrnehmung einer realitätsähnlichen Umgebung inklusive besonderer Eigenschaften in einer interaktiven virtuellen Umgebung (ebd., S. 9). Insbesondere VR bietet hier Anwendungspotenziale. So kann diese dazu eingesetzt werden, um Tatorte virtuell nachzubilden und mögliche Tatabläufe im Sinne eines. „Digitalen Zwilling des Tatortes“ zu simulieren (E2 2024, 24:50; E3 2024, 41:44). Hierzu müssen die betreffenden Tatorte zuvor detailliert eingescannt und auf Basis dieser Daten im Anschluss am Computer für eine dreidimensionale VR-Umgebung nachgebildet werden. Die polizeiliche Führungskraft verweist hierzu auf die „Cave“ des LKA Baden-Württemberg und das „Holodeck“ des LKA Bayern als erste praktische Beispiele für eine VR-gestützte Tatortrekonstruktion in Deutschland (E10 2024, 25:29). Letzteres wurde in der Vergangenheit bereits eingesetzt, um ein versuchtes Tötungsdelikt in der Münchner S-Bahn aufzuklären (Heitmüller 2023). Auch AR kann zur Unterstützung bei der Spurensicherung genutzt werden, indem Polizeibeamten an Tatorten oder bei Hausdurchsuchungen angezeigt wird, welche relevanten Beweismittel es zu sichern gilt. Der wissenschaftlicher Leiter des Cybersicherheitsunternehmens sieht hierin eine Chance zur Entlastung der Forensik, da diese sich so auf die Auswertung wesentlicher Beweismittel konzentrieren kann (E6 2024, 27:15)

Trotz dessen, dass diese Ansätze unter den interviewten Experten eine breite Zustimmung finden, weist der KI-Wissenschaftler darauf hin, dass sich aufgrund des Arbeitsaufwandes und damit verbundener Kosten ein Einsatz virtueller Tatorte nicht in jedem Fall lohnt (E4 2024, 41:37). Entsprechend sollten sich diese auf ausgewählte Kriminalfälle beschränken, wo sich erkennbare Vorteile für die Aufklärung und anschließende gerichtliche Verwertung ergeben. Der Aufwand und die Kosten einer virtuellen Tatortrekonstruktion dürften auch einer der Gründe sein, wieso diese in Deutschland noch keine allzu große Verbreitung gefunden hat (E2 2024, 26:17).

6.3.2. Unterstützung bei Vernehmungen

Ähnlich wie bei der Vorgangs- und Sachbearbeitung kann GKI auch zur Unterstützung bei der polizeilichen Vernehmung von Zeugen und Verdächtigen genutzt werden. Dies ist ebenfalls eine repressive Maßnahmen und dient dazu, mehr über einen konkreten Sachverhalt oder Tatverlauf zu erfahren.

Auch hier besteht in erster Linie die Möglichkeit, dass GKI dazu genutzt wird, um die mündlichen Aussagen in Form eines Vernehmungsprotokolls zu verschriftlichen und im Falle einer fremdsprachigen Person parallel auch eine Übersetzung vorzunehmen Der externe Berater des BMI verweist hier auf eine bereits existierende Anwendung zur polizeilichen Transkription (E9 2024, 18:49). Laut der polizeilichen Führungskraft ist insbesondere die Möglichkeit zur Übersetzung relevant, da vereidigte Dolmetscher oft nur schwer verfügbar sind (E10 2024, 23:03). Aus diesem Grund sei seiner Ansicht nach die Transkription und Übersetzung von Vernehmungen einer der ersten Anwendungsfälle für GKI, der für eine praktische Umsetzung in der Polizei in Betracht komme (ebd., 23:21). Sollen die Vernehmungsprotokolle im Anschluss als Beweismittel vor Gericht dienen, müssen auch diese zuvor notwendigerweise im Sinne des „Human-in-the-loop" kritisch geprüft und freigegeben werden. Laut des Juristen der NGO für Grund- und Menschenrechte ist dies vor allem dann wichtig, wenn mittels KI eine fremdsprachige Übersetzung vorgenommen wird (E7 2024, 24:33).

Der ehemalige Polizist und Mitarbeiter eines IT-Dienstleisters weist zudem auf die Möglichkeit hin, dass GKI während einer Vernehmung Vorschläge für Fragen erzeugt und auf mögliche Widersprüche zwischen verschiedenen Aussagen zu einem Sachverhalt hinweist (E3 2024, 38:18). Hierzu betont er aber, dass es nicht darum gehe, mögliche Lügen in den Vernehmungen aufzudecken, sondern Polizeibeamte dabei zu unterstützen, wichtige Aussagen und Zusammenhänge frühzeitig zu erkennen und die so Möglichkeit zu Rückfragen zu haben (ebd., 38:50). Trotz dieser Potenziale äußert er sich skeptisch, dass GKI in naher Zukunft hierzu eingesetzt werden kann (ebd., 39: 35).

6.3.3. Analyse biometrischer Daten zur Online-Fahndung

Aufgrund eines erheblichen Eingriffs in die Privatsphäre und der Sorge vor breiter staatlicher Überwachung ist dieser Anwendungsfall ähnlich umstritten wie die biometrische Fernidentifizierung, auf die bereits in Abschnitt 6.2.3. eingegangen wurde. Ursprünglicher Auslöser für die Debatte um den Einsatz solcher KI-Systeme in Deutschland war der Fall des ehemaligen Mitglieds der Roten Armee Fraktion (RAF) Daniela Klette. Bevor diese im Februar 2024 festgenommen wurde, war es Journalisten bereits 2023 gelungen, sie mithilfe alter Fahndungsbilder und dem Programm PimEyes auf online frei-verfügbaren Fotos zu identifizieren (Klein 2024). Zu diesem Zeitpunkt fehlte es der deutschen Polizei allerdings an einer Rechtsgrundlage, um selbst KI-Systeme zur Online-Identifizierung einzusetzen. Als Reaktion auf den Anschlag in Solingen wurde Mitte 2024 im Rahmen des sogenannten Sicherheitspaketes versucht, eine Rechtsgrundlage dafür zu schaffen, dass künftig die Bundespolizei und das BKA entsprechende KI-Systeme zum Abgleich mit öffentlich-zugänglichen biometrischen Daten aus dem Internet nutzen können, um Tatverdächtige zu identifizieren. Dies scheiterte zuletzt jedoch am Widerstand des Bundesrates (Stand 21.11.2024), wo der Leiter der bayrischen Staatskanzlei dessen Inhalt als unzureichend kritisierte (Tagesschau 2024a). Vorab war außerdem seitens mehrerer Sachverständiger und Experten kritisiert worden, dass die Vorgaben innerhalb des Gesetzesentwurfs nicht hinreichend genau seien, unter anderem bezüglich der verwendeten Technologie sowie der genauen Bedeutung von „öffentlich-zugänglichen" Daten (Kipker 2024; Sorge 2024). Letzteres spricht auch der Professor für Öffentliches Recht im Interview an (E1 2024, 32:52). Bislang besteht für die Polizei nur die Möglichkeit, retrograde biometrische Abgleiche mit Bildern aus der Datenbank des polizeilichen Informationssystems (INPOL) vorzunehmen (Rath 2024).

Seitens der KI-Verordnung wird die retrograde biometrische Online-Identifizierung zu Fahndungszwecken nach Anhang III Abs.1a) als Hochrisiko-KI eingestuft. Somit ist deren Einsatz zwar nicht grundsätzlich untersagt, allerdings ist der Einsatz an die Vorschriften für Hochrisiko-KI-Systeme in der Strafverfolgung geknüpft, welche die KI-Verordnung vorgibt. Der Jurist der NGO für Menschen- und Grundrechte weist jedoch im Interview auf die Problematik der zugrundeliegenden Datenbänke hin (E7 2024, 39:16). Konkret betrifft dies Art. 5 Abs.1 e) der KI-Verordnung, welcher den Einsatz von KI-Systemen verbietet, die Datenbanken zur Gesichtserkennung durch das ungezielte Auslesen von Gesichtsbildern aus dem Internet oder von Überwachungsaufnahmen erstellen oder erweitern. Auch Prof. Dr. Christoph Sorge sprach diese Problematik als Sachverständiger in einer Anhörung vor dem Innenausschuss an. Hierbei nannte er eine Reihe an Unklarheiten in Bezug auf den deutschen Gesetzentwurf, welche eine konkrete Auslegung erschweren (Sorge 2024). Hinsichtlich einer möglichen Umsetzung hat Art.

5 Abs.1 e) KI-VO allerdings zur Folge, dass bestehende kommerzielle Gesichtserkennungsprogramme wie Clearview und PimEyes nicht eingesetzt werden können, da diese ihre Datenbanken durch datenschutzwidrige Verfahren erstellen (E7 2024, 35:52). Für den Fall eines Einsatzes in Deutschland ergibt sich so die Notwendigkeit, ein eigenes System zur Online-Gesichtserkennung zu entwickeln, welches die Vorgaben der KI-Verordnung erfüllt.

6.3.4. Training und Ausbildung

Zusammen mit der bereits erläuterten Spurensicherung und Forensik sieht der überwiegende Teil der Experten Einsatzmöglichkeiten für VR und AR im Bereich der Ausbildung und des Trainings von Polizeibeamten.

Die polizeiliche Führungskraft verweist hierzu auf die Polizei Zürich, welche VR bereits zu Trainingszwecken einsetzt (E10 2024, 26:08). Er rechnet zudem damit, dass dies auch in Deutschland zeitnah eine verstärkte Anwendung finden wird, da VR die Möglichkeit biete, verschiedene Einsatzszenarien kostengünstig und realitätsnah zu trainieren (ebd., 26:23). Ähnlich sehen es zwei der Experten aus dem IT-Sektor, welche vor allem Trainingsansätze für polizeiliche Spezialeinheiten und Verhandlungsführer sehen (E2 2024, 24:10; E5 2024, 35:20). Insbesondere gefährliche Einsatzszenarien lassen sich so in einer sicheren, aber realitätsnahen Umgebung flexibel trainieren. In den vergangenen Jahren gab es bereits erste Testläufe für VR-Trainingsszenarien an verschiedenen deutschen Polizeihochschulen (von der Burg, Ebenau & Janssen 2023, S. 80f). Der Projektleiter des IT-Dienstleisters verweist außerdem auf das Metaverse, welches die Verbreitung von VR-Anwendung in naher Zukunft voraussichtlich weiter fördern wird (E5 2024, 35:30).

Der Vertriebsleiter und ehemalige Polizeibeamte sieht vor allem beim Training komplexerer Einsatzszenarien Potenzial für VR. Gleichzeitig merkt er an, dass seiner Ansicht nach das Potenzial von AR-Anwendungen für das polizeiliche Training stark unterschätzt würde. Als Vorteile nennt er, dass AR im Gegensatz zu VR flexibler eingesetzt werden kann, kostengünstiger sei und das regelmäßige Training alltäglicher aber ebenso essenzieller Einsatzabläufe ermögliche (E3 2024, 45:45). Als weiteren Vorteil nennt die polizeiliche Führungskraft die Möglichkeit, mittels AR Dinge haptisch zu präsentieren und so besser nachvollziehbar zu machen (E10 2024, 27:15).

Insbesondere beim Training mit VR gibt es allerdings eine Reihe an Anforderungen und offenen Fragen. So gilt es darauf zu achten, dass die verwendeten Trainingsszenarien zuvor ethisch reflektiert wurden, um Diskriminierung zu verhindern, welches später Auswirkungen auf das Verhalten der Auszubildenden im Polizeialltag haben könnte (Giessing & Frenkel 2022, S. 685). Weiterhin gilt es, mit den im Rahmen des Trainings erhobenen Daten

im Sinne des Datenschutz angemessen umzugehen (ebd., S. 685). Da VR-Training (zum Teil auch aus Kostengründen) bislang noch keine rege Verwendung gefunden hat, bestehen zudem Unklarheiten bezüglich Transfermöglichkeiten des virtuell erlernten in den „realen“ Polizeialltag (von der Burg, Ebenau & Janssen 2023, S. 84).

7. Herausforderungen, Anforderungen und Vorgaben

Während für die jeweiligen Anwendungsfälle in den Kapiteln fünf und sechs bereits eine Reihe an Herausforderungen, Anforderungen und Vorgaben genannt wurden, sollen diese nun genauer betrachtet und analysiert werden. Das folgende Kapitel beinhaltet deshalb einen Überblick über die wesentlichen Herausforderungen, Anforderungen und Vorgaben bei der Entwicklung, Einführung und dem Einsatz smarter Technologien, Big Data und KI in der Polizei.

7.1. Technische Herausforderungen

7.1.1. Technische Grundlagen und Infrastruktur

Damit die zuvor vorgestellten Anwendungsfälle und weitere Ansätze von Smarter Technologie, Big Data und KI bei der Polizei optimal eingesetzt werden können, bedarf es einer geeigneten IT-Infrastruktur zur Aufbewahrung, Aufbereitung, Verarbeitung und zum Austausch relevanter Daten. Auf den Bedarf einer souveränen Polizei-Cloud, polizeilicher Datenplattformen, leistungsfähiger Recherche-Analyse-Software und Polizei-Datenräume wurde bereits in den Abschnitten 6.1.1. bis 6.1.3. eingegangen.

Wie tief allerdings die grundsätzlichen Probleme in Deutschland liegen, unterstreichen der Projektleiter des IT-Dienstleistungsunternehmens und der wissenschaftliche Leiter des Cybersicherheitsunternehmens in ihren jeweiligen Interviews. Ersterer weist auf die Herausforderung einer angemessenen Datenqualität zum Training von KI-Systemen hin, da es hierzu strukturierter Daten bedarf. Laut ihm sind jedoch schätzungsweise 90% der polizeilichen Daten in Deutschland unstrukturiert und müssten zuerst mit einem entsprechenden Aufwand in strukturierte Daten umgewandelt werden (E5 2024, 9:13). Ein weiteres Problem ist die Unklarheit darüber, welche Daten überhaupt genau zur Verfügung stehen und wo diese genau liegen (ebd., 9:50). Hier besteht die Herausforderung, diese verstreut und voneinander abgekapselt liegenden Datensilos aufzubrechen und miteinander zu verknüpfen, wie es auch P20 zum Ziel hat (E2 2024, 16:10). Als ein weiteres Grundproblem nennt der wissenschaftliche Leiter des Cybersicherheitsunternehmens den mangelnden Stand des E-Government in der deutschen Polizei, ein Problem, welches auch zahlreiche andere Verwaltungsbereiche betrifft. Hier fordert er, zuallererst die bestendenden Aktenbestände zu digitalisieren, bevor man sich auf ambitionierte KI-Projekte einlässt (E6 2024, 26:36).

7.1.2. Technische Anforderungen

Mit der Gefahrenabwehr und Strafverfolgung erfüllt die Polizei sicherheitskritische Aufgaben, weshalb entsprechend hohe Anforderungen an die von ihr verwendete Technologie zu stellen sind. Zuallererst ist hier die Interoperabilität der polizeilichen Anwendungen zu nennen. Diese soll unter anderem durch eine Harmonisierung der polizeilichen IT-Architektur im Rahmen von P20 erreicht werden. Grundlage hierfür ist die 2016 beschlossene „Saarbrücker Agenda", da die zum damaligen Zeitpunkt herrschende heterogene Systemlandschaft der deutschen Polizeibehörden eine Vernetzung untereinander erschwerte (Gadorosi & Matthey 2023, S. 1412). Um die nötige Interoperabilität zu gewährleisten, braucht es künftig gemeinsame Standards und geeignete Schnittstellen für den Austausch offener und vertraulicher Daten (E5 2024, 20:48). Nach der Zielsetzung von P20 sollen die polizeilichen IT-Anwendungen und Dienste in Zukunft zusammen mit den Daten des Datenhauses einheitlich und zentral für alle Beteiligten zur Verfügung stehen (Gadorosi & Matthey 2023, S. 1418).

Mit Blick auf KI-Anwendungen unterstreicht der KI-Wissenschaftler im Rahmen des Interviews mehrfach die Bedeutung von klar problemorientierten Technologieansätzen, für die es nicht in jedem Fall einer KI-Lösung bedarf (E4 2024, 10:55, 13:00, 13:17). Entsprechend gilt es hier kritisch zu evaluieren und klare Anwendungsfälle zu formulieren, bevor KI-Projekte in der Polizei umgesetzt werden. Hierbei sollte vor allem eine langfristige und kontinuierliche Anwendbarkeit eine Rolle spielen und sich an den Bedürfnissen der Polizisten im Einsatz orientieren (ebd., 42:27). Ähnlich äußert sich hierzu der Vertriebsleiter und ehemalige Polizeibeamte, welcher hierzu ein eigenes Erfahrungsbeispiel aus der mobile Polizeiarbeit nennt (E3 2024, 8:50, 53:42). Weiterhin weist Jürgen Schäberle (2023 S. 1473) darauf hin, dass polizeiliche IT-Projekte häufig mit zu hohen Anforderungen an den fachlichen Bedarf verbunden sind, was die Umsetzung erschwert, für zusätzliche Kosten sorgt und schlimmstenfalls zum Scheitern eines Projektes führt. Entsprechend empfiehlt er, die Anforderungen an den fachlichen Bedarf unter Berücksichtigung des „Pareto-Prinzips"[11] so zu formulieren, dass die IT-Projekte zeitgerecht und im vorgesehenen finanziellen Rahmen umgesetzt werden können, während gleichzeitig weite Teile des fachlichen Bedarfs abgedeckt sind (ebd., S. 1473).

Des Weiteren gilt es, dass Problem der Nachvollziehbarkeit und Transparenz von KI-Ergebnissen zu adressieren. Dieses Problem besteht bei sogenannten „Black-Box"-KI-Systeme, bei denen die internen Entscheidungsprozesse für den menschliche Benutzer nicht nachvollziehbar sind (Rouse 2024). Die Ur-

[11] Laut dem „Pareto-Prinzip" lassen sich 80% der Ergebnisse mit 20% des Aufwandes erreicht, während die restlichen 20 % der Ergebnisse 80 % des Aufwands erfordern (Laoyan, 2024).

sache sind einerseits proprietäre IT, andererseits die Verwendung von Deep-Learning als Trainingsmethode, was diskriminierende KI-Entscheidungen zur Folge haben kann (ebd.). Speziell im Polizeibereich sind diese umso schwerwiegender, wie der Jurist der NGO für Grund- und Menschenrechte mit Blick auf Minderheiten betont (E7 2024, 33:35). Auch der Professor für öffentliches Recht verweist darauf, dass es aus rechtlichen Gründen zwingend notwendig sei, diskriminierende KI-Entscheidungen technisch in den Griff zu bekommen (E1 2024, 26:15). Als weiteres Problem sind an dieser Stelle „Halluzinationen" bei Ergebnissen von GKI zu nennen. Technisch müssen diese Probleme bereits beim Training eines KI-Systems mittels einer geeigneten Trainingsmethode und qualitativ-hochwertiger Trainingsdaten adressiert werden (E2 2024, 31:22; E9 2024, 38:05). Hierbei sollen ebenfalls KI-ethische Aspekte ins Training und in die Auswahl und Zusammenstellungen der Trainingsdaten miteinfließen, um diskriminierende Ergebnisse zu verhindern oder zumindest einzugrenzen (ebd., 35:40; ebd., 38:00). Um das Problem der „Halluzinationen" technisch zu adressieren, verweist der KI-Wissenschaftler auf den Ansatz der Erklärbaren KI (Englisch Explainable AI) mithilfe sogenannter Retrieval Augmented Generation (RAG), welche Querverweise zu den Quellen einer KI-Entscheidung erstellt (E4 2024, 30:17). Auch ein regelmäßiges Feintuning der verwendeten KI-Systeme ist notwendig (ebd., 31:09). Gleichzeitig betont er mit Blick auf das Risiko von „Halluzinationen": „Die sind immer inhärent, die kriege ich bei LLMs auch erstmal nicht raus, das ist so, das muss man so einfach mal einsehen." (ebd., 31:03). Dementsprechend wichtig ist es, dieses Risiko beim polizeilichen Einsatz von KIs und LLMs immer zu berücksichtigen. Der externe Berater des BMI verweist hier aber auch darauf, dass ein starker Fokus auf Transparenz im Gegenzug „Leistungseinbußen" bei den verwenden KI-Systemen beinhaltet (E9 2024, 39:15).

Weiterhin müssen die eingesetzten Anwendungen sowohl zuverlässig als auch anwenderfreundlich sein. Ersteres gilt hier insbesondere im Außeneinsatz, da die eingesetzte Technik unabhängig von Umwelteinflüssen einwandfrei funktionieren muss (E6 2024, 33:14). Die Voraussetzung der Anwenderfreundlichkeit bezieht sich hierbei sowohl auf ältere Polizeibeamte als auch auf die allgemeine Nutzbarkeit ohne zusätzliche Schulungen und Fachkenntnisse (E2 2024, 34:29; E3 2024, 53:20; E6 2024, 33:32). Der Vertriebsleiter und ehemalige Polizeibeamte betont, dass Zuverlässigkeit und Anwenderfreundlichkeit entscheidend dafür sind, um das Vertrauen von Polizeibeamten in die Technologie – insbesondere in kritischen Situationen – sowie in ihren Dienstherren zu stärken, welcher die Technologie zur Verfügung stellt (E3 2024, 54:52).

