Deutsche Hochschule
der Polizei
Universität der Polizeien
des Bundes und der Länder

Künstliche Intelligenz als Chance und Herausforderung für die Polizeiarbeit

Herausgegeben von Wilfried Honekamp

Band
30

Schriftenreihe
der Deutschen Hochschule der Polizei

Schriftenreihe
der Deutschen Hochschule der Polizei
neue Folge

Band 30

hrsg. vom Kuratorium der Deutschen Hochschule der Polizei

Deutsche Hochschule
der Polizei
Universität der Polizeien
des Bundes und der Länder

Künstliche Intelligenz als Chance und Herausforderung für die Polizeiarbeit

Herausgegeben von Wilfried Honekamp

Münster, 2026

Bibliografische Information der Deutschen Nationalbibliothek

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

Alle Rechte, auch die des Nachdrucks von Auszügen, der fotomechanischen Wiedergabe und der Übersetzung vorbehalten.

Fachbeirat:

Kriminaldirektor im Hochschuldienst Joachim Faßbender
Prof. Dr. Thomas Görgen
Prof. Dr. Stefan Jarolimek
Prof. Dr. Anja Schiemann
Prof. Dr. Dr. Antonio Vera

© Deutsche Hochschule der Polizei – Hochschulverlag
Zum Roten Berge 18–24
48165 Münster
ISBN 978-3-945856-32-1
ISSN 1865-0430

Inhaltsverzeichnis

7 **Möglichkeiten der Künstlichen Intelligenz zur Unterstützung der Polizeiarbeit aufzeigen**
Wilfried Honekamp

23 **Nutzung von KI zur automatisierten Lagedarstellung in komplexen polizeilichen Sofortlagen. Eine Untersuchung potenzieller Stärken, Schwächen, Chancen und Risiken**
Alexander Huber

36 **Künstliche Intelligenz: Betrachtung des Einsatzes von Multi-Agenten-Systemen in der öffentlichen Verwaltung**
Bastian Blum

50 **Einsatz von KI in der polizeilichen Sachbearbeitung – Effizienz und Grenzen**
André Müller

60 **Verantwortungsvolle KI: Eine ethische Betrachtung des Projekts FRANKA**
Jana Piorr

71 **KI-gestützte Videoanalyse: Ethische Bewertung automatisierter Verhaltens- und Bewegungserkennungssysteme in der niedersächsischen Landespolizei**
Marcel Janzik

86 **„AI-Snitching“: Ethische Spannungsfelder zwischen Schutz und Übergriff**
Maximilian Achmüller

98 **Konzeptionelle Bewertung der Datenanalysesoftware VeRA**
Robert Falk

115 **Die Polizei zwischen Automatisierung und Humanisierung: Auswirkungen der Künstlichen Intelligenz auf Mitarbeitende und Implikationen für die Organisation**
Sebastian Herrmann

127 **Leaving Experts - Bleibendes Wissen: Eine Untersuchung der Potenziale von KI zur Bewahrung von Wissen im öffentlichen Dienst am Beispiel der Polizei NRW**
Robin Strecker

140 **Predictive Policing im digitalen Raum: Eine SWOT-Analyse des Einsatzes Künstlicher Intelligenz zur Verhütung von Cyberkriminalität**
Enrico Schubert

153 **Der Einsatz von Diffusionsmodellen zur Erzeugung von Wahllichtbildvorlagen**
Sirko Trodler

166 **KI-gestützte Assistenzsysteme in der Todesermittlung: Potenziale und Grenzen bei der Ersteinschätzung von Todesumständen an Leichenfundorten**
Sabrina Wickert

Inhaltsverzeichnis

177 **Vorbereitung von Nachwuchskräften der Polizei auf technische, rechtliche und ethische Herausforderungen der Künstlichen Intelligenz**
Tobias Keller

189 **Nutzung von generativer Künstlicher Intelligenz als Large Language Model im Rahmen der polizeilichen Cold-Case-Sachbearbeitung**
Alexander Herdt

Möglichkeiten der Künstlichen Intelligenz zur Unterstützung der Polizeiarbeit aufzeigen

Wilfried Honekamp

Digitale Informationsverarbeitung hat in den vergangenen Jahren eine Qualität erreicht, die staatliches Handeln strukturell verändert. Datenbasierte Analyseverfahren und lernfähige Systeme durchdringen zunehmend operative und administrative Entscheidungsprozesse. In diesem Transformationsprozess gewinnt die Entwicklung und Anwendung Künstlicher Intelligenz (KI) eine besondere Bedeutung. Für die Polizeiarbeit entsteht daraus eine doppelte Herausforderung. Datengetriebene Verfahren eröffnen neue Möglichkeiten der Gefahrenprognose, der Ermittlungsunterstützung und der Ressourcensteuerung. Zugleich verschieben sie die Bedingungen polizeilicher Wissensproduktion und werfen grundlegende Fragen nach Rechtsstaatlichkeit, Transparenz, Verantwortungszuschreibung und organisationaler Einbettung auf (Honekamp et al. 2025).

Dieses Buch enthält Beiträge von Studierenden des Masterstudiengangs Öffentliche Verwaltung – Polizeimanagement, die im Rahmen des Moduls Künstliche Intelligenz im polizeilichen Umfeld entstanden sind und die Spannungsfelder aus unterschiedlichen disziplinären Perspektiven analysieren. Es nimmt technologische Entwicklungen ebenso in den Blick wie ihre rechtlichen, ethischen und organisationalen Implikationen und verfolgt das Ziel, die Bedingungen einer verantwortbaren Integration entsprechender Systeme in die Polizeiarbeit systematisch zu klären. Polizeiorganisationen sind wissensintensive Institutionen, deren Handlungsfähigkeit wesentlich von der Erhebung und Bewertung von Lageinformationen abhängt. Seit sich algorithmische Analyseverfahren etabliert haben, verändert sich diese Wissensproduktion grundlegend. An die Stelle primär erfahrungsbasierter, fallorientierter Routinen treten statistisch modellierte Verfahren, die große und heterogene Datenbestände automatisiert auswerten und in strukturierte Entscheidungsgrundlagen überführen (Europol 2024; Janssen et al. 2020).

Diese Systeme fungieren nicht lediglich als technische Assistenz. Sie verändern, welche Informationen sichtbar werden und wie Unsicherheit in Entscheidungen eingeht (Honekamp 2025; Bommasani et al. 2021). Dadurch verschiebt sich das Gewinnen polizeilicher Erkenntnisse von individueller Erfahrungsverdichtung hin zu formalisierten, modellbasierten Wissensformen. Wissensproduktion wird stärker datenanalytisch vermittelt und zunehmend durch probabilistische Logiken strukturiert (Jansen 2018). Besonders deutlich wird diese Entwicklung im Bereich vorausschauender Polizeiarbeit. Predictive-Policing-Ansätze nutzen historische Falldaten, um räumlich-zeitliche Risikomuster zu modellieren und Einsatzentscheidungen zu steuern. Diese Systeme beeinflussen die Allokation von Ressourcen und fokussieren die operative Aufmerksamkeit (Egbert 2024). Zugleich verdeutlichen kritische Analysen, dass algorithmische Prognosen von Datenqualität, Modellannahmen und institutionellen Selektionspraktiken abhängen. Rückkopplungseffekte können bestehende Kontrollmuster stabilisieren oder verstärken (Europol 2024; Richardson et al. 2019; O'Neil 2017). Datenbasierte Prognoseinstrumente wirken somit konstitutiv an der Definition polizeilicher Problemlagen mit.

Die wissenschaftliche Relevanz dieser Entwicklung liegt in einer doppelten Verschiebung. Zum einen verändert sich das institutionelle Selbstverständnis der Polizei, indem reaktive Gefahrenabwehr zunehmend durch proaktive, modellgestützte Steuerungslogiken ergänzt wird. Zum anderen entwickeln sich neue Formen wissensbezogener Abhängigkeit. Entscheidungsprozesse beziehen sich verstärkt auf algorithmisch generierte Risikobewertungen, deren interne Modelllogik für Anwenderinnen und Anwender häufig nur begrenzt zugänglich ist. Solche Systeme können kognitive Orientierungen strukturieren und professionelle Urteilsbildung rahmen, ohne formale Entscheidungsverantwortung zu übernehmen (Vydra & Klievink 2019; Janßen 2018; O'Neil 2017). Die Integration datengetriebener Systeme ist daher nicht vorrangig als bloße Steigerung operativer Effizienz zu verstehen. Sie verändert, welche Informationen innerhalb der Polizei als entscheidungsrelevant gelten und wie daraus Handlungsprioritäten entstehen. Damit verschieben sich Kriterien der Relevanz, Formen der Evidenz sowie die Prozesse, durch die Informationen zu entscheidungsrelevantem Wissen verdichtet werden. Die Bedingungen, unter denen Relevanz erzeugt, Risiken definiert und Handlungsprioritäten gesetzt werden, verändern sich (Honekamp et al. 2025; Vydra & Klievink 2019). Diese tiefgreifende Veränderung der Art und Weise, wie Wissen innerhalb der Polizei generiert und genutzt wird, bildet den analytischen Ausgangspunkt der folgenden Betrachtung. Im Fokus stehen dabei die rechtlichen Grenzen algorithmischer Entscheidungsunterstützung, Fragen ihrer normativen Rechtfertigung, ihre Einbindung in organisationale Strukturen sowie ihre regulatorische Ausgestaltung im europäischen Kontext.

Je stärker algorithmische Systeme polizeiliche Entscheidungsprozesse strukturieren, desto deutlicher stellt sich die Frage nach ihrer rechtlichen Einhegung (Kunze 2025; Honekamp 2025). Rechtsstaatlichkeit fungiert dabei als konstitutiver Rahmen staatlicher Machtausübung. Die Verlagerung der Wissensproduktion hin zu datenanalytisch vermittelten Entscheidungsgrundlagen ist daher zwingend an die dogmatischen Maßstäbe des öffentlichen Rechts rückzubinden. Mit der KI-Verordnung (EU KI-VO) hat die Europäische Union einen einheitlichen, risikobasierten Rechtsrahmen für den Einsatz von KI geschaffen, der ausdrücklich auch sicherheitsbehördliche Anwendungen erfasst (Pfeffer 2025). Die EU KI-VO klassifiziert KI-Systeme nach ihrem Gefährdungspotenzial und knüpft daran abgestufte Anforderungen. Für Hochrisiko-Systeme, zu denen zahlreiche Anwendungen im Bereich Strafverfolgung zählen können, normiert sie Pflichten zur Datenqualität, technischen Robustheit, Dokumentation, menschlichen Aufsicht und Konformitätsbewertung. Der Einsatz algorithmischer Systeme wird damit an nachweisbare Organisations- und Prüfstrukturen gebunden. Entscheidend ist, dass diese Anforderungen sowohl technische Qualitätskriterien als auch rechtliche Voraussetzungen für die Zulässigkeit des Einsatzes darstellen (Kraft 2025; Europol 2024; Janßen 2018). Die EU KI-VO wirkt jedoch nicht isoliert. Polizeiliche Datenverarbeitung unterliegt weiterhin dem Zusammenspiel mit der Datenschutz-Grundverordnung sowie der JI-Richtlinie (EU 2016/680) für die Verarbeitung personenbezogener Daten durch Strafverfolgungsbehörden. Dieses Normengefüge konkretisiert zentrale rechtsstaatliche Leitprinzipien, insbesondere Gesetzmäßigkeit, Zweckbindung, Datenminimierung und Rechenschaftspflicht. Im Mittelpunkt steht der Grundsatz der Verhältnismäßigkeit. Jede algorithmisch unterstützte Maßnahme muss geeignet, erforderlich und angemessen sein. Bei probabilistischen Prognosesystemen stellt sich damit die dogmatisch anspruchsvolle Frage,

wie Wahrscheinlichkeitsaussagen in eine Gefahren- oder Verdachtsbegründung einzuordnen sind und ob sie die Schwelle für grundrechtsrelevante Eingriffe tragen können (Kunze 2025; NIST 2023; O'Neil 2017).

Ein weiterer Kernpunkt betrifft die gerichtliche Prüfbarkeit. Eingeschränkte Nachvollziehbarkeit algorithmischer Entscheidungslogiken kann die effektive gerichtliche Überprüfung staatlichen Handelns erschweren. Der Anspruch auf effektiven Rechtsschutz setzt voraus, dass eine Entscheidung in tatsächlicher und rechtlicher Hinsicht überprüfbar ist (Weber 2025; Erdogan 2024; Pavlidis 2024). Nachvollziehbarkeit ist in diesem Sinne technische Transparenzanforderung und prozessuale Voraussetzung richterlicher Kontrolle. Konzepte wie Erklärbare KI (engl. Explainable AI) erhalten damit eine juristische Funktion: Sie soll sichtbar machen, auf welcher Grundlage eine Behörde gehandelt hat und wer für diese Grundlage einstehen muss (Kunze 2025; Pavlidis 2024; Europol 2024). Fragen nach möglichen Ausnahmen und Öffnungsklauseln im Sicherheitsbereich verdeutlichen zudem ein strukturelles Spannungsfeld. Einerseits ist der Staat verpflichtet, effektive Gefahrenabwehr und Strafverfolgung sicherzustellen. Andererseits ist er in besonderer Weise an die Grundrechte gebunden (Erdogan 2024). Die Charta der Grundrechte der Europäischen Union setzt hierfür verbindliche Maßstäbe, insbesondere im Hinblick auf Nichtdiskriminierung, Datenschutz und effektiven Rechtsschutz. Die rechtliche Bewertung algorithmischer Polizeisysteme bewegt sich daher stets im Spannungsfeld zwischen Sicherheitsauftrag und Grundrechtsbindung (Europäisches Parlament 2021). Rechtliche Einhegungen sind auch für die institutionelle Legitimität relevant (Guler et al. 2025). Die EU KI-VO und das Datenschutzrecht definieren Verfahrensanforderungen und begrenzen die Bedingungen, unter denen algorithmisch strukturierte Entscheidungen überhaupt zulässig sind. Die epistemische Transformation polizeilicher Wissensproduktion ist somit untrennbar mit der Frage verbunden, ob und unter welchen Voraussetzungen sie rechtsstaatlich gerechtfertigt werden kann.

Die Einführung von KI in der Polizeiarbeit berührt nicht nur Fragen rechtlicher Zulässigkeit, sondern grundlegende Probleme normativer Legitimität staatlichen Handelns (Honekamp et al. 2025). Während das Recht verbindliche Mindestanforderungen formuliert und die Grenzen zulässiger Machtausübung bestimmt, richtet die ethische Analyse den Blick auf die weitergehende Frage, unter welchen Bedingungen algorithmische Entscheidungsunterstützung als gerechtfertigt und gesellschaftlich verantwortbar gelten kann. Ethik fungiert insofern als eigenständige Reflexionsebene, die Bewertungsmaßstäbe für den Umgang mit Unsicherheit und struktureller Ungleichheit bereitstellt (Floridi et al. 2018). Im polizeilichen Kontext gewinnt diese Differenz besondere Bedeutung. Werden algorithmische Systeme in Prognose-, Klassifikations- oder Priorisierungsprozesse integriert, verändert sich die Form der Entscheidungsbegründung. An die Stelle individueller professioneller Einschätzung treten statistisch modellierte Wahrscheinlichkeitsannahmen. Die ethische Fragestellung zielt hier sowohl auf die formale Zulässigkeit solcher Modelle als auch auf ihre normative Angemessenheit. Es stellt sich die grundlegende normative Frage, ob und in welchem Umfang Freiheitsbeschränkungen oder priorisierende Ressourcenzuweisungen auf statistische Wahrscheinlichkeitsannahmen gestützt werden dürfen, die auf historischen Datenbeständen und modellierten Korrelationen beruhen. Damit berührt algorithmische Entscheidungsstützung den Kern rechtsstaatlicher Individualisierung staatlichen Handelns.

Internationale Leitlinien zur vertrauenswürdigen KI benennen Prinzipien wie Fairness, Schadensvermeidung, Verantwortlichkeit und Achtung der Autonomie als normative Orientierungspunkte (NIST 2023; Floridi et al. 2018; Europäische Kommission 2019). Ihre analytische Tragfähigkeit entfalten diese Prinzipien jedoch erst im konkreten Anwendungskontext. Algorithmische Systeme können bestehende Selektionslogiken in polizeilichen Datensätzen reproduzieren und unter bestimmten Bedingungen verstärken. Modelle implementieren historische Ungleichheiten und institutionelle Routinen in ihre Struktur (Kunze 2025; Kemme 2025; Richardson et al. 2019). Aufgrund der möglichen verheerenden Auswirkungen des Einsatzes solcher Modelle bezeichnet O'Neil (2017, S. 12) diese als „Weapons of Math Destruction". Die ethische Bewertung hat daher ausdrücklich zu prüfen, ob KI-Anwendungen bestehende Selektions- und Kontrollmuster institutionell verfestigen, marginalisierte Gruppen systematisch stärker exponieren oder verzerrte Datenlagen in scheinbar objektive Risikoprognosen transformieren. In diesem Fall würde algorithmische Rationalisierung nicht Neutralität erzeugen, sondern strukturelle Ungleichheit technisch reproduzieren (Richardson et al. 2019). Eine differenzierte ethische Analyse erfordert zudem eine mehrdimensionale Betrachtung. Auf individueller Ebene stehen Fragen nach Privatheit, Autonomie und prozeduraler Fairness im Vordergrund. Auf organisationaler Ebene betrifft die ethische Reflexion die Gefahr einer schleichenden Verschiebung professioneller Verantwortung hin zu technisch generierten Entscheidungsvorschlägen. Auf gesellschaftlicher Ebene stellt sich die Frage, welche Auswirkungen algorithmische Polizeisysteme auf Machtverhältnisse, soziale Kontrolle und demokratische Deliberationsprozesse haben (Singelnstein 2025). Akzeptanz ist eng mit wahrgenommener Gerechtigkeit und institutioneller Vertrauenswürdigkeit verbunden (Weber 2025; Guler et al. 2025). Legitimität ergibt sich aus dem Zusammenwirken von rechtlicher Zulässigkeit, ethischer Rechtfertigung und gesellschaftlicher Akzeptanz. Für die Polizei bedeutet dies, dass der Einsatz algorithmischer Systeme vor Gericht Bestand hat sowie gegenüber der Öffentlichkeit nachvollziehbar erklärt und institutionell verantwortet werden kann (Kunze 2025; Döring 2025).

Im Diskurs um Verantwortungsvolle KI (engl. Responsible AI) hat sich darüber hinaus die Einsicht etabliert, dass ethische Anforderungen nicht lediglich retrospektiv durch Evaluation adressiert werden können. Vielmehr sind sie als strukturierende Leitlinien in Entwicklungs-, Beschaffungs- und Implementierungsprozesse zu integrieren (Schiemann 2025; NIST 2023). Für die Polizeiarbeit folgt daraus, dass ethische Anforderungen in verbindliche Entscheidungs- und Kontrollprozesse zu überführen sind. Prinzipien wie Fairness oder Transparenz gewinnen erst dann normative Substanz, wenn sie in prüfbare Kriterien, dokumentierte Abwägungen und klar zugewiesene Verantwortlichkeiten übersetzt werden. Die Frage lautet nicht nur, ob ein System rechtmäßig ist, sondern ob sein Einsatz mit den normativen Selbstbindungen einer demokratischen Sicherheitsarchitektur vereinbar ist (Floridi et al. 2018; Europäische Kommission 2019). Damit wird die rechtliche Prüfung erweitert. Entscheidend ist, ob die Nutzung eines KI-Systems im konkreten polizeilichen Kontext verantwortet werden kann. Damit wird die normative Grundlage für die nachfolgende Betrachtung von Organisationsstrukturen und Implementierungen geschaffen, in denen diese Anforderungen praktisch eingelöst werden müssen.

Rechtliche und ethische Anforderungen entfalten nur dann praktische Wirkung, wenn sie in organisationsinterne Strukturen übersetzt und dauerhaft stabilisiert werden (Hoheisel-Gruler 2025; Coors 2025). Die Einführung von KI in Polizeiorganisationen ist daher als

Transformationsprozess institutioneller Ordnungen zu begreifen. Neben der technischen Implementierung einzelner Systeme gilt das Augenmerk auch der Reorganisation von Entscheidungswegen, Zuständigkeiten und internen Kontrollbeziehungen innerhalb komplexer Behördenstrukturen. Polizeien sind hoch regulierte Organisationen mit etablierten Routinen, hierarchischen Entscheidungsprozessen und spezifischen Mustern der Professionalisierung. Die Integration algorithmischer Systeme verändert damit die Frage, wer die Verantwortung für Entscheidungen übernehmen muss (Weber 2025; Waldtmann 2024; Mergel et al. 2019).

Technologische Innovation ist nur dann nachhaltig wirksam, wenn sie in formalisierte Steuerungsmechanismen eingebettet ist. Polizeibehörden müssen bereits vor der Beschaffung festlegen, wer das System fachlich verantwortet und wie dessen Leistung im Betrieb kontrolliert wird (UNICRI & INTERPOL, 2024; Janssen et al. 2020). Ohne eine solche Gesamtarchitektur besteht die Gefahr isolierter Pilotprojekte, die weder interoperabel noch strukturell verankert sind. Interne Kontrollarchitekturen müssen als kontinuierliche Beobachtungs- und Anpassungsprozesse ausgestaltet werden (Bommasani et al. 2021; Mergel et al. 2019). Dies bedeutet für Polizeiorganisationen zunächst, belastbare Revisionsmechanismen zu etablieren, die den Einsatz algorithmischer Systeme regelmäßig überprüfen. Treten Fehlfunktionen auf, müssen klar definierte Eskalationsstrukturen greifen, um Zuständigkeiten eindeutig zuzuweisen und eine zeitnahe Reaktion zu gewährleisten. Zudem sind standardisierte Dokumentationsroutinen erforderlich, damit Entscheidungen und Systemeingriffe jederzeit nachvollzogen und geprüft werden können. Algorithmische Systeme werden dadurch als reguläre Gegenstände interner Qualitätssicherung und Organisationsaufsicht behandelt (NIST 2023; Janssen et al. 2020).

Es ist jedoch zu berücksichtigen, dass die Implementierung nicht allein über formale Vorgaben gesteuert werden kann. Die Innovationsfähigkeit von Sicherheitsbehörden wird maßgeblich durch bestehende Pfadabhängigkeiten beeinflusst (Vydra & Klievink 2019). Technologische und organisatorische Entwicklungspfade werden durch frühere Entscheidungen festgelegt, von denen es schwer ist, abzuweichen. Hinzu kommen gewachsene Zuständigkeitsstrukturen, die Entscheidungsprozesse verfestigen und Veränderungsdynamiken einschränken. Selbst heterogene IT-Landschaften entfalten eine strukturierende Wirkung. Die Integration und die Anpassung neuer Anwendungen werden durch unterschiedliche Systeme, Schnittstellen und technische Standards zusätzlich erschwert (OECD 2025b; Mergel et al. 2019). Fehlt eine strategische Gesamtarchitektur, können KI-Initiativen fragmentiert bleiben oder symbolischen Charakter annehmen. Nachhaltige Integration setzt daher eine übergreifende Koordination voraus, die technische Interoperabilität und Standardisierung systematisch verbindet. Von besonderer Bedeutung ist die Anschlussfähigkeit neuer Systeme an die professionelle Praxis. Technische Instrumente werden nur dann wirksam, wenn sie in bestehende Arbeitslogiken integrierbar sind und als funktional plausibel wahrgenommen werden (OECD 2025b; Vydra & Klievink 2019). Die interne Steuerung erfüllt insofern neben der Kontrollfunktion auch eine Integrationsfunktion. Sie gestaltet die Bedingungen, unter denen technische Innovation mit fachlicher Expertise kooperieren kann, ohne professionelle Autonomie zu unterminieren.

Schließlich berührt die organisationale Steuerungsdimension Fragen technologischer Souveränität. Abhängigkeiten von externen Anbietern oder proprietären Systemarchitekturen können die interne Gestaltungs- und Anpassungsfähigkeit einschränken. Strategische Be-

schaffungsentscheidungen, vertraglich gesicherte Prüfzugänge und institutionalisierte Evaluationsverfahren sind daher zentrale Elemente organisationsinterner Steuerungsfähigkeit (OECD 2025a). Die Leistungsfähigkeit algorithmischer Polizeisysteme hängt nicht primär von ihrer technischen Raffinesse ab. Entscheidend ist die institutionelle Fähigkeit, sie in stabile Entscheidungs-, Prüf- und Lernstrukturen einzubetten (Hoheisel-Gruler 2025; Pavlidis 2024).

Die Nutzung von KI ist auch eng mit Fragen der Personalstruktur, des Wissensmanagements und der organisationalen Lernfähigkeit verknüpft. Polizeien sind wissensintensive Organisationen, deren Leistungsfähigkeit in hohem Maße auf erfahrungsbasiertem, situativem und häufig implizitem Wissen beruht. Der demografische Wandel führt durch pensionierungsbedingte Abgänge zu einem Verlust dieses organisationalen Gedächtnisses. Gleichzeitig steigen Datenvolumina, digitale Beweislasten und analytische Anforderungen. Diese Konstellation verändert die Grundlagen professioneller Polizeiarbeit. Organisationstheoretisch lässt sich dieser Wandel als Spannungsverhältnis zwischen implizitem Erfahrungswissen und formalisiertem, technologisch vermitteltem Wissen beschreiben. KI-Systeme können diesen Prozess unterstützen, indem sie Informationen aggregieren, Muster identifizieren und Entscheidungsgrundlagen systematisieren. Sie ersetzen jedoch nicht die kontextgebundene Urteilskraft erfahrener Fachkräfte. Vielmehr entsteht ein hybrides Wissensregime, in dem algorithmische Verdichtungen und professionelle Erfahrung in ein neues Verhältnis treten (Piesold & Krause 2025).

Europol (2024) hebt hervor, dass KI-gestützte Polizeiarbeit daten- und ressourcenintensiver wird und zusätzliche Infrastruktur, Expertise sowie Qualifizierung erfordert. KI fungiert in diesem Zusammenhang weniger als isolierte Effizienztechnologie denn als Auslöser struktureller Kompetenzverschiebungen. Die Leistungsfähigkeit algorithmischer Systeme hängt wesentlich davon ab, ob Organisationen über Mitarbeitende verfügen, die Datenmodelle verstehen, ihre Ergebnisse einordnen und ihre Grenzen erkennen können (Hoheisel-Gruler 2025; Just 2025). Kompetenzentwicklung im KI-Kontext umfasst daher mehrere Dimensionen. Neben technischen Fähigkeiten im Umgang mit Daten und Modellen sind rechtliche Kenntnisse und ethische Sensibilität erforderlich, um Anwendungen in ihrem normativen Kontext einzuordnen. Hinzu treten reflexive Kompetenzen, die es ermöglichen, algorithmische Vorschläge kritisch zu prüfen und in professionelle Entscheidungsprozesse zu integrieren (Hoheisel-Gruler 2025; Piesold & Krause 2025). Die von UNICRI & INTERPOL (2024) entwickelte Werkzeugsammlung zur verantwortlichen KI-Innovation in der Strafverfolgung beschreibt Bereitschaft (engl. Readiness) als organisationsweite Fähigkeit, Ressourcen, Rollen, Schulungsformate und Datenqualität strategisch aufeinander abzustimmen.

