Big Data und künstliche Intelligenz – Chancen und Risiken für die Polizeiarbeit der Zukunft

von KK`in Dr. Julia Fricke[i], KPB Recklinghausen

Die Autorin erhielt im Februar 2019 auf dem europäischen Polizeikongress für ihre Arbeit den „Zukunftspreis Polizei".

Das Phänomen Big Data steht für die Extraktion von Wissen aus Daten. Es beschreibt die Verarbeitung großer heterogener Datenmengen – wie sie zunehmend auch im Polizeialltag anfallen – in hoher Geschwindigkeit. Die hierzu verwendeten Methoden der Künstlichen Intelligenz (KI) setzen dabei dort an, wo herkömmliche Werkzeuge der Datenverarbeitung an ihre Grenzen stoßen. Sie ermöglichen es, Daten in einem noch nie dagewesenen Umfang zu analysieren, Muster oder Zusammenhänge zwischen ihnen zu erkennen und letztlich Aussagen über die Vergangenheit, Gegenwart und insbesondere die Zukunft abzuleiten. Damit haben Big Data-Analysen ein hohes Wertschöpfungspotenzial – auch für die deutsche Polizei.

Big Data und Künstliche Intelligenz

Big Data und Künstliche Intelligenz (KI) sind Technologien mit einem breiten und stetig steigenden Spektrum möglicher Anwendungen in unserer Lebens- und Arbeitsweise. So werden sie bereits im medizinischen Bereich zur Prognose von Grippe-Pandemien oder zur Unterstützung in der Krebsdiagnostik eingesetzt. In der Wirtschaft können sie entscheidend zur Optimierung von Geschäftsprozessen beitragen (Business Intelligence) und in der Finanzbranche die Kreditwürdigkeit bemessen (Scoring).[ii] Besonders für die Sprach-, Text- und Bilderkennungsfähigkeiten von Maschinen mit KI ergeben sich erstaunliche Anwendungsmöglichkeiten. Als Beispiel seien hier digitale Assistenten wie Apple Siri und Amazon Alexa genannt. Diese können mit rasanter Geschwindigkeit lernen, Fragen des Menschen verstehen und beantworten sowie Aufgaben selbstständig erledigen. Ein weiteres Anwendungsbeispiel ist das autonome Fahren durch selbstfahrende Fahrzeuge, was in einigen Jahren den Straßenverkehr entscheidend verändern könnte.[iii]

Big Data

Big Data wird in der Gesellschaft sehr unterschiedlich verstanden. So existieren unzählige Definitionen für den Begriff Big Data.[iv] Jedoch handelt es sich bei Big Data nicht bloß um große Mengen von Daten. Der Begriff steht auch für die Sammlung, Nutzung und Analyse solcher Datenmassen. Ebenso schließt er die zur Datenverarbeitung notwendigen

Technologien und analytischen Werkzeuge ein.[v] In der fachwissenschaftlichen Literatur wird die Technologie daher mit den sogenannten „3 V“ charakterisiert. Diese Merkmale stehen für „Volume“ (Datenmenge, Umfang), „Variety“ (unstrukturierte Daten, Heterogenität der Daten) und „Velocity“ (hohe Geschwindigkeit der Datengenerierung und -verarbeitung).[vi] Zusammengefasst beschreibt Big Data also die Analyse und Verarbeitung von Datenmassen aus unterschiedlichen Quellen (Text-, Bild-, Video- und Audiodateien) in enorm hoher Geschwindigkeit - teilweise sogar in Echtzeit.

Da das bloße Sammeln und Speichern der Datenmengen noch keinen Mehrwert hat, müssen die Daten mittels geeigneter Methoden und Analysewerkzeuge nutzbar gemacht werden.[vii] Herkömmliche Methoden der Datenverarbeitung und standardisierte Instrumente stoßen dabei an ihre Grenzen. Die Grundlagen einer solchen analytischen Verarbeitung (Big Data Analytics, auch Advanced Analytics)[viii] bilden daher Algorithmen, entweder in Form von vordefinierten mathematisch-statistischen Modellen („Regeln“) oder selbstlernenden Systemen.[ix] Die hierzu verwendeten Methoden sind das Data-Mining (Daten-Bergbau) und Machine Learning (Maschinelles Lernen).[x] Beide Methoden sind wiederum KI-Komponenten. Für die Auswertung und Analyse von Big Data sind also (unter anderem) KI-Methoden von großer Bedeutung.[xi]

Künstliche Intelligenz (KI)

Der Begriff der KI wird häufig mit Robotern und Maschinen, die intellektuelle Aufgaben – teilweise sogar besser als der Mensch – ausführen können, assoziiert („starke KI“). Die derzeitigen Entwicklungen zielen jedoch weniger darauf ab, den Menschen zu ersetzten, als ihn bei der Bewältigung seiner Aufgaben zu unterstützen („schwache KI“).[xii] Solche KI-Systeme sind in der Lage, „menschenähnliche“ Verhaltensweisen zu zeigen.[xiii] Sie können Informationen wie Texte, Sprache und Bilder inhaltlich verstehen, interpretieren, bewerten und Hypothesen erstellen. Zudem können sie mit dem Anwender in natürlicher Sprache kommunizieren und in Abhängigkeit von seinem Verhalten bzw. Feedback „lernen“.[xiv] Das wohl bekannteste „kognitive“ System ist Watson, welches von dem Innovationsführer IBM entwickelt wurde. Watson ist in der Lage, Informationen in natürlicher Sprache zu verarbeiten und somit auch Fragen in natürlicher Sprache zu beantworten. So war es Watson im Jahr 2011 möglich, gegen zwei menschliche Champions in der Quizshow „Jeopardy“ zu gewinnen.[xv]

Big Data in der Polizeiarbeit

Die polizeilich zur Verfügung stehenden Daten sind ein Beispiel einer Datenmenge, welche zur Erkenntnisgewinnung ausgewertet werden kann (auch wenn es sich dabei streng genommen eher um „Small Data“ handelt). So werden in einigen Bundesländern bereits Daten aus Vorgangsbearbeitungs-, Fahndungs- und Auskunftssystemen sowie Lagebildern oder der Polizeilichen Kriminalstatistik verwendet, um Straftaten zu prognostizieren. Diese Vorgehensweise wird als Predictive Policing, die „vorausschauenden Polizeiarbeit“, bezeichnet.[xvi]

Grundsätzlich kann dabei in orts- und personenbezogenes Predictive Policing unterschieden werden. In Deutschland wird hauptsächlich das ortsbezogene Predictive Policing durchgeführt. Das primäre Ziel dabei ist es, in Datenmengen der Vergangenheit zunächst Muster zu erkennen, um darauf basierend Wahrscheinlichkeiten für das Auftreten von künftigen Straftaten möglichst exakt raum-zeitlich zu berechnen (derzeit insbesondere zur Vorhersage von Wahrscheinlichkeiten für das Delikt des Wohnungseinbruchdiebstahls).[xvii] Auch wenn sich die Länderpolizeien hierzu unterschiedlicher Software bedienen,[xviii] so sind die Grundlagen der Predictive Policing-Systeme identisch. Sie basieren im Kontext des Data-Mining auf mathematisch-statistischen Analysen, um Muster und Relationen abzuleiten und diese auf die Zukunft zu transferieren.[xix]