7.1.3. Aktualität der Technik

Die Aktualität der Technik stellt in zweierlei Hinsicht eine Herausforderung dar. Erstere ist eng verbunden mit der bereits im vorherigen Abschnitt angesprochenen Interoperabilität. Der Projektleiter des IT-Dienstleistungsunternehmens verweist hierzu auf die Herausforderung, KI-Tools in sogenannte „Legacy-Systeme" zu integrieren, da viele polizeiliche IT-Systeme einen älteren Sachstand haben (E5 2024, 8:48). Damit eine Gesamtfunktionalität sichergestellt ist, müssen diese KI-Tools erfolgreich in bestehende Altsysteme integrierbar sein. Im Falle von Neubeschaffungen muss zudem darauf geachtet werden, dass es in Zukunft die Möglichkeit zur Weiterentwicklung und Anpassung gibt (E10 2024, 32:06).

Laut der polizeilichen Führungskraft ist es angesichts des rasanten technologischen Wandels und begrenzter finanzieller Mittel außerdem wichtig, den passenden Zeitpunkt für eine Beschaffung und Einführung in die Polizei zu wählen. Wichtig sei hier, nicht zu früh einzusteigen, da sonst das Risiko besteht, dass eine Technologie unausgereift oder bald wieder veraltet ist, gleichzeitig darf man auch nicht zu spät einzusteigen, da man sonst Gefahr laufe, den Anschluss zu verpassen (ebd., 33:16). Besonders hinderlich für die Aktualität der verwendeten Technologien sind laut dem wissenschaftlichen Leiter des Cybersicherheitsunternehmens lange und komplexe Vergabeverfahren, weshalb er diesbezügliche Reformen fordert (E6 2024, 44:36).

7.1.4. Cybersicherheit

Aufgrund ihrer Aufgabenstellung und Arbeit mit sensiblen Daten ist die Cybersicherheit bei der Polizei wie auch bei anderen Behörden und Organisationen mit Sicherheitsaufgaben (BOS) von essenzieller Bedeutung. Die Folgen eines Cyberangriffs auf die Polizei wurden erst jüngst in den Niederlanden sichtbar, wo (mutmaßlich durch einen anderen Staat) die persönlichen Daten von rund 65.000 Polizeibeamten erbeutet wurden (Tagesschau 2024b).

Einen Orientierungsansatz für die notwendige Cybersicherheit bieten die Richtlinien des Bundesamtes für Sicherheit in der Informationstechnik (BSI). Diese beinhalten unter anderem Maßnahmen wie Verschlüsselung, Datenauthentifizierung sowie Anforderungen an die Interoperabilität der verwendeten Systeme (Hellenthal & Wellershoff 2022). Im Falle von KI ergeben sich bedingt durch spezifische Angriffsarten wie Adversarial-Angriffe und Data Poisioning eigene Anforderungen an die Cybersicherheit (BSI 2021, S. 5). Spezifische Gegenmaßnahmen werden derzeit allerdings noch vom BSI erforscht (ebd., S. 6). Auch bei Cloud-Lösungen für den öffentlichen Sektor ergeben sich gesonderte Anforderungen an die Cybersicherheit (Müller & Köhl 2019, S. 23ff). Entsprechend betont der KI-Wissenschaftler die Notwen-

digkeit, möglichst von Anfang an und über den gesamten Lebenszyklus alles „by-Design“ zu konzipieren, was neben Cybersicherheit auch Datenschutz und -ethik miteinschließt (E4 2024, 47:39). Weiterhin sind die bereits im Kontext der Datenräume genannten klaren Rechte-Rollen-Konzepte eine zentrale Komponente für Cybersicherheit (ebd., 49:25). Abschließend sollte der Dienstherr auch dafür sorgen, dass keine „Schatten-IT“, also für die dienstliche Arbeit nicht zugelassene Systeme, verwendet werden, da diese ein erhebliches Cybersicherheitsrisiko bergen (Hellenthal & Wellershoff 2022).

7.2. Rechtlicher Rahmen und Grenzen

Polizeiliche Maßnahmen, insbesondere dann, wenn diese Eingriffe in Grundrechte beinhalten, müssen auf Grundlage von Gesetzen vorgenommen werden. Dieser Abschnitt widmet sich deshalb den wesentlichen Rechtsquellen, welche den Rahmen für die Einführung und den Einsatz moderner Technologien und KI in der Polizei bilden und diesem Grenzen setzen. Aufgrund der Vielzahl an verschiedenen Rechtsgrundlagen (unter anderem, da jedes der 16 Bundesländer ein eigenes Polizeigesetz hat) ist der folgende Abschnitt möglichst allgemein gehalten. Als Beispiele wird auf die jeweiligen Gesetze des Bundes und des Landes Baden-Württemberg verwiesen.

7.2.1. Grundgesetz und Verfassungen der Bundesländer

Das Verhältnis der Polizei zu den im Grundgesetz garantierten Grund- und Freiheitsrechten ist dichotom: Einerseits ist es Aufgabe der Polizei als Teil der Exekutive diese Freiheits- und Grundrechte der Bürger zu schützen, andererseits ist der Polizei im Rahmen ihres Handelns erlaubt, bestimmte Freiheits- und Grundrechte einzuschränken. Hier spiegelt sich das zuvor bereits erwähnte Spannungsverhältnis zwischen Freiheit und Sicherheit wider (Mann 2014, S. 105ff).

Welche Grundrechte bei präventiven polizeilichen Maßnahmen genau betroffen sind, ergibt sich aus den jeweiligen Polizeigesetzen von Bund und Ländern. Beispielhaft sei an dieser Stelle auf § 4 PolG Baden-Württemberg verwiesen, welches die Grundrechte auf Leben und körperliche Unversehrtheit (Art. 2 Abs. 2 Satz 1 GG), auf Freiheit der Person (Art. 2 Abs. 2 Satz 2 GG), auf Versammlungsfreiheit (Art. 8, Abs. 1 GG), das Brief-, Post- und Fernmeldegeheimnis (Art. 10 GG), auf Freizügigkeit (Art. 11 GG), die Unverletzlichkeit der Wohnung (Art. 13 GG) sowie auf Eigentum (Art. 14 GG) nennt, die im Rahmen polizeilicher Maßnahmen auf Grundlage des PolG eingeschränkt werden können. Vor dem Hintergrund dieser Arbeit ist als weiteres betroffenes Grundrecht erneut das Grundrecht auf informationelle Selbstbestimmung hervorzuheben, welches sich als allgemeines Persönlichkeitsrecht aus Art. 2 Abs. 1 GG in Verbindung mit Art. 1 Abs. 1 GG ergibt. Gleichzeitig gibt es aber auch Grundrechte, welche die Polizei zwingend zu achten

hat, allen voran der Schutz der Menschenwürde nach Art. 1 Abs. 1 GG (Metzner 2017). Ein weiteres Grundrecht, welches im Zusammenhang mit dem Einsatz von KI besonders hervorzuheben ist, ist das Diskriminierungsverbot nach Art. 3 GG. Speziell für die Polizei besagt dieses Verbot, dass polizeiliche Maßnahmen nicht an bestimmte persönliche Merkmale der Adressaten geknüpft werden dürfen, weshalb es laut dem Professor für Öffentliches Recht wichtig ist, die rechtlichen Vorgaben auch technisch umzusetzen (E1 2024, 26:20).

Neben dem Grundgesetz enthalten auch die Verfassungen der Bundesländer eigene Grundrechte. Da allerdings der Grundsatz „Bundesrecht bricht Landesrecht" (Art. 31 GG) gilt, hat es für den Bürger keine negativen Auswirkungen, wenn in den Landesverfassungen bestimmte Grundrechte nicht oder nicht im gleichen Ausmaß geregelt sind wie im Grundgesetz (Geuther & Metzner 2017).

7.2.2. Polizeigesetze

Sofern in den Polizeigesetzen eine in Grundrechte eingreifende Maßnahme geregelt wird, muss diese sowohl verhältnismäßig als auch bestimmt sein. In diesem Sinne muss der genaue Einsatzbereich für eine Maßnahme genannt sein, in dem die Maßnahme vorgenommen wird, sowie die Eingriffsschwelle anhand des Kriminalitätsbereiches, gegen die sich eine Maßnahme richtet (E1 2024, 23:09). Umso invasiver ein Grundrechtseingriff ist, desto höher muss hier die Eingriffsschwelle liegen. Des Weiteren betont der Professor für Öffentliches Recht, dass auch die Technologien, welche eingesetzt werden sollen, im Gesetz klar benannt sein müssen (ebd., 35:40).

In der Praxis ergaben sich hierbei in der jüngeren Vergangenheit mehrfach Probleme, da die zugrundeliegenden Gesetzesgrundlagen unzureichend ausgearbeitet waren und das BVerfG hier nachschärfen musste (ebd., 23:57). Im Rahmen dieser Arbeit wurden in Abschnitt 6.1.2. mit dem jüngsten Urteil zur Datenerhebung und -speicherung im BKA-Gesetz und dem Urteil zur automatisierten Massendatenauswertung von 2023 bereits Beispiele genannt. Der Jurist der NGO für Grund- und Menschenrechte weist des Weiteren darauf hin, dass oftmals auch auf alte und dementsprechend inhaltsfremde Rechtsgrundlagen wie die Rasterfahndung zurückgegriffen wird, um biometrische Abgleiche bei Videoaufnahmen zu rechtfertigen (E7 2024, 40:55). Ein weiteres großes Problem ist außerdem, dass bei Praxistests für grundrechtsinvasive Technologien häufig auf eine eigene Rechtsgrundlage verzichtet wird (ebd., 43:44). Anfang 2024 geriet deswegen die bayrische Polizei in die Kritik, da ihr die nötigen Rechtsgrundlagen für den Testeinsatz ihrer Recherche-Analyse-Software von Palantir fehlten (Kurz 2024b). Entsprechend sollte es auch Rechtsgrundlagen für Praxistests geben, um festzulegen, welche Akteure bei Tests neuer Technologien einzu-

beziehen sind, wie die Kontrolle erfolgt und welche Anforderungen an Testdaten zu stellen sind (E7 2024, 01:01:04).

Abseits unzureichender Rechtsgrundlagen für den Test und Einsatz besteht außerdem die Herausforderung, bestehende Rechtsgrundlagen an den technischen Fortschritt lernfähiger Systeme anzupassen. Eine Antwort hierauf kann im Ansatz eines lernfähigen Polizeirechts bestehen, welches vor dem Hintergrund der technischen Entwicklungen eine regelmäßige Evaluation und Nachbesserung der Polizeigesetze vorsieht (Golla 2020, S. 154).

7.2.3. Verordnung über künstliche Intelligenz (KI-Verordnung)

Einzelne Regelungen der KI-Verordnung wurden bereits im Rahmen der Use-Cases thematisiert. An dieser Stelle werden Regelungen der Verordnung vorgestellt, die speziell den Einsatz von Hochrisiko-KI-Anwendungen durch Polizeibehörden betreffen.

Neben der retrograden biometrischen Identifizierung listet Abs. 6 von Anhang III der KI-Verordnung eine Reihe weiterer KI-Systeme zum Zweck der Strafverfolgung auf, welche explizit als Hochrisikosysteme eingestuft werden. Hierzu gehören im Detail KI-Systeme als Lügendetektoren, zur Bewertung der Verlässlichkeit von Beweismitteln, zum Profiling bei Ermittlungen zu begangenen Straftaten sowie zum personenbezogenen Predictive Policing, wobei letzteres nochmals mit zusätzlichen Regelungen zur verwendeten Datenbasis verbunden ist, um nicht als verbotene KI nach Art. 5 KI-VO eingestuft zu werden. Die Einstufung als Hochrisiko-KI-System ist für die Polizei als Betreiber mit einer Reihe an Pflichten zum Daten- und Risikomanagement verbunden, um einen ordnungsgemäßen Einsatz sicherzustellen. Hierzu gehören unter anderem eine Datenschutz- und Grundrechte-Folgenabschätzung sowie die explizite Genehmigung seitens der zuständigen Behörden für den Einsatz von KI-Systemen zur biometrischen Identifizierung (Baum et al. 2024, S. 149-153).

Die KI-Verordnung selbst ist keine Ermächtigungsgrundlage für den Einsatz bestimmter KI-Systeme, sondern gibt nur die Rahmenbedingungen für nationale Gesetze zum KI-Einsatz vor. Diesbezüglich verweisen der KI-Wissenschaftler und die polizeiliche Führungskraft darauf, dass die weitere Regulierung in Zukunft vor allem von Gerichtsurteilen zum Risikostatus bestimmter KI-Systeme abhängen wird und es zu entsprechenden Nachschärfungen bei der Verordnung kommen muss (E4 2024, 36:11; E10 2024, 34:22). Laut der polizeilichen Führungskraft ist momentan eine Arbeitsgruppe der Polizeien von Bund und Ländern damit beschäftigt, Themen im Bereich der KI-Verordnung zu erfassen und damit verbundene Erwägungsgründe einzuordnen (E10 2024, 20:40).

Nachdem die KI-Verordnung zum 1. August 2024 in Kraft trat, befindet diese sich momentan noch am Beginn ihrer Umsetzung innerhalb der EU-Mitgliedsstaaten. Diese müssen innerhalb von 12 Monaten nach Inkrafttreten der Verordnung jeweils mindestens eine Marktüberwachungsbehörde und eine notifizierende Behörde für die nationale KI-Aufsicht ernennen (Martini & Botta 2024, S. 13f). Für Hochrisikosysteme aus dem Bereich der Strafverfolgung werden nach Art. 74 Abs. 8 KI-VO die Datenschutzaufsichtsbehörden mit der Marktaufsicht betraut. Weiterhin übernehmen diese nach Art. 43 Abs.1 KI-VO auch die Funktion der notifizierten Stelle zur Konformitätsbewertung. Abseits der Kontrollfunktion soll zudem Innovationsförderung für KI-Systeme betrieben werden, weshalb binnen 24 Monaten nach Inkrafttreten der Verordnung jeder Mitgliedsstaat über mindestens ein KI-Reallabor verfügen muss (ebd., S. 14). Diese Reallabore sind insbesondere für polizeiliche Anwendungen von großer Bedeutung, da diese nach Art. 59 KI-VO bei Entwicklungen im öffentlichen Interesse personenbezogene Daten weiterverarbeiten dürfen.

7.2.4. Rechtliche Regelungen zum polizeilichen Datenschutz

Die europarechtlichen Rahmenbedingungen für den polizeilichen Datenschutz ergeben sich aus der EU-Richtlinie 2016/680[12] (kurz JI-Richtlinie), welche in Ergänzung zur Datenschutzgrundverordnung (DSGVO) die Verarbeitung personenbezogener Daten durch die Polizei und Justiz regelt. Letztere schließt in Art. 2 Abs. 2d) DSGVO eine Anwendung für die Zwecke der Verbrechensbekämpfung und Strafverfolgung aus. Je nach Umstand kann allerdings auch die DSGVO unmittelbar für die Polizei gelten, beispielsweise bei der Amts- oder Vollzugshilfe und der Abwehr von Gefahren, welche sich nicht aus dem Straf- oder Ordnungswidrigkeitenrecht ergeben (Arzt 2021, S. 44). Zwischen der JI-Richtlinie und der DSGVO bestehen hohe inhaltliche Gemeinsamkeiten, jedoch sind die datenschutzrechtlichen Standards in der JI-Richtlinie nicht so hoch wie die der DSGVO (ebd., S. 44).

In Deutschland wurde die JI-Richtlinie vor allem im Rahmen des dritten Teils des Bundesdatenschutzgesetzes (BDSG) von 2017 umgesetzt, welches für die Polizeibehörden des Bundes gilt, während für die Landespolizeibehörden in erster Linie die Datenschutzgesetze ihrer jeweiligen Länder gelten (WD 2021, S. 3). Des Weiteren finden sich spezialgesetzliche Regelungen zur Erhebung, Verarbeitung und Nutzung personenbezogener Daten in den Polizeigesetzen von Bund und Ländern und der StPO (ebd., S. 3f). In Rechtlicher Hinsicht muss die Erhebung, Verarbeitung und Speicherung

[12] Offizielle Bezeichnung: Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates.

personenbezogener Daten durch die Polizei rechtlich klar geregelt, zweckgebunden und verhältnismäßig sein, da dies einen Eingriff in das bereits zuvor erwähnte Grundrecht auf informationelle Selbstbestimmung darstellt (Borell & Schindler 2019, S. 394).

Das Thema Datenschutz wird im folgenden Abschnitt zusammen mit der Datenethik vertiefend behandelt.

7.3. Datenschutz und Datenethik

7.3.1. Anforderungen

Die Grundsätze für die polizeiliche Verarbeitung personenbezogener Daten sind in § 47 BDSG geregelt und entsprechen mit Rechtmäßigkeit, Zweckbindung, Datenminimierung, Richtigkeit, Integrität und Vertraulichkeit jenen der DSGVO. Der Grundsatz der Rechtmäßigkeit wurde bereits im vorherigen Abschnitt vor dem Hintergrund der bestehenden Rechtsgrundlagen polizeilicher Arbeit beleuchtet. Mit Blick auf das Thema dieser Arbeit und einer häufigen Betonung in den Interviews wird im Folgenden der Fokus auf den Grundsatz der Zweckbindung gelegt.

Im Rahmen automatisierter Datenerhebung, -verarbeitung und -speicherung hat der Zweckbindungsgrundsatz als Anforderung eine hervorgehobene Rolle, da sich durch die neuen technischen Möglichkeiten zur Verknüpfung und Zusammenführung verschiedener Datenbestände wiederum negative und diskriminierende Folgen für Betroffene ergeben können. Die Notwendigkeit eines angemessenen Datenschutzes ergibt sich ebenfalls aus der zuvor erläuterten Black-Box-Problematik, da bei einer automatisierten Datenverarbeitung nicht von vornherein ersichtlich ist, wie KI-Ergebnisse zustande kommen (E8 2024, 41:17). Laut dem BVerfG dürfen personenbezogene Daten deshalb von der Polizei grundsätzlich nur zu dem Zweck verarbeitet werden, zu dem sie ursprünglich erhoben wurden (Bundesbeauftragte für den Datenschutz und Informationsfreiheit (BfDI) 2021, S. 2). Sollen die Daten nun zu einem anderen als dem ursprünglichen Zweck verarbeitet werden, bedarf es wiederum eigener gesetzlicher und verfassungskonformer Grundlagen (ebd., S. 2). Konkretisiert wurde dies mittels des Grundsatzes der hypothetischen Datenneuerhebung. Diese besagt im Wesentlichen, dass im Falle einer Zweckänderung Polizeibehörden Daten weiterverwenden dürfen, wenn der neue Zweck angesichts vergleichbarer Straftaten oder Gefahren eine ähnliche Datenerhebung rechtfertigen würde (E8 2024, 53:19). Aufgrund der Komplexität des Themas soll die hypothetische Datenneuerhebung hier nicht weiter vertieft werden. Abschließend sei nur darauf verwiesen, dass das Datenhaus von P20 den Versuch beinhaltet, die hypothetische Datenneuerhebung technisch umzusetzen (Gadorosi & Matthey 2023, S. 1420).

Ergänzend zu den gesetzlich festgelegten Regelungen des Datenschutzes gibt es den Bereich der Datenethik. Dieser beinhaltet Normen und Werte zum korrekten Umgang mit Daten, welche wiederum in die Gesetzgebung einfließen (E4 2024, 01:30:55). Speziell für das hier behandelte Thema der polizeilichen Datenverarbeitung und KI sind die ethischen Normen der Fairness und Gleichbehandlung hervorzuheben. In der Praxis betrifft dies die Zusammenstellung fairer Datensätze, faire Designs der Algorithmen und Fairness in Bezug auf die Ergebnisse und die Implementierung von KI-Systemen, um spätere Bias zu vermeiden (Braun Binder et al. 2021, S. 68). Fairness sollte dementsprechend eine zentrale Rolle bei der Bewertung besonders risikobehafteter KI-Anwendungen wie biometrische Identifizierung spielen (Brandner & Hirsbrunner 2023). Neben der Fairness betrifft Datenethik auch die Frage, wie präzise Entscheidungen von KI-Systemen sein müssen, um diese einzusetzen und wie man mit fehlerhaften Ergebnissen umgehen sollte (beispielsweise beim Predictive Policing) (Deutscher Ethikrat 2023, S. 323). Die bereits in Abbildung 2 auf Seite 34 gezeigte Kritikalitätspyramide kann hierbei für eine datenethische Bewertung von KI-Anwendungen für den Polizeieinsatz genutzt werden (von Lucke 2020, S. 121). Der KI-Wissenschaftler äußert sich auf Nachfrage jedoch dahingehend skeptisch, dass freiwillige datenethische Richtlinien – verglichen mit den bestehenden rechtlichen Vorgaben zum polizeilichen Einsatz bestimmter Technologien – in der Praxis keine ernstzunehmende Rolle spielen dürften (E4 2024, 01:34:14).

7.3.2. Verhinderung von Missbrauch

Um eine missbräuchliche Verwendung personenbezogener Daten zu verhindern, bedarf es einer entsprechenden praktischen Umsetzung der datenschutzrechtlichen Vorgaben und einer aktiven Datenschutzaufsicht.

Datenbestände sollten entsprechend ihres Zwecks gekennzeichnet und physikalisch und logisch getrennt voneinander gespeichert werden, um mögliche Diskriminierung und ungerechtfertigte polizeiliche Maßnahmen durch die Zusammenführung verschiedener Datenbestände einzuschränken (BfDI 2021, S. 4, 6; E7 2024, 9:50). Auch müssen die jeweiligen Recherchemöglichkeiten beim Datenabgleich technisch ihrem Zweck entsprechend eingeschränkt sein. So darf es beispielsweise nicht möglich sein, dass Daten aus dem Bereich der Strafverfolgung -falls eine klare Rechtsgrundlage vorliegt- mit Daten aus dem Bereich der Gefahrenabwehr zusammengeführt und angeglichen werden (BfDI 2021, S. 5).