Auch auf europäischer Ebene wird KI inzwischen als eigenständiges Qualifikationsfeld in der polizeilichen Aus- und Fortbildung verankert. Der Trainingskatalog der CEPOL weist KI-bezogene Inhalte als Lernziele für unterschiedliche Funktionsbereiche aus (CEPOL 2025). Dies deutet auf eine institutionelle Verschiebung hin: KI-Kompetenzen werden sowohl spezialisierten IT-Einheiten zugeschrieben als auch als organisationsweite Querschnittsqualifikation verstanden. Operative Kräfte, Führungspersonal und strategische Planungsbereiche sind gleichermaßen betroffen (Hoheisel-Gruler 2025; Piesold & Krause 2025). Zugleich erzeugt der Einsatz von KI neue Abhängigkeiten. Fehlende Modellkenntnisse oder unzureichendes Datenverständnis erhöhen die Gefahr unkritischer Übernahme algorithmischer Vorschläge

oder inadäquater Interpretation von Ergebnissen. Nachhaltige Nutzung technischer Systeme gelingt nur, wenn Mitarbeitende befähigt werden, deren Funktionslogik zu verstehen und kritisch zu reflektieren (OECD 2025b; Honekamp et al. 2023).

Somit entsteht eine doppelte Dynamik. Einerseits kann KI zur Sicherung und Strukturierung organisationalen Wissens beitragen, indem sie Informationsflüsse verdichtet und Entscheidungsprozesse unterstützt. Andererseits verschiebt sie Kompetenzanforderungen und macht neue Lernprozesse erforderlich. Die Stabilisierung polizeilicher Handlungsfähigkeit unter Bedingungen demografischer Veränderungen und wachsender digitaler Komplexität hängt daher entscheidend von der Fähigkeit ab, technologische Innovation mit systematischem Wissensmanagement und nachhaltiger Kompetenzentwicklung zu verbinden (Honekamp et al. 2023). Mit dem Aufkommen generativer KI und insbesondere großer Sprachmodelle verschiebt sich der Schwerpunkt polizeilicher KI-Anwendungen erneut. Während in der ersten Phase datengetriebener Systeme vor allem Mustererkennung, Klassifikation und Prognose im Vordergrund standen, treten nun Modelle hinzu, die eigenständig semantische Inhalte generieren. Large Language Models analysieren umfangreiche Textkorpora, verdichten Informationen, formulieren Hypothesen und erzeugen kohärente Textentwürfe (Europol 2024; Waldtmann 2024; Bommasani et al. 2021). Für wissensintensive Kernprozesse der Polizei eröffnen sich damit neue Anwendungsszenarien, etwa bei der Auswertung umfangreicher Ermittlungsakten, der Strukturierung digitaler Beweismittel oder der Vorbereitung schriftlicher Berichte (Honekamp 2025).

Diese Entwicklung stellt keine bloße Fortsetzung datenanalytischer Unterstützung dar, sondern eine qualitative Verschiebung. Generative Systeme greifen in die Auswahl oder Priorisierung von Informationen ein und wirken so unmittelbar auf die sprachliche und argumentative Ausgestaltung polizeilicher Dokumentation (Waldtmann 2024). Polizeiliche Arbeit ist in hohem Maße akten- und berichtsbasiert. Schriftliche Vermerke strukturieren interne Entscheidungsprozesse und bilden zugleich die Grundlage staatsanwaltschaftlicher und gerichtlicher Bewertungen. Wenn algorithmische Systeme Textvorschläge generieren oder Sachverhalte zusammenfassen, beeinflussen sie potenziell die Gewichtung von Indizien und die argumentative Struktur von Ermittlungsdarstellungen (Bender et al. 2021). Damit verschärft sich die bereits beschriebene epistemische Verschiebung, weil die Maschine sowohl Relevanzsignale setzt als auch kommunikative Inhalte mitgestaltet. KI-gestützte Berichtserstellung wird als entlastend wahrgenommen und verspricht Effizienzgewinne, zugleich erzeugt sie aber neue Unsicherheiten (Waldtmann 2024; O'Neil 2017). Unklarheiten entstehen insbesondere hinsichtlich der Reichweite menschlicher Kontrolle, der Zurechnung von Verantwortung und der Bewertung generierter Inhalte. Professionelle Urteilskompetenz wird nicht ersetzt, jedoch strukturell gerahmt. Die Verantwortung verbleibt rechtlich beim Menschen, faktisch kann sie jedoch durch die Suggestivkraft algorithmischer Vorschläge verschoben werden. Diese Diskrepanz zwischen formaler Verantwortungszuschreibung und tatsächlicher Entscheidungsdynamik bildet einen zentralen ethischen Problempunkt. Die Herausforderung besteht darin, algorithmisch produzierte Texte als heuristische Unterstützung zu nutzen, ohne ihre Formulierungsmacht unreflektiert zu übernehmen (Weber 2025).

Hinzu kommt die Problematik sogenannter Halluzinationen. Große Sprachmodelle operieren auf Grundlage statistischer Wahrscheinlichkeiten und erzeugen sprachlich plausible Inhalte, ohne über faktische Gewissheit oder semantisches Verständnis zu verfügen (Waldtmann 2024;

Bender et al. 2021). In strafrechtlichen Kontexten kann die Generierung unzutreffender oder unvollständig kontextualisierter Inhalte erhebliche Folgen für Ermittlungsrichtungen und die Dokumentationsqualität haben. Generative Systeme erfordern daher besonders ausgeprägte Validierungsroutinen und eine klare Zuordnung der inhaltlichen Verantwortung. Regulatorisch sind generative Modelle, sofern sie in sensiblen sicherheitsbehördlichen Kontexten eingesetzt werden, in das risikobasierte System der EU KI-VO einzuordnen. Die dort normierten Anforderungen an Dokumentation, menschliche Aufsicht und Risikomanagement betreffen generative Systeme in besonderer Weise, da sie unmittelbar in Entscheidungs- und Kommunikationsprozesse eingreifen (Pavlidis 2024). Die rechtliche Einordnung verdeutlicht, dass ihre Nutzung nicht als bloße technische Assistenz verstanden werden kann.

Wissenschaftlich betrachtet markieren generative KI-Systeme eine neue Phase der Mensch-Maschine-Interaktion im Sicherheitsbereich. Während frühere Systeme primär analytische Funktionen erfüllten, treten große Sprachmodelle in eine kooperative, dialogische Beziehung mit Anwenderinnen und Anwendern ein. Diese Form verändert die Arbeitsroutinen, Verantwortungswahrnehmung und Entscheidungsdynamik. Für Polizeiorganisationen entsteht damit die Aufgabe, generative Systeme so zu integrieren, dass sie Mitarbeitende unterstützen, ohne die narrative und argumentative Autonomie polizeilicher Arbeit zu unterminieren. Die zuvor entwickelten rechtlichen, ethischen und organisationalen Anforderungen verdichten sich im europäischen Kontext zu einer mehrschichtigen Regulierungsarchitektur für den Einsatz von KI.

Über diese Normen hinaus setzen Grund- und Menschenrechte den übergeordneten Bewertungsmaßstab. Die Charta der Grundrechte der Europäischen Union bindet staatliches Handeln insbesondere im Hinblick auf Nichtdiskriminierung, Verhältnismäßigkeit, Datenschutz und effektiven Rechtsschutz. Die praktische Herausforderung liegt weniger in der Existenz dieser Maßstäbe als in ihrer Operationalisierung bei der Klassifizierung, Entwicklung und Anwendung konkreter Systeme (Europäisches Parlament 2021; Europäische Kommission 2019). Auch die Rahmenkonvention des Europarats zu KI und Menschenrechten verpflichtet die Vertragsstaaten, den gesamten Lebenszyklus von KI menschenrechtskonform auszugestalten. KI-Regulierung wird damit in einen explizit menschenrechtlichen Kontext gestellt. Eine zentrale Rolle spielen in diesem Gefüge Folgenabschätzungen. Datenschutzrechtliche Folgenabschätzungen und weitergehende menschenrechtliche Impact Assessments dienen dazu, potenzielle Risiken systematisch zu identifizieren und ihre Tragweite zu dokumentieren. Impact Assessments fungieren somit als Bindeglied zwischen abstrakter Normsetzung und praktischer Anwendung (Erdogan 2024). Für die Polizeiarbeit bedeutet dies, dass der Einsatz von KI stets in ein komplexes externes Normgefüge eingebettet ist, dessen Einhaltung rechtliche Zulässigkeit, institutionelle Verantwortbarkeit und demokratische Bindung staatlicher Macht sichert. Die folgenden Beiträge zeigen an konkreten polizeilichen Anwendungsfeldern, wo der Einsatz von KI Vorteile bietet und welche Voraussetzungen für einen verantwortbaren Einsatz geschaffen werden müssen.

Alexander Huber eröffnet den Band mit einer Untersuchung von Potenzialen und Grenzen eines KI-gestützten Systems zur automatisierten Lagedarstellung in komplexen polizeilichen Sofortlagen. Ausgangspunkt ist die hohe Bedeutung eines belastbaren Lagebildes für Führungsentscheidungen unter Zeitdruck. Auf Grundlage einer systematischen Literaturrecherche entwickelt er ein theoretisches Modell zur KI-basierten Datenfusion und Visualisierung

polizeiinterner Informationsquellen und bewertet dieses mittels einer SWOT-Analyse. Dabei identifiziert er technische Leistungsstärken digitaler Systeme, verweist jedoch zugleich auf Risiken wie Bias, Halluzinationen, Intransparenz, rechtliche Unsicherheiten und Fragen der Mensch-Maschine-Interaktion.

Im Beitrag von Bastian Blum wird der Einsatz von KI-Agenten und Multi-Agenten-Systemen in der öffentlichen Verwaltung auf Grundlage einer literaturgestützten IST-Analyse untersucht. Die Ergebnisse werden systematisch mithilfe einer SWOT-Struktur erarbeitet. Im Zentrum stehen die technologischen Leistungsmerkmale, funktionalen Potenziale sowie systemischen Schwächen und Risiken agentenbasierter KI-Systeme. Der Beitrag zeigt, dass Multi-Agenten-Systeme einen Beitrag zur Bewältigung zentraler Herausforderungen wie Fachkräftemangel und Digitalisierung leisten können, ihre Nutzung jedoch an Fragen der Transparenz, Verantwortlichkeit, Akzeptanz und technischen Integrationsfähigkeit gebunden bleibt.

An einem Fallbeispiel erforscht André Müller, in welchem Umfang KI die Sachbearbeitung von Massendelikten entlasten kann und welche Grenzen einer Umsetzung entgegenstehen. Auf Basis einer theoretischen Einordnung und zweier Experteninterviews arbeitet er Entlastungsszenarien wie automatisierte Text- und Berichtserstellung, (Vor-)Klassifikation und assistierte Recherche heraus und kontrastiert operative Erwartungen mit der strategisch-technischen Perspektive. Als zentrale Hürden identifiziert der Beitrag Datenqualitätsprobleme, fehlende behördentaugliche Sprachmodelle, Risiken wie Bias und Halluzinationen sowie Anforderungen an Transparenz, menschliche Aufsicht und Revisionssicherheit im Kontext der EU KI-VO. Ergänzend werden organisatorische und governancebezogene Defizite wie fehlende KI-Strategie, Innovationsstrukturen und föderale Umsetzungshemmnisse diskutiert und Handlungsschritte für eine verantwortungsvolle Implementierung skizziert.

Jana Piorr analysiert in ihrem Beitrag die ethischen Implikationen des KI-Systems FRANKA für die polizeiliche Textauswertung im Deliktsfeld der Kinder- und Jugendpornografie. Als analytischer Referenzrahmen dient das Responsible AI Framework von Zühlke, das im Beitrag auf die menschliche Ebene fokussiert angewendet wird. Ergänzend führt die Autorin zwei leitfadengestützte Expertinnen- und Experteninterviews mit der Projektleitung durch und wertet diese mittels strukturierender qualitativer Inhaltsanalyse aus. Auf dieser Grundlage untersucht sie, inwieweit bei der Entwicklung von FRANKA Aspekte wie Gemeinwohlorientierung, Risiko-Mitigation, Transparenz, menschliche Kontrolle und Verantwortungszuweisung berücksichtigt werden. Der Beitrag identifiziert bestehende ethische Sensibilisierungen, weist jedoch zugleich auf konzeptionelle Lücken hin, etwa das Fehlen eines expliziten Ethikkonzepts und einer frühzeitigen regulatorischen Einordnung nach der EU KI-VO.

Der Beitrag von Marcel Janzik untersucht die ethische Bewertung KI-gestützter Verhaltens- und Bewegungserkennungssysteme im Kontext der niedersächsischen Landespolizei. Ausgangspunkt ist die Frage, unter welchen normativen Bedingungen ein solcher Technikeinsatz verantwortbar sein kann. Als Analyserahmen dient das MEESTAR-Modell, das exemplarisch auf die Dimensionen Gerechtigkeit und Privatheit angewendet wird und eine Bewertung auf individueller, organisationaler und gesellschaftlicher Ebene ermöglicht. Die Analyse zeigt, dass der Einsatz in beiden Dimensionen durchgehend als ethisch äußerst sensibel einzustufen ist. Identifiziert werden insbesondere Risiken algorithmischer Diskriminierung, institutioneller Verantwortungsverschiebung, funktionaler Zweckentfremdung sowie

gesellschaftlicher Überwachungsnormalisierung. Aus der normativen Einordnung werden konkrete Anforderungen an Transparenz, Auditierbarkeit, Zweckbindung, Kontrollmechanismen und organisationale Verantwortungsstrukturen abgeleitet. Der Beitrag versteht sich damit als ethische Orientierungsanalyse, die Mindestbedingungen für eine verantwortliche Implementierung formuliert.

Maximilian Achmüller untersucht die ethische Bewertung eines hypothetischen soziotechnischen Arrangements, in dem selbstständig agierende Sprachmodelle potenziell strafrechtlich relevante Nutzerinhalte eigeninitiativ an Strafverfolgungsbehörden übermitteln. Auf Grundlage des MEESTAR-Modells analysiert er schwerpunktmäßig die Dimensionen Sicherheit und Privatheit und differenziert jeweils zwischen individueller und gesellschaftlicher Ebene. In der Dimension Sicherheit identifiziert der Beitrag erhebliche Spannungsfelder zwischen Schadensprävention, Fehlerrisiken, Bias-Problematiken und rechtsstaatlichen Garantien und stuft die Anwendung als ethisch äußerst sensibel ein. In der Dimension Privatheit arbeitet er tiefgreifende Eingriffe in Autonomie, Vertrauen, geistige Freiheit sowie in demokratische Aushandlungsprozesse heraus und gelangt hier zu der Bewertung, dass eine solche Anwendung aus ethischer Sicht abzulehnen ist. Das Arrangement wird im Lichte der MEESTAR-Analyse als ethisch nicht vertretbar eingeordnet.

Eine polizeiliche Datenanalyseplattform unterzieht Robert Falk einer konzeptionell-prospektiven SWOT-Analyse. Er erläutert die technischen Grundlagen plattformbasierter Datenintegration, insbesondere semantische Modellierung und verfahrensübergreifende Vernetzung heterogener Datenbestände, und bewertet deren Potenziale für Effizienz, Kooperation und digitale Modernisierung. Zugleich arbeitet er strukturelle Schwächen sowie verfassungsrechtliche, datenschutzrechtliche und souveränitätspolitische Risiken heraus und formuliert Bedingungen für einen rechtsstaatlich tragfähigen Einsatz. Sebastian Herrmann analysiert die Auswirkungen des Einsatzes von KI auf die polizeiliche Sachbearbeitung. Auf Grundlage eines Scoping Reviews untersucht er, wie sich Arbeitsinhalte, Rollenprofile und Belastungsstrukturen durch KI verändern und welche digitalen sowie KI-spezifischen Kompetenzen künftig erforderlich sind. Darauf aufbauend leitet er organisationale Implikationen ab, insbesondere für Aus- und Fortbildung, Personalentwicklung, Führung und strategisches Kompetenzmanagement in Polizeiorganisationen.

Robin Strecker untersucht den möglichen Beitrag KI-gestützter Systeme zur Sicherung und Weitergabe von Erfahrungswissen im Kontext des demografischen Wandels bei der Polizei Nordrhein-Westfalen. Ausgangspunkt ist die Herausforderung des Wissensverlustes durch pensionierungsbedingtes Ausscheiden erfahrener Beschäftigter. Auf Grundlage einer theoretischen Einordnung von Wissensmanagement und KI analysiert der Beitrag mittels einer SWOT-Analyse die organisatorischen Voraussetzungen, Potenziale und Risiken einer KI-basierten Unterstützung von Wissenssicherungsprozessen. Neben technologischen Möglichkeiten wie Text Mining, generativer KI und assistierten Externalisierungsverfahren werden insbesondere Fragen der Datenqualität, Akzeptanz, Datenschutzanforderungen und organisatorischen Implementierung diskutiert. Inwiefern KI-gestützte Predictive-Policing-Ansätze im digitalen Raum zur Verhütung von Cyberkriminalität beitragen können, wird von Enrico Schubert kritisch analysiert. Auf Basis eines Scoping Reviews und einer SWOT-Analyse arbeitet er Effizienzpotenziale datenbasierter Prognosen heraus, etwa durch automatisierte Muster und Anomalieerkennung sowie eine gezieltere Ressourcensteuerung. Zugleich zeigt

er zentrale Grenzen und Risiken auf, die aus Datenqualität, Intransparenz, Fehlklassifikationen, Datenschutzanforderungen und möglichen Verzerrungen resultieren, und diskutiert die Bedeutung tragfähiger organisatorischer Voraussetzungen sowie klarer rechtlicher und ethischer Leitplanken für eine verantwortbare Umsetzung.

Der Beitrag von Sirko Trodler untersucht das Potenzial von Diffusionsmodellen zur Generierung synthetischer Füllpersonen für Wahllichtbildvorlagen im Strafverfahren. Auf Grundlage einer systematischen SWOT-Analyse bewertet er technische Leistungsfähigkeit, methodische Fairnessgewinne sowie infrastrukturelle Anforderungen und stellt diesen erhebliche psychologische, biasbezogene und rechtliche Risiken gegenüber. Der Beitrag gelangt zu einer differenzierten Einschätzung, wonach ein unmittelbarer operativer Einsatz derzeit nicht angezeigt ist, empfiehlt jedoch eine kontrollierte, forschungsnahe Erprobung unter Berücksichtigung strafprozessualer und regulatorischer Rahmenbedingungen.

Inwieweit KI-gestützte Assistenzsysteme die kriminalpolizeiliche Ersteinschätzung von Todesumständen am Leichenfundort unterstützen können, wird von Sabrina Wickert untersucht. Auf Grundlage einer systematischen Literaturrecherche und zweier Experteninterviews analysiert sie potenzielle Einsatzfelder, etwa die automatisierte Bild- und Musteranalyse, die strukturierte Auswertung medizinischer Unterlagen sowie die datenbasierte Plausibilitätsprüfung. Zugleich arbeitet sie technische, datenbezogene und kognitionsbezogene Grenzen heraus und betont die weiterhin zentrale Rolle menschlicher kriminalistischer Bewertung bei verantwortungskritischen Entscheidungen.

Tobias Keller untersucht die Vorbereitung polizeilicher Nachwuchskräfte auf KI-bezogene Herausforderungen. Auf Grundlage einer qualitativen Expertenbefragung analysiert er technische, rechtliche und ethische Kompetenzanforderungen, identifiziert Defizite in der gegenwärtigen curricularen Verankerung und leitet didaktische sowie organisatorische Implikationen für eine interdisziplinär ausgerichtete Ausbildung ab.

Abgeschlossen wird das Buch durch Alexander Herdt mit einer Analyse des Einsatzes von Large Language Models in der polizeilichen Cold-Case-Sachbearbeitung. Auf Grundlage einer modifizierten SWOT-Analyse arbeitet er Potenziale, Grenzen und Risiken heraus, ordnet diese rechtlich sowie organisatorisch ein und entwickelt Implikationen für Forschung, polizeiliche Praxis und regulatorische Weiterentwicklung.

Die im Buch versammelten Beiträge zeigen, dass der Einsatz von KI in der Polizeiarbeit weder als technische Modernisierung noch als isolierte Rechtsfrage adäquat erfasst werden kann. Er verändert, wie polizeiliche Informationen ausgewählt und bewertet werden. Polizeiliche Erkenntnis entsteht zunehmend im Zusammenwirken von KI-System und menschlicher Bewertung. Diese Transformation bleibt jedoch an rechtliche und normative Grenzen gebunden. Die unionsrechtlichen Vorgaben, insbesondere die EU KI-VO und das Datenschutzrecht, definieren nicht nur Verfahrensanforderungen, sondern auch materielle Bedingungen zulässiger Machtausübung (Kleemann & Aden 2025; Honekamp et al. 2025). Zugleich machen die ethischen Analysen deutlich, dass formale Rechtmäßigkeit eine notwendige, jedoch keine hinreichende Bedingung demokratischer Legitimität darstellt. Ein System kann unionsrechtlich zulässig sein und dennoch gesellschaftliches Vertrauen unterminieren, wenn seine Wirkungsweisen als intransparent oder strukturell benachteiligend wahrgenommen wer-

den. Fragen der Fairness, Nichtdiskriminierung, Transparenz und Verantwortungszurechnung betreffen die gesellschaftliche Tragfähigkeit algorithmisch gestützter Polizeiarbeit in substanzieller Weise (Kemme 2025; Schiemann 2025; O'Neil 2017).

Die zentrale Herausforderung liegt weniger im Vorhandensein eines dichten Normgefüges als in dessen kohärenter Integration in heterogene, föderal organisierte Behördenstrukturen. Normative Vorgaben entfalten nur dann praktische Wirksamkeit, wenn sie in belastbare Governance-Strukturen überführt werden. Erforderlich sind klar definierte Verantwortungsbereiche über den gesamten Systemlebenszyklus hinweg, institutionalisierte Prüfverfahren sowie funktionsfähige interne und externe Kontrollmechanismen (Schiemann 2025; OECD 2025a). Damit verschiebt sich die Leitfrage. Im Zentrum steht, unter welchen institutionellen Voraussetzungen der Einsatz von KI dauerhaft überprüfbar, kontrollierbar und lernfähig gestaltet werden kann. Diese institutionelle Dimension ist untrennbar mit der Personal- und Wissensebene verbunden. Polizeiliche Handlungsfähigkeit unter Bedingungen digitaler Komplexität setzt voraus, dass Mitarbeitende algorithmische Systeme verstehen, ihre Ergebnisse kritisch einordnen und ihre Grenzen reflektieren können. KI verändert Werkzeuge, Rollenbilder und Kompetenzanforderungen zugleich und erzeugt neue Formen organisatorischer Abhängigkeit, die professionell austariert werden müssen (Piesold & Krause 2025; Honekamp et al. 2023).

Mit generativen Modellen verschärft sich diese Konstellation. Wenn Systeme Daten analysieren und sprachliche sowie argumentative Strukturen mitformen, rückt die Schnittstelle zwischen Mensch und Maschine in das Zentrum institutioneller Verantwortung. Bewertet werden muss dann die statistische Validität von Prognosen sowie die Entstehung und Qualität narrativer Rahmungen und dokumentierter Entscheidungsgrundlagen. Die Frage nach Kontrolle und Zurechenbarkeit erhält eine zusätzliche kommunikative Dimension. Das Buch versteht sich daher als Beitrag zu einer systematischen Klärung dieser Interdependenzen. Es zeigt, dass die Zukunft polizeilicher KI weder durch Innovationsdynamik noch durch Regulierung isoliert bestimmt wird. Entscheidend ist, ob Behörden KI so einsetzen können, dass technische Unterstützung die polizeiliche Urteilsbildung stärkt, ohne Verantwortung und Kontrolle zu schwächen. Die maßgebliche Gestaltungsaufgabe liegt daher beim polizeilichen Führungspersonal. Dieses muss mit den Potenzialen und Risiken des KI-Einsatzes verantwortungsvoll umgehen.

Literaturverzeichnis

Bender, E. M., Gebru, T., McMillan-Major, A., & Shmitchell, S. (2021). On the dangers of stochastic parrots: Can language models be too big? In: Proceedings of the 2021 ACM Conference on Fairness, Accountability, and Transparency (610–623). ACM. doi.org/10.1145/3442188.3445922

Bommasani, R., Hudson, D. A., Adeli, E., et al. (2021). On the opportunities and risks of foundation models. Stanford Center for Research on Foundation Models. arxiv.org/abs/2108.07258

CEPOL (2025). Annex 3: CEPOL training catalogue of granted activities 2025. European Union Agency for Law Enforcement Training. www.cepol.europa.eu/api/assets/media/downloads/2025/Annex-3-CEPOL-Training-Catalogue-of-Granted-Activities-2025.pdf

Coors, B. (2025). Polizei 4.0: Herausforderungen bei der Einführung von Systemen der Künstlichen Intelligenz. In: W. Honekamp (Hrsg.): Künstliche Intelligenz in der Polizeiarbeit (Schriftenreihe der Deutschen Hochschule der Polizei, Band 25, S. 19–36). Deutsche Hochschule der Polizei – Hochschulverlag. dhpol.de/Bd_25_pdfA.pdf

Döring, C. (2025). Einsatz von Künstlicher Intelligenz bei der Polizei und deren gesellschaftliche Akzeptanz. In: W. Honekamp (Hrsg.): Künstliche Intelligenz in der Polizeiarbeit (Schriftenreihe der Deutschen Hochschule der Polizei, Band 25, S. 74–91). Deutsche Hochschule der Polizei – Hochschulverlag. dhpol.de/Bd_25_pdfA.pdf

Egbert, S. (2024). Algorithmisches Polizieren in Deutschland, Zeitschrift für Jugendkriminalrecht und Jugendhilfe, 35/2 122–130.

