Mit der Master Thesis von Sebastian Fritz liefert Band 19 der TOGI-Schriftenreihe einen Überblick zum derzeitigen Stand der Smarten Polizeiarbeit. Fritz analysiert die künftigen Chancen, Risiken und Herausforderungen. Dabei stellt er aktuelle Konzepte sowie Technologien und Anwendungen der Smarten Polizeiarbeit vor. Basierend auf den Einschätzungen aus 8 Experteninterviews werden die derzeitigen Ausprägungen einer Smarten Polizeiarbeit eingeordnet sowie Perspektiven und Visionen aufgezeigt. Abschließend werden Handlungsempfehlungen abgeleitet.

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: http://togi.zu.de

ISSN 2193-8946
ISBN 978-3-750277-35-9

zeppelin universität

The
Open Government Institute |TOGI

Big Data
Smart Government
Smart Policing

Perspektiven einer Smarten Polizeiarbeit

**Monographie am
The Open Government Institute |TOGI
der Zeppelin Universität**

ZU |TOGI

Band 19 der Schriftenreihe des
The Open Government Institute |TOGI
der Zeppelin Universität Friedrichshafen

zeppelin universität

The Open Government Institute | TOGI

Sebastian Fritz

Big Data
Smart Government
Smart Policing

Perspektiven einer Smarten Polizeiarbeit

Monographie am
The Open Government Institute | TOGI
der Zeppelin Universität

TOGI Schriftenreihe - Band 19

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

The Open Government Institute | TOGI
TOGI Schriftenreihe

Band 19

Herausgeber von Band 19

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

Herausgeber der TOGI Schriftenreihe

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

Impressum

Druck und Verlag: epubli GmbH, Berlin, http://www.epubli.de
Verlagsgruppe Holtzbrinck
ISBN 978-3-750277-35-9
ISSN 2193-8946

Vorwort

Unsere Sicherheitsbehörden sorgen auf Grundlage des staatlichen Gewaltmonopols für die öffentliche Sicherheit und Ordnung. In Deutschland gehören zu diesen Behörden die Bundespolizei (grenz- und bahnpolizeiliche Aufgaben), das Bundeskriminalamt, die Polizei beim Deutschen Bundestag, die Länderpolizei (mit Landespolizei, Bereitschaftspolizei, Landeskriminalamt, Polizeiverwaltungsämtern und polizeilichen Aus- und Fortbildungsstätten) sowie ergänzend die kommunale Vollzugspolizei.

Intelligent vernetzte Objekte wie Smartphones und Tablets, Überwachungskameras und Polizeidrohnen, smarte Uhren und smarte Uniformen werden die Sicherheitsbehörden künftig bei der Wahrnehmung ihrer Aufgaben unterstützen, indem sie Einsatzkräfte über Standorte, Einsätze und die Rahmenbedingungen informieren. Smarte Polizeibrillen und smarte Polizeihelme bringen relevante Informationen zur Person oder zum Objekt in das Blickfeld des Beamten. Diese können so Gefahrenlagen und geeignete Vorgehensweisen besser einschätzen und bewerten. Body-Cams und Fahrzeugkameras dokumentieren Eingriffe der Polizei. Diese Transparenz sichert einen fairen Umgang bei der Durchsetzung staatlicher Gewalt und schützt Einsatzkräfte in Fällen von Eskalation. Diverse Datenquellen, zum Teil sensorbasiert und in Echtzeit generiert, tragen künftig zu einem umfangreichen Gesamtlagebild in den Polizeiwachen und Einsatzzentralen bei, die sich durch visualisierte Cockpits und Dashboards ganz anders steuern lassen werden.

Diese ersten, im Jahr 2016 am The Open Government Institute der Zeppelin Universität entwickelten und mit unseren Studenten diskutierten Vorstellungen über den Einsatz von smarten Objekten und cyberphysischen Systemen in der Polizei weckten den Ehrgeiz meines Studenten Sebastian Fritz. Im Dezember 2017 kam er auf mich zu, als er Ausschau nach einem spannungsreichen Themenfeld für seine anstehende Master-Thesis hielt. Vor allem beschäftigte ihn die Frage, wie Smarte Polizeiarbeit aussehen soll, welche Konsequenzen sich daraus ableiten und wie sich diese Entwicklung mit Freiheit, Sicherheit und Überwachung vertragen wird.

Heute freut es mich, nach Vorlage der sehr guten Abschlussarbeit, der mündlichen Prüfung und der Auszeichnung als Best Master Thesis Award

der Zeppelin Universität im Studiengang PAIR, die Arbeit als 19. Band in der TOGI-Schriftenreihe veröffentlichen zu dürfen. Der Dank gilt an dieser Stelle auch Herrn Michael Meyer-Schaudwet für die Zweitbetreuung der Thesis sowie den Experten, die sich die Zeit für die Interviews nahmen.

Die vorgelegte Masterarbeit ist das Ergebnis einer intensiven Auseinandersetzung mit den Möglichkeiten einer Smarten Polizeiarbeit, unter maßgeblicher Einbindung von acht Experten aus dem Umfeld der Polizei und Polizeiinformatik. Auf Basis von Literaturrecherchen und Experteninterviews definiert, skizziert und analysiert Sebastian Fritz die Möglichkeiten für die Polizei und ihr Handeln, wenn sie sich moderner Informations- und Kommunikationstechnologien, insbesondere smarter Technologien, bedient. Dazu führte er im Frühjahr 2018 acht Experteninterviews und eine Dokumentenanalyse durch, die er darstellt, diskutiert und aus der er Handlungsempfehlungen ableitet. Sebastian Fritz hat sich sehr intensiv mit Big Data, smarten Objekten, cyberphysischen Systemen und ihren Entwicklungsmöglichkeiten bei den Polizeien in Deutschland auseinandergesetzt. Ein großes Interesse an dieser Thematik besteht bei der Bundes- und Landespolizei in Deutschland, denn es handelt sich für diese vielfach noch um „Neuland". Polizeibehörden eröffnen sich zahlreiche Konsolidierungspotentiale. Diese fachliche Aufbereitung kann als gelungen gelten. Herr Fritz hat das Themenfeld theoretisch fundiert, die Methodik des Experteninterviews sauber dargestellt und wertvolle Impulse generiert. Insgesamt überzeugt das Werk durch seine Inhalte, die kritische Auseinandersetzung mit der bestehenden Agenda, geeigneten Handlungsempfehlungen, Klarheit und Verständlichkeit. Für den interessierten Leser bringt diese Veröffentlichung echte Mehrwerte, da sie wertvolle Impulse und substantielle Kritik zur Weiterentwicklung von smarter Polizeiarbeit beinhaltet.

Friedrichshafen, der 31. Januar 2020

Jörn von Lucke

Zusammenfassung

Die Arbeit liefert einen Überblick zum derzeitigen Stand der Smarten Polizeiarbeit und analysiert die zukünftigen Chancen, Risiken und Herausforderungen. Als theoretische Grundlage dient hierfür vorrangig der Ansatz des intelligent vernetzten Regierungs- und Verwaltungshandelns (Smart Government). Dabei werden in einem ersten Schritt aktuelle Konzepte sowie Technologien und Anwendungen der Smarten Polizeiarbeit vorgestellt. Basierend auf den Einschätzungen aus acht Experteninterviews werden anschließend die derzeitigen Ausprägungen einer Smarten Polizeiarbeit eingeordnet sowie zukünftige Perspektiven und Visionen aufgezeigt. Abschließend werden auf Grundlage der erarbeiteten Ergebnisse Handlungsempfehlungen abgeleitet.

Abstract

This paper provides an overview on the current state of Smart Policing and analyses the future opportunities, risks and challenges. As the theoretical basis for this analysis primarily serves the approach of intelligently-networked government and administrative actions (Smart Government). In a first step, current concepts as well as technologies and applications of Smart Policing will be presented. Based on the assessments of eight expert interviews, the current characteristics of Smart Policing are then classified and future perspectives and visions are presented. Finally, recommendations for action are derived on the basis of the obtained results.

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

Abkürzungsverzeichnis

Abs.	Absatz
AR	Augmented Reality
Art.	Artikel
BfV	Bundesamt für Verfassungsschutz
BND	Bundesnachrichtendienst
BKA	Bundeskriminalamt
BMI	Bundesministerium des Innern, für Bau und Heimat
BMVI	Bundesministerium für Verkehr und digitale Infrastruktur
BPOL	Bundespolizei
BVerfG	Bundesverfassungsgericht
CDU	Christlich Demokratische Union
CSU	Christlich Soziale Union
CPS	Cyber-physisches System
E-Government	Electronic-Government
EUROPOL	Europäisches Polizeiamt
GdP	Gewerkschaft der Polizei
DPolG	Deutsche Polizeigewerkschaft
GG	Grundgesetz
G-20	Gruppe der 20 wichtigsten Industrie- und Schwellenländer
GPS	Global Positioning System
IBM	International Business Machines Corporation
IfmPt	Institut für musterbasierte Prognosetechnik
INPOL	Informationssystem der Polizei
INTERPOL	Internationale kriminalpolizeiliche Organisation
IKT	Informations- und Kommunikationstechnologien
IMK	Innenministerkonferenz
IoT	Internet of Things
IoS	Internet of Services

IP	Internet Protocol
IT	Informationstechnik
i.V.m	in Verbindung mit
KI	Künstliche Intelligenz
KfZ	Kraftfahrzeug
LKA	Landeskriminalamt
M2M	Machine to Machine
NSA	National Security Agency (USA)
NSU	Nationalsozialistischer Untergrund
ÖPNV	Öffentlicher Personennahverkehr
PAG	Neues Polizeiaufgabengesetz (Bayern)
PC	Personal Computer
PRECOBS	Pre-Crime-Observation-System
SPD	Sozialdemokratische Partei Deutschlands
SPI	Smart Policing Initiatives
SWOT	Strengths, Weaknesses, Opportunities, Threats
US	United States
USA	United States of America
WMP	West Midlands Police

1 Einleitung

1.1 Problemstellung und Relevanz

Die deutschen Polizeien befinden sich derzeit in einem tiefgreifenden Reform- und Wandlungsprozess. Herausforderungen wie der internationale Terrorismus, die Globalisierung und Internationalisierung von Kriminalität sowie innenpolitische und soziale Veränderungen, wie der demografische Wandel, beeinflussen die Polizeiarbeit zunehmend. Hinzu kommen die Auswirkungen der Digitalisierung aller Lebensbereiche sowie die rasanten Entwicklungen in den Informations- und Kommunikationstechnologien (IKT). Das Internet und die sich ständig weiterentwickelnden Technologien von Big Data und Social Media bis hin zu dem Internet der Dinge und dem Internet der Dienste beeinflussen dabei nicht nur wirtschaftliche und soziale Zusammenhänge, sondern erhöhen auch die Komplexität der Umgebungen, in denen die Polizeien agieren und ihren Aufgaben gerecht werden müssen (Rüdiger & Bayerl 2018, S. 11). Gleichzeitig ergeben sich durch eine Integration dieser Technologien vielfältige Potentiale für die polizeiliche Aufgabenbewältigung. Big Data-Analysen sowie intelligent vernetzte Informations- und Kommunikationstechnologien gewinnen für die Polizeiarbeit daher zunehmend an Bedeutung. In Deutschland lässt sich dies vor allem durch die ansteigende Verbreitung von Predictive-Policing Analysen sowie der zunehmenden Integration intelligent vernetzter Objekte innerhalb der Polizeien feststellen. Body-Cams, Dash-Cams, Überwachungsdrohnen, Smartphones und Tablets sowie intelligente Videoüberwachungssysteme stellen derzeit wohl die prominentesten Beispiele dar. Erhoffen sich die Polizeien und die politischen Entscheidungsträger hiervon Effizienzsteigerungen und Prozessoptimierungen sowie eine Verbesserung der öffentlichen Sicherheit und Ordnung, so bemängeln Datenschützer und Kritiker fehlende rechtliche Grundlagen für den Einsatz sowie die zunehmende Gefahr eines Abdriftens in überwachungsähnliche Zustände.

Die Implementierung moderner Informations- und Kommunikationstechnologien in die Polizeiarbeit wird dabei in der wissenschaftlichen Auseinandersetzung unterschiedlich bezeichnet (siehe 3.1). In Anlehnung an den „Smart Government" Ansatz nach von Lucke (2015), welcher das Gestaltungspotential für Staat und Verwaltung im Internet der Dinge und dem Internet der Dienste auslotet, soll hierfür im Folgenden der Begriff „Smarte

Polizeiarbeit“ (im Englischen: Smart Policing) verwendet werden. Unter Smarter Polizeiarbeit sollen dabei vor allem Prozesse im Zusammenhang mit dem polizeilichen Handeln und der Aufgabenbewältigung mit Hilfe von intelligent vernetzten Informations- und Kommunikationstechnologien, als auch der Analyse großer Datenmengen (Big Data) verstanden werden. Im Hinblick auf die zuvor skizzierte Problemstellung soll die vorliegende Arbeit folgende Forschungsfrage beantworten:

Welche Chancen, Risiken und Herausforderungen ergeben sich durch eine Smarte Polizeiarbeit und wie ist der Status Quo einzuordnen?

Dabei sollen sowohl zukünftige Perspektiven einer Smarten Polizeiarbeit für die Polizeien selbst als insbesondere auch für die Gesellschaft herausgearbeitet werden. Der Fokus der Untersuchung richtet sich dabei auf die Aufgabengebiete und Zuständigkeiten der deutschen Länderpolizeien. Zur Beantwortung der Forschungsfrage wird ein Überblick zu den derzeitigen Anwendungen und Technologien gegeben sowie eine eigene Arbeitsdefinition der Smarten Polizeiarbeit erstellt. Anhand von Interviews mit hochrangigen Experten[1] aus Politik, Verwaltung, Polizei, Wirtschaft und Wissenschaft sollen zukünftige Perspektiven aufgezeigt sowie aktuelle Ausprägungen einer Smarten Polizeiarbeit eingeordnet und bewertet werden.

Bisherige wissenschaftliche Studien konzentrieren sich meist auf die Auswirkungen einzelner intelligent vernetzter Objekte oder Big Data-Analysen in der Polizeiarbeit (vgl. Bretthauer 2017; Gusy 2014; Gerstner 2017 oder Seckelmann 2017). Des Weiteren lässt sich ein verstärkter Fokus auf die Untersuchung von polizeilichem Handeln im digitalen Raum feststellen, beispielsweise hinsichtlich Cyberkriminalität oder polizeilicher Social Media-Nutzung (vgl. Rüdiger & Bayerl 2018). Jedoch fehlen in der Literatur bislang wissenschaftliche Auseinandersetzungen, welche die Chancen, Risiken und Herausforderungen einer Smarten Polizeiarbeit in ihrer Gesamtheit analysieren. Die vorliegende Arbeit versucht daher diese Lücke zu verringern und zukünftige Pfade, Leitlinien und Handlungsempfehlungen aufzuzeigen.

[1] In der vorliegenden Arbeit werden aus Gründen der besseren Lesbarkeit ausschließlich die männlichen Formen verwendet. Diese beziehen stets Personen des weiblichen Geschlechts mit ein. Andernfalls wird dies ausdrücklich im Text erwähnt.

1.2 Aufbau der Arbeit

Das folgende Kapitel 2 behandelt zunächst die theoretischen Grundlagen der Arbeit. Hierbei geht es insbesondere um die Definition und Darstellung des Begriffs Big Data sowie des Ansatzes des intelligent vernetzten Regierungs- und Verwaltungshandelns im Internet der Dinge und dem Internet der Dienste. Eine Übersicht zu den Akteuren, der Organisation sowie den Aufgaben der Polizeien in Deutschland schließt das Kapitel ab. Darauf aufbauend werden in Kapitel 3 verschiedene Ansätze, Definitionen und Verständnisse einer Smarten Polizeiarbeit aus Literatur und Praxis vorgestellt. Anschließend erfolgt eine eigene Arbeitsdefinition der Smarten Polizeiarbeit, die für die nachfolgende empirische Untersuchung als Rahmensetzung fungiert. Hieran anknüpfend werden einige intelligent vernetzte Objekte sowie weitere Anwendungen vorgestellt, die derzeit von den Polizeien in Deutschland verstärkt eingesetzt werden. Beispiele einer Smarten Polizeiarbeit im Ausland sind ebenfalls Teil des Kapitels. Kapitel 4 stellt die Methodik und das Forschungsdesign für die empirische Untersuchung der Arbeit vor. Die vorliegende Arbeit verwendet einen qualitativen Forschungsansatz. In Kapitel 5 werden auf Basis von acht leitfadengestützten Experteninterviews unter anderem Status Quo, Thementreiber, Barrieren, Visionen und zukünftige Perspektiven einer Smarten Polizeiarbeit herausgearbeitet. Das Kapitel endet mit einem ersten Zwischenfazit. Kapitel 6 der Arbeit widmet sich der Eingangs skizzierten Problematik neuer Risiken und Möglichkeiten einer gesamtgesellschaftlichen Überwachung. Hierbei wird die Smarte Polizeiarbeit im Spannungsfeld zwischen Freiheit, Sicherheit und Überwachung diskutiert. In Kapitel 7 erfolgt dann eine Diskussion und Auswertung der erarbeiteten Ergebnisse aus den Experteninterviews mittels einer SWOT-Analyse. Auf Basis der Auswertung liefert das Kapitel daraufhin Handlungsempfehlungen für eine zukünftige Smarte Polizeiarbeit. Kapitel 8 schließt die Arbeit dann mit einem Fazit sowie einem kurzen Ausblick ab.

2 Theoretische Grundlagen

2.1 Big Data

Der Begriff Big Data ist seit Jahren allgegenwärtig. Dabei beschreibt dieser sowohl den immensen Bestand sowie das unermüdliche Wachstum an Daten, als auch die Methoden und Technologien, die eine Erfassung, Aufbereitung und Auswertung dieser Datenbestände ermöglichen.

2.1.1 Begriffliche Einordnung

Eine allgemeingültige Definition von Big Data, welche in der Wissenschaft beziehungsweise der Fachliteratur eine allseitige Akzeptanz erfährt, existiert nicht (vgl. Beinrott 2013, S. 108; De Mauro, Greco & Grimaldi 2016, S. 122; Plazek & Nürnberger 2017, S. 16). Tinnefeld, Buchner, Petri & Hof (2018, S. 8) definieren Big Data wie folgt:

> „Big Data beschreibt in Zeiten der Digitalisierung aktuelle technische Entwicklungen, welche die jederzeitige Erfassung, Speicherung und Analyse eines großen und beliebig erweiterbaren Volumens unterschiedlich strukturierter, komplexer Daten ermöglichen."

Diese Definition geht auf die Vielfältigkeit, die Schnelllebigkeit sowie auf das Volumen von Big Data ein und beschreibt gleichzeitig das zugrundeliegende Ziel, nämlich die Gewinnung und Nutzung dieser Datenbestände. Trotz des Mangels einer universalen Definition lassen sich in den wissenschaftlichen Auseinandersetzungen mit der Thematik fünf bestimmte Kernelemente identifizieren, die als eine Art Theoriegebäude von Big Data bezeichnet werden können. Diese Eigenschaften werden als die sogenannten „5 Vs" von Big Data bezeichnet und stehen für Volume, Variety, Velocity, Veracity und Value (Beinrott 2013; Marr 2015). Volume beschreibt dabei die riesige Menge an Daten, die durch die fortlaufende Digitalisierung aller Lebensbereiche in einer unvorstellbar großen Quantität existiert beziehungsweise entsteht. Das weltweit generierte Datenvolumen verdoppelt sich derzeit alle zwei Jahre und wird 2025 bei 163 Zettabyte liegen, also circa zehnmal so viel wie noch 2016 (statista 2018a). Unter Variety versteht man die unterschiedliche Beschaffenheit und die Vielfalt der Daten und Datenformate. Als Beispiel können hier persönliche Daten angeführt wer-

den, die durch die Social Media Interaktion anfallen sowie Daten, welche durch die Kommunikation zwischen Maschinen oder Objekten entstehen (Beinrott 2013, S. 110). Der Begriff Velocity umschreibt die hohe Geschwindigkeit, mit der die Daten erzeugt und ausgewertet werden. Insbesondere die sogenannte Echtzeit-Analyse von Big Data spielt in der heutigen Zeit zunehmend eine wichtige Rolle (Curry 2016, S. 30). Veracity umschreibt die Verlässlichkeit, Richtigkeit und Aussagekraft der Daten. Entscheidend sind hier der Informationsgehalt sowie die Qualität der Daten, welche erheblich divergieren können (Beinrott 2013, S. 110). Die letztlich intelligente Auswertung riesiger Mengen an Daten sowie der Aspekt der Relevanz und des Wertes jener wird durch Value beschrieben. Zusammenfassend lässt sich festhalten, dass die fünf Vs ein umfassendes Bild bezüglich des Phänomens Big Data ergeben: Die riesigen Datenmengen, die hohe Geschwindigkeit der Datengenerierung und –entstehung, die Vielfalt und Aussagekraft der Daten sowie insbesondere die Relevanz und der Wert der Daten beschreiben dabei die Kernelemente von Big Data (Beinrott 2013, S. 110; De Mauro et. al. 2016, S. 125).

In einer Organisation kann Big Data einerseits den Aufbau einer Wertschöpfungskette ermöglichen, die mit den erfassten Daten beginnt und über Informationen bis hin zu Wissen reicht. Diese kann dabei helfen, die Planung, Steuerung und Optimierung von Prozessen in Wirtschaft, Verwaltung und Zivilgesellschaft zu verbessern. Andererseits birgt die Anwendung von Big Data-Technologien ebenfalls zahlreiche Risiken, welche sich unter anderem aus der missbräuchlichen Nutzung, fehlenden rechtlichen Rahmenbedingungen oder unzulässigen und falschen Schlussfolgerungen aus der generierten Datenauswertung ergeben können (Eckert, Henckel & Hoeppner 2014, S. 5; Beinrott 2013).

2.1.2 Potentiale von Big Data für Staat und Verwaltung

Zu den in Big Data liegenden positiven Potentialen für die Behörden von Staat und Verwaltung wird unter anderem eine Verbesserung der Serviceleistung gegenüber den Bürgern, die Beschleunigung von internen Vorgängen, die Reduktion von Kosten, die Schaffung eines verbesserten Überblicks hinsichtlich aktueller Stimmungs- und Anspruchslagen, eine Transparenzsteigerung sowie die verbesserte Entscheidungsfindung dank breiterer Wissensbasis aufgezählt (Aggarwal 2016; Eckert et. al. 2014; Ehneß 2016). Von Lucke (2018, S. 37) ordnet Big Data im Häfler Stufenmodell (Ta-

belle 1) in das Web 3.0 (Internet der Daten) ein, welches bereits vorhandene Datenbestände vernetzt und sie somit für eine (offene) Weiternutzung durch Dritte erschließt. Durch eine Öffnung ihrer Daten (Open Data) und deren weitere Vernetzung (Linked Open Data) bieten sich für Behörden neue Potentiale zur Integration, Analyse und Nutzung großer vielfältiger Datenbestände (Big Data) (von Lucke 2018, S. 37). Es gilt in diesem Zusammenhang jedoch darauf hinzuweisen, dass der wirtschaftliche Nutzen, der oftmals aus dem Einsatz von Big Data gezogen werden soll, im Zusammenhang mit der öffentlichen Verwaltung unbedingt um die Zielvorgabe eines gesellschaftlichen Mehrwerts erweitert werden muss (Plazek & Nürnberger 2017, S. 16). Gleichzeitig dürfen die bereits angeführten Risiken von Big Data auch im Bereich des Staats- und Verwaltungshandelns nicht außer Acht gelassen werden.

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	Big Data, Big Data Analytics Linked Data, Open Data	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

Tabelle 1 Häfler Stufenmodell der Entwicklungsschritte des World Wide Web
Quelle: von Lucke 2016c, S. 175.

2.2 Intelligent vernetztes Regierungs- und Verwaltungshandeln

Durch das Internet der Dinge sowie das Internet der Dienste, welche im Häfler Stufenmodell im Web 4.0 eingeordnet werden, kommt es seit einigen Jahren zu einer zunehmenden intelligenten Vernetzung verschiedenster Objekte, welches mit dem begrifflichen Phänomen „smart“[2] am besten umschrieben werden kann (von Lucke 2015, S. 1). Für administrative Auf-

[2] Im Deutschen steht smart jedoch meist für „ausgefuchst, clever, gewitzt, einfallsreich, klug oder listig“ sowie für „chic, elegant oder exquisit“ (von Lucke 2015; Duden 2018).

gaben in Staat und Verwaltung ergeben sich hieraus zukünftig Konsequenzen und neue Perspektiven. Ein intelligent vernetztes Regierungs- und Verwaltungshandeln (Smart Government) nutzt die Potentiale smarter Objekte und cyber-physischer Systeme zukünftig zur effizienten und effektiven Erfüllung öffentlicher Aufgaben (von Lucke 2016b, S. 168). „Konkret geht es damit um die Anwendung des Internets der Dinge und der Dienste in der öffentlichen Verwaltung" (von Lucke 2016b, S. 168).

2.2.1 Internet der Dinge und Internet der Dienste

Das Internet der Dinge (auch „Internet of Things – IoT") hebt die Trennung zwischen realer und digitaler Welt auf, indem physische Objekte mittels einer digitalen Repräsentation vernetzt werden (Flügge & Fromm 2016, S. 4). Revolutionär ist hierbei die Rolle eingebetteter Systeme beziehungsweise Mikroprozessoren, die über Netzwerke miteinander verbunden sind und über diese miteinander kommunizieren können (von Lucke 2016b, S. 164). Eingebettete Systeme sind Hardware- und Softwarekomponenten, „die in ein Produkt implementiert werden, um hierdurch weitere produktspezifische Funktionsmerkmale zu realisieren" (ebd.). Die physischen Objekte werden also mit steuerbaren Mikrochips ausgestattet und über Funk vernetzt. Mittels dieser virtuellen Repräsentation im Internet erhalten die Objekte eine eigene und eindeutig ansprechbare digitale Identität. Durch Sensor- und Aktortechnologien kann die Funktionalität der Objekte um die Erfassung von Zuständen (zum Beispiel Temperatur oder Bewegung) beziehungsweise die Ausführung bestimmter Aktionen erweitert werden. Interagieren die Objekte nun miteinander oder mit Menschen, so wird ihnen umgangssprachlich eine „gewisse Intelligenz zugesprochen" (ebd., S. 165), wovon sich die gebräuchliche Bezeichnung „intelligent vernetzte Objekte" ableiten lässt (ebd.).

Deutlich komplexer und handlungsmächtiger sind cyber-physische Systeme (CPS), also die Anwendungen und Funktionen des Internets der Dinge (Djeffal 2017, S. 809). CPS sind heterogen vernetzte Gebilde, welche die physischen Objekte mit bestehenden digitalen Informations- und Kommunikationssystemen verknüpfen. Es handelt sich hier also um IT-Systeme als Teile von Geräten, Gebilden oder Prozessen, die mittels Sensoren Daten der realen Welt erfassen, in informationstechnische Repräsentationen umwandeln und basierend auf diesen Repräsentationen auf die reale Welt über Aktoren einwirken können (Tinnefeld et. al. 2018, S. 517; von Lucke

2015, S. 14). Im Vordergrund steht dabei vor allem die Speicherung und Auswertung der erfassten Daten (von Lucke 2016b, S. 165). Das Internet der Dinge verbindet die smarten Objekte mit ihren Sensoren und Aktoren sowie die darauf aufsetzenden CPS über IP-Protokolle miteinander. Eingebettete Alltagsgegenstände und CPS lassen sich dann von Personen oder Programmen über eine IP-Adresse eindeutig identifizieren, ansprechen, nutzen und auch steuern (von Lucke 2018, S. 38). Alltägliche Gegenstände werden dabei miteinander vernetzt und sind nun in der Lage, einen direkten Kommunikationsaustausch autonom und ohne menschliche Eingriffe zwischen Maschine und Maschine zu vollziehen (M2M- Kommunikation). Schätzungen zufolge wird es weltweit bis 2020 ca. 20,4 Milliarden vernetzte Gegenstände geben (statista 2018b), was wohl nur eine ungefähre Vorstellung bezüglich der Dimensionen des Internets der Dinge sowie des Ausmaßes im Hinblick auf Big Data zulässt.

Das Internet der Dinge ist außerdem eng verzahnt mit dem Internet der Dienste (auch „Internet of Services – IoS"), was darauf beruht, dass sich eine Vielzahl an realen Objekten bei mindestens gleichwertiger Funktionalität auch in webbasierte Dienste überführen und um ergänzende Funktionen erweitern lässt (von Lucke 2015, S. 19). Somit tritt anstelle der technischen Weiterentwicklung von Dingen zu intelligenten Objekten eine Neuentwicklung leistungsfähiger Web Services (Dienste) und virtueller Objekte „mit evolutionären wie teils disruptiven Folgen" (ebd.). Der webbasierte Dienst ist dabei meist deutlich effizienter und effektiver, was am Beispiel der elektronischen Akten- und Prozessunterstützungssysteme gegenüber Papierakten deutlich wird. Die gemeinsamen Bearbeitungs- und Einsichtsmöglichkeiten durch intelligente Cloud-Lösungen tragen hier zur Kostensenkung und Prozessoptimierung bei (von Lucke 2016b, S. 116).

Das Internet der Dinge und der Dienste ermöglicht sowohl neue Potentiale beispielsweise in der Prozessoptimierung, der Entscheidungsfindung sowie der Informationsgewinnung. Gleichzeitig ergeben sich jedoch auch einige Herausforderungen hinsichtlich Steuerungs- und Kontrollaufgaben, da Computer hierdurch zunehmend in der Lage sind, autonom Wahrnehmungen zu vollziehen, Entscheidungen zu treffen und diese durch Handlungen auszuführen (Djeffal 2017, S. 809). Das Internet der Dinge und das Internet der Dienste werden als disruptive Technologien dargestellt, die einen nachhaltigen Wandel aller Lebensbereiche bewirken könnten. Anders als

beim Konzept „Industrie 4.0“ jedoch schweigen die meisten offiziellen Konzepte hinsichtlich einer Revolution durch das Internet der Dinge und der Dienste im öffentlichen Sektor (ebd.). Ein Programm „Verwaltung 4.0“ als bloßes Begleitkonzept zu „Industrie 4.0“ wäre nach von Lucke (2016b, S. 169) jedoch nicht zielführend. Übertragen auf Staat und Verwaltung bedeutet dies, dass es ein gemeinsames Verständnis für ein intelligent vernetztes Regierungs- und Verwaltungshandeln unter dem Einsatz smarter Technologien auszuarbeiten gilt (von Lucke 2015, S. 4).

2.2.2 Smart Government

Ein einheitliches Verständnis des Begriffs Smart Government existiert nicht. Dies könnte in Bezug auf Deutschland zum einen an der in Staat und Verwaltung vorherrschenden Abneigung gegenüber Anglizismen (ebd.), als auch an dem Fehlen einer einheitlichen Definition liegen. Mellouli, Luna-Reyes & Zang (2014) beispielsweise verstehen unter Smart Government ganz allgemein „the extensive use of technology by governments“. Gil-Garcia (2012, S. 274) definiert das Konzept mit einer Erweiterung um die Dienstleistungsdimension des öffentlichen Sektors. Er versteht Smart Government als die Nutzung von ausgereiften Informationstechnologien, um Informationen, Prozesse, Institutionen und physische Infrastrukturen miteinander zu verbinden und zu integrieren und somit eine verbesserte Form der staatlichen Dienstleistung zu erwirken. Nach von Lucke (2016, S. 9) steht Smart Government für ein intelligent vernetztes Regierungs- und Verwaltungshandeln, welches vor allem auf intelligent vernetzten (smarten) Objekten und cyber-physischen Systemen basiert und sich dieser zur effizienten wie effektiven Ausführung öffentlicher Aufgaben bedient. In diesem Zusammenhang ist die „Häfler Definition von Smart Government“ entstanden:

> „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 Inter-

nets der Dienste, die technisch auf dem Internet der Systeme, dem Internet der Menschen und dem Internet der Daten aufsetzen [...]. Eingeschlossen ist der gesamte öffentliche Sektor, bestehend aus Legislative, Exekutive und Jurisdiktion sowie öffentliche Unternehmen" (von Lucke 2015, S. 4).

Die Häfler Definition von Smart Government verbindet dabei sowohl die Dimensionen des Web 1.0, Web 2.0 und Web 3.0 mit den neuen technischen Möglichkeiten im Web 4.0, als auch die daraus resultierende Zielsetzung einer verbesserten Erfüllung öffentlicher Aufgaben.

Eine erste Folgenabschätzung des Smart Government liefert das „Häfler Leitbild von Verwaltung 4.0"[3] (vgl. von Lucke 2015, S. 8). Mit den intelligent vernetzten IKT entstehen neuartige Optionen und Potentiale der Interaktion zwischen Staat, Verwaltung und Zivilgesellschaft (Prognos 2016, S. 5). Das Internet der Dinge und der Dienste ermöglicht Staat und Verwaltung durch die Öffnung und Vernetzung der Datenbestände von Objekten neuartige Potentiale sowohl zu Information und Analyse, als auch zur Automation und Kontrolle, was zu einer positiven Entscheidungsfindung beitragen kann, gleichzeitig aber auch neue Herausforderungen birgt (von Lucke 2016, S. 46). Somit beinhaltet Smart Government die Möglichkeit, das Regierungs- und Verwaltungshandeln massiv zu verändern. Es erscheint allerdings wichtig, darauf hinzuweisen, dass der Begriff nicht zwingend eine normative Dimension enthält. Ein intelligent vernetztes Regierungs- und Verwaltungshandeln führt nicht automatisch zu einer „besseren" Politik oder Verwaltung, sondern Möglichkeiten und Grenzen müssen durch Politik, Verwaltung und die Gesellschaft aktiv diskutiert und gestaltet werden (Prognos 2016, S. 5). Konkrete, auf öffentliche Aufgabenbereiche zugeschnittene, Visionen und Perspektiven bestimmter „Smarter Behörden" sowie Leitbilder des „Smarten Verwaltungshandelns" können dazu beitragen, diese Diskussion anzustoßen und das intelligent vernetzte Regierungs- und Verwaltungshandeln aktiv mitzugestalten sowie greifbarer und begrenzbarer zu machen (von Lucke 2015, S. 9).

2.2.3 Smarte Polizeiarbeit als Teil von Smart Government

Auch die deutschen Polizeien als Bestandteil der Exekutive werden von der Häfler Definition des Smart Government „erfasst". Wie die folgenden Sei-

[3] Das Leitbild sowie die Definition von „Verwaltung 4.0" finden sich in Anhang I.

ten aufzeigen werden, beeinflussen intelligent vernetzte IKT die Arbeit der deutschen Polizeien zunehmend. Diese Arbeit soll daher einen Gestaltungs- und Diskussionsimpuls zu einer intelligent vernetzten (Smarten) Polizeiarbeit liefern. Wie im vorherigen Punkt dargelegt, sollen hierdurch Perspektiven und Handlungsempfehlungen aufgezeigt werden. Der vermeintlich naheliegende Begriff „Smarte Polizei" ist hierbei irreführend, da *die* Polizei in Deutschland nicht existiert (siehe 2.3). „Smarte Polizeien" erscheint allerdings als ein eher umständlicher Ausdruck, weshalb in dieser Arbeit im Kontext des intelligent vernetzten polizeilichen Handelns der Begriff „Smarte Polizeiarbeit" verwendet werden soll. Eine Arbeitsdefinition sowie eine Eingrenzung des Begriffs erscheint sinnvoll und notwendig, um für die nachfolgende Untersuchung ein gemeinsames Verständnis zu erzeugen. Hierfür erfolgt zunächst eine Darstellung der Akteure, der Organisation sowie der Aufgaben der (Länder-)Polizeien in Deutschland. Daraufhin nähert sich Kapitel 3 dem Begriff aus einer wissenschaftlichen Perspektive, indem verschiedene Definitionen und Ansätze einer Smarten Polizeiarbeit vorgestellt werden. Auf Basis der nachfolgenden Seiten und in Anlehnung an die Häfler Definition von Smart Government soll dann in 3.2 eine eigene Arbeitsdefinition der Smarten Polizeiarbeit erfolgen.

2.3 Polizeien in Deutschland

Die Polizeien in Deutschland sind zentrale Akteure der inneren Sicherheit mit dem Auftrag, die öffentliche Sicherheit und Ordnung zu gewährleisten. Dabei sollen sie im Alltag und in Konfliktsituationen den handelnden Staat verkörpern und dürfen im Rahmen des staatlichen Gewaltmonopols als einzige Institution auch physische Gewalt anwenden (Groß 2012).

2.3.1 Akteure, Organisation und Aufbau

Die föderale Verfassungsordnung der Bundesrepublik Deutschland weist den 16 Bundesländern grundsätzlich die Polizeihoheit auf dem jeweiligen Staatsgebiet zu. In zentralen Bereichen des Polizeiwesens sieht das Grundgesetz jedoch originäre Aufgaben des Bundes vor (Feltes 2008, S. 108). Zu der Erfüllung dieser Aufgaben erlässt der Bund eigene Gesetze und führt Polizeibehörden in eigener Verantwortung (Art. 73 Nr. 10 i. V. m. Art. 87 Abs. 1 GG; Pekar-Milicevic 2016, S. 75). Aufgrund dieser Kompetenzverwaltung gibt es in Deutschland 16 Länderpolizeien, sowie die Polizeibehörden

des Bundes, welche sich in die Bundespolizei (BPOL) und das Bundeskriminalamt (BKA) gliedern und beide im Geschäftsbereich des Bundesministeriums des Innern liegen. Hinzu kommen die Polizei beim Deutschen Bundestag sowie in manchen Bundesländern kommunale Vollzugspolizeien.