Hingegen gibt es im internationalen Raum bereits Bemühungen zum personenbezogenen Predictive Policing, durch welches unter anderem (kriminelle) Handlungen einzelner Personen prognostiziert werden sollen.[xx] Ein Beispiel ist das in England von der Durham Constabulary entwickelte KI-basierte System „Harm Assessment Risk Tool“ (HART). Mit Hilfe dieses Systems soll das Risiko prognostiziert werden, mit dem ein Täter innerhalb der nächsten zwei Jahre weitere Straftaten begehen wird. Damit soll das HART die Polizei bei der Entscheidung unterstützen, welche Täter einem Resozialisierungsprogramm zugeführt werden können.[xxi] Zu diesem Zweck wurde das HART so trainiert, dass es bestimmte Muster in der Rückfälligkeit erkennt. Die verwendeten (Lern-) Daten stammen aus unterschiedlichen Kategorien und umfassen unter anderem das Alter, das Geschlecht, die Postleitzahl des Wohnortes sowie die (kriminelle) Vergangenheit. Somit ist der Algorithmus in der Lage, das Risiko für eine Rückfälligkeit einzelner Individuen als gering, mittel oder hoch zu klassifizieren.[xxii] In Deutschland wird personenbezogenes Predictive Policing (bisher) jedoch nicht durchgeführt.

Big Data zur polizeilichen Gefahrenabwehr

Auch wenn das in Deutschland bisher durchgeführte ortsbezogene Predictive Policing aus taktischer Sicht ein wirkungsvolles Instrument ist, so ist es dennoch in gewisser Weise beschränkt. Verwertbare polizeiliche Datensätze (z.B. Tatzeiten, Tatorte, Beute und Modi

Operandi) sind begrenzt auf Daten der Vergangenheit und die zugrundeliegenden Algorithmen werden von bereits bekannten (Kriminalitäts-) Theorien[xxiii] abgeleitet.[xxiv]

Vor diesem Hintergrund ist die methodisch-technische Weiterentwicklung von Predictive Policing durch KI-Komponenten, also eine „intelligente polizeiliche Datenanalyse", sowie die Verknüpfung mit personenbezogenen Daten, ähnlich des HART, besonders interessant. Eine „intelligente polizeiliche Datenanalyse" würde es ermöglichen, eine weitaus größere Menge von Daten aus unterschiedlichen Quellen zeitnah zu verarbeiten und auszuwerten.[xxv] Denkbar wäre es, Daten zu Wetterbedingungen, Feier- und Ferientagen, Veranstaltungen und Großereignissen sowie zur Verkehrslage in die Systeme einzuspeisen.[xxvi] Auch könnten die Systeme durch die Nutzung von Open-Source-Intelligence (OSINT), also öffentlich zugänglicher Informationen, erweitert werden. Hierzu zählen vor allem Informationen aus den sozialen Medien wie Facebook, Twitter und Instagram. In diesen sind personenbezogene Daten wie Lichtbilder, Kontakte, Aufenthaltsorte, Urlaubsreisen sowie (politische) Einstellungen und Meinungen zu bestimmten Themen offen zugänglich (abhängig von den Allgemeinen Geschäftsbedingungen der Dienste).[xxvii]

Derartige Informationen lassen sich durch die bereits aus der kommunikationswissenschaftlichen Forschung bekannten Methoden der „Social Media Analytics" (SMA) auf die Tonalität und die Sinnstruktur von Texten (Text-Mining), die Struktur von sozialen Netzwerken (soziale Netzwerkanalyse) sowie die Entwicklung von Themen (Trend-analyse) automatisiert analysieren.[xxviii] In einer in England durchgeführten Studie zur Hasskriminalität wurden mittels Algorithmen zehntausende Twitter-Meldungen (Tweets) hinsichtlich ausländer- und fremdenfeindlicher Inhalte bzw. Hashtags analysiert, um zeitliche sowie räumliche Muster aufzudecken.[xxix] Die Studie verdeutlicht, dass Daten aus sozialen Medien einen detaillierten Einblick in die Gedanken und Vorhaben tausender Menschen liefern können. Durch die Kombination von OSINT und polizeilichen Daten in Big Data-Analysen ließen sich Verhaltensmuster erkennen und Hypothesen über künftige Straftaten ableiten.[xxx] Eine weitere Möglichkeit Anwendung wäre in diesem Zusammenhang die Identifizierung von gesellschaftlichen Trends im Hinblick auf neue Gefahrenlagen.[xxxi]

Nicht zuletzt aus datenschutzrechtlichen Gründen gibt es aber bisher kaum recherchier- und belastbare Studien oder Informationen zu möglichen Anwendungen solcher Innovationen in der Polizeiarbeit.[xxxii] Die Potenziale einer „intelligenten polizeilichen Datenanalyse" lassen sich jedoch erahnen, betrachtet man das Beispiel des US-amerikanischen Durham Police Department. Die Polizei setzte hier intelligente IBM-Analysesysteme[xxxiii] ein, um aus riesigen Datenmengen (polizeiliche Daten, Notrufe, Informationen zu Bandenmitgliedern und ihren Verbündeten, Strafakten zu Gewaltverbrechen) bisher verborgene Zusammenhänge zischen Straftaten aufzudecken und neue Einblicke in kriminelle Netzwerke zu gewinnen. So fand sie heraus, dass etwa 20 % aller Notrufe, die aufgrund von Schusswaffengebrauch getätigt

wurden, aus einem Gebiet stammten, welches nur 2 % der Gesamtfläche der Stadt ausmachte. Weitere Analysen zeigten zudem, dass in diesem Gebiet eine ebenso unverhältnismäßig hohe Anzahl an Gewaltverbrechen, Prostitution und Drogenkriminalität verzeichnet wurde. Diese Informationen konnten anschließend genutzt werden, um Kräfte gezielt in diesem Gebiet einzusetzen, entsprechende Polizeimaßnahmen durchzuführen und Kriminalitätsraten zu senken.[xxxiv] Dieses Beispiel verdeutlicht, dass mittels Big Data-Analysen auch bisher unbekannte „Kriminalitätsmuster" und unbekannte Zusammenhänge (z.B. zwischen verschiedenen Deliktsbereichen) aufgedeckt werden können, um letztlich neue polizeilich relevante Erkenntnisse zu gewinnen.