Europäische Kommission (2019). Ethics guidelines for trustworthy AI. Publications Office. data.europa.eu/doi/10.2759/346720

Europäisches Parlament (2021). Künstliche Intelligenz im Strafrecht und ihre Verwendung durch die Polizei und Justizbehörden in Strafsachen (2020/2016(INI)) (OJ C, C/132, 24.03.2022, eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021IP0405)

Europol (2024). AI and policing: The benefits and challenges of artificial intelligence for law enforcement. Europol. europol.europa.eu/cms/sites/default/files/documents/AI-and-policing.pdf

Floridi, L., Cowls, J., Beltrametti, M., et al. (2018). AI4People −An ethical framework for a good AI society: Opportunities, risks, principles, and recommendations. Minds and Machines, 28 (4), 689–707. doi.org/10.1007/s11023-018-9482-5

Guler, A., Kula, S., & Boke, K. (2025). Examining public support for AI in policing: the role of perceived procedural justice. Police Practice and Research, 26(6), 673–695. doi.org/10.1080/15614263.2025.2516535

Hoheisel-Gruler, R. (2025). Polizeiliche Aus-, Fort- und Weiterbildung in Zeiten von künstlicher Intelligenz (KI). In: W. Honekamp & M. Klingelhöfer (Hrsg.): Polizei-Informatik 2025 (Schriftenreihe der Deutschen Hochschule der Polizei, Band 27, S. 12–28). Deutsche Hochschule der Polizei – Hochschulverlag. dhpol.de/Bd_27pdfA.pdf

Honekamp, W. (2025). Die Auswirkungen Künstlicher Intelligenz auf die Polizeiarbeit. Deutsches Polizeiblatt 43 (6), 15−18.

Honekamp, W., Kemme, S., & Struck, J. (2025). Fortschritt durch Verantwortung? Künstliche Intelligenz in der Polizeiarbeit der Zukunft. In: W. Honekamp, S. Kemme, & J. Struck (Hrsg.): Auswirkungen von Künstlicher Intelligenz auf die zukünftige Polizeiarbeit (V−X). Springer Gabler. link.springer.com/content/pdf/bfm:978-3-658-48425-5/1

Honekamp, W., Povalej, R., Rittelmeier, H., Fähndrich, J., Berner, S., Labudde, D. (2023). Technologiegetriebene Polizeiausbildung im Umgang mit Digitalen Spuren. In: T.-G. Rüdiger, P. S. Bayerl (Hrsg.): Handbuch Cyberkriminologie (673–702). Springer VS, Wiesbaden. doi.org/10.1007/978-3-658-35450-3_51-2

Erdogan, I. (2024). Diving into the Iceberg: Establishing Transparency in AI for Law Enforcement. European Papers 9 (3), S. 956−977. doi.org/10.15166/2499-8249/794

Jansen, F. (2018). Data driven policing in the context of Europe. Data Justice Project. datajusticeproject.net/wp-content/uploads/2019/05/Report-Data-Driven-Policing-EU.pdf

Janssen, M., Brous, P., Estevez, E., Barbosa, L. S., & Janowski, T. (2020). Data governance: Organizing data for trustworthy artificial intelligence. Government Information Quarterly, 37(3), 101493. doi.org/10.1016/j.giq.2020.101493

Just, C. (2025). KI-Kompetenzen für Polizeibeamtinnen und -beamte: Die Zukunft der Polizeiausbildung in Baden-Württemberg. In: W. Honekamp (Hrsg.): Künstliche Intelligenz in der Polizeiarbeit (Schriftenreihe der Deutschen Hochschule der Polizei, Band 25, S. 37–55). Deutsche Hochschule der Polizei – Hochschulverlag. dhpol.de/Bd_25_pdfA.pdf

Kemme, S. (2025). Zwischen Effizienz und Recht auf Fairness: Wie algorithmische Polizeiarbeit Diskriminierung verstärken kann. In: W. Honekamp, S. Kemme & J. Struck (Hrsg.): Auswirkungen von Künstlicher Intelligenz auf die zukünftige Polizeiarbeit (S. 281–299). Springer Gabler. doi.org/10.1007/978-3-658-48425-5_16

Kleemann, S., & Aden, H. (2025). Die Nutzung Künstlicher Intelligenz durch Strafverfolgungsbehörden – „Hintertüren“ der Verordnung der Europäischen Union über Künstliche Intelligenz. In: W. Honekamp, S. Kemme & J. Struck (Hrsg.): Auswirkungen von Künstlicher Intelligenz auf die zukünftige Polizeiarbeit (S. 3–30). Springer Gabler. doi.org/10.1007/978-3-658-48425-5_1

Kraft, S. (2025). Gemeinsamkeiten und Unterschiede der Datenschutz-Folgenabschätzung (DSFA) gem. Art. 35 DSGVO und der Grundrechte-Folgenabschätzung (GFA) gem. Art. 27 KI-Verordnung. In: W. Honekamp (Hrsg.): Künstliche Intelligenz in der Polizeiarbeit (Schriftenreihe der Deutschen Hochschule der Polizei, Band 25, S. 306–321). Deutsche Hochschule der Polizei – Hochschulverlag. dhpol.de/Bd_25_pdfA.pdf

Kunze, D. (2025). Künstliche Intelligenz im Polizeirecht – Verfassungsrechtliche Rahmenbedingungen, Bias-Risiken und Chilling Effects. In: W. Honekamp & M. Klingelhöfer (Hrsg.): Polizei-Informatik 2025 (Schriftenreihe der Deutschen Hochschule der Polizei, Band 27, S. 257–277). Deutsche Hochschule der Polizei – Hochschulverlag. dhpol.de/Bd_27pdfA.pdf

Mergel, I., Edelmann, N., & Haug, N. (2019). Defining digital transformation: Results from expert interviews. Government Information Quarterly, 36 (4), 101385. doi.org/10.1016/j.giq.2019.06.002

NIST (2023). Artificial Intelligence Risk Management Framework (AI RMF 1.0). National Institute of Standards and Technology. U.S. Department of Commerce. doi.org/10.6028/NIST.AI.100-1

OECD (2025a). Governing with artificial intelligence: The state of play and way forward in core government functions. OECD Publishing. doi.org/10.1787/795de142-en

OECD (2025b). Harnessing Artificial Intelligence in Social Security: Use Cases, Governance and Workforce Readiness, OECD Digital Government Studies, OECD Publishing, Paris. doi.org/10.1787/b52405c1-en

O'Neil, C. (2017). Angriff der Algorithmen: Wie sie Wahlen manipulieren, Berufschancen zerstören und unsere Gesundheit gefährden. Hanser.

Pavlidis, G. (2024). Unlocking the Black Box: Analysing the EU Artificial Intelligence Act's Framework for Explainability in AI. Law Innovation and Technology, 16 (1), S. 293–308. doi.org/10.1080/17579961.2024.2313795

Pfeffer, K. (2025). Der Einsatz künstlicher Intelligenz in der Polizeiarbeit nach dem AI-Act – Eine rechtswissenschaftliche Perspektive. In: W. Honekamp, S. Kemme & J. Struck (Hrsg.): Auswirkungen von Künstlicher Intelligenz auf die zukünftige Polizeiarbeit (S. 31–48). Springer Gabler. doi.org/10.1007/978-3-658-48425-5_2

Piesold, R.-R., & Krause, T. (2025). Anforderungen an die KI-Kompetenz von Beschäftigten der öffentlichen Verwaltung im Kontext des EU AI Acts. In: W. Honekamp, S. Kemme & J. Struck (Hrsg.): Auswirkungen von Künstlicher Intelligenz auf die zukünftige Polizeiarbeit (S. 99–117). Springer Gabler. doi.org/10.1007/978-3-658-48425-5_6

Richardson, R., Schultz, J. M., & Crawford, K. (2019). Dirty data, bad predictions: How civil rights violations impact police data, predictive policing systems, and justice. New York University Law Review Online, 94 (15), 16–55. nyulawreview.org/wp-content/uploads/2019/04/NYULawReview-94-Richardson_etal-FIN.pdf

Schiemann, A. (2025). Rechtlich-ethische Begleitforschung bei der Entwicklung KI-gestützter polizeilicher Ermittlungstools. In: W. Honekamp, S. Kemme & J. Struck (Hrsg.): Auswirkungen von Künstlicher Intelligenz auf die zukünftige Polizeiarbeit (S. 49–62). Springer Gabler. doi.org/10.1007/978-3-658-48425-5_3

Singelnstein, T. (2025). Die Sicherheit der Zukunft – Künstliche Intelligenz und soziale Kontrolle: Vom Predictive Policing zum Social Scoring. In: W. Honekamp, S. Kemme & J. Struck (Hrsg.): Auswirkungen von Künstlicher Intelligenz auf die zukünftige Polizeiarbeit (S. 267–280). Springer Gabler. doi.org/10.1007/978-3-658-48425-5_15

UNICRI & INTERPOL (2024). Toolkit for responsible AI innovation in law enforcement: Organizational roadmap. United Nations Interregional Crime and Justice Research Institute & International Criminal Police Organization. ai-lawenforcement.org/toolkit/download

Vydra, S., & Klievink, B. (2019). Techno-optimism and policy-pessimism in the public sector big data debate. Government Information Quarterly, 36 (4), 101383. doi.org/10.1016/j.giq.2019.05.010

Waldtmann, C. (2024). Einsatz KI-basierter Technologien zur Bewältigung des polizeilichen Vorgangsaufkommens bei Massendelikten. In: W. Honekamp & D. Labudde (Hrsg.): Polizei-Informatik 2024. Rediroma-Verlag.

Weber, K. (2025). Akzeptanz, Regulierung und soziotechnische Anforderungen an KI-Systeme für die automatisierte Strafverfolgung. In: W. Honekamp, S. Kemme & J. Struck (Hrsg.): Auswirkungen von Künstlicher Intelligenz auf die zukünftige Polizeiarbeit (319–334). Springer Gabler. doi.org/10.1007/978-3-658-48425-5_18

Nutzung von KI zur automatisierten Lagedarstellung in komplexen polizeilichen Sofortlagen. Eine Untersuchung potenzieller Stärken, Schwächen, Chancen und Risiken

Alexander Huber

Am 22. Juli 2016 erschoss ein 18-jähriger Täter im und am Olympia-Einkaufszentrum (OEZ) in München neun Menschen und verletzte zahlreiche weitere, bevor er sich selbst tötete. Aufgrund von Fehlinformationen gingen die Behörden zunächst von mehreren Tätern und Tatorten aus, was einen umfangreichen Einsatz der Polizei auslöste. Erst Stunden nach der eigentlichen Tat konnte das entstandene Bild eines groß angelegten Terroranschlags korrigiert werden (Bannenberg 2018, S. 4 und 9).

Dieses Ereignis verdeutlicht exemplarisch die grundlegende Schwierigkeit komplexer polizeilicher Sofortlagen, also von Einsätzen, deren Anlass ad hoc entsteht und die nicht konkret vorbereitet werden können: aus einer Vielzahl heterogener und teils widersprüchlicher Informationen in Echtzeit ein belastbares Lagebild in Form einer Lagedarstellung zu entwickeln (Heimann 2024, S. 167). Die Lagedarstellung bildet eine wesentliche Grundlage für das gemeinsame Lagebewusstsein der Einsatzkräfte und sie ermöglicht fundierte Entscheidungen des Polizeiführers als Gesamtverantwortlichem (Heimann 2024, S. 132 und 281). Unter Lagedarstellung wird hier die strukturierte visuelle Aufbereitung der wesentlichen Elemente der aktuellen Einsatzsituation verstanden. In komplexen Szenarien kann ein fehlerhaftes oder unvollständiges Lagebewusstsein zu gravierenden Fehleinschätzungen und Fehlentscheidungen führen (Endsley 1995, S. 2). Zugleich wird die anspruchsvolle Aufgabe der Lagedarstellung bislang weitgehend manuell, zumindest aber ohne den Einsatz von KI erfüllt (Ries 2025, S. 40), womit sie den natürlichen Grenzen menschlicher Wahrnehmungs- und Verarbeitungskapazitäten unterliegt (Heimann 2024, S. 84–102).

Künstliche Intelligenz (KI) bietet hier potenziell entscheidende Vorteile: die parallele Auswertung heterogener Datenquellen in Echtzeit, die automatisierte Zusammenführung relevanter Informationen sowie deren strukturierte Visualisierung. Entsprechend formuliert Ries (2025) die „Informationsanalyse und -visualisierung in komplexen [polizeilichen] Einsatzlagen“ als ausdrückliches Forschungsdesiderat (Ries 2025, S. 77). Ausgehend hiervon befasst sich der vorliegende Beitrag mit der Forschungsfrage: „Welche Potenziale und Grenzen bestehen für den Einsatz von KI-gestützten Systemen zur automatisierten Lagedarstellung in komplexen polizeilichen Sofortlagen?“

Ziel dieses Beitrags ist eine explorative Erstbetrachtung des Potenzials KI-gestützter Lagedarstellung in diesem spezifischen Anwendungskontext mittels systematischer Literaturrecherche und anschließender SWOT-Analyse (nähere Erläuterung im Kapitel „Material und Methoden“). Da die Recherche keine Hinweise auf bereits eingesetzte derartige Systeme für den Bereich deutschsprachiger Polizeien ergab, wird hier von einem theoretischen Modell ausgegangen, das mit Hilfe von KI Daten aus internen Quellen wie Einsatzleitsystemen, Messengern und – mittels KI automatisiert per Speech-to-Text transkribiertem – Digitalfunk zusammenführt und als Lagedarstellung in einem Einsatz nahezu in Echtzeit visualisiert.

Gemeint ist hier der Teil der Lagedarstellung, der Daten aus polizeiinternen Systemen wie Kerninformationen zum Einsatz, also beispielsweise Kategorisierung der Lage, Täterabsichten/Forderungen, Personen und deren Beziehungen untereinander, Orte sowie relevante Objekte umfasst – nicht jedoch die schlichte Wiedergabe des Inhalts von z. B. Einsatzleit-/Dokumentationssystemen oder Videoquellen. Kein Gegenstand dieses Beitrags sind Lagedarstellungen in der Einsatzvor- und Nachbereitungsphase sowie in der allgemeinen Stabsarbeit außerhalb konkreter Einsätze und die Darstellung polizeiexterner Daten wie beispielsweise die Ergebnisse von (automatisierten) Recherchen im Bereich Open Source Intelligence (OSINT). Der Fokus des Beitrags auf komplexe Sofortlagen liegt in deren Ad-hoc-Charakter, Informationsdichte und Zeitdruck begründet, was einen entsprechend großen Mehrwert einer automatisierten, KI-basierten Lagedarstellung erwarten lässt.

Hintergrund

In diesem Abschnitt werden die theoretischen Hintergründe der Lagedarstellung in Polizeieinsätzen sowie einer möglichen technischen Automatisierung dieses bisher manuellen Prozesses mittels KI-basierter Systeme dargelegt.

Lagedarstellung als elementarer Teil des polizeilichen Einsatzmanagements

Der Begriff „Lage“ bezeichnet im polizeilichen Kontext alle Umstände, die polizeiliches Handeln bestimmen und beeinflussen (Heimann 2024, S. 278). Für größere Einsätze richtet die Polizei Besondere Aufbauorganisationen (BAOen) ein, welche Führungsorgane wie den Polizeiführer (PF) und Führungsstäbe umfassen (Heimann 2024, S. 267, 275 und 281). Der PF trägt die Gesamtverantwortung in einer BAO, strukturiert den Einsatz und trifft die wesentlichen Entscheidungen. „Die Lagebilderstellung ist […] das Fundament des gesamten Einsatzes. Daher kommt insbesondere bei Sofortlagen der schnellen Informationsgewinnung, -verarbeitung und -weitergabe durch den jeweiligen Führungsstab eine besondere Bedeutung zu“ (Kleinschmidt und Rückheim 2009, Kapitel 1.3). Die Lagebilderstellung verfolgt drei Ziele: Überblick über vorhandene Daten, konfirmative Analyse (das beiläufige Hinterfragen der Informationen durch die Betrachter), Komplexitätsreduktion sowie Herstellung eines gemeinsamen Verständnisses (Lagebewusstseins) bei allen Beteiligten (Heimann 2024, S. 135 f.). Im englischsprachigen Raum wird dieses Verständnis als shared situational awareness bezeichnet, welche auf dem gemeinsamen Lagebild, dem common operational picture, fußt (Thorkildsen et al. 2019, S. 3). Die Lagedarstellung muss im Einsatzverlauf kontinuierlich fortgeschrieben werden (Heimann 2024, S. 132 und Kap. 4.3). Der Begriff „Lagebild“ wird in der Praxis auch außerhalb des Kontextes einzelner Polizeieinsätze wie beispielsweise im „Bundeslagebild zur Organisierten Kriminalität“ des Bundeskriminalamts (BKA) verwendet. In diesem Beitrag wird zur klaren Abgrenzung der Begriff „Lagedarstellung“ verwendet.

Polizeiinterne Rahmenvorgaben wie die Polizeidienstvorschrift (PDV) 100 (BMI 2024, Nr. 1.6.2.1) und die PDV 102 (BMI 2020) regeln die bei der Lagedarstellung zu nutzenden Bezeichnungen und Symbole. Eine umfassende Lagedarstellung komplexer Einsätze beinhaltet regelmäßig die BAO-Struktur einschließlich Gliederung der Einsatzabschnitte, Verantwortlichkeiten/Erreichbarkeiten, Kategorisierung der Lage, relevante Örtlichkeiten, Personen/Beziehungsgeflechte inkl. Fortbewegungsmittel sowie Eigensicherungshinweise

(Heimann 2024, S. 133). Nach Erfahrung des Autors hängt die Auswahl der darzustellenden Informationen und die Art der Darstellung in der Praxis stark von der Art des Einsatzes und der Präferenz der beteiligten Personen ab.

Grenzen der menschlichen Lagedarstellung

Bei sehr dynamischen (viele Änderungen in kurzer Zeit) oder großen Einsätzen (viele Kräfte, Einsatzabschnitte und/oder hohe Gliederungstiefe) ist der Informationsumsatz regelmäßig sehr groß (Heimann 2024, S. 81, 167). Obwohl das Informationsmanagement in polizeilichen Sofortlagen mit Digitalfunk und Einsatzleit-/Dokumentationssystemen digitalisiert ist, erfolgt die Aufbereitung und Visualisierung der Lage bislang manuell im Sinne von nicht automatisiert (beispielhaft Hofinger und Heimann 2022, S. 239, sowie Heimann 2024, S. 238 und 221). Die Qualität der Lagedarstellung unterliegt daher den biologischen Grenzen der dafür eingesetzten Personen, insbesondere der Aufnahme- und Verarbeitungskapazität, aber auch Denk- und Wahrnehmungsfehlern sowie Ermüdung/Erschöpfung (Heimann 2024, Kapitel 3.2 und 3.3). Die genannten Faktoren können zudem durch Stress oder gruppendynamische Prozessen zusätzlich verstärkt werden (Hofinger und Heimann 2022, S. 204 ff.).

Künstliche Intelligenz

Eine allgemeingültige Definition von Künstlicher Intelligenz (KI) existiert bis dato nicht. Grundsätzlich können „starke KI" – mit gleichen oder überragenden intellektuellen Fähigkeiten wie der Mensch – und „schwache KI" unterschieden werden. Schwache KI meint die Nachbildung bzw. Simulation menschlichen Denkens zur Lösung konkreter Anwendungsprobleme. Solche KI-Systeme sind zur Selbstoptimierung fähig und können unter anderem eingesetzt werden zum logischen Folgern, zur Modellierung von Wissen, Musteranalyse und Mustererkennung sowie Analyse von Sprache in Verbindung mit Bildern, Gestik und anderen Formen menschlicher Interaktion (Die Bundesregierung 2025, Startseite, Reiter „Definition"). Typische Beispiele hierfür sind Tools zur Umwandlung von Audiodaten in Text oder Large Language Models (LLMs) als eine Form generativer KI. Generative KI bezeichnet Systeme, die eigenständig neue Inhalte wie Texte, Bilder, Musik und Videos erzeugen (Haufe Akademie 2025). Prominente Risiken von LLMs sind das Halluzinieren, also die Ausgabe von realistisch erscheinender Informationen, die jedoch faktisch falsch sind oder nicht mit den Trainingsdaten übereinstimmen (BayStMFH 2025, S. 5), Bias als in Trainingsdaten angelegter Verzerrungen, die u. a. Voreingenommenheit und Diskriminierung widerspiegeln (BayStMFH 2025, S. 5), und die Blackbox-Problematik, nach der oft nicht nachvollziehbar ist, wie ein konkretes Ergebnis eines KI-Systems zustande gekommen ist (Schweizer Eidgenossenschaft 2019, S. 24).

Nutzung von KI zur Fusion und visuellen Darstellung von Daten

KI-Systeme ermöglichen automatisierte Datenfusion/-integration. Dies ist der Prozess der Zusammenführung von Daten aus verschiedenen Quellen, um einen einheitlichen, kohärenten und genaueren Datensatz zu erstellen. Verschiedene Daten(-ströme) – z. B. aus Einsatzleitsystemen oder Sensordaten wie Drohnenkameras – können kombiniert werden (Gao et al. 2020, S. 867 ff.). KI-basierte Systeme können diese Daten anschließend visuell aufbereiten, etwa als Graphen oder interaktive Dashboards (Wu et al. 2021, S. 5049 ff.). Dabei kommen u. a. Natural Language Processing (NLP) und generative KI, insbesondere LLMs, zum Einsatz.

Spezifische Nutzung von KI zur Lagedarstellung im Kontext des polizeilichen Einsatzmanagements sowie bei anderen BOS / Aktueller Forschungsstand

Zum Zeitpunkt der Recherche zu diesem Beitrag ergaben sich für den deutschsprachigen Raum keine Hinweise auf den bereits erfolgten Produktiveinsatz solcher Systeme. Dies wird durch Bein (2025) insbesondere für die KI-basierte Verarbeitung von Textdaten im Leitstellenumfeld gestützt (Bein 2025, S. 21). Die in diesem Kapitel genannten Technologien dürften nach Einschätzung des Autors jedoch geeignet sein, das im Kapitel „Einleitung" beschriebene theoretische Modell einer mehrstufigen Extraktion, Integration und Visualisierung von Daten aus polizeiinternen Quellen technisch zu realisieren.

Material und Methodik

Die methodische Grundlage dieses Beitrags bildet eine systematische Literaturrecherche mit anschließender SWOT-Analyse zur systematischen Einordnung und Bewertung der identifizierten Erkenntnisse.

Literaturrecherche

Die Literaturrecherche erfolgte mehrstufig im Zeitraum Oktober und November 2025 und umfasste primär Publikationen aus den Jahren 2016 bis 2025, mit Schwerpunkt auf den letzten fünf Jahren. In begründeten Einzelfällen wurden auch ältere Arbeiten einbezogen, sofern sie grundlegende, zeitunabhängige Erkenntnisse lieferten. Zunächst erfolgte eine systematische Recherche in Google Scholar und im Katalog der Deutschen Hochschule der Polizei (inkl. OpenAthens) nach peer-reviewten Publikationen (2020−2025) mit kombinierten Suchbegriffen: „KI"/„künstliche Intelligenz"/„artificial intelligence", „Einsatzmanagement"/„emergency management", „Lagedarstellung"/„situation awareness"/„common operational picture", „Polizei". Parallel erfolgten Anfragen beim KI-Campus des Bundesministeriums des Innern (BMI) und der Koordinierungsstelle KI des BKA zu bereits eingesetzten Systemen. Ergänzend wurde nach Standardwerken zu Eigenschaften von KI-Systemen recherchiert.

Erweiterung

Da diese Recherche keine hinreichend spezifischen Ergebnisse zum Forschungsgegenstand erbrachte, wurde die Strategie pragmatisch erweitert: Die Recherche bezog strukturell vergleichbare Kontexte (Rettungsdienst, Feuerwehr, behördliche Verwaltung, Notfall- und Krisenmanagement) mit ein. Militärische Anwendungen wurden ausgeschlossen, da militärische Operationen hinsichtlich zeitlicher und räumlicher Ausdehnung, Truppenstärke und rechtlichem Rahmen mit polizeilichen Sofortlagen nicht hinreichend vergleichbar erscheinen. Die Einschlusskriterien wurden auf qualitativ hochwertige graue Literatur (Behördenpublikationen, Verbandsstudien) und wissenschaftliche Online-Lexika zur Begriffserklärung erweitert. Das Schneeballprinzip sowie KI-gestützte Recherchewerkzeuge (Large Language Models mit Webzugriff) wurden ergänzend eingesetzt. Alle so identifizierten Quellen wurden kritisch auf wissenschaftliche Qualität geprüft. Die identifizierten Erkenntnisse wurden im

Rahmen eines transferorientierten Ansatzes auf den polizeilichen Kontext übertragen, da vergleichbare Rahmenbedingungen (zeitkritische Entscheidungen, dynamische Lagen, behördliche Strukturen in westlichen Demokratien) eine Übertragbarkeit rechtfertigen.

SWOT-Analyse als Bewertungsinstrument

Die SWOT-Analyse (Strengths, Weaknesses, Opportunities, Threats; auf Deutsch Stärken, Schwächen, Chancen, Risiken) dient als etabliertes Instrument zur systematischen Strategieentwicklung (Lippold 2020, S. 53). Sie ermöglicht eine differenzierte Beurteilung einer Organisation, eines Produkts oder – wie hier – eines theoretischen Modells: Stärken und Schwächen umfassen gegenwartsbezogene, intern kontrollierbare Faktoren; Chancen und Risiken beziehen sich auf zukunftsbezogene externe Faktoren und zeigen mögliche Auswirkungen des Einsatzes eines KI-basierten Systems zur Lagedarstellung (Künzli 2012, S. 126). Die Abgrenzung zwischen intern und extern erfolgt hier zwischen den inhärenten Eigenschaften des Modells oder direkt hieraus ableitbaren Folgen (intern) sowie der Verwendung der produzierten Ergebnisse durch den Menschen bzw. darauf basierender Auswirkungen auf Umwelten (extern).

Die Analyse basiert auf dem bereits erwähnten theoretischen Modell eines KI-gestützten Systems zur Extraktion, Integration und Visualisierung polizeiinterner Daten. Die Methode ist für den Charakter und den Umfang dieses Beitrags geeignet, da sie trotz begrenzter empirischer Datenlage eine strukturierte Erstbewertung ermöglicht.

Ergebnisse

Die identifizierten Faktoren des transferorientierten Ansatzes werden nachfolgend systematisch nach den vier SWOT-Dimensionen dargestellt.

Stärken

Aktuelle KI-Systeme weisen gegenüber der menschlichen Kognition in spezifischen Bereichen fundamentale Verarbeitungsvorteile auf: Digitale Systeme arbeiten im Vergleich zu biologischen Systemen wie dem Menschen mit einer millionenfach höheren Taktfrequenz. Hinzu kommen im Vergleich sehr große digitale Speicherkapazitäten mit nahezu verlustfreier Informationserhaltung sowie die Möglichkeit zur modularen Erweiterung durch zusätzliche Hardware-Ressourcen. Zudem unterliegen technische Systeme keinen biologischen Ermüdungseffekten und gewährleisten eine konstante Verarbeitungszuverlässigkeit (Russell und Norvig 2021, Kapitel 1.2). Diese physikalischen Eigenschaften ermöglichen es KI-Systemen, große Mengen an Daten zu verarbeiten und dabei Auffälligkeiten zu registrieren und Erkenntnisse zu liefern, die Menschen gerade in Hochstresssituationen übersehen könnten (Li et al. 2023, zitiert nach Bajwa 2025, S. 175).