Wie bereits im Zusammenhang mit Cybersicherheit erwähnt, sollten KI-Systeme von Anfang an „by-Design" konzipiert werden, was in § 71 Abs. 1 BDSG von den Polizeibehörden als Verantwortliche gefordert wird. Hierbei ist eine interdisziplinäre Herangehensweise notwendig, sodass die Polizei-

behörden bereits bei der Ausschreibung klare Vorgaben zur datenschutzkonformen Technikgestaltung machen können (Borell & Schindler 2019, S. 398f). Der Ansatz von „Datenschutz-by-design" baut darauf auf, dass KI-Systeme von Anfang und im Sinne einer Datenminimierung für ihre Funktion möglichst wenige bis keine personenbezogene Daten benötigen. Auch der Jurist der NGO für Grund- und Menschenrechte betont die Notwendigkeit, personenbezogene Daten bei der Erhebung und Verarbeitung technisch auf ein Mindestmaß zu reduzieren (E7 2024, 9:35). Ergänzend hierzu sieht der Professor für Öffentliches Recht einen praktischen Vorteil in einer sparsamen Datenerhebung, indem durch reduzierte Datenmengen das allgemeine Big-Data-Management erleichtert wird (E1 2024, 6:47). Bei der Anforderung zur Datenminimierung ergibt sich jedoch ein Spannungsverhältnis zur technischen Anforderung von KI-Systemen, für qualitativ hochwertige Ergebnisse über möglichst viele Daten zu verfügen. Um die gebotene Datenminimierung zu gewährleisten, empfiehlt die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) (2019, S. 17) vor und während des Einsatzes genau darauf zu achten, welche personenbezogenen Daten für den Output des KI-Systems zwingend erforderlich sind. Falls personenbezogene Daten von vornherein irrelevant sind oder dies im Laufe des Betriebs werden, sollten diese entfernt und das KI-System mit entsprechend reduzierten Trainingsdaten erneut trainiert werden (ebd., S. 17). Im Hinblick auf den Output gilt außerdem, dass nur diejenigen personenbezogenen Daten verarbeitet werden sollen, welche zwingend benötigt werden (ebd., S. 17). Zudem gilt zu prüfen, inwieweit es Möglichkeiten zur Anonymisierung und Pseudonymisierung gibt, ohne dass dies den vorgesehen Zweck eines KI-Systems beeinträchtigt (ebd., S. 17). Inwieweit dies für polizeiliche KI-Anwendungen der Fall ist, gilt es jeweils im Einzelfall zu prüfen. Das Beispiel der algorithmenbasierten Videoüberwachung in Mannheim zeigt, dass diesbezüglich Möglichkeiten bestehen. Ergänzend ließe sich eine Datenminimierung durch datenschutzkonforme Voreinstellungen erreichen, sodass nur für den jeweiligen Verarbeitungszweck notwendige Daten verarbeitet werden (Borell & Schindler 2019, S. 400). Voreinstellungen können des Weiteren zur automatischen oder fristgerechten Lösung von Daten genutzt werden (ebd., S. 399f).

„Datenschutz-by-Design" beinhaltet weiterhin Anforderungen an die Datensicherheit. Hierbei ergeben sich große Schnittmengen mit der bereits behandelten Cybersicherheit, da es vor allem darum geht, dass die Daten keinen unbefugten Personen gegenüber offenbart werden, verloren gehen oder unautorisiert verändert werden (ebd., S. 400). Um die Erhebung, Verarbeitung, Abfrage und Weitergabe von Daten nachzuvollziehen, sind diese einschließlich Begründung, Datum und Uhrzeit und -nach Möglichkeit- der Identität des Verantwortlichen technisch zu protokollieren (ebd., S. 401). Wie wichtig die Protokollierung in der Praxis ist, zeigen frühere Beispiele missbräuchlicher Identitätsabfragen durch Polizeibeamte (Golla 2019). Neben

technischen Sicherheitsmaßnahmen beim Zugriff auf Daten gilt es auch, zweckgebunden den Austausch und die Weitergabe von Daten zu regeln (E8 2024, 19:12; E9 2024, 11:19).

Eine zentrale organisatorische Rolle zur Gewährleistung des Datenschutzes nimmt der jeweilige polizeiinterne Datenschutzbeauftragte ein. Dessen Funktion ist gesetzlich in den jeweiligen Datenschutz- und Polizeigesetzen geregelt.[13] Das grundsätzliche Aufgabenportfolio umfasst dabei die Überwachung der Einhaltung datenschutzrechtlicher Vorschriften sowie der Unterrichtung und Beratung der mit der Datenverarbeitung betrauten Polizeibeamten (Borell & Schindler 2019, S. 395). Aus diesem Grund sollte der jeweilige Datenschutzbeauftragte möglichst von Anfang an in alle relevanten Planungsprozesse mit einbezogen und dessen Einschätzungen berücksichtigt werden (ebd., S. 395f). Neben den eigenen Datenschutzbeauftragten müssen die Polizeibehörden außerdem mit den jeweils für sie zuständigen Bundes- oder Landesdatenschutzbeauftragten kooperieren, welche ebenfalls eine Kontrollfunktion ausüben. Wichtig ist hierbei, dass die Polizeibehörden wie gefordert ein ordnungsgemäßes und aktuelles Verzeichnis über die Verarbeitung personenbezogener Daten führen (ebd., S. 397). Im Falle von ernsthaften Verstößen können die zuständen Datenschutzbeauftragten Gegenmaßnahmen gegen Verantwortliche anordnen. Hierbei kommt es allerdings auch auf die Stellung und Ausstattung der jeweiligen Datenschutzbeauftragten an und inwieweit diese ihre Befugnisse wirklich nutzen (Arzt 2021, S. 50f). Im Falle von Datenschutzverletzungen ist zudem wichtig, dass die verantwortliche Polizeibehörden diese unverzüglich an die zuständige Datenschutzaufsicht meldet und, sofern möglich, auch die Betroffenen benachrichtigt (Borell & Schindler 2019, S. 402ff). Hierfür muss auch die Möglichkeit bestehen, dass innerhalb einer Polizeibehörde Datenschutzverstöße vertraulich gemeldet werden können (ebd., S. 403). In beiden Fällen sorgt dies für einen transparenteren Umgang der Polizeibehörden mit Datenschutzverletzungen.

Mit Blick auf besonders grundrechtsinvasive Technologien wie biometrische Fernidentifizierung ist abschließend die Datenschutz-Folgenabschätzung als notwendiger Beurteilungsprozess hervorzuheben. Auch hier müssen die polizeilichen Datenschutzbeauftragten von Anfang an beteiligt werden. Grundlage für die Datenschutz-Folgeabschätzung sind § 67 BDSG und vergleichbare Normen in den Datenschutz- und Polizeigesetzen der Länder.[14] Einerseits wird im Rahmen der Folgenabschätzung der geplante Verarbeitungsvorgang sowie dessen Zweck beschrieben. Andererseits gilt es die Notwendigkeit und Verhältnismäßigkeit des genannten Zwecks zu bewerten und voraussichtliche Gefahren für die Grundrechte der Betroffenen

[13] Beispielhaft sei hier auf § 7 Abs. 1 BDSG und § 96 PolG Baden-Württemberg verwiesen.
[14] Im Falle Baden-Württembergs § 80 PolG.

zu analysieren. Weiterhin muss im Rahmen der Folgenabschätzung erläutert werden, welche Maßnahmen voraussichtlich ergriffen werden, um diesen Gefahren zu begegnen, beispielsweise mittels eines „Datenschutz-by-Design". Wie bereits im vorherigen Abschnitt thematisiert, sollten hierbei insbesondere auch datenethische Erwägung wie „Fairness" mit einbezogen werden (Brandner & Hirsbrunner 2023). Ergibt die Folgenabschätzung ein besonders hohes Risiko, ohne dass Maßnahmen zur Risikominimierung bestehen, oder beinhaltet die Form der Verarbeitung ein besonders hohes Risiko für die Rechte und Freiheiten der Betroffenen, ist die zuständige Datenschutzaufsichtsbehörde einzuschalten (Borell & Schindler 2019, S. 398). Wird die Datenschutzaufsichtsbehörde konsultiert, kann diese einerseits Empfehlungen für zusätzliche Maßnahmen für einen grundrechtskonformen Einsatz geben, andererseits kann sie auch von den ihr rechtlich zugestandenen Untersuchungs- und Abhilfebefugnissen Gebrauch machen (ebd., S. 398). Zudem verweist der Jurist der NGO für Grund- und Menschenrechte auf die Möglichkeit gerichtlicher Klagen als sehr effektives Mittel, um gegen Rechtsverstöße und besonders tiefe Grundrechtseingriffe vorzugehen (E7 2024, 45:52).

7.4. Politische und gesellschaftliche Herausforderungen

7.4.1. Finanzierung

In den Interviews äußert sich der überwiegende Teil der Experten zurückhaltend auf die Frage, wie sie die aktuelle Finanzierung der Polizei für den Einsatz moderner Technologien bewerten. Allerdings findet sich ein Grundtenor, dass die Finanzierung für die Digitalisierung und Technologieausstattung der Polizei zu gering beziehungsweise nicht zielgerichtet sei. Als Hauptgrund wird hier der Föderalismus in Deutschland genannt, wodurch je nach Bundesland unterschiedliche Prioritäten und finanzielle Kapazitäten vorliegen (E6 2024, 50:13; E9 2024, 57:11). Diesbezüglich äußert sich die polizeiliche Führungskraft zufrieden mit den Investitionen in seinem eigenen Bundesland und verweist auf ein kürzlich auf Landesebene verabschiedetes Sicherheitspaket (E10 2024, 1:05:09).

Auf die Frage, in welchen Bereichen es einer verstärkten Investition bedarf, werden eine flächendeckende Finanzierung polizeilicher Innovationslabore, Ausbildung, digitale Anwendungen mit einem allgemeinen Nutzwert, die zugrundeliegende IT-Infrastruktur und Datenbereitstellung sowie eine länderübergreifende Kooperation genannt (E2 2024, 52:57; E3 2024, 01:39:18; E5 2024, 53:38; E6 2024, 54:09; E9 2024, 57:24).

7.4.2. Politischer Wille

Auf die Frage, wie sie den politischen Willen in Deutschland bewerten, die notwendigen Schritte hin zur Weiterentwicklung zu einer smarten Polizei zu gehen, äußern sich die Experten sehr unterschiedlich. Sowohl der Professor für Strafrecht als auch der externe Berater des BMI betrachten den politischen Willen als grundsätzlich hoch, wobei Letzterer diesen unter dem allgemeinen politischen Ziel der Digitalisierung einordnet (E8 2024, 01:07:20; E9 2024, 54:52). Einen weiteren Punkt, welchen der externe Berater bezüglich dem politischen Willen betont, ist ein Wunsch nach „Waffengleichheit" gegenüber Kriminellen beim Technologieeinsatz (E9 2024,55:45). Den Wunsch und die Notwendigkeit einer „Waffengleichheit" nennt auch der KI-Wissenschaftler (E4 2024, 01:13:43). Zugleich weist er darauf hin, dass Rechtsgrundlagen für den Einsatz von Technologien nicht als bloße Reaktion auf einzelne Vorfälle wie Terroranschläge, sondern mit Blick auf einen allgemeinen Nutzen geschaffen werden sollten (ebd., 01:17:23). Vor dem Hintergrund des Föderalismus verweist der wissenschaftliche Leiter des Cybersicherheitsunternehmens darauf, dass der politische Wille ähnlich wie die finanziellen Mittel sich von Bundesland zu Bundesland unterscheiden. Mit Blick auf die Innenministerkonferenz nennt er Streitpunkte bei der Finanzierung über den Königsteiner Schlüssel, was Beschlüsse der Konferenz zur gemeinsamen Digitalisierung der Polizei erschwert (E6 2024, 49:47, 50:13).

Im Hinblick auf die politische Unterstützung für konkrete Vorhaben wie das Sicherheitspaket verweisen mehrere Experten neben politischem Druck als Folge von Anschlägen auf das parteipolitische Cleavage zwischen einer stärkeren Betonung von Sicherheit beziehungsweise Freiheitsrechten (E1 2024, 47:25; E2 2024, 50:31; E3 2024, 01:23:35; E7 2024, 53:37). Dass sich hier in der Praxis Überschneidungen ergeben können, zeigt das Beispiel des Sicherheitspaketes der Bundesregierung.[15] So wird ursprünglich im Koalitionsvertrag die Forderung geäußert, biometrische Erkennung im öffentlichen Raum europarechtlich auszuschließen (Bundesregierung 2021, S. 15). Gleichzeitig soll jedoch mit dem Sicherheitspaketes eine Rechtsgrundlage für den Einsatz von biometrischen Systemen zur Online-Fahndung geschaffen werden, was für Kritik sorgt (Vieth-Ditlmann & Sombetzki, 2024a).

7.4.3. Akzeptanz in der Bevölkerung

Ähnlich schwierig wie beim politischen Willen ist es, allgemeingültige Aussagen zur Akzeptanz der Bevölkerung für den Einsatzes smarter Technologien und KI durch die Polizei zu treffen. Der überwiegende Teil der Exper-

[15] Die Freie Demokratische Partei (FDP) verlies nach länger Streitigkeiten Mitte November 2024 frühzeitig die Koalition, welche nun nur noch aus der Sozialdemokratischen Partei Deutschlands (SPD) und Bündnis 90/Die Grünen besteht. In diesem Fall wird die FDP allerdings auf Basis des Koalitionsvertrages mit einbezogen.

ten sieht jedoch eine vergleichsweise hohe Akzeptanz aufseiten der Bevölkerung. Als Grund wird zum einen der allgemeine Wunsch seitens der Bevölkerung genannt, dass die deutschen Polizeibehörden über adäquate Technologien zur effizienten Gefahrenabwehr und Strafverfolgung verfügen sollen, um gegen moderne Kriminalitätsphänomene vorgehen zu können (E3 2024, 01:21:09; E5 2024, 50:40; E6 2024, 47:38). Diese Einschätzung deckt sich mit zwei Studien von Bitkom und PricewaterhouseCoopers (PwC). Laut der Studie von Bitkom wünschen sich 66% der Deutschen einen KI-Einsatz bei der Polizei, während die Studie von PwC ergibt, dass 52% der deutschen Bevölkerung die Ausstattung der Polizei als nicht auftragsadäquat betrachten und 84% eine verstärkte digitale Ausstattung für die Polizei fordern (Bitkom 2024, S. 18; Zink et al. 2022, S. 21, 26). Die konkrete Zustimmung variiert jedoch je nach Technologie, wobei besonders tiefe Grundrechtseingriffe durch die Technologie von einer Mehrheit der Befragten abgelehnt werden (Zink et al. 2022, S. 27). Zum anderen verweisen mehrere Experten vor dem Hintergrund des Anschlags von Solingen und des Sicherheitspaketes auf die Wahrnehmung einer angespannten Sicherheitslage in Deutschland, welche Einfluss auf die Zustimmung haben dürfte (E1 2024, 40:55; E2 2024, 45:08; E8 01:00:12). Mögliche individuelle Faktoren sind laut dem KI-Wissenschaftler das Alter und die persönliche Technologieaffinität, weshalb seiner Ansicht nach in Deutschland eine tendenzielle Skepsis gegenüber KI herrsche (E4 2024, 01:03:16). Weiterhin verweist der Jurist der NGO für Grund- und Menschenrechte auf den Einfluss der eigenen Informiertheit über staatliche Überwachungsmaßnahmen, die wiederum für Ablehnung und Kritik sorgt (E7 2024, 49:28).

Um die Akzeptanz für den polizeilichen Einsatz von KI und smarten Technologien in der Bevölkerung zu festigen und Vertrauen zu schaffen, bedarf es seitens der Polizei an Aufklärungsarbeit und Transparenz zum Technologieeinsatz. Als Beispiel nennt die polizeiliche Führungskraft die Bürgerbeauftragte seines Bundeslandes (E10 2024, 52:53). Während der wissenschaftliche Leiter des Cybersicherheitsunternehmens zwar grundsätzlich eine hohe Akzeptanz innerhalb der breiten Bevölkerung sieht, kritisiert er, dass vor allem polarisierende Ansichten in der öffentlichen Debatte zum Einsatz neuer Technologien präsent sind und so das Vertrauen in die Polizei negativ beeinflussen (E6 2024, 34:44, 35:38, 40:47, 47:38). Auch von Lucke (2020, S. 121f) verweist darauf, dass die Einführung moderner Technologien in der Polizei eher in geschlossenen Fachgremien diskutiert und beschlossen wird und diesbezügliche Debatten meist nur in einer kleinen Fachöffentlichkeit stattfinden. Aus diesem Grund unterstreicht der wissenschaftliche Leiter des Cybersicherheitsunternehmens die Notwendigkeit einer ausführlichen und breiten gesellschaftlichen Debatte, um Aufklärungsarbeit zu betreiben, breite Akzeptanz zu erzeugen und am Ende Ergebnisse zu erzielen, welche von einer Mehrheit der Bevölkerung getragen werden. Als vergleichbares Beispiel nennt er hier die Debatte zur Gleichgeschlechtlichen Ehe (E6 2024,

42:02). Diese Notwendigkeit einer breiten gesellschaftlichen Auseinandersetzung wird auch von weiteren der Experten betont (E5 2024, 44:50; E7 2024, 44:15; E10 2024, 54:20).

7.4.4. Digitale Souveränität

Laut des Kompetenzzentrum „Öffentliche IT" des Fraunhofer-Instituts für Offene Kommunikationssysteme FOKUS ist digitale Souveränität „(...) die Summe aller Fähigkeiten und Möglichkeiten von Individuen und Institutionen, ihre Rolle(n) in der digitalen Welt selbstständig, selbstbestimmt und sicher ausüben zu können" (Goldacker 2017, S. 3). Diese Herausforderung wurde bereits im Kontext der souveränen Cloud-Infrastruktur thematisiert. Abseits hiervon ergeben sich jedoch auch Herausforderungen einer digitalen Souveränität bei konkreten Anwendungen für den Polizeieinsatz. Bespielhaft hierfür steht die große Verbreitung von Recherche-Analyse-Software des US-amerikanischen Herstellers Palantir, da es an vergleichbaren deutschen Herstellern fehlt (Peglow 2024, S. 7f). Neben Problemen des Datenschutzes und der Datensicherheit können hier außerdem mit der Zeit Abhängigkeiten von privaten Anbietern aus dem außereuropäischen Ausland entstehen (Kelber 2024, S. 8; Ruf, 2024). Dem gegenüber besteht der Wunsch seitens der Polizeibehörden und zuständigen Innenministerien, über die leistungsfähigste Technologie zu verfügen, welche allerdings nicht immer von europäischen Herstellern angeboten wird (Teufele 2024; Wagner, 2024).

Der wissenschaftliche Leiter des Cybersicherheitsunternehmens kritisiert im Interview, dass es für deutsche und europäische Unternehmen kaum möglich sei, im Sicherheitsbereich Digitale Souveränität zu erlangen. Als Grund hierfür nennt er die von der EU gesetzten Nachhaltigkeitskriterien, welche Unternehmen daran hindern, das benötigte Risikokapital zu erhalten und sich über Banken oder den Kapitalmarkt zu refinanzieren (E6 2024, 40:10). Hier müssten laut ihm Anpassungen seitens der beteiligten Akteure vorgenommen werden, damit deutsche und europäische Unternehmen technisch aufholen können (ebd., 01:03:35). Als Alternative werden behördliche Eigenentwicklungen diskutiert. Allerdings ist hier fraglich, ob die Behörden über die nötige technische Erfahrung und Kapazitäten verfügen, welche auch eine fortwährende Betreuung und Weiterentwicklung mit einschließen (Dehmel 2024, S. 3). Des Weiteren besteht das Risiko, dass Eigenentwicklungen letztlich mit deutlich höheren Kosten verbunden sind als marktverfügbare Lösungen (ebd., S. 3). Wie wichtig es für Deutschland und Europa im Allgemeinen ist, digitale Souveränität zu erlangen und eigene Standards setzen zu können, unterstreicht der KI-Wissenschaftler mit Verweis auf den aktuellen weltweiten Wettbewerb um KI-Systeme (E4 2024, 01:00:25).

7.5. Polizeiinterne Herausforderungen

7.5.1. Akzeptanz aufseiten der Polizei

Auf die Frage nach der polizeiinternen Akzeptanz für den Einsatz smarter Technologien und KI verweisen mehrere Experten darauf, dass diese ähnlich divers sei wie in der allgemeinen Bevölkerung. Auch hier wurden das Alter und die persönliche Technikaffinität von Polizeibeamten als wesentliche Einflussfaktoren genannt (E3 2024, 01:33:24; E4 2024, 01:09:36; E9 2024, 49:20; E10 2024, 55:36). So seien jüngere und technikaffine Beamte gegenüber dem Einsatz neuer Technologien tendenziell offener eingestellt als ältere Beamte und Beamte ohne bisherige Berührungspunkte mit diesen Technologien und KI. Entsprechend äußern sich diese Beamten skeptisch verbunden mit der Sorge, von KI-Systemen „ersetzt zu werden". Umso wichtiger ist es deshalb, Aufklärungsarbeit zum tatsächlichen Potenzial von KI und dessen Einsatzmöglichkeiten zu betreiben (E5 2024, 1:33:20; 51:15; E9 2024, 50:08). Weiterhin verweisen der KI-Wissenschaftler und die polizeiliche Führungskraft auf die Möglichkeit, polizeiintern die Akzeptanz durch praktische Erfolge beim Technologieeinsatz zu stärken (E4 2024, 01:05:42; E10 2024, 56:05).