Big Data zur polizeilichen Strafverfolgung

Neben dem präventiven Einsatz können Big Data-Analysen auch wesentliche Vorteile für die kriminalpolizeiliche Ermittlungsarbeit haben. Mit der Generierung immer größerer Datenmengen und den fortschreitenden technischen Entwicklungen wie dem Internet der Dinge wird der Umfang zu analysierender und als Beweismittel zu sichernder Daten in den kommenden Jahren stetig zunehmen. Während früher hauptsächlich strukturierte Daten aus Datenbanken untersucht werden mussten, muss heute häufig eine unüberschaubare Menge von unstrukturierten Daten zeitnah ausgewertet werden. So sehen sich die Ermittler nicht selten mit dem Problem konfrontiert, unzählige Fotos, Videos, Telefongespräche, Textinhalte aus WhatsApp-, Facebook- und Twitter-Nachrichten oder E-Mails zeitnah auswerten zu müssen.[xxxv] Jedoch ist die manuelle Analyse sehr zeitaufwendig und nicht immer zielführend. Erschwerend kommt in einigen Fällen hinzu, dass auch fremdsprachige Daten eine Rolle spielen. Eine Aussage zum Inhalt von Text- oder Audiodateien und damit zur Ermittlungsrelevanz kann hier ohne Übersetzer nicht getroffen werden.[xxxvi] Allein für das Auffinden ermittlungsrelevanter Information ist somit bereits ein enormer Zeitaufwand erforderlich, bevor die Informationen tatsächlich ausgewertet werden können.[xxxvii] Dies stellt die Ermittlerinnen und Ermittler oft vor große Herausforderungen. Die Entwicklung und der Einsatz moderner polizeilicher Analyse- und Ermittlungsmethoden im Zeitalter von Big Data scheinen daher dringend geboten.[xxxviii]

In dieser Hinsicht bieten Big Data-Analysen mittels KI Möglichkeiten, die polizeiliche Ermittlungsführung zu unterstützen. Dies ist insbesondere auf drei Funktionalitäten zurückzuführen: Durch das **schnelle Filtern großer Datenmengen** wäre es möglich, die anfallenden Datenmenge automatisiert und zeitnah auf ermittlungsrelevante Inhalte zu reduzieren. Das **Text- und Sprachverständnis** intelligenter Systeme ermöglicht es, umfassende inhaltliche Zusammenhänge in Dokumenten oder Textpassagen zu finden. Weiterhin könnte die Sprachintelligenz kognitiver Systeme auch im Bereich der

Telekommunikationsüberwachung (TKÜ) genutzt werden, um für die Fallbearbeitung relevante Gesprächsinhalte aus Telefongesprächen herauszufiltern und bei Bedarf zeitgleich aus einer fremden Sprache zu übersetzen. Durch die **Bildverarbeitung** können beispielsweise Gesichter identifiziert und in hoher Geschwindigkeit mit polizeilichen Datenbanken abgeglichen werden. Ein weiteres mögliches Anwendungsfeld ist die gezielte Bildersuche. Intelligente Systeme könnten die Suche in einer großen und ungeordneten Menge von Bildern erheblich beschleunigen, wie zum Beispiel die Suche nach kinderpornographischem Material auf diversen Servern und Datenträgern.[xxxix] Zusammengefasst könnte ein intelligentes System wie zum Beispiel Watson auf Bilder, Videosequenzen oder Textpassagen hinweisen, in welchen sich für die Ermittlungsarbeit relevante Inhalte finden lassen könnten. Zudem wäre es möglich, dass Ermittler/-innen im Dialog gezielt bei Watson "nachfragen", um bei Bedarf eine detaillierte oder weiterführende Antwort auf ihre Fragen zu erhalten.[xl]

Aufgrund der oben dargestellten Multifunktionalität kognitiver Systeme ist auch ihr potenzielles Anwendungsspektrum in Ermittlungsverfahren breit. Grundsätzlich ist ihr Einsatz dort besonders zielführend, wo sich enorme Datenmassen der individuellen Betrachtung durch Ermittler/-innen entziehen oder unstrukturierte Daten diese vor große Herausforderungen stellen.[xli] Insbesondere bei Ermittlungen im Bereich der Cyber- und Organisierten Kriminalität sind personal- und zeitintensive Recherchearbeiten ein zentrales Problem. Diesem könnten durch die automatisierte Reduktion auszuwertender Massendaten auf ermittlungsrelevante Informationen im Rahmen einer „Big Data-Voranalyse“ entgegengewirkt werden.

Hinzu kommt die Tatsache, dass durch den technologischen Fortschritt immer neue Tatmittel und Angriffsflächen für Straftäter entstehen. So werden auch Kriminelle (wahrscheinlich) in Zukunft KI-Methoden als hochwertiges Tatmittel nutzen.[xlii] Dies trifft zum Beispiel auf die Verkehrsunfallaufnahme zu. Fahrzeuge sind längst rollende Computer. Damit könnte theoretisch online auf die Fahrzeugbetriebssysteme zugegriffen werden, um einen Unfall zu provozieren. Gleiches gilt für medizinische Geräte, welche durch Sabotage funktionsunfähig gemacht werden könnten. Damit sind in Zukunft digitale verübte Tötungsdelikte und Anschläge denkbar. Ähnlich gilt dies für das Internet der Dinge, wodurch Wohnungen, Kühlschränke, Fernseher, aber eben auch Türschlösser digital steuerbar sein werden. Die Gefahr des Missbrauchs ist umso höher, je mehr Daten digital werden. Dies stellt neue Herausforderungen an die Ermittler-/innen, die derartige Modi Operandi zum einen erstmal erkennen und zum anderen die digitalen Spuren bzw. Daten anschließend sichern und auswerten müssten.[xliii]

Strategische Ausrichtung der Polizei

Darüber hinaus könnte sich eine intelligente Datenauswertung und -nutzung im Kontext von Big Data auch positiv auf die strategische Ausrichtung der Polizei auswirken. So könnten beispielsweise personelle Ressourcen zur Lageanalyse geschont werden.[xliv] Zudem könnten durch die Möglichkeit, inhaltliche Zusammenhänge in Datenmassen zu erkennen, wesentlich umfassendere Lagebilder für die Gefahrenabwehr bzw. valide Kriminalitätslagebilder erstellt werden.[xlv] Auch wäre es denkbar, dass durch die Identifizierung gesellschaftlicher Trends der Entwicklung von (neuen) Kriminalitätsphänomenen frühzeitig im Hinblick auf die Personal- und Einsatzmittelplanung begegnet werden kann.[xlvi]

Risiken

Neben ihren unbestreitbaren Anwendungsmöglichkeiten ist der polizeiliche Einsatz intelligenter Systeme jedoch auch mit Risiken verbunden. So besteht bei der Verarbeitung von insbesondere personenbezogenen Daten die Gefahr der Diskriminierung bestimmter Personengruppen durch die sogenannte „algorithmische Voreingenommenheit“ (engl. Algorithmic Bias). Ursächlich für solche Bias können neben technischen Defiziten, was in falsch positiven und negativen Ergebnissen resultieren kann, auch fehlerhafte Algorithmen sein. Insbesondere bei dem Verfahren des Maschinellen Lernens müssen die Algorithmen zunächst anhand von Lerndaten trainiert werden. Dabei hängen die Gesetzmäßigkeiten, welche der Algorithmus während der Trainingsphase lernt, von der Zusammensetzung der Lerndaten ab.[xlvii] Dies bedeutet, dass Systeme unweigerlich die Bias reproduzieren werden, welche bereits durch die Lerndaten präsentiert waren. Haben sich also beispielsweise polizeiliche Maßnahmen unverhältnismäßig oft gegen bestimmte Minderheiten gerichtet, so wird auch der Algorithmus für diese Personen ein unverhältnismäßig hohes Risiko der Straftatenbegehung prognostizieren. In der Folge würde sich die Polizei wiederum verstärkt auf diese Minderheiten konzentrieren, sodass letztlich eine Feedbackschleife im Sinne einer selbsterfüllenden Prophezeiung des Systems entsteht.[xlviii] In den USA führte dies beispielsweise zur Rassendiskriminierung, indem ein Algorithmus systematisch dunkelhäutige Personen benachteiligte.[xlix]