KI-basierte Datenfusion, also die Integration von Daten aus verschiedenen Quellen wie Einsatzleitsystemen oder dem Digitalfunk, ermöglicht den Fokus auf relevante Daten, indem Redundanzen reduziert und (auch) damit die Verarbeitungszeiten verkürzt werden (Tilawat 2025a). Zudem kann die Datenfusion aufgrund der Nutzung mehrerer Quellen die Wahr-

scheinlichkeit von Fehlern und Verzerrungen, die in einzelnen Datensätzen vorhanden sind, reduzieren (Tilawat 2025a). Eine weitere technische Stärke ist das Potenzial zur kontinuierlichen Verbesserung: Durch Maschinelles Lernen und iterative Trainingsprozesse können sich die Modelle kontinuierlich anpassen und ihre Präzision über die Zeit hinweg steigern (Tilawat 2025b), sodass KI-basierte Lagedarstellungssysteme mit fortschreitender Nutzung „Einsatzerfahrung" sammeln – ohne menschlichen Limitierungen wie z. B. dem Vergessen zu unterliegen.

Bajwa (2025) kam bei einem systematischen Literaturreview von 424 Forschungsbeiträgen aus dem Bereich KI-basierter Notfallreaktionssysteme zu dem Ergebnis, dass der Einsatz von KI zu optimiertem Ressourceneinsatz, schnelleren Reaktionszeiten, verringerten menschlichen Fehlern sowie erhöhtem Lagebewusstsein geführt hat (Bajwa 2025, Kapitel Abstract). Diese Ergebnisse aus dem strukturell verwandten Kontext von Notfallreaktionssystemen legen nahe, dass KI-Systeme vergleichbare Stärken auch bei der automatischen Lagedarstellung in komplexen Polizeieinsätzen entfalten könnten.

Schwächen

KI-Systeme, insbesondere generative KI, können kognitive Biases, also systematisch verzerrte Informationsverarbeitung (Wirtz 2025), sowie soziale Stereotypisierungen (Bergius und Six 2025) aufweisen, da bereits die Trainingsdaten diese Effekte beinhalten (Buder et al. 2025, S. 173). Halluzinationen bei generativer KI bezeichnen zudem das Phänomen, dass KI-Modelle plausible, aber faktisch falsche Inhalte produzieren (Friedrich et al. 2024, S. 3). Die Qualität des Ergebnisses einer Datenfusion und damit der darauf aufbauenden späteren Lagedarstellung hängt schließlich maßgeblich von der Qualität der Eingabedaten, beispielsweise in Einsatzleitsystem und Digitalfunk, ab (Tilawat 2025a). Eine weitere Schwäche stellt die potenzielle Anfälligkeit für gezielte physische oder digitale Angriffe bzw. Sabotage dar, KI-spezifisch kommt eine mögliche gezielte Täuschbarkeit über manipulierte Eingaben hinzu (Schweizer Eidgenossenschaft 2019, S. 29).

Das Blackbox-Phänomen beschreibt, dass die internen Entscheidungsprozesse komplexer KI-Modelle für Menschen oft intransparent und nicht nachvollziehbar sind (Friedrich et al. 2024, S. 4), was Fragen nach der Verantwortlichkeit bei Fehlfunktionen aufwerfen kann. Die Erklärbarkeit eines KI-Systems ist wichtig, um Vertrauen, Nachvollziehbarkeit und Kooperation zwischen Mensch, hier also den potenziellen Nutzern und Betroffenen auf Basis des Systems getroffener Entscheidungen, und Maschine zu beeinflussen (Heine et al. 2023, S. 125). Darüber hinaus dürften sich für ein KI-basiertes System zur Lagedarstellung durch Planung, technische Entwicklung, Einführung mit Beschulung und Betrieb erhebliche Zeit-, Personal- und Kostenaufwände ergeben (analog zu Döbber 2025, Kapitel 8). Eine mögliche grundsätzliche Schwäche digitaler Darstellungsformen führt Heimann (2024) an: „Die Tendenz, Lagebilder über Computeranwendungen umzusetzen, ist nicht immer hilfreich. [...] Nicht selten sind analoge Methoden begreifbarer und handhabbarer als digitale Alternativen" (Heimann 2024, S. 139).

Chancen

Die Verbesserung der Funktionalität von Lagedarstellungen (des sogenannten Common Operating Picture) kann zu gesteigertem, geteiltem Situationsbewusstsein (Situational Awareness) und zu wirksameren, zeitnaheren Entscheidungen führen (Thorkildsen et al. 2022, Kapitel Abstract). KI trägt dazu bei, schnelle und richtige Entscheidungen treffen zu können (Rietzke 2021, Kapitel 4.1). Die Nutzung von KI zur Lagedarstellung kann bei erfolgreicher Implementierung zudem den Ausgangspunkt für spätere Weiterentwicklungen bilden, etwa KI-basierte Entscheidungsunterstützung durch Szenarienbildung und Vergleich mit historischen Einsätzen. Solche KI-basierten Entscheidungssysteme im Polizeikontext erwähnen beispielsweise Ries (2025) für die polizeiliche Stabsarbeit in BAOen (Ries 2025, S. 17) sowie Döbber (2025) zur Generierung automatischer Entscheidungsvorlagen für Einsatzleiter mittels Daten aus Kameras, Drohnen und Bodycams (Döbber 2025, S. 55).

Risiken

Von besonderem Gewicht sind ethische und rechtliche Unsicherheiten, die sich durch das Zusammenwirken von Mensch und KI-System ergeben. Der Deutsche Ethikrat skizziert in einer umfassenden Stellungnahme zu den Herausforderungen durch KI unter anderem Problemstellungen in den Bereichen Datenschutz (Deutscher Ethikrat 2023, Nr. 130), Verantwortlichkeit (Deutscher Ethikrat 2023, Nr. 43–47 und 62), Haftung (Deutscher Ethikrat 2023, Nr. 63 und 104) und dem sogenannten Automation Bias (Deutscher Ethikrat 2023, S. 65 und 105) – der Tendenz, Empfehlungen automatisierter Systeme ungeprüft zu übernehmen. Weitere ethische Risiken werfen die mangelnde Transparenz/Erklärbarkeit der Ausgaben von (generativer) KI sowie deren potenzielle Diskriminierung betroffener Personen durch algorithmische Verzerrungen (Bias) auf (Bitkom e. V. 2019, S. 43). Die rechtlichen Rahmenbedingungen sind mit der EU-KI-Verordnung (2024/1689 vom 13. Juni 2024), der EU-JI-Richtlinie (2016/680 vom 27. April 2016), dem deutschen Grundgesetz, den jeweiligen Polizeigesetzen der Länder und des Bundes sowie der Rechtsprechung komplex und erfordern eine sorgfältige Prüfung. Sofern das System als „Hochrisiko-KI-System“ gemäß AI Act eingestuft würde, hätte dies hohe regulatorische Aufwände zur Folge (Bitkom e. V. 2023, S. 10).

Stärken	Schwächen
• Sehr große Verarbeitungsgeschwindigkeit (vs. menschliche Kognition) • Ermüdungsfreie Zuverlässigkeit (Konstanz) • Effiziente Multi-Quellen-Datenfusion (Redundanzreduktion) • Iterative Selbstoptimierung (Lerneffekte) • Objektivierte Informationsverarbeitung	• Algorithmische Verzerrungen (Bias) • Faktische Inkorrektheit (Halluzinationen) • Abhängigkeit von Qualität der Eingabedaten • Mangelnde Nachvollziehbarkeit (Blackbox) • Hoher Implementierungsaufwand (Kosten/Zeit)
Chancen	**Risiken**
• Verbessertes Situationsbewusstsein (Situational Awareness) • Zeitgerechte Entscheidungsunterstützung • Fundament für weiteren KI-Ausbau (z. B. konkrete Entscheidungsvorschläge)	• Ethische Konflikte (Verzerrung/Diskriminierung/unklare Verantwortung) • Regulatorische Unsicherheiten (Recht/Compliance) • Psychologische Folgewirkungen (Automation Bias/Decision Fatigue) • Erweiterte Angriffsfläche (IT-Sicherheit) • Ggf. Herstellerabhängigkeit (Vendor Lock-in)

Abbildung 1: SWOT-Analyse KI-gestützter Lagedarstellung in polizeilichen Sofortlagen (eigene Darstellung)

Mit dem Betrieb eines KI-Systems vergrößert sich die Angriffsfläche im Hinblick auf die IT-Sicherheit, was die Möglichkeit von Datenlecks und Cyberangriffen steigert (BSI 2023, S. 3). Je nach konkreter Ausgestaltung des Systems könnte zudem bei langfristigem Einsatz und fehlenden Gegenmaßnahmen in der Mensch-Maschine-Interaktion eine „innere Abhängigkeit“ von der Technologie, die sogenannte Decision Fatigue, bei den Nutzenden entstehen (Stangl 2025). Zuletzt besteht die Gefahr, dass sich nachteilige Abhängigkeitsverhältnisse ergeben (vendor lockin), sofern proprietäre Systeme nicht deutscher bzw. nicht europäischer Hersteller eingesetzt werden (datacore.com 2025).

Diskussion

Die durchgeführte SWOT-Analyse identifiziert zentrale Eigenschaften von KI-Systemen, deren Relevanz für den Anwendungskontext „Lagedarstellung in polizeilichen Sofortlagen“ sich vor dem Hintergrund der eingangs dargestellten grundlegenden Bedeutung der Lagedarstellung für sämtliche wesentlichen Einsatzentscheidungen erschließt. Die identifizierten Stärken und Chancen – insbesondere die sehr hohe Verarbeitungsgeschwindigkeit, große Speicherkapazitäten, konstante Leistungsfähigkeit ohne Ermüdungseffekte sowie die parallele Verarbeitung heterogener Datenströme (Russell und Norvig 2021, Kap. 1.2; Tilawat 2025a) – dürften in der Praxis eine simultane Auswertung von Funkverkehr, Einsatzleitsystemmeldungen und Messenger-Inhalten bei gleichzeitiger Mustererkennung ermöglichen.

Demgegenüber stehen konkrete Anwendungsrisiken aus den identifizierten Schwächen und Gefahren: Systematische soziale Diskriminierungen könnten einzelne Einsatzbeteiligte beispielsweise als gefährlicher darstellen als angemessen (Bitkom e. V. 2019, S. 43). Halluzinationen können die Lagedarstellung durch nicht existente Informationen verfälschen

(nach Friedrich et al. 2024, S. 3). Feindliche Angriffe können eingesetzte Systeme gezielt manipulieren (Schweizer Eidgenossenschaft 2019, S. 29). Automation Bias begünstigt die unkritische Übernahme fehlerhafter KI-Ausgaben durch den menschlichen Anwender, sodass dieser zwar letzter Entscheider ist, de facto seine Aufsichtsfunktion jedoch nicht mehr gewissenhaft wahrnimmt und so eventuell fehlerhafte Lagedarstellungen in wichtigen Einsätzen übersieht. Ethische und rechtliche Unsicherheiten (Deutscher Ethikrat 2023) erweisen sich im Verwaltungskontext und insbesondere im Polizeibereich oftmals als K.-o.-Kriterium gegen die Einführung neuer Anwendungen, sodass eine sorgfältige Prüfung zwingende Voraussetzung zum Betrieb solcher Systeme ist.

Das trotz dieser Risiken erhebliche Potenzial verdeutlicht folgende Wirkungskette: KI-Systeme können Lagedarstellungen schneller, umfassender und vollständiger als Menschen erstellen (Russell und Norvig 2021; Tilawat 2025a; Bajwa 2025). Da hierauf zentrale Einsatzentscheidungen – Kräftedisposition, taktische Ziele, Einsatzmittel – basieren, dürfte eine qualitativ hochwertige KI-Lagedarstellung zu schnelleren und präziseren Entscheidungen mit potenziell erfolgreicherer Einsatzbewältigung, reduzierten Gefahren für Einsatzkräfte und unbeteiligte Personen sowie möglicherweise geringerem Ressourceneinsatz führen (eigene Schlussfolgerung auf Basis von Rietzke 2021, Kap. 4.1; Thorkildsen et al. 2022, Abstract). In hochdynamischen Szenarien mit Informationsüberfluss, wie etwa dem Amoklauf im OEZ 2016, könnte KI möglicherweise überhaupt erst die Generierung einer systematischen, vollständigen Lagedarstellung erlauben. Die Perspektive modularer Weiterentwicklung hin zu KI-gestützten Entscheidungsunterstützungssystemen (Ries 2025, S. 17) unterstreicht zudem das langfristige Potenzial einer KI-basierten Lagedarstellung.

Die gewählte Methode der SWOT-Analyse auf Basis systematischer Literaturrecherche erwies sich als geeignet für die strukturierte Bewertung strategischer Entscheidungsgrundlagen (Lippold 2020, S. 53). Methodische Herausforderungen ergaben sich aus der fehlenden inhaltlichen Gewichtung identifizierter Faktoren, was eine möglichst vollständige Wiedergabe erforderlich machte, detaillierte Erläuterungen im vorgegebenen Umfang jedoch verhinderte. Die Abgrenzung interner und externer Faktoren erwies sich in der Praxis als anspruchsvoll.

Die Aussagekraft dieses Beitrags unterliegt entsprechenden Einschränkungen: Der fachliche Bedarf wurde auf Basis praktischer Erfahrungen des Autors angenommen, jedoch nicht empirisch erhoben. Die technische Machbarkeit des untersuchten Systems erscheint plausibel, ist aber nicht empirisch belegt. Konkrete Gefahren und Nutzen eines KI-basierten Systems zur Lagedarstellung hängen maßgeblich von der spezifischen Umsetzung, den Einsatzbereichen und der organisatorischen Einbindung ab.

Dieser Beitrag ermöglicht einen ersten strukturierten Überblick über Möglichkeiten und Grenzen KI-gestützter Lagedarstellung. Da sie auf theoretischer Analyse basiert, können die Ergebnisse als Ausgangspunkt für weiterführende empirische Untersuchungen dienen, nicht jedoch als abschließende Machbarkeitsbewertung.

Schlussfolgerungen

Die Ergebnisse zeigen das enorme Potenzial KI-gestützter Systeme zur Lagedarstellung in Polizeieinsätzen, nach Ansicht des Autors auch über den hier betrachteten Bereich der komplexen Sofortlagen hinaus. Die geschilderten Herausforderungen sind jedoch nicht minder groß und bedürfen einer sorgfältigen Betrachtung, um ein solches System erfolgreich und in Übereinstimmung mit ethischen und rechtlichen Vorgaben einzusetzen.

Angesichts der fortschreitenden technologischen Professionalisierung von Akteuren insbesondere in den Bereichen Organisierte Kriminalität, Terrorismus, Cybercrime und hybrider Konfliktführung erscheint denkbar, dass die Komplexität einzelner, aber gleichzeitig sehr bedeutender polizeilicher Sofortlagen in Zukunft weiter zunehmen wird. KI-gestützte Lagedarstellung dürfte daher perspektivisch weiter an Relevanz gewinnen.

Für die polizeiliche Praxis können die identifizierten Faktoren zum einen als Entscheidungsgrundlage hinsichtlich der näheren Befassung mit der Thematik dienen, zum anderen als inhaltliche Anknüpfungspunkte für etwaige Umsetzungsvorhaben. Hierbei bieten sich die Einbeziehung der Angebote des KI-Campus des Bundesinnenministeriums sowie – aufgrund des theoretisch deutschlandweiten Bedarfs – eine enge Kooperation mit anderen Ländern bzw. dem Bund an.

Aus Forschungssicht und für eine etwaige praktische Umsetzung gleichermaßen wären weitere Untersuchungen sinnvoll: Zunächst sollte der fachliche Bedarf empirisch erhoben und konkretisiert werden. Darauf aufbauend bedarf es einer vertieften rechtlichen und ethischen Bewertung, der Prüfung der technischen Realisierbarkeit, der Untersuchung der Mensch-Maschine-Interaktion sowie daraus resultierender Vorgaben für das Systemdesign bzw. die organisatorische Einbindung in bestehende Prozesse. Sollte ein praktisch einsatzfähiges System vorliegen, wäre eine empirische Evaluation zur tatsächlichen Leistungsfähigkeit im Vergleich zu konventionellen (menschlichen) Methoden der Lagedarstellung wünschenswert.

Literaturverzeichnis

Bajwa, A. (2025). AI-based emergency response systems: A systematic literature review on smart infrastructure safety. *American Journal of Advanced Technology and Engineering Solutions, 1*(01), 174–200. doi.org/10.63125/xcxwpv34 (12.11.2025).

Bannenberg, B. (2018). Die Amoktat des David (Ali) Sonboly. Kriminologische Betrachtung der Tat in München am 22. Juli 2016. Gutachten für das Bayerische Landeskriminalamt. forensik.de/fileadmin/user_files/forensik/Rechtsprechung/Bannenberg_Gutachten_zu_Amoktat_M%C3%Bcnchen_2016_Bayerische_Polizei_2018.pdf (23.11.2025).

Bayerisches Staatsministerium der Finanzen und für Heimat (2025). KI-Leitfaden für Behörden im öffentlichen Dienst in Bayern. finanzministerium.bayern.de/digitalisierung/ki/KI-Leitfaden_Behoerden_2025.pdf (12.11.2025).

Bein, T. (2025). Einsatz von künstlicher Intelligenz in polizeilichen Leitstellen: Überwindung menschlicher Grenzen durch KI-basierte Systeme zur Spracherkennung und Entscheidungsunterstützung bei der Einsatzbearbeitung. Masterarbeit, Münster (20.11.2025).

Bergius, J., Wilhelm, & Six, B. (2025). Stereotyp. In: Lexikon der Psychologie. Hogrefe. dorsch.hogrefe.com/stichwort/stereotyp-stereotyp (25.10.2025).

Bitkom e. V. (2019). Blick in die Blackbox. Nachvollziehbarkeit von KI-Algorithmen in der Praxis. bitkom.org/sites/main/files/2019-10/20191016_blick-in-die-blackbox.pdf (08.11.2025).

Bitkom e. V. (2023). KI in der Polizei – Einsatzpotentiale und Lösungsansätze zur Implementierung. bitkom.org/sites/main/files/2023-10/bitkom-positionspapier-ki-polizei-einsatz-implementierung.pdf (08.11.2025).

Buder, J., Lindner, M., Oestermeier, U., Huff, M., Gerjets, P., Utz, S., & Cress, U. (2025). Generative Künstliche Intelligenz. *Psychologische Rundschau*, 76(3), 171–183. doi.org/10.1026/0033-3042/a000699 (12.11.2025).

Bundesamt für Sicherheit in der Informationstechnik (2023). *Die Lage der IT-Sicherheit in Deutschland 2023*. bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2023.pdf (16.11.2025).

Bundesministerium des Inneren (2020). PDV102. *Grafische Darstellung von Einsätzen. VS-NfD.*

Bundesministerium des Inneren (2024). PDV100. *Führung und Einsatz der Polizei. VS-NfD.*

datacore.com (2025). Break Free from Vendor Lock-in: Choose Flexibility and Innovation for Your Data. Glossary. datacore.com/glossary/vendor-lock-in/ (18.10.2025).

Deutscher Ethikrat (2023). Mensch und Maschine – Herausforderungen durch Künstliche Intelligenz. Stellungnahme. ethikrat.org/fileadmin/Publikationen/Stellungnahmen/deutsch/stellungnahme-mensch-und-maschine.pdf (03.11.2025).

Die Bundesregierung (2025). Nationale KI-Strategie der Bundesregierung. ki-strategie-deutschland.de (12.11.2025).

Döbber, F. (2025). *Datenschutz- und rechtsstaatskonforme Ansätze smarter Technologien und künstlicher Intelligenz für die Polizei* (Bd. 26). Berlin.

Endsley, M. R. (1995). Toward a Theory of Situation Awareness in Dynamic Systems. Human Factors: *The Journal of the Human Factors and Ergonomics Society, 37*(1), 32–64. doi.org/10.1518/001872095779049543 (24.11.2025).

Fraunhofer IOSB (2025). „Unsere XAI-Tools bringen Licht in die Black Box". Explainable Artificial Intelligence (XAI): Wichtiges Tool für KI-Engineering und den planbaren, systematisierten Einsatz von KI in anspruchsvollen Anwendungsfeldern. iosb.fraunhofer.de/de/geschaeftsfelder/kuenstliche-intelligenz-autonome-systeme/xai-tools-ki-engineering-interview.html (25.10.2025).

Friedrich, J.-D., Tobor, J., & Wan, M. (2024). 9 Mythen über generative KI in der Hochschulbildung. In *Diskussionspapier* (Bd. 29). Gehalten beim Hochschulforum Digitalisierung, Stifterverband für die Deutsche Wissenschaft e. V. hochschulforumdigitalisierung.de/publikationen/diskussionspapier-nr-29-9-mythen-ueber-generative-ki-in-der-hochschulbildung (25.10.2025).

Gao, J., Li, P., Chen, Z., & Zhang, J. (2020). A Survey on Deep Learning for Multimodal Data Fusion. *Neural computation*, 32(5), 829–864. doi.org/10.1162/neco_a_01273 (12.11.2025).

Haufe Akademie (2025). Generative KI. In *Glossar Data&KI*. haufe-akademie.de/blog/glossar/generative-ki (12.11.2025).

Heimann, R. (2024). *Handbuch Stabsarbeit der Polizei*: Führung und Einsatz. Stuttgart; München; Hannover; Berlin; Weimar; Dresden: Boorberg.

Heine, M., Dhungel, A.-K., Schrills, T., & Wessel, D. (2023). *Künstliche Intelligenz in öffentlichen Verwaltungen: Grundlagen, Chancen, Herausforderungen und Einsatzszenarien*. Wiesbaden; Heidelberg: Springer Gabler.

Hofinger, G., & Heimann, R. (Hrsg.) (2022). *Handbuch Stabsarbeit: Führungs- und Krisenstäbe in Einsatzorganisationen, Behörden und Unternehmen* (2. Auflage.). Berlin; Heidelberg: Springer.

Kleinschmidt, H., & Rückheim, S. (2009). *Der polizeiliche Planungs- und Entscheidungsprozess im Vergleich: Forschungsbericht* (Bd. 1/2009). Berlin: Hochschule für Wirtschaft und Recht Berlin.

Künzli, B. (2012). SWOT-Analyse: Klassisches Instrument der Strategieentwicklung mit viel ungenutzem Potenzial. *Zeitschrift Führung + Organisation*.

Lippold, D. (2020). *Die 75 wichtigsten Management- und Beratungstools: Von der BCG-Matrix zu den agilen Tools*. Berlin; Boston: De Gruyter Oldenbourg.

Ribeiro, M. T., Singh, S., & Guestrin, C. (2016). Why Should I Trust You? In: B. Krishnapuram, M. Shah, A. Smola, C. Aggarwal, D. Shen, & R. Rastogi (Hrsg.): *Proceedings of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining* (S. 1135−1144). New York, NY, USA: ACM. doi.org/10.1145/2939672.2939778 (12.11.2025).

Ries, G. (2025). *Unterstützung der Entscheidung von Polizeiführern durch KI-basierte Systeme zur Datenanalyse. VS-NfD*. Masterarbeit, Frankfurt am Main.

Rietzke, E. (2021). *Modellierung, Visualisierung und Ausführung wissensintensiver Prozesse unter Verwendung Semantischer Technologien*. Trier: Universität Trier.

Russell, S. J., & Norvig, P. (2021). *Artificial intelligence: a modern approach* (Fourth Edition). Hoboken, NJ: Pearson.

Schweizer Eidgenossenschaft (2019). *Herausforderungen der künstlichen Intelligenz. Bericht der interdepartementalen Arbeitsgruppe »Künstliche Intelligenz« an den Bundesrat*. https://www.kmu.admin.ch/dam/de/sd-web/XIDPoOD3jfSk/herausforderungen-der-kuenstlichen-intelligenz.pdf (12.11.2025).

Stangl, W. (2025). Decision Fatigue. In: *Lexikon für Psychologie und Pädagogik*. lexikon.stangl.eu/7608/abulie (09.11.2025).

Thorkildsen, Z., Wohl, E., Bryson, B., Lafferty, J., & Dockstader, J. (2019). Common Operational Picture Technology in Law Enforcement: Three Case Studies. Office of Justice Program. National Criminal Justice Reference Service. cna.org/reports/2019/12/irm-2019-u-022450-final.pdf (18.10.2025).

Thorkildsen, Z., Wohl, E., Bryson, B., Lafferty, J., & Dockstader, J. (2022). *Common Operational Picture Technology in Law Enforcement: Three Case Studies*, Baton Rouge, Louisiana, Camden County, New Jersey, Chicago, Illinois, 2015−2019. ICPSR − Interuniversity Consortium for Political and Social Research. doi.org/10.3886/ICPSR37582.v1 (12.11.2025).

Tilawat, M. (2025a). Was ist Datenfusion? KI-Glossar. allaboutai.com/de-de/ki-glossar/datenfusion (18.10.2025).

Tilawat, M. (2025b). Kontinuierliches Lernen. KI-Glossar. allaboutai.com/de-de/ki-glossar/lebenslanges-lernen-in-ki/ (18.10.2025)

Wirtz, M. (2025). Kognitive Fehler. In: *Lexikon der Psychologie*. Hogrefe. dorsch.hogrefe.com/stichwort/stereotyp-stereotyp (25.10.2025).

Wu, A., Wang, Y., Shu, X., Moritz, D., Cui, W., Zhang, H., et al. (2021). *AI4VIS: Survey on Artificial Intelligence Approaches for Data Visualization*.

Zhang, Y., Li, Y., Cui, L., Cai, D., Liu, L., Fu, T., et al. (2025, September 16). Siren's Song in the AI Ocean: A Survey on Hallucination in Large Language Models. arXiv. doi.org/10.48550/arXiv.2309.01219 (12.11.2025).