7.5.2. Organisationsentwicklung in der Polizei

Die verstärkte Einführung smarter Technologien und insbesondere KI sorgt dafür, dass sich die Polizeibörden in mehreren Punkten als Organisation weiterentwickeln müssen.[16] Allen voran betrifft dies den Umgang mit KI-Anwendungen. Hierzu wird es zum einen nötig sein, dass auch die Polizei technisches Fachpersonal für den Umgang mit KI-Anwendungen anwirbt (E10 2024, 58:05). Hier dürfte es allerdings schwierig werden, im Wettbewerb um Fachpersonal mit dem Privatsektor Schritt zu halten (E3 2024, 01:45:42). Zum anderen muss aber auch Polizeibeamten im Allgemeinen die Fähigkeit zum Umgang mit KI-Systemen vermittelt werden, was nach Art.4 KI-VO von der Polizei als Betreiber von KI-Systemen explizit gefordert wird. Eine solche KI-Kompetenz beinhaltet dabei idealerweise ein grundlegendes Verständnis für die Funktionsweise von KI und mögliche Bias, die Fähigkeit, Empfehlungen und Ergebnisse von KI-Systemen kritisch zu beurteilen und Grundkenntnisse zu den rechtlichen Grundlagen und Datenschutz beim KI-Einsatz (Wolf-Engels 2024, S. 6f). Laut dem KI-Wissenschaftler sei hierbei vor allem wichtig, den Ausbau der KI-Fähigkeiten innerhalb der Polizei inklusiv zu gestalten und mit einer Stärkung der allgemeinen Akzeptanz und des Verständnisses für KI zu verbinden, um mögliche Widerstände zu reduzieren (E4 2024 01:07:33). Des Weiteren empfiehlt der externe Berater des BMI, möglichst früh anzusetzen und KI-Kompetenz Bestandteil der polizeilichen

[16] Einen ausführlichen Überblick über allgemeine Herausforderungen bei polizeilichen IT-Projekten inklusive Lösungsansätzen bietet Jürgen Schäberle (2023).

Grundausbildung zu machen (E9 2024, 52:36). Außerdem verweist die polizeiliche Führungskraft auf die Notwendigkeit einer stärkeren Verbindung zwischen der analogen und digitalen Polizeiarbeit in der Aus- und Fortbildung und im täglichen Polizeidienst (E10 2024, 58:48). Die Vermittlung und Stärkung von KI-Fähigkeiten ist dabei eng verbunden mit dem Bedarf einer allgemein stärkeren Digitalisierung in der Polizei (E4 2024, 01:06:57; E10 2024, 58:23). Abseits der Vermittlung von KI-Fähigkeiten verweist der Jurist der NGO für Grund- und Menschenrechte außerdem auf die Notwendigkeit, Polizeibeamte für die Folgen von Grundrechtseingriffen durch KI zu sensibilisieren und die Ergebnisse des Technologieeinsatzes stärker evidenzbasiert auszuwerten (E7 2024, 50:34).

Auch die Polizei sieht sich mit der Herausforderung des demographischen Wandels konfrontiert. Hier besteht die Herausforderung, neben der Vermittlung von KI-Fähigkeiten gegenüber älteren Beamten Möglichkeiten zur Automatisierung zu identifizieren und zukünftige Personalengpässe vorzubeugen. Diesbezüglich wird seitens der Experten vereinzelt kritisch angemerkt, dass es aufgrund der Grundrechtsrelevanz bei der polizeilichen Arbeit weniger Möglichkeiten zur Verfahrensautomatisierung gibt als in anderen Verwaltungsbereichen (E1 2024, 46:30). Zudem bedeutet Verfahrensautomatisierung nicht, dass Personal eingespart werden kann, sondern dass in Zukunft ebenso viel Personal wie zuvor benötigt wird und neue Personalbedarfe im Zusammenhang mit der Digitalisierung entstehen (E3 2024, 01:35:43). Gleichzeitig kann KI jedoch dabei helfen, bestimmte, insbesondere repetitive Verwaltungsaufgaben einfacher und schneller zu erledigen, sodass das verfügbare Personal gezielter bei schwierigen Aufgaben eingesetzt werden kann, welche eine menschliche Beteiligung notwendigerweise erfordern (E9 2024, 53:38).

Zuletzt betrifft die polizeiliche Organisationsentwicklung auch die Notwendigkeit einer verstärkten technischen und fachlichen Kooperation zwischen den verschiedenen Polizeibehörden wie beispielsweise im Rahmen von P20. Technologien sollten künftig gemeinsam entwickelt und beschafft werden, damit diese mittel- bis langfristig interoperabel sind und Mehrarbeit verhindert wird (E3 2024, 01:28:47; E9 2024, 51:48). Diesbezüglich verweist der Vertriebsleiter und ehemalige Polizist auf das Problem, dass einzelne Landespolizeien versuchen, sich durch besondere Leuchtturmprojekte hervorzutun, ohne dass diese Projekte einen allgemeinen Mehrwert haben (E3 2024, 01:29:27). Entsprechend fordert er, mehr in Projekte zu investieren, welche in der Breite zu Erleichterungen im Polizeialltag führen (ders., 01:30:12). Des Weiteren sollte die Schaffung vereinzelter „Insellösungen" vor Ort vermieden werden. Diese versprechen zwar eine schnelle Lösung spezieller Bedarfe vor Ort, gleichzeitig sorgen diese aber für eine ganze Reihe an Problemen, welche unter anderem auch die Interoperabilität betreffen (Schäberle 2023, S.1474f).

8. Zielbild und SWOT-Analyse

Zur Bewertung der neuen Einsatzmöglichkeiten aus Kapitel sechs hinsichtlich vorhandener Stärken, Schwächen und sich daraus ergebenden Chancen und Risiken wird in diesem Kapitel eine SWOT-Analyse (Englisch für *Strengths* (Stärken)*, Weaknesses* (Schwächen)*, Opportunities* (Chancen) *und Threaths* (Risiken)) vorgenommen. Bevor die Analyse vorgenommen wird, soll ein Zielbild formuliert werden, welches den Idealzustand für die Einführung und den Einsatz smarter Technologien durch die Polizei beschreibt und als Bezugspunkt für die Analyse dient.

8.1. Zielbild für den Polizeieinsatz

Das Zielbild soll das einer modernen, gut ausgestatteten und finanzierten und gleichzeitig für die Risiken und negativen Folgen des Technologieeinsatzes sensibilisierten Polizei sein. Der Einsatz von KI-Systemen und smarten Technologien erfolgt im Rahmen klar definierter Anwendungsfälle, welche einen messbaren Mehrwert bei der Gefahrenabwehr und Strafverfolgung bieten. Dadurch wird die Polizei in die Lage versetzt, in Zukunft Kriminellen technisch auf Augenhöhe zu begegnen.

Neben gesetzlichen Vorgaben sollen auch ethische Aspekte in die Folgenabschätzung mit einfließen. Weiterhin sollen Polizeibeamte über die gebotene KI-Kompetenz verfügen, welche neben dem praktischen Umgang mit KI-Systemen auch die Fähigkeit zur kritischen Reflexion des Einsatzes und dessen Folgen beinhaltet. Um die smarten Technologien und KI-Systeme optimal einsetzen zu können, soll die Polizei in Zukunft auf eine souveräne IT-Infrastruktur zugreifen können. Weiterhin soll auch hinsichtlich der Technologien für den Polizeieinsatz eine digitale Souveränität bestehen, sodass nicht mehr der Bedarf zur Beschaffung bei umstrittenen Herstellern aus dem außereuropäischen Ausland besteht. Vonseiten des Gesetzgebers werden Rechtsgrundlagen geschaffen, welche sowohl die Möglichkeiten als auch Grenzen des Einsatzes klar aufzeigen. Handelt es sich hierbei um besonders umstrittene Technologien und Anwendungsfälle, setzt dies eine ausführliche öffentlichen Debatte voraus, welche für Transparenz, Legitimität und eine umfassende Reflexion vor dem Einsatz sorgt.

Im Ergebnis soll der Einsatz von KI und smarten Technologien eine breite Akzeptanz in der Bevölkerung und innerhalb der Polizei finden, um eine effektive, verantwortungsvolle und zukunftsorientierte Polizeiarbeit zu gewährleisten und das Vertrauen in die Polizei und den Staat zu stärken.

8.2. SWOT-Analyse der identifizierten Einsatzmöglichkeiten

Im Rahmen dieses Zielbildes wird nun eine SWOT-Analyse der identifizierten Einsatzmöglichkeiten vorgenommen. Als Instrument dient die SWOT-Analyse dazu, wichtige Entwicklungen und Faktoren für die Erreichung eines Zieles mit den Kategorien der internen Stärken und Schwächen sowie externen Chancen und Bedrohungen zu erfassen (Wollny & Paul 2015, S. 189). Abbildung 3 beinhaltet eine erste Übersicht der zentralen Punkte, welche im Folgenden vertieft werden.

Stärken	**Schwächen**
• Leistungsfähigere Datenaufbereitung und -verarbeitung • Komplementierung bestehender smarter Systeme • Nachträgliche Rekonstruktion von Tatorten • vereinfachte und realitätsnahe Kompetenzvermittlung • Zeitersparnis • Polizei hat das Potenzial von KI erkannt • Öffentliches Bild einer „Modernen Polizei“	• Mangelhafte Datenqualität • Fehlende IT-Infrastruktur und Vernetzung • Fehlende KI-Fähigkeiten und Fachpersonal • Föderalismus • Finanzierung • Fehlende Rechtsgrundlagen • Fehlende Digitale Souveränität • "Black-Box-KI" • Unklarer Mehrwert
Chancen	**Risiken**
• Effizienterer Ressourceneinsatz • Zeiteffizienz • Bessere Entscheidungsgrundlagen nahezu in Echtzeit • Messbare Verbesserungen bei Gefahrenabwehr und Strafverfolgung • Abfederung des Demographischen Wandels • Steigerung Akzeptanz und Vertrauen durch erfolgreichen Einsatz	• Verlust von Vertrauen und Akzeptanz • Folgenschwere „Automation Bias“ • Breite staatliche Überwachung • Diskriminierung bestimmter Personengruppen • Ungerechtfertigte Grundrechtseinschränkungen • Überregulation • Datensicherheit • Verlust sensiblen Polizeiwissens

Abbildung 3: SWOT-Analyse der identifizierten Einsatzmöglichkeiten

8.2.1. Stärken

Eine wesentliche Stärke von KI-Systemen besteht in der schnelleren Aufbereitung und Verarbeitung von Big Data, wodurch sich Potenziale zur (Teil)automatisierung von Verfahren und Prozessen ergeben. Eine weitere allgemeine Stärke von KI besteht in der Mustererkennung, wodurch sich neue und detailliertere Erkenntnisse gewinnen lassen (E9 2024, 26:23).

Mittels KI lassen sich so bereits vorhandene Technologien wie Drohnen, Roboter, Sensorsysteme, Überwachungskameras und andere CPS komplementieren, indem die Auswertung der mit diesen Technologien gesammelten Daten beschleunigt wird. Die im Einsatz befindlichen Polizeibeamten verfügen so über ein aktuelleres Lagebild. Bereits heute finden sich in der Praxis erste Ansätze bei der Bearbeitung und Übersetzung von Notrufen und dem Alarmrouting auf Basis von aktueller Geodaten (Krameyer 2022; Lasserre 2024). Auch VR wurde bereits erfolgreich dazu genutzt, um Straftaten und Unfälle aufzuklären (Müller 2023). Auch zu Trainings- und Ausbildungszwecken erhält VR zunehmend Einzug bei der deutschen Polizei, beispielsweise seit Ende 2023 in NRW (Holland 2023). Seitens der Experten wird in den Interviews allgemein die Möglichkeit von VR und AR zu einer flexiblen und realitätsnahen Ausbildung genannt, insbesondere für komplexe Einsatzszenarien wie Terroranschläge und Amoklagen. Erste Studien bestätigen hier, dass beim Training in einer VR-Umgebung hinsichtlich Stressempfinden, mentaler Anstrengung und körperlicher Beanspruchung Ergebnisse erzielt werden, welche mit denen eines Realtrainings vergleichbar sind (Kleygrewe, Hutter, Koedijk & Oudejans 2024). Weiterhin ermöglicht die Nutzung von GKI Zeitersparnisse bei der Vorgangsbearbeitung. Während in Deutschland ein möglicher Einsatz noch offen ist, gibt es in den USA bereits erste Tests, mittels KI auf Basis von Bodycam-Aufnahmen automatisierte Einsatzberichte zu generieren (Fuhrmann 2024).

Nach Ansicht der interviewten Experten wurde die Relevanz und der allgemeine Mehrwert von KI seitens der Polizei erkannt. Als Folge werden seitens der Polizeibehörden auch erste Anstrengungen unternommen, um KI besser zu verstehen und neue Einsatzansätze zu identifizieren, beispielsweise in Form des KI-Campus der Polizei (BMI 2024, S. 8). Hier verweist die polizeiliche Führungskraft jedoch darauf, dass man bei der Erforschung der grundsätzlichen Nutzbarkeit von GKI noch ziemlich am Anfang stehe (E10 2024, 17:23). Weiterhin trägt der Einsatz von KI, VR und AR dazu bei, das öffentliche Bild einer „modernen Polizei“ zu stärken, wodurch die Polizei als Arbeitgeber wiederum an Attraktivität gewinnt (E4 2024, 43:27; E6 2024, 56:10).

8.2.2. Schwächen

Abbildung 3 zeigt, dass hinsichtlich des Einsatzes der diskutierten Technologien eine Vielzahl an Schwächen besteht. Ein Großteil hiervon lässt sich unter dem Oberbegriff „Fehlender Grundlagen" zusammenfassen. Technisch mangelt es neben ausreichend strukturierten Daten vor allem an der nötigen IT-Infrastruktur in Form souveräner Cloud-Lösungen und Datenräumen, wie dies zuvor bereits in Abschnitt 6.1. und 7.1. thematisiert wurde. Als weitere Schwäche ist zudem auf eine mangelnde Vernetzung polizeilicher Systeme zu verweisen, welche einen sinnvollen Datenaustausch erschweren (E6 2024, 31:27). Auch Fritz (2020, S.92) nennt die mangelnde Digitalisierung als Schwäche. Eine weitere Schwäche besteht einerseits im Mangel an hierfür benötigten Fachkräften bei der Polizei, deren Gewinnung aufgrund des Konkurrenzdrucks durch den Privatsektor auch langfristig schwierig bleiben dürfte. Andererseits verweist eine Mehrheit der Experten darauf, dass bereits vorhandene KI-Kompetenz bei Polizeibeamten von persönlichen Faktoren wie dem Alter oder eigenen Technologieinteresse abhängt. Dementsprechend schwierig dürfte es sein herauszufinden, wie viele Beamte mit ausreichender KI-Kompetenz bereits zu Verfügung stehen. Zudem besteht die Herausforderung darin, ältere Polizeibeamte mit KI-Systemen vertraut zu machen (E3 2024, 01:33:25).

Der Föderalismus bei der deutschen Polizei kann in zweierlei Weise als Schwäche eingestuft werden: Einerseits mit Blick auf die Finanzierung von teils kostenintensiven KI-Projekten, andererseits mit Blick auf unterschiedliche Schwerpunkte und Präferenzen in einzelnen Bundesländern. Aus den Experteninterviews ergab sich, dass die finanziellen Mittel je nach Bundesland unterschiedlich hoch ausfallen und unterschiedliche Schwerpunkte haben, welche nicht in jedem Fall eine verstärke Digitalisierung betreffen (E5 2024, 52:37; E6 2024, 52:35). Des Weiteren erfordert ein Grundrechtseingriff mittels smarten Technologien und KI, dass in jedem Bundesland und auf Ebene des Bundes hierfür eine eigene Rechtsgrundlage vorliegen muss, was momentan aber nicht überall der Fall ist (E4 2024, 43:44).

Weiterhin ist auf die mangelnde digitale Souveränität bei marktverfügbaren Technologien und Software zusammen mit einer Abhängigkeit von umstrittenen außereuropäischen Anbietern wie Palantir zu nennen. Als Antwort werden häufig Software-Eigenlösungen für die Polizei gefordert. Diese tragen zwar zur digitalen Souveränität bei und bieten die Möglichkeit zur Berücksichtigung individueller Anforderungen, gleichzeitig sind Eigenlösungen meist mit erhöhten Kosten und einem zusätzlichen Fach- und Implementierungsaufwand verbunden (Laude, Reinhard & Bomert 2023, S. 1511f).

Eine weitere Schwäche besteht in der mangelhaften Nachvollziehbarkeit von KI-Ergebnissen im Sinne einer „Black-Box" und damit verbundene Bias und „Halluzinationen". Aufgrund ihrer technischen Ursachen werden sie an dieser Stelle als Schwäche eingestuft. Auf Ansätze und Strategien, um mit diesem Problem umzugehen, wurde bereits in Abschnitt 7.1.2. eingegangen. In der Praxis gilt es hier vor allem zwischen Leistungseinbußen zugunsten einer transparenteren KI abzuwägen. Dennoch weisen der KI-Wissenschaftler und der externe Berater des BMI darauf hin, dass diese Probleme im Kern immer vorhanden bleiben (E4 2024, 31:00; E9 2024, 38:46).

Abschließend sind Unklarheiten hinsichtlich des tatsächlichen Mehrwertes beim Einsatz smarter Anwendungen und KI-Systemen als Schwäche zu nennen. Auch Fritz (2020, S. 92) benennt den unklaren Mehrwert einer flächendeckenden Videoüberwachung als Schwäche. Im Rahmen der Experteninterviews kritisiert im Besonderen der Jurist der NGO für Grund- und Menschenrechte, dass Grundrechtseinschränkungen ohne einen tatsächlichen Nachweis zum Mehrwert der Technologie in Kauf genommen werden (E7 2024, 27:48). Auch die polizeiliche Führungskraft verweist darauf, dass im Falle von KI-Anwendungen vieles noch unklar sei und bislang noch notwendige Daten zur Effizienz einzelner Anwendungsfälle fehlen (E10 2024, 30:55).

8.2.3. Chancen

Trotz der bislang (noch) fehlenden Nachweise wird seitens der meisten Experten die Chance einer effizienteren Polizeiarbeit betont, wobei Effizienz hier unterschiedliche Bezugspunkte hat.

Zum einen können repetitive Verfahren nach Möglichkeit automatisiert und freigewordenes Personal anderweitig und sinnvoller eingesetzt werden (E3 2024, 01:31:12). Diesbezüglich besteht auch die Chance, eine durch den demographischen Wandel hervorgerufene Personalknappheit abzufedern. Inwieweit hierzu die Möglichkeiten besteht, gilt es allerdings immer für den Einzelfall zu prüfen, da in den meisten Fällen weiterhin eine abschließende manuelle Prüfung der Ergebnisse von Nöten ist. Zum anderen besteht die Chance, durch genauere Prognosen vor und während eines Einsatzes die verfügbaren Einsatzkräfte und Einsatzmittel möglichst effizient einzusetzen, ohne dass zusätzliche Kräfte nachgefordert werden müssen. Der Projektleiter des IT-Dienstleisters verweist auf die Möglichkeit, mithilfe von KI Synergieeffekte zu erzeugen (E5 2024, 36:50). Neben einem effizienteren Personaleinsatz besteht außerdem die Chance einer zeitlichen Effizienz, indem durch die Nutzung von KI mehr Fälle mit einem gleich großen oder sogar geringeren Zeitaufwand bearbeitet werden können (E4 2024, 01:13:06).

Neben Effizienz werden eine allgemein verbesserte Gefahrenabwehr und Strafverfolgung als Chancen genannt. Dank einer schnelleren Datenaus-

wertung können Einsatzleiter in Echtzeitlagen beispielsweise frühzeitig auf mögliche Gefahrenherde reagieren und rechtzeitig einschreiten, bevor es zu einer Eskalation kommen kann (E2 2024, 29:32). Idealerweise lassen sich diesbezügliche Entwicklungen mittel bis langfristig messen, um evidenzbasiert nachzuweisen, dass der Einsatz der KI-Systeme und smarten Technologien einen echten Mehrwehrt mit sich bringt. Erfolgreiche KI-Einsätze durch die Polizei können außerdem dazu beitragen, dass die Akzeptanz in der Bevölkerung allgemein zunimmt, ebenso wie das Vertrauen gegenüber dem Staat und der Polizei (E4 2024, 01:05:56).

8.2.4. Risiken

Statt der Chance, Akzeptanz und Vertrauen zu stärken, sehen die Experten auch das Risiko, dass durch Fehler, Missbrauch oder exzessive staatliche Eingriffe genau das Gegenteil eintritt und wertvolle Akzeptanz und Vertrauen in der Bevölkerung verloren gehen. Auch von Lucke (2020, S. 121) verweist auf dieses Risiko und die Schwierigkeit, verlorenes Vertrauen in die Sicherheitsbehörden wieder aufzubauen. Einzelne Risiken wurden bereits im Zusammenhang mit den Anwendungsfällen in Abschnitt 6. thematisiert, weshalb im Folgenden ein allgemeiner Überblick gegeben werden soll.