Die Bundespolizei nimmt polizeiliche Aufgaben vor allem im Bereich des Grenzschutzes, der Bahnpolizei und der Luftsicherheit wahr (Pekar-Milicevic 2016, S. 71). Das BKA mit Sitz in Wiesbaden und Berlin ist die zentrale Kriminalpolizeibehörde Deutschlands. Seine Aufgabenschwerpunkte liegen in der nationalen Zentralstellenfunktion, der Bekämpfung des Drogen- und Menschenhandels, des Terrorismus, der Geldwäsche sowie von Cyberkriminalität und der organisierten Kriminalität. Es ist außerdem für die internationale Zusammenarbeit mit ausländischen Polizeibehörden zuständig und ist zugleich Verbindungsstelle zu internationalen Behörden wie INTERPOL oder EUROPOL (Feltes 2008, S. 108; Groß 2012). Wie in der Einleitung bereits dargelegt, soll der Fokus der Untersuchung auf den Aufgabenbereichen der 16 Länderpolizeien liegen, deren Aufbau und Zuständigkeiten daher im Folgenden detaillierter behandelt werden.

Die Landespolizei untersteht in allen Bundesländern dem jeweiligen Innenminister beziehungsweise Innensenator. Hier ist daher auch die politische Verantwortung im demokratischen Rechtsstaat angesiedelt, nämlich innerhalb der Exekutive (Frevel & Groß 2016, S. 67). In den einzelnen Organigrammen gibt es hingegen wenige Übereinstimmungen zwischen den jeweiligen Länderpolizeien. Grundlegend kann zwischen zwei organisatorischen Behördensystemen unterschieden werden. Im Polizeibehördensystem ist die Polizei mit allen Tätigkeiten betraut, welche die Abwehr von Gefahren sowie die Verfolgung von Straftaten und Ordnungswidrigkeiten betreffen. Im Ordnungsbehördensystem erfolgt eine strikte Differenzierung zwischen Fach- und Vollzugspolizei (Pekar-Milicevic 2016, S. 76). Generell ist es auf die Organisationshoheit der Länder im föderalen System der Bundesrepublik zurückzuführen, welche es ihnen erlaubt, die Organisationsmodelle sowie einzelne Bezeichnungen frei zu wählen (Groß 2008, S. 23). Die klassischen Behördenstrukturen mit klaren Zuständigkeiten, hierarchischen Prinzipien und langen Dienstwegen lassen sich jedoch bei allen Länderpolizeien feststellen (Vera & Jablonowski 2017, S. 482). Des Weiteren unterlagen so gut wie alle Länderpolizeien in den letzten Jahren einer Reihe von Polizeireformen. Diese hatten meist das Ziel, eine Straffung der

Strukturen herbeizuführen sowie die Bildung größerer territorialer und organisatorischer Einheiten zu forcieren.[4]

Gemeinsames Merkmal aller Länderpolizeien ist zudem die interne Spartenteilung in Schutzpolizei (ca. 80 % der Gesamtstärke), Kriminalpolizei sowie Bereitschaftspolizei. Jedes Land hat zudem ein eigenes Landeskriminalamt (LKA), dessen Zuständigkeiten im Bereich der organisierten Kriminalität, der Sexualstraftaten, des Drogenhandels und des Staatsschutzes liegen (Groß 2012). 2016 gab es in Deutschland rund 220.000 Polizeibeamte in den Länderpolizeien (Statista 2018c). Ostdeutsche Länder weisen dabei in der Regel eine höhere Polizeidichte auf als westdeutsche Länder, was unter anderem auf kriminalgeographische Unterschiede zurückzuführen ist (Frevel & Groß 2016, S. 66). Kam es zwischen 2008 und 2014 noch zu einem Abbau von Stellen aufgrund finanzieller Restriktionen resultierend aus der Föderalismusreform II (ebd.) bei fast allen Länderpolizeien, so ist in den vergangenen Jahren eine Steigerung der Stellen unter anderem in Baden-Württemberg, Bayern, Nordrhein-Westfalen und Berlin zu erkennen - in Brandenburg, Sachsen, Thüringen und Sachsen-Anhalt jedoch ein kontinuierlicher Stellenabbau.

2.3.2 Aufgaben und Befugnisse

Die Rechtsgrundlagen für die Landespolizeiarbeit in Deutschland sind neben den bundeseinheitlichen Strafgesetzen und der Straßenverkehrsordnung die Polizeigesetze der Länder, die für die jeweilige Landespolizei Aufgaben und Befugnisse regeln, sich im Wesentlichen aber kaum unterscheiden. Je nachdem, welches Bundesland man betrachtet, lassen sich jedoch unterschiedliche Schwerpunktsetzungen bei der Verfolgung und Aufklärung beziehungsweise der Verhinderung und Vorbeugung von Straftaten feststellen (Groß 2012). Grundsätzlich liegen die Aufgaben der Länderpolizeien im Bereich der Bekämpfung und Ermittlung von Straftaten, der Spuren- und Beweissicherung, der Regelung des Straßenverkehrs, der Ausbildung des polizeilichen Nachwuchses, der Bekämpfung von Umweltkatastrophen, der Begleitung von Demonstrationen und Großveranstaltungen sowie der Sicherung von Wasserstraßen. Gleichzeitig hat die Polizei eine klare Dienstleisterfunktion gegenüber der Bevölkerung, mit dem Ziel,

[4] So wurden beispielsweise in Baden-Württemberg im Jahr 2014 vier Landespolizeipräsidien und 37 Polizeidirektionen zu 12 Flächenpräsidien umstrukturiert (Frevel & Groß 2016, S. 68).

die Freiheitsrechte der Bürger zu wahren (Stierle & Lakner 2017, S. 1008). Im alltäglichen Leben ist die Polizei Ansprechpartner der Bürger („Die Polizei dein Freund und Helfer"), Konfliktmanager und Ratgeber, aber auch Vollzieher der Gesetze sowie Garant der Menschenrechte und Schützer der der Bevölkerung (Siller 2017, S. 698).

Somit ergibt sich für die Polizeien ein facettenreiches Aufgabenspektrum mit dem vorrangigen Ziel, die öffentliche Sicherheit und Ordnung in den Ländern zu gewährleisten. Dabei lassen sich zwei übergeordnete Prinzipien des polizeilichen Auftrags feststellen: Die Strafverfolgung beziehungsweise *Repression* und die Gefahrenvorbeugung beziehungsweise *Prävention* (Kühne 2012). Auf den Bereich der Prävention soll in Punkt 6.2 dieser Arbeit detaillierter eingegangen werden, da nach Einschätzung einiger Experten in den letzten Jahren seitens der Polizei ein verstärkter Fokus auf präventive Aufgaben festzustellen ist, den es kritisch zu hinterfragen gilt (vgl. Glaeßner 2016; Moser-Knierim 2014; Thiel 2011; Prantl 2010).

Dennoch weisen die landesgesetzlichen Regelungen den Länderpolizeien teilweise ausdrücklich Kompetenzen der Gefahrenvorbeugung zu. Hierbei sollen insbesondere Daten und Informationen vorgehalten werden, welche die Verfolgung zukünftiger Straftaten erleichtern (Thiel 2011, S.102). Im Hinblick auf die Nutzungsmöglichkeit moderner IKT im Zeitalter von Big Data und dem Internet der Dinge und der Dienste kommt dem Präventivbereich der Polizeiarbeit daher eine völlig neue Bedeutung zu. Der verstärkte Fokus auf vorbeugende und vorsorgliche Maßnahmen sowie die zunehmende Integration moderner IKT ist dabei auch neuen Heraus- und Anforderungen geschuldet, mit welchen sich die Polizeien zunehmend konfrontiert sehen (Moser-Knierim 2014, S. 50).

2.3.3 Neue Heraus- und Anforderungen

Terrorismus und politischer Extremismus

Der islamistische Terrorismus ist spätestens nach den Anschlägen in mehreren europäischen Großstädten in den letzten Jahren wieder ein dauerhaft präsentes Thema in der deutschen Öffentlichkeit (Steinberg 2017). Auch der politische Extremismus spielt durch die Aufdeckung der NSU-Anschlagsserie wieder eine Rolle im gesellschaftlichen Sicherheitsgefühl. Gewaltsame Angriffe gegen Politiker und Asylbewerberheime sowie die G-

20 Krawalle in Hamburg tragen ebenfalls zur Verunsicherung bei. Beide Phänomene sowie die andauernde Diskussion um potentielle islamistische „Gefährder" haben zu einem verstärkten und angespannten Sicherheitsdiskurs in der deutschen Öffentlichkeit geführt, der von einer allgemeinen Verunsicherungslage geprägt ist (Völlinger 2017).

Europäisierung und Globalisierung

Durch gemeinsame europäische Ermittlungsgruppen werden neue Sicherheitsstrukturen geschaffen. Die Grenzen zwischen äußerer und innerer Sicherheit in Zeiten der Globalisierung verschwimmen zunehmend. Dadurch ergibt sich ein Kooperationsbedarf der Länderpolizeien mit anderen Akteuren der Sicherheitspolitik, wie der Bundeswehr, Geheimdiensten, EUROPOL, INTERPOL oder privaten Sicherheitsdiensten (Monroy 2017; Frevel & Groß 2016, S.81). Auch unter den Länderpolizeien bedarf es künftig einer intensiven Kommunikation und Zusammenarbeit, denn kaum ein kriminalistisches Phänomen macht mehr vor nationalen Grenzen beziehungsweise Ländergrenzen halt (Feldmann 2018).

Private Sicherheitsdienste und Privatisierung von Polizeiaufgaben

Im Jahr 2013 gab es in Deutschland 4.000 private Sicherheitsfirmen, die insgesamt einen Umsatz von 5,15 Milliarden € erzielten. Die Mitarbeiterzahl von insgesamt 186.00 Beschäftigten liegt nur knapp unter der Zahl an Landespolizeibeamten, wobei die Branche einen regen und kontinuierlichen Zuwachs erfährt (Birken & Eick 2017). Die Aufgabenbereiche umfassen dabei Justizvollzugsanstalten, den ÖPNV, Umweltschutz sowie die Bewachung von privatem Eigentum und öffentlichen Einrichtungen. Insbesondere in Kommunen und Städten kann ein starkes Anwachsen privater Sicherheitsdienste beobachtet werden. Der jahrelang auferlegte Sparzwang der Polizeien hat dazu geführt, dass der Staat gewisse Aufgaben im Bereich der öffentlichen Sicherheit an private Sicherheitsdienste „beliehen" hat (Schnee & Unterberg 2016). Die Gefahr einer zunehmenden Privatisierung von Sicherheit liegt jedoch darin, dass hierdurch Zweifel an der Schutzfähigkeit des Staates entstehen. Hieraus können sich dann Legitimations- und Demokratiedefizite seitens der Bürger entwickeln (Lange & Frevel 2008, S. 133).

Demografischer Wandel

Sinkende Bevölkerungszahlen, der Anstieg des Anteils der älteren Bevölkerungsgruppen, der Rückgang der erwerbstätigen Bevölkerung sowie zunehmende Migration prägen die demografische Entwicklung Deutschlands (Kühn 2017). Die ansteigende gesellschaftliche Urbanisierung sowie ein anwachsender Fachkräftemangel sind ebenfalls Phänomene, mit welchen sich die Polizeien vermehrt konfrontiert sehen. Insbesondere die Gewinnung sowie die Erhaltung von qualifiziertem Fachpersonal wird für die Polizei zu einer zunehmenden Herausforderung, da Spezialisierung sowie ein hoher Grad an Professionalität in vielen Bereichen unabdingbar für die Ausübung des Polizeiberufs sind. Die Nachwuchsgewinnung wird außerdem dadurch erschwert, dass die Polizei verstärkt in einem Wettbewerb um IT-Fachpersonal mit der öffentlichen Hand sowie insbesondere der freien Wirtschaft steht (Pekar-Milicevic 2016, S. 81-82).

Digitalisierung und neue Informations- und Kommunikationstechnologien

Die mit den oben genannten Begriffen einhergehende Phänomene des steigenden Vernetzungsgrads sowie der rasanten Verbreitung von Information verändern auch die Polizeiarbeit. Bis 2020 wird es in Deutschland ca. 56 Millionen Nutzer mobiler Endgeräte und ca. 800 Millionen vernetzte Geräte geben (Donner 2016; Jansen 2017). Durch die voranschreitende Digitalisierung kommt es auch zu einer neuen Erwartungshaltung innerhalb der Bevölkerung gegenüber der Polizei. Papierbasierte Dienste, Kommunikation sowie Aktenführung werden als nicht mehr zeitgemäß wahrgenommen. Bürger erwarten, dass sie schon heute, aber erst recht in Zukunft, Behördengänge zeit- und ortsunabhängig sowie elektronisch erledigen können (Hogrebe & Kruse 2014, S.157). Ein Großteil der Deutschen wünscht sich bereits jetzt, dass die Polizei verstärkt digital arbeitet und in Erscheinung tritt, beispielsweise mittels mobiler Apps und Informationsportale, aber auch im Bereich der Kriminalitätsbekämpfung sowie zur alltäglichen Arbeitsunterstützung (Klein 2015). Der Bürger wird durch die mittlerweile fast selbstverständliche Nutzung von Smartphone, Tablet und weiteren Anwendungen im Internet der Dinge und der Dienste selbst immer „smarter" und erwartet dies zunehmend auch von Staat und Verwaltung (von Lucke 2015, S. 10).

Die Datenbestände der Polizeien wachsen durch die Digitalisierung aller Lebensbereiche beträchtlich an, wodurch sich für die Organisationen neue Potentiale sowie Herausforderungen im Umgang mit Big Data ergeben. Neue smarte Objekte und Systeme erhalten ebenfalls Einzug in die Polizeiarbeit. Dies kann die Arbeit der Polizei verbessern, erfordert aber auch neue Kompetenzen der Mitarbeiter. Die Digitalisierung kann seitens der Polizei aber vor allem zu einer Effizienzsteigerung ihrer Arbeit führen und damit auch den Folgen des genannten Fachkräftemangels entgegenwirken.

Insgesamt befinden sich die Länderpolizeien derzeit in einer Situation, in der sie bei sinkenden Ressourcen, finanziellen Restriktionen und neuen gesellschaftlichen Herausforderungen einen steigenden Aufgabenzuwachs bewältigen beziehungsweise neuen Anforderungen gerecht werden müssen (Frevel & Groß 2016; Klöpfer 2017; Pekar-Milicevic 2016). Hinzu kommt eine von der Politik getriebene und aufgeheizte öffentliche Sicherheitsdebatte, in der die praktische Relevanz der Forderungen teils nebensächlich scheint und die Polizei zusätzlich unter Druck setzt (Strauß 2017). Um den Schutz der Bevölkerung sowie die Sicherheit und Ordnung in den Ländern weiterhin zu gewährleisten und dem politischen Druck gerecht zu werden, bedarf es seitens der Polizei somit neuer strategischer Ausrichtungen. Intelligent vernetzte IKT sowie Big Data-Analysen nehmen dabei zunehmend eine zentrale Rolle ein.

3 Smart Policing – Smarte Polizeiarbeit

Im Folgenden werden in einer begrifflichen Einordnung zuerst verschiedene Ansätze und Definitionen Smarter Polizeiarbeit vorgestellt. Daran anknüpfend erfolgt eine eigene Arbeitsdefinition der Smarten Polizeiarbeit. Im Anschluss werden einige ausgewählte Technologien sowie intelligent vernetzte Objekte und Anwendungen vorgestellt, die derzeit von den Polizeien in Deutschland verstärkt eingesetzt werden. Abschließend werden zwei Beispiele einer Smarten Polizeiarbeit im Ausland aufgezeigt.

3.1 Begriffliche Einordnung

Behr (2006, S. 69) thematisiert Smart Policing bereits 2006 als eine Handlungslogik der Polizeiarbeit in Abgrenzung zu einem Zero-Tolerance-Ansatz. Demnach impliziert Smart Policing insbesondere, dass die Polizeien bürgernäher werden und sich in den spezifischen Balanceakt einer demokratischen Polizei zwischen Kontrolle und Repression in der Verbindung mit Service und Anteilnahme begeben müssen. Behr sieht dies als eine Antwort des Staates beziehungsweise der Polizeien auf eine immer kritischer werdende Öffentlichkeit. Stone (2017, S. 111) stellt Smart Policing im Kontext des White Paper on Policing 2016 der Südafrikanischen Regierung vor. Demnach stehe Smart Policing für „a framework to establish an accountable, professional, competent and highly skilled police service" (ebd.). Ziel von Smart Policing sei es, die Transparenz polizeilichen Handelns zu erhöhen sowie unter dem Einsatz moderner smarter Technologien und Anwendungen die Arbeit der Polizeien zu verbessern (ebd., S. 113). Brandl (2018) untersucht die vom U.S. Department of Justice, Bureau of Justice Assistance im Jahr 2009 eingeführten sog. Smart Policing Initiatives (SPI)[5]. Smart-Policing steht hierbei für die Zusammenarbeit von Polizeibehörden und Forschungseinrichtungen, „to form partnerships and work together to identify solutions to local crime problems" (ebd., S. 323). Dabei seien die Konzepte stets eng vernetzt mit Data-Driven-Policing, welches für eine datenbasierte und datenunterstützte Polizeiarbeit steht, in der

[5] SPI bietet Fördergelder für Polizeiorganisationen in den USA, um zusammen mit Universitäten Forschungspartnerschaften zu gründen, welche die Polizeiarbeit evidenzbasierter und wirksamer machen sollen. Seit 2009 haben 52 Polizeiorganisationen SPI-Fördergelder erhalten (Brandl 2018, S. 324).

die Polizei Big Data-Analysen zur Entscheidungsfindung in der alltäglichen Arbeit nutzt (ebd., S. 326). Coldren, Huntoon & Medaris (2013, S. 275) thematisieren Smart Policing ebenfalls im Zuge der SPI. Sie heben gleichermaßen den evidenzbasierten Ansatz der Polizeiarbeit mittels Forschungskooperationen hervor, erweitern das Konzept aber um die Integration von „Data and Smart Analytics". Insbesondere Anwendungen wie Body-Cams, smarte Videoüberwachungskameras, Überwachungsdrohnen, Smartphones und Predictive-Policing werden in den einzelnen SPI-Projekten besonders stark eingesetzt und sollen die Arbeitseffizienz der Polizeien steigern. Einen stark technologiebasierten Ansatz des Smart-Policing liefern die Autoren Moon, Bin-Choi & Lee (2017) aus Südkorea. Smart Policing wird hier als die Integration von Anwendungen und Technologien rund um Big Data, dem Internet der Dinge sowie Künstlicher Intelligenz[6] und maschinellem Lernen in die Polizeiarbeit verstanden. Ziel sei die Produktion einer „Effective Real-time Response in Crime" (ebd., S. 2). Als Beispiele werden von den Autoren unter anderem Predictive-Policing Anwendungen, smarte Videoüberwachung mit Gesichts- und Bewegungserfassung, smarte Polizeieinsatzwagen sowie portable DNA-Testlabore genannt (ebd., S. 5), welche von der Polizei in Südkorea bereits genutzt werden.

Der Vorsitzende der Gewerkschaft der Polizei (GdP), Oliver Malchow, forderte auf der GdP-Fachtagung in Brüssel 2017 eine „smarte Polizei". Hierunter versteht er eine flächendeckende Ausstattung mit intelligenten polizeilichen Informations- und Ermittlungssystemen, sodass zukünftig jeder Polizeibeamte gespeicherte und relevante Informationen „auf Knopfdruck erhalten kann" (GdP 2017). Das BKA sowie die Bundespolizei sind seit einigen Jahren an verschiedenen Forschungsprojekten beteiligt, mit deren Hilfe die Arbeit der Polizei mittels der Integration modernster Technik „intelligent" werden soll (Krempl 2016). Diese Projekte werden unter dem Schlagwort „Smart Police" zusammengefasst, wie aus der Antwort der Bundesregierung auf eine kleine Anfrage einiger Abgeordneter der Fraktion Die Linke aus dem Jahr 2016 hervorgeht (Deutscher Bundestag 2016).

Zusammenfassend lässt sich festhalten, dass die vorgestellten Ansätze und Konzepte von Smart Police, Smart Policing, Smarter Polizei beziehungs-

[6] Künstliche Intelligenz (KI) beschäftigt sich mit Methoden, die es einem Computer ermöglichen, solche Aufgaben zu lösen, die, wenn sie vom Menschen gelöst werden, Intelligenz erfordern (Siepermann 2018).

weise Smarter Polizeiarbeit zwar teils unterschiedliche Schwerpunktsetzungen beinhalten, sich größtenteils jedoch in einigen wesentlichen Punkten ähneln:

1. Die polizeiliche Arbeit soll effizienter, effektiver, bürgernäher, transparenter und evidenzbasierter werden.

2. Erreicht werden soll dies mit der Integration intelligent vernetzter Objekte, CPS und moderner IT-Systeme sowie durch die Analyse anfallender Datenbestände (Big Data).

3.2 Arbeitsdefinition: Smarte Polizeiarbeit

In Anlehnung an die Häfler Definition von Smart Government und die Skizzierung des polizeilichen Auftrags und der Aufgaben sowie im Hinblick auf die Definitionsansätze aus Wissenschaft und Praxis soll Smarte Polizeiarbeit in dieser Arbeit wie folgt definiert und untersucht werden:

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.

Die Arbeitsdefinition hebt die besondere Bedeutung intelligent vernetzter IKT im Internet der Dinge und der Dienste sowie von Big Data-Analysen für die Smarte Polizeiarbeit hervor. Des Weiteren liefert die Definition eine Zielvorgabe, die durch eine Smarte Polizeiarbeit erfüllt werden soll.

3.3 Smarte Objekte und Anwendungen

Wie aus der bisherigen Arbeit hervorgegangen ist, sind verschiedene intelligent vernetzte, also smarte, Objekte und Anwendungen für die Polizeiarbeit von zunehmender Bedeutung. Im Folgenden sollen daher sieben smarte Objekte, Applikationen für Smartphones und Tablets sowie das Predictive-Policing als Big Data-Analyse vorgestellt werden. Die hierbei getroffene Auswahl richtet sich nach dem aktuellen Status Quo innerhalb der deutschen Länderpolizeien. Ziel ist hierbei vorrangig die Vorstellung der Funktionsweise und Einsatzbereiche der Objekte und Anwendungen.

Typ	*Technik*	*Einsatzziele*
Body-Cam und Dash Cam	Smartes Objekt, Kamera	Bild- und Tonaufnahmen, Deeskalation/Beweissicherung
(Smarte) Videoüberwachung	Smartes Objekt/CPS, Kamera	Bildaufnahmen, Beweissicherung/ Muster- & Gesichtserkennung
Überwachungsdrohne	Smartes Objekt/CPS, Kamera, Sensoren	Bildaufnahmen, Tatort- & Situationsanalysen
Smartphone und Tablet	Smartes Objekt, (Kamera)	Information/Kommunikation/ Prozessoptimierung
Apps für Smartphone und Tablet	Anwendung im Internet der Dienste – IoS	Information/Kommunikation/ Prozessoptimierung
Smarter Polizeieinsatzwagen	Smartes Objekt/CPS	Mobiler Informations- & Kommunikations-Hub
Predictive-Policing	Big Data-Analyse	Prognose von Straftaten

Tabelle 2 Smarte Objekte und Anwendungen in der Polizeiarbeit

Eine kritische Einordung erfolgt in Kapitel 5 und 7 der Arbeit. Tabelle 2 liefert vorab einen Überblick zu den Objekten und Anwendungen, deren technischen Komponenten und möglichen Einsatzbereichen.

3.3.1 Body-Cam und Dash-Cam

Bei der sogenannten *Body-Cam* handelt es sich um eine kleine Kamera, die im Schulter- oder Brustbereich auf der Weste des Polizeibeamten befestigt ist (Seckelmann 2017, S. 292). Der Begriff leitet sich von den englischen Worten *body* und *cam(era)* ab – wörtlich übersetzt steht er für „Körperkamera". Unter dem Begriff wird eine Vielzahl unterschiedlicher Geräte und Modelle zusammengefasst (Hauptmann 2017, S. 5; Zander 2016, S. 15). Je nach den Polizeigesetzen der Länder kann die Body-Cam unterschiedlich eingesetzt werden: Für Bildaufnahmen, für Bild-Ton-Aufnahmen sowie für das sog. *Pre-Recording*[7] (Seckelmann 2017, S. 292). In Gefahrensituationen beziehungsweise bei Betreten eines Einsatzraums kann der Streifenpolizist den Aufnahmeknopf der Kamera nach vorheriger sprachlicher Ankündigung aktivieren, wodurch die Aufzeichnung fortan gespeichert wird. Die Speicherung erfolgt auf einem festen Speicher im Gerät oder einer herausnehmbaren Speicherkarte (Hauptmann 2017, S. 6). Einige Modelle in den USA hingegen senden die Videoaufnahmen bereits in Echtzeit an die zuständige Einsatzzentrale zur dortigen Speicherung und Auswertung (Stroud 2016).

Durch Body-Cams werden also Eingriffe durch die Polizei mittels Bild- oder Bild-Ton-Aufnahmen dokumentiert. Hierdurch soll eine neue unabhängige Beweissicherung in Gefährdungslagen erfolgen und die Transparenz polizeilichen Handelns gefördert werden. Sie sollen außerdem der zunehmenden Gewalt gegenüber Polizeibeamten vorbeugen, wobei Pilotprojekte und bisherige Einsätze hierzu noch keine signifikanten Befunde liefern konnten (Steinke 2017). Polizeibeamte, die eine Body-Cam tragen, sind durch entsprechende Aufschriften auf der Polizeiweste erkennbar. Ein Großteil der 16 Länderpolizeien sowie die Bundespolizei befinden sich derzeit in Pilotprojekten bezüglich des Einsatzes der Body-Cam. Andere Polizeien haben

[7] Dabei „werden über einen gewählten Zeitraum (30, 60 oder 90 Sekunden) vorab Aufzeichnungen, die in einem Zwischenspeicher gesichert werden, getätigt. Diese Aufnahmen werden auch aufgezeichnet, wenn der Aufnahmemodus der Kamera nicht aktiviert ist. Zudem werden sie fortlaufend überschrieben. Nur beim Betätigen der Aufnahmetaste wird diese Sequenz der Aufnahme vorangestellt, um den gewählten Zeitraum zu speichern" (Hauptmann 2017, S. 6; Müller 2016, S. 16).

diese bereits fest in ihre alltägliche Arbeit mittels gesetzlicher Eingriffsgrundlagen integriert, so wie unter anderem Hessen, Hamburg oder auch die Bundespolizei (Martini, Nink & Wenzel 2016; Steinke 2017; Kurpjuweit 2018). Im Zusammenhang mit der Body-Cam ist auch auf die sog. *Dash-Cam* („Armaturenbrett-Kameras") hinzuweisen. Hierbei handelt es sich um eine kleine Kamera, die in den Polizeieinsatzwagen aber auch in privaten Fahrzeugen angebracht ist und mit vergleichbarer Technik und Einsatzziel das Geschehen im Straßenverkehr dokumentieren soll (Seckelmann 2017, S. 293).

3.3.2 (Smarte) Videoüberwachung

Neben mobilen smarten Kameras, wie Body-Cam und Dash-Cam, spielen auch stationäre Videokameras zunehmend eine wichtige Rolle in der Polizeiarbeit. Videokameras, die öffentliche Räume überwachen, ermöglichen der Polizei immer wieder Fahndungserfolge, erfassen Straftaten sowie Ordnungswidrigkeiten und ermöglichen polizeiliche Verkehrslenkungsmaßnahmen. Insbesondere an „Kriminalitätsschwerpunkten" setzt die Polizei auf Videoüberwachung zur Gefahrenabwehr und zur Bekämpfung von Sicherheitsstörungen. Sichtbar angebrachte Schilder müssen dabei stets auf die Videoüberwachung hinweisen. Zudem werden die Aufnahmen immer wieder überschrieben, um nicht gegen datenschutzrechtliche Vorgaben zu verstoßen (Leubecher & Kade 2016). Den entscheidenden Schritt von der herkömmlichen zur *smarten* Videoüberwachung[8] markiert der technische Fortschritt im Bereich der Bildanalyse, -interpretation und -auswertung (Bretthauer 2017, S. 35). Neue Ansätze integrieren nun biometrische Gesichtserkennungssoftware sowie Systeme, die bestimmte Bewegungsmuster scannen (ebd.).

Seit dem 1. August 2017 läuft in Berlin das Pilotprojekt „Sicherheitsbahnhof Berlin Südkreuz" [9] unter dem Einsatz smarter Videoüberwachung mit Gesichtserkennungstechnik (BMI 2017a). Hierbei werden Gesichter gescannt und von einem Programm in Echtzeit mit einer Datenbank verglichen. Bei einem Treffer alarmiert der Computer dann die zuständige Bundespolizei. In Zukunft sollen Terroristen, mögliche „Gefährder" und

[8] Smarte Videoüberwachung bezeichnet Videoüberwachung unter Einsatz von Videoanalyse und Datenabgleich (Bretthauer 2017, S. 36).

[9] Hierbei handelt es sich um ein gemeinsames Pilotprojekt des Bundesministeriums des Innern, der Bundespolizei, des BKAs sowie der Deutschen Bahn AG.

Straftäter somit bereits vor einem Anschlag oder Verbrechen automatisch gescannt und von der Polizei festgenommen werden (Rabenstein 2017). In Mannheim wird derzeit eine Software eingesetzt, die auf 71 Kameras an 28 Standorten in der Stadt Aufnahmen tätigt und mittels eines Computerprogramms des *Fraunhofer-Instituts IOSB* auswertet. Bei hektischen oder untypischen Bewegungen, etwa Schlagen, Rennen oder Fallen, meldet das System Alarm und ein Polizist kann die Szene am Bildschirm bewerten (Jung 2018). Auch im neuen Koalitionsvertrag findet sich eine Passage zur smarten Videoüberwachung. CDU/CSU und SPD betonen, dass die Videoüberwachung an Brennpunkten verstärkt eingesetzt, effektiv ausgebaut und dabei auch technisch verbessert werden soll. „Intelligente [smarte] Videoüberwachung kann dabei eine Weiterentwicklung sein" (Koalitionsvertrag 2018, S. 127). Das Pilotprojekt am Berliner Südkreuz soll dabei entscheidende Hinweise zur möglichen weiteren Implementierung smarter Videoüberwachung liefern (ebd.).

Der Einsatz smarter Videokameras mit Gesichtserkennung sowie die immer flächendeckendere Videoüberwachung im Allgemeinen sind jedoch umstritten. Datenschützer sehen in der Gesichtserkennungstechnik erhebliche Grundrechtseingriffe und bemängeln das Fehlen einer gesetzlichen Grundlage. Die Freiheit, sich in der Öffentlichkeit anonym zu bewegen, könne mit einer flächendeckenden (smarten) Videoüberwachung gänzlich zerstört werden (Krempl 2017). Zudem sei unklar, ob Videoüberwachung Straftaten tatsächlich verhindere sowie dazu beitrage, Täter auf frischer Tat zu ertappen (Wangemann 2016).

3.3.3 Überwachungsdrohne

„Unbemannte Luftfahrzeuge" (BMVI 2018), sogenannte Drohnen, werden seit einiger Zeit auch von der Mehrheit der Länderpolizeien[10] sowie der Bundespolizei eingesetzt. Die Steuerung der Drohnen erfolgt mittels eines „Controllers" am Boden oder autonom durch softwaregestützte Programmierung (Altmann 2012, S. 8). Mit hochauflösenden Kameras, Radarsystemen, Sensoren und Aktoren ausgestattet, können sie Gebiete stunden- und tagelang beobachten sowie Übersichtsaufnahmen aus verschiedensten

[10] Die Länderpolizeien in Bayern, Berlin, Brandenburg, Niedersachsen, Hessen, Mecklenburg-Vorpommern, Nordrhein-Westfalen, Rheinland-Pfalz, Sachsen, Sachsen-Anhalt, Saarland sowie Schleswig-Holstein setzen derzeit bereits Überwachungsdrohnen ein oder befinden sich in Pilotprojekten.

Höhen und Winkeln senden, um Tat- und Schadensorte zu untersuchen (Tinnefeld et. al. 2018, S.11). Hierdurch ergeben sich neue und verbesserte Möglichkeiten der Tatorterfassung und -vermessung. Großflächige und schwer zugängliche Gebiete können aus der Luft abgesucht werden, beispielsweise bei der Fahndung nach vermissten Personen oder bei Umweltkatastrophen. Auch für die Täterverfolgung können Überwachungsdrohnen eingesetzt werden (Truscheit 2017). Im Hinblick auf die Regelung des Straßenverkehrs können smarte Überwachungsdrohnen Lagebilder zur Verkehrssituation in Echtzeit an die Beamten senden. Im Vergleich zu bemannten Polizeihubschraubern bieten Überwachungsdrohnen ebenfalls einige Vorteile, da sie günstiger, leichter, witterungsresistenter und nahezu geräuschlos sind, was insbesondere bei Observierungseinsätzen einen entscheidenden Vorteil darstellt (Tönnemann 2018).

Unter datenschutzrechtlichen Aspekten ist der polizeiliche Einsatz von Überwachungsdrohnen umstritten. So dürfen diese nicht im Zuge von Versammlungen und Demonstrationen eingesetzt werden, da durch die Bildaufnahmen nach geltendem Recht die Versammlungsfreiheit eingeschränkt wird (Truscheit 2017). Auch der Art. 13 Abs.1 GG (Unverletzlichkeit der Wohnung), im Falle von Wohnungsaufnahmen oder Aufnahmen außerhalb der Wohnung sowie der Art. 2 Abs. 1 GG in Ausprägung des Rechts auf informationelle Selbstbestimmung[11] beziehungsweise des Rechts am eigenen Bild (sofern die Aufnahmen geeignet sind, Informationen über die Person zu ermitteln, aufzuzeichnen oder bildlich festzuhalten) können durch den Drohneneinsatz verletzt werden (Gusy 2014, S. 2).

3.3.4 Smartphone und Tablet

Die potentiellen Einsatzmöglichkeiten von Smartphones und Tablets in der Polizeiarbeit sind vielfältig. Die Integration in den Arbeitsalltag der Polizeien in Deutschland verläuft jedoch sehr heterogen. Generell soll mit dem Einsatz von Smartphones und Tablets die Kommunikation, der Informationsaustausch sowie die Serviceleistung gegenüber den Bürgern verbessert

[11] Bezeichnet das vom Bundesverfassungsgericht angesichts der Entwicklung der elektronischen Datenverarbeitung als Ausfluss des allgemeinen Persönlichkeitsrechts und der Menschenwürde (Art 2 Abs. 1 i. V. m. Artikel 1 Abs. 1) anerkannte Recht des Einzelnen grundsätzlich selbst über Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten zu bestimmen. Eingriffe in dieses Recht durch staatliche Informationserhebung und -verwertung sind nur im überwiegenden Allgemeininteresse zulässig und bedürfen einer gesetzlichen Grundlage (bpb 2018).

und Prozesse optimiert werden. Die Polizei Bayern beispielsweise will bis Ende 2018 alle Streifenbeamte mit speziellen Smartphones für den alltäglichen Einsatz ausstatten. Durch einen polizeilichen Messenger-Dienst können Ermittlungshinweise, Fahndungsfotos oder Einsatzbefehle dann schneller an die Beamten übermittelt werden (Holland 2017). Vor Ort können die Beamten selbst digitale Fotos zur Beweissicherung aufnehmen oder eine mobile Unfallaufnahme durchführen. Die saarländische Polizei hat in einem Pilotprojekt Verkehrsunfälle auf Smartphones und Tablets aufgenommen. Hierdurch konnte die Datenerfassung vor Ort verbessert und der einzelne Prozessaufwand deutlich reduziert werden, da die aufgenommenen Daten nicht wie bisher auf der Polizeistation von handschriftlichen Notizen erneut abgetippt, sondern direkt an die Zentrale übermittelt wurden (icomedias 2016). In Niedersachsen werden seit einem Pilotversuch im Jahr 2016 ebenfalls Anzeigen und Unfälle per Tablet aufgenommen (Kutsche 2017).

Mobile smarte Endgeräte ermöglichen der Polizei schnelleres und effizientes Arbeiten, insbesondere durch die Einmalerfassung der Daten direkt am Einsatzort, als auch durch die verbesserte Informationsvermittlung und Kommunikation. Die zugrundeliegenden Betriebssysteme lassen sich außerdem weiterentwickeln und ermöglichen eine unkomplizierte Aufstockung weiterer Anwendungen. Gleichzeitig müssen die Systeme der Smartphones und Tablets unbedingt den hohen Anforderungen an die IT-Sicherheit genügen, da hiermit sensible personenbezogene Daten gespeichert und weitergeleitet werden (Ehneß 2016b).

3.3.5 Apps für Smartphone und Tablet

Der Funktionsumfang von Smartphones und Tablets kann durch mobile Applikationen (Apps) deutlich erweitert werden (Hof 2017, S. 483). Folglich werden diese auch für die Polizeiarbeit immer relevanter. Nicht nur für die eigene Arbeitserleichterung, wie im vorherigen Punkt thematisiert, sondern insbesondere auch, um mit dem Bürger in Kontakt zu treten sowie verbesserte und neue Dienstleistungen anzubieten, spielen mobile Apps eine entscheidende Rolle. Die „Polizei-App“ der Landespolizei Brandenburg beispielsweise beinhaltet unter anderem einen Dienststellenfinder, eine Notruffunktion, Verkehrsübersichten sowie aktuelle Meldungen aus der Region (Polizei Brandenburg 2016). Die sog. „Präventions-App“ der Polizeibehörde Offenbach, sendet Warnmeldungen an die Nutzer. Hierdurch sollen An-

wohner vor Kriminellen oder Unfallgefahren gewarnt werden. Ebenfalls eingebunden ist das vom *Fraunhofer-Institut FOKUS* entwickelte Informations- und Bevölkerungswarnsystem „KATWARN“, mit dem ortsbezogene Gefahren- und Naturkatastrophenwarnungen deutschlandweit an Nutzer verschickt werden können (Monroy 2018; KATWARN 2018).