Weitere Kritikpunkte sind sicherlich eine mangelnde Transparenz der Systeme und eine schwierige Nachvollziehbarkeit der von ihnen getroffenen Entscheidungen und Bewertungen (Stichwort „Black Box“). Damit steigt auch das Risiko, dass die von den Systemen produzierten Ergebnisse nicht nicht die Denkweise der Polizei widerspiegeln.[l]

Eine weitere Herausforderung ist die zentrale Verwaltung von Daten. Grundsätzlich gilt, dass diese Technologien ihr Potenzial nur entfalten können, wenn die zu analysierende Datenmenge einen großen Umfang hat.[li] Damit ist unter anderem eine zentrale Daten-verwaltung mindestens auf bundesweiter Ebene essentiell. Dieser Anforderung wird das bisherige polizeiliche Informationsmanagement jedoch nicht gerecht, denn oft sind

vorhandene Datenbanken nicht über Ländergrenzen hinweg verfügbar. Eine einheitliche vom Bundeskriminalamt zentral verwaltete Informationsarchitektur soll nun mit dem Programm „Polizei 2020“[lii] geschaffen werden.[liii] Damit wird auch der Weg zur erfolgreichen Durchführung von Big Data-Analysen in der Polizeiarbeit geebnet.

Datenschutzrechtliche Zulässigkeit

Eine zentrale Problemstellung ergibt sich insbesondere im Hinblick auf die datenschutzrechtliche Zulässigkeit der Analysen. Durch die Möglichkeit, personenbezogene Daten in einem noch nie dagewesenen Umfang zu verarbeiten, bergen Big Data-Analysen hohe Risiken für die informationelle Selbstbestimmung (Art. 2 I i.V.m. 1 I GG). Sie widersprechen daher den Zielen des Datenschutzes.

Für die Verarbeitung personenbezogener Daten durch die Polizei ist die Datenschutzrichtlinie[liv] von hoher Relevanz. Diese ist neben der Datenschutz-Grundverordnung[lv] (EU-DSGVO) Teil des EU-Datenschutzpakets 2018 und wird in Teil 3 der Neufassung des Bundesdatenschutzgesetzes (vgl. Datenschutz-Anpassungs- und Umsetzungsgesetzes EU, DSAnpUG-EU[lvi])[lvii]sowie im Fachrecht umgesetzt.[lviii]

Personenbezug der Daten?

Big Data-Analysen können grundsätzlich mit anonymen oder personenbezogenen Daten durchgeführt werden.[lix] Der grundlegende Ansatzpunkt für die Anwendung datenschutzrechtlicher Bestimmungen ist daher ein (möglicher) Personenbezug der Daten.[lx] Somit unterfallen polizeiliche Big Data-Analysen den datenschutz-rechtlichen Vorschriften nur, wenn personenbezogene Daten in die Systeme eingespeist werden. Werden ausschließlich anonyme Daten verarbeitet, so sind die datenschutzrechtlichen Bestimmungen nicht anzuwenden.[lxi] Polizeiliche Big Data-Analysen mit ausschließlich nicht-personenbezogenen Daten sollten daher datenschutzrechtlich unbedenklich und weitgehend zulässig sein.[lxii] Denkbare Einsatzbereiche ohne Personenbezug sind zum Beispiel strategische Auswertungen, die auf der Grundlage der vorhandenen (polizeilichen) Daten abstrakte Lagebilder zur Entwicklung von Kriminalitätsphänomenen erstellen.[lxiii] Auch dem ortsbezogenen Predictive Policing stehen datenschutzrechtliche Bedenken zunächst nicht entgegen.[lxiv] Werden im Rahmen von Weiterentwicklungen des Systems jedoch zunehmend mehr Daten in die Analyse miteinbezogen, beispielsweise durch die Nutzung von OSINT, lässt sich ein (möglicher) Personenbezug nicht gänzlich ausschließen.[lxv]

Auch durch die „Anonymisierung“, d.h. durch das Entfernen personenbezogener Daten aus dem Datensatz,[lxvi] kann ein Personenbezug nicht gänzlich ausgeschlossen werden. So besteht stets die Gefahr einer „Re-Identifizierung“, also der Aufhebung oder Vereitelung von Anonymität.[lxvii] Durch die Möglichkeit, vorhandene Datensätze zu erweitern und mit neuen

Daten zu verknüpfen, besteht stets das Risiko, dass sich ein Personenbezug – selbst wenn dieser zu Beginn aufgrund der Verwendung von ausschließlich anonymen bzw. anonymisierten Daten ausgeschlossen wurde – im Zuge der Big Data-Analyse herstellen lässt. Werden vorhandene Daten während der Speicherdauer mit neuen Daten verknüpft, könnten hierdurch ausreichend viele Merkmale zusammengeführt werden, um eine Person zu (re-) identifizieren.[lxviii] Da dies im Voraus nicht immer eindeutig abschätzbar ist, sollte im Zweifel ein möglicher Personenbezug angenommen und die datenschutzrechtlichen Vorschriften beachtet werden. In einigen Publikationen wird eine Anonymität im Rahmen von Big Data-Analysen daher gänzlich in Frage gestellt.[lxix]