Künstliche Intelligenz: Betrachtung des Einsatzes von Multi-Agenten-Systemen in der öffentlichen Verwaltung

Bastian Blum

Bisherige Megatrends des technologischen Fortschritts wie Künstliche Intelligenz (KI) oder die Digitalisierung werden im Jahr 2025 weiterhin als Bestandteil einer der elf Megatrends wahrgenommen, auch wenn sie inzwischen unter dem neuen Megatrend Konnektivität gefasst werden (Zukunftsinstitut 2025). Auch die öffentliche Verwaltung mit dem Fachbereich Polizei ist mit Megatrends und ihren gesamtgesellschaftlichen Folgen konfrontiert (Markus und Meuche 2022, 10). Bei der KI, Artifical Intelligence (AI) in Englisch (Dyck 2025, 11), gab es in den letzten Jahren zunehmend Fortschritte. So liegen die Ursprünge für die ersten Rechenmaschinen bei den ersten Informatikern Leibniz, Zuse und von Neumann (Spitzer 2025, 76), aber erst durch „[…] die Kombination aus leistungsstarker Architektur, umfangreichen Trainingsdaten und hohen Parameterzahlen […]“ (Leible et al. 2024, 350) ist die KI letztlich in Gestalt von generativer KI und Large Language Models (LLMs) mit GPT-4 oder Gemini im Jahr 2023 ins Interesse einer breiten Öffentlichkeit getreten (Leible et al. 2024, 346–349). Jüngst wird von KI-Agenten, beispielsweise mit AlphaEvolve (Novikov et al. 2025) im Jahr 2023, gesprochen und bereits „Microsoft Build 2025 läutet das Zeitalter der KI-Agenten ein“ (Shaw 2025). Bei Agenten handelt es sich um KI, die zu eigenständigen Entscheidungen und zu letztlich selbstständigen Aktionen, wie beispielsweise der Anpassung eines Produktionsprozesses zur Effizienzsteigerung, fähig ist (Dyck 2025, 50). Daraus kann die Hypothese gebildet werden, dass der Megatrend Konnektivität mit den Möglichkeiten dieser KI-Agenten auch der Polizei von Nutzen sein könnte. So wäre möglicherweise anderen Megatrends, wie dem Fachkräftemangel im Rahmen der demografischen Entwicklung (Markus und Meuche 2022, 13) oder Auswirkungen der Digitalisierung, besser zu begegnen. Die daraus ableitbare Frage ist, ob sich diese Hypothese mit einer wissenschaftlichen Methode systematisch analysieren und darstellen lässt.

Das Ziel des Beitrags ist die Betrachtung des Einsatzes von KI-Agenten in der öffentlichen Verwaltung im Hinblick auf die konkreten Stärken, Schwächen, Chancen und Risiken sowie die Schlussfolgerung, welchen konkreten Herausforderungen damit begegnet werden kann, aber auch, welche möglicherweise auftretenden Einschränkungen dabei beachtet werden sollten.

Hintergrund

Um die Einsatzmöglichkeiten von KI-Agenten in der öffentlichen Verwaltung näher zu beleuchten, werden denkbare Trends bzw. Megatrends sowie Herausforderungen innerhalb der öffentlichen Verwaltung skizziert, das Themenfeld KI im historischen und aktuellen Kontext eingeordnet und abschließend die KI-Agenten dargestellt. Reduziert lässt sich ein Trend wie folgt definieren: „Ein Trend ist ein theoretisches Konstrukt, das sich durch eine ‚vereinfachende Beschreibung einer übergreifenden Entwicklung, die sich aus den Wechselwirkungen eines inhaltlichen Kerns mit seiner Umwelt ergibt und über einen für den jeweiligen Kontext relevanten Zeitraum anhält‘ auszeichnet“ (Keicher et al. 2021, 5). Darüber hinaus charakterisiert das sogenannte Zukunftsinstitut einen Megatrend dadurch, dass er über eine Dauer von mehreren Jahrzehnten anhält, Auswirkungen auf alle gesellschaftlichen Bereiche

hat, sich global auswirkt und komplex ist (Zukunftsinstitut 2025). In einer Umfrage des KI-Campus, einer Lernplattform des Stifterverbands für KI, wurde bei Personen aus Politik und öffentlicher Verwaltung, Wirtschaft, Wissenschaft und Zivilgesellschaft die Bedeutsamkeit verschiedener Megatrends in den nächsten zehn Jahren erhoben. Überschneidend werden KI, Klimawandel, Digitalisierung, Demokratische Kultur und Desinformation als die fünf bedeutsamsten Megatrends genannt (KI-Campus 2025). Als Herausforderungen für die öffentliche Verwaltung für die kommenden Jahre und Jahrzehnte werden die Globalisierung, der demografische Wandel, Migration, Fachkräftemangel und Digitalisierung genannt (Möltgen-Sicking et al. 2019, 328–337). Eine Begriffsdefinition für Digitalisierung diskutieren Denkhaus sowie Falkhofen, bevor sie ausführen: „Im Sinne einer pragmatischen Annäherung kann mit ‚Digitalisierung' ein Prozess beschrieben werden, der im Wesentlichen auf der intelligenten Vernetzung von Prozessketten und einer durchgängigen Erfassung, Aufbereitung, Analyse und Kommunikation von Daten beruht" (Seckelmann 2024, 50–51). Es werden also analoge Informationen zu nutzbaren, digitalen Daten gemacht. „Künstliche Intelligenz bezeichnet die Nachbildung menschlicher Fähigkeiten durch IT-Systeme, vor allem in den Bereichen des Wahrnehmens, des Verarbeitens natürlicher Sprache, des Schlussfolgerns, des Lernens und des Vorausplanens" (Bundesministerium für Wirtschaft und Energie 2019, 5).

Die Grundgedanken der Künstlichen Intelligenz gehen zurück auf die Beschreibung der ersten modernen Computer 1936 nach Turing in Gestalt der Computing Mashines, die vereinfacht dargestellt in der Lage sein sollten, nach einer festgelegten Konfiguration selbstständig eine Ausgabe zu generieren (Turing 1936, 232). Ähnlich beschreibt es auch der Begriff Algorithmus mit „[…] eine eindeutige Handlungsvorschrift, um ein vorab definiertes Problem zu lösen. […]

Ein algorithmisches System […] setzt sich aus einem oder mehreren Algorithmen zusammen […]" (Kalogeropoulos et al. 2025, 5). In einer Studie 1955 beschreibt McCarthy die mögliche Fähigkeit von Maschinen zur AI: „The study is to proceed on the basis of the conjecture that every aspect of learning or any other feature of intelligence can in principle be so precisely described that a machine can be made to simulate it. An attempt will be made to find how to make machines use language, form abstractions and concepts, solve kinds of problems now reserved for humans, and improve themselves" (McCarthy et al. 2006). 2018 stellt Döbel den Begriff KI wie folgt dar: „Künstliche Intelligenz ist ein Teilgebiet der Informatik mit dem Ziel, Maschinen zu befähigen, Aufgaben ‚intelligent' auszuführen. Dabei ist weder festgelegt, was ‚intelligent' bedeutet, noch welche Techniken zum Einsatz kommen" (Döbel et al. 2018, 8). Für die weitere Befassung wird KI definiert als „das Nachahmen menschlichen Denkens durch Maschinen, im speziellen durch Computersysteme" (Winkler et al. 2025, 25). Unterbegriffe zur KI sind das Maschinelle Lernen (ML), tiefergehende Lernprozesse (TL) und die generative KI (GKI). Beim ML werden Daten und Algorithmen genutzt, um selbstständig zu lernen. Im TL versuchen Computer, wie das menschliche Gehirn zu arbeiten. Bei GKI nutzen Algorithmen sogenannte Prompts und bestehende Daten, um neue Inhalte zu generieren (Winkler et al. 2025, 25). Prompts sind textuelle Eingaben, auf denen die Verarbeitung basiert (Bundesamt für Sicherheit in der Informationstechnik 2025, 2). Gemäß EU AI Act ist ein „KI-System: ein maschinengestütztes System, das so konzipiert ist, dass es mit unterschiedlichem Grad an Autonomie betrieben werden kann und nach seiner Einführung Anpassungsfähigkeit zeigt, und das für explizite oder implizite Ziele aus den Eingaben, die es erhält,

ableitet, wie es Ausgaben wie Vorhersagen, Inhalte, Empfehlungen oder Entscheidungen generieren kann, die physische oder virtuelle Umgebungen beeinflussen können; […]“ (Verordnung (EU) 2024/1689, Art. 3 Nr. 1).

Überdies wird zwischen schwacher und starker KI unterschieden. „Starke KI-Systeme sollen die gleichen intellektuellen Fähigkeiten (u. a. logisches Denkvermögen, Kreativität, Entscheidungs-, Planungs- und Lernfähigkeit) wie der Mensch besitzen oder diese sogar übersteigen, während schwache KI konkrete Lösungen für bestimmte Probleme bereitstellt, die auf Methoden der Mathematik und Informatik basieren und zunehmend in der Lage sind, sich selbst zu optimieren“ (Giering 2022, 53). Eine merkliche Leistungszunahme erlangte KI spätestens 1997, als der Schachcomputer Deep Blue den Schachgroßmeister Garri Kasparow schlug (Campbell et al. 2002, 59). Eine signifikante Verbesserung beim Lernverhalten von KI und in der Bilderkennung wurde mit dem Modell Alexnet 2012 erzielt (Krizhevsky et al. 2017, 84). Als weiterer Meilenstein in der Entwicklung wird der Sieg von AlphaGo über den südkoreanischen Go-Spieler Lee Sedol 2016 angesehen (Silver et al. 2016).

2023 verzeichneten die Large Language Models (LLM), die großen Sprachmodelle, eine Leistungszunahme (Leible et al. 2024, 349–350). Wir befinden uns trotz der aktuellen Entwicklung weiter im Bereich der schwachen KI (Winkler et al. 2025, 24). Ein KI-Agent kann in seiner einfachsten Form beschrieben werden mit: „An agent is anything that can be viewed as perceiving its environment through sensors and acting upon that environment through actuators“ (Russell und Norvig 2022, 54). Dies ergänzen zwei Autoren: Ein Agent sollte sich weiter durch eine Wechselwirkung mit seiner Umgebung, durch Autonomie in der Wahl seiner Handlung, durch die Fähigkeit zu Schlussfolgerungen und der Reaktion auf Veränderungen seiner Umgebung sowie ein vorausschauendes Verhalten auszeichnen. Überdies soll er trotz seiner Autonomie mit anderen Akteuren zur Zielerreichung interagieren (Balaji und Srinivasan 2010, 2–3). Eine Steigerung dieser Agenten sind sogenannte Multi-Agent-Systeme (MAS), auch Cooperativ Distributed Problem-Solving. Diese erklärt Sycara 1998 auf Grundlage von Durfee aus 1989: „Cooperative Distributed Problem-Solving [.] studies how a loosely coupled network of problem solvers can work together to solve problems that are beyond their individual capabilities“ (Durfee et al. 1989, 1). „The characteristics of MASs are that (1) each agent has incomplete information or capabilities for solving the problem and, thus, has a limited viewpoint; (2) there is no system global control; (3) data are decentralized; and (4) computation is asynchronous“ (Sycara 1998, 80).

Die aktuelle Entwicklung zu MAS kann so eingeordnet werden, dass „[…] die Grundlagen für agentenbasierte Systeme nicht neu sind, aber die jüngsten Fortschritte in der generativen KI – insbesondere bei den großen Sprachmodellen (LLMs) – diesen Konzepten zu neuem Leben und ungeahnten Fähigkeiten verhelfen. Durch die Fähigkeit der Agenten, zu reflektieren, zu planen und Tools zu nutzen, können sie nun Aufgaben bewältigen, die bisher unerreichbar schienen“ (Siebert 2025). Der sogenannte Gartner Hype Cycle für neue Technologien prognostiziert 2025, dass „[…] die Weiterentwicklung der agentenbasierten KI-Produkte, Dienstleistungen und Anwendungsfälle transformieren wird, indem sie autonome Abläufe, erweiterte Führung, Maschinenkunden und selbstanpassende Produkte zu einer vollständig programmierbaren Wirtschaft zusammenführt“ (Stephan 2025, 424).

Methodik

Ziel dieses Beitrags ist es, die Möglichkeiten von KI-Agenten in der öffentlichen Verwaltung systematisch zu analysieren und darzustellen. Als methodisches Instrument soll SWOT genutzt werden. „Die SWOT-Analyse wurde bereits in den 1960er-Jahren an der Harvard Business School entwickelt. Anhand der Analyse des Ist-Zustandes kann die Positionierung des eigenen Unternehmens oder der eigenen Einheit festgestellt werden. Danach kann eine Strategieentwicklung mit den erforderlichen Maßnahmen in die Wege geleitet werden“ (Gerlach 2023, 201). Der Begriff SWOT steht als Akronym für „Strengths – Stärken, Weaknesses – Schwächen, Opportunities – Chancen, Threats – Risiken“ (Gerlach 2023, 201). Dem entgegen wird SWOT beschrieben mit: „Die SWOT ist das Instrument, welches in der Praxis mangels Kenntnis am häufigsten falsch eingesetzt wird. Sie ist kein Analyseinstrument, sondern eine Methode der Ordnung und Zusammenfassung. Durch sie wird die Transparenz über die wesentlichsten Erkenntnisse aus einem intensiven Analyseprozess erhöht. Der Leser erhält ein durchgehendes Beispiel, welches ihm die vier Perspektiven aufzeigt, anhand derer die Ergebnisse der strategischen Ausgangslage strukturiert werden“ (Kaufmann 2021, 289). Kaufmann führt dazu weiter aus: „Daher ist es notwendig und sinnvoll, die wichtigsten Erkenntnisse über die Ist-Situation des Unternehmens in einer Vier-Felder-Matrix nochmals übersichtlich zusammenzuführen“ (Kaufmann 2021, 290). Damit schließe sich der Kreis zur ersten Darstellung von SWOT, die ebendiese Vier-Felder-Matrix darstelle. Diese besteht aus: „Die Innensicht auf die Stärken und Schwächen des Unternehmens [sic!]. Die oberen beiden Felder Strenghts and Weaknesses fassen die wichtigsten Resultate aus der Analyse des Unternehmens zusammen und beantworten damit die Frage: Welche relevanten Stärken und Schwächen des Unternehmens haben die durchlaufenen Analysen […] enthüllt? Die Außensicht auf die Chancen und Risiken aus dem Umfeld [sic!]. Die beiden unteren Felder Opportunities und Threats bilden die wichtigsten Resultate aus der Analyse des Umfeldes des Unternehmens ab […] und zeigen komprimiert auf, welchen konkreten Chancen und Risiken das Unternehmen durch sein Umfeld ausgesetzt ist“ (Kaufmann 2021, 290). Es bleibt festzustellen, dass für beide Sichtweisen von SWOT eine Analyse des IST-Zustandes oder der Ausgangslage notwendig ist.

„Unter Ist-Zustand ist die Analyse der aktuellen Situation zu verstehen. Die präzise und möglichst wertungsfreie Zusammenstellung aller betriebswirtschaftlich relevanten Daten und Fakten sind Grundlage des Konzeptes und Voraussetzung für die Messbarkeit von Veränderungen im Unternehmen. Der Ist-Zustand wird durch Dokumentenanalyse […] ermittelt“ (Collin 2010). In den Beschreibungen bezieht sich die IST-Analyse und SWOT auf Unternehmen, aber: „SWOT-Analysen können darüber hinaus auch in der Produktentwicklung, der Prozessentwicklung, zu Evaluationszwecken oder zur Lösungsfindung konkreter Fragestellungen u. v. m. angewandt werden“ (Bundesministerium des Innern 2025). Schlussfolgernd kann diese Vorgehensweise auf den Kontext der Fragestellung adaptiert werden. Hierzu wird im Sinne einer Dokumentenanalyse eine literaturgestützte IST-Analyse durchgeführt. Dazu wird Literatur mit Bezug zur Anfangszeit der Künstlichen Intelligenz bis in die heutige Zeit analysiert. Die Analyseergebnisse werden in der Folge mithilfe der vier SWOT-Bestandteile geordnet und dargestellt. Dieser Beitrag befasst sich dabei lediglich mit der Analysephase und deren Aufbereitung durch SWOT, wobei SWOT hier in abgewandelter Form auf die KI-Agenten bezogen wird. Eine Strategieentwicklung oder die Herausarbeitung von Handlungsfeldern ist kein Teil dieses Beitrags.

Ergebnisse

Eine Stärke von KI-Systemen dürfte ihre Leistungsfähigkeit sein. Bereits schlichte algorithmische Systeme zur Durchführung von mathematischen Operationen können Ergebnisse regelmäßig schneller und zuverlässiger produzieren als der Mensch (Kreyßing 2025, 62). Dies gilt entsprechend auch gesteigert für die Leistungsfähigkeit „nächsthöherer Entwicklungsstufe[n] von KI“ (Kreyßing 2025, 27). Dabei kann die Rechenleistung und damit die Leistungsfähigkeit skaliert werden, sodass die KI an ihre Aufgabe angepasst werden kann (Dyck 2025, 47). KI kann sich wiederholende Aufgaben in Prozessen schneller und effizienter erledigen als der Mensch, wodurch Prozesse durch KI automatisiert werden können (Dyck 2025, 39). KI-Agenten können, abgestimmt auf verschiedene Teilprozesse, hin zu einem Gesamtprozess zusammenarbeiten (Immich 2025). Überdies leistet KI die Analyse historischer Daten, erkennt Folgen und kann Alternativen vorschlagen, sie kann daher zur optimierten Entscheidungsfindung dienen und in der Folge auch in Echtzeit Entscheidungen treffen und Parameter anpassen (Dyck 2025, 50). Das Nichtvorhandensein von Gefühlen oder Moral kann, je nach gewünschter Objektivität, als Stärke angesehen werden (Kreyßing 2025, 90). „[…] KI-Systeme sind [.] nicht zum moralischen Handeln – im umfassenden und herkömmlichen Sinne − fähig [.]“ (Kreyßing 2025, 90). Grundsätzlich kann sie die menschliche Intelligenz nicht abbilden, „[…] die sich durch Empathie, Gefühle, Sinn, Intention und Vorsatz auszeichnet“ (Dyck 2025, 15). Dies kann aber ebenso als Schwäche von KI gewertet werden. Denn Technologie denkt nicht, sie kann nicht verantwortlich sein: „Ein Mensch in diesem Unternehmen wird für diese Handlungen verantwortlich und rechenschaftspflichtig gemacht werden“ (Belcic und Stryker 2025). Dies wird anschaulich durch das Gedankenexperiment des sogenannten chinesischen Zimmers.

Darin beschreibt der Autor, dass er zwar einen Input mit chinesischen Schriftzeichen, nach einer Zeit des Lernens mit einer Übersetzung, in einen korrekten Output mit solchen Schriftzeichen verwandeln kann und dies wie Denken scheinen kann, ohne tatsächlich ein solches zu sein (Searle 1980, 424). Divergentes Denken in der Form, wie es Menschen beherrschen, ist für KI-Systeme gegenwärtig nicht möglich. Menschliches Denken, das auch von Emotionen, Spontanität geprägt ist, ist nicht mit der Funktionsweise von Algorithmen gleichzusetzen (Kreyßing 2025, 92). Dazu existiert nach Kreyßing auch eine Gegenmeinung (Maamar 2021).

Ebenso ist KI unfähig zur Kontextualisierung, also Entscheidungen oder vorgesehene Handlungen mit den Rahmenbedingungen und der Lebenswirklichkeit übereinzubringen, zu reflektieren und abzuwägen (Kreyßing 2025, 93). Eine weitere Schwäche von KI ist, gerade bei der Systemkomplexität etwa von MAS, das Bias. Dieser Begriff wird im Bereich KI im Kontext der technisch und menschlich induzierten Bias verwendet. So handelt es sich bei technisch bedingten Bias um unerwünschte Verzerrungen, wonach beispielsweise, verursacht durch unausgewogene Trainingsdaten, ein Geschlecht beim Gender-Bias strukturell diskriminiert wird. Menschliche Bias können durch Werteeinstellungen der Programmierer selbst entstehen, die die Algorithmen und Trainingsdaten entsprechend prägen. Selbst ein repräsentatives Abbild der Realität in den Trainingsdaten gewährleistet infolge systemimmanenter Verzerrungen kein diskriminierungsfreies oder sonstig fehlerfreies KI-System (Kreyßing 2025, 75–80). Die Schwäche Bias könnte auch als Risiko im Sinne von SWOT gedeutet werden. Ein weiteres Risiko ist, dass es ferner nur schwer nachvollziehbar ist, auf welchen Annahmen und unter welchen Prämissen eine Entscheidung eines KI-Systems zustande kommt

(Kreyßing 2025, 80). Auch wenn die verwendeten KI-Systeme auf verhältnismäßig einfachen Methoden basieren (Datenethikkommission der Bundesregierung 2019, 61), „so verwendet beispielsweise das Natural-Language-Processing-Modell namens GPT-3 rund 175 Milliarden Parameter (Brown et al. 2020, 8) oder das Sprachmodell von Google PaLM rund 540 Milliarden Parameter (Narang und Chowdhery 2025, 2025)“ (Kreyßing 2025, 84). Daraus ergibt sich: „Wie KI zu den Lösungen findet und weshalb das System bestimmte Antworten gibt, ist selbst für die Experten nicht vollständig nachvollziehbar. Damit besteht ein Dilemma, dass sich die Berechnungen und Ergebnisse der KI nicht abschließend erklären lassen“ (Dyck 2025, 15). Dies wird auch als Blackbox bezeichnet (Kreyßing 2025, 113). Ferner dürfte ein hinreichend komplexes KI-System auch in sich eine Systemanfälligkeit und einen Wartungsaufwand beinhalten. Daraus kann sich ein kaum abschätzbares Fehlerpotenzial ergeben, was enorme Auswirkungen auf einzelne Personen oder die Gesellschaft haben kann (Kreyßing 2025, 97).

Bei der Einführung von KI im Arbeitsalltag könnten durch fehlende Technologieakzeptanz und Vertrauen Widerstände entstehen (Engelmann und Puntschuh 2020, 19).

Gerade hinsichtlich des Vertrauens könnte man durch die interaktive Einbindung eines menschlichen Amtswalters (Official-in-the-Loop), die Überprüfung und Kontrolle des KI-Systems durch menschliche Amtswalter (Official-on-the-Loop) oder die Gesamtsteuerung durch menschliche Amtswalter (Official-in-Command) den Menschen als Entscheider einführen (Guckelberger 2019, 484–532). Die Nachvollziehbarkeit der Algorithmen könnte durch sogenannte Greybox-Modelle, das sind partiell transparente und nachvollziehbare Modelle und Whitebox-Modelle, also Modelle, deren Systemarchitektur und entscheidungsrelevanten Gründe mit geringem Aufwand nachvollzogen werden können, verbessert werden (Kreyßing 2025, 81–83). Dadurch könnten trotz Risiken auch Chancen ermöglicht werden. Mehrere KI-Systeme könnten verschiedene spezialisierte Aufgaben und Rollen wahrnehmen. Beispielsweise hat ein Unternehmen ein Multi-Agent-System entwickelt, welches als Produktentwicklungsteam Software entwickelt (Immich 2025). Diese werden dazu von einem übergeordneten Agenten orchestriert, also sozusagen verbunden (Kargwal 2025). Obwohl KI Rechenleistung benötigt, um zu arbeiten, funktioniert sie gleichzeitig auch mit geringer Bandbreite im Netzwerk und wird zunehmend günstiger (Belcic und Stryker 2025). KI-Systeme können Daten analysieren und Muster erkennen, und der Mensch interpretiert diese im Kontext und durchdenkt unvorhergesehene Ereignisse (Dyck 2025, 39). „Neben der Prozessoptimierung für bestehende Abläufe können mithilfe von KI-Systemen auch neue Prozesse und Abläufe initiiert werden, die wiederum zu einer höheren Servicequalität führen“ (Spellerberg et al. 2021, 30). So könnten KI-Systeme für bestimmte Einsatzfelder in der Verwaltung konzipiert werden und die entstehenden Expertensysteme zu einer höheren Akzeptanz in der Verwaltungsentscheidung führen als bei klassischen, menschlichen Entscheidungen (Kreyßing 2025, 63). Hierbei könnten Agenten mit verschiedenen Blickwinkeln die Qualität des Bearbeitungsprozesses verbessern, indem sie in ihrer Rolle arbeiten und ihren individuellen Beitrag zu einem Auftrag leisten (IBM 2025).

Diskussion

Überschneidend werden Künstliche Intelligenz, Klimawandel, Digitalisierung, Demokratische Kultur und Desinformation als die fünf bedeutsamsten Megatrends genannt (KI-Campus 2025). „Überdies können (Mega-)Trends sich überlagern, gegenseitig beeinflussen oder bedingen und sie haben Wechselwirkungen untereinander sowie mit der Umwelt. Zudem können entgegengesetzte Trends parallel existieren“ (Keicher et al. 2021, 6). Dies könnte beispielsweise für das Verhältnis zwischen den Megatrends Digitalisierung und Künstliche Intelligenz gelten.

Für die öffentliche Verwaltung bedeutsam werden Globalisierung, der demografische Wandel, Migration, Fachkräftemangel und Digitalisierung genannt (Möltgen-Sicking et al. 2019, 328–337). Gerade dem demografischen Wandel, dem Fachkräftemangel, aber auch der Migration könnte durch die Möglichkeiten der Digitalisierung begegnet werden. Nachdem 2022 ChatGPT veröffentlicht wurde und 2023 im Zeichen der KI stand, setzte sich diese Entwicklung 2024 durch bessere, schnellere und günstigere Systeme fort. Für das Jahr 2025 wurden mehr und bessere KI-Agenten erwartet (Pillay und Booth 2025). Heute können KI-Agenten bereits Daten auswerten, Muster erkennen und einfache Abläufe teilweise automatisiert abwickeln (Belcic und Stryker 2025). Durch den Einsatz von KI-Systemen in der öffentlichen Verwaltung können knappe Personalressourcen durch Automatisierung von Routinetätigkeiten entlastet und Tätigkeiten der Beschäftigten auf anspruchsvollere fachliche Aufgaben verlagert werden, was angesichts des prognostizierten Fachkräftemangels sowie im Hinblick auf Motivation und Arbeitszufriedenheit der Beschäftigten besonders bedeutsam ist. Zudem besteht ein Potenzial zur Schonung finanzieller Ressourcen, da etwa im Forderungsmanagement durch durchgängig automatisierte Bearbeitung, KI-gestützte Kommunikation mit Schuldnern und abgesenkte Wertgrenzen für die Niederschlagung von Kleinbeträgen zusätzliche Einnahmen realisiert werden können, während zugleich die Kosten je Vorgang sinken. Insgesamt könnten durch optimierte KI-basierte Workflows sowohl Personal- als auch Geldmittel effizienter genutzt werden (Kreyßing 2025, 69–71). Ob dabei MAS ein Ansatz sein könnten, kann auf fünf Fragen reduziert werden: Kann das Problem in verschiedene Schritte zerlegt werden? Benötigt man separate Entitäten, um jedes Problem separat zu lösen? Sind diese Entitäten in gewissem Sinne autonom? Wie werden diese Entitäten interagieren, um das Problem zu lösen? Müssten dynamische Entitäten hinzugefügt oder entfernt werden? (Siebert 2025). Entitäten sind eindeutig bestimmbare Attribute, wie Personen, Objekte oder eben auch (KI-)Software, innerhalb einer Domäne. Eine Domäne beschreibt dabei einen Wertebereich, also das Umfeld. Entitäten sind alle Dinge, die den Regeln dieser Domäne unterliegen bzw. für deren Funktionieren relevant sind (Anke 2025, 7). Allerdings fehlen für wirklich autonome Systeme, die selbstständig komplexe Entscheidungen treffen, noch große Fortschritte beim Kontextverständnis und beim Umgang mit Sonderfällen. Für einfache Aufgaben wählen Agenten zuverlässig passende Werkzeuge, bei schwierigen, anspruchsvollen Szenarien stößt die Technik aber noch an Grenzen (Belcic und Stryker 2025). Dennoch verbessern KI-Systeme gerade den einfachen Verwaltungsservice, indem sie Wartezeiten durch kluge Terminbuchung und schnellere Abläufe verkürzen. Eine zentrale KI-Hilfe leitet Anfragende einfach und autonom sowie ohne Zuständigkeitsfragen durch Verfahren.