Im Zusammenhang mit polizeilichen Apps ist auch auf die Bedeutung von Social Media in der Polizeiarbeit hinzuweisen. Die Anzahl polizeilicher *Twitter*-, *Facebook*-, *Instagram*- oder *YouTube*-Accounts ist in den vergangenen zwei Jahren stark gestiegen. Insgesamt gibt es in Deutschland derzeit etwa 300 offizielle Polizei-Accounts, die oftmals von eigenen „Social Media-Teams“ der jeweiligen Polizeibehörden betreut werden (Reuter, Fanta & Bröckling 2018). Die Accounts helfen der Polizei einerseits zur sofortigen Informations*gewinnung*, insbesondere in Krisensituationen, andererseits kann hierdurch die eigene Informations*vermittlung* gesteigert und auf verschiedenen Kanälen kommuniziert werden. Eine verbesserte Beziehungsbildung mit der Bevölkerung und neue Möglichkeiten der Nachwuchsgewinnung sind hier ebenfalls als Potentiale anzuführen. Gleichzeitig erscheint es als zeitgemäß und unabdingbar, dass die Polizei in ihrer Schutz- und Ordnungsfunktion auch im digitalen Raum Präsenz zeigt.[12]

3.3.6 Smarter Polizeieinsatzwagen

Auch polizeiliche Einsatzfahrzeuge werden durch die neuen technologischen Möglichkeiten zu intelligent vernetzten Objekten. Die Polizei Brandenburg beispielsweise fährt ihre Einsätze in interaktiven Funkstreifenwagen mit integriertem Multifunktions-PC, der in die IT-Infrastruktur der Polizei integriert ist. Der Bildschirm im Armaturenbrett liefert Informationen zu Einsätzen und Einsatzorten. Eine integrierte Kamerafunktion im Wagen filmt das Geschehen und sendet die Aufnahmen bei Bedarf in Echtzeit an die Einsatzzentrale. Über eine abgesicherte Breitbandverbindung zum Polizeinetz sind außerdem alle polizeilichen Office- und Webanwendungen, wie Fahndungs- oder Vorgangsbearbeitungssysteme, im Fahrzeug verfügbar. Somit können am Einsatzort direkt Informationen oder Anzeigen aufgenommen und weitergeleitet werden. Die verbesserte Vorgangsbearbeitung durch Einmalerfassung und Mehrfachnutzung unterstützt die Polizei-

[12] Eine ausführlichere Analyse des Social Media Einsatzes der deutschen Polizeien findet sich unter anderem bei Bayerl & Rüdiger (2017).

beamten zudem darin, einen Großteil der Büroarbeiten nicht mehr in der Dienststelle, sondern direkt vor Ort zu erledigen. Durch eingebaute GPS-Sender kann die Einsatzzentrale die Einsatzwagen jederzeit lokalisieren und eine verbesserte und effiziente Verteilung der verfügbaren Kräfte ermöglichen (Kutsche 2017; T-Systems 2018). Vergegenwärtigt man sich die derzeitigen Möglichkeiten und technischen Innovationen im Bereich der Automobilindustrie, ist in Zukunft auch der Einsatz selbstfahrender Polizeiwagen nicht unrealistisch.

3.3.7 Predictive-Policing

Predictive-Policing bezeichnet Big Data-Analyseprogramme, welche Polizeidaten und Statistiken mit externen Datensätzen verknüpfen, um zukünftige Straftaten und Gefahren mit Hilfe von Algorithmen zu prognostizieren. Ausgangspunkt hierfür sind von der Polizei erhobene anonymisierte Daten zu Tatzeit, Tatort oder Art des Verbrechens (Kästner & Kuhlmann 2016). In Deutschland liegt der Einsatzschwerpunkt derzeit bei der Einbruchskriminalität. Grund dafür ist, dass hier besonders häufig Serientäter zu Gange sind, die nach einem bestimmten Muster vorgehen (Krempl 2018). Dieses Muster hat sich das Programm *PRECOBS*[13] zunutze gemacht, welches derzeit von den meisten Polizeibehörden, die Predictive-Policing verwenden oder testen, eingesetzt wird. Das Programm errechnet anhand eingegebener Daten zu Ort, Zeit und Art des Verbrechens mit Hilfe von psychologischen und kriminologischen Theorien, wie der „Near-Repeat-Theorie“[14], die Wahrscheinlichkeit von künftigen Einbrüchen in bestimmten Regionen. Die zuständige Polizeibehörde kann dann gezielt in diesen Gebieten ihre Präsenz erhöhen, um mögliche Straftaten zu unterbinden (IfmPt 2018). Durch die Auswertung und Analyse großer Datenbestände (Big Data) kann die Polizei somit ihre Effizienz steigern sowie den Schutz und die Sicherheit der Bürger verbessern. Mehrere Länderpolizeien nutzen bereits Predictive-Policing Anwendungen, darunter die Stadtstaaten Hamburg und Berlin, aber auch Nordrhein-Westfalen, Niedersachsen, Bayern und Baden-Württemberg. In vielen Städten sank seit der Einführung die Zahl der Wohnungseinbrüche (Jordan 2017). Inwieweit dies jedoch auf den Einsatz der Prog-

[13] *Precobs* steht für „Pre Crime Observation System“ und wurde vom Institut für musterbasierte Prognosetechnik (IfmPt) in Oberhausen entwickelt.

[14] Die Theorie besagt, dass geografische Bezirke, in denen ein Einbruch erfolgt ist, häufig in kurzer Zeit und im direkten Umfeld mit Folgedelikten rechnen müssen (ImfPt 2018).

nosemodelle zurückzuführen ist, kann derzeit noch nicht eindeutig belegt werden (Gerstner 2017, S. 85).

3.4 Konzept Polizei 2020

Im Zusammenhang mit Smarter Polizeiarbeit beziehungsweise dem polizeilichen Einsatz smarter Anwendungen muss auch auf die IT-Systeme der Polizeien eingegangen werden, auf welchen die erfassten Daten (beispielsweise generiert durch smarte Objekte) gespeichert und weiterverarbeitet werden. Die IT der Bundespolizei sowie die der Länderpolizeien ist über Jahrzehnte organisch gewachsen. Mittlerweile existieren verschiedene Systeme und Verfahren, die nur zum Teil miteinander verbunden sind und nur einen begrenzten Datenaustausch untereinander zulassen. In Zeiten globaler Gefahrenlagen und einer voranschreitenden Digitalisierung ist dies nach Ansicht des Bundesinnenministeriums jedoch nicht mehr zeitgemäß und behindert die mittlerweile notwendige Zusammenarbeit der einzelnen Polizeien (Schulzki-Haddouti 2017). Im November 2016 haben sich die Innenminister auf der Innenministerkonferenz[15] daher auf die „Saarbrückener Agenda" bezüglich der künftigen Informationsarchitektur der deutschen Polizeien verständigt, um das Informationsmanagement grundlegend zu modernisieren und zu vereinheitlichen. Kernziele sind die Verbesserung der Verfügbarkeit polizeilicher Informationen, die Erhöhung der Wirtschaftlichkeit sowie die Stärkung des Datenschutzes durch Technik (BMI 2017, S. 2).

Mit dem in diesem Zusammenhang aufgesetzten Konzept „Polizei 2020"[16] soll ein neues polizeiliches IT-System für Bund und Länder implementiert werden. Das Informationswesen der Polizeien des Bundes und der Länder soll vereinheitlicht und harmonisiert werden, indem die verschiedenen Systeme konsolidiert und an zentraler Stelle einheitliche, moderne Verfahren entwickelt werden, die dann von allen Polizeien nach gleichen Standards implementiert und genutzt werden (BMI 2017, S. 2). Das einheitliche länderübergreifende IT-Verbundsystem mit zentraler Datenhaltung im BKA

[15] Die Innenministerkonferenz (IMK) ist eine zweimal im Jahr stattfindende Konferenz der Innenminister und Innensenatoren der deutschen Länder. Der Bundesinnenminister nimmt als Gast ebenfalls an den Konferenzen teil. Wesentlicher Bestandteil dieser Konferenzen sind die länderübergreifenden Strategien und Beschlüsse zur Inneren Sicherheit.

[16] Für ein Schaubild des Konzepts siehe Anhang II.

stellt das sog. „Datenhaus“ dar. Hier soll die einheitliche Informationstechnik zur Verfügung gestellt und Prozesse koordiniert werden (Ehneß 2017; Schulzki-Haddouti 2017).

Ein weiterer Grund für die Überarbeitung und Modernisierung der polizeilichen IT-Systeme ist das BKA-Urteil des Bundesverfassungsgerichts aus dem Jahr 2016. Hierin wurden die verfassungsrechtlichen Anforderungen an Zweckbindung und Zweckänderung von Daten fortentwickelt. Die Verhältnismäßigkeitsanforderungen für eine solche Zweckänderung haben sich am Grundsatz der *hypothetischen Datenneuerhebung*[17] zu orientieren. Mit „Polizei 2020“ sollen diese Anforderungen umgesetzt sowie ein intelligenter Datenschutz und die sichere Gestaltung der IT-Systeme verwirklicht werden. Personendaten werden fortan nicht mehrfach in verschiedenen Systemen gespeichert, sondern zentralisiert im Datenhaus des BKA, wo der Zugriff auf die Daten über zielgerichtete und strenge Berechtigungskonzepte reglementiert wird (BMI 2017, S. 3). Das bisherige polizeiliche Informationssystem INPOL[18] erfülle die Vorgaben aus dem BKA-Urteil nicht, was eine Umstrukturierung der polizeilichen IT-Systeme notwendig mache (Ehneß 2017).

Kritiker, wie die Partei *Bündnis 90/Die Grünen*, sehen in dem Programm eine Ermächtigungsgrundlage für das BKA, alle polizeilichen Informationen und Daten ohne Zweckbindung (einem Eckpfeiler des Datenschutzes) zu sammeln und durch Verfahren miteinander abzugleichen. Hierdurch ergäben sich neue undifferenzierte Raster- und Suchmöglichkeiten in den polizeilichen Datenbeständen (Ehneß 2017).

3.5 Smarte Polizeiarbeit im Ausland

Im Folgenden sollen zwei Beispiele einer Smarten Polizeiarbeit im Ausland vorgestellt werden. Anhand des Beispiels aus Dubai sollen die bereits exis-

[17] Danach muss die Nutzung von Daten dem Schutz von Rechtsgütern oder der Aufdeckung von Straftaten eines solchen Gewichts dienen, die verfassungsrechtlich ihre Neuerhebung mit vergleichbar schwerwiegenden Mitteln rechtfertigen können. Eine konkretisierte Gefahrenlage wie bei der Datenerhebung ist demgegenüber grundsätzlich nicht erneut zu verlangen; erforderlich, aber auch ausreichend ist in der Regel das Vorliegen eines konkreten Ermittlungsansatzes (Bundesverfassungsgericht 2016b, Abs. 4)

[18] INPOL ist ein polizeiliches IT-Verbundsystem, welches von den Polizeibehörden des Bundes und der Länder gemeinsam genutzt wird.

tierenden technischen Möglichkeiten aufgezeigt werden. Das Beispiel des West Midlands Police Departments hingegen kann im Hinblick auf die Arbeitsdefinition einer Smarten Polizeiarbeit als Best-Practice-Beispiel eingeordnet werden.

Das Emirat Dubai hat 2009 das „Dubai Smart Government Department" errichtet, mit dem die Zuständigkeiten für das Gesamtangebot an Verwaltungsinformationen und elektronischen Verwaltungsleistungen neu gebündelt wurden (von Lucke 2015, S. 3). Bis 2021 sollen Maschinen ein Viertel der Polizeiaufgaben in Dubai übernehmen - bis 2030 soll die gesamte öffentliche Verwaltung Dubais ohne Papier auskommen. Einen Schritt in diese Richtung stellt die weltweit erste unbemannte smarte Polizeistation dar. Diese bietet 60 verschiedene Serviceleistungen an. Bürger können hier Bußgelder bezahlen sowie digital Anzeigen aufgeben. Strafzettel werden in Dubai per App ausgestellt und gezahlt, smarte Polizeieinsatzwagen mit smarten Videoüberwachungskameras auf dem Dach liefern umfassende Lagebilder. Flächendeckend angebrachte stationäre Videokameras nehmen so gut wie jeden Winkel der Stadt auf. Autonome Polizeiroboter, ausgestattet mit Aufklärungsdrohnen, Gesichtsscannern und Wärmebildkameras patrouillieren durch Straßen und Parks. Die gesammelten Daten sowie die Live-Bilder aller smarten Anwendungen werden in die Leitstelle der Polizei gesendet, wo die Daten in Echtzeit mit verschiedenen Datenbanken abgeglichen werden, die etwa Gesichtsprofile gesuchter Personen oder Nummernschilder gestohlener Autos enthalten (Krüger 2017; Al Shouk 2017; Wilkens 2017). Die neueste technische Innovation der Polizei Dubai ist ein lebensgroßer humanoider Polizeiroboter, der ab 2019 flächendeckend zum Einsatz kommen soll. Der Roboter ist mit zwei Kameraaugen ausgestattet, welche Gesichter, Körpersprache und Gesten erkennen können und Live-Bilder in die Polizeizentrale senden. Über ein Stimmerkennungsprogramm kann der Roboter in Englisch und Arabisch kommunizieren. Mittels eines Touchscreens auf Brusthöhe können Anzeigen aufgenommen, Informationen abgerufen sowie eine Sprechverbindung zu einem Polizeioffizier hergestellt werden. Ziel der Polizei Dubai ist es, bis 2030 ein Viertel ihrer Polizeibeamten durch humanoide Polizeiroboter zu ersetzen (Breslin 2017). Datenschutz sowie rechtliche Grenzen der Datensammlung und des -abgleichs existieren in Dubai allerdings nur in geringem Maße. Kombiniert man die Gesichts- und Nummernschilderkennung sowie die Überwachung öffentlicher Verkehrsmittel und Straßen scheint die Polizei hier in der Lage

lückenlose und umfassende Bewegungsprofile aller Bürger zu erstellen. Inwieweit dies zum selbsternannten Ziel der „glücklichsten Stadt der Welt" beiträgt, erscheint in Kombination mit dem Vorwurf zahlreicher Menschenrechtsverletzungen seitens des Emirats höchst fraglich (Krüger 2017; Amnesty International 2018).

2015 startete die britische Polizeibehörde *West Midlands Police* (WMP) ein umfassendes Transformationsprogramm mit den Zielen, die Kosten polizeilicher Arbeiten zu senken, die Effektivität der Polizei zu steigern sowie die Bürger durch neue und verbesserte Dienstleistungen stärker in die Arbeit der Polizei einzubinden (McCarthy 2015). Hieraus entstand die Vision „WMP 2020", welche sich aus 30 verschiedenen Projekten und Komponenten zusammensetzt. Bürgerbeteiligung, Nachhaltigkeit sowie die Integration intelligent vernetzter IKT bilden dabei die drei Grundpfeiler (West Midlands Police 2018). Über ein Bürger-Uploadportal können beispielsweise digital Anzeigen aufgegeben, Delikte gemeldet und Informationen abgerufen werden. Des Weiteren kann der aktuelle Bearbeitungsstand eines Falls oder einer Anzeige jederzeit eingesehen werden. Der Faktor Nachhaltigkeit soll durch evidenzbasierte Entscheidungen mittels neuer Möglichkeiten polizeilicher Big Data-Analysen gesichert werden. Die eingesetzten intelligent vernetzten IKT umfassen unter anderem 1.500 Body-Cams sowie 3.000 Smartphones und Tablets mit Zugang zu einer digitalen Polizei-Plattform. Ein Echtzeitinformationszentrum versorgt die Beamten am Einsatzort sowie auf Streife mit benötigten Informationen. Predictive-Policing sowie weitere integrierte Big Data-Analysen sollen zu einer effektiven und effizienten Erledigung polizeilicher Aufgaben und der Vorbeugung von Straftaten beitragen (Accenture 2018; McCarthy 2015).

4 Methodik

Dieses Kapitel setzt den methodischen Rahmen für die nachfolgende empirische Untersuchung. Ziel dieser Untersuchung ist eine Analyse des Status Quo der Smarten Polizeiarbeit sowie ein Aufzeigen der hieraus resultierenden perspektivischen Chancen, Risiken und Herausforderungen für die Bürger, als auch für die Polizeien selbst. Diese Arbeit, beziehungsweise die folgende Analyse, bewegt sich somit im Feld der empirischen Sozialforschung. Da es sich bei der Untersuchung zum einen um die Deskription empirischer Sachverhalte und Prozesse handelt, politisch-gesellschaftliche Phänomene untersucht werden und zum anderen nur wenig wissenschaftliche Fachliteratur besteht, wurde ein qualitativ-exploratives Forschungsdesign gewählt. Hiermit lassen sich jene Sachverhalte, Prozesse und Phänomene bestmöglich identifizieren und analysieren (Dieckmann 2013, S. 532; Gläser & Laudel 2010, S. 71). Als qualitative Methode wurde das leitfadengestützte Experteninterview verwendet, da die Befragung nach wie vor als „das Standardinstrument empirischer Sozialforschung" (Schnell, Hill & Esser 2008, S. 321) bei der Ermittlung und Bewertung von Fakten, Wissen, Meinungen oder Einstellungen im sozialwissenschaftlichen Anwendungsbereich gilt (ebd.). Im Folgenden soll daher das Experteninterview kurz definiert und als Methode vorgestellt werden. Daran anknüpfend wird im Sinne der Transparenz und des Gütekriteriums der intersubjektiven Nachvollziehbarkeit (Kaiser 2014, S. 71) die Auswahl der Experten und die Erstellung des Leitfadens skizziert sowie abschließend auf die Auswertung der Interviews eingegangen.

4.1 Experteninterview als Methode

Kaiser (2014) definiert qualitative Experteninterviews als ein „systematisches und theoriegeleitetes Verfahren der Datenerhebung in Form der Befragung von Personen, die über ein exklusives Wissen verfügen" (S. 6). Der Befragte ist dabei weniger als Person, sondern in seiner Funktion als Experte für ein bestimmtes Themenfeld interessant (Mayer 2006, S. 37). Basierend auf der Typologie von Menz, Bogner & Littig (2009, S. 64) kann die vorliegende Untersuchung als „systematisierend" eingeordnet werden. Aufbauend auf dem Wissen, das sich der Forscher bereits durch Literatur-

und Dokumentenanalyse angeeignet hat, ist das systematisierende Experteninterview auf die Teilhabe an exklusivem Expertenwissen ausgerichtet. Der Experte ist hierbei als Inhaber von spezifischen gültigen Kenntnissen und Informationen zu sehen, der über ein bestimmtes, dem Forscher nicht zugängliches, Fachwissen verfügt (Menz et. al. 2009, S. 65).

4.2 Expertenauswahl

Generell lassen sich zwei maßgebliche Kriterien zur Identifikation von relevanten Experten feststellen: Zum einen Position und Status und zum anderen Funktionswissen (Kaiser 2014, S. 41). Als Experte kann also gelten, wer in irgendeiner Art und Weise Verantwortung trägt für den Entwurf, die Implementierung oder die Kontrolle einer Problemlösung beziehungsweise über einen privilegierten Zugang zu Informationen über Personengruppen oder Prozesse verfügt (Meuser & Nagel 2004, S. 73). Als Experte kann aber auch gelten, wer über relevantes Wissen über die Prozesse und/oder Problemlösungen verfügt (Kaiser 2014, S. 41). Es gilt zu berücksichtigen, dass die Zuschreibung der Expertenrolle immer durch den Forscher selbst im konkreten Forschungsprozess erfolgt. Er muss also letztlich entscheiden, wer vor dem Hintergrund der jeweiligen Forschungsfragen(n) über privilegierte Informationen verfügt und bereit ist, diese preiszugeben (ebd., S. 39). Eine festgelegte oder notwendige Anzahl geführter Interviews existiert nicht, sondern ergibt sich vielmehr aus der Verteilung von Informationen unter den Akteuren (Gläser & Laudel 2010, S. 104). Eine größere Anzahl an Interviews ist daher kein zwingendes Argument für die „größere Richtigkeit“ der Informationen beziehungsweise der nachfolgenden Analyse (ebd., S. 105).

Im Vordergrund der qualitativen Expertenbefragung steht daher vielmehr die Einbeziehung diverser Perspektiven und Interessenslagen seitens der Experten (Mayer 2006, S. 38). Um diese Perspektivenvielfalt zu gewährleisten, wurde versucht, Experten aus unterschiedlichen Sektoren und Bereichen miteinzubeziehen (van Dyck 2016, S. 54). Siller (2017, S. 1023-1024) vollzieht eine Analyse der Anspruchsgruppen (Stakeholder) der „Dienstleistungsorganisation Polizei“. Neben internen Stakeholdern, die Mitarbeiter der Polizei selbst, definiert er unter anderem als externe Stakeholder Vertreter aus den folgenden Bereichen: Politik, Bürger/Wähler, Wirtschaft, Justiz, Medien, öffentliche Verwaltung und Wissenschaft. Basierend auf dieser

Einordnung und der eigenen Recherche sollen die Experten demnach aus den folgenden Sektoren beziehungsweise Bereichen kommen: Polizei, Politik, Wirtschaft, Justiz, Verwaltung, Medien und Wissenschaft. Die Auswahl der kontaktierten Experten aus den oben genannten Bereichen orientierte sich an folgenden drei Kriterien:

1. Welche Experten verfügen über die relevanten Informationen?
2. Welcher dieser Experten ist am ehesten in der Lage, präzise Informationen zu geben?
3. Welcher dieser Experten ist am ehesten bereit und verfügbar, diese Informationen zu geben? (Gläser & Laudel 2010, S. 117).

Von 25 kontaktierten Experten haben 19 geantwortet. Sechs davon haben direkt abgesagt und bei drei Experten kam es aus diversen Gründen nicht zu einem Interview. Insgesamt wurden zehn Interviews mit Experten geführt, wovon zwei jedoch einer Sprachaufnahme nicht zugestimmt haben und daher nur als Hintergrundgespräche in die Analyse aufgenommen werden können.

Kürzel	*Position*	*Bereich/Sektor*
E1	Führungskraft in einem Landespolizeipräsidium	Polizei
E2	Wissenschaftler	Wissenschaft
E3	Politischer Vertreter auf Landesebene	Politik
E4	Führungskraft in einem Technologieunternehmen	Wirtschaft
E5	Landesbeauftragter für den Datenschutz	Unabhängige Institution
E6	Berater in einem Technologieunternehmen	Wirtschaft
E7	Mitarbeiter in einem Bundesministerium	Verwaltung
E8	Politischer Aktivist (Journalist)	Zivilgesellschaft/Medien

Tabelle 3 Übersicht zu den geführten Experteninterviews mit Bezeichnung und Einordnung in die Expertenbereiche

Tabelle 3 zeigt die anonymisierte Übersicht zu den acht geführten Experteninterviews.[19] [20]

4.3 Erstellung des Interviewleitfadens

Das in 4.1 thematisierte Fachwissen des Experten sollte stets durch einen relativ ausdifferenzierten Leitfaden erhoben werden (Menz et. al. 2009, S. 65). Der Leitfaden ist das Instrument der Datenerhebung und erhöht die Vergleichbarkeit der Daten. Er dient als Gerüst und stellt sicher, dass keine wesentlichen Aspekte der Forschungsfrage im Interview übergangen werden (Mayer 2006, S. 36). Die *Übersetzung* der Forschungsfragen in die Interviewfragen des Leitfadens wird als *Operationalisierung* bezeichnet, welche in zwei konkreten Schritten verläuft. Erstens muss der Forschungsgegenstand so konkretisiert werden, dass sich daraus geeignete Fragen für ein Interview entwickeln lassen (konzeptionelle Operationalisierung). Zweitens muss daraufhin überlegt werden, mit welcher Art von Fragen die gewünschten Informationen am besten erhalten werden können (instrumentelle Operationalisierung). Ziel der Operationalisierung ist es, den eigenen Forschungsgegenstand in den jeweiligen Kontext des befragten Experten zu übertragen, so dass dieser in der Lage ist, die Informationen zu liefern, die für die Beantwortung der Forschungsfragen notwendig sind (Gläser & Laudel 2010, S. 142; Kaiser 2014, S. 55). So musste in dieser Arbeit die Forschungsfrage, welche Perspektiven sich durch eine Smarte Polizeiarbeit ergeben und wie der derzeitige Status Quo einzuordnen ist, in geeignete Interviewfragen übersetzt werden.[21] Entsprechend des Grundsatzes der Offenheit ist eine Abweichung vom Leitfaden in der konkreten Interviewsituation, etwa durch Nachfragen, ausdrücklich möglich (Kaiser 2014, S. 53). Der Leitfaden ist daher vielmehr eine Richtschnur, welche die unbedingt zu stellenden Fragen enthält (Gläser & Laudel 2010, S. 42). Vier der acht Interviews wurden persönlich und vier telefonisch durchgeführt.

[19] Um eine vollständige Anonymisierung zu gewährleisten, wird im Folgenden in Bezug auf die befragten Expertinnen und Experten ausschließlich die männliche grammatikalische Form verwendet.

[20] Für eine ausführlichere Übersicht zu den Experteninterviews siehe Anhang III.

[21] Eine Übersicht zur Operationalisierung der Forschungsfragen sowie der Fragebogen selbst finden sich in Anhang IV und V.

4.4 Auswertung der Interviews

Ziel der Auswertung ist es, durch den Vergleich der erhobenen Interviews das Überindividuell-Gemeinsame sowie die Unterschiede in den Expertenaussagen herauszuarbeiten (Mayer 2006, S. 46). Die Auswertung erfolgte mittels der qualitativen Inhaltsanalyse, welche sich in diesem Bereich als eine zuverlässige Methode bewährt hat (Gläser & Laudel 2010, S. 197). Bei der Auswertung sind dabei vier Schritte zu beachten:

1. Das Aufbauen eines geschlossenen Kategoriensystems vor der Analyse
2. das Zerlegen des Textes in Analyseeinheiten
3. das Durchsuchen des Textes auf relevante Informationen und
4. das Kodieren, also die Zuordnung dieser Informationen zu den Kategorien (Gläser & Laudel 2010, S. 197).

Um diese Auswertung zu ermöglichen, müssen die geführten Experteninterviews transkribiert werden. Die Transkription sowie die anschließende qualitative Inhaltsanalyse erfolgten mittels des Programms *MaxQDA*, welche das Vergleichen von Textstellen durch einfache Handhabung sowie die Visualisierung des Kategoriensystems und das schnelle Kodieren von Textstellen ermöglicht (Kuckartz 2005, S. 20). Dabei wurden die Experteninterviews paraphrasiert und den jeweiligen Kategorien zugeordnet beziehungsweise kodiert.[22] Die Auswertung der Experteninterviews wird an manchen Stellen außerdem um die Analyse von Dokumenten erweitert. Diese Ergänzung, welche in der qualitativen Politikforschung als gängige Methode gilt, bezeichnet man als „Triangulation" (Gläser & Laudel 2010, S. 105; Kaiser 2014, S. 111). Ziel der Erweiterung der Datenbasis ist es, die Expertenaussagen zu kontextualisieren sowie gleichzeitig den wissenschaftlichen Ertrag der Analyse zu steigern und zusätzliche Perspektiven einfließen zu lassen (Kaiser 2014, S. 114).

Im Folgenden soll zuerst eine wertfreie Darstellung der Expertenaussagen in den jeweiligen Kategorien erfolgen, ehe eine kritische Einordnung und Analyse der Kernaussagen in Kapitel 7 vorgenommen wird (vgl. Kaiser 2014).

[22] Das Kategoriensystem orientiert sich dabei an den Analysedimensionen und Fragenkomplexen, die durch die Operationalisierung der Forschungsfrage festgelegt wurden.

5 Darstellung der empirischen Ergebnisse

Im Folgenden werden die Ergebnisse der Expertenbefragung urteilsfrei dargestellt und strukturiert aufbereitet. Aus den Interviews wurden 540 relevante Textstellen gewonnen. Zur besseren Strukturierung wurden diese verschiedenen Kategorien zugeordnet. Dabei soll zuerst der bisherige Status Quo der Smarten Polizeiarbeit thematisiert werden. Welches Begriffsverständnis teilen die Experten in Bezug auf eine Smarte Polizeiarbeit? Wie werden die vorgestellten smarten Objekte und Anwendungen bewertet? Welche Barrieren existieren derzeit und wer sind die Thementreiber einer Smarten Polizeiarbeit? Daran anknüpfend werden Potentiale smarter Objekte und Anwendungen für die Aufgabengebiete der Polizeien thematisiert sowie Visionen und zukünftige Themenfelder einer Smarten Polizeiarbeit aufgezeigt.

5.1 Wofür steht Smarte Polizeiarbeit?

Wie in dieser Arbeit bereits dargelegt werden konnte, mangelt es in Wissenschaft und Praxis derzeit an einem einheitlichen Begriffsverständnis einer smarten Polizeiarbeit. Für den Großteil der Experten impliziert der Begriff *Smarte Polizeiarbeit* vor allem die Nutzung moderner, intelligenter IT-Lösungen und Technologien in der Polizeiarbeit (E1 2018, 01:44; E3 2018, 02:40; E4 2018, 04:26; E6 2018, 14:06; E7 2018, 02:30). Dies geschehe, um bestehende Prozesse zu vereinfachen (E1 2018, 02:55; E4 2018, 04:45; E7 2018, 03:02) sowie komplexe Strukturen aufzuweichen und zu verschlanken (E7 2018, 03:10). Für die Führungskraft in einem Landespolizeipräsidium bedeutet *smart* in diesem Zusammenhang außerdem die Ableitung eines strukturierten Nutzens für die Polizeien mittels Big Data-Analysen (E1 2018, 01:44). Die Steigerung der Produktivität sowie die Verbesserung der Einsatzbewältigung mittels digitaler Technologien seien ebenfalls als Elemente einer Smarten Polizeiarbeit zu nennen (E3 2018, 02:40; E6 2018, 14:10;). Nach Ansicht der Führungskraft in einem Technologieunternehmen sowie dem Mitarbeiter eines Bundesministeriums erstrecke sich Smarte Polizeiarbeit insbesondere auch auf den Einsatz mobiler smarter Endgeräte (E4 2018, 04:40; E7 2018, 03:30). Der Landesdatenschutzbeauftrage versteht unter Smarter Polizeiarbeit vor allem polizeiliche IT-Systeme und Anwen-

dungen, „die etwas mehr oder weniger autonom verarbeiten" (E5 2018, 01:47). Smart bedeute hierbei aber gleichzeitig auch, eine gesellschaftliche Verantwortung wahrzunehmen, im Sinne einer „Social Responsibility" (E6 2018, 14:30), sowie responsiv auf gesellschaftliche Entwicklungen einzugehen (E2 2018, 00:20).

„Ich habe große Probleme mit dem Begriff" (E8 2018, 02:49) konstatiert hingegen der politische Aktivist. Demnach ginge es den Polizeien derzeit vor allem darum, mit allen technischen Mitteln die Überwachung der Bevölkerung zu verbessern. Smarte Polizeiarbeit oder auch *Smart Policing* sei dabei vielmehr ein „smarter Begriff, der [...] kaschiert, worum es eigentlich geht" (E8 2018, 03:25). Auch der Wissenschaftler hat Schwierigkeiten mit dem Begriff, da die Polizeien zwar in der Lage seien, mittels smarter Informations- und Kommunikationstechniken „einiges zu machen, was sicherlich auch der Sicherheit dient" (E2 2018, 00:37), ob dies dann aber rechtsstaatskonform oder datenschutzfreundlich ist, sei dabei oftmals ungeklärt (E2 2018, 01:15).

Auf die Frage, wie die Experten den derzeitigen Status Quo der Polizeiarbeit in Bezug auf die Digitalisierung bewerten, war sich die Mehrheit der Befragten darüber einig, dass eine flächendeckende Bewertung aufgrund der Heterogenität der Polizeien zwar nicht unproblematisch sei (E1 2018, 04:40; E3 2018, 03:05; E4 2018, 05:35; E7 2018, 04:10; E8 2018, 04:25), insgesamt jedoch in fast allen Bereichen und Behörden teils erheblicher Nachholbedarf bestehe (E1 2018, 04:43; E3 2018, 04:16, 08:11; E4 2018, 06:00; E6 2018, 19:52; E7 2018, 04:35). Die nur schleppend voranschreitende Digitalisierung der öffentlichen Verwaltung in Deutschland könne auch auf die Polizeien übertragen werden (E5 2018, 03:55). Insgesamt hinke man von den Möglichkeiten ausgehend, die derzeit bestehen, eindeutig hinterher (E1 2018, 04:56; E6 2018, 19:52). „[...] zum Teil ist es an manchen Stellen einfach Steinzeit" (E7 2018, 06:20). Generell befinde man sich derzeit vor allem im Web 1.0 (E1 2018, 06:39) und durch die zunehmende Verbreitung polizeilicher Social Media-Accounts in der Interaktion mit dem Bürger auch mehrheitlich im Web 2.0-Bereich (E1 2018, 06:18; E2 2018, 01:27; E4 2018, 07:16). Anwendungen im Web 3.0-Bereich fände man vor allem bei Länderpolizeien, die bereits Predictive-Policing oder andere Big Data-Analysen einsetzen (E1 2018, 05:58; E4 2018 07:36; E5 07:20). „Es gibt auch schon IoT-Anwendungen [...] also in einigen Pilotprojekten ist man da auf der

Ebene Web 4.0 angekommen“ (E4 2018, 07:43). Der Berater in einem Technologieunternehmen schätzt den Status Quo der Bundespolizei sowie des BKAs dabei bereits fortgeschrittener ein, als den der Länderpolizeien (E6 2018, 24:29).

5.2 Bewertung der smarten Objekte und Anwendungen

Die Funktionsweisen und Einsatzszenarien der smarten Objekte und weiteren Anwendungen wurden bereits in Punkt 3.3 vorgestellt. Im Folgenden sollen die Einschätzungen und Bewertungen der Experten hierzu dargelegt werden.

Body Cam

Grundsätzlich vertreten die Experten hinsichtlich des polizeilichen Einsatzes der Body-Cam unterschiedliche Standpunkte. Für den politischen Vertreter auf Landesebene nehme hierdurch vor allem die Transparenz polizeilichen Handelns zu (E3 2018, 33:08). Nachweisbar ginge auch die Gewalt gegenüber Einsatzkräften „massiv zurück“ (E3 2018, 34:00). Die Body-Cam liefere außerdem einen entscheidenden Beitrag zur Situationsaufklärung, da im Internet oftmals *YouTube*-Videos privater Nutzer kursierten, auf denen nur noch zu sehen sei, wie die Polizei bereits eingreife. Durch den Einsatz der Body-Cam könne nun auch transparent festgestellt werden, wie es zur Eskalation der Lage kam (E3 2018, 33:28). Für den Wissenschaftler liegen die Potentiale der Body-Cam ebenfalls in der Deeskalation und der Beweissicherung (E2 2018, 04:26). Letztlich diene die Body-Cam dazu, in alle Richtungen Beweise liefern zu können, was dann natürlich auch für Verfehlungen der Polizei selbst gelte (E4 2018, 19:35).

Der Landesdatenschutzbeauftragte steht dem Einsatz von Body-Cams kritisch gegenüber. Er bemängelt vor allem die bisherigen Pilotversuche. Es sei hierbei unklar, auf welcher wissenschaftlichen Grundlage die Kriterien in den derzeitigen Pilotprojekten entwickelt wurden, um mögliche Grundrechtsbeeinträchtigungen messen zu können (E5 2018, 22:51). Grundrechtseingriffe fänden beim Einsatz der Body-Cam in zweierlei Hinsicht statt: Zum einen in die Grundrechte der Personen, welche die Polizei beobachte und aufnehme. Die Aufnahme durch eine Body-Cam stelle einen gezielten Eingriff in das Persönlichkeitsrecht dar, welcher wesentlich inten-

siver sei als beispielsweise die Überwachung öffentlicher Räume (E5 2018, 23:55). Zum anderen sei auch die bereits thematisierte Pre-Recording Funktion als problematisch einzustufen: Werden die Polizeibeamten zukünftig standardmäßig und flächendeckend mit Body-Cams ausgestattet, sehe er hierin eine verfassungswidrige Vorratsdatenspeicherung, da kein Betroffener, weder die Polizisten noch die Bürger, vorhersehen könne, wann die Aufnahme einer Situation nun wirklich gestartet wurde. Es könne hierdurch zu einer dauerhaften mobilen Überwachung der Bürger kommen. „Das wäre aus meiner Sicht verfassungswidrig" (E5 2018, 24:55). Auch aus der Sicht der Polizeibeamten sei die Body-Cam als problematisch einzuordnen, da sie sich dazu eigne, das Verhalten sowie die Leistung des Beamten jederzeit zu kontrollieren (E5 2018, 28:14). Er lehne den Einsatz der Body-Cam daher in der derzeitigen Ausprägung aus den angeführten datenschutzrechtlichen Gründen ab (E5 2018, 30:35).

(Smarte) Videoüberwachung

Gegen die stationäre Videoüberwachung an sogenannten Brennpunkten beziehungsweise Kriminalitätsschwerpunkten sei laut des Wissenschaftlers grundsätzlich nichts einzuwenden (E2 2018, 05:22; E6 2018, 46:40). Der Berater eines Technologieunternehmens verweist darauf, dass eine Reihe von Straftaten[23] in den letzten Jahren insbesondere durch die Auswertung von Videos aus Überwachungskameras aufgeklärt werden konnten (E6 2018, 46:45). Bezüglich des Einsatzes von smarter Videoüberwachung verweist die Führungskraft eines Landespolizeipräsidiums auf das Mannheimer Projekt, in dem algorithmusbasiert auffällige Verhaltensmuster erkannt und gemeldet werden (siehe 3.3.2). Dies diene in erster Linie dazu, Ressourcen zu sparen, da Einsatzkräfte nun gezielter koordiniert werden könnten (E1 2018, 14:49). Für den Einsatz smarter Videoüberwachung mit unterlegter Gesichtserkennungssoftware, wie im Falle des Pilotprojekts am Berliner Südkreuz, fehle jedoch die Rechtsgrundlage, konstatiert der Landesdatenschutzbeauftragte (E5 2018, 11:51). Die gesetzlichen Regelungen zur Videoüberwachung würden hierbei nicht ausreichen und die bestehenden Regelungen bezüglich des polizeilichen Datenabgleichs ebenfalls nicht. Man müsse hier also zuerst die rechtliche Grundlage für den Einsatz smarter

[23] Gemeint sind hier die Geschehnisse rund um die Kölner Silvesternacht 2015 sowie der Versuch sechs Jugendlicher, im Dezember 2016 einen Obdachlosen in einer Berliner U-Bahn-Station in Brand zu setzen. In beiden Fällen konnten Videoaufnahmen zur Überführung einiger beziehungsweise der Täter beitragen (E6 2018, 46:34; Gehrke 2017).