Datenschutzrechtlicher Grundsatz der Zweckbindung

Ein grundlegender Konfliktpunkt besteht darin, dass Big Data-Analysen den Fokus auf das Verarbeiten einer möglichst großen Datenmenge legen, während die Datenschutzrichtlinie die Datenverarbeitung auf ein Minimum reduzieren will. Die Datenschutzrichtlinie formuliert in Art. 4 allgemeine Grundsätze der Datenverarbeitung. Den Kern der allgemeinen Datenschutzgrundsätze bildet der Zweckbindungsgrundsatz. Er steht mit weiteren datenschutzrechtlichen Grundsätzen wie der Datenminimierung und der Speicherbegrenzung in einem engen Zusammenhang. Nach dem Zweckbindungsgrundsatz dürfen personenbezogene Daten nur für einen vorher festgelegten, eindeutigen und rechtmäßigen Zweck erhoben (Zweckfestlegung) und nicht in einer mit diesem Zweck nicht zu vereinbaren Weise verarbeitet werden (Zweckbindung).[lxx] Das Ziel von Big Data-Analysen ist es jedoch, möglichst große Datenmengen zu verarbeiten, um zum einen gesuchte, zum anderen aber insbesondere neue und unbekannte Erkenntnisse zu gewinnen. Es geht also darum, möglichst viele Daten zu oft auch unbekannten Zwecken zu erheben, zu analysieren, zu speichern und mit Daten der Zukunft zu verknüpfen. Es handelt sich um explorative Vorgehensweisen ohne zuvor festgelegte Ziele bzw. Zwecke.[lxxi] Damit stehen die von der JI-RL vorgeschriebenen datenschutzrechtlichen Grundprinzipien zweckoffenen polizeilichen Big Data-Analysen unter Verwendung personenbezogener Daten grundsätzlich entgegen. Eine Datenerhebung auf „Vorrat“ für unbestimmte Zwecke, um diese im weiteren Verlauf immer wieder frei miteinander kombinieren zu können, ist mit dem Zweckbindungsgrundsatz der Datenschutzrichtlinie nicht zu vereinbaren.[lxxii] Die Angabe eines verallgemeinerten Endzwecks wird dieser datenschutzrechtlichen Forderung ebenso wenig gerecht wie ein Verarbeitungs-zweck, der sich erst aus dem Ergebnis der Datenanalyse ergibt. Das Endergebnis der Auswertung muss hingegen nicht konkretisiert werden, da sich dieses erst im Zuge der Analyse ergibt.[lxxiii]

Aber auch wenn ein rechtmäßiger Zweck eindeutig festgelegt ist, so ist dieser bei im Nachhinein erfolgenden Verarbeitungen grundsätzlich einzuhalten. Folglich würde durch das

Zusammenführen und Verknüpfen von für konkrete Zwecke erhobenen Daten die jeweilige Zweckfestlegung missachtet und der datenschutzrechtliche Grundsatz verletzt werden.[lxxiv]
Der von der Richtlinie vorgeschriebene datenschutzrechtliche Zweckbindungsgrundsatz steht also zweckoffenen polizeilichen Big Data-Analysen unter Verwendung personenbezogener Daten grundsätzlich entgegen. Durch die Zweckbindung werden die vielfältigen Verknüpfungsmöglichkeiten der Daten im Rahmen der Analysen ausgeschlossen oder zumindest stark begrenzt.
Jedoch wird eine Zweckänderung zur Weiterverarbeitung im Nachhinein datenschutzrechtlich nicht gänzlich ausgeschlossen. So ist gemäß Art. 4 II d eine Zweckänderung legitimiert, wenn sie unter anderem durch spezifische Ermächtigungen im Fachrecht explizit geregelt werden.[lxxv] Auch können durch die Verarbeitung personenbezogener Daten mehrere Zwecke zugleich verfolgt werden. Somit ist es möglich, zu Beginn der Analyse nicht nur aktuelle Zwecke, sondern eben auch solche, die in naher Zukunft angestrebt werden, festzulegen.[lxxvi] Als problematisch könnte es sich in diesem Fall jedoch erweisen, den Zweck i.S.d. Zweckbindungsgrundsatzes im Vorfeld ausreichend konkretisieren zu können. Fraglich ist in diesem Zusammenhang auch, ob die Verarbeitung von Daten „als Beweismittel“ (z.B. §§ 94, 98 StPO) im Rahmen kriminalpolizeilicher Big Data-Analysen dem Grundsatz der Zweckbindung genügen würde.[lxxvii]
Um die datenschutzrechtliche Zulässigkeit von Big Data-Analysen in der Polizeiarbeit eingehender beurteilen zu können, ist in weiteren Untersuchungen eine umfassende Prüfung der konkreten Forderungen des Zweckbindungsgrundsatzes unerlässlich. In diesem Zusammenhang ergeben sich auch die Erfordernisse, (eingriffs-) rechtliche Rahmenbedingungen zu prüfen bzw. zu schaffen. Vor allem die polizeilichen Ermächtigungen im Strafprozessrecht und Polizeirecht der Länder sind mit Blick auf die Datenschutzrichtlinie zu überprüfen und gegebenenfalls an diese anzupassen.

Ebenfalls sind technische (z.B. Datenverfügbarkeit, zentrale Verwaltung von Daten) und finanzielle Aspekte (z.B. Anschaffungskosten, Lizenzgebühren) sowie personelle Fragen (z.B. Fortbildungen, Involvierung von Spezialisten, Outsourcing) zu klären, um den Wert von Big Data-Analysen für die Polizeiarbeit der Zukunft abschließend beurteilen zu können. Mit Blick auf die stetig wachsenden Mengen von anfallenden Daten bieten sie in jedem Fall der Polizei die Chance, ihre bisherige Vorgehensweise zu verbessern und sich insbesondere zukunftsorientiert auszurichten. Weitere Anwendungspotenziale lassen sich erahnen, denkt man an eine Verknüpfung des Predictive Policing mit der intelligenten Videoüberwachung des öffentlichen Raumes. Jedoch sollen Big Data-Analysen traditionelle Polizeiarbeit nicht ersetzen, sondern vielmehr als kreative und effektive Hilfsmittel dienen.

Literatur

Angwin, J., Larson, J., Mattu, S., Kirchner, L. (2016). Machine Bias. There´s software used across the country to predict future criminals. And it´s biased against blacks. *ProPublica*. URL: https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing (Stand: 04.05.2018)

Babuta, A. (2017). Big Data and policing. An assessment of law enforcement requirements, expectations and priorities. London: Royal United Services Institute for Defence and Security Studies.

Baraniuk, C. (2017). Durham Police AI to help with custody decisions. BBC News. URL: http://www.bbc.com/news/technology-39857645 (Stand: 25.04.2018)

Bitkom (Hrsg.) (2017). Entscheidungsunterstützung mit Künstlicher Intelligenz. Wirtschaftliche Bedeutung, gesellschaftliche Herausforderungen, menschliche Verantwortung. Berlin. URL: https://www.uni-kassel.de/fb07/fileadmin/datas /fb07/5-Institute/IWR/Hornung/170901-KI-Gipfelpapier-online.pdf (Stand: 19.04.2018)

Breuer, S. (2016). Smarter Policing – eine vollständige End-to-End Lösung für die öffentliche Sicherheit. *Polizei Praxis.* URL: https://www.polizeipraxis.de/ausgaben/2016/detailansicht-2016/artikel/smarter-policing.html (Stand: 02.05.2018)

Bundesministerium der Innern (Hrsg.) (2018). Polizei 2020. White Paper. URL: https://www.bmi.bund.de/SharedDocs/downloads/DE/veroeffentlichungen/2018/polizei-2020-white-paper.pdf?__blob=publicationFile&v=1 (Stand: 21.05. 2018)

Burgess, M. (2018). UK police are using AI to inform custodial decisions – but it could be discriminating against the poor. Wired. URL: http://www.wired.co.uk/article/police-ai-uk-durham-hart-checkpoint-algorithm-edit (Stand: 25.04.2018)

Conrad, S.C. (2017). Künstliche Intelligenz – Die Risiken für den Datenschutz. *DUD – Datenschutz und Sicherheit.* 41 (12). S. 740-744.