Chatbots beraten rund um die Uhr mehrsprachig und in einfacher Sprache. Das Prinzip, Daten nur einmal abzugeben, spart Aufwand bei Anträgen und lässt Personal für schwierige Fälle frei bzw. entlastet grundsätzlich Personal (Kreyßing 2025, 66–68). Interpretiert man die Ergebnisse, so könnten KI-Agenten inzwischen die Fähigkeit erlangt haben, die beispielhaft aufgeführten Verbesserungen in der öffentlichen Verwaltung herbeizuführen, wenn auch nicht in allen Bereichen. Allerdings sind die Ergebnisse im Rahmen dieses Beitrags aber auch Limitationen unterworfen. Die Thematik ist einer Schnelllebigkeit ausgesetzt, wodurch Ergebnisse in kurzen Abständen bereits überholt sein können. Damit einhergehend laufen auch Wissensquellen Gefahr, schnell veraltet sein zu können. Die Themenfülle, so beispielsweise eine ethische oder rechtliche Betrachtung, kann im Rahmen dieses Beitrags nicht umfassend abgedeckt werden.

Schlussfolgerung

Die Ergebnisse von SWOT lassen die Interpretation zu, dass mithilfe der Stärken und Chancen von MAS wesentlichen Herausforderungen aus den Trends begegnet werden könnte, aber eben auch Schwächen und Risiken bestehen. Auch bestehen infolge der fortlaufenden Entwicklung Unwägbarkeiten, womit Zukunftsszenarien letztlich nur antizipiert werden können. Zeichnet man eine Dystopie, so könnten Agenten-Systeme haushälterisch, rechtlich und/oder ethnisch nicht umsetzbar, auf keine Akzeptanz stoßen, zu risikobehaftet oder nicht in bestehende IT-Landschaften integrierbar sein. Stellt man dieser Prognose eine Utopie gegenüber, so könnten KI-Systeme in allen Bereichen noch besser werden, Fachkräfte durch zielgerichtete Unterstützung effizienter machen und durch verlässliche Simultanübersetzung Sprachbarrieren kompensieren. Der demografische Wandel könnte, durch Auslagerung von bisher menschenbedienten Prozessen, abgeschwächt und die öffentliche Verwaltung letztlich insgesamt gestärkt werden. Fusioniert man beide Zukunftsszenarien zu einem Beispiel, so könnte ein bezahlbares und tatsächlich umsetzbares MAS erschaffen werden, das infolge einer einfachen Zugänglichkeit auf Akzeptanz stieße. Der erste Agent könnte im Dialog dem wenig technikaffinen Mitarbeitenden in einer beliebigen Sprache assistieren, einen Urlaubsantrag digital einzureichen. Was paradox klingen mag, könnte trotzdem fruchten: Es erscheint wesentlich einfacher, einen Prompt zum Einreichen eines Urlaubsantrags zu formulieren und diesen Auftrag automatisiert bearbeiten zu lassen, als in einer Software die entsprechenden Einzelschritte abzuarbeiten. Danach würden verschiedene Agenten kollaborieren, von der rechtlichen Prüfung bis hin zur Dienstplangestaltung und den Entscheidungen über die Verteilung der infolge des Urlaubs perspektivisch nicht bearbeiteten Arbeitsvorgänge. Letztlich würde das Ergebnis des MAS einem menschlichen Entscheider vorgelegt, der die finale Entscheidung treffen könnte. Dieses skizzierte Beispielszenario erscheint fast beliebig modifizierbar.

So darf, auf die Forschungsfrage Bezug genommen, geschlossen werden, dass mit dem Einsatz von MAS durchaus konkreten Herausforderungen im Sinne der Megatrends begegnet werden könnte, auch wenn deren Einsatz mit Einschränkungen verbunden ist. Daraus bieten sich Chancen für eine Anschlussfähigkeit.

So könnten die Bereiche rechtliche und ethische Umsetzbarkeit in einer separaten Arbeit intensiver betrachtet werden, um mögliche Einschränkungen näher zu beleuchten. Der skizzierte Beispielprozess eines Urlaubsantrags wäre im Rahmen einer Analyse, beispielsweise durch Übertragung in ein Swimlane-Diagramm, näher untersuchbar. Hinsichtlich einer umfangreicheren Arbeit böte sich eine Machbarkeitsstudie hinsichtlich des Einsatzes von KI-Agenten in der öffentlichen Verwaltung an.

Literaturverzeichnis

Anke, Jürgen (2025). Digitale Identitäten und Nachweise. Lösungsansätze für vertrauenswürdige Interaktionen zwischen Menschen, Unternehmen und Verwaltung. Wiesbaden, Springer Nature; Springer Fachmedien Wiesbaden Imprint.

Balaji, Parasumanna Gokulan/Srinivasan, Dipti (2010). An Introduction to Multi-Agent Systems. In: Janusz Kacprzyk/Dipti Srinivasan/Lakhmi C. Jain et al. (Hrsg.): Innovations in multi-agent systems and applications. Berlin, Springer, 1–27.

Belcic, Ivan/Stryker, Cole (2025). KI-Agenten im Jahr 2025: Erwartungen vs. Realität. Online verfügbar unter ibm.com/de-de/think/insights/ai-agents-2025-expectations-vs-reality (abgerufen am 26.11.2025).

Brown, Tom/Mann, Benjamin/Ryder, Nick/Subbiah, Melanie/Kaplan, Jared/Dhariwal, Prafulla/Neelakantan, Arvind/Shyam, Pranav/Sastry, Girish/Askell, Amanda/Agarwal, Sandhini/Herbert-Voss, Ariel/Krueger, Gretchen/Henighan, Tom/Child, Rewon/Ramesh, Aditya/Ziegler, Daniel M./Wu, Jeffrey/Winter, Clemens/Hesse, Christopher/Chen, Mark/Sigler, Eric/Litwin, Mateusz/Gray, Scott/Chess, Benjamin/Clark, Jack/Berner, Christopher/McCandlish, Sam/Radford, Alec/Sutskever, Ilya/Amodei, Dario (2020). Language Models are Few-Shot Learners. Online verfügbar unter arxiv.org/pdf/2005.14165 (abgerufen am 04.12.2025).

Bundesamt für Sicherheit in der Informationstechnik (2025). Generative KI-Modelle: Chancen und Risiken für Industrie und Behörden. Online verfügbar unter bsi.bund.de/SharedDocs/Downloads/DE/BSI/KI/Generative_KI-Modelle.html (abgerufen am 18.11.2025).

Bundesministerium des Innern (2025). SWOT-Analyse. Online verfügbar unter orghandbuch.de/Webs/OHB/DE/OrganisationshandbuchNEU/4_MethodenUndTechniken/Methoden_A_bis_Z/SWOT_Analyse/swot_analyse_inhalt.html#doc21101608bodyText7 (abgerufen am 01.12.2025).

Bundesministerium für Wirtschaft und Energie (2019). Künstliche Intelligenz − Impulse zu einem Megatrend. Online verfügbar unter bundeswirtschaftsministerium.de/Redaktion/DE/Publikationen/Technologie/kuenstliche-intelligenz-impulse-zu-einem-megatrend.pdf?__blob=publicationFile&v=1 (abgerufen am 18.11.2025).

Campbell, Murray/Hoane, A. Joseph/Hsu, Feng-hsiung (2002). Deep Blue 134 (1–2), 57–83. doi.org/10.1016/S0004-3702(01)00129-1.

Collin, Matthias (2010). Der Ist-Zustand. In: Matthias Collin/Evelin Voigt-Eggert (Hrsg.): In zwölf Schritten einfach besser werden. Praxisleitfaden zur Unternehmensoptimierung. Wiesbaden, Betriebswirtschaftlicher Verlag Gabler, 17–25.

Datenethikkommission der Bundesregierung (2019). Gutachten der Datenethikkommission. Online verfügbar unter bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/it-digitalpolitik/gutachten-datenethikkommission.html (abgerufen am 04.12.2025).

Döbel, Inga/Leis, M./Molina Vogelsang, Manuel/Neustroev, D./Petzka, Henning/Riemer, A./Rüping, Stefan/Voß, Angelika/Wegele, M./Welz, Juliane (2018). Maschinelles Lernen. Eine Analyse zu Kompetenzen, Forschung und Anwendung. Online verfügbar unter publica.fraunhofer.de/entities/publication/47f259bb-c191-4b17-84f4-2b3824cc3a0a.

Durfee, Edmund/Lesser, Victor/Corkill, Daniel (1989). Trends in cooperative distributed problem solving. IEEE Transactions on Knowledge and Data Engineering 1 (1), 63–83. doi.org/10.1109/69.43404.

Dyck, Brigitte (2025). Künstliche Intelligenz in der Führung. Chancen, Entscheidungen und Strategien für morgen. Freiburg, Haufe-Lexware GmbH & Co. KG.

Engelmann, Jan/Puntschuh, Michael (2020). KI im Behördeneinsatz. Erfahrungen und Empfehlungen. doi.org/10.24406/PUBLICA-FHG-301015.

Gerlach, Dieter (2023). Praxishandbuch Strategisches Personalmanagement. München, Haufe.

Giering, Oliver (2022). Künstliche Intelligenz und Arbeit: Betrachtungen zwischen Prognose und betrieblicher Realität. Zeitschrift für Arbeitswissenschaft 76 (1), 50–64. doi.org/10.1007/s41449-021-00289-0.

Guckelberger, Annette (2019). Öffentliche Verwaltung im Zeitalter der Digitalisierung. Analysen und Strategien zur Verbesserung des E-Governments aus rechtlicher Sicht. Baden-Baden, Nomos Verlagsgesellschaft mbH & Co. KG.

IBM (2025). KI-Agenten-Lösungen. Online verfügbar unter ibm.com/de-de/solutions/ai-agents?utm_content=SRCWW&p1=Search&p4=2280458384380&p5=b&p9=184432711856&gclsrc=aw.ds&gad_source=1&gad_campaignid=22907569192&gbraid=0AAAAAoK3j5Z44TVVv-ZXgZEnIXtzV3ds&gclid=Cj0KCQiA_8TJBhDNARIsAPX5qx-QTMgkXXNR89j61X83y-gzoaARIsICBZJhyuy4RQT05Y_2MZErljAcaAuTUEALw_wcB (abgerufen am 04.12.2025).

Immich, Thomas (2025). KI-Agenten. Teil 1: Revolution in der digitalen Produktentwicklung. Heise Medien. Online verfügbar unter heise.de/hintergrund/KI-Agenten-Teil-1-Kuenstliche-Intelligenz-entwickelt-Software-im-Team-10367251.html (abgerufen am 26.11.2025).

Kalogeropoulos, Elena/Lammers, Anne/Müller-Brehm, Jaana/Puntschuh, Michael (2025). Wegweiser Digitale Debatten. Online verfügbar unter bmbfsfj.bund.de/resource/blob/186298/975f96f2e962ef4354ce9b54c81822c7/wegweiser-digitale-debatten-teil-1-data.pdf (abgerufen am 02.12.2025).

Kargwal, Aryan (2025). KI-Agenten-Orchestrierung: Wie man mehrere KI-Agenten koordiniert. Online verfügbar unter botpress.com/de/blog/ai-agent-orchestration (abgerufen am 04.12.2025).

Kaufmann, Traute (2021). Strategiewerkzeuge aus der Praxis. Berlin, Heidelberg, Springer Berlin Heidelberg.

Keicher, Lukas/Beichter, Tim/Kaiser, Manuel/Pallaks, Manuel (2021). Leitfaden zur Identifikation und Analyse von technologischen Trends für die berufliche Weiterbildung. doi.org/10.24406/PUBLICA-115.

KI-Campus (2025). KI als zentraler Megatrend: Chancen, Herausforderungen und notwendige Future Skills. Online verfügbar unter ki-campus.org/blog/ki-als-megatrend (abgerufen am 17.11.2025).

Kreyßing, Robert (2025). Verwaltungsentscheidungen durch Künstliche Intelligenz. Implikationen und verwaltungsrechtliche Rahmenbedingungen. Wiesbaden, Springer Fachmedien.

Krizhevsky, Alex/Sutskever, Ilya/Hinton, Geoffrey Hinton (2017). ImageNet classification with deep convolutional neural networks. Communications of the ACM 60 (6), 84–90. doi.org/10.1145/3065386.

Leible, Stephan/Gücük, Gian-Luca/Simic, Dejan/Brackel-Schmidt, Constantin von/Lewandowski, Tom (2024). Zwischen Forschung und Praxis: Fähigkeiten und Limitationen generativer KI sowie ihre wachsende Bedeutung in der Zukunft. HMD Praxis der Wirtschaftsinformatik 61 (2), 344–370. doi.org/10.1365/s40702-024-01050-x.

Maamar, Niklas (2021). Computer als Schöpfer. Der Schutz von Werken und Erfindungen künstlicher Intelligenz. Tübingen, Mohr Siebeck.

Markus, Heike/Meuche, Thomas (2022). Die Öffentliche Verwaltung heute und in der Zukunft. In: Heike Markus/Thomas Meuche (Hrsg.): Auf dem Weg zur digitalen Verwaltung. Ein ganzheitliches Konzept für eine gelingende Digitalisierung in der öffentlichen Verwaltung. Wiesbaden/Heidelberg, Springer Gabler, 1–34.

McCarthy, John/Marvin, Minsky/Nathaniel, Rochester/Claude, Shannon (2006). A Proposal for the Dartmouth Summer Research Project on Artificial Intelligence, August 31, 1955. AI Magazine 27 (4), 12. doi.org/10.1609/aimag.v27i4.1904.

Möltgen-Sicking, Katrin/Otten, Henrique Ricardo/Schophaus, Malte/Vargas Côrtes Soraya (2019). Öffentliche Verwaltung in Brasilien und Deutschland. Vergleichende Perspektiven und aktuelle Herausforderungen. Wiesbaden/Heidelberg, Springer.

Narang, Sharan/Chowdhery, Aakanksha (2025). Pathways Language Model (PaLM): Scaling to 540 Billion Parameters for Breakthrou. Online verfügbar unter research.google/blog/pathways-language-model-palm-scaling-to-540-billion-parameters-for-breakthrough-performance/ (abgerufen am 04.12.2025).

Novikov, Alexander/Vũ, Ngân/Eisenberger, Marvin/Dupont, Emilien/Huang, Po-Sen/Wagner, Adam Zsolt/Shirobokov, Sergey/Kozlovskii, Borislav/Ruiz, Francisco J. R./Mehrabian, Abbas/Kumar, M. Pawan/See, Abigail/Chaudhuri, Swarat/Holland, George/Davies, Alex/Nowozin, Sebastian/Kohli, Pushmeet/Balog, Matej (2025). AlphaEvolve: A coding agent for scientific and algorithmic discovery.

Pillay, Tharin/Booth, Harry (2025). 5 Predictions for AI in 2025. Online verfügbar unter time.com/7204665/ai-predictions-2025/ (abgerufen am 26.11.2025).

Russell, Stuart/Norvig, Peter (2022). Artificial intelligence. A modern approach. Boston, Pearson.

Searle, John R. (1980). Minds, brains, and programs. Behavioral and Brain Sciences 3 (3), 417–424. doi.org/10.1017/S0140525X00005756.

Seckelmann, Margrit (Hrsg.) (2024). Digitalisierte Verwaltung − Vernetztes E-Government. 3. Aufl. Berlin, Erich Schmidt Verlag GmbH & Co. KG.

Shaw, Frank X. (2025). Microsoft Build 2025: Das Zeitalter der KI-Agenten und der Aufbau des Open Agentic Web – News Center. Online verfügbar unter news.microsoft.com/de-at/microsoft-build-2025-das-zeitalter-der-ki-agenten-und-der-aufbau-des-open-agentic-web/ (abgerufen am 10.12.2025).

Siebert, Julien (2025). Agentic AI – Multi-Agenten-Systeme im Zeitalter generativer KI − Blog des Fraunhofer IESE. Online verfügbar unter iese.fraunhofer.de/blog/agentic-ai-multi-agenten-systeme/ (abgerufen am 17.11.2025).

Silver, David/Huang, Aja/Maddison, Chris J./Guez, Arthur/Sifre, Laurent/van den Driessche, George/Schrittwieser, Julian/Antonoglou, Ioannis/Panneershelvam, Veda/Lanctot, Marc/Dieleman, Sander/Grewe, Dominik/Nham, John/Kalchbrenner, Nal/Sutskever, Ilya/Lillicrap, Timothy/Leach, Madeleine/Kavukcuoglu, Koray/Graepel, Thore/Hassabis, Demis (2016). Mastering the game of Go with deep neural networks and tree search. Nature 529 (7587), 484–489. doi.org/10.1038/nature16961.

Spellerberg, Annette/Berg, Matthias/Memmel, Martin/Ehbrecht, Michaela/Walter, Ricarda/Bleisinger, Oliver/Malek, Christian (2021). Künstliche Intelligenz in Mittelstädten − Mittendrin oder außen vor? Ideen, Konzepte und Entwicklungen von KI in kleinen Mittelstädten in Rheinland-Pfalz.

Spitzer, Manfred (2025). Künstliche Intelligenz. Dem Menschen überlegen − wie KI uns rettet und bedroht. München, Droemer.

Stephan, Christian (2025). Gartner Hype Cycle™ für neue Technologien. Online verfügbar unter gartner.de/de/artikel/hype-cycle-fuer-neue-technologien (abgerufen am 23.12.2025).

Sycara, Katia (1998). Multiagent Systems. AI Magazine (19(2)). doi.org/10.1609/aimag.v19i2.1370.

Turing, Alan (1936). On computable numbers, with an application to the Entscheidungs-pro-blem. A correction. Proceedings of the London Mathematical Society 42 (2), 230–265.

Winkler, Katrin/Niedermeier, Sandra/Yuan, Katrin J. (Hrsg.) (2025). KI-Wissen für Führungskräfte. Entscheidungsgrundlagen und Insights für unternehmerisches Handeln. Stuttgart/Freiburg, Schäffer-Poeschel Verlag.

Zukunftsinstitut (2025). Megatrend Konnektivität. Online verfügbar unter zukunftsinstitut.de/zukunftsthemen/megatrend-konnektivitaet (abgerufen am 01.12.2025).

Zukunftsinstitut (2025). Was sind Megatrends? Online verfügbar unter zukunftsinstitut.de/zukunftsthemen/megatrends (abgerufen am 17.11.2025).

Einsatz von KI in der polizeilichen Sachbearbeitung – Effizienz und Grenzen

André Müller

Die Digitalisierung des öffentlichen Sektors und der Sicherheitsbehörden konfrontiert Verwaltungen mit substanziellen Herausforderungen. Der Umfang der Daten steigt exponentiell, während gleichzeitig die verfügbaren Personalressourcen sinken. Diese Problematik gibt es ebenfalls in den Polizeibehörden des Bundeslandes Brandenburg (Ursuleac 2023, S. 35). In der verwaltungswissenschaftlichen Diskussion wird betont, dass digitale Technologien das Potenzial besitzen, Abläufe zu beschleunigen, Informationsflüsse zu strukturieren und Bearbeitungskapazitäten zu erweitern. Klan (2024, 192−193) betont, dass Verwaltungen angesichts wachsender Datenvolumina vor der Aufgabe stehen, operative und analytische Prozesse stärker zu automatisieren, um eine nachhaltige Aufgabenerfüllung zu gewährleisten. In diesem Zusammenhang rücken Maßnahmen zur Implementierung Künstlicher Intelligenz (KI) verstärkt in den Fokus von Modernisierungsbestrebungen im Verwaltungssektor. KI-Systeme versprechen die Automatisierung repetitiver Aufgaben sowie eine Reduktion des Ressourcenaufwands. Gleichzeitig werden jedoch fundamentale Fragen in Bezug auf Legalität und Transparenz aufgeworfen.

Auch in polizeilichen Kontexten wird die Nutzung algorithmischer Systeme zunehmend als Ansatz gesehen, um standardisierte Vorgänge zu unterstützen und repetitive Arbeitsschritte effizienter zu bewältigen (Hoheisel-Gruler 2024, S. 12). Es besteht die Möglichkeit, dass technisch unterstützte oder automatisierte Verfahren dazu beitragen können, Sachbearbeitende von Routinearbeiten zu entlasten und somit Kapazitäten für qualifiziertere investigative Aufgaben freizustellen. Der Einsatz von KI ist jedoch rechtlich nicht unproblematisch. Gemäß der europäischen Verordnung 2024/1689 – auch als Artificial Intelligence Act (AI Act) bezeichnet – werden KI-Anwendungen im Kontext der Strafverfolgung als Hochrisiko-Systeme klassifiziert. Dies impliziert spezifische Konformitätsanforderungen, zu denen Dokumentationspflichten, menschliche Aufsicht und Transparenzanforderungen zählen. Der Einsatz von KI in der polizeilichen Sachbearbeitung ist demnach nicht nur eine technische, sondern auch eine rechtliche Herausforderung.

Der vorliegende Beitrag untersucht die Frage, inwiefern Künstliche Intelligenz zur Optimierung der polizeilichen Sachbearbeitung von Massendelikten in Brandenburg beitragen kann. Im Rahmen der Analyse werden die Chancen, die sich insbesondere in Form von Entlastungspotenzialen durch den Einsatz von KI ergeben, sowie die Herausforderungen, die aus rechtlichen, technischen und organisatorischen Aspekten bei einer praktischen Implementierung entstehen, untersucht (Meier 2025, S. 42). Ziel des vorliegenden Beitrags ist eine qualitative Analyse der Frage, in welchem Umfang KI-Systeme zur Entlastung beitragen können. Dies erfolgt auf Grundlage einer theoretischen Einordnung und empirischer Erkenntnisse aus Experteninterviews. Zudem werden die dabei zu beachtenden rechtlichen und strukturellen Bedingungen untersucht. Schließlich werden die Anforderungen einer verantwortungsvollen Implementierung diskutiert.

Massenkriminalität und deren Umfang in Brandenburg

Die Definition und Strukturierung von Massenkriminalität in Brandenburg erfolgt gemäß der Verfügung zur Zentralen Anzeigenbearbeitung (ZENTRAB) des Polizeipräsidiums vom 20. Dezember 2018. Gemäß dieser Regelung werden „geeignete Delikte der Massen- und Häufigkeitskriminalität“ in eigenständigen Kriminalkommissariaten bearbeitet, um eine landesweit einheitliche, strukturierte und effiziente Abarbeitung zu gewährleisten. Die ZENTRAB-Verfügung sieht dabei vor, dass das Kriminalkommissariat ZENTRAB einen Bearbeitungsanteil von bis zu 58 Prozent aller Ermittlungsverfahren anstreben soll. Die Polizeiliche Kriminalstatistik (PKS) des Bundeslandes Brandenburg für das Jahr 2024 dokumentiert das Ausmaß dieser Massenkriminalität präzise. Die unter ZENTRAB fallende Massenkriminalität umfasst insgesamt 126.615 Fälle und stellt somit 80,8 Prozent aller erfassten Straftaten ohne ausländerrechtliche Verstöße dar (Polizeipräsidium des Landes Brandenburg 2025, S. 7–14).

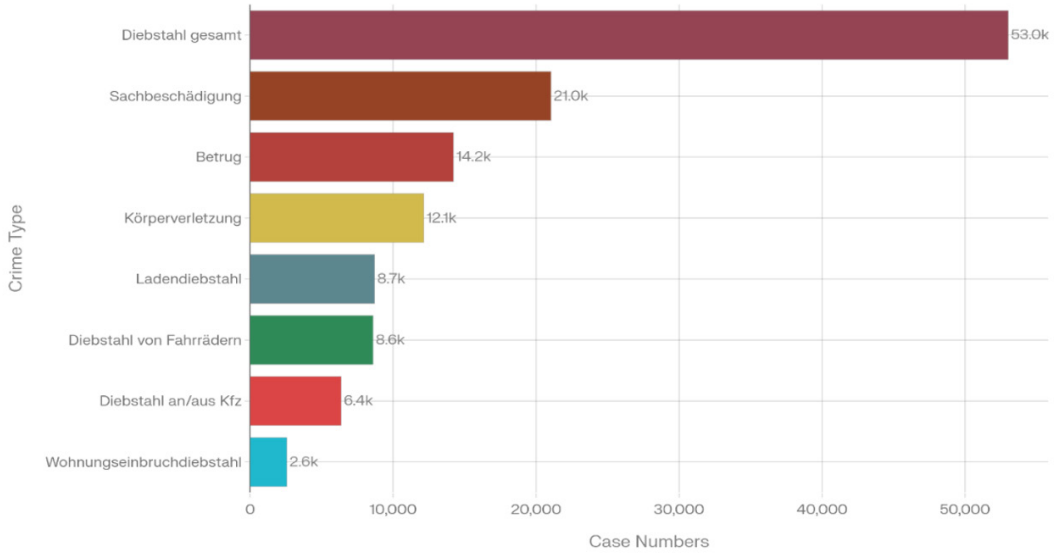

Abbildung 1: ZENTRAB-Delikte in Brandenburg 2024: Massenkriminalität nach Delikttyp (Fallzahlen) (Polizeipräsidium des Landes Brandenburg, 2025)

Die Kategorie „Diebstahl“ weist mit 53.021 Fällen die höchste Anzahl an Fällen auf, gefolgt von Sachbeschädigungen mit 21.034 Fällen und Betrugsdelikten mit 14.221 Fällen. Darüber hinaus wurden 12.141 Fälle von Körperverletzung, 8.697 Fälle von Ladendiebstahl, 8.591 Fälle von Diebstahl von Fahrrädern, 6.353 Fälle von Diebstahl an und aus Kraftfahrzeugen sowie 2.557 Fälle von Wohnungseinbruchdiebstahl verzeichnet (Polizeipräsidium des Landes Brandenburg 2025, S. 51–58). Die Arbeitsbelastung aufgrund dieser Massenverfahren stellt die Sachbearbeitenden der Polizei vor erhebliche Herausforderungen. Eine Analyse der bundesweiten Datenmenge verdeutlicht diese Entwicklung. Die deutschen Polizeien erzeugen jährlich etwa 10 Millionen Vorgänge, die in über 250 Millionen Informationsobjekte und einen strukturierten Datenbestand von über 150 Terabyte Daten resultieren (Klan 2024, S. 192). In Brandenburg allein bedeutet dies eine Arbeitsbelastung, die eine systematische Bearbeitung ohne Digitalisierungshilfen erschwert.