Videoüberwachung schaffen. Hier brauche man „gesonderte verfassungsrechtliche Schutzwälle zum Schutz des Persönlichkeitsrechts“ (E5 2018, 12:40). Der bisherige Einsatz sei daher als höchst kritisch einzuordnen.

> „Es darf keine flächendeckende smarte Videoüberwachung geben [...]. Dass das Berlin Südkreuz [Pilotprojekt] auf alle Bahnhöfe ausgedehnt wird, wäre schlichtweg verfassungswidrig“ (E5 2018, 13:52).

Der Mitarbeiter eines Bundesministeriums stellt ebenfalls fest, dass man bei der smarten Videoüberwachung im Zusammenhang mit der Gesichtserkennung derzeit noch an rechtliche Grenzen stoße, die es zu klären und deren Schranken es einzuhalten gelte. Systeme, die musterbasiert beispielsweise liegengebliebene Gepäckstücke identifizieren und melden, seien seiner Meinung nach jedoch durchaus legitim und sinnvoll (E7 2018, 31:30).

Überwachungsdrohne

Der Experte der Polizei stellt fest, dass Überwachungsdrohnen in einigen polizeilichen Aufgabenbereichen bereits zur Arbeitsunterstützung beitragen (E1 2018, 25:45). Im Falle einer Gefahrenlage, bei der beispielsweise giftige Chemikalien austraten, die den Zugang der Polizeibeamten zum Tatort erschwerten, konnten durch den Einsatz der Überwachungsdrohnen erste Aufklärungsbilder gesendet werden. Auch bei Großveranstaltungen trage die Drohne zu einer verbesserten Situationsanalyse für die zuständige Polizeibehörde bei (E1 2018, 25:46). Gleichzeitig sei die Abwehr privater Drohnen ebenfalls ein Feld, dem man sich zunehmend widmen würde (E1 2018, 26:50). Drohnenbilder gepaart mit Social Media-Analysen würden für die Polizei neue und verbesserte Möglichkeiten der Lage-erörterung bieten (E3 2018, 18:00). Auch bei der Täterverfolgung könnten polizeiliche Überwachungsdrohnen zukünftig vermehrt eingesetzt werden, da sie im Vergleich zu einem Polizeihubschrauber einige Vorteile bieten (E3 2018, 19:00; Punkt 3.2.3). Die Überwachung von Versammlungen durch polizeiliche Überwachungsdrohnen sei allerdings aus verfassungsrechtlicher Sicht höchst problematisch, da dies einen Eingriff in die Versammlungsfreiheit nach Art. 8 GG darstelle (E5 2018, 14:15).

Smartphone, Tablet und Apps

Zielrichtung für die kommenden Jahre müsse es sein, dass die mobile polizeiliche Vorgangs- und Fallbearbeitung vor Ort letztlich komplett durch Smartphones oder Tablets erfolge.

> „Momentan sind wir da aber nicht mal bei Web 1.0, sondern bei *Web 0.5*, indem wir letztlich alles in Papierform aufnehmen und es dann auf der Dienststelle nochmals abgetippt wird" (E1 2018, 24:25).

Dies müsse sich hinsichtlich einer Smarten Polizeiarbeit in Zukunft anders darstellen. Die Übertragung vom Händischen ins Digitale sei nicht mehr zeitgemäß und müsse daher effizienter und effektiver gestaltet werden, indem die Daten einmal digital aufgenommen und dann strukturiert abgelegt und weiterverarbeitet werden (E1 2018, 25:00). Eine auf dem Smartphone oder Tablet aufsetzende App-Suite für die mobile Polizeiarbeit sei hier beispielsweise ein Schritt in die richtige Richtung (E4 2018, 21:50). Hierdurch könnten verschiedene Systeme, wie KfZ-Halter-Datenbanken, Einwohnermeldesysteme oder INPOL-Fahndungssysteme parallel abgerufen werden, was die Arbeit der Polizei deutlich effektiver gestalten würde. Dies würde zu einer erheblichen Effizienzsteigerung der Polizeiarbeit führen im Vergleich zu dem,

> „[...] was der Polizist heute noch mit seinem [...] Digitalfunkknochen macht, [...] indem er die Daten durchgibt und dann Auskunft erhält [...], so ist ja heute noch der Standard" (E4 2018, 16:27).

Eine sichere Messenger-Lösung für Polizeibeamte fordert der Experte aus der Politik. Es sei ansonsten eine Verlagerung auf private Messenger-Dienste zu befürchten, was aufgrund der sensiblen Kommunikationsinhalte als höchst problematisch einzustufen sei (E3 2018, 11:40). Durch die standardmäßige Ausstattung von Smartphones oder Tablets könne auch die Erfassung einer Einsatzlage im Sinne des Social Media Monitorings (Punkt 3.3.5) deutlich verbessert werden (E4 2018, 18:31). Erste Meldungen zu Anschlägen oder Naturkatastrophen liefen eben meist nicht über die 110-Notrufnummer, sondern kämen bei *Twitter* oder *Facebook* auf (E4 2018, 18:40). Der Mitarbeiter eines Bundesministeriums verweist in diesem Zusammenhang auf das Konzept „Polizei 2020", dessen Kernpunkt unter anderem die Einführung eines polizeilichen „App-Stores" sei (E7 2018, 14:10). Hierdurch könne der jeweilige polizeiliche Bedarf besser adressiert werden,

beispielsweise mit zugeschnittenen App-Lösungen für die Unfallaufnahme oder für die Vermessung eines Tatorts, welche jeder Polizeibeamte aus jedem Bundesland dann auf seinem Smartphone oder Tablet installieren könne (E7 2018, 14:30).

Predictive-Policing

Die Beurteilung der Predictive-Policing Anwendungen durch die Experten fällt unterschiedlich aus. In erster Linie entscheidend für den Erfolg der Anwendungen sei immer das Vorhandensein einer Datenmenge, die eine bestimmte *kritische* Größe überschreite, da ansonsten keine signifikanten Ergebnisse erzielt werden könnten (E5 2018, 07:50). Daher sei der Einsatz prinzipiell nur in Großstädten möglich, wie dies im Bundesland Bayern in München und Nürnberg der Fall ist. Andere bayerische Städte würden sich aufgrund der Einwohnerzahl nicht für die Anwendung eignen (E5 2018, 08:10). Diese Erkenntnis bestätigt auch der Berater eines Technologieunternehmens. Problematisch sei jedoch, dass politische Entscheidungsträger dann bemängeln würden: „Ihr [die Polizeien] setzt das nur in Großstädten ein, ihr benachteiligt den ländlichen Raum" (E6 2018, 42:10).

Generell gebe es innerhalb der Polizeien derzeit eine Diskussion, welcher Mehrwert durch den Einsatz von Predictive Policing erzielt werden könne (E4 2018, 08:51). Die Sinnhaftigkeit und die Ergebnisqualität seien derzeit noch nicht eindeutig messbar, „[...] also das, was da *raus kommt*, das weiß ein guter Polizist auf der Straße auch ohne Big Data-Anwendung" (E4 2018, 09:18). Einzig die Ressourcenknappheit im Bereich des Personals rechtfertige derzeit ein weiteres Investment in die Predictive-Policing Anwendungen (E4 2018, 09:26). Die Führungskraft eines Landespolizeipräsidiums ist hier ähnlicher Meinung: „Ich halte es derzeit in der momentanen Ausprägung für überbewertet, [...] lehne es aber grundsätzlich nicht ab" (E1 2018, 19:49). Im Moment stellten die Programme jedoch noch keine wesentliche Arbeitserleichterung dar. Eine unmittelbar personenbezogene Vorhersage, wie dies in den USA bereits eingesetzt wird (vgl. Kartheuser 2018), wäre in Deutschland verfassungsrechtlich unzulässig (E5 2018, 09:20). Es dürfe also immer nur eine tatort- beziehungsweise tatzeitbezogene Vorhersage mittels der Anwendung erfolgen, wodurch zukünftig insbesondere Wohnungseinbrüche sowie KfZ-Diebstähle prädiktiv analysiert werden könnten (E5 2018, 09:45; E6 2018, 42:00).

5.3 Barrieren einer Smarten Polizeiarbeit

Im Folgenden werden Barrieren dargestellt, die nach Einschätzung der Experten derzeit die Länderpolizeien bei der Transformation hin zu einer Smarten Polizeiarbeit einschränken. Auf Basis der Aussagen der Befragten hat der Autor einzelne Kategorien zur Kodierung der Experteninterviews gebildet. Eine Zuordnung der Aussagen zu den Kategorien hat der Autor selbst vorgenommen. Tabelle 4 bietet einen Überblick über die Verteilung der Kodierungen.

Barriere	*Experten*	*Kodierungen*
Finanzielle Ressourcen	6	14
Personelle Ressourcen	5	13
Rechtliche Rahmenbedingungen	7	12
Bestehende Strukturen innerhalb der Polizeien	4	6
Prozesse in Staat und Verwaltung	7	21
Technologie	3	4
Moralische und ethische Bedenken	1	1
Politik	3	7

Tabelle 4 Barrieren der Smarten Polizeiarbeit
Quelle: Eigene Darstellung in Anlehnung an van Dyck 2016, S. 75.

In Spalte 2 der Tabelle wird die Anzahl der Experten dargestellt, die im jeweiligen Interview mindestens eine Aussage zu der entsprechenden Barriere getätigt haben. Die Zahl der Kodierungen in Spalte 3 zeigt die Anzahl der insgesamt erfolgten Aussagen zu einer Barriere und kann als Indikator für die Relevanz dieser dienen (van Dyck 2016, S. 76). Die größte Herausforderung stellen derzeit die Prozesse in Staat und Verwaltung dar, gefolgt von finanziellen Ressourcen und rechtlichen Rahmenbedingungen. Eine nur untergeordnete Rolle spielen moralische und ethische Bedenken sowie technologische Barrieren.

Finanzielle Ressourcen

Laut dem Mitarbeiter eines Bundesministeriums haben die auferlegten Sparzwänge der vergangenen Jahre das Innovationspotential sowie die technische Weiterentwicklung der Länderpolizeien gebremst (E7 2018, 04:08). Auch der Landesdatenschutzbeauftragte sieht die finanzielle Mittelknappheit als eine Barriere der Smarten Polizeiarbeit (E5 2018, 1:04:01). Des Weiteren stünden die Polizeien bei Projekt- und Mittelbewilligungen auch stets in Konkurrenz mit anderen Politik- und Verwaltungsbereichen, wie beispielsweise Straßenbauvorhaben oder Bildungsthemen (E1 2018, 46:27). Generell ließe sich aber erkennen, dass eine finanzielle Mittelbewilligung für die Polizeien langsam zunehme (E2 2018, 10:43; E4 2018, 33:44).

Personelle Ressourcen

Das Finden von geeignetem Führungs- und Fachpersonal stelle auch für die deutschen Länderpolizeien aufgrund finanzieller Restriktionen sowie des Fachkräftemangels eine Herausforderung dar (E1 2018, 47:31; E4 2018, 35:33).

> „Sie kriegen ja die ganzen technischen Experten nicht [...]. Die können wir für das, was wir zahlen, nicht einkaufen [...] Und das ist, glaube ich, wirklich ein ganz großes Problem. Sie kriegen die Stellen einfach nicht besetzt" (E7 2018, 25:55).

Eine etwas gegensätzliche Meinung vertritt der Berater eines Technologieunternehmens. Es sei vielmehr das Problem, dass unter den Verantwortlichen ein Sichtbild herrsche, lediglich in personellen Dimensionen zu denken. Der technische Fortschritt käme insbesondere deshalb nicht zur Entfaltung, da die Bereitwilligkeit „jederzeit 1.500 Planstellen einzurichten" deutlich höher sei, „als in eine smarte Lösung zu investieren, die 115.000 Euro kostet" (E6 2018, 01:06:30).

Rechtliche Rahmenbedingungen

Eine Vielzahl der Experten sieht die hohen Datenschutz- und Datensicherheitsanforderungen als eine Herausforderung für eine Smarte Polizeiarbeit (E1 2018, 48:30; E2 2018, 09:53; E6 2018, 24:17; E8 2018, 32:23). Auch das Vergaberecht sei aufgrund der langen Zeitläufe sowie der europaweiten Ausschreibungsverfahren als ein Hindernis einzustufen, da es die benötigte rasche Integration der modernen Informations- und Kommunikationstech-

niken in die Polizeiarbeit verzögere (E1 2018, 49:00). Der Landesdatenschutzbeauftragte sieht im Kontext der rechtlichen Rahmenbedingungen das Konzept „Polizei 2020" kritisch, da die Zweckbindung der polizeilichen Datenspeicherung hierbei informationstechnisch unterlaufen und verschleiert würde. Die gesetzliche Trennung zwischen Bundes- und Länderpolizeikompetenzen würde außerdem weitgehend aufgehoben (E5 2018, 41:27).

Bestehende Strukturen innerhalb der Polizeien

Ein weiteres Hindernis stellen die behördlichen Strukturen innerhalb der Polizeien dar, die von steifen Hierarchien und Alterskonflikten geprägt seien (E1 2018, 50:07; E8 2018, 25:38). Eine zukünftige Herausforderung sei es daher, die Arbeitswelt der Polizeien an die gesellschaftliche und technologische Realität anzupassen (E7 2018, 15:19). Zudem sei ein übermäßiger Perfektionsdrang seitens der Polizeien im Hinblick auf smarte Anwendungen festzustellen, der als kontraproduktiv eingestuft werden könne (E6 2018, 50:11). Gleichzeitig sei aber auch ein zunehmender Wille seitens der Polizeien zu verspüren, das interne Innovationspotential zu fördern und den technischen Fortschritt voranzutreiben (E7 2018, 16:14).

Prozesse in Staat und Verwaltung

Die föderalen Strukturen der Bundesrepublik Deutschland werden von der Mehrheit der Experten als größte Herausforderung eingeordnet (E1 2018, 50:24; E3 2018, 05:21; E5 2018, 43:14; E6 2018, 1:00:05; E7 2018, 17:07). Die in der heutigen globalisierten Welt notwendigen abstimmenden Maßnahmen in Richtung einer länderübergreifenden Harmonisierung der (Smarten) Polizeiarbeit seien aufgrund mangelnder Zusammenarbeit sowie des Fehlens eines gemeinsamen Strategiekonzepts nur schwerlich zu koordinieren (E1 2018, 50:24). Ein fehlendes abgestimmtes Konzept bemängelt auch der Landesdatenschutzbeauftragte. Dies beziehe sich sowohl auf polizeiliche Aufgaben, wie die Straftatenbekämpfung, als auch auf die Implementierung smarter Objekte oder Lösungen. Die deutsche Polizeilandschaft sei gekennzeichnet von „Insellösungen" (E5 2018, 40:27). Die polizeilichen IT-Systeme seien nicht aufeinander abgestimmt, was eine Zusammenarbeit erheblich blockiere (E5 2018, 43:14). Die 16 Länderpolizeien könnten in diesem Zusammenhang als eine Art Geleitzug betrachtet werden, bei dem

stets das langsamste Glied das Tempo vorgebe, wodurch sich Modernisierungsmaßnahmen erheblich verzögerten (E7 2018, 17:20).

Technologie

Neben den heterogenen IT-Systemen stellten auch die immer kürzer werdenden Innovationszyklen moderner Technologien eine Herausforderung für die Smarte Polizeiarbeit dar (E1 2018, 45:10). Daher sei es wichtig, „auch mal mit einer 80% Lösung auf den Markt zu gehen", die dann im Betrieb immer noch fortentwickelt werden könne (E1 2018, 46:00). Technische Herausforderungen gebe es zudem im Bereich der smarten Videoüberwachung, bei welcher die biometrische Gesichtserkennung sowie die Mustererkennungen oftmals noch fehleranfällig seien[24] (E8 2018, 33:30), als auch in der Bewältigung der zunehmenden Informationsflut mittels Big Data-Analysen (E1 2018, 51:30).

Politik

Generell nehme der politische Druck auf die Polizeien zu, jegliche Gefahren für die Bevölkerung in einer scheinbar immer unsichereren Zeit abzuwenden (E5 2018, 01:04:11). Es schiene, als hätten die politischen Vertreter keine andere Antwort auf die derzeitige Gefährdungslage, als ihre gesellschaftliche und demokratische Verantwortung auf die Polizeien zu übertragen (E6 2018, 01:08:38). Aus dieser Erwartungshaltung sei beispielsweise auch die Anti-Terror Datei[25] entstanden, deren wirklicher Nutzen für die Polizeien als höchst fraglich einzustufen sei (E5 2018, 35:27). Die politische Unterstützung und Mittelbereitstellung richte sich zudem nicht immer auf smarte Lösungen, welche die Arbeit der Polizei effektiv unterstützen und effizienter gestalten könnten, sondern vermehrt auf öffentlichkeitswirksame Maßnahmen (E1 2018, 52:06).

[24] Ein gegensätzliches Bild zeichnet hier das Bundespolizeipräsidium. Demnach sei man mittlerweile in der Lage (Februar 2018), in den Pilotprojekten eine Trefferquote mit bis zu neunzigprozentiger Sicherheit zu erzielen (Behörden Spiegel 2018).

[25] Die Anti-Terror-Datei (ATD) ist eine gemeinsame Datei des Bundes und der Länder zur Aufklärung und Bekämpfung des internationalen Terrorismus mit Bezug zur Bundesrepublik Deutschland. Die Datei wird beim Bundeskriminalamt (BKA) geführt und steht den Polizeibehörden und Nachrichtendiensten des Bundes und der Länder zur Verfügung (BfV 2018).

Moralische und ethische Bedenken

Der Berater in einem Technologieunternehmen ordnet zudem ethische und moralische Bedenken seitens der Polizeien und der politischen Verantwortlichen als eine Barriere der Smarten Polizeiarbeit ein (E6 2018, 24:00).

5.4 Thementreiber einer Smarten Polizeiarbeit

Die folgenden Seiten geben die Einschätzungen der Experten wieder, welche Akteure im Bereich der Smarten Polizeiarbeit als Hauptthementreiber einzuordnen sind. Abbildung 1 fasst die Erkenntnisse grafisch zusammen.

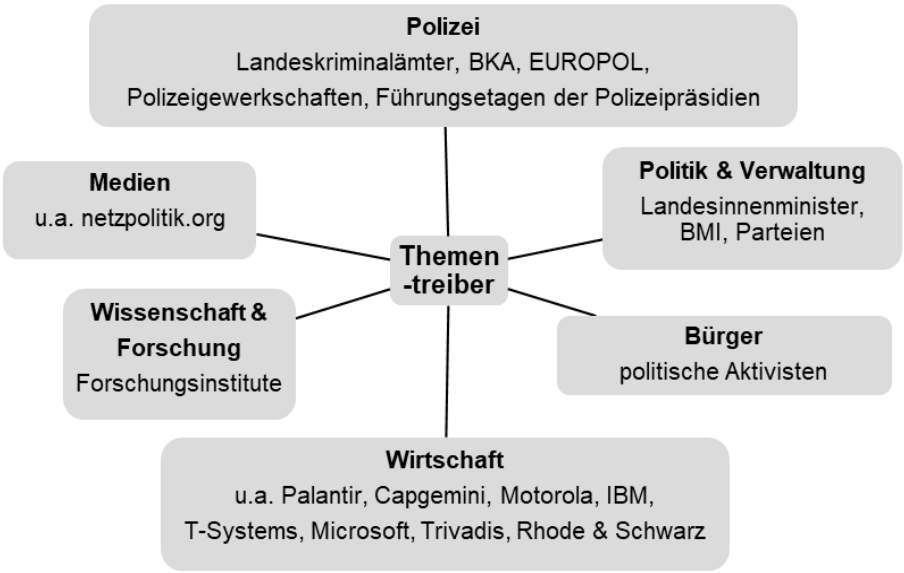


Abbildung 1: Thementreiber der Smarten Polizeiarbeit

5.4.1 Polizei

Der Experte der Polizei sieht in den Führungskräften der Landeskriminalämter zentrale Akteure für die Zielformulierungen der Smarten Polizeiarbeit (E1 2018, 34:30). Hier seien daher auch geschulte IT-Fachkräfte angesiedelt, die an innovativen und smarten Lösungen für die Polizeien arbeiten (E1

2018, 35:10). Als Führungskraft in der Abteilung für polizeiliche Informationstechnik sieht er seine Behörde in einer Mittlerfunktion zwischen den Experten der fachlichen und der technischen Seite innerhalb der Landespolizei (E1 2018, 32:00). Der politische Aktivist sieht die polizeilichen Leiter der technischen Abteilungen ebenfalls als Hauptthementreiber sowie als Zielgruppe der Akteure aus der Wirtschaft, die ihrerseits ebenfalls Einfluss in der Polizeiarbeit ausüben wollen (E8 2018, 22:52).

Ein etwas gegensätzliches Bild zeichnet die Führungskraft eines Technologieunternehmens. „Ich würde mir wünschen, dass es tatsächlich die Polizeiführung wäre [...], aber das sind eben meine Wunschakteure" (E4 2018, 23:42). Vielmehr seien das BKA oder auch der BND als Hauptthementreiber zu bezeichnen, die generell ein starkes Interesse daran hätten, durch Big Data getriebene Analysesysteme zu besseren Erkenntnissen zu gelangen (E4 2018, 24:18). EUROPOL sei ebenfalls als einer der wesentlichen Akteure einzuordnen, da es zum Ziel der Organisation gehöre, die Mitgliedsstaaten bei der Einführung von smarter Technik in die Polizeiarbeit zu unterstützen (E8 2018, 25:21). Das BKA sei wiederum innerhalb von EUROPOL „ein sehr starker Motor" (E8 2018, 25:25). Der Landesdatenschutzbeauftragte nennt außerdem die Polizeigewerkschaften, welche hier ebenfalls eine Thementreiberrolle einnähmen (E5 2018, 33:56). Insgesamt seien die Akteure der Polizeien von personellen und finanziellen Ressourcenmängeln getrieben, wodurch man sich von allen Seiten eine Entlastung durch digitalisierte Prozesse und smarte Lösungen erhoffe (E4 2018, 24:50).

5.4.2 Politik und Verwaltung

Im politischen Bereich seien insbesondere die Innenminister der Länder, als auch der Bundesinnenminister als Hauptthementreiber einzuordnen (E1 2018, 37:30; E2 2018, 06:35; E7 2018, 19:10). Gerade das Bundesinnenministerium sei hier federführend und gebe die Impulse und Vorgaben dann auf der Innenministerkonferenz an die Minister der Länder weiter (E2 2018, 06:35). Für die Implementierung smarter Lösungen wäre dies insofern relevant, da

> „letztendlich die Dinge, die politisch forciert werden [...], die haben natürlich immer einen anderen *Drive*, weil sie eine andere Hinterlegung haben mit finanziellen Ressourcen [...]. Also es ist natürlich einfacher die Projekte umzusetzen, die politischen Rückenwind haben [...]. Wenn

eben politisch die Einführung der Body-Cam erwünscht ist, dann wird es auch finanziert." (E1 2018, 37:32).

Der Bedarf einer smarten Anwendung, der aus der polizeilichen Praxis heraus entstehe, jedoch nicht so öffentlichkeitswirksam vermarktet werden könne, müsse oftmals erst zu politischen Entscheidungsträgern transportiert werden und sei daher meist schwieriger umzusetzen (E1 2018, 37: 50). Dabei gebe es durchaus Situationen, in welchen die politischen Entscheider „die Polizei zum Jagen trägt" (E5 2018, 34:41). Dass die Polizeien sich wiederum nicht gegen zusätzliche Befugnisse oder Mittel stemmen würden, dürfe nicht verwundern (E5 2018, 35:00). Die Einführung der Anti-Terror-Datei sei beispielsweise von der Politik getrieben worden, obwohl von Seiten der Polizeien aus kein Bedarf für eine Verwendung dieser bestehe. „Die Polizei hat hierdurch null Mehrwert" (E5 2018, 35:28). Der politische Vertreter auf Landesebene bestätigt die vorherigen Aussagen tendenziell. Als Polizeibeauftragter seiner Fraktion könne er ebenfalls Impulse setzen. Die Politik sei gefordert, entsprechende finanzielle Mittel zukünftig bereitzustellen, um eine Smarte Polizeiarbeit zu fördern (E3 2018, 37:45). Er stehe daher im Austausch mit der Polizei und könne so auch Forderungen an die politischen Thementreiber herantragen. „Ich schreibe dann eben an das Innenministerium [...] also man kann [die Themen] schon immer wieder drücken" (E3 2018, 39:00).

5.4.3 Wirtschaft

„Wir sind auf jeden Fall auch Thementreiber" konstatiert die Führungskraft eines Technologieunternehmens (E4 2018, 26:25). Akteure aus der Wirtschaft hätten durch ihre Arbeit als Dienstleister einen Zugang zu internen polizeilichen Prozessen und wüssten, „was wirkliche Polizeiarbeit heute bedeutet [...] im alltäglichen Tagesgeschäft" (E4 2018, 26:40). Insbesondere Polizei-Messen spielten für die Akteure der Wirtschaft eine wichtige Rolle, sich mit den Polizeien in Verbindung zu setzen und ihre Lösungen anzubieten (E1 2018, 38:35; E8 2018, 19:31). Eine Thematik, die in einigen Experteninterviews aufkam, war die Rolle ausländischer Anbieter und Dienstleister. Aktuell sei ein Trend spürbar, dass insbesondere US-amerikanische Softwarelösungen sowie smarte Anwendungen angeboten und in die deutsche Polizeiarbeit implementiert würden (E4 2018, 49:00; E6 2018, 54:14). Ein Name, der in diesem Zusammenhang immer wieder aufkam, war das ame-

rikanische Unternehmen *Palantir Technologies*[26] (E4 2018, 49:20; E7 2018, 06:00; E8 2018, 21:00). Das grundsätzliche Problem liege darin, dass immer noch unklar sei, welchen Zugriff amerikanische Geheimdienste auf deutsche Daten (der Polizeien) hätten. Dies scheine seit dem Abklingen der NSA-Affäre immer mehr in Vergessenheit zu geraten (E4 2018, 50:20).

In diesem Zusammenhang soll auf einen Artikel im Magazin *Der Spiegel* (Ausgabe 18/2018) hingewiesen werden: Die hessische Polizei nutzt seit Anfang des Jahres das Analyseprogramm „Gotham" der Firma *Palantir Technologies*. Die Software sei dabei auf Druck des Wiesbadener Innenministeriums angeschafft worden – der hessische Innenminister soll den Kauf des Programms (641.000 €) ohne vorherige Ausschreibung vorangetrieben haben. Ziel des Programms ist es, Daten aus verschiedenen polizeilichen Quellen, wie zum Beispiel Fahndungssystemen, mit Informationen aus sozialen Netzwerken oder Geodaten zusammenzuführen, um Profile zur Terrorbekämpfung zu gewinnen. Dabei obliegt die Wartung der Software den Mitarbeitern von *Palantir Technologies*, wodurch nach Ansicht von polizeilichen IT-Experten Daten unbemerkt an die US-Firma und damit möglicherweise auch an US-amerikanische Geheimdienste gelangen könnten (Ulrich 2018). Eine Thematisierung dieser Problematik sei in der Öffentlichkeit bisher zu kurz gekommen, beziehungsweise so gut wie nicht vorhanden, müsse zukünftig aber unbedingt kritisch geführt werden (E4 2018, 49:45). Die Unternehmen *Rhode & Schwarz*, *Capgemini*, *Motorola*, *IBM*, *Microsoft* sowie *T-Systems* wurden ebenfalls mehrfach als Thementreiber aus der Wirtschaft genannt.

5.4.4 Weitere

Akteure aus der Wissenschaft spielten ebenfalls eine Rolle, wenn auch nur eine untergeordnete (E7 2018, 19:52). Der Mitarbeiter eines Bundesministeriums weist darauf hin, dass Forschungskooperationen zwischen dem Bundesministerium und wissenschaftlichen Institutionen regelmäßig durchgeführt würden. Es sei außerdem wichtig, dass eine gesellschaftliche und öffentliche Debatte von Akteuren begleitet werde, die den Polizeien generell kritischer gegenüberstehen, betont die Führungskraft eines Technologieunternehmens (E4 2018, 25:24). Als einen Akteur in diesem Bereich

[26] Palantir Technologies, Inc. ist ein US-amerikanischer Anbieter von Software und Dienstleistungen, der sich unter anderem im Polizeibereich auf Big Data-Analysen spezialisiert hat.

führt er die Nachrichten-Website *netzpolitik.org* auf. „Wenn man [...] den Polizeiakteuren komplett freien Lauf lassen würde, dann hätten wir vielleicht bald [...] schwierige Verhältnisse“ (E4 2018, 25:34).

5.5 Potentiale für polizeiliche Aufgabengebiete

Die polizeilichen Aufgaben sind vielfältig und wurden in Punkt 2.3.2 bereits vorgestellt. In diesem Punkt folgt nun die Einschätzung der Experten, in welchen der Polizei zugewiesenen Aufgabengebieten smarte Objekte und Anwendungen zur Zeit vor allem eingesetzt werden und in welchen Aufgabenfeldern die Arbeit der Polizei dadurch verbessert werden kann.

5.5.1 Präventive Aufgaben

Ein Großteil der Experten sieht eine erhebliche Effizienzsteigerung mittels Smarter Polizeiarbeit im Bereich der Prävention (E1 2018, 09:23; E2 2018, 02:15; E5 2018, 07:15; E6 2018, 29:00; E8 2018, 10:26). Die Führungskraft in einem Landespolizeipräsidium hebt unter diesem Aspekt die Möglichkeit hervor, polizeiliches Handeln „im Vorfeld mit der Unterstützung von Informationsunterlegung zu verbessern“ (E1 2018, 09:23). Hierbei spielen für die Experten vor allem die bereits thematisierten Predictive-Policing Verfahren eine Rolle (E4 2018, 08:51; E5 2018, 07:10; E8 2018, 08:45). Der Berater in einem Technologieunternehmen beschreibt die Möglichkeiten, die sich durch neue digitale Analyseverfahren für die Polizeiarbeit im Bereich der Prävention ergeben wie folgt:

> „[...] in der Vergangenheit war die Analyse auf die Tat selbst beschränkt, in der Gegenwart auf den Täter und in der Zukunft geht es um die Vorhersage des Tatortes“ (E6 2018, 31:05).

Intelligent vernetzte Objekte und CPS wie Body-Cams und smarte Videoüberwachungskameras würden ihr Potential ebenfalls im präventiven Bereich entfalten, indem ihnen zum einen eine deeskalierende Funktion zugeschrieben wird (Body-Cams und Videoüberwachung) und sie zum anderen bereits im Vorfeld auf nahende Gefahrensituationen hinweisen könnten (beispielsweise durch intelligente Bewegungsmustererkennung) (E2 2018, 04:26; E3 2018, 33:08).

5.5.2 Repressive Aufgaben

Auch im Rahmen der Ermittlungsarbeit beziehungsweise bei der Spuren- und Beweissicherung sehen die Experten zukünftiges Potential einer Smarten Polizeiarbeit. Heutzutage gebe es kein Ermittlungsverfahren mehr, bei dem nicht in irgendeiner Art und Weise digitale Daten anfallen würden – oftmals jedoch unstrukturiert und aus verschiedensten Quellen (siehe 2.1.1). Hier gehe es in Zukunft darum, diese Daten mittels Big-Data-Analysen aufzubereiten und in eine strukturierte Form zu bringen und diese für die weitere Ermittlungsarbeit verwertbar zu speichern (E1 2018, 07:20). Für die Aufnahme von Spuren und Beweisen vor Ort plädiert der politische Vertreter auf Landesebene für eine Tablet-Lösung (E3 2018, 08:46).

Auch die digitale Entgegennahme von Anzeigen sei ein wichtiges Zukunftsthema (E1 2018, 10:19). Hinweisportale wie nach den G-20 Krawallen in Hamburg, in denen Bürger Video- und Bilddateien hochladen konnten, stellten hierbei einen Schritt in die richtige Richtung dar (E1 2018, 10:19, E6 2018, 47:02). Für Fahndungstätigkeiten sei die Ausstattung der Polizisten mit smarten Endgeräten zentral, da hierdurch die interne Kommunikation und Koordination deutlich zielgerichteter vorgenommen werden könne. Für die Führungskraft eines Technologieunternehmens steige vor allem die Effizienz der mobilen Streifenpolizei durch die Integration smarter Objekte und Anwendungen. Von der Verkehrsunfallaufnahme, über die Strafanzeige bis hin zur Fahndung seien hierbei zukünftig die größten Effekte zu verzeichnen (E4 2018, 08:18). Ähnlich sieht dies auch der Experte der Polizei. Der Streifenbeamte vor Ort könne durch eine smarte Tablet-Lösung jederzeit mit Daten und neuen Erkenntnissen versorgt werden. Hiermit könne auch sichergestellt werden, „dass der Beamte nicht mehr in der ´Holschuld´ ist, sondern ihm die Informationen zielgerichtet bereitgestellt werden“ (E1 2018, 08:35).

5.5.3 Weitere

Bezüglich der Begleitung von Großereignissen seien die polizeilichen Social Media Accounts sowie Social Media-Analysen von zentraler Bedeutung (E1 2018, 14:00; E3 2018, 10:40; E4 2018, 18:30). Hierbei sei entscheidend, dass man die Deutungshoheit über Situationen behalte, wozu die polizeiliche Informationsvermittlung beispielsweise durch den Nachrichtendienst *Twitter* besonders erfolgsversprechend sei (E1 2018, 14:25). Social Media-

Desks würden außerdem dazu beitragen, dass man Zugriffe auf Fotos und Videos des Geschehens im Netz erhalte, was zu einem verbesserten Lagebild seitens der Polizei und damit zu einer verbesserten Sicherheit führe (E3 2018, 11:00). Einige Pilotprojekte in diesem Bereich würden sich außerdem mit dem „Crowd-Management" von Großveranstaltungen beschäftigen. Durch das Erfassen von Besuchermengen mittels smarter Videoüberwachungskameras könne rechtzeitig vor Verdichtungen oder Anzeichen einer Massenpanik gewarnt werden (E1 2018, 15:46). Auch der Einsatz von Gesichtserkennungssoftware sei hier in Zukunft denkbar. Gesuchte Personen könnten dann in einer Menge gescannt und durch die Kameras automatisiert verfolgt werden (E1 2018, 12:16).

Für den Mitarbeiter eines Bundesministeriums habe der Informationsaustausch der Polizeien untereinander zukünftig eine zentrale Bedeutung. Das Beispiel der NSU-Anschlagsserie habe gezeigt, dass ein Informationsaustausch unter den Polizeien kaum stattfindet, da die Daten aufgrund mangelnder Kommunikation sowie der Heterogenität der IT-Systeme oft nicht zusammengeführt werden können. Eine Optimierung dieser Zustände erhoffe er sich insbesondere vom Konzept „Polizei 2020" (E7 2018, 06:27). Im Bereich der Regelung des Straßenverkehrs sowie der Gewährleistung der Straßenverkehrssicherheit seien zukünftig vor allem smarte Kennzeichenlesesysteme erfolgsversprechend (E1 2018, 11:21), selbstredend unter Einhaltung der rechtlichen Grenzen, die dies nur anlassbezogen und punktuell zuließen (E1 2018, 11:35; E5 2018, 13:12). Ein weiteres positives Potential wird außerdem der automatischen Spracherkennung zugeschrieben. Hierdurch könnten Zeugenaussagen sowie Protokollierungen direkt in schriftliche digitale Dokumente übersetzt werden, was zu einer erheblichen Prozessoptimierung beitrage (E6 2018, 45:46).

5.6 Visionen einer Smarten Polizeiarbeit

Die folgenden Seiten liefern einen zusammengefassten Überblick zum idealtypischen Zustand einer Smarten Polizeiarbeit, basierend auf den Aussagen der Experten sowie deren jeweilige zeitliche Einschätzung der Umsetzung. Potentielle Risiken und negative Visionen einer Smarten Polizeiarbeit werden anschließend ebenfalls aufgezeigt.

5.6.1 Idealtypischer Zustand

Eine idealtypische Smarte Polizeiarbeit gewährleistet einen umfassenden mobilen Zugriff auf vorhandene Daten und stellt diese den Beamten strukturiert und vor allem interaktiv in einem performanten digitalen Netzwerk zur Verfügung (E1 2018, 40:12). Über mobile smarte Objekte, wie Smartphones oder Tablets, kann der Polizeibeamte jederzeit die benötigten Informationen abrufen. Eine Smarte Polizeiarbeit verfügt über Big Data-Analysen, welche die strukturierte Erfassung sowie eine abgesicherte Speicherung und Auswertung der steigenden Datenmengen garantieren. Im Vordergrund steht dabei, aus dem unstrukturierten Datenwuchs ein strukturiertes Ermittlungsergebnis zu ziehen (E1 2018, 42:20). Durch den Einsatz von Überwachungsdrohnen entstehen neue Möglichkeiten für Tatortanalysen sowie für polizeiliche Lagebilder (E3 2018, 17:29). Durch die Kopplung einer Notruf-App mit der Verifizierung von Geodaten können Drohnen vor dem Eintreffen der Beamten bereits Aufnahmen des Geschehens in die Einsatzzentrale sowie an smarte Polizeieinsatzwagen senden (E3 2018, 19:41). Intelligent vernetzte Polizeibrillen mit „Augmented-Reality (AR)“[27] Funktion liefern neue Möglichkeiten unter anderem im Einsatzbereich der Straßenverkehrssicherheit[28] (E3 2018, 12:50).