Das Risiko diskriminierender polizeilicher Maßnahmen als Folge fehlerhafter oder voreingenommener KI-Systeme wird von einer Mehrheit der Experten genannt. Abseits einer persönlichen Voreingenommenheit von Polizeibeamten kann die Ursache dafür in einem „Automation Bias" liegen. In diesem Fall werden fehlerhafte oder diskriminierende Ergebnisse und Empfehlungen von KI-Systemen übernommen, ohne dass diese seitens der menschlichen Anwender kritisch hinterfragt werden (E9 2024, 37:09). Technische Ursache ist die bereits als Schwäche eingeordnete „Black-Box"-Problematik von KI-Systemen. Ein Risikopotenzial entsteht wiederum dann, wenn ein Bias oder „Halluzinationen" des KI-Systemen aufgrund mangelnder KI-Kompetenz in der Einsatzpraxis reproduziert werden. Dies ist insbesondere dann fatal, wenn Minderheiten als Folge des Automation-Bias durch polizeiliche Maßnahmen diskriminiert werden. Neben polizeilicher Diskriminierung kann ein „Automation Bias" bei Polizeibeamten außerdem dazu führen, dass entgegen rechtlicher Vorgaben ein KI-System indirekt grundrechtseinschränkende Entscheidungen fällt, wenn der menschliche Anwender diese nicht ausreichend hinterfragt (E10 2024, 29:52). In diesem Zusammenhang besteht auch das Risiko, dass ein zu starker Fokus auf KI und IT dafür sorgt, dass essenzielle menschliche Kompetenzen wie Empathie und Vernehmungstechniken vernachlässigt werden (E3 2024, 01:36:51). Auch Fritz verweist in seiner Arbeit auf das Risiko, dass menschliche Polizeibeamte in Teilen durch einen Technologieeinsatz „obsolet" werden können (Fritz 2020, S. 97).

Weiterhin ist das Risiko einer weitreichenden staatlichen Überwachung zu nennen, sollten die im Rahmen der KI-Verordnung gewährten Ausnahmen und Rahmenbedingungen für den Einsatz biometrischer Identifizierung bei der noch ausstehenden Gesetzgebung voll ausgeschöpft werden. In diesem Zusammenhang verweist der Jurist der NGO für Grund- und Menschenrechte auf die Problematik des „Gläsernen Bürgers“ und das Aufkommen eines versteckten Gefühls staatlicher Überwachung (E7 2024, 32:51). Hierzu reiche es bereits aus, über die bestehenden Möglichkeiten staatlicher Überwachung Bescheid zu wissen. Vor diesem Hintergrund wurde nach Verabschiedung der KI-Verordnung von mehreren Seiten gefordert, in Deutschland von vornherein den polizeilichen Einsatz von KI-Systemen zur biometrischen Fernidentifizierung sowohl in Echtzeit als auch retrograd zu verbieten (Vieth-Ditlmann & Sombetzko 2024b, S. 6-9). Im Gegenzug wird von einzelnen Experten das Risiko einer Überregulierung und umfassender Verbote und Einschränkungen für den polizeilichen KI-Einsatz genannt (E9 2024, 58:30; E10 2024, 01:07:00). Mögliche Folgen einer solchen Überregulierung wären Einbußen bei der digitalen Souveränität und die Abhängigkeit von ausländischen Behörden bei der Abwehr und Bekämpfung von Kriminalität und Terrorismus. An dieser Stelle erneut das Spannungsverhältnis zwischen Freiheit und Sicherheit deutlich.

Ein weiteres Risiko, welches seitens mehrerer Experten geäußert wurde, betrifft den Verlust oder die Manipulation sensibler Daten und polizeilichen Wissens durch Cyberangriffen und daraus resultierende Folgen für die Öffentlichkeit und Polizei. In diesem Zusammenhang nennt der Vertriebsleiter des IT-Dienstleisters und ehemalige Polizeibeamte auch das Risiko, dass im Rahmen einer Kooperation mit Unternehmen aus dem Privatsektor sensibles Polizeiwissen verloren geht und im Anschluss von Kriminellen zur Begehung von Straftraten genutzt wird (E3 2024, 01:48:55).

9. Handlungsempfehlungen

Die SWOT-Analyse ergibt, dass KI zusammen mit smarten Technologien grundsätzlich das Potenzial besitzt, im Sinne der in Kapitel fünf genannten Definition einer Smarten Polizeiarbeit zu einer effizienteren und effektiveren Erfüllung polizeilicher Aufgaben und Gewährleistung der Öffentlichen Sicherheit und Ordnung beizutragen. Momentan überwiegen allerdings sowohl bestehende Schwächen die vorhandenen Stärken als auch potenzielle Risiken die voraussichtlichen Chancen. Dementsprechend empfiehlt sich hier eine Strategie der „Vermeidung", welche um eine Strategie des „Aufholens" ergänzt werden kann, da die Ursache einer Mehrheit der Schwächen in fehlenden Grundlagen für den KI-Einsatz liegt (Fleig 2023). Dies beinhaltet, Zusammenhänge zwischen Schwächen und Risiken zu erkennen und vorhandene Schwächen zu beseitigen oder auszugleichen, um im Gegenzug die sich ergebenden Chancen nutzen zu können. Im Folgenden werden diesbezügliche Handlungsempfehlungen vorgestellt.

Notwendige Grundlagen schaffen

Im Rahmen der Experteninterviews wurde mehrfach auf die Notwendigkeit einer souveränen und skalierbaren Cloud-Infrastruktur zum Big Data Management und KI-Einsatz hingewiesen. Aufgrund der Sicherheitsrelevanz des Polizeibereichs gilt es hierbei besonders darauf zu achten, mit welchen Anbietern aus dem Privatsektor und außereuropäischen Ausland man hier zusammenarbeitet. Im Fall des bereits genannten Gaia-X-Projekt sorgte beispielsweise eine Beteilung von Palantir und des chinesischen Telekommunikationsunternehmens Huawei für Kritik (Krempl 2021). Hier gilt es im Besonderen auf die Vertrauenswürdigkeit der Partnerunternehmen und die Sicherheit sensibler Daten und polizeilichen Wissens zu achten. Parallel zur souveränen Cloud-Infrastruktur muss außerdem die allgemeine Digitalisierung der deutschen Polizeibehörden weiter vorangebracht werden. Gleiches gilt für die nationale Umsetzung der europäischen KI-Verordnung, in diesem Falle vor allem die Einrichtung der Reallabore zur Innovationsförderung. Hier bietet sich an, mindestens ein eigenes KI-Reallabor für die Erprobung von polizeilichen Anwendungen einzurichten, wobei empfohlen wird, die Reallabore bei den notifizierten Stellen einzurichten (in diesem Falle beim BfDI) (Goitowski et al. 2022, S. 5). Alternativ könnten auch der KI-Campus der Polizei beim BMI oder das BKA hierfür in Frage kommen. Neben den technischen Grundvoraussetzungen gilt es auch, gegenüber Polizeibeamten von Anfang an klar zu kommunizieren, was der Einsatz von KI alles beinhaltet. Dies soll in erster Linie dazu dienen, überzogene Erwartungen im Sinne „KI als Allheilmittel" und die Angst, durch KI-Systeme ersetzt zu werden, zu dämpfen (E5 2024; 51:21; E9 2024, 28:12; Wolf-Engels 2024).

Einfache und nutzenorientierte Anwendungsfälle

Um sowohl innerhalb der Polizei als auch in der Bevölkerung Akzeptanz für den Einsatz von KI zu schaffen, empfiehlt es sich, zur praktischen Erprobung einfache Anwendungsfälle zu wählen. Diese sollten keine Grundrechtseingriffe beinhalten, da diese eine eigene Rechtsgrundlage erfordern würden. Gleichzeitig sollten sie einen voraussichtlich hohen Nutzwert für den Anwender bieten. Mit Blick auf die in dieser Arbeit vorgestellten Anwendungsfälle dürfte dies vor allem bei GKI-Systemen zur Unterstützung bei der Vorgangsbearbeitung und zur Transkription und Übersetzung von Vernehmungen der Fall sein. Letzteres wurde auch vom BfDI als Beispiel für eine weniger eingriffsintensive polizeiliche KI-Anwendung genannt (BfDI 2024, S. 6). Auch erste Tests einer KI-unterstützten Planung von Großeinsätzen sind vorstellbar. Hierbei sollten allerdings zum einen keine personenbezogenen Daten verwendet werden. Zum anderen muss auch genau geprüft werden, ob die KI-unterstützte Einsatzplanung einen echten Mehrwert gegenüber einer analogen Einsatzplanung bietet, welche auf menschlicher Erfahrung und Intuition basiert.

VR und AR in der Breite einsetzen

Angesichts erster Beispiele für einen erfolgreichen Einsatz bietet es sich an, dass VR und AR-Anwendungen in den Bereichen Tatortrekonstruktion und Training und Ausbildung weitere Verbreitung finden. Angesichts damit verbundener Kosten bietet es sich an, dass sich kleinere und weniger finanzstarke Bundesländer bei der Beschaffung und Nutzung zusammentun, um Synergieeffekte zu erzeugen. Des Weitern kann das BKA in seiner Zentralstellenfunktion eine eigene VR-Umgebung zur Tatortrekonstruktion schaffen, auf welche die Polizeibehörden der Bundesländer bei Bedarf zugreifen können, wenn diese über keine eigene verfügen. Darüber hinaus sollte auch untersucht werden, inwieweit die verschiedenen VR und AR-Anwendungen evidenzbasierte Mehrwerte für die Polizeiarbeit mit sich bringen und wo noch Bedarf zur Nachbesserung besteht.

Test und kritische Evaluierung der weiteren Anwendungsfälle

Angesichts der möglichen Anwendungsbreite und weiterhin offenen Fragen empfiehlt es sich, für das KI-unterstützte Einsatzmanagements in Echtzeit zuallererst eine genauere Konzeption zu erstellen. Diese sollte beinhalten, welche Daten sinnvollerweise für ein Einsatzmanagement in Echtzeit benötigt werden und auf welchem Wege diese Daten während des Einsatzes gesammelt und ausgewertet werden (beispielsweise per Bodycams, Überwachungskameras, oder Drohnen). Weiterhin sollte geprüft werden, inwieweit neben den technischen Voraussetzungen auch die nötigen Rechtsgrundlagen vorliegen beziehungsweise geschaffen werden müssten, wenn

Grundrechtseingriffe vorgenommen werden sollen. Hierbei empfiehlt es sich, das System möglichst „by-Design" zu konzipieren, insbesondere hinsichtlich des gebotenen Datenschutzes. Die Konzeption soll zuallererst rein theoretischer Natur sein. Falls die notwendigen technischen und rechtlichen Voraussetzungen vorliegen, kann die Konzeption wiederum für erste Testläufe des KI-unterstützten Echtzeiteinsatzmanagements genutzt werden.

Mit Blick auf die beiden Anwendungsfälle zur Analyse biometrischer Daten empfiehlt es sich, vorerst von einer Umsetzung abzusehen. Grund hierfür sind weiterhin fehlende Rechtsgrundlagen, die Schranken und Vorgaben seitens der KI-Verordnung sowie die erheblichen Grundrechtseingriffe im Falle eines Einsatzes, welche ein besonnenes Handeln und eine umfassende Folgenabschätzung notwendig machen. Bevor in Zukunft mögliche Rechtsgrundlagen geschaffen werden, sollte zuerst die in Abschnitt 6.3.3. genannte Frage der zugrundliegenden Datenbanken für biometrische Daten hinreichend geklärt sein. Weiterhin gilt es sicherzustellen, dass innerhalb der gesetzlichen Regelung genau erörtert wird, welche Technologien wie eingesetzt werden sollen. Dies wurde im Fall des Sicherheitspaketes seitens der Sachverständigen im Innenausschuss als nicht ausreichend kritisiert (Averdung 2024). Zudem empfiehlt es sich zu prüfen, ob die benötigte Kameratechnik und Software bereits von deutschen oder europäischen Hersteller angeboten wird oder ob Eigenlösungen notwendig sind. Auf die Beschaffung bei umstrittenen und unsicheren Anbietern aus dem außereuropäischen Ausland sollte verzichtet werden (Greis 2024, S. 2). Abschließend sollte eine ausführlichen öffentliche und parlamentarische Debatte geführt werden, um Transparenz zu fördern und die Zustimmung der gesellschaftlichen Mehrheit für den Einsatz biometrischer Identifikationssysteme zu gewährleisten (E6 2024, 01:02:00). Hierbei gilt es auch kritisch zu evaluieren und abzuwägen, ob die zu erwartenden Freiheitseinschränkungen durch einen messbaren Mehrwert für die öffentliche Sicherheit gerechtfertigt sind. Hierfür bietet es sich an, auf die Ergebnisse der früheren Teststudie von August 2017 bis Juli 2018 am Berliner Bahnhof Südkreuz zurückzugreifen. Entgegen dem positiven Urteil des BMI wurden die ermittelten Erkennungsraten allerdings seitens zivilgesellschaftlicher Organisationen als unzureichend kritisiert und sorgen damit für Zweifel hinsichtlich eines klaren Mehrwerts dieser Technologie (Dachwitz 2018).

Stärkung der KI-Kompetenz und neue Anwendungsfälle

Als Teil der polizeilichen Organisationsentwicklung wurde das Thema der KI-Kompetenz bereits in Abschnitt 7.5.2. angesprochen. Diese kann als notwendige Voraussetzung dafür betrachtet werden, um das Risiko eines fatalen „Automation Bias" zu reduzieren. Polizeibeamte werden so frühzeitig mit der Arbeit mit KI-Systemen vertraut gemacht und über mögliche Limitationen aufgeklärt, um anschließend die Ergebnisse der KI entsprechend

kritisch hinterfragen zu können (E9 2024, 36:40). Um den Ausbau der polizeiinternen KI-Kompetenz zu gewährleisten und KI-Modelle für polizeiliche Anwendungen zu trainieren, sollten eigene KI-Kompetenzzentren der Polizei eingerichtet werden (E1 2024, 44:04; E2 2024, 01:00:27). Mit dem KI-Campus der Polizei beim BMI und der Beteilung der Landespolizei Baden-Württemberg am Innovation Park Artificial Intelligence gibt es hier bereits erste Ansätze (Landesregierung Baden-Württemberg 2023b). Der Projektleiter des IT-Dienstleisters äußert diesbezüglich das Ziel eines interdisziplinären Ökosystems, bestehend aus Staat, Wirtschaft und Wissenschaft, um optimale Ergebnisse erzielen zu können (E5 2024, 56:42). Dies soll auch die Möglichkeit beinhalten, gemeinsam entwickelte Lösungen direkt in Reallaboren zu testen. Weiterhin können im Rahmen der Kompetenzzentren neue Anwendungsfälle konzipiert werden. Hierbei sollten unbedingt die Anforderungen Beachtung finden, welche in Kapitel sieben dieser Arbeit vertiefend behandelt wurden. Wichtig ist vor allem auch, dass die Polizei von Anfang an verantwortungsvoll mit neuen KI-Anwendungen umgeht, damit das öffentliche Vertrauen nicht durch Missbrauch oder anderweitige Vorfälle negativ beeinflusst wird (E6 2024, 01:02:18). Auch sollte die Politik es vermeiden, Gesetze „durchzupeitschen“, wenn diese die Rechtsgrundlage für Grundrechtseingriffe bilden sollen. Dies wurde beispielsweise auch im Zusammenhang des Sicherheitspaketes kritisiert (Reuter 2024).

10. Fazit und Ausblick

10.1. Fazit

KI ist ein Zukunftsthema, welches auch seitens der Polizei erkannt wurde. Jedoch befinden sich die Polizeibehörden in Deutschland noch ganz am Anfang eines breiten Einsatzes von KI. Im Rahmen dieser Arbeit wurde eine Reihe an möglichen Anwendungsfällen für präventive, repressive und doppelfunktionale Maßnahmen beleuchtet, welche in Zukunft die Polizeiarbeit im Sinne einer Polizei 4.0 und 5.0 transformieren können. Als besonders vielversprechend haben sich Ansätze von GKI erwiesen, welche die Polizei bei der Bewältigung von Routineaufgaben und der Vorgangsbearbeitung unterstützen. Hierdurch bieten sich Möglichkeiten zur Teilautomatisierung, welche dabei helfen können, die Folgen des demographischen Wandels abzufedern. Ergänzend dazu erlauben die Technologien von VR und AR neue Ansätze der Spurensicherung und Tatortrekonstruktion sowie die Möglichkeit zu einem flexiblen und realitätsnahen Training von Hochrisiko-Einsatzszenarien. Bereits heute kommen diese Technologien in einigen Bundesländern zum Einsatz und dürften in Zukunft eine größere Verbreitung erfahren. Dem gegenüber stehen umstrittene Anwendungsfälle mit Systemen zur biometrischen Identifikation, welche auf erhebliche Weise in das Grundrecht auf informationelle Selbstbestimmung eingreifen. Nicht gänzlich klar sind die Potenziale von KI-Systemen, um die Polizei bei der Planung von Großeinsätzen zu unterstützen und diese nahezu in Echtzeit zu managen. Hier bietet sich an, genauere theoretische Konzeptionen vorzunehmen und erste Tests durchzuführen, bei welchen auf den Gebrauch personenbezogener Daten verzichtet werden sollte.

Von zentraler Bedeutung ist hierbei, dass KI und smarte Technologien interoperabel, benutzerfreundlich und sicher gestaltet werden und im Falle von Grundrechtseingriffen der Einsatz auf einer klaren Rechtsgrundlage beruht. Diese muss wiederum den Vorgaben aus der Verfassung, dem Datenschutzrecht und der KI-Verordnung entsprechen. Weiterhin sind umfangreiche Folgenabschätzungen unter reger Beteiligung der Datenschutzbeauftragten notwendig. Um die Vorteile von KI und smarten Technologien vollständig auszuschöpfen, müssen mit einer weiteren Digitalisierung der Polizeibehörden und einer digital-souveränen IT-Infrastruktur zunächst die nötigen Grundlagen geschaffen werden. Gerade bei kritischen Technologien wie der biometrischen Fernidentifizierung muss der Gesetzgeber ein ausgewogenes und evidenzbasiertes Verhältnis zwischen Sicherheit und Freiheit gewährleisten. Eine offene öffentliche Debatte ist dabei essenziell, um sowohl Verständnis als auch Akzeptanz für den Technologieeinsatz zu fördern. Werden grundrechtsinvasive KI-Systeme ohne die gebotene Transparenz eingeführt, droht ein verdecktes Gefühl der Überwachung in der Bevölkerung, das nicht nur die allgemeine Akzeptanz für den Einsatz von KI

und smarten Technologien, sondern auch das Vertrauen in die Polizei insgesamt gefährdet.

10.2. Limitationen

Aufgrund der Größe des Themas und einem allgemeinen Fokus auf die Polizei in Deutschland konnte der Einsatz von KI und smarten Technologien innerhalb der Arbeit zwar in seiner Breite, jedoch nicht vertiefend behandelt werden, ohne dass dies den vorgesehenen inhaltlichen Umfang überschreiten würde. Die in Kapitel sechs behandelten Anwendungsfällen sollen einen ersten Ausblick auf das Thema geben. Weitere mögliche Anwendungsfälle, welche im Rahmen der Experteninterviews genannt wurden, finden sich in Anhang III und bieten die Möglichkeit für weitere Fallstudien zum Thema. Der überwiegende Teil dieser Anwendungsfälle adressiert jedoch vor allem das Ziel einer Effizienzsteigerung, während mit der Transparenzerhöhung und verbesserten Serviceleistungen für den Bürger andere Ziele einer Smarten Polizeiarbeit offenbleiben.

Weiterhin konnten nicht alle relevanten Perspektiven im Rahmen der Experteninterviews abgedeckt werden. So wurde beispielsweise auf Interviews mit Vertretern der Bundes- und Landespolitik zugunsten einer vertieften Betrachtung des Themas der Rechtsstaatlichkeit verzichtet. Auch wurden keine Interviews mit Datenschutzbeauftragten geführt, welche das Thema des polizeilichen Datenschutzes und der Datenethik näher beleuchten. Ebenso konnte lediglich ein Interview mit einem Vertreter einer Landespolizeibehörde geführt und ausgewertet werden. Dementsprechend sind die Ergebnisse und Positionen hinsichtlich dem Einsatz von KI und smarten Technologien, Finanzierung, Digitalisierungsstand und Gesetzeslage nicht repräsentativ für alle deutschen Polizeibehörden.

Wie bereits zum Ende von Abschnitt 6.1.3. erwähnt, konnte nicht abschließend geklärt werden, wie das Verhältnis zwischen dem zentralen Datenhaus im Rahmen von P20 und dem Konzept eines dezentralen Polizei-Datenraumes genau gestaltet ist. Grund hierfür dürften zum Teil auch Verständnisprobleme zum Begriff des Datenraumes seitens der interviewten Experten sein. Da sich das Datenhaus momentan noch im Aufbau befindet und öffentlich verfügbare Informationen zur technischen Gestaltung begrenzt sind, ist ein genauerer Vergleich mit dem Konzept des Datenraumes schwierig. Ende Oktober 2024 wurde seitens der Bundesregierung berichtet, dass die Konzeptionsphase für das Datenhaus abgeschlossen sei und die reine Umsetzungsphase beginne (Krempl 2024). Dementsprechend besteht die Aussicht, dass bald mehr Details zum Verhältnis zwischen dezentralem Datenraum und zentralen Datenhaus vorliegen.

10.3. Ausblick

Der zukünftige Einsatz von KI in den deutschen Polizeibehörden wird unter anderem vom Ergebnis der nächsten Bundestagswahl im kommenden Jahr abhängen, welche voraussichtlich zu einem vorgezogenen Termin am 23. Februar 2025 stattfinden soll (Rzepka 2024). Die nächste Bundesregierung wird dabei für die weitere Umsetzung der KI-Verordnung und die Schaffung von Rechtsgrundlagen für den polizeilichen Einsatz von Hochrisiko-KI verantwortlich sein. Entsprechend lohnt es sich, diese Entwicklungen weiter im Auge zu behalten, auch mit Blick auf die parallele Umsetzung in anderen EU-Ländern.