Demos (2016). Hate Speech after Brexit. London: Center for Analysis of Social Media. URL: https://www.demos.co.uk/project/hate-speech-after-brexit/ (Stand: 19.05.2018)

Dix, A. (2016). Datenschutz im Zeitalter von Big Data. Wie steht es um den Schutz der Privatsphäre? *Stadtforschung und Statistik.* 29 (1). S. 59-64.

Dorschel, W. & Dorschel, J. (2015). Einführung. In: Dorschel, J. (Hrsg.). *Praxishandbuch Big Data. Wirtschaft – Recht – Technik*. Wiebaden: Springer Gabler. S. 1-13.

Dutcher, J. (2014). What is Big Data? Berkeley: School of Information. URL: https://data-science.berkeley.edu/what-is-big-data/ (Stand: 17.04.2018)

Eberl, U. (2018). Was ist Künstliche Intelligenz – Was kann sie leisten? *Aus Politik und Zeitgeschichte.* 68. S. 8-14.

Eberl, U. (2016). Wo künstliche Intelligenz den Menschen schon übertrifft. Zeit Online. URL: http://www.zeit.de/digital/internet/2016-10/deep-learning-ki-besser-als-menschen (Stand: 19.04.2018)

Egbert, S. (2017). Siegeszug der Algorithmen? Predictive Policing im deutschsprachigen Raum. *Aus Politik und Zeitgeschichte*. 67. S. 17-23.

Epple, G., Dudenhausen, I., Kahr, R., Ludewig, F. (2017). Mehr Sicherheit durch gezielte Internetaufklärung in Leitstellen. Das Forschungsprojekt SENTINEL der Deutschen Hochschule der Polizei (DHPOL). *Kriminalistik*. 71 (12). S. 734-739.

Gentsch, P. (2018). Künstliche Intelligenz für Sales, Marketing und Service. Mit AI und Bots zu einem Algorithmic Businee – Konzepte, Technologien und Best Practices. Wiesbaden: Sprenger Gabler.

Gluba, A. (2016). Mehr offene Fragen als Antworten. Was für eine Bewertung des Nutzens von Predictive Policing noch zu klären ist. *Die Polizei*. 107 (2). S. 53-57.

Gluba, A. (2014). Predictive Policing – eine Bestandsaufnahme. Historie, theoretische Grundlagen, Anwendungsgebiete und Wirkung. *Kriminalistik*. 68 (6). S. 347-352.

Groff, E.R., La Vigne, N.G. (2002). Forecasting the Future of Predictive Crime Mapping. In: Tilly, N. (Ed.). *Analysis for Crime Prevention*. Monsey, N.Y., Willian Publishing Devon, U.K.: Criminal Justice Press. P. 29-57.

Haar, T. (2017). Big Data: Neue Datenschutz-Grundverordnung ändert einiges. Neue Spielregeln. *iX – Magazin für professionelle Informationstechnik*. 2017 (11). S. 80-82.

Hardyns, W., Rummens, A. (2017). Predictive Policing as a new tool for law enforcement? Recent developments and challenges. *European Journal on Criminal Policy and Research*. P. 1-18.

Heitmüller, U. (2017). Predictive Policing: Die deutsche Polizei zwischen Cyber-CSI und Minority Report. Heise online. URL: https://www.heise.de/news-ticker/meldung/Predictive-Policing-Die-deutsche-Polizei-zwischen-Cyber-CSI-und-Minority-Report-3685873.html (Stand: 25.04.2018)

Hornung, G., Herfurth, C. (2018). Datenschutz bei Big Data – Rechtliche und politische Implikationen. In: König, C., Schröder, J., Wiegand, E. (Hrsg.). *Big Data. Chancen, Risiken, Entwicklungstendenzen*. Wiesbaden: Springer VS. S. 149-183.

International Business Machines Corporation, IBM (Hrsg.) (2017). Durham Police Department. Cuts violent crime by 39 percent using insight into patterns of criminal

activity. Armonk, NY. URL: https://public.dhe.ibm.com/common/ssi/ecm/gp/en/gpc12346usen/global-markets-government---public-safety-and-security-gp-case-study-gpc12346usen-20170823.pdf (Stand: 28.02.2018)

Jaeger, R.R. (2017). Künstliche Intelligenz – Hilfsmittel oder Konkurrenz für die Polizei. Predictive Policing, Biometrische Identifikation und Polizeidrohnen – mit künstlicher Intelligenz (KI) auf Verbrecherjagd! *Der Kriminalist*. 2017 (3). S. 8-15.

Johannes, P.C., Weinhold, R. (2018). Das neue Datenschutzrecht bei Polizei und Justiz. Europäisches Datenschutzrecht und deutsche Datenschutzgesetze. Baden-Baden: Nomos.

Kessler, K., Lenzen, T. (2015). Big Data: Großes Potential durch semantische Datenanalyse des BKA. Polizei Praxis. URL: https://www.polizeipraxis.de/themen/forensik/detailansicht-forensik/artikel/big-data-grosses-potential-durch-semantische-datenanalyse-des-bka.html (Stand: 02.05.2018)

King, S. (2014). Big Data. Potential und Barrieren der Nutzung im Unternehmenskontext. Wiesbaden: Springer VS.

Körffer, B. (2014). Auswertung personenbezogener Daten für Strafverfolgung und Gefahrenabwehr – genügen die gesetzlichen Grundlagen zum Schutz des Rechts auf informelle Selbstbestimmung? 37 (4). *Datenschutz Nachrichten*. S. 146-150

Kranawetter, M. (2017). Öffentliche Sicherheit im Zeitalter der vernetzen Maschinen – Risiken und Potenziale für die Polizei. Langfassung. *Polizei im Umbruch – Herausforderungen und Zukunftsstrategien*. Ingelheim am Rhein: BKA Herbsttagung, 15.-16. November 2017. URL: https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/Herbsttagungen/2017/herbsttagung2017KranawetterLangfassung.pdf (Stand: 05.05.2018)

Kring, M. (2014). Big Data und der Grundsatz der Zweckbindung. In: Plödereder, E., Grunske, L., Schneider, E., Ull, D. (Hrsg.). *Informatik 2014.* Bonn: Gesellschaft für Informatik e.V.. S. 551-562.

Kudyba, S., Kwatinetz, M. (2014). Introduction to the Big Data Era. In: Kudyba, S. (Ed.). *Big Data, mining, and analytics. Components of strategic decision making*. Boca Raton, FL et al.: CRC Press. P. 1-15.

Lanquillon, C., Mallow, H. (2015). Advanced Analytics mit Big Data. In: Dorschel, J. (Hrsg). *Praxishandbuch Big Data. Wirtschaft – Recht – Technik*. Wiesbaden: Springer Gabler. S. 55-89.

Marnau, N. (2016). Anonymisierung, Pseudonymisierung und Transparenz für Big Data. *Datenschutz und Datensicherheit – DuD*. 40 (7). S. 428-433.