Durch „Polizei 2020“ werden die polizeilichen Informationssysteme vereinheitlicht und verschlankt. Mittels eines smarten und dynamischen Rollen- und Rechtekonzepts wird ein moderner und gezielter Datenschutz gewährleistet (E7 2018 20:55). Apps für Smartphones und Tablets ersetzen die monolithischen und schwerfälligen Verfahren der Länderpolizeien durch einheitliche Standards. Ein partizipativ gestalteter polizeilicher „App-Store“ stellt diese allen Länderpolizeien zur Verfügung (E7 2018, 23:10). Die polizeiliche Zusammenarbeit und Abstimmung zwischen Bund, Ländern und Kommunen funktioniert reibungslos (E2 2018, 09:20). Smarte papierlose Aktenführung ermöglicht eine vernetzte sowie behördenübergreifende

[27] Bezeichnet eine computerunterstützte Wahrnehmung sowie Darstellung, welche die reale Welt um virtuelle Aspekte erweitert. Mit der Integration von Kameras in immer mehr mobile Geräte (bspw. Brillen) können zusätzliche Informationen oder Objekte direkt in ein aktuell erfasstes Abbild der realen Welt eingearbeitet werden. Dabei kann es sich um Informationen jedweder Art (bspw. Textinformationen oder Abbildungen) handeln (Markgraf 2018).

[28] Die steigende Anzahl von Hochvoltbereich/Elektro-Autos im Straßenverkehr stellt bei Unfällen ein Sicherheitsrisiko dar, da die Abschaltvorrichtungen der Autos (derzeit) nicht genormt sind. Durch eine smarte Einsatzbrille könnte mittels AR eine Anleitung der Abschaltvorrichtung in das Blickfeld des Beamten projiziert werden (E3 2018, 12:50).

Bearbeitung von Fällen (E6 2018, 59:16). Die zahlreichen smarten Anwendungen sowie die Automatisierung und Digitalisierung interner Prozesse ermöglichen den Polizeibeamten dabei eine Zeitersparnis von bis zu 80 % (E6 2018, 58:12).

In der datenbasierten Polizeiarbeit sind die Systemlösungen in der Lage, sowohl die vorliegenden Informationen effektiv zu nutzen und zu verarbeiten, als auch datenschutzrechtliche Belange zu gewährleisten. Eine klare Protokollierung mit Abfragegrund und Ergänzungstext, die eine transparente Grundlage für Eingriffe und Recherchen darstellt, ist hierfür elementar (E4 2018, 29:37). Die schutzwertigen Belange der von den polizeilichen Maßnahmen betroffenen Menschen, auch die der Verdächtigen, werden geachtet. Intelligente Videoüberwachungskameras sind beispielsweise in der Lage zu erkennen, dass Fenster von privaten Wohnungen erfasst werden und schwärzen diese automatisch (E5 2018, 37:45). Eine Smarte Polizeiarbeit beinhaltet zukünftig daher auch, dass smarte Lösungen nicht nur für eine effektivere und effiziente Erledigung polizeilicher Aufgaben eingesetzt werden, sondern dass die Privatsphäre sowie die Grundrechte der Bürger „smart geschützt werden" (E5 2018, 39:00).

5.6.2 Zeitliche Einordnung

Zu welchem Zeitpunkt die oben aufgeführten Teilkomponenten einer idealtypischen Smarten Polizeiarbeit nach Einschätzung der Experten realistisch umgesetzt sein könnten, soll durch Abbildung 2 dargestellt werden.

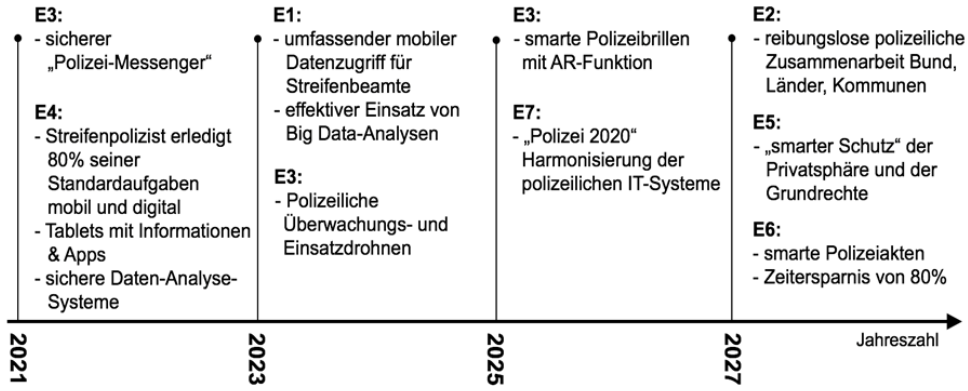


Abbildung 2: Zeitliche Einordnung der Teilkomponenten einer idealtypischen smarten Polizeiarbeit

Die Abbildung verdeutlicht, dass ein Großteil der Maßnahmen, welche in ihrer Gesamtheit dann zu einer Smarten Polizeiarbeit beitragen, nach Einschätzung der Experten wahrscheinlich in den nächsten fünf bis zehn Jahren umgesetzt werden könnten. Es muss an dieser Stelle darauf hingewiesen werden, dass es sich hierbei um ungefähre Einschätzungen sowie wünschenswerte Zielvorstellungen seitens der Experten handelt. Somit kann die zeitliche Einordnung zwar als eine grobe Richtschnur dienen, sollte in ihrer jeweiligen Ausführung aber kontinuierlich überprüft und mit aktuellen Entwicklungen abgeglichen werden.

5.6.3 Risiken und Herausforderungen

Die Mehrheit der Experten ist sich darüber einig, dass durch eine Smarte Polizeiarbeit gleichzeitig auch Risiken entstehen (E1 2018, 56:36; E2 2018, 13:48; E3 2018, 16:54; E4 2018, 41:50; E5 2018, 48:57; E8 2018, 07:10). Derzeit seien beispielsweise noch rechtliche Fragen bezüglich der Generierung von Daten im Zuge der smarten Videoüberwachung ungeklärt. Welche Daten dürften gespeichert werden, wo, wie lange und wann müssten diese wieder gelöscht werden (E2 2018, 13:48)? Der Experte aus der Politik verweist außerdem auf die zunehmenden sensiblen Daten (Bankinformationen oder auch Schutzsystemdaten von Atomkraftwerken), die in den Systemen hinterlegt werden (E3 2018, 16:54). Je mehr Daten man fortan digital abspeichere, desto angreifbarer mache man sich auch. „Es gibt kein unknackbares System [...] siehe Bundestag oder Pentagon“ (E3 2018, 27:00). Mangelnde Datensicherheit sei daher ein Risiko Smarter Polizeiarbeit. Hierunter könne auch die in 5.4.3 thematisierte Problematik amerikanischer Dienstleister eingeordnet werden (E4 2018, 49:00). Auch für die Polizeibeamten selbst entstünden Risiken, da durch intelligent vernetzte Anwendungen ihr Verhalten sowie ihre Leistung überwacht werden könnten (E5 2018, 28:14).

Die Anhäufung digitaler Daten in verschiedensten Datenbanken wecke zudem Begehrlichkeiten, diese auch zu analysieren und auszuwerten. Rechtlich seien Datenabgleiche zwischen verschiedenen polizeibehördlichen Datenbanken zwar verboten, jedoch bestehe eine Gefahr, dass die Hemmschwelle sinke, „in diesen Datenbanken mal nach bestimmten Personen zu suchen“ (E8 2018, 07:50). Der Landesdatenschutzbeauftragte sieht gewalti-

ge Risiken einer Smarten Polizeiarbeit für die Gesellschaft und die Rechtsstaatlichkeit, falls Big Data-Analysen das polizeiliche Handeln zukünftig dominieren oder gar bestimmen würden (E5 2018, 49:48). Beispiele aus den USA, wo personenbezogene Analysesysteme flächendeckend zum Einsatz kommen, hätten gezeigt, dass diese oftmals einen diskriminierenden Charakter besäßen (E5 2018, 50:00). Polizeiliche Vorhersage- und Bewertungssysteme beruhten auf statistischen Erfahrungen und Abgleichen. „Das wird aber unter Umständen [...] der persönlichen Sondersituation eines Menschen nicht gerecht" (E5 2018, 50:44). Daher seien die Diskriminierungsneigungen der Analysesysteme sowie das Überstülpen von Statistiken auf spezifische Einzelfallsituationen als zwei zukünftige Hauptrisiken einer Smarten Polizeiarbeit einzuordnen (E5 2018, 51:40).

5.6.4 Die Gefahr des „gläsernen Bürgers"

Der „gläserne Bürger", der für die Polizeiarbeit beziehungsweise den Staat vollumfänglich transparent ist und nur noch auf die von ihm zur Verfügung stehenden und gesammelten Daten reduziert wird, ist nach Einschätzung der Mehrheit der Experten zukünftig als ein reales Risiko zu betrachten (E1 2018, 56:40; E2 2018, 15:00; E4 2018, 41:32; E5 2018, 52:25; E6 2018, 01:13:21; E8 2018, 39:24). Dass Bürger auf Daten und Statistiken reduziert werden, sei nach Auffassung des Landesdatenschutzbeauftragten bereits seit einigen Jahren eine konkrete Gefahr. Eine *Entkontextualisierung* persönlicher Umstände sei bereits dann vorhanden, wenn personenbezogene Daten aus einem „konkreten Verwendungszweck herausgenommen und in zentrale Datenbanken eingespeist werden" (E5 2018, 52:34). Hierdurch seien die Hintergründe für die ursprüngliche Datenerhebung bei der weiteren Datenverwendung oft nicht mehr nachvollziehbar. Bei smarten Objekten und CPS, wie smarten Videoüberwachungskameras, bestehe durch die automatisierte Erfassung von Daten eben genau diese Gefahr, nämlich, dass der Entstehungsprozess der Datensammlung und -speicherung nur noch eingeschränkt transparent sei (E5 2018, 53:00). Es dürfe außerdem unter keinen Umständen zur Anwendung personenbezogener Analyse- und Vorhersagesysteme in der Polizeiarbeit kommen, „[...] da dies den Menschen durchaus auf eine „Datensammlung" reduzieren kann" (E5 2018, 55:00).

Zwar sei eine Tendenz in die oben skizzierte Richtung durchaus erkennbar, nach Einschätzung des Wissenschaftlers könne man dem Staat aber nicht

unterstellen, „dass er es darauf anlegt" (E4 2018, 15:00), den Bürger immer stärker zu überwachen. Der Experte aus der Wirtschaft verweist außerdem auf die hiesigen parlamentarischen und demokratischen Strukturen, welche eine Thematisierung sowie Eindämmung der Problematik ermöglichen würden (E4 2018, 41:40). Nach Aussage des Experten der Polizei habe der „unbescholtene Bürger" nichts zu befürchten. „Wer nix getan hat, dessen Daten sind auch nirgendwo gespeichert" (E1 2018, 58:10). Er bewerte den Begriff des gläsernen Bürgers daher in gewisser Weise auch positiv. Das übergeordnete Ziel der Polizeien sei schließlich die Sicherheit der Bürger zu gewährleisten (E1 2018, 59:30). Je mehr Daten anfielen und ausgewertet würden, desto besser könne man beispielsweise rechtswidrige Bestrebungen sowie terroristische Aktivitäten erkennen und unterbinden (E1 2018, 58:55). Der Aspekt der Polizeiarbeit spiele in dieser Debatte für ihn generell nur eine untergeordnete Rolle. Problematischer seien in diesem Kontext vielmehr private Unternehmen, die durch die Datensammlung ausschließlich kommerzielle Ziele verfolgten und im Gegensatz zu den deutschen Polizeien kaum durch politische und rechtliche Instanzen kontrolliert würden (E1 2018, 57:00). Hier sei der Bürger daher deutlich gläserner. Diese Einschätzung teilen eine Reihe der anderen Experten (E3 2018, 29:36; E6 2018, 45:05; E7 2018, 28:31).

5.6.5 Zur Relevanz von Künstlicher Intelligenz

Die zukünftige Rolle von Künstlicher Intelligenz (KI) sehen die Experten im Bereich der Smarten Polizeiarbeit vor allem in einer unterstützenden Funktion. Dass ein Computersystem zukünftig Einsätze eigenständig koordiniert oder gar Verhaftungen veranlasst, wird von der Mehrheit der Experten als eine unrealistische Zukunftsvision eingeordnet (E1 2018, 17:00; E4 2018, 13:10; E5 2018,16:20; E6 2018, 36:40; E7 2018, 08:35; E8 2018, 11:41). Vorstellbar sei vielmehr, dass eine Künstliche Intelligenz künftig verschiedene Handlungsvarianten vorschlage, auf Basis derer die Polizeibeamten dann das weitere Vorgehen planen könnten (E1 2018, 18:00). Die bisherige Ausprägung des Predictive-Policing bei den Länderpolizeien könne hierunter eingeordnet werden (E7 2018, 08:34). Die Entscheidungshoheit über zu treffende Maßnahmen müsse dabei stets den Polizeibeamten selbst obliegen (E5 2018 20:30). In Deutschland sei der restriktiv gehandhabte polizeiliche Einsatz von Künstlicher Intelligenz dabei vor allem auf kulturelle und ethische Faktoren und Überzeugungen zurückzuführen – die technischen

Möglichkeiten für einen deutlich umfassenderen Einsatz von Künstlicher Intelligenz seien längst vorhanden (E5 2018, 16:10; E7 2018, 08:34; E8 2018, 11:20). Auch wenn derzeit die Entscheidungshoheit wohl bei den Polizeibeamten selbst liege, könne nach Ansicht des politischen Aktivisten keine verlässliche Prognose für den zukünftigen Einsatz von Künstlicher Intelligenz in der Smarten Polizeiarbeit getroffen werden. Hierbei handle es sich um eine Technologie, welche gerade erst Einzug in die Arbeit der deutschen Polizeien erhalten habe und erst in den kommenden Jahren ihre vollen Entfaltungs- und Einsatzmöglichkeiten offenbaren werde (E8 2018, 14:01).

5.7 Zukünftige Themenfelder einer Smarten Polizeiarbeit

Die von den Experten skizzierten zukünftigen Themenfelder einer Smarten Polizeiarbeit lassen sich in drei Teilbereiche untergliedern. Wichtig sei erstens, dass die Polizeien die thematisierten smarten Objekte und Anwendungen in Zukunft deutlich stärker in ihre Arbeit implementieren (E1 2018, 01:02:40). Smarte mobile Endgeräte, wie Tablets und Smartphones sowie Body-Cams oder Big Data-Analysen, beispielsweise in Form des Predictive-Policing, müssten sinnvoll eingesetzt werden, um eine Steigerung der polizeilichen Arbeitseffizienz herbeizuführen (E3 2018, 34:18). Auch die Kooperation der Länderpolizeien untereinander sowie zwischen Bundespolizei und den Länderpolizeien müsse vorangetrieben werden. Hierunter falle auch der Austausch erfasster Daten in konkret vorliegenden Gefahrensituationen sowie im Zuge von Ermittlungen. „Die schnelle Übermittlung [der Daten] von Land A nach Land B zu jeder Behörde innerhalb von Sekunden [...] ist ein sehr wichtiges Zukunftsthema“ (E6 2018, 01:16:26). Investitionen in die polizeiliche Infrastruktur und Ausrüstung seien daher in den kommenden Jahren unbedingt notwendig (E4 2018, 46:20). Dabei reiche es nicht aus, lediglich in Insellösungen zu investieren. Es müsse zu einer intelligenten Vernetzung der Polizeiarbeit kommen, indem die smarten Objekte, Anwendungen und Big Data-Analyseverfahren in breiter Kombination und Abdeckung integriert werden (E4 2018, 46:55).

Das zweite Themenfeld beziffern die Mehrheit der Experten als die Gestaltung der rechtlichen Rahmenbedingungen im Sinne der Einhaltung der datenschutzrechtlichen Regelungen sowie der Achtung der Bürgerrechte.

> „Sie [die Polizei] muss im Prinzip den Spagat leisten können zwischen effektiver Smarter Polizeiarbeit und Grundrechtskonformität“ (E5 2018, 55:53).

Hier seien auch die Politik sowie die Justiz gefordert, Eckpfeiler festzusetzen, inwieweit die thematisierten IKT zukünftig verfassungskonform eingesetzt werden könnten (E4 2018, 43:53, E7 2018, 32:35, E8 2018, 44:00).

Eine bürgernähere Polizeiarbeit sowie die Verbesserung der Serviceleistungen spiegelt nach Ansicht der Experten das dritte Themenfeld wider. Hierfür seien insbesondere polizeiliche Social Media Accounts vielversprechend, die zukünftig zur Informationsvermittlung einen entscheidenden Beitrag leisten sowie zu einer erhöhten Transparenz des polizeilichen Handelns beitragen könnten (E1 2018, 01:01:18; E3 2018, 24:00; E6 2018, 01:10:55). Der klassische Streifenpolizist, welcher mit den Bürgern im alltäglichen Kontakt steht, sollte ebenso weiterhin präsent bleiben. Es bestünde ansonsten die Gefahr, dass man seitens der Polizei bald nur noch über das Internet mit der Bevölkerung kommuniziere und somit der „reale Bezug zu den Bürgern verloren ginge“ (E2 2018, 15:30). Eine verbesserte Serviceleistung durch die Digitalisierung der polizeilichen Arbeitsprozesse könne beispielsweise auch in Form der digitalen Anzeigenaufnahme erreicht werden (E1 2018, 10:30; E6 2018, 18:10).

Essentiell sei zudem, dass die Prinzipien der Offenheit und der Transparenz zu zentralen Grundpfeilern einer Smarten Polizeiarbeit werden. Je mehr Offenheit die Polizeien an den Tag legten, desto mehr Verständnis für polizeiliches Handeln könne seitens der Bürger künftig erreicht werden (E1 2018, 54:00). Nach dem herrschenden deutschen Verfassungsverständnis seien die Polizeien in Deutschland dadurch gekennzeichnet, dass sie im Grundsatz den Bürgern gegenüber offen und transparent aufzutreten hätten. „Transparenz ist im Grundsatz also ein Verfassungsgebot“ (E5 2018, 47:28). Es müsse daher stets die notwendige Offenheit über jegliche getroffenen polizeilichen Maßnahmen eingehalten werden, welche die Bürgerrechte beschränken könnten (E4 2018, 36:10). Gleichzeitig gebe es aber Ermittlungs- und Einsatzbereiche, in denen Transparenz und Offenheit nicht als Leitprinzipien polizeilichen Handelns eingesetzt werden könnten. Dies gelte vor allem im Zuge von strafrechtlichen Ermittlungen sowie bei terroristischen Bedrohungen (E5 2018, 55:26).

Der politische Aktivist fordert zudem eine verstärkte gesellschaftliche Debatte darüber, welche smarten Technologien und Anwendungen in der Polizeiarbeit zukünftig eingesetzt werden und mit welchen Befugnisse die deutschen Polizeien hierbei ausgestattet werden sollten (E8 2018, 38:31). Er merkt an, dass eine Verunsicherung innerhalb der Bevölkerung wahrzunehmen sei, die mit jedem Schritt der Digitalisierung polizeilicher Arbeit und Prozesse anwachse (E8 2018, 37:00). Es würde außerdem zunehmend unklarer, wo die Grenzziehung zwischen polizeilichen und geheimdienstlichen Befugnissen läge. Es müsse daher zu einer Form der öffentlichen Diskussion kommen, in der sich jeder Bürger äußern und seine Meinung einbringen könne, unabhängig davon, wer die „größte Lobby oder das meiste Geld besitzt" (E8 2018, 39:00).

5.8 Zwischenfazit: Smarte Polizeiarbeit in Deutschland

Nach der Präsentation der empirischen Ergebnisse aus den Expertenbefragungen erscheint ein Zwischenfazit zur Smarten Polizeiarbeit in Deutschland auf Basis der bisherigen Erkenntnisse sinnvoll. Obwohl seitens der Experten kein einheitliches Verständnis einer Smarten Polizeiarbeit herrscht, finden sich die wesentlichen Merkmale der in 3.2 dargelegten Arbeitsdefinition dennoch in den Aussagen wieder: Smarte Objekte, CPS, Big Data-Analysen sowie automatisierte und digitalisierte Prozesse sollen zu einer Effizienzsteigerung und Transparenzerhöhung der polizeilichen Arbeit führen. Es besteht seitens einiger Experten jedoch eine Tendenz, Smarte Polizeiarbeit als eine grundsätzliche Digitalisierung polizeilicher Arbeitsprozesse einzuordnen, ohne Hauptfokus auf Anwendungen im Internet der Dinge und der Dienste oder Big Data-Analysen. Dies unterstreicht die Bedeutung der Erarbeitung eines zukünftigen gemeinsamen Begriffsverständnisses. Im Hinblick auf die Hauptthementreiber der Smarten Polizeiarbeit ergibt sich ein breites Feld an Akteuren. Dabei gilt es insbesondere die Rolle US-amerikanischer Dienstleister sowie jene der politischen Thementreiber kritisch zu hinterfragen. Zivilgesellschaftliche Akteure werden in den Einordnungen der Experten weitgehend vermisst. Als größte Barriere der Smarten Polizeiarbeit können die föderalen Strukturen bezeichnet werden sowie personelle Ressourcen und unklare rechtliche Rahmenbedingungen.

Die in Kapitel 3 vorgestellten smarten Objekte und CPS (Body-Cam, Smartphone und Tablet, Drohnen und smarte Videoüberwachung) sowie Big Data-Analysen erfahren unterschiedliche Bewertungen. Zusammenfassend lässt sich festhalten, dass die Anwendungen sowohl die präventive, als auch repressive Arbeit der Polizeien unterstützen, ihre Effizienz hierbei erhöhen und zur Verbesserung der öffentlichen Sicherheit beitragen können. Intelligent vernetzen Objekten wird dabei insbesondere im Bereich der mobilen Polizeiarbeit ein erhebliches positives Potential zugesprochen. Verbesserte Dienstleistungen für den Bürger ergeben sich beispielsweise durch Upload-Portale sowie die digitale Anzeigenaufnahme, deren Inhalte und Daten dann in smarte, einsehbare Akten eingepflegt werden können. Durch polizeiliche Service-Apps kann zudem die Informationsvermittlung an den Bürger verbessert werden.

Gleichzeitig konnte aufgezeigt werden, dass sich durch eine Smarte Polizeiarbeit auch einige nicht zu vernachlässigende Risiken, insbesondere für die Gesellschaft beziehungsweise die Bürger ergeben. Mit der Implementierung intelligent vernetzter Objekte wie Drohnen, Body-Cams oder der smarten Videoüberwachung sowie der Integration von Big Data-Analysen steigt gleichsam die Gefahr von Freiheitsbeschränkungen sowie einer zunehmenden Überwachung der Bevölkerung. Auf die Gefahr des gläsernen Bürgers wird seitens der Experten ebenfalls hingewiesen. Die Smarte Polizeiarbeit bewegt sich damit in einem triangulären Spannungsfeld zwischen Freiheit, Sicherheit und Überwachung. Dies soll im folgenden Kapitel kritisch hinterfragt und diskutiert werden, ehe eine abschließende Diskussion und Einordnung der erarbeiteten Ergebnisse erfolgt.

6 Smarte Polizeiarbeit zwischen Freiheit, Sicherheit und Überwachung

Für die folgende Diskussion muss zunächst das Verhältnis zwischen Freiheits- und Sicherheitsinteressen in der heutigen Informationsgesellschaft skizziert werden. Der zunehmend festzustellende Präventionsfokus der deutschen Sicherheitsbehörden sowie neue Möglichkeiten der (staatlichen) Überwachung, welche sich durch eine Smarte Polizeiarbeit ergeben können, werden daraufhin kritisch diskutiert.

6.1 Freiheit und Sicherheit in der Informationsgesellschaft

Die Freiheit ist ein Wert von Verfassungsrang. Dies gründet sich letztlich durch ihre Rückbindung an das oberste Verfassungsprinzip: Die Menschenwürdegarantie (Art. 1 Abs. 1 GG), welche den Menschen als *freies* Individuum versteht, das in Ausübung seiner Dignität zur Freiheit berufen ist (Thiel 2011, S. 138). Anders als bei der Freiheit besteht in Deutschland jedoch kein Grundrecht auf Sicherheit (Moser-Knierim 2014, S. 115). Allerdings ist die Gewährleistung von innerer und äußerer Sicherheit die „ureigenste Aufgabe des demokratischen Rechtsstaates" (Thiel 2011, S. 149). Gemäß der ständigen Rechtsprechung des BVerfG ist die Sicherheit der Bevölkerung daher ein Verfassungswert, der mit den anderen (wie der Freiheit) in gleichem Rang steht und unverzichtbar ist (Moser-Knierim 2014, S. 110). Damit ist dem modernen Verfassungsstaat ein Doppelauftrag zugewiesen: Er muss sowohl Freiheit, als auch Sicherheit gewährleisten, welche in einem wechselseitigen Abhängigkeitsverhältnis stehen. Freiheit ohne die Sicherheit gewährende Funktion des Staats führt in die Anarchie und Sicherheit ohne die Freiheit gewährende Funktion des Rechts in den Polizei- beziehungsweise Überwachungsstaat (Hanning 2008, S. 191). In Freiheitsgrundrechte darf und muss unter bestimmten Voraussetzungen eingegriffen werden, um Sicherheit und Ordnung zu gewährleisten. Grenzen werden diesen Eingriffen wiederum durch den Verhältnismäßigkeitsgrundsatz und die Menschenwürdegarantie gesetzt (Moser-Knierim 2014, S. 122).

In der heutigen „Informationsgesellschaft" realisieren sich Freiheit und Sicherheit unter neuen Rahmenbedingungen, namentlich der Digitalisie-

rung aller Lebensbereiche sowie der Globalisierung (Moser-Knierim 2014, S. 9). Die Informationsgesellschaft kann als eine auf Informations- und Kommunikationstechniken basierende Gesellschaft beschrieben werden, die durch die Durchdringung sämtlicher Lebensbereiche mit dieser Technik („Informatisierung") gekennzeichnet ist (Moser-Knierim 2014, S. 17). Mit der Fülle an Informationen und den Möglichkeiten des grenzüberschreitenden, globalen Informationsaustauschs geht eine Erhöhung der Komplexität und der Unsicherheit einher, welche als wesentliche Merkmale der Informationsgesellschaft gelten (Thiel 2011, S. 7). Die gesellschaftlichen Gegebenheiten Deutschlands sind aufgrund des stetigen Fortschritts im Bereich der IKT einem tiefgreifenden Wandel unterworfen. Durch die globale Vernetzung ergeben sich zum einen neue Freiheiten, wie das weltweite Reisen und Arbeiten, als auch neue Unsicherheiten und Risiken (Moser-Knierim 2014, S. 12). Veränderte Bedrohungslagen, beispielsweise durch die technische Abhängigkeit der Gesellschaft sowie insbesondere aufgrund des Terrorismus, haben zu einer breiten Verunsicherung geführt. Risiken scheinen allgegenwärtig und nicht mehr greifbar zu sein. Für die zur Gefahrenabwehr berufenen staatlichen Behörden hat sich daraus ein neues Verständnis des Sicherheitsbegriffs ergeben: Wurde Sicherheit lange Zeit als die Unversehrtheit von Rechtsgütern seitens Privater definiert, so wird sie heute zunehmend als die Abwesenheit von Risiken verstanden (ebd.). Der Gesichtspunkt der Gefahren*vermeidung* tritt damit in den Vordergrund polizeilichen Handelns (Thiel 2011, S. 12).

6.2 Vom Rechtsstaat zum Präventionsstaat?

Wesensmerkmal neuerer Sicherheitsgesetze ist daher eine immer weiter ins Vorfeld verlagerte Eingriffsbefugnis im Sinne einer Risikoprävention. Der Staat soll dabei möglichst früh eingreifen dürfen, um befürchtete Gefahren oder Risiken von der Gesellschaft abzuwenden. Damit einher gehen Beobachtung, Kontrolle und schließlich die Überwachung von Personen, denen die Polizeien wegen bestimmter Persönlichkeitsmerkmale einen Verstoß zutrauen (Petri 2012, S. 124).[29] Dabei wächst die Gefahr, dass aus

[29] Die vorbeugenden Maßnahmen gehen nach Ansicht mancher Experten insoweit über den traditionellen Wirkbereich der Polizei hinaus, als dass diese zumeist „Vorfeldmaßnahmen" vor dem Eintritt konkreter Gefahrensituationen darstellen und daher generell in den Kompetenzbereich der „nachrichtendienstlichen Tätigkeiten" fallen müssten (Thiel 2011, S. 100).

dem freiheitlichen Rechtsstaat ein überfürsorglicher Präventionsstaat wird (Prantl 2010; Albers 2012, S. 108; Sokol 2012). Die Nichtgefährlichkeit des Bürgers und seines Verhaltens gilt nicht mehr als selbstverständlich, sondern als Ausnahme, dessen Vorliegen der Bürger jederzeit beweisen muss (Thiel 2011, S. 69). „Die bloße Mutmaßung wird zur Maxime des Eingreifens" (Prantl 2018). Zu beobachten ist dies unter anderem im neuen bayerischen Polizeiaufgabengesetz (PAG), in dem das Polizeirecht den Anknüpfungspunkt der *konkreten* Gefahr verlässt und mit der Einführung des unscharfen Begriffs der „drohenden Gefahr"[30] eine umfassende Legitimationsgrundlage für tiefgreifende präventive Eingriffe schafft (Thurm 2018). Seitens der Sicherheitsbehörden hat sich also eine „ausgreifende Risikoverwaltung" (Thiel 2011, S. 68) etabliert, die mit einer präventiven Vorfeldverlagerung polizeilichen Handelns sowie erweiterter Eingriffsgrundlagen versucht, jeglichen Risiken vorzubeugen und eine Art Frühwarnsystem zu schaffen.[31] Diese Präventionslogik fußt auf der Annahme, dass Prävention stets das mildere Mittel im Vergleich zu reaktiven und repressiven Maßnahmen sei, womit ihr eine scheinbare Alternativlosigkeit innewohnt (Moser-Knierim 2014, S. 60).

Dabei ist die Präventionslogik selbst mit erheblichen Risiken für den freiheitlich demokratischen Rechtsstaat verbunden. Die Grundrechte der Bürger werden im Präventionsstaat in erster Linie nicht mehr als Grund*freiheiten* und originäre Abwehrrechte gegen staatliche Eingriffe aufgefasst, sondern verwandeln sich in primäre Schutzpflichten des Staates und damit in Eingriffsermächtigungen (Denninger 2008, S. 85). Die Bevormundung des Staates schränkt den Bürger zunehmend in seinen Freiheitsrechten ein. Die größte Gefahr, die der Präventionslogik innewohnt, ist jedoch ihre generelle Grenzen- und Zügellosigkeit (Moser-Knierim 2014, S. 60). Macht es sich der Staat zukünftig zur Aufgabe, jede Möglichkeit eines künftigen Schadenseinritts zu regulieren und letztlich zu unterbinden, ist eine freie Betätigung des menschlichen Willens und Handelns schlicht nicht mehr möglich (Thiel 2011, S. 87). Die Beseitigung jedes Risikos setzt dann voraus, dass

[30] Der Begriff wurde jedoch nicht vom bayerischen Innenministerium neu eingeführt, sondern vom Bundesverfassungsgericht im Zuge des BKA-Urteils 2016 als Eingriffserweiterungsgrundlage festgelegt. Kritiker halten der bayerischen Staatsregierung jedoch vor, dass dieser nur für den Ermittlungsbereich des Terrorismus vorgesehen ist und nicht auf andere Straftatbestände übertragbar sei (Schnell 2018; Bundesverfassungsgericht 2016).

[31] U.a. die Anti-Terror Datei, die Online-Durchsuchung, die Rasterfahndung oder die Videoüberwachung öffentlicher Orte werden hier als Beispiele von den Autoren aufgeführt.

die staatlichen Sicherheitsbehörden alles wissen, alles können und alles dürfen müssen. Die Gefahr, durch diesen „Präventionsaktionismus“ schleichend in einen Überwachungsstaat abzudriften, wächst dabei im Hinblick auf die polizeilichen Nutzungsmöglichkeiten moderner Informations- und Kommunikationstechniken, insbesondere im Internet der Dinge und der Dienste, stetig an (Breithut & Böhm 2016; Moser-Knierim 2014, S. 71; Thiel 2011, S. 102).

6.3 Neue Formen und Risiken der Überwachung

Der Begriff der Überwachung kennzeichnet das zielgerichtete Beobachten einer Aktion, eines Objekts oder einer Person und das damit verbundene Sammeln von Informationen (Hansen 2012, S. 78). Die Digitalisierung aller Lebensbereiche in der Informationsgesellschaft führt zu einem enormen Zuwachs an personenbezogenen Daten und Informationen (siehe 2.1). Die staatliche „Datenkontrolle“ im Sinne eines Informationsvorsprungs des Hoheitsträgers hinsichtlich personenbezogener Daten hat sich daher zunehmend als eine scheinbar unverzichtbare Voraussetzung für die Gewährleistung von Sicherheit beziehungsweise für die Vorbeugung von Risiken erwiesen (Thiel 2011, S. 9). Damit steigt jedoch die Gefahr, dass diese „Datenkontrolle“ angesichts einer grenzenlosen Risikoprävention in ein ausuferndes Überwachungssystem mündet, welches die Freiheitsrechte der Bürger beschneidet und in dem der Einzelne zunehmend zu einem „gläsernen Bürger“ zu werden droht (Moser-Knierim 2014, S 20). Mit der Sammlung und Auswertung von Daten geht die Möglichkeit einher, hieraus umfassende Informationen über den Einzelnen ermitteln zu können. Wie diese Arbeit bereits aufzeigen konnte, besteht auch bei einer Vielzahl der Anwendungen einer Smarten Polizeiarbeit ein Kollisionsrisiko mit den bürgerlichen Freiheitsrechten. Die Smarte Polizeiarbeit läuft daher Gefahr, zu einem Instrumentarium für Überwachungsmaßnahmen zu werden sowie zu einer Beschränkung der grundrechtlichen Freiheiten im demokratischen Rechtsstaat beizutragen.

Mit dem fortschreitenden Einsatz von Body-Cams, smarter Videoüberwachung, Überwachungsdrohnen, Smartphones sowie Big Data-Analysen in der Polizeiarbeit steigt gleichzeitig auch die Anzahl personenbezogener Daten und Informationen, welche den Polizeien zur Verfügung stehen und für weitere Ermittlungen genutzt werden könnten. Personenprofile können

dann umso umfassender erstellt werden, je umfangreicher der Datenbestand ist (Roßnagel, Moser-Knierim & Schweda 2013, S. 107). Dabei steigt die Gefahr, dass der einzelne Bürger zunehmend „informationalisiert" und in eine „Datensammlung verwandelt" wird (Baumann & Lyon 2014, S. 165). Die Erstellung von Persönlichkeitsprofilen hat das Bundesverfassungsgericht jedoch als Ableitung aus der Menschenwürderechtsgarantie verboten („Verbot der Profilbildung") (Roßnagel et. al. 2013, S. 106). Dabei wird die Würde des Menschen in dem Moment verletzt, in dem der konkrete Mensch zum „Objekt, zu einem bloßen Mittel, zur vertretbaren Größe herabgewürdigt wird" (Dürig 1956, S. 117). Predictive-Policing Anwendungen sowie polizeiliche Big Data-Analysen sind daher äußerst kritisch zu hinterfragen, da sie zu dieser Profilbildung beitragen können.

Insbesondere durch Kameras und Sensoren von intelligent vernetzten Objekten wie Body-Cams, Überwachungsdrohnen sowie der smarten Videoüberwachung ist die Polizei zukünftig in der Lage eine umfassende Videoüberwachung öffentlicher als auch privater Lebensbereiche zu vollziehen. Jedoch ergeben sich hierbei Kollisionsgefahren mit dem vom Bundesverfassungsgericht aufgestellten „Verbot der totalen Erfassung und Registrierung" (Roßnagel et. al. 2013, S. 107). Die Freiheit des Individuums, in seiner „Freiheitswahrnehmung nicht total erfasst und registriert zu werden", also anonym zu handeln, ist dabei die wesentliche Voraussetzung für die Wahrnehmung jeglicher Freiheitsgrundrechte (ebd.). Eine umfassende gesamtgesellschaftliche Überwachung der Freiheitswahrnehmung aller Bürger ist daher mit der Verfassung nicht vereinbar (ebd., S. 108). Fraglich ist also, ob durch Smarte Polizeiarbeit diese umfassende Überwachung theoretisch hergestellt werden kann.

Hierzu stelle man sich beispielhaft eine deutsche Stadt vor, in der an jeder vierten Straßenecke eine Videoüberwachungskamera installiert ist, die Hälfte der Streifenpolizisten mit Body-Cams sowie jeder Einsatzwagen mit einer Dash-Cam ausgestattet ist und in welcher die Polizei über zwei Überwachungsdrohnen verfügt, die jederzeit in die Luft steigen können. Betrachtet man den Verbreitungsgrad der einzelnen smarten Objekte und CPS erscheint dies im ersten Moment noch wenig bedenklich. Vergegenwärtigt man sich aber, dass ein Bürger nun theoretisch damit rechnen muss, jederzeit in seinen Handlungen von einer Kamera erfasst zu werden, läuft eine Smarte Polizeiarbeit Gefahr, eine umfassende gesamtgesellschaftliche

Überwachung herbeizuführen und in die Freiheitsgrundrechte der Bürger einzugreifen.