Des Weiteren können sich zukünftige Forschungsarbeiten vertiefend mit den in Kapitel sechs beschriebenen Anwendungsfällen beschäftigen und eigene SWOT-Analysen zu den jeweiligen Anwendungsfällen vornehmen. Zusätzlich können die Anwendungsfälle aus Anhang III vertiefend behandelt werden, auf die in dieser Arbeit nicht näher eingegangen werden konnte. Zudem bietet der Bereich der Cyberforensik und Bekämpfung von Cyberkriminalität einen ganz eigenen Bereich für KI-Anwendungen, welcher in dieser Arbeit nicht behandelt wurde. Zukünftige Forschungsarbeiten können sich außerdem den Einsatzmöglichkeiten von KI in der Justiz und bei Geheimdiensten widmen, da mit den Bereichen der Strafermittlung und Terrorismusabwehr hier erwartungsgemäß Schnittmengen mit der polizeilichen Arbeit bestehen dürften.

Anhang

I. Übersicht zu den geführten Interviews

Kürzel	Position	Datum	Interviewform
E1	Professor für Öffentliches Recht	01.10.2024	Online
E2	Mitarbeiter in einem IT-Dienstleistungsunternehmen	08.10.2024	Online
E3	Vertriebsleiter in einem IT-Dienstleistungsunternehmen, ehemaliger Polizeibeamter	15.10.2024	Online
E4	KI-Wissenschaftler in einem deutschen Forschungsinstitut	17.10.2024	Online
E5	Projektleiter in einem IT-Dienstleistungsunternehmen	18.10.2024	Online
E6	Wissenschaftlicher Leiter eines Cybersicherheitsunternehmen	26.10.2024	Online
E7	Jurist in einer NGO für Grund- und Menschenrechte	29.10.2024	Online
E8	Professor für Strafrecht	31.10.2024	Online
E9	Berater des Bundesinnenministeriums	05.11.2024	Online
E10	Führungskraft in einem Polizeipräsidium (Landespolizei)	12.11.2024	Online

Tabelle 2: Übersicht zu den geführten Interviews

Zusätzlich wurde am 05.11.2024 ein weiteres Interview mit zwei Führungskräften aus einem Landesinnenministerium geführt. Dieses Interview konnte nicht aufgezeichnet werden und diente stattdessen als Hintergrundgespräch für weitere Recherchen.

II. Verwendeter Interviewleitfaden

Das Ziel meiner Arbeit ist es herauszufinden, welche neuen Ansätze und Einsatzszenarien es speziell für smarte Technologien, Big Data, erweiterte und virtuelle Realität und fortgeschrittene künstliche Intelligenz gibt, um Polizeibehörden in Deutschland bei ihrer Arbeit zu unterstützen und welche Anforderungen, Probleme und Risiken sich hieraus ergeben. Im Ergebnis der Arbeit sollen die identifizierten Einsatzmöglichkeiten mittels SWOT-Analyse überprüft und basierend auf den Analyseergebnissen Handlungsempfehlungen abgeleitet werden. Das Interview ist Teil einer Reihe von Interviews mit verschiedenen Expertinnen und Experten aus der Polizeipraxis, Verwaltung, Informations- und Telekommunikationsbranche und Wissenschaft. Zur späteren Auswertung soll das Interview mit Ihrer Zustimmung aufgezeichnet werden. Die Ergebnisse des Interviews werden für die Verweise innerhalb der Masterthesis anonymisiert.

Einstieg

1. Stellen Sie sich zum Einstieg bitte kurz selbst vor, ihre Position in ihrer Organisation und ihr Aufgabenfeld.
2. Was verstehen Sie unter dem Begriff „smart“?
3. Was verstehen Sie unter „smarter Technologie“?
4. Was verstehen Sie persönlich unter „smarter Polizeiarbeit“?
5. Welche Beispiele für smarte Technologien fallen ihnen spontan ein, die bereits heute bei der Polizei in Deutschland im Einsatz sind?
6. Geben Sie bitte eine kurze Bewertung über diese Beispiele ab? Wie stehen Sie dazu

Neue Einsatzfelder

7. Smarte Technologien erzeugen sensorgestützt smarte Daten, die es für die Polizeiarbeit auszuwerten gilt. Wie ließe sich ihrer Meinung nach die immer größer werdende Menge an Daten (Big Data) bei der polizeilichen Arbeit IT- technisch am besten managen?
8. Der GaiaX Hub Deutschland definiert sogenannte Datenräume wie folgt: „Eine föderierte (dezentrale), interoperable, offene Infrastruktur für souveränen Datenaustausch, die auf gemeinsamen Vereinbarungen, Regeln und Standards beruht.“
   Wie bewerten Sie die Schaffung solcher Datenräume als Ergänzung zum zentralen Datenhaus von P20 für die Polizeien von Bund & Ländern?
9. Welche Daten sollten diese Datenräume sinnvollerweise beinhalten?

10. Welche geographische Ausdehnung sollte ein Verbund solcher Polizeidatenräume sinnvollerweise haben?
11. Mit Sprachmodellen wie ChatGPT, CoPilot und Co. finden generative KIs immer mehr Verbreitung.
    Welche Potenziale für den Einsatz generativer und anderer fortschrittlicher KI's fallen ihnen in den folgenden drei Bereichen ein, um die Arbeit der Polizei zu unterstützen bzw. zu verbessern?
    a. Einsatzmanagement
    b. Operative Prozesse
    c. Polizeiliche Kernaufgaben
12. Welche Einsatzmöglichkeiten sehen Sie in Zukunft für die Technologien virtueller (VR) und erweiterte Realität (AR), um die Arbeit der Polizei zu unterstützen bzw. zu verbessern?
13. Welche Stärken und Chancen sehen Sie im Einsatz von Smarten Technologien, Big Data, KI, AR und VR verglichen mit der aktuellen, „analogen" Polizeipraxis?
14. Welche Schwächen bestehen ihrer Ansicht nach beim Einsatz dieser Technologien? Wo wird der Mehrwert dieser Technologien möglicherweise überschätzt?

Anforderungen, Herausforderungen und Risiken

15. Welche technischen Anforderungen gilt es an smarte Technologien, Big Data, KI, AR und VR zu stellen, damit diese effektiv durch die Polizei eingesetzt werden können?
16. Was sind ihrer Ansicht nach momentan die größten Herausforderungen für die Einführung und den Einsatz von smarten Technologien, KI, Big Data, AR und VR durch die Polizei?
17. Auf welche Risiken muss man sich beim Einsatz dieser Technologien durch die Polizei vorbereiten?
18. Das kürzlich vom Bundestag beschlossene Gesetz zur Verbesserung der Terrorismusbekämpfung soll die Rechtsgrundlage dafür schaffen, dass Bundespolizei und BKA in Zukunft KI-basierte Abgleiche von öffentlich zugänglichen biometrischen Daten aus dem Internet vornehmen können. Ist dies ihrer Ansicht nach eine längst überfällige Maßnahme, um den Sicherheitsbehörden in Deutschland das nötige technische Handwerkszeug zur Abwehr und Bekämpfung schwerster Kriminalität in die Hand zu geben? Oder treibt dies die Grenzen des Machbaren weiter in Richtung eines dystopischen Überwachungsstaates voran?

19. Welche anderen rechtlichen Rahmenbedingungen müssen ihrer Meinung nach noch geschaffen oder angepasst werden, um die Einführung und den Einsatz der hier besprochenen smarten Technologien, KI, AR, VR und Big Data zu erleichtern?
20. Wie ließe ich ihrer Ansicht nach eine angemessene externe Qualitätssicherung gewährleisten, wenn diese Technologien wie hier besprochen eingesetzt werden, damit das gebotene Maß zwischen Freiheit und Sicherheit nicht überschritten wird?
21. Welche Rolle sollte ihrer Ansicht nach hierbei die Zivilgesellschaft spielen?
22. Wie bewerten Sie in Kürze die Akzeptanz für den Einsatz dieser Technologien durch die Polizei in der allgemeinen Bevölkerung?
23. Wie bewerten Sie in Kürze die polizeiinterne Akzeptanz für den Einsatz dieser Technologien?
24. Wo und wie muss sich die Polizei als Organisation im Zusammenhang mit dem Einsatz von Smarten Technologien, KI, Big Data, AR und VR weiterentwickeln?
25. Wie können diese Technologien den Polizeibehörden dabei helfen, den Folgen des demographischen Wandels zu begegnen?
26. Wie bewerten Sie angesichts des vorgeschlagenen Gesetzes zur Verbesserung der Terrorismusbekämpfung den politischen Willen in Deutschland, die notwendigen Schritte hin zur Weiterentwicklung zu einer smarten Polizei zu gehen?
27. Wie bewerten Sie die aktuelle Finanzierung für den Einsatz moderner Technologien durch die Polizei? Falls diese aufgestockt werden soll, in welchen Bereich(en)?

Abschluss und Blick in die Zukunft

28. Was wäre aus Ihrer Sicht ein „Worst-Case-Szenario“ für die Einführung und den Einsatz smarter Technologien, Big Data, KI, VR und AR in der Polizei?
29. Wie sähe im Gegenzug für Sie ein „Best-Case-Szenario“ aus?
30. Vor dem Hintergrund der hier im Interview besprochenen Punkte: Nennen Sie abschließend drei Handlungsempfehlungen, um der Polizei in Zukunft einen rechtsstaats- und datenschutzkonformen Einsatz von Smarten Technologien, Big Data, KI, VR und AR zu ermöglichen.
31. Gibt es noch etwas, dass Sie gerne anfügen würden oder haben Sie Literaturempfehlungen, die Sie mir gerne mitgeben würden?

III. Weitere mögliche Anwendungsfälle für KI und smarte Technologie

Generative KI zur Verarbeitung und Verwaltung von polizeilichen Massen daten

GKI kann dazu eingesetzt werden, um Daten aus verschiedenen polizeilichen Datenbanken zusammenzuführen sowie in kompakter Form und in natürlicher Sprache eine Antwort auf Anfragen zu erhalten, welche ebenfalls in natürlicher Sprache gestellt wurden (ohne notwendigerweise eine datenbankspezifische Programmiersprache zu beherrschen) (E4, 2024, 23:58). Des Weiteren besteht die Möglichkeit, mittels KI multifunktional auch unstrukturierte Daten und Bilder abzufragen und mittels Wissensgraphen ins Verhältnis zueinander zu setzen (ebd., 24:28).

KI zur Unterstützung und Individualisierung von Training und Ausbildung

Chatbots können auf Basis von Benutzerhandbüchern oder Online-Anleitungen dazu eingesetzt werden, um Polizeibeamten bei der Nutzung von komplexen technischen Anwendungen zu unterstützen (E2, 2024, 22:00). Des Weiteren können GKI-Systeme auf Basis des aktuellen Ausbildungsstandes und des individuellen Lerntyps personalisierte Trainings- und Fortbildungsangebote für Polizeibeamte entwickeln. (E5, 2025, 29:17).

Emotionserkennung mittels Infrarotsystemen

Seitens der Polizei können Systeme zur Emotionserkennung ähnlich wie Bodycams in kritischen Situationen zur Eskalationsvermeidung und zum Schutz von Einsatzkräften vor Übergriffen dienen (E4, 2024, 01:21:10). Ähnlich wie bei den Systemen zur biometrischen Identifizierung stellt ein solches System zur Emotionserkennung einen erheblichen Eingriff in die Persönlichkeitsrechte dar und ist entsprechend kritisch zu bewerten (ebd., 01:21:00). Unklar ist hier auch, inwieweit solche Systeme seitens der KI-Verordnung zugelassen sind oder ob diese überhaupt rechtlich seitens der Verordnung reguliert werden (und hier notwendigerweise ein Bedarf zur Anpassung besteht) (ebd., 35:44).

Erweitere Bild- und Video- und Tonanalysen für Ermittlungen

KI-Systeme können im Rahmen von automatisierte Bild- und Video- und Tonanalysen dazu genutzt werden (nicht personenbezogene) Ermittlungsansätze aus dem zugrundeliegenden Material herauszufiltern, beispielsweise dem Ort, an dem die Aufnahme sehr wahrscheinlich stattfand und damit auch mögliche Ermittlungsansätze (E5, 2024, 31:12). Weiterhin können KI-Systeme auch dazu eingesetzt werden, um automatisiert bestimmte verfassungsfeindliche Symbole oder Parolen zu identifizieren (E9, 2024, 20:50).

KI-unterstützte Beweismittelverwaltung

GKI kann dazu eingesetzt werden, basierend auf Bildern eines Beweismittels hiervon eine automatisierte Beschreibungen zu erzeugen. Im Anschluss kann diese Beschreibung für plattformbasierte Abgleiche verwendet werden, um vergleichbare Beweismittel aus anderen Fällen zu identifizieren und Ansatzpunkte für Ermittlungen zusammenzuführen (E10, 2024, 23:54).

Literaturverzeichnis

Adams et al. 2019: Adams, Yasmina; van den Heuvel, Elrike; Yan, Shun-Jie & Korz, Johannes: Bodycams bei der Polizei.in: Gesellschaft Für Informatik e.V., Bonn 23. April. Online: https://gi.de/themen/beitrag/bodycams-bei-der-polizei.

Alexy et al. 2023: Alexy, Lennart Alexy; Fisahn, Andreas; Hähnchen, Susanne; Mushoff, Tobias & Trepte, Uwe: Sicherheit und Ordnung, öffentliche, in: Das Rechtslexikon. Begriffe, Grundlagen, Zusammenhänge, 2. Auflage, Verlag J.H.W. Dietz, Bonn 2023. Online: https://www.bpb.de/kurz-knapp/lexika/recht-a-z/324035/sicherheit-und-ordnung-oeffentliche/.

Alt 2018: Alt, Rainer: Big Data, Gabler Banklexikon, Wiesbaden 2018. Online: https://www.gabler-banklexikon.de/definition/big-data-99809/version-337011.

Apelt & Möllers 2011: Apelt, Maja und Möllers, Norma: Wie „intelligente" Videoüberwachung erforschen? Ein Resümee aus zehn Jahren Forschung zu Videoüberwachung, Zeitschrift Für Außen- Und Sicherheitspolitik, Wiesbaden 2011, Bd. 4, 4, S. 585–593.

Arndt 2018: Arndt, Boris: Drohnen im Polizeieinsatz - modernste Technik im Test!, Drohnen Journal, Köln August 2018. Online: https://www.drohnen-journal.de/drohnen-im-polizeieinsatz-1718.

Arzt 2021: Arzt, Clemens: EU-Datenschutz und Polizei: Die JI-Richtlinie im deutschen Polizeirecht, Bürgerrechte & Polizei/CILIP, Berlin Dezember 2021, Bd. 127, 3, S. 43–52.

Averdung 2024: Averdung, Franz Ludwig: Regierungskatalog in der Experten-Kritik, Das Parlament, Berlin 27. September. Online: https://www.das-parlament.de/inland/innenpolitik/regierungskatalog-in-der-experten-kritik.

Baum et al. 2024: Baum, Sandra; Beer, Frank; Behrendt, Eric; Bischoff, Susan; Böken, Arnd; Breuer, Jan; Dalerci, Camilla; ... Wisselink, Frank: Umsetzungsleitfaden zur KI-Verordnung: Compliance in der Praxis – Schritt für Schritt, Bitkom, Berlin 2024. Online: https://www.bitkom.org/sites/main/files/2024-10/241028-bitkom-umsetzungsleitfaden-ki.pdf.

Bendel 2023: Bendel, Oliver: Polizeiroboter, Gabler Wirtschaftslexikon, Wiesbaden Januar 2023. Online: https://wirtschaftslexikon.gabler.de/definition/polizeiroboter-124917/version-387741.

Benöhr-Laqueur 2018: Benöhr-Laqueur, Susanne: 2018-das Jahr, in dem die deutsche Polizei erstmals Drohnen gegen Gefährder einsetzte: Anmerkungen zu Art. 47 Bayerisches Gefahrenabwehrgesetz (PAG), TATuP-Zeitschrift Für Technikfolgen-

abschätzung in Theorie Und Praxis/Journal for Technology Assessment in Theory and Practice, München 2018, Bd. 27, 3, S. 14–19.

Bitkom 2024: Künstliche Intelligenz in Deutschland: Perspektiven aus Bevölkerung & Unternehmen, Bitkom e.V., Berlin 2024. Online: https://www.bitkom.org/sites/main/files/2024-10/241016-bitkom-charts-ki.pdf.

Bogner 2009: Bogner, Alexander; Littig, Beate & Menz, Wolfgang: Experteninterviews: Theorien, Methoden, Anwendungsfelder, 3. Auflage, VS Verlag für Sozialwissenschaften, Wiesbaden 2009.

Borell & Schindler 2019: Borell, Anne und Schindler, Stephan: Polizei und Datenschutz, in David Geihs und Lange Stumm: INFORMATIK 2019: 50 Jahre Gesellschaft für Informatik – Informatik für Gesellschaft, Gesellschaft für Informatik e.V., Bonn 2019, S. 393–406.

Brandner & Hirsbrunner 2023: Brandner, Lou Therese und Hirsbrunner, Simon David: Algorithmische Fairness in der polizeilichen Ermittlungsarbeit: Ethische Analyse von Verfahren des maschinellen Lernens zur Gesichtserkennung, TATuP - Zeitschrift Für Technikfolgenabschätzung in Theorie und Praxis /Journal for Technology Assessment in Theory and Practice, München 2023, Bd. 32, 1, S. 24-29.

Braun Binder et al. 2021: Braun Binder, Nadja; Spielkamp, Matthias; Egli, Catherine; Freiburghaus, Laurent; Kunz, Eliane; Laukenmann, Nina; ... Wulf, Jessica: Einsatz Künstlicher Intelligenz in der Verwaltung: rechtliche und ethische Fragen, Staatskanzlei Kanton Zürich, Zürich 2021.
Online: https://edoc.unibas.ch/83846/1/20210703091148_60e00db459b55.pdf.

BSP Business School Berlin 2021: KI-Kochbuch- Rezepte für den Einsatz Künstlicher Intelligenz in Unternehmen, Berlin 2021. Online: https://www.digitalzentrum-zukunftskultur.de/wp-content/uploads/2021/03/LUK_KI_kochbuch_210508.pdf.

Büchel & Engler 2024: Büchel, Jan und Engler, Jan: Generative KI in Deutschland: Künstliche Intelligenz in Gesellschaft und Unternehmen, IW-Report, Bd. 23, Institut der der deutschen Wirtschaft (IW), Köln 2024.
Online: https://hdl.handle.net/10419/294841.

Bundesamt für Sicherheit in der Informationstechnik (BSI) 2021: Sicherer, robuster und nachvollziehbarer Einsatz von KI: Probleme, Maßnahmen und Handlungsbedarfe, Bonn 2024. Online: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/KI/Herausforderungen_und_Massnahmen_KI.pdf?__blob=publicationFile&v=6.

Bundesbeauftragte für den Datenschutz und Informationsfreiheit (BfDI) 2021: Positionspapier des Bundesbeauftragten für den Datenschutz und die

Informationsfreiheit zum Grundsatz der Zweckbindung in polizeilichen Informationssystemen, Bonn 2021. Online: https://www.bfdi.bund.de/SharedDocs/Downloads/DE/DokumenteBfDI/Stellungnahmen/2021/Positionspapier_Zweckbindung-Polizei.pdf?__blob=publicationFile&v=4.

Bundesbeauftragte für den Datenschutz und Informationsfreiheit (BfDI) 2024: Datenschutzrechtliche Grundlagen beim Einsatz von Künstlicher Intelligenz (KI) im Bereich der Sicherheitsbehörden des Bundes: Handreichung des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit, Bonn 2024. Online: https://www.bfdi.bund.de/SharedDocs/Downloads/DE/DokumenteBfDI/Dokumente-allg/2024/Handreichung-BfDI-KI-Sicherheitsbeh%C3%B6rden.pdf?__blob=publicationFile&v=3.

Bundesministerium des Inneren und für Heimat o.D.: Unsere Behörden und Einrichtungen – Bundespolizei, Bundesministerium des Inneren und für Heimat, Berlin o.D. Online: https://www.bmi.bund.de/SharedDocs/behoerden/DE/bpol.html.

Bundesministerium des Innern und für Heimat 2018: White Paper zum Programm Polizei 20/20, Bundesministerium des Inneren und für Heimat, Berlin 2018. Online: https://www.bmi.bund.de/SharedDocs/downloads/DE/veroeffentlichungen/2018/polizei-2020-white-paper.pdf?__blob=publicationFile&v=8.

Bundesministerium des Innern und für Heimat 2024: KI-Leitbild für das Ressort BMI, Bundesministerium des Inneren und für Heimat, Berlin 2024. Online: https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/it-digitalpolitik/BMI24014.pdf?__blob=publicationFile&v=3.

Bundesregierung, Deutsche 2021: Mehr Fortschritt wagen- Bündnis für Freiheit, Gerechtigkeit und Nachhaltigkeit: Koalitionsvertrag 2021-2025 zwischen der Sozialdemokratischen Partei Deutschlands (SPD), Bündnis 90/Die Grünen und den Freien Demokraten (FDP), Berlin 2021. Online: https://www.spd.de/fileadmin/Dokumente/Koalitionsvertrag/Koalitionsvertrag_2021-2025.pdf.