Potenzial Künstlicher Intelligenz bei der Bearbeitung von Massendelikten

Die Leistungsfähigkeit von KI übertrifft die klassischen Grenzen der Halbleitertechnologie erheblich. Moores Gesetz postuliert eine Verdopplung der Rechnerleistung alle 18 Monate. Moderne KI-Systeme demonstrieren jedoch am Beispiel der Proteinfaltungsvorhersage eine qualitativ andere Wachstumsdynamik. So wurde die Ausbeute bei der Strukturvorhersage menschlicher Proteine innerhalb von 18 Monaten erst um das Tausendfache und anschließend in nur einem Jahr nochmal um das Zehntausendfache gesteigert. Und das bei einer Steigerung der Genauigkeit um den Faktor vier. Dies lässt den Schluss zu, dass der Durchbruch der Künstlichen Intelligenz weniger auf eine exponentielle Steigerung der Hardware-Kapazitäten, sondern vielmehr auf eine intelligente Algorithmik, große Datenmengen und optimierte Netzwerkarchitekturen zurückzuführen ist. Diese Entwicklung übersteigt das klassische, vorhersehbare Halbleiter-Wachstum bei Weitem und unterstreicht damit das transformative Potenzial der Künstlichen Intelligenz (Spitzer 2023).

Der Einsatz von KI kann also eine effektive Methode zur Bewältigung der o. g. Herausforderung darstellen. Der Fokus liegt auf der Automatisierung repetitiver und datenintensiver Aufgaben, der Übertragung spezifischer Aufgaben an Maschinen zur Erledigung und der Bereitstellung von mehr Zeit für andere Aufgaben für Sachbearbeitende (vgl. von Lucke 2024, S. 76; zit. nach Hoheisel-Gruler 2025, S. 12). Für die ZENTRAB-Bearbeitung sind drei KI-Anwendungen von besonderer Relevanz: Erstens besteht die Möglichkeit, dass Datenanalyse und Mustererkennung dazu beitragen, dass Straftaten automatisch vorklassifiziert werden können. Das Programm P20, das der Modernisierung der polizeilichen Sachbearbeitung dient, demonstriert, dass intelligente Systeme aus großen Datenmengen „Muster erkennen“ und somit „eine Vorauswahl für eine menschliche Entscheidung“ treffen können (Ursuleac 2023, S. 36). Dies hat den Vorteil, dass zeitaufwändige manuelle Zuordnungen nicht erforderlich sind. Zweitens ermöglicht Chatbot-gestützte Sachbearbeitung in Kombination mit Sprachsteuerung eine Beschleunigung der Vorgangserfassung „bis zum 5- bis 6-Fachen gegenüber der Nutzung einer Schreibtastatur“ (Meier 2024, S. 43), da Sachbearbeitende ihre Erkenntnisse direkt diktieren können. Drittens können intelligente Recherchesysteme unter Beachtung von Zugriffs- und Rollenkonzepten „[k]omplexe Aufgaben mit aufwändigen Analysen in erheblich reduzierter Zeit sicher [abschließen]“ (Meier 2024, S. 44), indem sie aus Millionen gespeicherter Dokumente innerhalb von Sekunden definierte Informationen extrahieren.

Zusammenfassend lässt sich konstatieren, dass KI klassische polizeiliche Prozesse „ergänzt und verbessert, indem sie Entscheidungsgrundlagen liefert und die Komplexität moderner Aufgaben bewältigbar macht“ (Honekamp und Klingelhöfer 2025, S. 11). Dabei ist entscheidend, dass KI-Systeme stets in Kombination mit menschlicher Expertise zum Einsatz kommen. Der Mensch sollte das Recht auf finale Entscheidungen nicht an die Technik abtreten. Stattdessen sollte KI als ein Instrument zur Mustererkennung und zur Unterstützung bei der Entscheidungsfindung genutzt werden (Ursuleac 2023, S. 36). Im Kontext des EU AI Acts wird dies durch die Anforderung an ein „ausreichendes Maß an KI-Kompetenz“ bei Operatoren unterstrichen (Hoheisel-Gruler 2025, S. 17). Die vorliegende KI-Kompetenz wird gemäß der rechtlichen Definition als die „Fähigkeiten, Kenntnisse und das Verständnis“ definiert, um „KI-Systeme sachkundig einzusetzen sowie sich der Chancen und Risiken von KI und möglicher Schäden, die sie verursachen kann, bewusst zu werden“ (Hoheisel-Gruler 2025, S. 18).

Insbesondere bei der Bearbeitung standardisierter Massendelikte können KI-gestützte Vorlagen und Automatisierungen eine Entlastung der Sachbearbeitenden bewirken. Gleichzeitig bleibt die rechtliche Eigenverantwortung der Polizei sowie die Einhaltung des Rechtsstaatsprinzips gewährleistet, wenn die KI transparent und unter menschlicher Kontrolle eingesetzt wird. Diese Forderung steht im Einklang mit den Prinzipien des EU AI Acts, welcher an KI-Systeme in der Strafverfolgung besondere Anforderungen an Transparenz, Dokumentation und menschliche Aufsicht stellt (Hoheisel-Gruler 2025, S. 18). Die praktische Umsetzung erfordert demnach „ein Zusammenspiel aus juristischem und technischem Verständnis“ (Winterhalter 2025), um sicherzustellen, dass die Technologie nicht zum „Bremsklotz“ wird, sondern als effektives und effizientes, unterstützendes Werkzeug fungiert.

Methodisches Vorgehen

Aufgrund des explorativen Charakters des Untersuchungsgegenstandes – der Implementierung von KI in der polizeilichen Sachbearbeitung – wurde ein qualitatives Forschungsdesign gewählt. Das Ziel des vorliegenden Beitrags besteht in der Erlangung tiefgreifender Einblicke in die technischen Machbarkeiten, organisatorischen Herausforderungen und praktischen Bedürfnisse und weniger in einer quantitativen Analyse. Als Erhebungsmethode wurden daher leitfadengestützte Experteninterviews durchgeführt. Die Selektion der beiden Interviewpartner erfolgte mit größter Sorgfalt (purposive sampling), um das Forschungsfeld aus zwei komplementären Perspektiven zu beleuchten. Um ein möglichst vollständiges Bild der Situation in der Polizei Brandenburg zu erhalten, wurden Experten aus der operativen Anwendung und der strategisch-technischen Planung ausgewählt.

Expertin A (operative Ebene): In ihrer Funktion als Standortleiterin der Zentralen Bearbeitung von Massenkriminalität (ZENTRAB) repräsentiert sie die Anwenderseite. Sie trägt die direkte Verantwortung für die Abarbeitung von Massendelikten und hat damit umfassenden Einblick in die praktischen Bedürfnisse und organisatorischen Herausforderungen. Auf der strategisch-technischen Ebene ist Experte B als KI-Beauftragter des Zentraldienstes der Polizei (ZDPol) tätig. Seine Aufgabe besteht darin, die technische Dienstleister- und Planungsebene mit Schwerpunkt auf IT-Infrastruktur, Machbarkeitsstudien und Datenschutz zu vertreten. Im Rahmen der Datenerhebung wurden im Dezember 2025 mit beiden Experten leitfadengestützte Interviews durchgeführt. Der Leitfaden wurde auf der Grundlage der theoretischen Vorarbeit entwickelt und in vier Themenblöcke strukturiert:

1. Die Herausforderungen der aktuellen Sachbearbeitung,
2. die Einsatzpotenziale von KI,
3. die Risiken und Hürden
4. sowie die notwendigen Rahmenbedingungen

sind zu berücksichtigen. Die halbstandardisierte Form der Datenerhebung gewährleistet die Vergleichbarkeit der Aussagen, lässt jedoch genügend Raum für die Berücksichtigung individueller Schwerpunkte der Experten. Die Interviews wurden aufgezeichnet und als geglättete Transkripte verschriftlicht. Anschließend wurden signifikante Aspekte aus dem Material extrahiert und auf Grundlage eines Kategoriensystems systematisch geordnet. Der Auswertungsprozess umfasste drei Schritte:

Zunächst erfolgt eine deduktive Kategorienbildung auf Grundlage des Leitfadens und der Theorie (siehe Kapitel Ergebnisse). Im weiteren Verlauf werden diese Kategorien induktiv um spezifische technische Kategorien ergänzt, wie beispielsweise Datenpersistenz oder strategische Defizite. Im zweiten Schritt erfolgt die Zuordnung, Paraphrasierung und Generalisierung relevanter Textstellen zu den zuvor definierten Kategorien. Im dritten Schritt erfolgt eine fallübergreifende Gegenüberstellung (Cross-Case Analysis), mit dem Ziel, sowohl Gemeinsamkeiten als auch Unterschiede zwischen operativer und strategischer Perspektive zu identifizieren. Dieses Vorgehen gewährleistet, dass die subjektiven Sichtweisen der Experten in strukturierter und nachvollziehbarer Weise in die Beantwortung der Forschungsfrage einfließen.

Ergebnisse

Im Folgenden werden die Ergebnisse der leitfadengestützten Experteninterviews dargestellt. Die Analyse ist in thematische Bereiche analog der Themenblöcke in den Interviews unterteilt, die sich den Herausforderungen, dem Einsatzpotenzial, den Risiken sowie den notwendigen Rahmenbedingungen widmen. Die beiden Experten identifizieren die Bewältigung von Massendelikten als derzeit kritischstes Problem bei der Sachbearbeitung der Polizei in Brandenburg. Allerdings setzen sie unterschiedliche Schwerpunkte hinsichtlich der Ursachen. Die Expertin A charakterisiert die Situation aus der operativen Praxis als Grenzerfahrung. Die schiere Quantität der Verfahren – spezifiziert auf ca. 1.250 Vorgänge pro Sachbearbeitenden jährlich – resultiert in einer reinen „Verwaltung der Kriminalität“. Insbesondere bei Betrugsdelikten (beispielsweise der massenhaften Versendung von Phishing-Nachrichten) stößt die manuelle Bearbeitung an ihre Grenzen, da es möglich ist, „mit einem Klick tausende Nachrichten“ zu versenden, während die polizeiliche Abarbeitung jedoch linear und analog erfolgt.

Experte B bestätigt diesen Befund („Lochen und Abheften“) und erweitert die Problemanalyse um den Aspekt der Datenqualität. Er kritisiert, dass bereits der „Erste Angriff“ (die Anzeigenaufnahme) oft Daten von geringer Qualität liefert. Die Verwendung handschriftlicher Anhörbögen sowie unstrukturierter Informationen verhindert eine effektive digitale Weiterverarbeitung. Während Expertin A die Menge als primäres Problem identifiziert, sieht Experte B die fehlende digitale Struktur der Daten als das eigentliche Hindernis für eine Automatisierung. Konsens herrscht über die Notwendigkeit der Entlastung in den gewünschten Einsatzfeldern von KI. Die konkreten Szenarien unterscheiden sich jedoch je nach fachlichem Fokus.

Die Expertin A zeigt eine starke Fokussierung auf die Automatisierung bürokratischer Prozesse. Gemäß ihrer Analyse weist die Generierung von Anhörbögen, das automatisierte Verfassen von Schlussberichten sowie die Erstellung von Textbausteinen für die Staatsanwaltschaft das größte Potenzial auf. Das vorrangige Ziel besteht in diesem Kontext in einer quantitativen Abarbeitung der Rückstände sowie der Bewältigung der täglichen Fallzahlen („Land sehen“).

Experte B skizziert deutlich komplexere, qualitativ orientierte Anwendungsfälle. Er betrachtet KI dabei nicht lediglich als eine Art „Schreibkraft“, sondern als ein Assistenzsystem, das:

- rechtliche Einordnungen (Subsumtion) vornehmen kann,
- Widersprüche in Vernehmungsprotokollen oder zwischen Zeugenaussagen erkennt,
- mittels Tools wie „Axon“ Bodycam-Aufnahmen direkt in strukturierte Berichte überführt.

Er betont zudem das Potenzial von KI als „Kreativitätsquelle“, die Ermittlungsansätze liefert, die im Routinebetrieb untergehen würden. Die vergleichende Analyse offenbart eine Ambivalenz der Entlastungseffekte, die durch den Einsatz von KI zu erwarten sind.

Expertin A erwartet eine spürbare Reduktion von Frust und Überlastung durch den KI-Einsatz. Die Automatisierung von „Massendelikten“ soll Freiräume für „echte kriminalistische Arbeit“ schaffen. Die Effizienzsteigerung im Arbeitsalltag ist für sie der Nachweis der zu erwartenden Akzeptanz.

Experte B warnt vor einer Verschiebung der psychischen Belastung. Wenn KI die emotional neutrale Routinearbeit übernimmt, bleiben beim Menschen ausschließlich komplexe, emotionale Fälle. Die psychische Beanspruchung könnte sich dadurch intensivieren. Zudem thematisiert er „Überwachungsängste“. Die Sorge, dass KI-Tools zur Emotionserkennung oder Leistungskontrolle missbraucht werden könnten, ist ein Hindernis, das in der rein operativen Betrachtung von Expertin A nicht auftauchte.

Die rechtlichen Hürden sieht Expertin A in der Abstimmung mit der Staatsanwaltschaft und der Wahrung der Entscheidungshoheit („Human-in-the-Loop“). Experte B deckt fundamentale systemische Defizite auf: die Abhängigkeit von meist US-amerikanischen Sprachmodellen (LLMs) mit einem „anglophonen Bias“, der nicht die spezifische Terminologie der deutschen Polizei widerspiegelt. Es fehlen souveräne, europäische Modelle für den Behördeneinsatz.

Ein wesentlicher Befund von Experte B ist die Problematik der Versionierung: KI-Modelle sind dynamisch (Updates verändern das Antwortverhalten). Für eine gerichtliche Verwertbarkeit muss rekonstruierbar sein, welche Version des Modells zu einem bestimmten Zeitpunkt welche Entscheidungsgrundlage lieferte. Dieses technische Archivierungsproblem ist in der operativen Praxis (Expertin A) kaum im Bewusstsein.

Experte B weist auf das Problem hin, dass LLMs Informationen wie Namen von Tatverdächtigen nicht „vergessen“ können. Dies steht im Konflikt mit Datenschutzvorgaben (Löschfristen), wenn sich ein Tatverdacht nicht erhärtet („Recht auf Vergessenwerden“).

Experte B identifiziert signifikante Diskrepanzen in der strategischen Implementierung, die über die operative Ebene hinausreichen. Er äußert sich kritisch zum Fehlen einer landesweiten KI-Strategie in Brandenburg sowie zum Fehlen von „Innovation Labs“, in denen Fehler ohne Sanktionsdruck gemacht werden dürfen.

Das föderale Prinzip („Einer für Alle“) im Rahmen des Programms P20 wird als zu träge wahrgenommen. Während die operative Ebene (Expertin A) die Notwendigkeit funktionierender Tools betont, legt die strategische Ebene (Experte B) dar, dass die Voraussetzungen in Bezug auf das Beschaffungsrecht und die Kultur (z. B. Fehlerkultur, agile Verträge) noch nicht gegeben sind.

Die Synthese der Interviews offenbarte eine Diskrepanz zwischen dem operativen Bedarf und der strategischen Machbarkeit. Die operative Praxis (A) stellt die Erwartung auf, dass KI primär eine quantitative Entlastung (Mengenbewältigung) bewirken wird. Die strategische IT-Sicht (B) fokussiert sich auf eine qualitative Aufwertung der Polizeiarbeit, die durch verbesserte Analysen und eine Re-Professionalisierung durch den Ansatz des „Rausgehens zum Bürger" erreicht werden soll. Ferner ist festzustellen, dass es zu einer Verantwortungsdiffusion kommt. Auf der einen Seite besteht auf der operativen Ebene die Haltung, dass eine Unterschrift ausreichend ist. Auf der anderen Seite zeigt die technische Analyse, dass dies bei komplexen Blackbox-Modellen zu einer Farce werden kann, wenn die Entscheidungsgrundlage der KI für den Menschen nicht mehr nachvollziehbar oder revisionssicher erklärbar ist.

Diskussion

Die vorliegenden Ergebnisse stützen die Hypothese, dass der Einsatz von KI in der polizeilichen Sachbearbeitung von Massendelikten ein signifikantes Potenzial zur Effizienzsteigerung birgt, jedoch durch erhebliche technische, rechtliche und organisatorische Hürden limitiert wird. Im Folgenden werden die zentralen Erkenntnisse der Experteninterviews im Kontext der aktuellen Forschungslage diskutiert und dabei insbesondere die spezifische Situation im Land Brandenburg mit den Erkenntnissen aus Niedersachsen (Coldewei 2024) verglichen. Die Experten aus Brandenburg identifizieren Entlastungspotenzial in der Automatisierung administrativer und repetitiver Tätigkeiten. Konkret genannt wurden die automatisierte Erstellung von Berichten, Transkription von Vernehmungen und Vorselektion von Massendaten. Dies deckt sich mit der Literatur, die KI als Schlüsseltechnologie zur Bewältigung steigender Datenmengen und sinkender Personalkapazitäten beschreibt (Ursuleac 2023, S. 35). Diese Einschätzung wird durch Waldtmann (2024, S. 259 ff.) gestützt, der ebenfalls hervorhebt, dass KI-basierte Technologien essenziell sind, um das steigende Vorgangsaufkommen bei Massendelikten effizient zu bewältigen.

Interessant ist ein Vergleich zu den niedersächsischen Polizeiergebnissen von Coldewei (2024). Dort wird ein Potenzial für die Automatisierung von „einfach gelagerten Delikten" auf bis zu 50 % geschätzt, insbesondere bei Diebstahls- und Betrugsdelikten ohne Ermittlungsansätze. Während Coldewei (2024, S. 9) auf vollständige Dunkelverarbeitung fokussiert, betonen die Brandenburger Experten zusätzlich die qualitative Unterstützung im „Human-in-the-Loop"-Ansatz. Dies deutet darauf hin, dass in Brandenburg der Fokus aktuell stärker auf der Unterstützung der Sachbearbeitungsprozesse liegt, während in Niedersachsen bereits offensiver über das vollständige Ersetzen menschlicher Arbeitsschritte nachgedacht wird. Zentrale Hemmnisse sind die mangelnde Datenqualität und die fehlende Verfügbarkeit leistungsfähiger, polizeispezifischer Sprachmodelle. „Consumer-Modelle" entsprechen nicht der spezifischen Polizeisprache und internen Logiken. Dies bestätigt die Warnung von Hoheisel-Gruler (2025, S. 12–15), der betont, dass KI-Systeme in der Polizei nicht nur technisch funktionieren, sondern auch in die organisatorischen und rechtlichen Kontexte eingebettet sein müssen.

Besonders kritisch ist das Risiko von „Halluzinationen" und Bias. Wenn KI-Systeme fehlerhafte Zusammenhänge generieren (z. B. falsche Verdachtsmomente), gefährdet dies den einzelnen Ermittlungserfolg und die Rechtsstaatlichkeit. Hier zeigt sich eine interessante Parallele zur Diskussion um den EU AI Act: Während die rechtliche Regulierung (z. B. Verbot von

Emotionserkennung am Arbeitsplatz) in der Theorie klar scheint, fehlt es in der Praxis oft an der technischen Überprüfbarkeit der KI-Entscheidungen (Winterhalter 2024). Die Forderung von Experte B nach einer „KI-Konfigurationsmanagement-Datenbank“ zur Sicherstellung der Revisionssicherheit ist ein innovativer Lösungsansatz, der in der breiten Literatur bisher wenig Beachtung findet, aber für die gerichtliche Verwertbarkeit von KI-Ergebnissen essenziell sein könnte. Die Ergebnisse zeigen, dass Technologie allein nicht reicht. Beide Experten warnen, dass die Einführung von KI eine Anpassung der Organisations- und Qualifikationsstruktur erfordert. Das „Wissenstransferdefizit“ durch die Trennung von Schutz- und Kriminalpolizei in Brandenburg (Experte B) stellt eine spezifische Hürde dar, die in anderen Bundesländern weniger ausgeprägt sein könnte.

Die Akzeptanzfrage ist ebenfalls zentral. Expertin A betont, dass Akzeptanz nur durch Entlastung entsteht. Coldewei (2024, S. 9) zufolge resultieren Widerstände oft aus der Sorge vor Qualitätsverlust oder dem Gefühl der Ersetzbarkeit. Die Brandenburger Ergebnisse ergänzen diese Perspektive um den Aspekt des „Modellvertrauens“: Wenn Beamte die Funktionsweise von KI und Datenschutz nicht verstehen, meiden sie die Systeme – unabhängig von der Leistungsfähigkeit. Brandenburg steht im Vergleich zu Bayern oder Niedersachsen noch am Anfang einer systematischen KI-Strategie, da es an einer zentralen „Innovation Unit“ oder einem KI-Labor mangelt. Das Fehlen dieser Einrichtungen stellt einen strategischen Nachteil dar (Experte B). Das P20 (Programm Polizei 2020) dient als Rahmen für gemeinsame Standards, doch die praktische Umsetzung bleibt häufig an föderalen Hürden hängen (Klan 2024, S. 193). Eine erfolgreiche KI-Integration in die Massendeliktsbearbeitung scheitert demnach weniger an der Verfügbarkeit der Technologie als vielmehr an der strategischen Verankerung und der mangelnden Harmonisierung von Daten und Prozessen über Ländergrenzen hinweg. KI ist demnach kein „Plug and Play“-Werkzeug zur Beseitigung des Personalmangels, sondern ein tiefgreifendes Transformationsprojekt, das die polizeiliche Aufbau- und Ablauforganisation maßgeblich verändert. Die Chancen für eine Beschleunigung der Verfahren sind real, vorausgesetzt, dass Datenqualität, Rechtssicherheit und Mitarbeiterkompetenz gleichermaßen entwickelt werden.

Schlussfolgerungen

Die Studie offenbart: KI kann bei der Bewältigung steigender Fälle und sinkender Personalressourcen im Bereich Massendelikte helfen. KI ist jedoch nicht als Ersatz für kriminalistisches Denken gedacht, sondern für administrative Routinen – von der Transkription bis zum Schlussvermerk. Ein unmittelbarer Vergleich der gewonnenen Erkenntnisse mit denen aus Niedersachsen (Coldewei 2024) offenbart signifikante Diskrepanzen in der aktuellen strategischen Ausrichtung. In Niedersachsen werden bereits aktive Szenarien der vollständigen Dunkelverarbeitung für Bagatelldelikte diskutiert und durch zentrale Einheiten vorangetrieben. In Brandenburg ist der Ansatz derzeit noch stark auf den „Human-in-the-Loop“-Ansatz fokussiert.

Die befragten Brandenburger Experten priorisieren die Unterstützung der einzelnen Sachbearbeitenden (beispielsweise durch Formulierungshilfen oder Datenaufbereitung) gegenüber der vollautomatischen Fallabschließung. Dies lässt auf eine Zurückhaltung schließen, die maßgeblich von der Sorge um Datenqualität und Rechtssicherheit determiniert ist. Zudem manifestiert sich in Brandenburg ein struktureller Nachteil, der in der Abwesenheit

einer zentralen Entwicklungsstelle begründet liegt. Eine solche Institution, wie sie Coldewei (2024, S. 7) mit dem „Dezernat 64 – Data Solutions“ für Niedersachsen beschreibt, würde die einheitliche Implementierung fördern und das Entstehen von Inselwissen verhindern. Gemäß der Analyse wurde die striktere Trennung von Schutz- und Kriminalpolizei in Brandenburg als Hemmnis für einen durchgängigen digitalen Workflow identifiziert. Die Polizei Brandenburg muss das identifizierte Entlastungspotenzial heben, ohne die Rechtsstaatlichkeit zu gefährden. Dafür sind folgende Schritte erforderlich:

Es wird eine zentrale Koordinierungsstelle eingerichtet, die KI-Tools technisch prüft und für die spezifischen Brandenburger Prozesse (z. B. ComVor, E-Akte) fachlich passend ist. Es werden Pilotprojekte in hochstandardisierten Bereichen (z. B. Tankbetrug, Fahrraddiebstahl, ohne Täterhinweise) in abgegrenzten Deliktsfeldern gestartet. Die Staatsanwaltschaft ist dabei einzubeziehen, damit die gerichtliche Verwertbarkeit der KI-Berichte gewährleistet werden kann. Und es werden Qualifizierungsoffensiven für die Methodenkompetenz der Sachbearbeitenden angeboten. Vor der Beschaffung komplexer Sprachmodelle muss die Basisdatenqualität erhöht werden (Pflichtfelder, Plausibilitätsprüfungen). Brandenburg steht an einem Scheideweg: Bleibt das Land ein passiver Nutzer von Standardsoftware, droht eine Überlastung der Sachbearbeitung. Entscheidet man sich jedoch für eine aktive Gestaltung mit zentraler Steuerung und Mut zu Pilotprojekten, kann KI zum entscheidenden Hebel werden, um trotz des Personalmangels handlungsfähig zu bleiben.

Literaturverzeichnis

Coldewei, T. (2024). Einsatz von künstlicher Intelligenz bei der polizeilichen Sachbearbeitung von Massendelikten der Alltagskriminalität. In: Honekamp, W. (Hrsg.): Künstliche Intelligenz in der Polizeiarbeit, Deutsche Hochschule der Polizei – Hochschulverlag, Münster, S. 110–26.

Hoheisel-Gruler, R. (2025). Polizeiliche Aus-, Fort- und Weiterbildung in Zeiten von künstlicher Intelligenz (KI). In: Honekamp, W., und Klingelhöfer, M. (Hrsg.): Polizei-Informatik 2025, Deutsche Hochschule der Polizei – Hochschulverlag, Münster, S. 12–28.

Honekamp, W., und Klingelhöfer, M. (2025). Polizei-Informatik. Deutsche Hochschule der Polizei – Hochschulverlag, Münster.

Klan, D. (2024). P20 – Polizeiliche Sachbearbeitung der Zukunft schon heute. In: Honekamp, W., und Klingelhöfer, M. (Hrsg.): Polizei-Informatik 2024. Rediroma-Verlag, Remscheid, S. 192–199.

Meier, H.-D. (2025). Künstliche Intelligenz (KI) in der Polizeiarbeit: UPDATE. In: pvt POLIZEI VERKEHR + TECHNIK, Ausgabe 2/25, S. 42–44.

Polizeipräsidium Brandenburg (2018). Zuständigkeiten der Zentralen Anzeigenbearbeitung der ZENTRAB I/II. Verfügung des Polizeipräsidenten des Landes Brandenburg, Fassung vom 20.12.2018. Unveröffentlichtes behördeninternes Dokument; zitiert nach Vorlage des Verfassers.

Polizeipräsidium des Landes Brandenburg (2025). Polizeiliche Kriminalstatistik 2024. Version 2.0, Stand 21.03.2025, Potsdam. Online verfügbar unter: mik.brandenburg.de/sixcms/media.php/9/PKS_2024_Stand21032025.pdf (Zugriff am 24.11.2025).