Unter dem Aspekt des Präventionsfokus deutscher Sicherheitsbehörden, in welchem der Bürger seine „Unverdächtigkeit" zunehmend beweisen muss, kann dies dazu führen, dass Menschen ihr Verhalten aufgrund des bloßen Gefühls eines möglichen Überwachtwerdens anpassen (Moser-Knierim 2014, S. 62). Dies käme einem Eingriff in das „Recht auf informationelle Selbstbestimmung" gleich, einem Eckpfeiler des Datenschutzes, welches dem Einzelnen die Chance sichert, seine Individualität auch unter Einfluss subtiler Informationstechnologien zu entwickeln (Tinnefeld et. al. 2017, S. 5). Die daraus resultierende freie Partizipations- und Kommunikationsfähigkeit des Bürgers, welche als Grundlage unserer freien demokratischen Gesellschaft gilt (ebd.), wird dann durch den manipulativen Charakter der staatlichen Überwachung (Hofstetter 2016, S. 83) deutlich eingeschränkt. Das oben angeführte Beispiel scheint nicht allzu weit von der heutigen Realität entfernt zu sein.[32] Es wirft daher die Frage auf, inwiefern verfassungsrechtliche Verbote und Vorgaben es tatsächlich vermögen, das Abdriften in überwachungsähnliche Zustände effektiv zu begrenzen (Moser-Knierim 2014, S. 231).

Grundsätzlich gilt es in diesem Zusammenhang auch die Rolle der Privatwirtschaft kritisch zu hinterfragen. Diese wird vom Staat immer weiter eingebunden, wenn es um die Gewährleistung der öffentlichen Sicherheit geht. Die Videoüberwachung von Tankstellen, Fußballstadien oder Diskotheken ist mittlerweile allgegenwärtig und der Staat kann sich dieser Videoaufnahmen bei Verdacht jederzeit bedienen (Demuth 2017). Private Dienstleister nehmen auch in der Smarten Polizeiarbeit eine entscheidende Rolle ein, vertreiben sie doch letzten Endes die smarten Objekte und sind für die Wartung der IT-Systeme und Softwarelösungen zuständig (siehe Beispiel *Palantir*). Welchen Zugriff sie dabei auf personenbezogene Daten erhalten, ist nicht immer eindeutig geklärt. Für viele Unternehmen, insbesondere im Bereich der neuen Medien, haben personenbezogene Informationen heute einen enormen Wirtschaftswert entwickelt, was eine Speiche-

[32] So werden beispielsweise die Bürger der Stadt Köln (Stand: Juni 2018) an offiziell 3866 öffentlichen Standorten inklusive Züge, Busse und Bahnen von stationären Videokameras erfasst. Hinzu kommen Body-Cams der Polizei sowie Dash-Cams an Streifenwagen. Das ergaben Recherchen bei der Stadt, der Polizei Köln, der Bundespolizei, dem Kölner Verkehrsbund sowie der Deutschen Bahn (Stinauer 2018).

rung und Auswertung dieser zufolge hat (ebd., S. 70). Intelligent vernetzte Alltagsgeräte im Internet der Dinge schaffen zudem neue Formen der Spurensicherung. Smarte Fitnessarmbänder oder Lautsprecher liefern den Sicherheitsbehörden dabei neue Möglichkeiten der Datenerfassung. Dies kann zwar helfen, Straftaten aufzuklären, ist aber gleichzeitig problematisch, da die Geräte manipulierbar sind und die Datenaussagekraft nicht immer eindeutig ist (Kühl 2017; Roßnagel et. al. 2013, S. 107). Insgesamt machen die angeführten Beispiele deutlich, dass unter Umständen nicht das Abdriften in einen Überwachungs*staat*, sondern vielmehr in eine Überwachungs*gesellschaft* droht (Moser-Knierim 2014, S. 71).

Wie eine solche Überwachungsgesellschaft aussehen kann, und dass diese keine Fiktion im „Orwellschen" Sinne mehr ist, zeigt sich derzeit in China. Staat und Privatwirtschaft bauen hier gemeinsam ein System zur Bewertung des Sozial- und Wirtschaftsverhaltens der Bürger auf. Dieses „Social Credit System" soll bereits im Jahr 2020 landesweit eingeführt werden. In die Bewertung fließen dabei unter anderem persönliche Daten aus Kranken- und Gerichtsakten, Suchanfragen im Internet oder getätigte Einkäufe per Kreditkarte ein. Jeder Nutzer verfügt dann über ein eigenes Punktekonto, welches verhaltensbasiert auf- oder abgewertet wird. Je nach persönlichem „Scorewert" entscheidet am Ende das System über den Zugang zu akademischer Ausbildung, vergünstigten Krediten oder welchen Job man ausüben darf. So wurden beispielsweise von Januar bis Mai 2018 mehr als 11 Millionen Flüge von Chinesen blockiert, die ihre Schulden nicht gezahlt hatten (Rotenberger 2018). In Kombination mit einer flächendeckenden Videoüberwachung und Gesichtserkennungssoftware soll ab 2020 in allen chinesischen Großstädten dann auch das Verhalten der Bürger in der Öffentlichkeit komplett erfasst und bewertet werden können[33] (Kerkmann 2018; Lee 2017). Die gesamtgesellschaftliche Überwachung sowie eine Objektifizierung des Menschen auf seine zur Verfügung stehenden Daten ist dann Realität.

[33] Die chinesische Polizei setzt seit Anfang des Jahres zudem AR-Brillen mit Gesichtserkennungssoftware ein. Die Brillen scannen Gesichter in Bruchteilen von Sekunden und gleichen diese automatisch mit einer lokal gespeicherten Datenbank auf den Smartphones der Polizisten ab. In dieser Datenbank mit derzeit 100.000 gesuchten Personen kann die Brille Verdächtige in nur 100 Millisekunden erkennen und den Beamten melden (Herbig 2018).

6.4 Kompromissfindung

An dieser Stelle ist darauf hinzuweisen, dass den deutschen Sicherheitsbehörden und Polizeien nicht unterstellt werden soll, den Ausbau eines Überwachungsstaats zu forcieren. Es konnte zudem bereits aufgezeigt werden, dass eine Smarte Polizeiarbeit ebenso eine Vielzahl an positiven Potentialen beinhaltet. Dennoch zeigt sich, dass durch die erwiesene Vorfeldverlagerung polizeilichen Handelns, der Bedeutung des Datenzuwachses in der Informationsgesellschaft sowie mittels der polizeilichen Nutzungsmöglichkeiten des Internets der Dinge und der Dienste die Gefahr einer gesamtgesellschaftlichen Überwachung nicht unterschätzt werden sollte. Eine solche Überwachung schränkt die Freiheitsgrundrechte der Bürger klar ein. Gleichzeitig führt sie keineswegs automatisch zu mehr Sicherheit (Schaar 2017). Dieses Paradoxon gründet sich daraus, dass die Sicherheitsgesetzgebung der letzten Jahre vielmehr zu einer breiten gesellschaftlichen Verunsicherung beigetragen hat (ebd.). Je mehr heutige Gesellschaften von Sicherheitsmaßnahmen und Überwachungsmechanismen durchdrungen sind, „desto mehr produzieren sie unvermeidlich Unsicherheiten“ (Baumann & Lyon 2014, S. 134). Die gesellschaftliche Überwachung kann daher nie das Ziel eines demokratischen Verfassungsstaates sein, da hierdurch seine Kernwerte, die Freiheit und die Sicherheit, beide eingeschränkt werden.

Wie aber soll nun seitens der Polizeien zukünftig auf neue Bedrohungslagen und Risiken in der heutigen Informationsgesellschaft reagiert werden? Als Garant von Sicherheit und Freiheit muss der Staat das Handeln unter Unsicherheitsbedingungen als solches annehmen und strukturieren (Thiel 2011, S. 71). Dass hierzu ein gewisser Grad an Überwachungsmaßnahmen und punktuellen Eingriffen in Freiheitsrechte nötig sein kann, soll nicht bestritten werden. Um die gewünschte Balance zwischen Freiheit und Sicherheit im demokratischen Rechtsstaat herzustellen, bedarf es letzten Endes aber vor allem einer breiten gesellschaftlichen Debatte unter Einbeziehung aller Interessen und eines gemeinsamen Vorgehens von Staat, Polizeien und Bürgern. Der Gesetzgeber sollte dabei rational und besonnen das Ziel verfolgen, einen transparenten und optimierten Interessensausgleich im Spannungsverhältnis von Freiheit und Sicherheit zu schaffen. Insbesondere der Datenschutz zwingt ihn dabei zur Reflektion und verlangt nach einer von Beginn an behutsamen Gestaltung präventiver Maßnahmen (Al-

bers 2012, S. 112). Ein solches Vorgehen trägt dann auch wesentlich zu einer Akzeptanz innerhalb der Bevölkerung für Sicherheitsmaßnahmen bei (Moser-Knierim 2014, S. 254). Unabhängige Expertenkommissionen können außerdem eingesetzt werden, um Sicherheitsmaßnahmen zu bewerten und auf ihre Wirkung zu überprüfen. Von seinen Schutzpflichten sollte der Staat zudem vor allem gegenüber der Privatwirtschaft Gebrauch machen, in welcher der einzelne Bürger zunehmend auf seine Daten reduziert zu werden droht.

Auch eine Smarte Polizeiarbeit kann dazu beitragen, einen optimierten Ausgleich zwischen Sicherheits- und Freiheitsinteressen zu erwirken. Durch Smarte Polizeiarbeit, kann die Transparenz polizeilichen Handelns erhöht, als auch eine tatsächliche Verbesserung der öffentlichen Sicherheit hergestellt werden. Zukünftig wird es also darauf ankommen, in welcher Form und mit welchen Motiven intelligent vernetzte Anwendungen in der Polizeiarbeit eingesetzt werden - liefern sie doch sowohl neuartige Potentiale, Freiheit und Sicherheit zu stärken, als diese auch durch neue Möglichkeiten der polizeilichen Überwachung einzuschränken. Eine gesellschaftliche Debatte hierzu muss zeitnah erfolgen, denn die Technologien mit all ihren Fähigkeiten stehen längst bereit und finden zunehmend Einzug in die deutsche Polizeiarbeit. Letztlich geht es dabei auch um die Zielformulierung, welche Rolle die Polizeien zukünftig in der Gesellschaft einnehmen soll. Dies erscheint unter der folgenden Gleichung als besonders relevant: Die Sicherheitsbehörden eines Rechtsstaats können alles, was sie dürfen – die Sicherheitsbehörden eines Überwachungsstaats dürfen alles, was sie können (Prantl 2018).

7 Diskussion und Handlungsempfehlungen

Die zentrale Fragestellung dieser Arbeit lautet, welche Chancen, Risiken und Herausforderungen sich durch eine Smarte Polizeiarbeit ergeben. Gleichzeitig soll der bisherige Status Quo in Deutschland aufgezeigt werden. Die SWOT-Analyse[34] mit der Gegenüberstellung der bestehenden Stärken sowie Schwächen und der perspektivischen Chancen sowie Risiken erscheint daher für die Darstellung und Diskussion der erarbeiteten Ergebnisse aus Literatur und den Experteninterviews als geeignetes Mittel. Anschließend sollen auf Grundlage dieser Analyse Handlungsempfehlungen für die Zukunft abgeleitet werden.

[34] Zur Funktionsweise und Erklärung der SWOT-Analyse siehe Anhang VI.

7.1 SWOT-Analyse

Abbildung 3 bietet eine Übersicht mit einigen der zentralen Punkte der Stärken, Schwächen, Chancen und Risiken der Smarten Polizeiarbeit. Eine ausführliche Analyse erfolgt in den jeweiligen ausformulierten Unterpunkten.

Stärken	**Schwächen**
▪ Verbesserte Beweis- und Spurensicherung ▪ Verbesserte Datenauswertung ▪ Verbesserte Kommunikation und Informationsvermittlung für Bürger und Polizei ▪ Erste Effizienz- und Effektivitätssteigerung durch smarte Objekte ▪ Polizeien haben Handlungsbedarf erkannt ▪ Verbesserte Interaktion zwischen Polizeien und Bürgern	▪ Nachholbedarf in Bezug auf Digitalisierung und smarte Lösungen ▪ Mangel an finanziellen Ressourcen ▪ Hinderliche föderale Strukturen ▪ Mangel an IT-Fachkräften ▪ Bürokratisch-hierarchische Behördenkultur ▪ Akteursfeld/Thementreiber ▪ Flächendeckende Videoüberwachung ▪ Fehlendes gemeinsames Verständnis
Chancen	**Risiken**
▪ Verbesserte Entscheidungsfindung ▪ Entgegenwirken des Fachkräftemangels ▪ Verbesserte Tatort- und Situationsanalysen ▪ Erhöhung der Transparenz ▪ Ablauf- und Prozessoptimierungen ▪ Effiziente Koordination von Einsatzkräften ▪ Neue und verbesserte Dienstleistungen ▪ Behörden- und Länderübergreifende Zusammenarbeit ▪ Arbeitserleichterung und Kostenreduktion ▪ Intelligente Mustererkennung ▪ Polizei 2020	▪ Gefahr des „gläsernen Bürgers“ ▪ gesamtgesellschaftliche Überwachung ▪ Objektifizierung des Bürgers ▪ Datensicherheit ▪ Manipulation von Systemen, Daten und ▪ Algorithmen ▪ Distanzierende Wirkung ▪ Unklare Folgewirkungen ▪ Polizei 2020

Abbildung 3: SWOT-Analyse der Smarten Polizeiarbeit

7.1.1 Stärken

Als Stärken einer Smarten Polizeiarbeit können zu einem wesentlichen Teil die in 3.3 skizzierten bisherigen Einsätze smarter Objekte und Anwendungen in den deutschen Polizeien eingeordnet werden. Die deeskalierende Wirkung von Body-Cams an Polizeiuniformen führt dazu, dass die Gewalt gegenüber Polizeibeamten, welche diese an der Uniform tragen, rückläufig ist (Eichner 2018). Des Weiteren erfolgt durch den Einsatz von Body-Cam und Dash-Cam eine neue Form der Beweissicherung sowie eine Steigerung der Transparenz im Hinblick auf polizeiliches Handeln. In Großstädten, in welchen Predictive-Policing eingesetzt wird, sind sinkende Einbruchszahlen festzustellen. Hier gilt es allerdings noch abzuwarten, inwiefern dies auf den Einsatz der Big Data-Analysen zurückzuführen ist. Das Erfahrungswissen von Polizeibeamten kann es derzeit wohl noch nicht ersetzen aber bereits ergänzen. Die Analyse großer Datenmengen ermöglicht der Polizei jedoch schon heute ein verbessertes Potential der Informationsbeschaffung und -auswertung (Neuerer 2018). Durch den Einsatz von Smartphones und Tablets können die Polizeibeamten ihre Arbeitseffizienz erhöhen. Die digitale Unfallaufnahme vor Ort ermöglicht Zeitersparnisse sowie ein intelligent vernetztes Arbeiten, wenn die eingegebenen Daten direkt in die polizeilichen IT-Systeme eingepflegt werden und zur weiteren Verarbeitung zukünftig in smarten Akten zur Verfügung stehen. Auch die Kommunikation unter den Polizeibeamten wird durch den Einsatz smarter mobiler Endgeräte verbessert. Die Experten waren sich einig, dass polizeiliche Social Media-Accounts neuartige Möglichkeiten der Situationsanalyse und Informationsvermittlung an die Bürger liefern. Zudem helfen sie den Beamten, die Deutungshoheit bei Großereignissen und Katastrophenlagen zu behalten (Bayerl & Rüdiger 2017). Verbesserte Dienstleistungen werden beispielsweise durch Polizei-Apps erwirkt. Mit der Benutzung dieser können die Bürger Informationen zu Polizeimeldungen, Revierstandorten oder Fahndungen jederzeit abrufen. Integrierte Warnhinweise sowie Notruffunktionen tragen dabei zur Gewährleistung der öffentlichen Sicherheit und Ordnung bei und vermitteln dem Bürger das Vorhandensein eines dauerhaften Ansprechpartners. Stationäre Videokameras an Brennpunkten ermöglichen den Polizeien derzeit Fahndungserfolge, indem sie Straftäter, Straftaten sowie Ordnungswidrigkeiten erfassen. Aus den Experteninterviews ging hervor, dass die Polizeien zudem den Handlungsbedarf sowie die Potentia-

le von Big Data-Analysen und der Anwendungen im Internet der Dinge und Dienste erkannt haben, was ebenfalls als Stärke eingeordnet werden kann.

7.1.2 Schwächen

Wie aus Abbildung 3 entnommen werden kann, existieren im Hinblick auf eine Smarte Polizeiarbeit derzeit jedoch auch eine Vielzahl von Schwächen. Hierunter fällt der von allen Experten formulierte erhebliche Nachholbedarf der Polizeien in Bezug auf die Digitalisierung. Auch fehlende finanzielle Ressourcen stellen die Polizeien derzeit vor Probleme; sind die Produkte und Lösungen hin zu einer Smarten Polizeiarbeit doch mit teils erheblichen Kosten verbunden (Eichner 2018). Finanzielle Zuschüsse erfahren die Polizeien dabei vor allem öffentlichkeitswirksam kurz vor Bundestags- oder Landtagswahlen, nicht aber zwingend dann, wenn sie es gerade dringend benötigen (Gammelin 2016). Des Weiteren konnte durch das Experteninterview mit dem Vertreter der Polizei herausgearbeitet werden, dass sich die Mittelbewilligungen oftmals auf Anwendungen und Bereiche verteilen, die von politischem Interesse sind. Gleichzeitig formuliert die Politik einen zunehmenden Erwartungsdruck an die Polizeien unter veränderten Rahmenbedingungen in der Informationsgesellschaft, Sicherheit und Ordnung zu gewährleisten.

Weder aus den Experteninterviews noch aus der Literatur wird der Mehrwert einer immer flächendeckenderen Videoüberwachung in Deutschland ersichtlich. Wissenschaftliche Studien, die beweisen, dass Videoüberwachung zu einer Verbesserung der öffentlichen Sicherheit führt, existieren (noch) nicht (Demuth 2017). Die Konferenz der Datenschutzbehörden des Bundes und der Länder bezeichnet die Videoüberwachung zudem als „schlicht überflüssig“ (Breithut & Böhm 2016). Beim Einsatz von smarter Videoüberwachung mit unterlegter Gesichtserkennungssoftware muss das Ergebnis des Pilotprojekts in Berlin abgewartet werden. Datenschützer äußern jedoch bereits jetzt erhebliche Bedenken.

Unklare rechtliche Rahmenbedingungen stellen derzeit ebenfalls noch eine Barriere dar, ebenso wie ein fehlendes übergreifendes Strategiekonzept. Dies ist auch den föderalen Strukturen und Prozessen geschuldet, die eine Zusammenarbeit sowie einen Wissenstransfer unter den Polizeien erschweren. Damit einher geht die derzeitige Heterogenität der IT-Systeme und polizeilichen Datenbanken, welche jedoch durch „Polizei 2020“ har-

monisiert werden sollen. Eine Zusammenarbeit der Länderpolizeien wird in der heutigen Zeit immer wichtiger, da Straftäter Ländergrenzen übergreifend agieren.

Der herrschende Fachkräftemangel trifft auch die deutschen Polizeien. Dass die Digitalisierung polizeilicher Prozesse sowie eine Integration smarter Objekte den Folgen des Fachkräftemangels entgegenwirken kann, scheinen nach Meinung eines Experten noch nicht alle Verantwortlichen erkannt zu haben. Das Denken in vorrangig personellen Dimensionen kann als Schwäche bezeichnet werden. Ohne die benötigten IT-Fachkräfte wird eine Implementierung der smarten Objekte und Anwendungen jedoch gleichzeitig erschwert. Die Konsequenz ist eine Auslagerung der Dienste an private Anbieter. In diesem Zusammenhang gilt es daher auch das in Kapitel 5 aufgezeigte Akteursfeld kritisch zu hinterfragen. Die zunehmende Einbindung US-amerikanischer Dienstleister kann unter dem Aspekt, dass immer noch nicht geklärt scheint, welche Zugriffs- und Einsichtsmöglichkeiten die amerikanischen Geheimdienste besitzen, als Schwäche eingeordnet werden. Aus den Experteninterviews ist zudem hervorgegangen, dass sich die Thementreiber einer Smarten Polizeiarbeit primär aus einem kleinen Kreis von Vertretern aus Polizei, Politik und Verwaltung sowie Wirtschaft zusammensetzen.

Die behördlichen Strukturen innerhalb der Polizeien sind ebenfalls ein bestehender Schwachpunkt. Bürokratische Abläufe, steife Hierarchien und lange Dienstwege können innovationshemmend wirken und kollidieren mit den Eigenschaften moderner IKT, wie nicht-hierarchische Kommunikation, schnelle Reaktion und Interaktion sowie langfristige Verfügbarkeiten (Mergel, Müller & Schulz 2013, S. 75). Smarte Objekte und Anwendungen im Internet der Dinge als Technologien mit disruptiven Wirkungen können außerdem zu Unsicherheiten und Skepsis seitens der Beamten führen. Damit einher gehen bestehende technologische Herausforderungen. Da Body-Cams, Drohnen, Big Data-Analysen oder auch Smartphones und Tablets erst seit einigen Jahren Einzug in die Polizeiarbeit erhalten, müssen die Beamten auch hinsichtlich der technischen und funktionellen Besonderheiten eingearbeitet werden. Dass weder in der Literatur noch seitens der Experten ein gemeinsames Begriffsverständnis bezüglich Smarter Polizeiarbeit herrscht, kann ebenfalls als Schwäche eingeordnet werden, da dies

eine gemeinsame Strategieformulierung sowie die Bestimmung künftiger Rahmenbedingungen erschwert.

7.1.3 Chancen

Eine Smarte Polizeiarbeit beinhaltet vielfältige positive Potentiale, wie die Befragung der Experten ergeben hat. Die Integration smarter Objekte sowie digitalisierte Prozessoptimierungen ermöglichen eine intelligente Vernetzung des polizeilichen Arbeitens und können im Sinne der eingangs vorgestellten Definition zur Effizienzsteigerung, Transparenzerhöhung und verbesserten Dienstleistungen für die Bürger beitragen. Der Einsatz von Überwachungsdrohnen liefert der Polizei dabei verbesserte Möglichkeiten der Situationsanalyse. Durch 360-Grad-Kameras können diese aus unterschiedlichen Blinkwinkeln zu einem verbesserten Lagebild in verschiedenen polizeilichen Einsatzszenarien beitragen (siehe 3.3.3). Durch smarte Videoüberwachungskameras, die bestimmte Muster erkennen und melden, ergeben sich insbesondere Potentiale im Bereich der Verkehrslenkung, als auch im Zuge von Großereignissen, um Verkehrsstaus oder Massenpaniken vorzubeugen.

Smartphones und Tablets sowie ein smarter Polizeieinsatzwagen ermöglichen den Polizeibeamten zukünftig neue Möglichkeiten der mobilen Informationsbeschaffung. Die mobile digitale Aufnahme von Anzeigen, Unfällen oder Personendaten, welche dann in smarte Akten eingepflegt werden, schafft Zeitersparnisse und Ablaufoptimierungen. Spracherkennungssoftware bietet hierbei zukünftig ebenfalls eine erhebliche Effizienzsteigerung, beispielsweise in der Berichterstattung und im Zuge der Aufnahme von Zeugenaussagen. Intelligent vernetzte Polizeiakten können dann behördenübergreifend (bspw. Staatsanwaltschaft oder Versicherungen) eingesehen oder bearbeitet werden. Klare Protokollierung und Zugriffsbestimmungen sowie datenschutzrechtliche Vorgaben sind hierfür jedoch elementar. Smarte Polizeibrillen mit AR-Funktion können den Beamten in Zukunft wichtige Hinweise direkt in ihr Blickfeld projizieren, beispielsweise zu gesichteten Objekten oder Fahrzeugkennzeichen. Auch eine intelligente Vernetzung der Polizeiuniformen, der Polizeihelme sowie der Dienstwaffen ist durch das Internet der Dinge künftig möglich. Über Sensoren kann dann beispielsweise ein Alarm an die Einsatzzentrale gesendet werden, wenn der Puls des Beamten stark ansteigt oder dieser seine Waffe zieht (Gehm 2017). Im Einsatzzentrum können die gesammelten Daten, welche unter

anderem in Echtzeit durch die Sensoren und Kameras der smarten Objekte gesendet werden, gespeichert und ausgewertet werden. Big Data-Analysen können dann dazu beitragen, aus den generierten Daten strukturierte Ermittlungsergebnisse und Verknüpfungen zu vollziehen. Durch die intelligente Vernetzung von Einsatzzentrum, Polizeieinsatzwagen sowie der smarten Objekte lassen sich die Einsatzkräfte zukünftig wesentlich besser koordinieren und orten.

Die von den Experten als wichtiges Zukunftsthema eingeordnete Transparenz polizeilicher Maßnahmen und Handlungen soll durch Smarte Polizeiarbeit ebenfalls verbessert werden. Basierend auf dem Beispiel des „West Midlands Police 2020" Modells könnten mittels digitaler Bürgerportale Informationen abgerufen sowie Anzeigen aufgegeben und Delikte gemeldet werden. Der aktuelle Bearbeitungsstand eines Falls oder einer Anzeige kann dann jederzeit von den betroffenen Bürgern eingesehen werden und trägt zur Transparenzsteigerung bei. Durch die Kameratechnik in einigen der smarten polizeilichen Objekte erfolgt eine erweiterte Form der Beweissicherung. Werden die Aufnahmen in einem gewissen Rahmen auch den betroffenen beziehungsweise aufgezeichneten Bürgern zur Verfügung gestellt, so erhöht dies ebenfalls die Transparenz sowie die Akzeptanz polizeilichen Handelns. Wie bereits aufgeführt, bieten Polizei-Apps für Bürger neue Formen der Dienstleistung und Informationsvermittlung. Für die interne Verwendung bieten sie den Vorteil, dass sich bereits bestehende Datenbanken und Systeme in Apps umwandeln lassen. Installiert auf Smartphones und Tablets können diese jederzeit aufgerufen und bearbeitet werden. In diesem Zusammenhang kann auch der „polizeiliche App-Store" durch das Konzept „Polizei 2020" als Chance eingeordnet werden. Können hier demnächst alle Polizeien eigene Lösungen präsentieren sowie jene aus anderen Bundesländern herunterladen, führt dies zu einer Harmonisierung der Prozesse, als auch zu einem gesteigerten Wissenstransfer (E7 2018, 45:33). „Polizei 2020" bietet außerdem das Potential, die Zusammenarbeit zwischen den Länderpolizeien zu fördern, sowie die IT-Sicherheit und den Datenschutz im Hinblick auf polizeiliches Arbeiten zu verbessern und zu gewährleisten.

Als eine weitere Chance der Smarten Polizeiarbeit kann die Möglichkeit eingeordnet werden, hierdurch dem skizzierten Fachkräftemangel beziehungsweise fehlenden personellen Ressourcen entgegenzuwirken

(Detempele, Düsing, & Schramm 2017). Durch Prozessoptimierungen sowie dem Einsatz smarter Objekte lassen sich Einsatzkräfte bündeln und zu einem gewissen Grad auch einsparen. In Anbetracht der demografischen Entwicklung sollte dies als Chance verstanden werden. Die in 5.6.2 skizzierte zeitliche Einordnung einiger Teilkomponenten der Smarten Polizeiarbeit verdeutlicht jedoch, dass mit einer Umsetzung der meisten Maßnahmen wohl erst in den nächsten fünf bis zehn Jahren zu rechnen ist.

7.1.4 Risiken

Dass im Hinblick auf die Smarte Polizeiarbeit auch einige Risiken beziehungsweise Herausforderungen bestehen, wurde in Kapitel 6 der Arbeit bereits diskutiert. Auf die Gefahren des gläsernen Bürgers, der Objektifizierung des Menschen sowie der gesamtgesellschaftlichen Überwachung soll an dieser Stelle daher nicht noch einmal gesondert eingegangen werden. Durch die Diskussion sowie mittels der Experteninterviews konnte verdeutlicht werden, dass die oben genannten Risiken keineswegs aus der Luft gegriffen sind. Deshalb gilt es in Zukunft Gesetzgeber und Polizeien aufzufordern, die Freiheitsrechte der Bürger nicht als zweitrangig zu betrachten. Eine breite gesellschaftliche Debatte scheint hierzu unabdingbar. Die Demonstrationen im Zuge des bayerischen PAG im Frühjahr dieses Jahres zeigen, dass diese Diskussion notwendig und seitens der Zivilgesellschaft dringend erwünscht ist. Dass einige der Experten in dieser Hinsicht vorrangig nur auf die Gefahren im Zusammenhang mit Großkonzernen *wie Facebook, Google* oder *Amazon* verwiesen haben, nicht aber auf die Risiken einer staatlichen Überwachung, ist bedenklich und muss an dieser Stelle kritisiert werden. In Anbetracht des stetig wachsenden Datenvolumens stellt auch die zukünftige Datensicherheit in Bezug auf die polizeilichen IT-Systeme eine Herausforderung dar. Das Konzept „Polizei 2020“ verdeutlicht, dass hier Handlungsbedarf besteht. Ein weiteres Risiko besteht in der Fehlinterpretation der Daten. Ein breites und vielseitiges Spektrum an gesammelten Daten sagt noch nichts über den wirklichen Informationsgehalt dieser Daten aus beziehungsweise bedeutet nicht, dass dies automatisch zu einer verbesserten Entscheidungsfindung führt. Gleichzeitig bleibt bei „Polizei 2020“ abzuwarten, inwieweit das Programm möglicherweise als polizeiübergreifende Datensammlung für das BKA dient, in welcher es durch abgleichende Verfahren und einer informationstechnischen Unterlaufung der Zweckbindung neue Raster- und Suchmöglichkeiten erhält. Die

Aussagen des Landesdatenschutzbeauftragten lassen zumindest Fragen hinsichtlich der Verfassungsmäßigkeit des Vorhabens aufkommen (E5 2018, 42:40), welche es zukünftig zu klären gilt.

Auch die Manipulation (beispielsweise durch Cyber-Attacken) von Daten, IT-Systemen und insbesondere Algorithmen, welche als Grundlage der vorhersagebasierten Polizeiarbeit dienen, ist als ein zukünftiges Risiko einzuordnen. Smarte Objekte beziehungsweise deren zugrundeliegende Software sowie die cyber-physischen Systeme sind ebenfalls manipulierbar (Kühl 2017). Geschieht eine solche Manipulation (unbemerkt), kann dies zu weitreichenden negativen Konsequenzen für Bürger und Polizei führen (Krüger 2018). Kann eine Smarte Polizeiarbeit auf der einen Seite dem Fachkräftemangel entgegenwirken, so beinhaltet sie gleichzeitig das Risiko, den Polizeibeamten als Menschen obsolet werden zu lassen. Durch automatisierte Prozesse und Entscheidungsfindungen wird die Arbeitskraft der Polizeibeamten in bestimmten Bereichen ersetzbar. Es besteht unter anderem die Gefahr, dass der klassische Streifenpolizist, der seit jeher Bürgernähe vermittelt und als Ansprechpartner eine wichtige Funktion der Dienstleistungsorganisation Polizei übernimmt, durch Automatisierung oder Maschinen ersetzt wird (siehe Polizeiroboter Dubai). Dies beraubt Polizei und Bürger jedoch der oftmals notwendigen zwischenmenschlichen Beziehung und der Empathie. In diesem Kontext ist ebenfalls auf die noch nicht absehbare Rolle der Künstlichen Intelligenz in der Polizeiarbeit zu verweisen, auch wenn sich die Mehrheit der Experten hierbei optimistisch zeigt, dass die Technologie zukünftig lediglich zu unterstützenden Zwecken eingesetzt wird.

7.2 Einordnung der Ergebnisse

Die Diskussion und Analyse der Ergebnisse zeigt, dass im Hinblick auf den Status Quo zwar bereits einige bestehende Stärken einer Smarten Polizeiarbeit festzustellen sind, die Faktoren der bestehenden Schwächen jedoch derzeit überwiegen. Gleichzeitig ergeben sich zukünftig vielfältige Potentiale und Perspektiven, sowohl negativer als auch vermehrt positiver Natur. Die bestehenden Risiken sind bekannt und wurden hinreichend diskutiert. Sie in Zukunft zu vernachlässigen und außer Acht zu lassen, wäre fahrlässig und zugleich gefährlich. Die Ergebnisdiskussion konnte allerdings aufzeigen, dass die positiven Potentiale einer Smarten Polizeiarbeit überwie-

gen. Im Sinne der Häfler Smart Government Definition können smarte Objekte sowie cyber-physische Systeme zukünftig zu einer „effizienten wie effektiven Erfüllung“ polizeilicher Aufgaben beitragen. In Anlehnung an die eingangs vorgenommene Definition einer Smarten Polizeiarbeit bietet die Integration smarter Objekte, cyber-physischer Systeme sowie Big Data-Analysen die Chance, die Effizienz und Transparenz polizeilichen Handelns zu stärken und zu verbesserten Dienstleistungen für die Bürger beizutragen.

Die Body-Cam sowie die polizeiliche Überwachungsdrohne erfahren von den Experten eine überwiegend positive Bewertung. Der Landesdatenschutzbeauftrage äußert hier jedoch zugleich Bedenken, die es zukünftig zu berücksichtigen gilt. Hinsichtlich des Predictive-Policing bleibt abzuwarten, ob der Rückgang von Einbrüchen tatsächlich auf das Programm zurückzuführen ist. Smartphones und Tablets sowie hierauf aufsetzende App-Lösungen werden durchgehend positiv bewertet und können zu einer erheblichen Effizienzsteigerung polizeilichen Arbeitens beitragen. Der smarte Polizeieinsatzwagen wurde von den Experten zwar nicht explizit bewertet, kann aber auf Basis der Fachliteratur sowie bisheriger Praxisbeispiele ebenfalls sehr positiv eingeordnet werden. Differenzierter einzuordnen ist die smarte Videoüberwachung. Die automatische Gesichtserkennung muss derzeit höchst kritisch hinterfragt werden. Ob ein Einsatz an bestimmten Knoten- sowie Brennpunkten sinnvoll sein kann, bleibt zu beobachten. Die unterlegten Mustererkennungen der smarten Videoüberwachung scheinen hingegen vielfältiges positives Potential zu beinhalten.

Die Diskussion der Stärken, Schwächen, Chancen und Risiken verdeutlicht, dass die bestehenden Schwächen sowie die zukünftigen positiven Potentiale einer Smarten Polizeiarbeit derzeit am signifikantesten in Erscheinung treten. Aus dieser Schwäche-Chancen Kombination der SWOT-Analyse ergibt sich die Strategie des *Aufholens* (Meffert, Burmann, & Kirchgeorg 2012, S. 241). Vorhandene Schwächen müssen abgebaut und bestenfalls beseitigt werden, um die sich ergebenden positiven Möglichkeiten zukünftig auszuschöpfen. Folgende Handlungsempfehlungen können die verantwortlichen Akteure hierbei unterstützen.

7.3 Handlungsempfehlungen

Gemeinsames Verständnis erarbeiten

Die vorliegende Arbeit konnte aufzeigen, dass es derzeit an einem gemeinsamen und einheitlichen Verständnis einer Smarten Polizeiarbeit mangelt. Dies erschwert sowohl die wissenschaftliche, als auch insbesondere die praktische Auseinandersetzung mit der Thematik. Daher ist es für die Zukunft der Smarten Polizeiarbeit elementar, dass sich alle betroffenen Akteure an einer gemeinsamen Diskussion beteiligen und ein einheitliches Verständnis einer Smarten Polizeiarbeit entwickeln und festigen. Hier gilt es primär die Meinungen und Bedürfnisse der Zivilgesellschaft zu berücksichtigen, gleichzeitig aber auch jene der Polizeibeamten nicht zu vernachlässigen. Auf Grundlage des erarbeiteten Verständnisses beziehungsweise einer gemeinsamen Definition können dann Handlungsempfehlungen ausgearbeitet werden, die zu einer entsprechenden Zielformulierung beitragen. Die in dieser Arbeit vorgestellte Arbeitsdefinition der Smarten Polizeiarbeit kann hierfür erste Leitlinien aufzeigen.

Transparente Expertenbegleitung und -beurteilung von Projekten

Der unermüdliche technische Fortschritt im Bereich des Internets der Dinge und der Dienste wird die deutsche Polizeiarbeit auch in den nächsten Jahren erheblich beeinflussen. Neue smarte Objekte sowie digitale Lösungen und Anwendungen werden dabei zukünftig in der polizeilichen Aufgabenbewältigung eine immer zentralere Rolle einnehmen. Um die Bürger hierfür zu sensibilisieren sowie den tatsächlichen Nutzen zukünftiger Szenarien einer Smarten Polizeiarbeit zu bewerten, bedarf es einer Disziplinenübergreifenden Expertenbegleitung der Projekte: Polizisten für die Fachkenntnisse zu möglichen Einsatzbereichen, IT-Experten für die Soft- und Hardware hinter den Lösungen, Sozialwissenschaftler für die Vermittlung zwischen Technik und Gesellschaft, Wirtschaftswissenschaftler zur Errechnung des Kosten-Nutzen-Verhältnisses und Juristen zur Formulierung und Einhaltung der rechtlichen Rahmenbedingungen (Eigenseer, Humer, & Lederer 2018, S. 156). Werden die Zielformulierungen und Ergebnisse den Bürgern transparent und offen dargelegt, kann dies zu einer breiten Akzeptanz für polizeiliche Maßnahmen führen. Die Veröffentlichung der einzelnen Schritte des jeweiligen Projektes kann dann beispielsweise durch einen

einsehbaren Politikzyklus[35] erfolgen. Des Weiteren sollten die Polizeien verstärkt Forschungskooperationen mit wissenschaftlichen Instituten oder Universitäten schließen. Als Vorbild können hier die in 3.1 skizzierten „Smart Policing Initiatives" aus den USA dienen, in welchen die Implementierung smarter Objekte und Big Data-Analysen in die Polizeiarbeit von Forschungseinrichtungen begleitet und evaluiert werden.