Bundesverfassungsgericht 2024: Einzelne gesetzliche Befugnisse des BKA zur Datenerhebung (§ 45 Abs. 1 Satz 1 Nr. 4 BKAG) und Datenspeicherung (§ 18 Abs. 1 Nr. 2 BKAG) sind in Teilen verfassungswidrig, Bundesverfassungsgericht, Karlsruhe 1. Oktober 2024. Online: https://www.bundesverfassungsgericht.de/SharedDocs/Pressemitteilungen/DE/2024/bvg24-083.html.

Dachwitz 2018: Dachwitz, Ingo: Überwachungstest am Südkreuz: Geschönte Ergebnisse und vage Zukunftspläne, Netzpolitik.org, Berlin 16. Oktober 2018. Online: https://netzpolitik.org/2018/ueberwachungstest-am-suedkreuz-geschoente-ergebnisse-und-vage-zukunftsplaene/.

Dampz 2022: Dampz, Nils: Mit Polizeirobotern gegen Gewalttäter, tagesschau.de, Hamburg 3. Dezember 2022. Online: https://www.tagesschau.de/ausland/amerika/san-francisco-polizeiroboter-101.html.

Datenethikkommission der Bundesregierung 2019: Gutachten der Datenethikkommission, Berlin 2019. Online: https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/it-digitalpolitik/gutachten-datenethikkommission.pdf?__blob=publicationFile&v=6.

De Mauro et al. 2015: De Mauro, Andrea; Greco, Marco & Grimaldi, Michele: What is big data? A consensual definition and a review of key research topics, AIP Conference Proceedings, Madrid 2015, Bd. 1644, 1, S. 97–104.

Dehmel 2024: Dehmel, Susanne: Stellungnahmen Anhörung des Innenausschusses des Deutschen Bundestages zum Projekt „VeRA" am 22.04.2024, Deutscher Bundestag/bitkom e.V., Berlin 2024. Online: https://www.bundestag.de/resource/blob/999084/a551fff433721072ec52e0cbda42c6bd/20-4-418-G.pdf.

Deutscher Ethikrat 2023: Mensch und Maschine-Herausforderungen durch Künstliche Intelligenz: Stellungnahme, Berlin 2023. Online: https://www.ethikrat.org/fileadmin/Publikationen/Stellungnahmen/deutsch/stellungnahme-mensch-und-maschine.pdf.

Dieckert 2017: Dieckert, Ulrich: Der fliegende Kommissar, Drohnen Magazin 2017, Bd. 2, 1, S. 32–35.

Djeffal 2017: Djeffal, Christian: Das Internet der Dinge und die öffentliche Verwaltung–Auf dem Weg zum automatisierten Smart Government?, Deutsches Verwaltungsblatt, Köln Juli 2017, Bd. 132, 13, S. 808–816.

Duden o.D.: smart - Rechtschreibung und Bedeutungsübersicht, Dudenverlag, Berlin o.D.. Online: https://www.duden.de/rechtschreibung/smart.

Eckert et al. 2014: Eckert, Klaus-Peter; Henckel, Lutz und Hoeppner, Petra: Big Data - Ungehobelte Schätze oder digitaler Albtraum?, in: Fraunhofer FOKUS Newsletter, Ausgabe März 2014, Berlin 2014.

Etscheid et al. 2020: Etscheid, Jan; von Lucke, Jörn und Stroh, Felix: Künstliche Intelligenz in der Öffentlichen Verwaltung: Anwendungsfelder und Szenarien, Fraunhofer IAO, Stuttgart 2020.

Europäische Kommission 2020: Mitteilung der Kommission an das Europäische Parlament, den Rat und den europäischen Wirtschaft- und Sozialausschuss und den Ausschuss der Regionen: Eine europäische Datenstrategie, Europäische

Kommission, Brüssel 2020. Online: https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A52020DC0066.

Farthofer 2022: Farthofer, Hilde: Der Einsatz von Künstlicher Intelligenz in der Kriminalprävention, in: Thomas-Gabriel Rüdiger und P. Saskia Bayerl (Hrsg.): Handbuch Cyberkriminologie, Springer VS, Wiesbaden 2022, S. 1-24.

Fengler 2023: Fengler, Denis: Intelligente Videobeobachtung: Hamburger Polizei lässt Bewegungen von künstlicher Intelligenz auslesen, welt.de, Berlin 1. Juli 2023. Online: https://www.welt.de/regionales/hamburg/article246144998/Intelligente-Videobeobachtung-Hamburger-Polizei-laesst-Bewegungen-von-kuenstlicher-Intelligenz-auslesen.html.

Fichter & Wüstholz 2020: Fichter, Adrienne und Wüstholz, Florian: Die Polizei weiss, was Sie morgen vielleicht tun werden, Republik, Zürich 11. Dezember 2020. Online: https://www.republik.ch/2020/12/11/die-polizei-weiss-was-sie-morgen-vielleicht-tun-werden.

Fleig 2023: Fleig, Jürgen: So wird eine SWOT-Analyse erstellt, business-wissen.de, Karlsruhe 2023. Online: https://www.business-wissen.de/artikel/swot-analyse-so-wird-eine-swot-analyse-erstellt/.

Flügge & Fromm 2016: Flügge, Matthias und Fromm, Jens: Public IoT - Das Internet der Dinge im öffentlichen Raum, Fraunhofer FOKUS, Berlin 2016.

Frevel 2018: Frevel, Bernhard: Innere Sicherheit: Eine Einführung, Springer Fachmedien, Wiesbaden 2018.

Fritz 2020: Fritz, Sebastian: Big Data, Smart Government, Smart Policing – Perspektiven einer Smarten Polizeiarbeit, epubli GmbH, Berlin 2020.

Fuhrmann 2024: Fuhrmann, Marvin: Polizisten sollen Bodycam-Aufnahmen per KI auswerten – doch das könnte für Probleme sorgen, T3n – Digital Pioneers, Hannover 24. April 2024. Online: https://t3n.de/news/polizisten-ki-bodycam-aufnahmen-1620905/.

Gadorosi & Matthey 2023: Gadorosi, Holger und Matthey, Susanne: Auf dem Weg zu einer digitalen und vernetzten Polizei – P20, in: Dieter Wehe und Helmut Siller (Hrsg.): Handbuch Polizeimanagement, Springer Gabler, Wiesbaden 2023, S. 1411–1429.

Geuther & Metzner 2017: Geuther, Gudula und Metzner, Mathias: Grundrechte in anderen Verfassungen, Bundeszentrale für politische Bildung, Bonn 9. August 2017. Online: https://www.bpb.de/shop/zeitschriften/izpb/grundrechte-305/254039/grundrechte-in-anderen-verfassungen/.

Giessing & Frenkel 2022: Giessing, Laura und Frenkel, Marie Ottilie: Virtuelle Realität als vielversprechende Ergänzung im polizeilichen Einsatztraining – Chancen, Grenzen und Implementationsmöglichkeiten, in: Mario Staller und Swen Koerner (Hrsg.): Handbuch Polizeiliches Einsatztraining, Springer Gabler, Wiesbaden 2022, S. 677–692.

Glaser 2023: Glaser, Bettina: Wie Drohnen Einsatzkräfte im Verkehrsalltag unterstützen. Auto- und Reiseclub Deutschland e. V. (ARCD), Bad Windsheim 13. April 2023. Online: https://www.arcd.de/magazin/verkehrssicherheit/drohnen-im-verkehrsalltag/.

Gläser & Laudel 2010: Gläser, Jochen und Laudel, Grit: Experteninterviews und qualitative Inhaltsanalyse, VS Verlag für Sozialwissenschaften, Wiesbaden 2010.

Goitowski et al. 2022: Goitowski, Stefan; Hein, Tabea; Lorenz, Alina; Klingel, Anita; Renfer, Jürgen; Rensmann, Benjamin; … Wirth, Markus: Umsetzung der KI-Verordnung der EU in Deutschland, NExT e. V., Berlin 2022. Online: https://next-netz.de/wp-content/uploads/2022/05/NExTwerkstatt-KI-Verordnung-der-EU-CC-BY-NC-40.pdf.

Golda et al. 2023: Golda, Thomas; Cormier, Mickael und Beyerer, Jürgen: Intelligente Bild- und Videoauswertung für die Sicherheit, in: Dieter Wehe und Helmut Siller (Hrsg.): Handbuch Polizeimanagement, Springer Gabler, Wiesbaden 2023, S. 1487–1507.

Goldacker 2017: Goldacker, Gabriele: Digitale Souveränität, Fraunhofer FOKUS, Berlin 2017.

Golla 2019: Golla, Sebastian: Missbrauch polizeilicher Informationssysteme: Neugier und Datenkriminalität, Legal Tribune Online, Hürth 16.August 2019. Online: https://www.lto.de/recht/hintergruende/h/polizei-datenbanken-missbrauch-datenkriminalitaet-abfragen-daten-schutz.

Golla 2020: Golla, Sebastian: Lernfähige Systeme, lernfähiges Polizeirecht, Kriminologisches Journal, Weinheim 2020, Bd. 52, 2, S. 149–161.

Greis 2024: Greis, Friedhelm: Gesichtserkennung: Keiner weiß, wie es funktionieren soll, golem.de, Berlin 24. September 2024.
Online: https://www.golem.de/news/gesichtserkennung-keiner-weiss-wie-es-funktionieren-soll-2409-189222.html.

Groß 2012: Groß, Hermann: Polizeien in Deutschland, Bundeszentrale für politische Bildung, Bonn 14. Juni 2012. Online: https://www.bpb.de/themen/innere-sicherheit/dossier-innere-sicherheit/76660/polizeien-in-deutschland/.

Gruber 2018: Gruber, Angela: Gesichtserkennung am Südkreuz: Überwachung soll ausgeweitet werden, Spiegel Online, Berlin 12. Oktober 2018. Online: https://www.spiegel.de/netzwelt/netzpolitik/berlin-gesichtserkennung-am-suedkreuz-ueberwachung-soll-ausgeweitet-werden-a-1232878.html.

Gusy 2014: Gusy, Christoph: Aufklärungsdrohnen im Polizeieinsatz: Grundgesetzliche Vorgaben und Grenzen beim präventiv-polizeilichen Einsatz von Drohnen, Die Kriminalpolizei - Zeitschrift der Gewerkschaft der Polizei, Berlin März 2014. Online: https://www.kriminalpolizei.de/ausgaben/2014/maerz/detailansicht-maerz/artikel/aufklaerungsdrohnen-im-polizeieinsatz.html.

Hegemann 2022: Hegemann, Jan-Erik: Roboter-Hund erkundet Brandruine, Feuerwehr-Magazin, Bremen 23. Februar 2022. Online: https://www.feuerwehrmagazin.de/nachrichten/roboter-hund-erkundet-brandruine-113412.

Heitmüller 2023: Heitmüller, Ulrike: Missing Link: Digitale Polizei – in München steht ein Holodeck, Heike Online, Hannover 6. August 2023. Online: https://www.heise.de/hintergrund/Missing-Link-Digitale-Polizei-in-Muenchen-steht-ein-Holodeck-9235487.html?seite=all.

Hellenthal & Wellershoff 2022: Hellenthal, Markus und Wellershoff, Sascha: Sichere Kommunikation für BOS: Gefahrenvorsorge und Ermittlungsarbeit stecken im Digital-Dilemma, eGovernment, Augsburg 7. Juli 2022. Online: https://www.egovernment.de/gefahrenvorsorge-und-ermittlungsarbeit-stecken-im-digital-dilemma-a-9c8a1a190dfe4451638e55420f4551a2/.

Holland 2023: Holland, Martin: 3D- und 4D-Effekte: Polizei von NRW soll künftig in VR-Umgebung trainieren, Heise Online, Hannover 10. Juli 2023. Online: https://www.heise.de/news/Die-Polizei-in-NRW-soll-kuenftig-auch-in-VR-Umgebung-trainieren-9211275.html.

Hornung & Schindler 2017: Hornung, Gerrit und Schindler, Stephan: Das biometrische Auge der Polizei. Rechtsfragen des Einsatzes von Videoüberwachung mit biometrischer Gesichtserkennung, Zeitschrift Für Datenschutz, München 2017, Bd. 2017, 5, S. 203–209.

Hub 2021: Hub, Ralph: "Precobs" gescheitert: Der digitale Polizist ist ein Flop, Abendzeitung München, München 27. Oktober 2021. Online: https://www.abendzeitung-muenchen.de/muenchen/precobs-gescheitert-der-digitale-polizist-ist-ein-flop-art-766671.

Huber 2022: Huber, Moritz: Smart Security: konzeptionelle Ansätze für intelligent vernetzte Sicherheitslösungen und eine urbane Sicherheitsstrategie 4.0., Nomos, Baden-Baden 2022.

Hummelsheim-Doss 2017: Hummelsheim-Doss, Dina: Objektive und subjektive Sicherheit in Deutschland, Bundeszentrale für politische Bildung, Bonn 4. August 2017. Online: https://www.bpb.de/shop/zeitschriften/apuz/253609/objektive-und-subjektive-sicherheit-in-deutschland/.

Irnich 2021: Irnich, Bastian: Präventiv polizeilicher Einsatz von Drohnen: Aktuelle Fragen des Polizeirechts unter besonderer Berücksichtigung der Covid-19-Pandemie, KSV Polizeipraxis, Wiesbaden 25. März 2021. Online: https://ksv-polizeipraxis.de/praeventiv-polizeilicher-einsatz-von-drohnen/.

Kaiser 2014: Kaiser, Robert: Qualitative Experteninterviews: Konzeptionelle Grundlagen und praktische Durchführung, Springer VS, Wiesbaden 2014.

Kelber 2024: Kelber, Ulrich: Stellungnahme des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit zur öffentlichen Anhörung des Innen-ausschusses des Deutschen Bundestags am 22. April 2024: Handlungsfähigkeit der Strafverfolgungsbehörden sichern – Entscheidung des Bundesministeriums des Innern und für Heimat bezüglich der polizeilichen Analyse-Software Bundes-VeRA revidieren (BT-Drs. 20/9495), Deutscher Bundestag, Berlin 2024. Online: https://www.bundestag.de/resource/blob/999052/89b9c46f0d68547c21bed3336816e940/20-4-418-A.pdf.

Kerner 2018: Kerner, Hans-Jürgen: Entwicklung der Kriminalprävention in Deutschland, in: Maria Walsh, Benjamin Pniewski, Marcus Kober und Andreas Armborst (Hrsg.): Evidenzorientierte Kriminalprävention in Deutschland, Springer VS, Wiesbaden 2018, S. 21–36.

Kessel 2023: Kessel, Wolfgang: Pilotprojekt Videoüberwachung mit KI in Mannheim: Verlängerung bis 2026, SWR.de, Stuttgart 4. Dezember 2023. Online: https://www.swr.de/swraktuell/baden-wuerttemberg/mannheim/videoueberwachung-kameras-videoschutz-polizei-mannheim-innenstadt-sicherheit-strobl-100.html.

Kipker 2017: Kipker, Dennis-Kenji: Transparenzanforderungen an den Einsatz polizeilicher „Body-Cams", Datenschutz Und Datensicherheit - DuD, Wiesbaden 2017, Bd. 41, 3, S. 165–168.

Kipker 2024: Kipker, Dennis-Kenji: Schriftliche Stellungnahme Entwurf eines Gesetzes zur Verbesserung der Terrorismusbekämpfung (BT-Drucksache 20/12806), Institut für Informations-, Gesundheits- und Medizinrecht (IGMR), Bremen 2024. Online: https://intrapol.org/wp-content/uploads/2024/09/Dennis-Kenji-Kipker-Stellungnahme-BT-Drs-2012806.pdf.

Kirchner 2022: Kirchner, Malte: Abstandskontrolle von oben: Polizeidrohne überführt drängelnde LKWs auf der A2, Heise Online, Hannover 7. Juli 2022. Online:

https://www.heise.de/news/Abstandskontrolle-von-oben-Polizeidrohne-ueberfuehrt-draengelnde-LKWs-auf-der-A2-7165517.html.

Klein 2024: Klein, Oliver: Warum Polizei RAF-Terroristin Klette nicht eher aufspürte, ZDFheute, Mainz 29. Februar 2024. Online: https://www.zdf.de/nachrichten/politik/deutschland/daniela-klette-verhaftung-gesichtserkennung-pimeyes-100.html.

Kleygrewe et al. 2024: Kleygrewe, Lisanne; Hutter, R. I.Vana; Koedijk, Matthijs; Oudejans, Raôul R.D.: Virtual reality training for police officers: a comparison of training responses in VR and real-life training, Police Practice and Research, Police Practice and Research, Amsterdam 2024, Bd. 25, 1, S. 18-37.

Knobloch 2018: Knobloch, Tobias: Vor die Lage kommen: Predictive Policing in Deutschland, Bertelsmann Stiftung, Gütersloh 2018. Online: https://www.bertelsmann-stiftung.de/fileadmin/files/BSt/Publikationen/GrauePublikationen/predictive.policing.pdf.

Knoll & Stieglitz 2022: Knoll, Matthias und Stieglitz, Stefan: Augmented Reality und Virtual Reality– Einsatz im Kontext von Arbeit, Forschung und Lehre, HMD Praxis der Wirtschaftsinformatik, Wiesbaden 2022, Bd. 59, 1, S. 6-22.

Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder 2019: Positionspapier der DSK zu empfohlenen technischen und organisatorischen Maßnahmen bei der Entwicklung und dem Betrieb von KI-Systemen. Online: https://www.datenschutzkonferenz-online.de/media/en/20191106_positionspapier_kuenstliche_intelligenz.pdf.

Koppers & Weidling 2021: Koppers, Margarete und Weidling, Matthias: Verhältnis der Staatsanwaltschaft zur Polizei, in: Ralf Peter Anders, Kirsten Graalmann-Scheerer und Jan Henrik Schady (Hrsg.): Innovative Entwicklungen in den deutschen Staatsanwaltschaften, Springer, Wiesbaden 2021, S. 73-91.

Krameyer 2022: Krameyer, Christof: Wie die Polizei dank künftiger Einsatzleitsysteme schneller am Unfallort ist und intelligenter Verbrecher jagt, CGI Deutschland, Leinfelden-Echterdingen 11. Januar 2022. Online: https://www.cgi.com/de/de/blog/public-services/wie-die-polizei-dank-kuenftiger-einsatzleitsysteme-schneller-am-unfallort-ist.

Krempl 2021: Krempl, Stefan: EU-Cloud: Gaia-X-Allianz begrüßt Palantir, Huawei, Alibaba & Co. als Mitglieder, Heise Online, Hannover 5. April 2021. Online: https://www.heise.de/news/EU-Cloud-Gaia-X-Allianz-begruesst-Palantir-Huawei-Alibaba-Co-als-Mitglieder-6005511.html.

Krempl 2023: Krempl, Stefan: "Halbgar": KI-Verordnung öffnet Hintertüren für biometrische Massenüberwachung, Heise Online, Hannover 9. Dezember 2023. Online: https://www.heise.de/news/Halbgar-KI-Verordnung-oeffnet-Hintertueren-fuer-biometrische-Massenueberwachung-9569614.html.

Krempl 2024: Krempl, Stefan: Bundesregierung: IT-Großprojekt Polizei 2020 kommt langsam, aber stetig voran, Heise Online, Hannover 30. Oktober 2024. Online: https://www.heise.de/news/Bundesregierung-IT-Grossprojekt-Polizei-2020-kommt-langsam-aber-stetig-voran-10000320.html.

Kugelmann 2012: Kugelmann, Dieter: Rahmenbedingungen des Polizei- und Ordnungsrechts, in: Polizei- und Ordnungsrecht, Springer Berlin, Heidelberg 2012, S. 1-11.

Kurz 2023: Kurz, Constanze: Automatisierte Datenanalyse: Der Wilde Westen beim Data-Mining der Polizei ist vorbei. Netzpolitik.org, Berlin 16. Februar 2023. Online: https://netzpolitik.org/2023/automatisierte-datenanalyse-der-wilde-westen-beim-data-mining-der-polizei-ist-vorbei/.

Kurz 2024a: Kurz, Constanze: Automatisierte Datenanalyse bei der Polizei: Bundesländer nicht scharf auf Palantir, Netzpolitik.org, Berlin 3. Januar 2024. Online: https://netzpolitik.org/2024/automatisierte-datenanalyse-bei-der-polizei-bundeslaender-nicht-scharf-auf-palantir/.

Kurz 2024b: Kurz, Constanze: Automatisierte Polizeidatenanalyse: Bayern testet rechtswidrig Palantir-Software, Netzpolitik.org, Berlin 24. Januar 2024. Online: https://netzpolitik.org/2024/automatisierte-polizeidatenanalyse-bayern-testet-rechtswidrig-palantir-software/.

Laoyan 2024: Laoyan, Sarah: Das Pareto-Prinzip: So einfach funktioniert die 80-20 Regel!, Asana, San Francisco 2024. Online: https://asana.com/de/resources/pareto-principle-80-20-rule.

Landesregierung Baden-Württemberg 2023a: Roboter-Hund „Spot" an die Polizei übergeben, Pressemitteilung, Stuttgart 28. April 2023. Online: https://www.baden-wuerttemberg.de/de/service/presse/pressemitteilung/pid/roboter-hund-spot-an-die-polizei-uebergeben.

Landesregierung Baden-Württemberg 2023b: Polizei will Innovationsplattform für KI unterstützen, Pressemitteilung, Stuttgart 19. Dezember 2023. Online: https://www.baden-wuerttemberg.de/de/service/presse/pressemitteilung/pid/polizei-will-innovationsplattform-fuer-ki-unterstuetzen.

Lasserre 2024: Lasserre, Pascal: Leitstelle Ludwigshafen: Notruf mit Künstlicher Intelligenz, SWR Aktuell, Stuttgart 24. August 2024. Online:

https://www.swr.de/swraktuell/rheinland-pfalz/ludwigshafen/leitstelle-ludwigshafen-bei-notruf-kuenstliche-intelligenz-100.html.