Martini, M. (2014). Big Data als Herausforderung für den Persönlichkeitsschutz und das Datenschutzrecht. *Deutsches Verwaltungsblatt – DVBl*. 23. S. 1481-1489

Mayer-Schönberger, V. (2015). Big Data – Eine Revolution, die unser Leben verändern wird. *Bundesgesundheitsplatt – Gesundheitsforschung – Gesundheitsschutz*. 58 (8). S. 788-793.

Mnich, M. (2018). Big Data algorithms beyond machine learning. *KI – Künstliche Intelligenz*. 32 (1). P. 9-17.

Münch, H. (2017). Polizeiliche Herausforderungen und Zukunftsstrategien aus Sicht des Bundeskriminalamtes. Langfassung. *Polizei im Umbruch – Herausforderungen und Zukunftsstrategien*. Ingelheim am Rhein: BKA Herbsttagung, 15.-16. November 2017. URL: https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/Herbsttagungen/2017/ herbsttagung2017MuenchLangfassung.html (Stand: 07.05. 2018)

Rolfes, M. (2017). Predictive Policing: Beobachtungen und Reflexionen zur Einführung und Etablierung einer vorhersagenden Polizeiarbeit. In: Fachgruppe Geoinformatik des Instituts für Geographie der Universität Potsdam (Hrsg.). *Geoinformation & Visualisierung: Pionier und Wegbereiter eines neuen Verständnisses von Kartographie und Geoinformatik.* Potsdam: Universitätsverlag Potsdam. S. 51-76.

Roßnagel, A., Geminn, C., Jandt, S., Richter, P. (2016). Datenschutzrecht 2016. „Smart" genug für die Zukunft? Ubiquitous Computing und Big Data als Herausforderungen des Datenschutzes. Kassel: ITeG Wissenschaftliches Zentrum für Informationstechnik-Gestaltung.

Roßnagel, A. (2013). Big Data – Small Privacy? Konzeptionelle Herausforderungen für das Datenschutzrecht. *Zeitschrift für Datenschutz – ZD*. S. 562-567.

Sarunski, M. (2016). Big Data – Ende der Anonymität? *Datenschutz und Datensicherheit – DuD*. 40 (7). S. 424-427.

Schaar, P. (2013). Zwischen Big Data und Big Brother – zehn Jahre als Bundesbeauftragter für den Datenschutz und die Informationsfreiheit. Recht der Datenverarbeitung – RDV. S. 223-227

Schefzig, J. (2014). Big Data = Personal Data? Der Personenbezug von Daten bei Big Data-Analysen. *Kommunikation und Recht – K&R*. 2014 (12). S. 772-777.

Schroeck, M., Schockley, R., Smart, J., Romero-Morales, D., Tufano, P. (2012). Analytics: Big Data in der Praxis. Wie innovative Unternehmen ihre Datenbestände effektiv

nutzen. Ehningen u.a.. URL: https://www935.ibm.com/services/de/gbs/thoughtleadership/GBE03519-DEDE-00.pdf (Stand: 18.4.2018)

Schürmann, D. (2015). „SKALA“ Predictive Policing als praxisorientiertes Projekt der Polizei NRW. Düsseldorf: Ministerium des Innern des Landes NRW. URL: https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/ForumKI/ForumKI2015/kiforum2015SchuermannPositionspapier.pdf;jsessionid=FEB6B8E046212E320FACA88635EA702B.live0612?%20(Stand:%2024.04.2018) (Stand: 24.4.2018)

Schulz, A. (2017). Künstliche Intelligenz – Hilfsmittel oder Konkurrenz für die Polizei. *Der Kriminalist*. 2017 (3). S. 16-18.

Schweer, T. (2015). „Vor dem Täter am Tatort“. Musterbasierte Tatortvorhersagen am Beispiel des Wohnungseinbruches. *Die Kriminalpolizei*. 2015 (1). S. 13-16.

Schwichtenberg, S. (2016). Die “kleine Schwester” der DSGVO: Die Richtlinie zur Datenverarbeitung bei Polizei und Justiz. *DUD – Datenschutz und Sicherheit.* 40 (9). S. 605-609.

Sommerer, L. (2017). Geospatial Predictive Policing – Research outlook & a call for legal debate. *NK – Neue Kriminalpolitik*. 29 (2). P. 147-164

Stahlhut, A. (2017). Automatisierte Datenreduzierung auf beweisrelevante Inhalte – Ergänzende Analyse mit KNIME. *Der Kriminalist*. 2017 (10). S. 26-31.

Stark, J. (2017). Künstliche Intelligenz – Chancen und Herausforderungen von kognitiven Systemen im polizeilichen Umfeld. *Der Kriminalist*. 2017 (3). S. 4-7.

Steglitz, S., Linh, D.-X., Bruns, A., Neuberger, C. (2014). Social Media Analytics. Ein interdisziplinärer Ansatz und seine Implikationen für die Wirtschaftsinformatik. *Wirtschaftsinformatik.* 56 (2). S. 101-109.

Steinebach, M., Winter, C., Halvani, O., Schäfer, M., Yannikos, Y. (2015). Chancen durch Big Data und die Frage des Privatsphärenschutzes. Begleitpapier Bürgerdialog. Stuttgart: Fraunhofer Verlag.

van Brakel, R.-E. (2016). Pre-emptive Big Data surveillance and its (dis)empowering consequences: the case of Predictive Policing. In: van der Sloot, B., Broeders, D., Schrijvers, E. (Ed.). *Exploring the boundaries of Bid Data*. Amsterdam: University Press. P. 117-141.

Wroblewski, S. (2015). Wir brauchen digitales Denken für Ermittler und Einsatzkräfte. Interview mit dem Landeskriminaldirektor Dieter Schürmann. *Streife, Sonderausgabe Cybercrime*. 2015 (09). S. 18-19.

Wulff, J. (2017). Artificial intelligence and law enforcement. InfoSec Reading Room. SANS Institute. URL: https://www.sans.org/reading-room/whitepapers/threatintelligence/artificial-intelligence-law-enforcement-37925 (Stand: 20.05.2018)

[i] Die Autorin hat nach dem Studium der Biowissenschaften (B.Sc.) und Biotechnologie (M.Sc.) im Bereich der Naturwissenschaften promoviert. Zur Zeit ist sie als Kriminalkommissarin bei der KPB Recklinghausen.

[ii] Steinebach, Winter, Halvani, Schäfer, Yannikos, 2015, S. 8, 11 ff.

[iii] Eberl, 2018, S. 8; Conrad, 2017, S. 740 f.; Eberl, 2016

[iv] Für eine Liste von über 40 Definitionen s. Dutcher, 2014

[v] Hornung & Herfurth, 2018, S. 150 f.; Mayer-Schönberger, 2015, S. 14; Roßnagel, 2013, S. 562; Martini, 2014, S. 1482

[vi] Gentsch, 2018, S. 9 f.; Mnich, 2018, P. 9-15; Dorschel & Dorschel, 2015, S. 6 ff.; Steinebach, Winter, Halvani, Schäfer, Yannikos, 2015, S. 21; King, 2014, S. 35; Kring, 2014, S. 552; Kudyba & Kwatinetz, 2014, P. 2 ff.; Schroeck, Shockley, Smart, Romero-Morales, Tufano, 2012, S. 3 ff.