Verstärkte Investitionen in smarte Lösungen

Die Mehrheit der befragten Experten ist sich einig, dass es zukünftig verstärkter Investitionen in smarte Lösungen bedarf. Die politischen Entscheidungsträger sowie die hierfür Verantwortlichen seitens der Polizeien sollten in Zukunft finanzielle Ressourcen insbesondere für die flächendeckende Anschaffung von Smartphones und Tablets bereitstellen. Die bisherige Arbeit konnte aufzeigen, dass durch die Integration dieser smarten Objekte erhebliche Effizienzsteigerungen erreicht werden können. In der Kombination mit einem smarten Polizeieinsatzwagen als Kommunikations- und Informations-Hub kommt es zu einer mobilen intelligenten Vernetzung polizeilichen Arbeitens. Jeder Polizist sollte zukünftig von überall und zu jeder Zeit einen mobilen Zugriff auf die für seinen Einsatz benötigten Informationen haben. Im Hinblick auf App-Lösungen sollten die Polizeien versuchen, bestehende Erfassungs- und Auskunftssysteme rasch in digitale Anwendungen umzuwandeln. Dabei kann es durchaus Sinn machen, mit einer Testversion in Betrieb zu gehen, welche dann stufenweise weiterentwickelt wird.

Zusammenarbeit und Informationsaustausch der Länderpolizeien verbessern

Eine verbesserte Zusammenarbeit sowie ein regelmäßiger Informationsaustausch zwischen den Länderpolizeien ermöglicht es, die Erfolge, Schwächen, Chancen und Risiken einer Smarten Polizeiarbeit in ihrer Gesamtheit zu erkennen, zu fördern oder zu verhindern. Von einem erhöhten Wissenstransfer mit dem Aufzeigen von bereits vorhandenen und zukünftigen Best-Practice Beispielen einer Smarten Polizeiarbeit profitieren dabei alle Seiten. Zudem bedarf es im Hinblick auf die heutigen Herausforderun-

[35] Ein Schaubild zum Politikzyklus findet sich in Anhang VII.

gen globalisierter und Bundesländergrenzen überschreitender Kriminalität eines verbesserten Datenaustauschs der Polizeien untereinander.

Rechtliche Rahmenbedingungen schaffen

Der Gesetzgeber muss die rechtlichen Rahmenbedingungen einer smarten Polizeiarbeit schaffen und perspektivisch weiterentwickeln. Dabei dürfen die Freiheitsrechte der Bürger nicht als zweitrangig gegenüber der Gewährleistung der öffentlichen Sicherheit erachtet werden. Gleichzeitig muss der Datenschutz möglicherweise hinsichtlich der technischen und gesellschaftlichen Gegebenheiten teils neu ausgelegt und angepasst werden. Sollten hierbei zukünftig tatsächlich verstärkt punktuelle Eingriffe aufgrund bestehender Gefahrenlagen notwendig sein, so bedarf dies jedoch einer sorgfältigen juristischen Prüfung sowie insbesondere eines breiten gesellschaftlichen Konsens.

Smarte Polizeiarbeit als Chance begreifen

Trotz nicht zu vernachlässigender Risiken sollte eine Smarte Polizeiarbeit letztendlich als Chance begriffen werden, aus der sowohl die Bürger als auch die Polizeien erheblichen Mehrwert und Nutzen ziehen können. Der Bürger profitiert hierbei von verbesserten digitalen Dienstleistungen, einer stärkeren Partizipation, beispielsweise durch Bürgerportale, sowie der Erhöhung der öffentlichen Sicherheit und Ordnung. Für die Polizeien bieten die Anwendungen und Lösungen im Internet der Dinge und Dienste sowie die Big Data-Analysen Effizienzsteigerungen und Prozessoptimierungen. Für eine erfolgreiche Smarte Polizeiarbeit bedarf es dabei vor allem eines stetigen Dialogs zwischen Polizeien und Bürger. Hier gilt es zukünftig Formate zu schaffen, in welchen dieser partizipativ gestaltet werden kann. Smarte Polizeiarbeit betrifft letztendlich die gesamte Gesellschaft und darf nicht ausschließlich in Fachkreisen oder unter Ausschluss der Öffentlichkeit diskutiert werden.

7.4 Limitationen

Hinsichtlich der geführten Experteninterviews muss auf Limitationen hingewiesen werden. Wie bereits dargelegt, teilen die Experten kein einheitliches Verständnis einer Smarten Polizeiarbeit. In einigen Interviews wurde deutlich, dass die Experten hierunter eine grundsätzliche Digitalisierung der polizeilichen Arbeit verstehen, ohne Fokus auf Anwendungen im Internet der Dinge und Dienste oder Big Data. Dementsprechend können Verzerrungen im Hinblick auf die Ergebnisdarstellung nicht ausgeschlossen werden. Die Komplexität der untersuchten Thematik erforderte einen breit aufgefächerten Fragebogen. Nicht jeder Experte konnte dabei zu allen Themenbereichen des Fragebogens qualitativ hochwertige Aussagen tätigen, wodurch manche Expertenmeinungen eine höhere Repräsentativität in der Untersuchung erfahren als andere. Seitens des Interviewers wurde zudem nicht immer genug darauf geachtet, dass die Experten speziell die Chancen und Risiken einer Smarten Polizeiarbeit aus Sicht der Bürger in ihre Ausführungen miteinbeziehen. Andererseits kann die Einnahme einer Fremdrolle durch einen Experten die getroffenen Aussagen qualitativ einschränken (Kaiser 2014, S. 133; Krumtung 2018, S. 91). Im Sinne der in Kapitel 4 dargestellten Perspektivenvielfalt einer qualitativen empirischen Untersuchung wäre daher eine weitere Expertenmeinung eines Vertreters der Zivilgesellschaft wünschenswert gewesen. Aus Ressourcengründen musste auf diese Perspektive sowie auf jene weiterer Experten aus den Bereichen Polizei und Justiz verzichtet werden. Die Validierung der Ergebnisse aus den Interviews durch die Experten selbst konnte aufgrund des Zeitrahmens nicht erfolgen, was zu einer qualitativen Schwächung der Ergebnisse führen kann (ebd.).

Des Weiteren handelt es sich bei den hier dargestellten Meinungen und Ergebnissen um „Ist-Aufnahmen“ aus dem Jahr 2018. Aufgrund des technologischen Fortschritts sowie der sich verändernden gesellschaftlichen Rahmenbedingungen wird die Smarte Polizeiarbeit in den nächsten Jahren einem stetigen Wandel unterliegen. Die Gültigkeit der Ergebnisse bedarf daher zukünftig einer regelmäßigen Überprüfung. Der Forschungsgegenstand der Smarten Polizeiarbeit hat sich zudem als ein komplexes und breites Themenfeld erwiesen. Dessen ungeachtet war es das Ziel der Untersuchung, Smarte Polizeiarbeit in ihrer Gesamtheit zu analysieren. Dem begrenzten Umfang dieser Arbeit ist es dabei geschuldet, dass einige Berei-

che und Problemlagen nur oberflächlich aufgegriffen und thematisiert wurden. Gleichzeitig konnten hierdurch möglicherweise anschließende Forschungsfelder aufgezeigt werden.

Für zukünftige Forschungsarbeiten wäre beispielsweise eine genauere Akteursanalyse der Smarten Polizeiarbeit interessant. Fokus der Arbeit könnte eine Betrachtung der Akteure, ihrer Motive und Interessenslagen sowie die Analyse der Beziehungen untereinander sein, um daraus Implikationen für die zukünftige Smarte Polizeiarbeit abzuleiten (van Dyck 2016, S. 107). Eine bundeslandspezifische Untersuchung der Smarten Polizeiarbeit unter Einbeziehung aller verwendeten smarten Objekte, CPS und Big Data-Anwendungen stellt ebenfalls ein sinnvolles Forschungsvorhaben dar. Je mehr Untersuchungen dieser Art existieren, umso besser lassen sich dann Best-Practice Ansätze sowie bundesländerübergreifende Defizite und Problemlagen einer Smarten Polizeiarbeit identifizieren.

8 Fazit und Ausblick

Ziel dieser Arbeit war es, einen Überblick über den Status Quo der Smarten Polizeiarbeit in Deutschland zu geben und die perspektivischen Chancen, Risiken und Herausforderungen aufzuzeigen. Dabei konnte dargelegt werden, dass bereits eine Vielzahl der Länderpolizeien unter anderem Body-Cams, Überwachungsdrohnen, Smartphones und Tablets sowie Predictive-Policing und weitere Big Data-Analysen in ihre Aufgabenbewältigung integrieren, sich hierbei jedoch meist noch in Anfangsstadien oder Pilotprojekten befinden. Dennoch wurde aus den skizzierten Beispielen bereits ersichtlich, dass sich durch eine Smarte Polizeiarbeit Chancen ergeben, von denen Polizeien und Bürger gleichermaßen profitieren können. Gleichzeitig stellt sich die Smarte Polizeiarbeit als ein komplexes Themenfeld dar, in dem die erwünschte Effizienzsteigerung stets die Gefahr unerwünschter Eingriffe in die Freiheitsrechte des Bürgers beinhaltet.

Die rasante Entwicklung im Bereich der Informations- und Kommunikationstechnologien (man denke nur an Technologiesprünge wie die Erfindung des Smartphones) lassen keinen Zweifel daran, dass die Polizeiarbeit in Zukunft immer intelligent vernetzter werden wird. Neue smarte Technologien sowie das Taktile Internet mit dem Mobilfunkstandard *5G*, welches die Kommunikation von smarten Objekten und CPS in Echtzeit ermöglichen soll, stehen bereits vor der Tür. Die Chancen und Möglichkeiten, welche sich hieraus ergeben, werden dabei in gewisser Weise sicherlich unsere heutigen Vorstellungen übertreffen. Neue Potentiale ergeben sich durch den technologischen Fortschritt jedoch ebenso bezüglich der aufgezeigten Risiken und Gefahren - zum Beispiel hinsichtlich einer gesamtgesellschaftlichen Überwachung oder des gläsernen Bürgers. Letztendlich bleibt eine Smarte Polizeiarbeit auch immer Mittel zum Zweck für bestimmende Interessen in Politik und Verwaltung. Daher ist es für eine freiheitlich demokratische Gesellschaft unabdingbar, zukünftige Rahmenbedingungen festzulegen, in welchen der Schutz der Freiheitsrechte und der Datenschutz nicht als zweitrangig angesehen werden. Die inhaltliche Gestaltung einer Smarten Polizeiarbeit muss dabei künftig in einem transparenten konstruktiven Dialog von Politik, Verwaltung, Polizei, Wissenschaft, Wirtschaft und insbesondere der Zivilgesellschaft geführt und bewältigt werden.

Anhang

I. Häfler Definition und Häfler Leitbild von Verwaltung 4.0

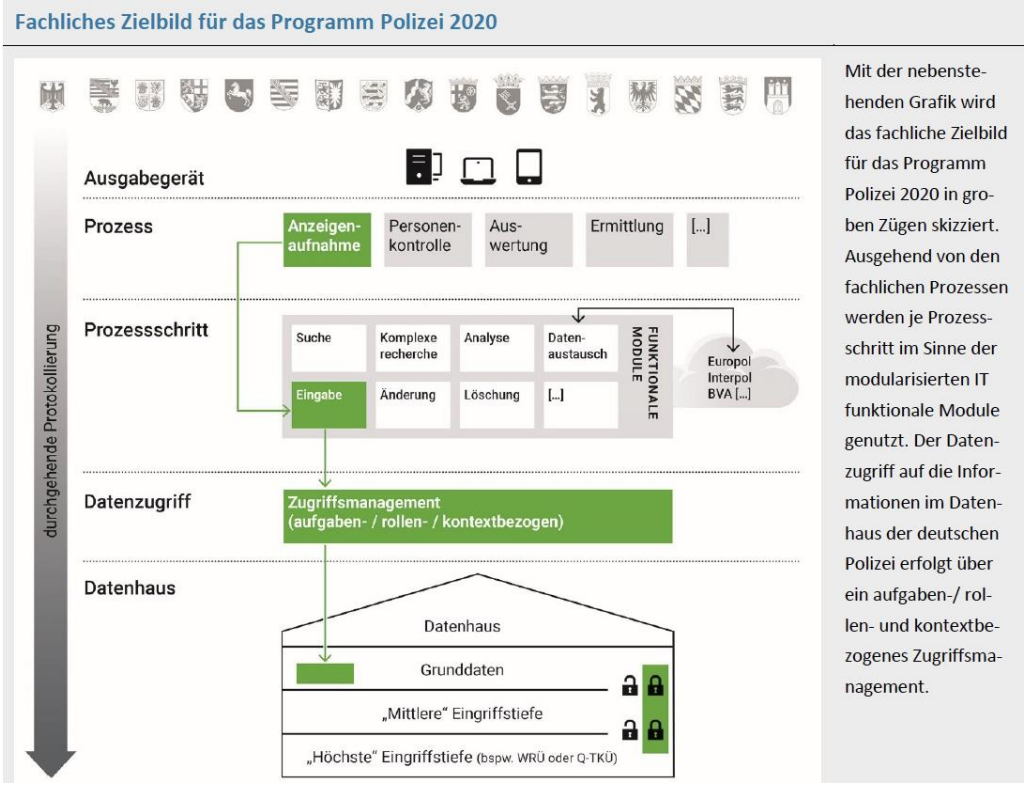
Häfler Definition von Verwaltung 4.0:

„Verwaltung 4.0 meint im Kern die technische Integration von cyberphysischen Systemen in die öffentliche Verwaltung sowie die Anwendung des Internets der Dinge und der Dienste im Rahmen der Prozesse des Regierens und Verwaltens – einschließlich der sich daraus ergebenden Konsequenzen für die Wertschöpfung, die Geschäftsmodelle sowie die nachgelagerten Dienstleistungen und die Arbeitsorganisation" (von Lucke 2015, S. 8).

Häfler Leitbild für Verwaltung 4.0:

"Intelligente Objekte wie etwa smarte Brillen, smarte Fernseher, interaktive Leinwände und vernetzte Kleidungsstücke können in Ministerien, Behörden, Entscheidungsprozessen und Verfahrensabläufen sehr unterschiedliche Verwendung finden. Das gewaltigste Veränderungspotential liegt jedoch nicht im intelligenten Papier, sondern in dessen Überführung in ein intelligentes elektronisches Format. Die flächendeckende Einführung interoperabler elektronischer Akten- und Vorgangsbearbeitungssysteme verlagert Dokumente, Akten, Vorgänge und darauf aufsetzende Dienste in das Internet der Dinge und das Internet der Dienste. Zentrale Aufgaben der Informationsverarbeitung und Entscheidungsfindung lassen sich hochautomatisiert gestalten, ohne (dabei) menschliche Entscheidungsträger aus ihrer Verantwortung zu entlassen. Dies ermöglicht eine stärkere Massenbearbeitung von Einzelanträgen, Rechnungen und Genehmigungsprozessen. Intelligente Vorgänge unterstützen aktiv die Vorgangsbearbeitungsprozesse. Vorgänge steuern sich selbst durch Zuständigkeiten und dynamische Wertschöpfungsnetzwerke. Autonome, sich selbst organisierende Vorgangsbearbeitungssysteme mit Genehmigungsfiktion ersetzen die bewährte papierbasierte wie botenlastige Aktenhaltung. Portalbasierte einheitliche Ansprechpartner kümmern sich um das gesamte Anliegen der Bürger und Unternehmen, ohne diese mit administrativen Kenntnissen zu überfordern. Proaktive Verwaltungsleistungen und intelligente Bescheide ergänzen das Leistungsportfolio. All diese neuartigen kooperativen Ansätze stärken die dynamische Selbstorganisation und können zur Auflösung von klassischen Zuständigkeits- und Fachbereichsgrenzen führen" (von Lucke 2015, S. 8).

II. Schaubild: Fachliches Zielbild für „Polizei 2020“



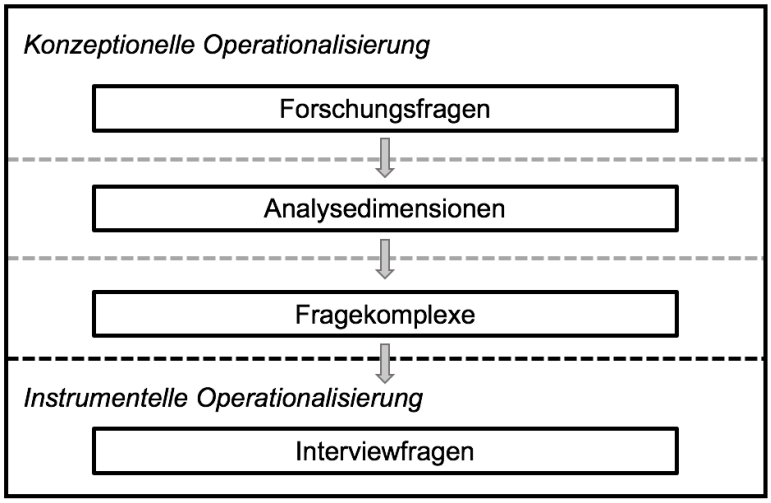
Quelle: Bundesministerium des Innern, für Bau und Heimat: Polizei 2020 – White Paper 2017, S. 15.

Siehe:
https://www.bmi.bund.de/SharedDocs/downloads/DE/veroeffentlichungen/2018/polizei-2020-white-paper.pdf?__blob=publicationFile&v=1.

III. Übersicht zu den geführten Experteninterviews

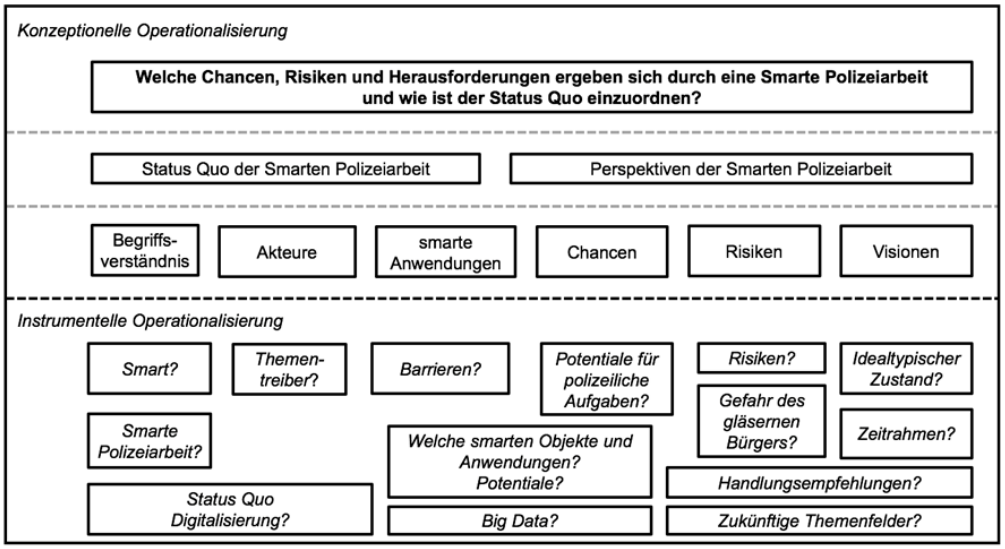
Kürzel	Position	Datum	Interviewform
E1	Führungskraft in einem Landespolizeipräsidium	20.03.2018	Persönlich
E2	Wissenschaftler in einem deutschen Forschungsinstitut	19.03.2018	Telefonisch
E3	Politischer Vertreter auf Landesebene	26.03.2018	Telefonisch
E4	Führungskraft in einem Technologieunternehmen	27.03.2018	Telefonisch
E5	Landesbeauftragter für den Datenschutz	03.04.2018	Persönlich
E6	Berater in einem Technologieunternehmen	06.04.2018	Telefonisch
E7	Mitarbeiter in einem Bundesministerium	12.04.2018	Persönlich
E8	Politischer Aktivist (Journalist)	14.04.2018	Persönlich

IV. Schaubild: Operationalisierung der Forschungsfrage



Schema: Konzeptionelle und instrumentelle Operationalisierung

(Eigene Darstellung in Anlehnung an Kaiser 2014, S. 57; Krumtung 2018, S. 50)



Konzeptionelle und instrumentelle Operationalisierung der Forschungsfrage

(Eigene Darstellung in Anlehnung an: Kaiser 2014, S. 57-62; Krumtung 2018, S. 51.)

V. Verwendeter Leitfaden für die Experteninterviews

Ziel dieser Untersuchung ist es, eine Analyse der Smarten Polizeiarbeit in Deutschland zu vollziehen. Hierbei soll aufgezeigt werden, wer die relevanten Akteure sind, welche Anwendungen und Technologien genutzt werden und welche Chancen bzw. Herausforderungen sich bezüglich einer Smarten Polizeiarbeit ergeben und gesehen werden. Der Fokus der Untersuchung soll dabei auf der Beantwortung der Frage liegen, welchen Nutzen bzw. Mehrwert eine Smarte Polizeiarbeit für die Gesellschaft mit sich bringt sowie welche Risiken hieraus entstehen können. Dieses Interview mit Ihnen ist Teil einer Reihe von Interviews mit verschiedenen Experten, die jeweils aus ihrer Perspektive eine Einschätzung zum Status Quo und den perspektivischen Chancen und Herausforderungen der Smarten Polizeiarbeit geben sollen. Ziel ist es, einen umfassenden und fundierten Gesamtüberblick zu erhalten und Perspektiven aufzuzeigen. Zur späteren Auswertung werde ich das Interview aufzeichnen. Sind Sie hiermit einverstanden? Auf Wunsch können die Ergebnisse des Interviews auch anonymisiert werden.

Einstieg

1. Bitte fassen Sie in wenigen Worten Ihre Position und Ihr Aufgabenfeld zusammen.

2. Was verstehen Sie unter dem Begriff „smart"?

3. Was verstehen Sie unter smarter Polizei/Smarter Polizeiarbeit?

4. Wie bewerten Sie den Status Quo der Polizeiarbeit in Deutschland in Bezug auf die Digitalisierung?

Anwendungen/Technologien

5. In welchen Aufgabenfeldern kann Ihrer Meinung nach mittels smarter Anwendungen und Technologien die Arbeit der Polizei besonders verbessert bzw. unterstützt werden?

6. a) In welchen Bereichen setzt die Polizei bereits auf die Analyse großer Datenmengen/Big Data, für eine wirtschaftliche und sparsame Erledigung von Polizeiaufgaben?

b) Können Sie sich vorstellen, dass Computer zukünftig eigenständig und autonom Einsätze koordinieren oder auch Verhaftungen veranlassen?

7. Die Polizei kann unterschiedlichste smarte Anwendungen nutzen. Welche smarten Anwendungen und Technologien sind Ihrer Meinung nach am erfolgversprechendsten?

Akteure

8. Wen würden Sie im Bereich der Smarten Polizeiarbeit als Hauptthementreiber bezeichnen?

Vision

9. Skizzieren Sie bitte Ihren idealtypischen Zustand einer digitalisierten und Smarten Polizeiarbeit?

10. a) Welche Rolle spielen smarte Technologien und Objekte zur Erreichung dieses idealtypischen Zustands?

    b) Sehen Sie eine Chance diesen Zustand in den nächsten 1, 3, 5 oder 10 Jahren zu erreichen?

11. Skizzieren Sie bitte Barrieren vor welchen die Polizei bei dieser Umsetzung derzeit steht.

12. Welche Rolle spielt Ihrer Meinung nach Offenheit und Transparenz sowie die Partizipation der Bürger im Hinblick auf eine Smarte Polizeiarbeit?

Risiken

13. Sehen Sie Risiken einer Smarten Polizeiarbeit für die Bürger und die Gesellschaft?

14. Wie realistisch schätzen Sie in diesem Zusammenhang die Gefahr des „gläsernen Bürgers“ ein, der für die Polizeiarbeit sehr transparent ist und nur noch auf die von ihm zur Verfügung stehenden Daten reduziert wird?

Sonstiges

15. Welches sind Ihrer Meinung nach die drei größten Themenfelder, welche die Polizei in einer zunehmend digitalisierten Welt zukünftig besetzen muss?

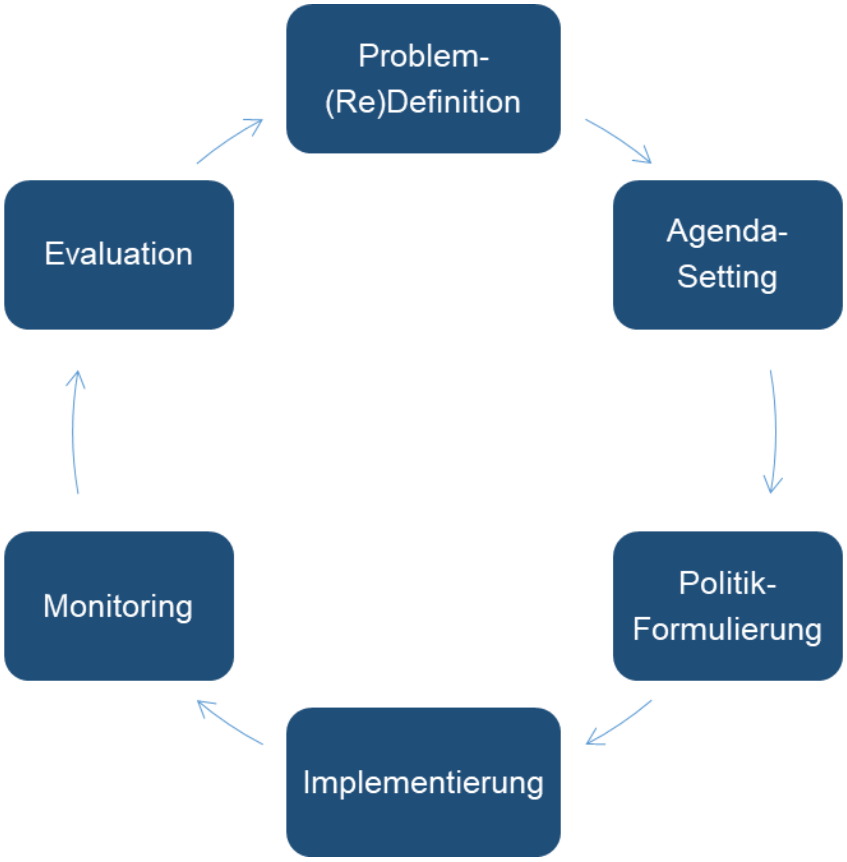
16. Zum Abschluss, welche Vorschläge haben Sie noch parat, um eine Smarte Polizeiarbeit weiter zu fördern und zu etablieren?

17. Gibt es noch etwas, dass Sie gerne anfügen würden oder Literaturempfehlungen, die Sie mir gerne auf den Weg mitgeben würden?

VI. Funktionsweise der SWOT-Analyse

Die SWOT-Analyse ist eine Methode der strategischen Planung, die vorrangig für die spezifische Situationsanalyse eines Unternehmens und dessen Umwelt eingesetzt wird (Feig 2016). Sie eignet sich jedoch ebenso gut für die Strategieplanungen und Situationsanalysen von Institutionen und Behörden der öffentlichen Verwaltung (Wollny & Paul 2015, S. 190). Die SWOT-Analyse dient als Instrument, um wichtige Trends und Faktoren für das Erreichen von Organisationszielen mittels der vier Kategorien der bestehenden Stärken und Schwächen sowie der perspektivischen Chancen und Risiken systematisch zu erfassen. Insbesondere bei der Implementierung neuer Dienstleistungen dient die Analyse dabei als wichtige Unterstützung zur Erarbeitung zukünftiger Strategien. Je nachdem, welche der vier Kategorien abschließend maßgeblich in Erscheinung treten, lassen sich daraufhin konkrete Handlungsempfehlungen ableiten (Meffert, Burmann, & Kirchgeorg 2012, S. 241).

VII. Schaubild zum (sechsstufigen) Politikzyklus



Quelle: Eigene Darstellung in Anlehnung Blum & Schubert 2018, S. 156.

Literaturverzeichnis

Accenture 2018: Accenture Dienstleistungen GmbH: West Midlands Police – Erfolgreicher Umbau, Accenture Dienstleistungen GmbH, Kronberg im Taunus 2018. Online: https://www.accenture.com/de-de/success-transforming-west-midlands-police.

Aggarwal 2016: Aggarwal, Anil K.: Opportunities and Challenges of Big Data in the Public Sector, in: Aggarwal, Anil K. (Hrsg.): Managing Big Data Integration in the Public Sector, IGI Global, Hershey 2016, S. 289-301.

Al Shouk 2017: Al Shouk, Ali: Dubai Police: Era of innovative policing begins, Gulf News, Ausgabe vom 27. Dezember 2017, Dubai 2017.
Online: https://gulfnews.com/news/uae/government/dubai-police-era-of-innovative-policing-begins-1.2147813.

Albers 2012: Albers, Marion: Das Präventionsdilemma, in: Jan-Hinrik Schmidt und Thilo Weichert: Datenschutz: Grundlagen, Entwicklungen und Kontroversen, Bundeszentrale für politische Bidung, Bonn 2012, S. 102-115.

Altmann 2012: Altmann, Jürgen: Armed Robots and Preventive Arms Control, in: Michael Decker: Robo- und Informationethics, LIT Verlag, Zürich 2012, Bd. 3.

Amnesty International 2018: United Arab Emirates 2017/2018, Amnesty International, London 2018. Online: https://www.amnesty.org/en/countries/middle-east-and-north-africa/united-arab-emirates/report-united-arab-emirates/.

Anabah 2018: Anabah, Kerstin: Dashcam-Videos vor Gericht zulässig, Tagesschau.de, Hamburg 15. Mai 2018. Online: https://www.tagesschau.de/inland/dashcam-urteil-101.html.

Baecker 2007: Baecker, Dirk: Studien zur nächsten Gesellschaft, Suhrkamp Verlag, Frankfurt a.M. 2007.

Baumann & Lyon 2014: Baumann, Zygmunt & Lyon, David: Daten, Drohnen, Disziplin, Suhrkamp Verlag, Berlin 2014.

Bayerl & Rüdiger 2017: Bayerl, Petra-Saskia & Rüdiger, Thomas-Gabriel: Die polizeiliche Nutzung sozialer Medien in Deutschland: Die Polizei im digitalen Neuland, in: Jürgen Stierle, Dieter Wehe und Helmut Siller: Handbuch Polizeimanagement, Springer Fachmedien, Wiesbaden 2017.

Behörden Spiegel 2018: Moderne Technik bietet erhebliche Potenziale: Gesichtserkennung mit hoher Trefferquote, Behörden Spiegel Februar 2018, Bonn, S. 40.

Behr 2006: Behr, Rafael: Polizeikultur: Routinen - Rituale - Reflexionen, VS Verlag für Sozialwissenschaften, Wiesbaden 2006.

Beinrott 2013: Beinrott, Viktoria: Big Data in der öffentlichen Verwaltung in Deutschland, in: Jörn von Lucke: TOGI Schriftenreihe: Potential einer Öffnung von Staat und Verwaltung, Bd. 8, epubli GmbH, Friedrichshafen 2013, S. 106-120.

Bundesamt für Verfassungsschutz 2018: Anti-Terror-Datei (ATD), Bundesamt für Verfassungsschutz, Köln 2018.
Online: https://www.verfassungsschutz.de/de/service/glossar/anti-terror-datei-atd.

Birken & Eick 2017: Birken, Kendra & Eick, Volker: Pazifizierungsagenten - Zu einem Tätigkeitsprofil kommerzieller Sicherheitsdienste, in: Joachim Häfele et al. (Hrsg.): Sicherheit und Kriminalprävention in urbanenen Räumen, Springer VS, Wiesbaden 2017, S. 91-109.

bitkom 2018: Arbeitskreis Big Data und Advanced Analytics, bitkom.org, Berlin 2018. Online: https://www.bitkom.org/Bitkom/Organisation/Gremien/Big-Data-und-Advanced-Analytics.html.

Blum & Schubert 2018: Blum, Sonja & Schubert, Klaus: Politikfeldanalyse: Eine Einführung, Springer Fachmedien, Wiesbaden 2018.

Bundesministerium des Innern, für Bau und Heimat 2017: "Sicherheitsbahnhof Berlin Südkreuz", Bundesministerium des Innern, für Bau und Heimat, Berlin 2017. Online:
https://www.bmi.bund.de/SharedDocs/pressemitteilungen/DE/2017/08/gesichtserkennungstechnik-bahnhof-suedkreuz.html.

Bundesministerium des Innern, für Bau und Heimat 2017: Polizei 2020 - White Paper, Bundesministerium des Innern, Berlin 2017.

Bundesministerium für Verkehr und digitale Infrastruktur 2018: Klare Regeln für Betrieb von Drohnen, Bundesministerium für Verkehr und digitale Infrastruktur, Berlin 2018. Online: http://www.bmvi.de/SharedDocs/DE/Artikel/LR/151108-drohnen.html.

Borchers 2017: Borchers, Detlef: Automatische Gesichtserkennung: Test der Bundespolizei bringt "gesteigertes Sicherheitsgefühl" oder "Überwachungsdruck",

heise online, Hannover 2. August 2017,
Online: https://www.heise.de/newsticker/meldung/Automatische-Gesichtserkennung-Test-der-Bundespolizei-bringt-gesteigertes-Sicherheitsgefuehl-oder-3789990.html.

Bundeszentrale für politische Bildung 2018: Informationelle Selbstbestimmung, Bundeszentrale für politische Bildung, Bonn 2018.
Online: http://www.bpb.de/nachschlagen/lexika/recht-a-z/22392/informationelle-selbstbestimmung.

Brand 2018: Brandl, Steven G.: Police in America, London : SAGE Publications Inc., Chicago 2018.

Breithut & Böhm 2016: Breithut, Jörg & Böhm, Markus: Schleichend zum Überwachungsstaat, Spiegel Online, Hamburg 27. November 2016. Online: http://www.spiegel.de/netzwelt/netzpolitik/deutschland-schleichend-zum-ueberwachungsstaat-a-1121162.html.

Breslin 2017: Breslin, Susannah: Meet The Terrifying New Robot Cop That´s Patrolling Dubai, Forbes, Jersey City 2017.
Online: https://www.forbes.com/sites/susannahbreslin/2017/06/03/robot-cop-dubai/#6e3446df6872.

Bretthauer 2017: Bretthauer, Sebastian: Intelligente Videoüberwachung: Eine datenschutzrechtliche Analyse unter Berücksichtigung technischer Schutzmaßnahmen, Nomos Verlagsgesellschaft, Frankfurt a.M. 2017.

Bundeskriminalamt 2018: Fakten und Zahlen, Bundeskriminalamt.de, Wiesbaden 2018. Online: https://www.bka.de/DE/DasBKA/FaktenZahlen/faktenzahlen_node.html.

Bundespolizei 2018: Zahlen, Daten, Fakten, Bundespolizei.de, Berlin 2018. Online: https://www.bundespolizei.de/Web/DE/05Die-Bundespolizei/07Daten-Fakten/Daten-Fakten_node.html.

Bundesrat, Eidgenössischer 2007: E-Government-Strategie Schweiz, Auflage Mai 2009, Bern 2009.

Bundestag, Deutscher 2016: Antwort der Bundesregierung, Drucksache 18/7966, auf die Kleine Anfrage der Abgeordneten Andrej Hunko, Herbert Behrens, Eva Bulling-Schröter, weiterer Abgeordneter und der Fraktion DIE LINKE - Drucksache 18/7638, Berlin, 23. März 2016.

Bundesverfassungsgericht 2016a: Verfassungsbeschwerde gegen die Ermittlungsbefugnisse des BKA zur Terrorismusbekämpfung teilweise erfolgreich, Bundesverfassungsgericht, Karlsruhe 20. April 2016. Online: https://www.bundesverfassungsgericht.de/SharedDocs/Pressemitteilungen/DE/2016/bvg16-019.html.

Bundesverfassungsgericht 2016b: Urteil des Ersten Senats vom 20. April 2016, Bundesverfassungsgericht, Karlsruhe 20. April 2016. Online: https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/2016/04/rs20160420_1bvr096609.html.

Coldren et al. 2013: Coldren, James R., Huntoon, Alissa & Michael Medaris: Introducing Smart Policing: Foundations, Principles and Practices, Police Quarterly, Dallas 2013, Bd. 16, 3, S. 275-286.

Curry 2016: Curry, Edward: The Big Data Value Chain: Definitions, Concepts, and Theoretical Approaches, in: Jose Maria Cavanillas, Edward Curry und Wolfgang Wahlster: New Horizons for a Data-Driven Economy, Springer, Wiesbaden 2016, S. 29-39.

De Mauro et al. 2016: De Mauro, Andrea; Greco, Marco & Grimaldi, Michele: A formal definition of Big Data based on its essential features, Library Review 2016, 65, S. 122-135.

Demuth 2017: Demuth, Kerstin: Überwachung ist nicht Sicherheit - Überwachung ist Überwachung, digitalcourage.de, Bielefeld 2017. Online: https://digitalcourage.de/blog/2017/ueberwachung-ist-nicht-sicherheit-ueberwachung-ist-ueberwachung.

Denninger 2008: Denninger, Erhard: Prävention und Freiheit - Von der Ordnung der Freiheit, in: Stefan Huster und Karsten Rudolph: Vom Rechtsstaat zum Präventionsstaat, Suhrkamp Verlag, Frankfurt a.M. 2008.

Detempele et al. 2017: Detempele, Peter; Düsing, Sandra & Schramm, Thorsten: Fachkräftemangel im öffentlichen Dienst, PricewaterhouseCoopers GmbH Wirtschaftsprüfungsgesellschaft, Frankfurt a. M. 2017.

Diekmann 2013: Diekmann, Andreas: Empirische Sozialforschung: Grundlagen, Methoden, Anwendung, Rowohlt Taschenbuch Verlag, Hamburg 2013.

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.