Laude et al. 2023: Laude, Thorsten; Reinhardt, Carsten und Bomert, Christian: Einsatz von künstlicher Intelligenz, Data Science und Big Data: Anwendungsbeispiele zur Bewältigung von Massendaten in der niedersächsischen Polizei, in: Dieter Wehe und Helmut Siller (Hrsg.): Handbuch Polizeimanagement, Springer Gabler, Wiesbaden 2023, S. 1509–1529.

Mahnke 2024: Mahnke, Lars: Fluch und Segen der KI – BKA-Herbsttagung in Wiesbaden, Behörden Spiegel, Bonn 29. November 2024. Online: https://www.behoerden-spiegel.de/2024/11/29/fluch-und-segen-der-ki-bka-herbsttagung-in-wiesbaden/.

Mann 2014: Mann, Thomas: „Freiheit in Sicherheit" – Grundrechte als Schutzgut und Barriere im Polizei- und Ordnungsrecht, in: Eötvös Loránd Universität Budapest (Hrsg.): Annales Universitatis Scientiarum Budapestinensis - Sectio Iuridica, Budapest 2014, S. 105-117.

Martini & Botta 2024: Martini, Mario und Botta, Jonas: Nationale KI-Aufsicht-Aufgaben, Befugnisse und Umsetzungsoptionen, Bertelsmann-Stiftung, Gütersloh 2024. Online: https://www.bertelsmann-stiftung.de/fileadmin/files/PicturePark/2024-05/Nationale_KI-Aufsicht_2024_final.pdf.

MDR Thüringen 2023: Acht Polizeidrohnen in Thüringen angeschafft, mdr.de, Leipzig, 19.August 2023. Online: https://www.mdr.de/nachrichten/thueringen/polizei-drohnen-kauf-100.html.

Metzner 2017: Metzner, Mathias: Schutz der Menschenwürde, Bundeszentrale für politische Bildung, Bonn 15. August 2017. Online: https://www.bpb.de/shop/zeitschriften/izpb/grundrechte-305/254383/schutz-der-menschenwuerde/.

Michel 2024: Michel, Ralf: Polizei Bremen nutzt Drohnen, die auf Schwarzer Liste der USA stehen, Weser Kurier, Bremen 18. Januar 2024. Online: https://www.weser-kurier.de/bremen/politik/polizei-bremen-nutzt-drohnen-die-auf-schwarzer-liste-der-usa-stehen-doc7tr6w3dplfn1h7p03l8m.

Ministerium des Inneren, für Digitalisierung und Kommunen Baden-Württemberg 2023: Innere Sicherheit: Aktionsplan „Mehr Sicherheit für Mannheim", Pressemitteilung, Stuttgart 4. Dezember 2023. Online: https://im.baden-wuerttemberg.de/de/service/presse-und-oeffentlichkeitsarbeit/pressemitteilung/pid/aktionsplan-mehr-sicherheit-fuer-mannheim.

Müller & Köhl 2019: Müller, Heidrun und Köhl, Stefanie: Sicherheitsanforderungen und -nachweise bei Cloud-Diensten- Grundlagen für öffentliche Auftraggeber, Nationales E-Government Kompetenzzentrum e. V., Berlin 2019. Online: https://negz.org/wp-content/uploads/2022/12/7_Kurzstudie_Sicherheitsanforderungen-Cloud-Dienste-2019.pdf.

Müller 2023: Müller, Ralf: Neue VR-Technik für die Polizei Bayern: Verbrecherjagd in 3D, Abendzeitung München, München 5. Juni 2023. Online: https://www.abendzeitung-muenchen.de/bayern/neue-vr-technik-fuer-die-polizei-bayern-verbrecherjagd-in-3d-art-906109.

Pansa 2023: Pansa, Sören: Von Hilfsbeamten und Ermittlungspersonen: Die Anordnungsbefugnis der Staatsanwaltschaft i.S.d. § 152 GVG, Die Kriminalpolizei - Zeitschrift der Gewerkschaft der Polizei, Berlin Juni 2023. Online: https://www.kriminalpolizei.de/ausgaben/2023/juni/detailansicht-juni/artikel/von-hilfsbeamten-und-ermittlungspersonen.html.

Papier 2011: Papier, Hans-Jürgen: Das Bundeskriminalamt im Fokus – verfassungsrechtliche Entwicklungslinien und Diskurse im Spannungsfeld zwischen Freiheit und Sicherheit, BKA-Herbsttagung, Wiesbaden 2011, S. 1–16. Online: https://www.polizei.de/SharedDocs/Downloads/DE/Publikationen/Herbsttagungen/2011/herbsttagung2011PapierLangfassung.html.

Peglow 2024: Peglow, Dirk: Stellungnahme des Bund Deutscher Kriminalbeamter e.V. (BDK) zum Antrag der Fraktion CDU/CSU Handlungsfähigkeit der Strafverfolgungsbehörden sichern – Entscheidung des Bundesministeriums des Innern und für Heimat bezüglich der polizeilichen Analyse- Software Bundes-VeRA revidieren, Drucksache 20/9495, Deutscher Bundestag, Berlin 2024. Online: https://www.bundestag.de/resource/blob/999090/8bc101466ac35051f44a58ff2e7ae528/20-4-418-l.pdf.

Perry et al. 2013: Perry, Walter; McInnis, Brian; Price, Carter; Smith, Susan und Hollywood, John: Predictive Policing: The Role of Crime Forecasting in Law Enforcement Operations, RAND Corporation, Santa Monica 2013.

Plazek 2016: Plazek, Michael: Big Data: Große Chancen für den öffentlichen Sektor?, Public Governance, Ausgabe Herbst 2016, Berlin 2016, S. 6-11. Online: https://publicgovernance.de/media/PG_Herbst2016_Schwerpunkt_BigData.pdf.

Polizei Hessen 2022: Smartphone-Apps machen die Polizeiarbeit schneller: Die „Mobile-IT"-Projektleiter Marcel Schmidt und Tristan Münz im Interview, INNOVATION HUB 110, Wiesbaden 11. Februar 2022. Online: https://www.polizei.hessen.de/icc/internetzentral/nav/9a4/broker.jsp?uCon=db8404f3

-c716-ee71-505e-78150e44dfc9&uTem=bff71055-bb1d-50f1-2860-72700266cb59&uMen=9a47f8e0-f4b3-8712-6bda-13300b9ef7c4.

Polster & Labudde 2022: Polster, Heiko und Labudde, Dirk: Das Auto als forensischer Datenspeicher: Technische Hilfsmittel und Möglichkeiten einer forensischen Auswertung von Kfz-Elektroniksystemen, in: Sucky, Eric; Biethahn, Niels; Werner, Jan und Dobhan, Alexander (Hrsg.): Mobility in a Globalised World 2021, University of Bamberg Press, Bamberg 2022, S. 269–287.

Rat der Europäischen Union 2024: Gesetz über künstliche Intelligenz (KI): Rat gibt grünes Licht für weltweit erste KI-Vorschriften, Pressemitteilung, Brüssel 21. Mai 2024. Online: https://www.consilium.europa.eu/de/press/press-releases/2024/05/21/artificial-intelligence-ai-act-council-gives-final-green-light-to-the-first-worldwide-rules-on-ai/.

Rath 2024: Rath, Christian: Gesetzentwurf zur Gesichtserkennung lässt Fragen offen, Legal Tribune, Hürth 12. August 2024. Online: https://www.lto.de/recht/hintergruende/h/gesetzentwurf-zur-gesichtserkennung.

Reiberg et al. 2022: Reiberg, Abel; Niebel, Crispin und Kraemer, Peter: Was ist ein Datenraum?, White Paper, Nr. 1, Gaia-X Hub Germany, München 2022. Online: https://www.bmwk.de/Redaktion/DE/Publikationen/Digitale-Welt/whitepaper-definition-des-konzeptes-datenraum.pdf?__blob=publicationFile&v=6.

Reuter 2024: Reuter, Markus: Umstrittenes Gesetz: Ampel verkündet Einigung beim Überwachungspaket, Netzpolitik.org, Berlin 11. Oktober 2024. Online: https://netzpolitik.org/2024/umstrittenes-gesetz-ampel-verkuendet-einigung-beim-ueberwachungspaket/.

Rouse 2024: Rouse, Margaret: Black Box KI, Techopedia 2024. Online: https://www.techopedia.com/de/definition/black-box-ki.

Ruf 2024: Ruf, Simone: Stellungnahme der Gesellschaft für Freiheitsrechte (GFF) zu dem Antrag der Fraktion der CDU/CSU „Handlungsfähigkeit der Strafverfolgungsbehörden sichern – Entscheidung des Bundesministeriums des Innern und für Heimat bezüglich der polizeilichen Analyse-Software Bundes-VeRA revidieren“ (BT-Drs. 20/9495), Deutscher Bundestag, Berlin 2024. Online: https://www.bundestag.de/resource/blob/999074/e58c5b84d5056da493e47c3ffdf83dea/20-4-418-D.pdf.

Rzepka 2024: Rzepka, Dominik: Einigung zwischen CDU und SPD: Bundestagswahl soll am 23. Februar stattfinden. ZDFheute, Mainz 12. November 2024. Online: https://www.zdf.de/nachrichten/politik/deutschland/bundestagswahl-termin-februar-ampel-aus-neuwahl-100.html.

Schäberle 2023: Schäberle, Jürgen: IT-Projekte in der Polizei – Herausforderungen besonderer Art, in: Dieter Wehe und Helmut Siller (Hrsg.): Handbuch Polizeimanagement, Springer Gabler, Wiesbaden 2023, S. 1471-1486.

Schoch 2013: Schoch, Friedrich: Doppelfunktionale Maßnahmen der Polizei, JURA - Juristische Ausbildung, Berlin 2013, Bd. 35, 11, S. 1115–1123.

Schönfelder 2023: Schönfelder, Susann: Sicheres Public Viewing durch Drohnen: So setzt die Polizei sie ein, Südwest Presse, Ulm 17. Juli 2023. Online: https://www.swp.de/lokales/goeppingen/polizei-baden-wuerttemberg-hilfe-aus-der-luft_-wenn-drohnen-tatorte-inspizieren-71197947.html.

Seckelmann 2017: Seckelmann, Margrit: Body-Cams als „New Tools of Governance"?, in: Jörn von Lucke und Klaus Lenk (Hrsg.): Verwaltung, Informationstechnik & Management, Baden-Baden: Nomos Verlagsgesellschaft, Baden-Baden Januar 2017, S. 291–304.

Sorge 2024: Sorge, Christoph: Stellungnahme zum Entwurf eines Gesetzes zur Verbesserung der Inneren Sicherheit und des Asylsystems, BT-Drucksache 20/12805 sowie zum Entwurf eines Gesetzes zur Verbesserung der Terrorismusbekämpfung, BT-Drucksache 20/12806, Deutscher Bundestag Berlin 2024, Online: https://www.bundestag.de/resource/blob/1019996/34caffc9b50ac49f4ef42169a4d37144/20-4-493-M.pdf.

Steffen 2015: Steffen, Wiebke: Gutachten für den 19. Deutschen Präventionstag 12. & 13. Mai 2014 in Karlsruhe Prävention braucht Praxis, Politik und Wissenschaft, in: Erich Marks und Wiebke Steffen (Hrsg.): Prävention braucht Praxis, Politik und Wissenschaft-Ausgewählte Beiträge des 19. Deutschen Präventionstages 12. und 13. Mai 2014 in Karlsruhe, Forum Verlag Godesberg GmbH, Mönchengladbach 2015, S. 53–148.

Stock 2023: Stock, Oliver: Datafizierung, Cloudifizierung, Virtualisierung und KI: das polizeiliche Auftragsverständnis zur Verteidigung der Freiheit im digitalen Zeitalter, in: Dieter Wehe und Helmut Siller (Hrsg.): Handbuch Polizeimanagement, Springer Gabler, Wiesbaden 2023, S. 1445-1470.

Susanka 2023: Susanka, Sandra: Überwachung in Mannheim: Wenn Umarmungen wie Würgen aussehen, ZDFheute, Mainz 4. August 2023. Online: https://www.zdf.de/nachrichten/politik/deutschland/videoueberwachung-mannheim-pilotprojekt-polizei-100.html.

Tack 2019: Tack, Jochen: 20.000 Smartphones für die Polizei in Nordrhein-Westfalen werden ausgeliefert, Pressemitteilung Innenministerium NRW, Düsseldorf 9. September 2019. Online: https://polizei.nrw/presse/20000-smartphones-fuer-die-polizei-in-nordrhein-westfalen-werden-ausgeliefert.

Tagesschau 2024a: Massiver Hackerangriff auf niederländische Polizei, Hamburg 3. Oktober 2024. Online: https://www.tagesschau.de/ausland/europa/niederlande-polizei-hacker-100.html.

Tagesschau 2024b: "Sicherheitspaket" scheitert in Teilen am Bundesrat, Hamburg 18. Oktober 2024. Online: https://www.tagesschau.de/inland/innenpolitik/sicherheitspaket-im-bundesrat-gestoppt-100.html.

Teufele 2024: Teufele, Klaus: Stellungnahme Bayrisches Landeskriminalamt zum Antrag der Fraktion CDU/CSU: Handlungsfähigkeit der Strafverfolgungsbehörden sichern - Entscheidungen des Bundesministeriums des Innern und für Heimat bezüglich der polizeilichen Analyse-Software Bundes-VeRA revidieren (BT-Drucksache 20/9495), Deutscher Bundestag, Berlin 2024. Online: https://www.bundestag.de/resource/blob/999060/0901a13494e86ea12bda38076bb98698/20-4-418-B.pdf.

Vieth-Ditlmann & Sombetzki 2024a: Vieth-Ditlmann, Kilian und Sombetzki, Pia: Gesichtserkennung im „Sicherheitspaket": Koalition bricht ihr Versprechen im Schnellverfahren, algorithmwatch.org, Berlin 10. September 2024. Online: https://algorithmwatch.org/de/gesichtserkennung-sicherheitspaket/.

Vieth-Ditlmann & Sombetzki 2024b: Vieth-Ditlmann, Kilian und Sombetzki, Pia:. Stellungnahme /AlgorithmWatch zur öffentlichen Anhörung des Ausschuss für Digitales am 15. Mai 2024 zur nationalen Umsetzung der KI-Verordnung, Deutscher Bundestag, Berlin 2024. Online: https://algorithmwatch.org/de/wp-content/uploads/2024/05/240515_StellungnahmeAIA_ADi_algorithmwatch.pdf.

Volkmann 2022: Volkmann, Uwe: Zwischen individueller Freiheit und staatlicher Sicherheitsgewähr: Wandlungen des Rechtsstaats in unsicheren Zeiten, Bundeszentrale für politische Bildung, Bonn 5. August 2022. Online: https://www.bpb.de/shop/zeitschriften/apuz/freiheit-und-sicherheit-2022/511503/zwischen-individueller-freiheit-und-staatlicher-sicherheitsgewaehr/.

von der Burg et al. 2023: von der Burg, Léon; Ebenau, Johannes und Janssen, Jasper: Training in der Zukunft? Virtual Reality bei deutschen Polizeibehörden, Bürgerrechte & Polizei/CILIP, Berlin März 2023, Bd. 131, 1, S. 76-87.

von Lucke 2015: von Lucke, Jörn: Smart Government - Wie uns die intelligente Vernetzung zum Leitbild "Verwaltung 4.0" und einem smarten Regierungs- und Verwaltungshandeln führt, The Open Government Institute Whitepaper, Friedrichshafen 2015.

von Lucke 2016: von Lucke, Jörn: Deutschland auf dem Weg zum Smart Government - Was Staat und Verwaltung von der vierten industriellen Revolution,

von Disruptionen, vom Internet der Dinge und dem Internet der Dienste zu erwarten haben, Verwaltung & Management, Bd. 22, 4, Nomos, Baden-Baden 2016, S. 171-186.

von Lucke 2018: von Lucke, Jörn: Vom Smart Government zum Real-Time Government, Innovative Verwaltung, Bd. 40, 9, Springer Gabler, Wiesbaden 2018, S. 10–13.

von Lucke 2020: von Lucke, Jörn: Wie smart darf Polizeiarbeit eigentlich werden? Verwaltung & Management, Bd. 26, 3, Nomos, Baden-Baden 2020, S. 107–124.

von Lucke 2024: von Lucke, Jörn: KI-Technologien und ihre Auswirkungen auf die Verwaltungsarbeit, PDV NEWS, Bd. 20, 1, PDV GmbH, Erfurt 2024, S. 9-11.

Wagner 2024: Wagner, Roland: Stellungnahme Antrag der CDU/CSU-Bundestagsfraktion: „Handlungsfähigkeit der Strafverfolgungsbehörden sichern - Entscheidung des Bundesministeriums des Inneren und für Heimat bezüglich der polizeilichen Analyse-Software Bundes-VeRA revidieren“ (20/9495), Deutscher Bundestag, Berlin 2024. Online: https://www.bundestag.de/resource/blob/999068/56d49caa4b09129db7cddab4980ff83c/20-4-418-C.pdf.

Weiz 2023: Weiz, Bettina: Gesichtserkennung & Co: EU einigt sich auf welterstes KI-Gesetz, BR24, München 9. Dezember 2023.
Online: https://www.br.de/nachrichten/bayern/gesichtserkennung-and-co-eu-einigt-sich-auf-welterstes-ki-gesetz,TxurybR.

Wissenschaftliche Dienste des Deutschen Bundestages 2021: Sachstand Verarbeitung personenbezogener Daten durch die Polizei Rechtsgrundlage in den deutschen Nachbarländern, Deutscher Bundestag, Berlin 2021. Online: https://www.bundestag.de/resource/blob/870378/d19944dc96a88e7f9281c62581fd58a1/WD-3-162-21-pdf.pdf.

Wissenschaftliche Dienste des Deutschen Bundestages 2017: Vergleich ausgewählter präventivpolizeilicher Standardmaßnahmen im Recht des Bundes und der Länder, Deutscher Bundestag, Berlin 2017. Online: https://www.bundestag.de/resource/blob/503044/.../wd-3-020-17-pdf-data.pdf.

Wissenschaftliche Dienste des Deutschen Bundestages 2021: Ausarbeitung zum staatlichen Einsatz von Drohnen bei Versammlungen, Deutscher Bundestag, Berlin 2021. Online: https://www.bundestag.de/resource/blob/836412/c319203d3d2f57778b340f50c3115370/WD-3-036-21-pdf.pdf.

Wolf-Engels 2024: Wolf-Engels, Benjamin: KI-Befähigung für die Verwaltung: Worauf kommt es an?, Public Governance, Ausgabe Sommer 2024, Berlin 2024, S. 4-7. Online: https://publicgovernance.de/media/PG_Sommer_2024_KI_Befaehigung_fuer_die_Verwaltung.pdf.

Wollny & Paul 2015: Wollny, Volrad und Paul, Herbert: Die SWOT-Analyse: Herausforderungen der Nutzung in den Sozialwissenschaften, in: Marlen Niederberger und Sandra Wassermann (Hrsg.): Methoden der Experten- und Stakeholdereinbindung in der sozialwissenschaftlichen Forschung, Springer VS, Wiesbaden 2015, S. 189–213).

Zand-Vakili 2020: Zand-Vakili, André: Drohnen-Offensive bei der Hamburger Polizei, Hamburger Abendblatt, Hamburg 28. Juli 2020.
Online: https://www.abendblatt.de/hamburg/article229606896/Drohnen-Hamburger-Polizei-Unbemannte-Fluggeraete-Fahndung-Kriminalitaet.html.

Zink et al. 2022: Zink, Wolfgang; Heinzelmann, Patrick; Ridderbusch, Marnie; Schulte, Nils: Vertrauen, Präsenz und digitale Kompetenz – Wie sieht die Öffentlichkeit in Deutschland ihre Polizei?, PricewaterhouseCoopers GmbH Wirtschaftsprüfungsgesellschaft, Frankfurt a.M. 2022.
Online: https://pages.pwc.de/studie-vertrauen-in-die-polizei?utm_source=linkedin&utm_medium=social&utm_campaign=public_services&utm_id=7014L000000YJnkQAG.

Verzeichnis der zitierten Richtlinien und Gesetze

Bundesdatenschutzgesetz (BDSG) vom 30. Juni 2017 (BGBl. I S. 2097), das zuletzt durch Artikel 7 des Gesetzes vom 6. Mai 2024 (BGBl. 2024 I Nr. 149) geändert worden ist.

Datenschutzgrundverordnung (DSGVO)): Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG.

Grundgesetz für die Bundesrepublik Deutschland (GG) in der im Bundesgesetzblatt Teil III, Gliederungsnummer 100-1, veröffentlichten bereinigten Fassung, das zuletzt durch Artikel 1 des Gesetzes vom 20. Dezember 2024 (BGBl. 2024 I Nr. 439) geändert worden ist.

JI-Richtlinie: Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates.

Polizeigesetz (PolG) des Landes Baden-Württemberg vom 6. Oktober 2020 (GBl. 2020, 735, ber. S. 1092).

Verordnung über künstliche Intelligenz (KI-VO): Verordnung (EU) 2024/1689 des Europäischen Parlaments und des Rates vom 13. Juni 2024 zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz und zur Änderung der Verordnungen (EG) Nr. 300/2008, (EU) Nr. 167/2013, (EU) Nr. 168/2013, (EU) 2018/858, (EU) 2018/1139 und (EU) 2019/2144 sowie der Richtlinien 2014/90/EU, (EU) 2016/797 und (EU) 2020/1828.