[vii] Weiterhin sind Technologien zur Datenhaltung (z.B. In-Memory-Technologien und NoSQL-Datenbanken) und zum verteilten Rechnen (Aufteilung der Rechenlast auf mehrere Rechner) erforderlich. (Steinebach, Winter, Halvani, Schäfer, Yannikos, 2015, S. 21)

[viii] Lanquillon & Mallow, 2015, S. 55 ff.

[ix] Gentsch, 2018, S. 13

[x] Lanquillon & Mallow, 2015, S. 55, S. 62 f.; Steinebach, Winter, Halvani, Schäfer, Yannikos, 2015, S. 23

[xi] Gentsch, 2018, S. 10, 34, 37

[xii] Gentsch, 2018, S. 29; Bitkom, 2017, S. 29

[xiii] Bitkom, 2017, S. 28 f.

[xiv] Stark, 2017, S. 5

[xv] Steinebach, Winter, Halvani, Schäfer, Yannikos, 2015, S. 12

[xvi] Hardyns & Rummens, 2017, P. 1; Gluba, 2016, S. 53

[xvii] Egbert, 2017, S. 17; Gluba, 2016, S. 53; Schweer, 2015, S. 13; Gluba, 2014, S. 349

[xviii] In Bayern und Baden-Württemberg setzt die Polizei die kommerzielle Prognosesoftware „Pre Crime Observation System“ (PRECOBS) ein. Hiervon unabhängig entwickelte das LKA in NRW eigenständig das Programm „System zur Kriminalitätsauswertung und Lageantizipation“ (SKALA), das LKA in Berlin das Programm „KrimPro“, das LKA in Niedersachsen das System „PreMAP“ und das LKA in Hessen die Software „Kriminalitätslagebild (KLB) -operativ“. (Egbert, 2017, S. 17; Heitmüller, 2017)

[xix] Egbert, 2017, S. 20; Schürmann, 2015, S. 3

[xx] Egbert, 2017, S. 19; Sommerer, 2017, P. 149 f.

[xxi] Burgess, 2018

[xxii] Babuta, 2017, P. 23; Baraniuk, 2017

[xxiii] Zu Kriminalitätstheorien im Kontext von Predictive Policing s. Schweer 2015, S. 13; Gluba, 2014, S. 348

[xxiv] Egbert, 2017, S. 20; Schweer, 2015, S. 13-16; Gluba, 2014, S. 347 f.; Groff & La Vigne, 2002, P. 36

[xxv] Rolfes, 2017, S. 57

[xxvi] Breuer, 2016

[xxvii] Epple, Dudenhausen, Kahr, Ludewig, 2017, S. 734 ff.

[xxviii] Für weiterführende Informationen vgl. Steglitz, Linh, Bruns, Neuberger, 2014

[xxix] Demos, 2016

[xxx] Babuta, 2017, P. 27; Wulff, 2017, P. 1

[xxxi] Kranawetter, 2017, S. 5

[xxxii] Rolfes, 2017, S. 57; Schulz, 2017, S. 18

[xxxiii] Die detaillierte technische Funktionsweise der Systeme wurde nicht veröffentlicht.

[xxxiv] IBM, 2017, S. 1 f.

[xxxv] Stahlhut, 2017, S. 26, 29; Wroblewski, 2015, S. 59 f.

[xxxvi] Kessler & Lenzen, 2015

[xxxvii] IBM, 2017, S.3

[xxxviii] Stahlhut, 2017, S. 26

[xxxix] Kranawetter, 2017, S. 3, 5

[xl] Stark, 2017, S. 5

[xli] Stahlhut, 2017, S. 29
[xlii] Kranawetter, 2017, S. 2, 8; Münch, 2017, S. 3
[xliii] Wroblewski, 2015, S. 18 f.

[xliv] Egbert, 2017, S. 17

[xlv] Kranawetter, 2017, S. 5

[xlvi] Breuer, 2016

[xlvii] van Brakel, 2016, P. 8
[xlviii] Babuta, 2017, P. 24
[xlix] Angwin, Larson, Mattu, Kirchner, 2016
[l] Stark, 2017, S. 5 f.

[li] Babuta, 2017, P. 24

[lii] Bundesministerium des Innern, 2018

[liii] Jaeger, 2017, S. 11; Münch, 2017, S. 2-6
[liv] Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27.04.2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zweck der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum fairen Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates, EU ABl. L 119 vom 04.05.2016, S. 89; im Folgenden Datenschutzrichtlinie

[lv] Verordnung (EU) 2016/679 des europäischen Parlaments und des Rates vom 27.04.2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum fairen Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG, EU ABl. L 119 vom 04.05.2019, S. 1
[lvi] Gesetz zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680, BGBl, Teil 1, Nr. 44 vom 05.07.2017, S. 2097
[lvii] Johannes & Weinhold, 2018, § 1, Rn. 59
[lviii] Johannes & Weinhold, 2018, § 1, Rn. 55, 385 ff.
[lix] Roßnagel, Geminn, Jandt, Richter, 2016, S. 46

[lx] Haar, 2017, S. 80; Hornung & Herfurth, 2018, S. 156: Dix, 2016, S. 60

[lxi] Erwägungsgrund 21 Datenschutzrichtlinie

[lxii] Roßnagel, Geminn, Jandt, Richter, 2016, S. 25, 125

[lxiii] Körffer, 2014, S. 147

[lxiv] Babuta, 2017, S. 23; Gluba, 2016, S. 56

[lxv] Dix, 2016, S. 63

[lxvi] Hornung & Herfurth, 2018; Schefzig, 2017; Dix, 2016; Marnau, 2016; Martini, 2014

[lxvii] Haar, 2017, S. 81; Schefzig, 2017, S. 776 f; Dix, 2016, S. 61; Roßnagel, Geminn, Jandt, Richter, 2016, S. 85 f.

[lxviii] Marnau, 2016, S. 429; Roßnagel, 2013, S. 563, 566

[lxix] Hornung & Herfurth, 2018, S. 165; Sarunski 2016, S.424

[lxx] Johannes & Weinhold, 2018, § 1, Rn. 129
[lxxi] Hornung & Herfurth, 2018, S. 146, 167

[lxxii] Roßnagel, Geminn, Jandt, Richter, 2016, S. 122 f.

[lxxiii] Kring, 2014, S. 555 ff.

[lxxiv] Kring, 2014, S. 557; Roßnagel, 2013, S. 565; Schaar, 2013, S. 225

[lxxv] Johannes & Weinhold, 2018, § 1, Rn. 150 ff.

[lxxvi] Hornung & Herfurth, 2018, S. 169

[lxxvii] Schwichtenberg, 2016, S. 606