Donner 2016: Donner, Andreas: 2020: fast 800 Mio. vernetzte Geräte in Deutschland, IP Insider, Augsburg 16. Juni 2016. Online: https://www.ip-insider.de/2020-fast-800-mio-vernetzte-geraete-in-deutschland-a-537991/.

Dubai Police 2018: Smart Dubai., Dubai 2018. Online: [Zitat vom: 24. April 2018.] http://www.smartdubai.ae/dubai_police.php.

Duden 2018: smart - Rechtschreibung und Bedeutungsübersicht, Dudenverlag, Berlin 2018. Online: https://www.duden.de/rechtschreibung/smart.

Dürig 1956: Dürig, Günter: Der Grundrechtssatz von der Menschenwürde, Archiv des öffentlichen Rechts (AöR), Heidelberg 1956, Band 81.

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

E-Government Schweiz Geschäftstelle 2010: Informatikstrategieorgan: facts and figures Umsetzung Strategie, Bund ISB, Bern 2010.

Ehneß 2017: Ehneß, Susanne: Startschuss für IT-Projekt "Polizei 2020", in: eGovernment Computing, Augsburg 2. Mai 2017. Online: https://www.egovernment-computing.de/startschuss-fuer-it-projekt-polizei-2020-a-604441/.

Ehneß 2016a: Ehneß, Susanne: Big Data macht Behörden effektiver und servicefreundlicher, in: eGovernment Computing, Ausgabe Februar 2016, Augsburg 2016.

Ehneß 2016b: Ehneß, Susanne: Tablets für die mobile Polizeiarbeit, eGovernment Computing, Augsburg 23. Juli 2016. Online: https://www.egovernment-computing.de/tablets-fuer-die-mobile-polizeiarbeit-a-542847/.

Eichner 2018: Eichner, Jochen: Polizisten in Bayern bekommen Bodycams, Bayerischer Rundfunk, München 28. Februar 2018. Online: https://www.br.de/nachrichten/bayerns-polizisten-bekommen-bodycams-100.html.

Eigenseer et al. 2018: Eigenseer, Alex Elisabeth; Humer, Stephan & Lederer, Anna: Von der konventionellen zur intelligenten Videoüberwachung - Chancen und Risiken für Polizei und Gesellschaft, in: Thomas-Gabriel Rüdiger und Petra Saskia

Bayerl: Digitale Polizeiarbeit – Herausforderungen und Chancen, Springer Fachmedien GmbH, Wiesbaden 2018, S. 147-157.

Factsheet eGovernment Switzerland 2018: eGovernment in Switzerland, Brüssel 2018. Online: https://joinup.ec.europa.eu/sites/default/files/inline-files/eGovernment_in_Switzerland_2018_0.pdf.

Feig 2016: Feig, Jürgen: SWOT-Analyse, business-wissen.de, Karlsruhe 2. Februar 2016. Online: http://www.business-wissen.de/artikel/swot-analyse-so-wird-eine-swot-analyse-erstellt/.

Feldmann 2018: Feldmann, Marco: Ohne Vernetzung geht es nicht mehr: Ermittler müssen heutzutage grenzüberschreitend zusammenarbeiten, Behörden Spiegel, Bonn Feburar 2018, S. 38.

Feltes 2008: Feltes, Thomas: Akteure der Inneren Sicherheit: Vom Öffentlichen zum Privaten, in: Hans-Jürgen Lange, H. Peter Ohly und Jo Reichertz (Hrsg.): Auf der Suche nach neuer Sicherheit: Fakten, Theorien und Folgen, VS Verlag für Sozial-wissenschaften, Wiesbaden 2008, S. 105-115.

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

Frevel & Große 2016: Frevel, Bernhard und Groß, Hermann: "Polizei ist Ländersache!" - Polizeipolitik unter den Bedingungen des deutschen Föderalismus, in: Achim Hildebrandt und Frieder Wolf (Hrsg.): Die Politik der Bundesländer, Springer Fachmedien, Wiesbaden 2016, S. 61-86.

Gammelin 2016: Gammelin, Cerstin: Haushalt 2017: Mehr Geld für Bundeswehr und Polizei, in: Süddeutsche Zeitung, München 23. März 2016. Online: http://www.sueddeutsche.de/politik/haushalt-mehr-geld-fuer-bundeswehr-und-polizei-1.2920594.

GdP (Gewerkschaft der Polizei) 2017: GdP-Fachtagung in Brüssel: GdP-Vorsitzender Malchow forder "smarte" Polizei, Gewerkschaft der Polizei, Hilden 2017. Online: https://www.gdp.de/gdp/gdp.nsf/id/DE_GdP-Vorsitzender-Malchow-fordert-smarte-Polizei?open&ccm=000.

Gehm 2017: Gehm, Florian: Wenn aus Einsatzkräften smarte Cyborgs werden, welt.de, Berlin 20. Oktober 2017.
Online: https://www.welt.de/wirtschaft/article169828785/Wenn-aus-Einsatzkraeften-smarte-Cyborgs-werden.html.

Gehrke 2017: Gehrke, Kerstin: Obdachloser angezündet - Prozess beginnt, Der Tagesspiegel, Berlin 8. Mai 2017.
Online: https://www.tagesspiegel.de/berlin/feuerattacke-in-berliner-u-bahnstation-obdachloser-angezuendet-prozess-beginnt/19768934.html.

Gerstner 2017: Gerstner, Dominik: Predictive Policing als Instrument zur Prävention von Wohungseinbruchsdiebstahl, Max-Planck-Institut für ausländisches und internationales Strafrecht, forschung aktuell, Freiburg 2017.

Gil-Carcia 2012: Gil-Garcia, J. Ramon: Towards a smart State? Inter-agency collaboration, information integration, and beyond, Information Polity, 2012, S. 269-280.

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

Groß 2008: Groß, Hermann: Deutsche Länderpolizeien, Aus Politik und Zeitgeschichte: Polizei, Bonn November 2008, Bd. 48, S. 18-24.

Groß 2012: Groß, Hermann: Polizeien in Deutschland, Bundeszentrale für politische Bildung, Bonn 14. Juni 2012. Online: http://www.bpb.de/politik/innenpolitik/innere-sicherheit/76660/polizeien-in-deutschland?p=all.

Guendez et al. 2017: Guenduez, Ali Asker; Mettler, Tobias & Schedler, Kuno: Smart Government - Partizipation und Empowerment der Bürger im Zeitalter von Big Data und personalisierter Algorithmen, Springer Fachmedien, Wiesbaden 2017.

Gusy 2014: Gusy, Christoph: Aufklärungsdrohnen im Polizeieinsatz, in: Die Kriminalpolizei - Zeitschrift der Gewerkschaft der Polizei, Ausgabe März, Hilden 2014.

Hanning 2008: Hanning, August: Sicherheit gewährleisten - Freiheit wahren, in: Stefan Huster und Karsten Rudolph (Hrsg.): Vom Rechtsstaat zum Präventionsstaat, Suhrkamp Verlag, Frankfurt 2008, S. 191-207.

Hansen 2012: Hansen, Marit: Überwachungstechnologie, in: Jan-Hinrik Schmidt und Thilo Weichert: Datenschutz: Grundlagen, Entwicklungen und Kontroversen, Bundeszentrale für politische Bildung, Bonn 2012, S. 78-88.

Hauptmann 2017: Hauptmann, Alexander: Rechtliche Zulässigkeit des polizeilichen Einsatzes von Body-Cams im Land Bremen, Masterarbeit im Studiengang Public Administration, Universität Kassel, 14. Januar 2017.

Herbig 2018: Herbig, Daniel: Chinesische Polizei setzt Überwachungsbrillen zur Gesichtserkennung ein, heise online, Hannover 9. Februar 2018. Online: https://www.heise.de/newsticker/meldung/Chinesische-Polizei-setzt-Ueberwachungsbrillen-zur-Gesichtserkennung-ein-3964810.html.

Heuermann et al. 2018: Heuermann, Roland; Tomenendal, Matthias & Bressem, Christian: Digitalisierung in Bund, Ländern und Gemeinden - IT-Organisation, Management und Empfehlungen, Springer Gabler, Wiesbaden 2018.

Hof 2017: Hof, Joachim: Datenschutz mittels IT-Sicherheit, in: Marie-Theres Tinnefeld, et al. (Hrsg.): Einführung in das Datenschutzrecht, De Gruyter, Berlin 2017, S. 469-511.

Hofstetter 2016: Hofstetter, Yvonne: Das Ende der Demokratie - Wie die Künstliche Intelligenz die Politik übernimmt und uns entmündigt, C. Bertelsmann Verlag, München 2016.

Holland 2017: Holland, Martin: Bayern: Neuer Polizei-Messenger für Streifenbeamte, heise online, Hannover 2017. Online: https://www.heise.de/newsticker/meldung/Bayern-Neuer-Polizei-Messenger-fuer-Streifenbeamte-3725791.html.

icomedias 2016: Pilotprojekt zu Mobile Policing im Saarland zeigt deutliches Einsparungspotenzial in der Administration, icomedias.com, Graz 2016. Online: http://www.icomedias.com/de/saarland-mobile-policing/.

IfmPt 2018: Near Repeat Prediction Method: Predictive Policing made in Germany, Institut für musterbasierte Prognosetechnik, Oberhausen 2018. Online: http://www.ifmpt.de.

Jähnichen 2015: Jähnichen, Stefan: Von Big Data zu Smart Data – Herausforderungen für die Wirtschaft, in: Smart Data Begleitforschung: Smart Data Newsletter, Berlin August 2015.

Jansen 2017: Jansen, Jonas: 8,4 Milliarden vernetzte Geräte im Internet der Dinge, Franfurter Allgemeine, Frankfurt 7. Feburar 2017.
Online: http://www.faz.net/aktuell/wirtschaft/netzwirtschaft/digitalisierung-8-4-milliarden-vernetzte-geraete-im-internet-der-dinge-14865654.html.

Jordan 2017: Jordan, Christin: "Predictive Policing" Mit Vorhersage Software gegen Verbrecher?, tagesschau.de, Hamburg 16. November 2017. Online: https://www.tagesschau.de/inland/polizei-prognosesoftware-101.html.

Jung 2018: Jung, Wolfgang: Projekt mit intelligenten Kameras: Rennen und Fallen sind in Mannheim bald verdächtig, Spiegel-Online, Mannheim 14. Februar 2018. Online: http://www.spiegel.de/netzwelt/netzpolitik/mannheimer-weg-2-0-pilotprojekt-mit-intelligenten-kameras-startet-bald-a-1193622.html.

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

Kartheuser 2018: Kartheuser, Boris: Kontrolle ist gut, Überwachung ist besser, in: Spiegel-Online, Hamburg 27. Januar 2018.
Online: http://www.spiegel.de/panorama/justiz/predictive-policing-in-los-angeles-kontrolle-ist-gut-ueberwachung-ist-besser-a-1188578.html.

Kästner & Kuhlmann 2016: Kästner, Ann-Kristin und Kuhlmann, Simone: Predictive Policing - Prädikative Polizeiarbeit zwischen Innovationsbegeisterung und rechtlichen Schranken, Junge Wissenschaft im Öffentlichen Recht, Kiel 2016.

Kerkmann 2018: Kerkmann, Christof: Big Brother durch Big Data, Handelsblatt, Düsseldorf 9. März 2018, 49, S. 57.

Klein 2015: Klein, Manfred: IT in der Polizeiarbeit - Digitale Gesellschaft fordert digitale Polizei, eGovernment Computing, Augsburg 8. April 2015.

Klöpfer 2017: Klöpfer, Inge: Deutschland braucht mehr Polizisten, Frankfurter Allgemeine Zeitung, Frankfurt 4. März 2017.
Online: http://www.faz.net/aktuell/wirtschaft/polizei-in-deutschland-leidet-unter-personalmangel-14896320.html?printPagedArticle=true#pageIndex_0.

Koalitionsvertrag zwischen CDU, CSU und SPD 2018: Ein neuer Aufbruch für Europa, Eine neue Dynamik für Deutschland, Ein neuer Zusammenhalt für unser Land, Februar 2018.

Koch 2011: Koch, Max: Wieviel Leadership verträgt die Schweizer Demokratie?, Glarus : Rüegger-Verlag, Bern 2011.

KPMG 2017: Big Data, große Baustelle - Mit Daten Werte schaffen 2017, Sonderausgabe für die öffentliche Verwaltung, Frankfurt 2017.

Krempl 2016: Krempl, Stefan: "Intelligente Polizei": Mit "Linked Data" und "smarten Maulwürfen" auf Verbrecherjagd, heise.de, Hannover 30. März 2016. Online: https://www.heise.de/newsticker/meldung/Intelligente-Polizei-Mit-Linked-Data-und-smarten-Maulwuerfen-auf-Verbrecherjagd-3157558.html.

Krempl 2017: Krempl, Stefan: Datenschützerin warnt vor Videoüberwachung mit Gesichtserkennung, heise.de, Hannover 24. Februar 2017. Online: https://www.heise.de/newsticker/meldung/Datenschuetzerin-warnt-vor-Videoueberwachung-mit-Gesichtserkennung-3634544.html.

Krüger 2018: Krüger, Julia: Wie der Mensch die Kontrolle über den Algorithmus behalten kann, netzpolitik.org, Berlin 19. Januar 2018.
Online: https://netzpolitik.org/2018/algorithmen-regulierung-im-kontext-aktueller-gesetzgebung/.

Krüger 2017: Krüger, Paul-Anton: Die einen sagen "Smart City", die anderen "Polizeistaat", in: Süddeutsche Zeitung, München 6. August 2017.
Online: http://www.sueddeutsche.de/digital/dubai-die-einen-sagen-smart-city-die-anderen-polizeistaat-1.3611810.

Kuckartz 2005: Kuckartz, Udo: Einführung in die computergestützte Analyse qualitativer Daten, VS Verlag für Sozialwissenschaften, Wiesbaden 2005.

Kühl 2017: Kühl, Eike: Das Internet der Dinge vor Gericht, Zeit.de, Hamburg 9. Mai 2017. Online: https://www.zeit.de/digital/datenschutz/2017-05/republica-internet-der-dinge-iot-gericht-beweise.

Kühn 2017: Kühn, Franka: Die demografische Entwicklung in Deutschland, Bundeszentrale für politische Bildung, Bonn 29. August 2017. Online: http://www.bpb.de/politik/innenpolitik/demografischer-wandel/196911/fertilitaet-mortalitaet-migration.

Kühne 2012: Kühne, Eberhard: Informationsverarbeitung und Wissensmanagement der Polizei beim Aufbruch in eine digitalisierte Welt, Loreri Verlag für Polizeiwissenschaften, Frankfurt 2012.

Kurpjuweit 2018: Kurpjuweit, Klaus: Bundespolizei wird mit Bodycams ausgestattet, Der Tagesspiegel, Berlin 12. Januar 2018.
Online: https://www.tagesspiegel.de/berlin/neue-sicherheitstechnik-bundespolizei-wird-mit-bodycams-ausgestattet/20843164.html.

Kutsche 2017: Kutsche, Katharina: Digital im Einsatz, in: Süddeutsche Zeitung, München 9. Oktober 2017.
Online: http://www.sueddeutsche.de/wirtschaft/modernisierung-des-arbeitsalltags-digital-im-einsatz-1.3700561.

Ladner & Bühlmann 2007: Ladner, Andreas und Bühlmann, Marc: Demokratie in den Gemeinden, Rüegger Verlag, Zürich 2007.

Lange & Frevel 2008: Lange, Hans-Jürgen und Frevel, Bernhard: Innere Sicherheit im Bund, in den Ländern und in den Kommunen, in: Hans-Jürgen Lange, H. Peter Ohly und Jo Reichertz (Hrsg.): Auf der Suche nach neuer Sicherheit: Fakten, Theorien und Folgen, VS Verlag für Sozialwissenschaften, Wiesbaden 2008, S. 115-149.

Lee 2017: Lee, Felix: Die AAA-Bürger, Zeit.de, Hamburg 30. November 2017. Online: https://www.zeit.de/digital/datenschutz/2017-11/china-social-credit-system-buergerbewertung.

Leubecher & Kade 2016: Leubecher, Marcel und Kade, Claudia: Videoüberwachung: "Datenschutz darf nicht zum Täterschutz werden", Welt.de, Berlin 28. Dezember 2016. Online: https://www.welt.de/politik/deutschland/article160643348/Datenschutz-darf-nicht-zum-Taeterschutz-werden.html.

Markgraf 2018: Markgraf, Daniel: Augmented Reality Definition, Gabler Wirtschaftslexikon, Wiesbaden 16. Februar 2018. Online: https://wirtschaftslexikon.gabler.de/definition/augmented-reality-53628/version-276701.

Marr 2015: Marr, Bernard: Why only one of the 5 Vs of Big Data really matters, IBM Big Data & Analytics Hub, 19. März 2015. Online: http://www.ibmbigdatahub.com/blog/why-only-one-5-vs-big-data-really-matters.

Martini et al. 2016: Martini, Mario; Nink, David & Wenzel, Michael: Bodycams zwischen Bodyguard und Big Brother, Neue Zeitschrift für Verwaltungsrecht – Extra, München 2016, Bd. 24, S. 1-18.

Mayer 2006: Mayer, Horst O: Interview und schriftliche Befragung: Entwicklung, Durchführung und Auswertung, Oldenbourg Verlag, München 2006.

McCarthy 2015: McCarthy, Nick: West Midlands Police facing 2,500 more job cuts in bid to save £130 million, Birmingham Mail, Birmingham 17. März 2015. Online: https://www.birminghammail.co.uk/news/midlands-news/west-midlands-police-facing-2500-8858756.

Meffert et al. 2012: Meffert, Heribert; Burmann, Christoph & Kirchgeorg, Manfred (Hrsg.): Grundlagen des Marketing, Springer Gabler, Wiesbaden 2012.

Mellouli 2014: Melloui, Sehl; Luna-Reyes, Luis F. & Zhang, Jing: Smart government, citizen participation and open data, Information Polity, 2014, 19, S. 1-4.

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

Mergel et al. 2013: Mergel, Ines; Müller, Peter; Parycek, Peter & Schulz, Sönke E.: Praxishandbuch Soziale Medien in der öffentlichen Verwaltung, Springer Verlag, Wiesbaden 2013.

Meuser & Nagel 2005: Meuser, Michael und Nagel, Ulrike: Experteninterviews - vielfach erprobt, wenig bedacht: Ein Beitrag zur qualitativen Methodendiskussion, in: Alexander Bogner, Beate Littig und Wolfgang Menz: Das Experteninterview: Theorie, Methode, Anwendung, VS Verlag für Sozialwissenschaften, Wiesbaden 2005, S. 71-93.

Möllers 2018: Möllers, Martin: Die Interaktion zwischen Mensch und Computer - Chancen und Nutzen für Bürgerinnen und Bürger, für Polizeibehörden und das Polizeiverwaltungsverfahren, in: Thomas-Gabriel Rüdiger und Petra Saskia Bayerl: Digitale Polizeiarbeit: Herausforderungen und Chancen, Springer Fachmedien, Wiesbaden 2018, S. 39-65.

Monroy 2017: Monroy, Matthias: Deutsche Polizeibehörden erhalten Direktzugriff auf Europol-Dateien, netzpolitik.org, Berlin 16. März 2017. Online: https://netzpolitik.org/2017/deutsche-polizeibehoerden-erhalten-direktzugriff-auf-europol-dateien/.

Monroy 2018: Monroy, Matthias: Warnen bis es quietscht: Offenbach auf dem Weg zur "umfassenden Polizei-App", netzpolitik.org, Berlin 12. Februar 2018. Online: https://netzpolitik.org/2018/warnen-bis-es-quietscht-offenbach-auf-dem-weg-zur-umfassenden-polizei-app/.

Moon et al. 2017: Moon, Hyungbin; Choi, Hyunhong; Lee, Jongsu & Lee, Ki Soo: Attitudes in Korea towards Introducing Smart Policing Technologies: Differences between the General Public and Police Officers, Sustainability, Seoul 2017, Bd. 9, S. 1-17.

Moser-Knierim 2014: Moser-Knierim, Antonie: Vorratsdatenspeicherung: Zwischen Überwachungsstaat und Terrorabwehr, Springer Vieweg, Wiesbaden 2014.

Mühlenmeier 2017: Mühlenmeier, Lennart: Chronik des Überwachungsstaats, netzpolitik.org, Berlin 20. September 2017.
Online: https://netzpolitik.org/2017/chronik-des-ueberwachungsstaates/.

Müller 2016: Müller, Marcel: Bodycam: Eine Erfolgsgeschichte nimmt ihren Lauf, in: Gewerkschaft der Polizei (Hrsg.): Deutsche Polizei, Berlin 2016, S. 9.

Münch 2017: Münch, Holger: Polizeiarbeit in digitalen Zeiten – Wie Ermittler und IT-Spezialisten gemeinsam Kriminalität bekämpfen, cebit.de, Hannover 2017. Online: https://www.bka.de/SharedDocs/Reden/DE/muenchGastbeitragCebit.html

Neuerer 2018: Neuerer, Dietmar: Wie Big Data für die Verbrechensbekämpfung von Nutzen sein kann, Handelsblatt, Düsseldorf 3. April 2018. Online: http://www.handelsblatt.com/politik/deutschland/minority-report-laesst-gruessen-wie-big-data-fuer-die-verbrechensbekaempfung-von-nutzen-sein-kann/21135740.html?ticket=ST-1090609-lYouh1oGvHqzvlwsfrpC-ap1.

Ohlberg et al. 2017: Ohlberg, Mareike; Ahmed, Shazeda & Lang, Bertram: The complex implementation of China´s Social Credit System, Mercator Institute for China Studies, Berlin 2017.

Palfrey & Urs 2008: Palfrey, John und Gasser, Urs: Generation Internet, Carl Hanser Verlag, München 2008.

Pekar-Milicevic 2016: Pekar-Milicevic, Mirjam: Polizeiliches Performance Management - Theorie, Implementierung und Wirkung, Springer VS, Wiesbaden 2016.

Petri 2012: Petri, Thomas: Sicherheitsbehördliche Datenschutzverarbeitung, in: Jan-Hinrik Schmidt und Thilo Weichert: Datenschutz: Grundlagen, Entwicklungen und Kontroversen, Bundeszentrale für politische Bildung, Bonn 2012, S. 115-129.

Plazek & Nürnberger 2017: Plazek, Michael und Nürnberger, Henrik: Big Data: Herausforderungen bei der Datenanalyse, Public Governance Herbst/Winter, Berlin 2017, S. 16-19.

Polizei Brandenburg 2016: Polizei-App - Service für unterwegs, Polizei Brandenburg, Potsdam 23. Januar 2016. Online: https://polizei.brandenburg.de/seite/polizeiapp.

Polizei NRW 2017: Pilotprojekt mit Tablets für NRW-Polizei gestartet, Polizei Nordrhein-Westfalen, Düsseldorf März 2017.
Online: https://polizei.nrw/artikel/pilotprojekt-mit-tablets-fuer-nrw-polizei-gestartet.

Prantl 2018: Prantl, Heribert: Bayern macht aus der Polizei eine Darf-fast-alles-Behörde, in: Süddeutsche Zeitung, München 14. Mai 2018, S. 4.

Prantl 2010: Prantl, Heribert: Der große Rüssel, in: Süddeutsche Zeitung, München 19. Mai 2010. Online: http://www.sueddeutsche.de/politik/vom-umbau-des-rechtsstaats-in-einen-praeventionsstaat-der-grosse-ruessel-1.884547.

Prognos 2016: Smart Government: Regieren und Verwalten in Deutschland im Jahr 2030, ProPress Verlagsgesellschaft mbH, Bonn 2016.

Rabenstein 2017: Rabenstein, Andreas: Polizei testet Gesichtserkennung an Berliner Bahnhof, Spiegel-Online, Hamburg 28. Juli 2017.
Online: http://www.spiegel.de/netzwelt/netzpolitik/gesichtserkennung-test-am-berliner-suedkreuz-beginnt-am-1-august-a-1160079.html.

Reuter et al. 2018: Reuter, Markus; Fanta, Alexander; Bröckling, Marie & Hammer, Luca: Influencer in Uniform: Wenn die Exekutive viral geht, netzpolitik.org, Berlin 5. März 2018. Online: https://netzpolitik.org/2018/wenn-die-exekutive-viral-geht-twitter-wird-zum-lieblings-werkzeug-der-deutschen-polizei/.

Roßnagel et al. 2013: Roßnagel, Alexander; Moser-Knierim, Antonie & Schweda, Sebastian: Interessensausgleich im Rahmen der Vorratsdatenspeicherung, Nomos Verlagsgesellschaft, Baden-Baden 2013.

Rotenberger 2018: Rotenberger, Julia: China verwehrt Bürgern mehr als 11 Millionen Flüge - wegen schlechten Benehmens, Handelsblatt, Düsseldorf 25. Mai 2018. Online: http://www.handelsblatt.com/politik/international/chinas-sozialpunktesystem-china-verwehrt-buergern-mehr-als-11-millionen-fluege-wegen-schlechten-benehmens-/22602814.html.

Rüdiger & Bayerl 2018: Rüdiger, Thomas-Gabriel und Bayerl, Petra-Saskia: Digitale Polizeiarbeit: Von Herausforderungen zu Chancen, Springer Fachmedien, Wiesbaden 2018, S. 11-19.

Schaar 2017: Schaar, Peter: Es hilft nicht mehr Überwachung, sondern mehr Intelligenz, in: Deutschlandfunk Kultur, Berlin 7. Oktober 2017.
Online: http://www.deutschlandfunkkultur.de/peter-schaar-ueber-terrorabwehr-es-hilft-nicht-mehr.1270.de.html?dram:article_id=397667.

Schnee & Unterberg 2016: Schnee, Philipp und Unterberg, Swantje: Privatisierung von Polizeiaufgaben - Ein Rückzug des Staates, in: Deutschlandfunk.de, Köln 14. Juli

2016. Online: http://www.deutschlandfunk.de/privatisierung-von-polizeiaufgaben-ein-rueckzug-des-staates.724.de.html?dram:article_id=360178.

Schnell 2018: Schnell, Lisa: Bedrohlich, in: Süddeutsche Zeitung, München 15. Mai 2018. Online: http://www.sueddeutsche.de/politik/polizeiaufgabengesetz-bedrohlich-1.3980429.

Schnell et al 2008: Schnell, Rainer; Hill, Paul B. & Esser, Elke: Methoden der empirischen Sozialforschung, Oldenbourg, München 2008, Bd. 8.

Schulzki-Haddouti 2017: Schulzki-Haddouti, Christiane: "Polizei 2020": Datenzugriff "jederzeit und überall", in: heise online, Hannover 14. Dezember 2017. Online: https://www.heise.de/newsticker/meldung/Polizei-2020-Datenzugriff-jederzeit-und-ueberall-3918494.html.

Schweiz E-Government 2011: Facts & Figures zum Stand der Strategieumsetzung 2011/II, Schweizerische Eidgenossenschaft und KdK, Bern 2011.

Schweizer Geschäftsstelle E-Government 2011: Erneuerung der Rahmenvereinbarung E-Government Schweiz; erläuternder Bericht, Bern 2011.

Seckelmann 2017: Seckelmann, Margrit: Body-Cams als New Tools of Governance, in: Jörn von Lucke und Klaus Lenk: Verwaltung, Informationstechnik & Management - Festschrift für Heinrich Reinermann zum 80. Geburtstag, edition Sigma in der Nomos Verlagsgesellschaft, Baden-Baden 2017, S. 291-303.

Siepermann 2018: Siepermann, Markus: Künstliche Intelligenz (KI), Gabler Wirtschaftslexikon, Wiesbaden 2018. Online: https://wirtschaftslexikon.gabler.de/definition/kuenstliche-intelligenz-ki-40285.

Siller 2017: Siller, Helmut: Stakeholder-Management, in: Jürgen Stierle, Dieter Wehe und Helmut Siller (Hrsg.): Handbuch Polizeimanagement, Springer Fachmedien, Wiesbaden 2017, S. 1019-1035.

Singelnstein 2018: Singelnstein, Tobias: Innere Unsicherheit, in: Süddeutsche Zeitung, München 13. April 2018. Online: http://www.sueddeutsche.de/politik/gastkommentar-innere-unsicherheit-1.3943397.

Sokol 2012: Sokol, Bettina: Grundrechte sichern!, in: Jan-Hinrik Schmidt und Thilo Weichert: Datenschutz: Grundlagen, Entwicklungen und Kontroversen, Bundeszentrale für politische Bildung, Bonn 2012, S. 137-145.

statista 2018a: Statista GmbH: Prognose zum Volumen der jährlich generierten digitalen Datenmenge weltweit in den Jahren 2016 und 2025, Statista GmbH, Hamburg 2018.
Online: https://de.statista.com/statistik/daten/studie/267974/umfrage/prognose-zum-weltweit-generierten-datenvolumen/.

statista 2018b: Statista GmbH: Prognose zur Anzahl der vernetzten Geräte im Internet der Dinge (IoT) weltweit in den Jahren 2016 bis 2020 (in Millionen Einheiten), Statista GmbH, Hamburg 2018.
Online: https://de.statista.com/statistik/daten/studie/537093/umfrage/anzahl-der-vernetzten-geraete-im-internet-der-dinge-iot-weltweit/.

statista 2018c: Statista GmbH: Anzahl der Polizisten in Deutschland nach Bundesländern im Jahr 2016, Statista GmbH, Hamburg 2018.
Online: https://de.statista.com/statistik/daten/studie/516101/umfrage/polizisten-in-deutschland-nach-bundeslaendern/.

statista 2018d: Statista GmbH: Fürchten Sie, dass es in nächster Zeit in Deutschand terroristische Anschläge geben wird oder fürchten Sie dies nicht?, Statista GmbH, Hamburg 2018.
Online: https://de.statista.com/statistik/daten/studie/493158/umfrage/umfrage-zur-angst-vor-terroranschlaegen-in-deutschland/.

Steinberg 2017; Steinberg, Guido: Islamistischer Terrorismus: Sechs Thesen auf dem Prüfstand, in: Internationale Politik, Mai/Juni 2017, Berlin 2017, S. 62-67.

Steiner et al. 2011: Steiner, Reto; Geser, Hans; Meuli, Urs; Ladner, Andreas & Horber-Papazian, Katia: Die Exekutivmitglieder in den Schweizer Gemeinden, Rüegger Verlag, Glarus 2011.

Steinke 2017: Steinke, Ronen: Wie die Polizei mit Bodycams Gewalt verhindern will, in: Süddeutsche Zeitung, München 14. April 2017.
Online: http://www.sueddeutsche.de/panorama/ueberwachung-wie-die-polizei-mit-bodycams-gewalt-verhindern-will-1.3460601.

Stierle & Lakner 2017: Stierle, Jürgen und Lakner, Sven: Employer Branding – Arbeitgebermarke Polizei, in: Jürgen Stierle, Dieter Wehe und Helmut Siller: Handbuch Polizeimanagement: Polizeipolitik - Polizeiwissenschaft - Polizeipraxis, Wiesbaden : Springer Fachmedien, 2017, S. 993-1019.

Stinauer 2018: Stinauer, Tim: Überwachte Stadt: Kölner werden mit mehr als 4000 Kameras fast dauerhaft gefilmt, Kölner Stadt Anzeiger, Köln 19. Mai 2018. Online:

https://www.ksta.de/koeln/ueberwachte-stadt-koelner-werden-mit-mehr-als-4000-kameras-fast-dauerhaft-gefilmt-30424870.

Stone 2017: Stone, Kelly E.: Smart Policing and the Use of Body Camera Technology: Unpacking South Africa´s Tenuous Commitment to Transparency, Policing: A Journal of Policy and Practice, Oktober 2017, Bd. 12, S. 109-115.

Strauß 2017: Strauß, Hagen: Die Politik und die aufgeheizte Sicherheitsdebatte: Wettbewerb der Hardliner, Westdeutsche Zeitung, Wuppertal 12. Juni 2017. Online: http://www.wz.de/home/leitartikel/die-politik-und-die-aufgeheizte-sicherheitsdebatte-wettbewerb-der-hardliner-1.2453926.

Stroud 2016: Stroud, Matt: The Company That´s Livestreaming Police Body Camera Footage Right Now, Motherboard - Vice Magazine, New York City 26. Juli 2016. Online: https://motherboard.vice.com/en_us/article/9a3ddv/visual-labs-police-body-camera-livestream.

Thiel 2011: Thiel, Markus: Die "Entgrenzung" der Gefahrenabwehr, Mohr Siebeck, Tübingen 2011.

Thurm 2018: Thurm, Frida: In Bayern droht bald überall Gefahr, in: Zeit Online, Hamburg 28. März 2018.
Online: http://www.zeit.de/gesellschaft/zeitgeschehen/2018-03/polizeigesetz-bayern-csu-sicherheit-ueberwachung-gewaltenteilung.

Tinnefeld et al. 2018: Tinnefeld, Marie Theres; Buchner, Benedikt; Petri, Thomas & Hof, Hans-Joachim: Einführung in das Datenschutzrecht - Datenschutz und Informationsfreiheit in europäischer Sicht, De Gruyter Oldenbourg, Berlin 2018.

Tönnemann 2018: Tönnemann, Curd: Landespolizei: Mit Drohnen auf Verbrecherjagd, Lübecker Nachrichten, Lübeck 11. Februar 2018. Online: http://www.ln-online.de/Nachrichten/Norddeutschland.

Truscheit 2017: Truscheit, Karin: "Leiser als Hubschrauber", faz.net, Frankfurt 20. November 2017. Online: http://www.faz.net/aktuell/gesellschaft/kriminalitaet/die-bayerische-polizei-will-kuenftig-mehr-drohnen-nutzen-15301940.html.

T-Systems 2018: Mobil einsatzfähig - interaktiver Funkstreifenwagen, Telekom Solutions for Public, Berlin 2018. Online: https://www.telekom-sfp.com/produkte-loesungen/einsatzmanagement/funkstreifenwagen/artikel-704908.

Van Dyck 2016: Van Dyck, Marc: Entwicklungsperspektive für die Digitale Agenda, TOGI Schriftenreihe Friedrichshafen, Band 15, epubli GmbH, Berlin 2016.

Vera & Jablonowski 2017: Vera, Antonio und Jablonowski, Lara: Organisationskultur der Polizei, in: Helmut Siller: Handbuch Polizeimanagement: Polizeipolitik – Polzeiwissenschaft – Polizeipraxis, Springer Fachmedien GmbH, Wiesbaden 2017, S. 475-495.

Voigt 2012: Voigt Rüdiger: Sicherheit versus Freiheit - Verteidigung der staatlichen Ordnung um jeden Preis?, Springer VS, Wiesbaden 2012.

Völlinger 2017: Völlinger, Veronika: Aber sicher doch, Zeit Online, Hamburg 16. September 2017. Online: http://www.zeit.de/politik/deutschland/2017-09/innere-sicherheit-terrorabwehr-geheimdienste-wahlprogramme.

von Lucke 2018: von Lucke, Jörn: Digitalisierung in der Kernverwaltung – Konzepte, in: Roland Heuermann, Matthias Tomenedal und Christian Bressem: Digitalisierung in Bund, Ländern und Gemeinden, Springer Gabler, Wiesbaden 2018.

von Lucke 2016a: von Lucke, Jörn: Smart Government, in TOGI | Schriftenreihe Friedrichshafen: Smart Government - Intelligent vernetztes Regierungs- und Verwaltungshandeln in Zeiten des Internets der Dinge und des Internets der Dienste, epubli GmbH, Berlin 2016, S. 19-69.

von Lucke 2016b: von Lucke, Jörn: Intelligent vernetztes Regierungs- und Verwaltungshandeln (Smart Government) im einsetzenden Zeitalter des Internets der Dinge und der Dienste, in Detlef Rätz: Digitale Transformation: Methoden, Kompetenzen und Technologien für die Verwaltung, Lecture Notes in Informatic (LNI), Gesellschaft für Informatik, Bonn 2016, S. 163-174.

von Lucke 2016c: 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, Baden-Baden 2016, S. 171-186.

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.

Wangemann 2016: Wangemann, Ulrich: Videoüberwachung hilft kaum bei Festnahmen, Märkische Allgemeine, Potsdam 3. November 2016. Online:

http://www.maz-online.de/Brandenburg/Videoueberwachung-hilft-kaum-bei-Festnahmen.

Ulrich 2018: Ulrich, Andreas: Warnung vor "Gotham", in: DER SPIEGEL 18/2018, Hamburg 2018, S. 25.

Welt 2017: Zahl der Polizisten erreicht neuen Höchststand, in: welt.de, Berlin 15. November 2017.
Online: https://www.welt.de/politik/deutschland/article170625072/Zahl-der-Polizisten-erreicht-neuen-Hoechststand.html.

West Midlands Police 2018: WMP 2020, west-midlands.police.uk, Birmingham 2018.
Online: https://www.west-midlands.police.uk/about-us/transformation-programme.

Wilkens 2017: Wilkens, Andreas: Polizeiroboter soll in Dubai Streife fahren, heise online, Hannover 30. Juni 2017.
Online: https://www.heise.de/newsticker/meldung/Polizeiroboter-soll-in-Dubai-Streife-fahren-3759813.html.

Wollny & Paul 2015: Wollny, Vollrad und Paul, Herbert: Die SWOT-Analyse: Herausforderung der Nutzung in den Sozialwissenschaften, in: Marlen Niederberger und Sandra Wassermann: Methoden der Experten- und Stakeholdereinbindung in der sozialwissenschaftlichen Forschung, 3. Auflage, Springer Verlag, Mainz 2015, S. 189-213.

Zander 2016: Zander, Jens: Body-Cams im Polizeieinsatz, Verlag für Polizeiwissenschaft, Frankfurt 2016.

ZEIT 2017: Bundestag ermöglicht mehr Videoüberwachung, Die ZEIT, Hamburg 10. März 2017. Online: https://www.zeit.de/politik/deutschland/2017-03/sicherheit-videoueberwachung-parlamentsbeschluss-bundestag-gewalttaten.