Spitzer, M. (2023). Künstliche Intelligenz. Dem Menschen überlegen – wie KI uns rettet und bedroht. Vorgelesen von Julian Mehne: argon Sachhörbuch (Track 24, Kapitel 2 Was bisher geschah, Teil 8, ab Minute 0:30).

Ursuleac, S. (2023). KI in der Polizei: zahllose Möglichkeiten – begrenzter Einsatzrahmen. In: pvt POLIZEI VERKEHR + TECHNIK, Ausgabe 4/23, S. 35–37.

Waldtmann, C. (2024). Einsatz KI-basierter Technologien zur Bewältigung des polizeilichen Vorgangsaufkommens bei Massendelikten. In: Honekamp, W., und Klingelhöfer, M. (Hrsg.): Polizei-Informatik 2024. Rediroma-Verlag, Remscheid, S. 259–263.

Winterhalter, J. (2025). KI-Verordnung als Bremse der Digitalisierung? Legal Tribune Online, 02.09.2025. Online verfügbar unter: lto.de/recht/hintergruende/h/ki-verordnung-praxis-verwaltung-unklare-rechtsbegriffe (Zugriff am 25.11.2025).

Verantwortungsvolle KI: Eine ethische Betrachtung des Projekts FRANKA

Jana Piorr

Die Integration Künstlicher Intelligenz (KI) in die polizeiliche Arbeit gewinnt zunehmend an Bedeutung (Haas 2024, S. 80; Povalej et al. 2021). Dabei eröffnen Large Language Models (LLMs) neue Möglichkeiten, komplexe Analysen von Massendaten zu automatisieren, Ermittlungsprozesse zu unterstützen und Daten effizient auszuwerten (Abteilung Digitalisierung und Zentrales IT-Management der Landesregierung (StK 3) 2024, S. 88; Haas 2024, S. 80–83). Das Projekt „Frage- und Antwortsystem für KI-basierte Auswertung von Chats und Texten" (FRANKA) in Schleswig-Holstein, das den Einsatz eines LLMs innerhalb der polizeilichen Arbeit im Bereich Ermittlungen von Kinder- und Jugendpornografie vorsieht, repräsentiert diese technologische Entwicklung. Das Projekt zielt darauf ab, durch automatisierte Textanalyse und ein gezieltes Frage- und Antwortsystem verfügbare Daten effizienter zu nutzen und dadurch die Effektivität und Qualität der polizeilichen Ermittlungsarbeit im Bereich der Kinder- und Jugendpornografie zu steigern (Landesportal Schleswig-Holstein 2023).

Neben Vorteilen birgt der Einsatz von KI-Systemen gleichzeitig auch Risiken. Darunter sind ethische Herausforderungen aufzuführen, die eine verantwortungsvolle Entwicklung sowie Anwendung von KI erfordern (Deutscher Ethikrat 2023, S. 108). Responsible AI beschreibt KI-Systeme, die nicht allein leistungsorientiert sind, sondern auf den Prinzipien der Nachhaltigkeit, Erklärbarkeit, Gleichheit und Interpretierbarkeit basieren, also verantwortungsvoll sind (Zühlke 2023). Besonders im Kontext Polizei ist eine sorgfältige ethische Betrachtung der KI-Systeme maßgeblich (Bitkom e. V. 2023, S. 9–12). Der vorliegende Beitrag widmet sich dem Projekt FRANKA und betrachtet, inwiefern ethische Kriterien einer verantwortungsvollen KI bei der Entwicklung des Tools beachtet und umgesetzt werden.

Hintergrund

KI und im Speziellen LLMs sind seit der Vorstellung von ChatGPT im November 2022 im Fokus von Diskussionen zu Einsatzmöglichkeiten, welche sich auch auf die Polizei entfalten (Ebers 2024, S. 51 f.). KI bietet das Potenzial, die Effizienz der Polizeiarbeit signifikant zu steigern, und findet dort bereits moderate Anwendung (Bitkom e. V. 2023, S. 3). Im Rahmen von Ermittlungsverfahren nach §§ 184b, c StGB, welche die Verbreitung, den Erwerb und den Besitz kinder- und jugendpornografischer Inhalte betreffen, liegt der Schwerpunkt bei der polizeilichen Sachbearbeitung bislang bei der Auswertung von Bild- und Videomaterial. Die Landespolizei Schleswig-Holstein nutzt hierfür bereits ein KI-Tool, Magnet Griffeye, das eine automatische Kategorisierung der Mediendateien ermöglicht. Neben dieser visuellen Beweislage gewinnen auch Texte aus Foren und Chats zunehmend an Bedeutung, da sie wichtige Hinweise auf Vernetzungen im Deliktsfeld sowie auf laufende Missbrauchsdelikte liefern können. Die derzeitige manuelle Textauswertung stößt jedoch angesichts der großen Datenmengen an ihre Grenzen und kann nicht mehr vollständig bewältigt werden (Polizei Schleswig-Holstein 2025, S. 4 f.).

Vor diesem Hintergrund wird im Rahmen des Projekts FRANKA ein Tool entwickelt, das die computerunterstützte Auswertung von Texten realisieren soll. Es ist der Einsatz eines LLMs aus dem Bereich Deep Learning beabsichtigt. Die Nutzung einer Retrieval-Augmented-Generation-Architektur (RAG-Architektur) ermöglicht dabei, Textdateien bei FRANKA hochzuladen und mittels gezielter Fragestellungen fall- und kontextbezogene Informationen zu generieren. Damit werden auch ein generelles Textverständnis und die Klassifizierung der Textinhalte hinsichtlich ihrer Relevanz für das Ermittlungsverfahren geboten. Es ist bereits ein Prototyp entwickelt, welcher nach Testungen weiter optimiert werden soll. Nach der Implementierung des Tools ist eine Beschleunigung und Effizienz- sowie Qualitätssteigerung der Ermittlungsarbeit potenziell möglich (Polizei Schleswig-Holstein 2025, S. 4–7).

Trotz der Chancen, die der Einsatz von KI-Systemen wie FRANKA bietet, ist es essenziell, auch die damit verbundenen Risiken kritisch zu betrachten (Bundesamt für Sicherheit in der Informationstechnik 2025, S. 13). Ethik als philosophische Disziplin beschäftigt sich mit Fragen nach dem Richtig und Falsch sowie dem Guten und Schlechten (Grimm, Kuhnert 2024, S. 94; Heine et al. 2023, S. 168). Die KI-Ethik reflektiert dabei systematisch, was KI-Systeme leisten sollen (Müller, Hähnel 2024, S. 12 f.). Zudem entfalten ethische Leitlinien und Empfehlungen eine Bedeutung, um aufzeigen zu können, welche Werte im Zentrum einer Entwicklung stehen (Grimm, Kuhnert 2024, S. 96). Die Beachtung einer verantwortungsvollen Entwicklung und Anwendung von KI-Systemen, wie hier FRANKA, stellt eine wichtige Grundlage für die Akzeptanz der Anwendungen dar (Heesen et al. 2020, S. 3) und ist bei der Polizei maßgeblich. Eine individuelle Analyse einzelner Tools ist dabei erforderlich, da unterschiedliche KI-Systeme verschiedene Risiken mit sich bringen. Im Fokus sollte der Nutzen hinsichtlich des Wohls der Menschen stehen. Bei polizeilichen Anwendungen ist zusätzlich hervorzuheben, dass diese funktionieren und die finalen Entscheidungen beim Menschen liegen müssen (Bitkom e. V. 2023, S. 12 f.).

Eine Regulierung von KI zeigt sich in dem am 01.08.2024 in Kraft getretenen Artificial Intelligence Act (AI Act). Die europäische Verordnung schafft eine neue rechtliche Grundlage und bezieht dabei auch ethische Komponenten mit ein. Die Förderung einer vertrauenswürdigen und menschenzentrierten KI sowie die gleichzeitige Gewährleistung eines hohen Schutzniveaus vor schädlicher Wirkung von KI in Bezug auf Sicherheit, Gesundheit und Grundrechte sind neben der Förderung von Innovation als Ziele des AI Acts zu nennen. Die Verordnung verfolgt einen risikoorientierten Ansatz, unterscheidet dabei zwischen vier Kategorien (minimales, geringes, hohes und unannehmbares Risiko) und macht verschiedene Vorgaben oder Verbote wie Transparenz- und Kontrollanforderungen je nach Einordnung (Ebers 2024, S. 64 f., 68 f.). Eine Berücksichtigung von Ethik in Bezug auf KI wird somit durch die rechtliche Regulierung systematisch verankert.

Damit stellt die Ethik einen elementaren Bestandteil der Entwicklung von KI dar und mögliche Risiken müssen sorgfältig geprüft werden (Grimm, Kuhnert 2024, S. 98). Es können verschiedene Leitfäden zur ethischen KI-Entwicklung herangezogen werden, welche von der Unternehmens- bis hin zur internationalen Ebene gestaltet werden (Bitkom e. V. 2023, S. 13; Deutscher Ethikrat 2023, S. 108 f.; Grimm, Kuhnert 2024, S. 96 f.; Heine et al. 2023, S. 168; Heesen et al. 2020, S. 3; Zühlke 2023). Im Folgenden wird sich auf das Responsible AI Framework von Zühlke bezogen (Zühlke 2023).

Material und Methoden

Das Responsible AI Framework von Zühlke bietet einen umfassenden Bewertungsrahmen, der ethische, rechtliche und technische Anforderungen gleichermaßen adressiert. Es handelt sich um eine systematische und praxisorientierte Methodik zur ethischen Bewertung und Entwicklung von KI und wird in diesem Beitrag auf FRANKA angewendet. Das Framework ermöglicht die strukturierte Reflexion entlang klar definierter Kriterien. Es werden dabei die menschliche, die Daten-, die Modell- und die Nachhaltigkeitsebene betrachtet (Zühlke 2023). Aufgrund des begrenzten Umfangs dieses Beitrags wird sich ausschließlich auf die menschliche Ebene bezogen. Eine abschließende ethische Bewertung von FRANKA auf Grundlage des Frameworks erfolgt somit nicht.

Um relevante Informationen zu erlangen, wurden zwei qualitative, leitfadengestützte Expert*inneninterviews geführt (Gläser, Laudel 2010, S. 111–116) und mit einer strukturierenden qualitativen Inhaltsanalyse ausgewertet (Dresing, Pehl 2024, S. 33–41; Gläser, Laudel 2010, S. 197–204). Die Interviews wurden mit der Projektleiterin (PLin, Interview I) sowie dem stellvertretenden Projektleiter (stellv. PL, Interview II) von FRANKA geführt. Die Stichprobe ist bewusst gewählt, da beide Personen projektspezifische Rollen einnehmen, über relevantes Wissen verfügen und so die Sicht der Entwickler*innen darstellen können. Der stellv. PL (zuvor Projektleiter) ist dabei im Gegensatz zur aktuellen PLin von Beginn an mit FRANKA betraut, sodass der gesamte Entwicklungszeitraum abgedeckt wird (Interview I, 2; Interview II, 4). Anzumerken ist, dass nicht alle beteiligten Entwickler*innen interviewt werden. Auch die Wahrnehmung potenzieller Anwender*innen, die an dem Entwicklungsprozess beteiligt sind, wird durch diese Vorgehensweise nicht abgedeckt (Gläser, Laudel 2010, S. 117 f.). Die Teilnehmenden wurden vor den Interviews über den Forschungszweck in Kenntnis gesetzt und Einverständniserklärungen wurden eingeholt. Die Interviews fanden am 16.10.2025 in Präsenz statt und wurden mit Zustimmung aufgezeichnet. Die Verschriftung erfolgte mithilfe des Programms aTrain nach einem Regelsystem für eine inhaltlich-semantische Transkription (Dresing, Pehl 2024, S. 21–32).

Ergebnisse

Im Rahmen der Interviews wurde einleitend auf den polizeilichen Hintergrund von der PLin und dem PL sowie allgemein auf das Projekt FRANKA eingegangen. Anschließend wurde FRANKA ethisch betrachtet und die vier Ebenen des Responsible AI Frameworks thematisiert (Interview I; Interview II). Grundlegend kann festgestellt werden, dass im Rahmen der Interviews kein ethisches Konzept hinsichtlich der Entwicklung von FRANKA thematisiert oder beschrieben wird. Die PLin betont allgemein eine ethische Relevanz (Interview I, 26) und der stellv. PL berichtet, an verschiedenen Fachvorträgen dazu teilgenommen zu haben. Ein Bewusstsein für die Relevanz der Ethik ist aus seiner Sicht vorhanden (Interview II, 22). Perspektivisch könnten auf Grundlage von Nutzerfeedbacks auf der ethischen Ebene weitere Entwicklungen erfolgen (Interview II, 64).

Weiter ist festzuhalten, dass sich FRANKA aktuell im Entwicklungs- bzw. Forschungsstadium befindet. Hierbei erfolgt die fortlaufende Integration verschiedener Funktionalitäten, welche zu einer abweichenden regulatorischen Einordnung führen könnten (Interview I, 20;

Interview II, 12). Die abschließende Einordnung von FRANKA im Kontext des AI Acts ist daher bislang nicht abschließend erfolgt und wird nach Abschluss der technischen Entwicklung durchgeführt (Interview II, 16, 18). Es werden im Folgenden die Ergebnisse der Interviews hinsichtlich der menschlichen Ebene kategorisiert dargestellt. Diese Ebene fokussiert auf die Auswirkungen und Risiken des KI-Einsatzes für Individuen und gesellschaftliche Gruppen. Im Mittelpunkt steht die Frage, inwieweit eine KI-Anwendung das Wohl der betroffenen Menschen fördert und ob mögliche negative Folgen ausreichend berücksichtigt und gemindert werden. Diese Ebene verlangt zudem menschenzentrierte Kontroll- und Aufsichtsmechanismen, damit Fehlentwicklungen erkannt und korrigiert werden können (Zühlke 2023).

Förderung des Wohls der Menschheit

FRANKA wird als Ermittlungsunterstützung entwickelt, deren Hauptnutzen im Auswerten großer Textmengen und Generieren von Hinweisen durch ein Sprachmodell besteht (Interview I, 6, 24). Es soll die polizeiliche Sachbearbeitung durch Zusammenfassungen, Klassifizierungen (nach relevant bzw. nicht relevant) und Priorisierungen von Daten erleichtern und gezielte Rückfragen ermöglichen (Interview I, 24). Die massive Entlastung und Zeitersparnis in der Sachbearbeitung sind zudem erklärtes Ziel (Interview II, 10, 20). Hervorzuheben ist, dass FRANKA ausschließlich als Hilfsmittel gedacht ist und die menschlichen Sachbearbeiter*innen sowie deren Expertise nicht ersetzen soll (Interview I, 64; Interview II, 10, 20). Ein zentrales Thema bei der Entwicklung von FRANKA ist die Sicherstellung der Qualität sowie die dafür notwendigen Rahmenbedingungen. Die IT-Sicherheit und der Datenschutz werden als wichtige Fokusthemen genannt. Es wird darauf geachtet, den entsprechenden Anforderungen zu genügen und somit eine adäquate Sicherheit zu gewährleisten (Interview I, 20).

Als weiterer Aspekt wird das Vertrauen der Sachbearbeiter*innen in FRANKA angesprochen. Der stellv. PL unterstreicht, dass ein nachhaltiges Vertrauen in das Tool nur durch ein fundiertes Verständnis seiner Funktionsweise entstehen kann. Durch gezielte Schulungen kann es maßgeblich aufgebaut werden. Zudem trägt die Nachvollziehbarkeit der Systemantworten sowie deren Qualität entscheidend dazu bei, das notwendige Vertrauen zu fördern (Interview I, 32; Interview II, 28). Der stellv. PL hebt die Verlässlichkeit der KI als wesentlichen Wert hervor. Diese soll gewährleisten, dass FRANKA der polizeilichen Arbeit effektiv dient und zuverlässig funktioniert (Interview II, 24, 26). Die PLin betont, dass FRANKA kontinuierlich weiterentwickelt und an aktuelle Standards sowie Anforderungen angepasst werden muss (Interview I, 62). Auch potenzielle Nutzer*innen werden in den Prozess in Form von Testungen und eines Austausches einbezogen, um mit Grundlage der Fachexpertise Anregungen geben zu können und so zum Nutzen und der Optimierung der KI beizutragen (Interview I, 34; Interview II, 30, 32).

Berücksichtigung von negativen Folgen und Fehlern sowie deren Mitigierung

Die PLin beschreibt, dass fehlerhafte Zusammenfassungen polizeilich relevante Informationen ausblenden könnten. Dadurch könnten wichtige Hinweise verloren gehen oder übersehen werden, sodass die Wirksamkeit der Strafverfolgung und Gefahrenabwehr eingeschränkt werden könnte. Ferner besteht die Gefahr, dass FRANKA Hinweise benennt, die

gar nicht existieren (Halluzinationen) (Interview I, 26). Der stellv. PL ergänzt dazu die Gefahr der falschen Nutzung des Tools. Er erläutert, dass es zu unvollständigen Auswertungen führen könnte, wenn im Rahmen von Priorisierungen beispielsweise nicht mehr alle Chats von einem Asservat betrachtet werden. Straftaten aus anderen Deliktsbereichen könnten dadurch möglicherweise nicht erkannt werden. Dabei hält er offen, ob dies tatsächlich ein großes Problem darstellt. Er gibt an, dass eine Kommunikation zur Begegnung dieses Risikos erforderlich ist (Interview II, 38, 40). Verzerrungen (Bias) und nicht intendiertes Verhalten von KI-Anwendungen sind mehrfach problematisiert und im Rahmen von Fachvorträgen thematisiert worden. An diesen hat der stellv. PL beigewohnt und ein Bewusstsein dafür ist generiert worden (Interview II, 22). Er hebt die Verlässlichkeit des Tools als wesentlichen Wert hervor. Diese soll gewährleisten, dass FRANKA der polizeilichen Arbeit effektiv dient und zuverlässig funktioniert (Interview II, 24, 26). Trotz der benannten Herausforderungen wird aktuell kein standardisierter Benchmarktest eingesetzt, um die fehlerfreie Funktion zu überprüfen (Interview II, 22) und es wurden nicht viele Maßnahmen zur Vermeidung von Bias und Diskriminierung durchgeführt (Interview II, 46).

Weiter wird von der PLin und dem stellv. PL beschrieben, dass im Rahmen der Nutzung von FRANKA die Sachbearbeiter*innen gezielt durch eine Hinweisseite auf den Nutzen des Systems aufmerksam gemacht werden, wobei eine Bestätigung dieser Hinweise erforderlich ist. Dabei wird auch ausdrücklich darauf hingewiesen, dass FRANKA Fehler machen kann. Dieser Hinweis zur Fehleranfälligkeit wird zudem regelmäßig auch in der Benutzeroberfläche der Anwendung wiederholt. Ergänzend wird die vorgesehene Nutzung von FRANKA ausführlich in einem Benutzerhandbuch beschrieben, welches den Nutzer*innen als Orientierung dient (Interview I, 28; Interview II, 34, 36). Für die PLin stellt die Verwendung halluzinierter Inhalte als Beweis vor Gericht ein unvertretbares Risiko dar (Interview I, 36). Der stellv. PL benennt im Gegensatz dazu die missbräuchliche Nutzung des Tools. Diesem kann mit Nutzungsbedingungen und Einverständniserklärungen begegnet werden, was eng mit Schulungen verbunden ist (Interview II, 34, 36).

Zur Reduzierung und dem Entgegenwirken von Fehlern wie Verzerrungen und Halluzinationen wird ein RAG-System ergänzend zum Sprachmodell eingesetzt. Dadurch wird sichergestellt, dass nur relevante Inhalte aus den Dokumenten verwendet und Allgemeinwissen ausgeschlossen wird, wobei Fehler nicht ganz vermieden werden können. Durch eine menschliche Nachprüfung aller Hinweise von FRANKA ist das Risiko jedoch minimiert (Interview I, 26, 46). Werden Fehler durch Kontrollen und Routinetests im Rahmen der Entwicklung festgestellt, werden diese durch Systemanpassungen, Sicherheitsmechanismen, Kontexteinstellungen oder gezielte Systemverbesserungen behoben bzw. ihnen entgegengewirkt (Interview I, 26; Interview II, 64, 34, 36). Die Sicherstellung der Qualität und die dafür notwendigen Maßnahmen stehen bei der Entwicklung von FRANKA im Mittelpunkt (Interview I, 20). Eine Sensibilisierung der Sachbearbeiter*innen hinsichtlich eines Feedbacks zu Fehlern im Echtbetrieb ist aus Sicht des stellv. PL notwendig (Interview II, 52).

Kontroll- und Aufsichtsmechanismen durch den Menschen

Einen zentralen Aspekt im Umgang mit FRANKA stellt die menschliche Kontrolle durch die zukünftigen Nutzer*innen dar. Um den Risiken entgegenzuwirken, wird eine sorgfältige Verifikation der vom System generierten Inhalte gefordert. Die Projektleitung betont, dass die Angaben von FRANKA lediglich als Hinweise zu verstehen sind. Die eigentlichen Beweise müssen von den Ermittler*innen eigenständig mittels der Originaldaten generiert werden. Zudem ist es nicht zulässig, von FRANKA erstellte Zusammenfassungen direkt in die Ermittlungsakte zu übernehmen. Risiken sind daher mitigiert (Interview I, 26, 28, 64; Interview II, 18, 54, 56). Ein wesentlicher Mechanismus zur Kontrolle und Verstärkung der positiven Effekte von FRANKA ist die Sicherstellung der Nachvollziehbarkeit der generierten Antworten. Geplant ist, dass FRANKA künftig die Quellverweise direkt bei den Ausgaben anzeigt, wodurch eine unmittelbare Überprüfung der Informationen ermöglicht wird. Diese Transparenz dient nicht nur der Kontrolle durch die Nutzer*innen, sondern kann auch das Vertrauen in das System nachhaltig stärken (Interview I, 30).

Um diese Kontroll- und Aufsichtsmechanismen sicherzustellen, ist eine umfassende Schulung der Nutzer*innen erforderlich. In dieser sollen sie über die Funktionsweise von Sprachmodellen aufgeklärt werden sowie über die potenziellen Risiken, die mit der Nutzung solcher Systeme einhergehen (Interview I, 26, 28; Interview II, 34, 36). Es wird im Rahmen der Interviews verdeutlicht, dass die Nutzer*innen die vollständige Verantwortung für ihre Ermittlungsergebnisse tragen und FRANKA ausschließlich als Unterstützungstool zu verstehen ist (Interview I, 48; Interview II, 54, 56).

Diskussion

Im Folgenden werden die gewonnenen Erkenntnisse hinsichtlich der menschlichen Ebene diskutiert und insbesondere die in Abschnitt 4 dargestellten Ergebnisse kritisch betrachtet. Trotz der bewussten Auswahl der Interviewpartner*innen ist zu bedenken, dass die Aussagen von zwei Personen keine repräsentativen Rückschlüsse zulassen dürfen. Es werden vielmehr die subjektiven Ansichten der Projektleitung dargestellt. Die Wahrnehmung potenzieller Anwender*innen sowie weiterer Entwickler*innen werden beispielsweise nicht abgedeckt. Zudem ist anzumerken, dass die PLin nicht während des gesamten Entwicklungszeitraums mit dem Projekt betraut war und somit nicht alle Entwicklungsschritte begleitet hat (Interview I, 2).

Dass im Rahmen der Interviews kein ethisches Konzept benannt wird, führt zu der Erkenntnis, dass bei der Entwicklung von FRANKA kein leitfadengestützter Umgang mit der Ethik verfolgt wurde. Ein gezielter Umgang mit Ethik wird jedoch von verschiedenen Stellen gefordert bzw. empfohlen (Bitkom e. V. 2023, S. 3; Grimm, Kuhnert 2024, S. 96 f.; Heesen et al. 2020, S. 3; Zühlke 2023). Zudem erschwert die fehlende Kategorisierung von FRANKA durch die Projektleitung hinsichtlich des AI Acts die gezielte Betrachtung etwaiger geforderter ethischer Voraussetzungen (Ebers 2024, S. 64–69; Interview I, 20; Interview II, 16, 18). Es stellt sich daher die Frage, ob die geforderte verantwortungsvolle Entwicklung von KI bei FRANKA erfüllt wird.

Förderung des Wohls der Menschheit

KI sollte das Potenzial bieten, zum Wohl der Menschheit beizutragen (Bitkom e. V. 2023, S. 12 f.; Heesen et al. 2020, S.3; Zühlke 2023). Dies könnte als allgemeine Trivialität bewertet werden (Müller, Hähnel 2024, S. 28) und sollte daher näher definiert werden. Dabei ist der Ansatz verfolgbar, dass der polizeiliche Einsatz von KI das Ziel anstrebt, den staatlichen Auftrag zur Gewährleistung von Sicherheit effektiv zu unterstützen (Golla 2022, S. 1202). Hinsichtlich FRANKA ist dabei die Effizienz- und Qualitätssteigerung der polizeilichen Ermittlungsarbeit im Bereich der Kinder- und Jugendpornografie aufzuführen (Haas 2024, S. 82 f.; Polizei Schleswig-Holstein 2025, S. 4–7). Die Analyse der Interviewergebnisse sowie der Projektunterlagen zeigt auf, dass das Tool mit dieser Zielrichtung entwickelt wird und dass diese Vorteile im Rahmen eines verantwortungsvollen Einsatzes einer adäquaten Strafverfolgung dienen sollen. Die massive Entlastung der Sachbearbeiter*innen durch die Nutzung der Ermittlungsunterstützung kann zu einer effizienteren Fallbearbeitung führen, eine vollständige Auswertung von Chats ermöglichen und somit einen positiven gesellschaftlichen Beitrag leisten. Es wird betont, dass FRANKA dabei ausschließlich als Hilfsmittel fungiert und menschliche Ermittler*innen nicht ersetzt (Interview I, 6, 24, 64; Interview II, 10, 20).

Ein flexibler Entwicklungsprozess mit regelmäßiger Anpassung an Erkenntnisse aus der Praxis wird durch die Projektleitung ebenso wie durch die Literatur als notwendig erachtet, um die Funktionalität, Qualität und Akzeptanz von FRANKA nachhaltig sicherzustellen (Haas 2024, S. 85; Interview I, 34, 62; Interview II, 30, 32). Unbeantwortet bleibt, inwiefern ein fertiges Produkt tatsächlich zur Steigerung der Effizienz und Qualität beitragen wird und wie es messbar dargestellt werden kann. Es scheint erforderlich, diese Aspekte zu evaluieren, um einen etwaigen positiven Nutzen nachweisen zu können. Das Vertrauen der Sachbearbeiter*innen in FRANKA stellt eine grundlegende Voraussetzung für die erfolgreiche Nutzung dar. Erst auf dieser Basis werden eine Akzeptanz sowie eine zweckmäßige Nutzung des Systems möglich und somit das Wohl der Menschheit im Sinne einer effizienteren und sichereren Ermittlung gefördert (Heesen et al. 2020, S. 3). In den Interviews sind Schulungen sowie schriftliche Hinweise und Erläuterungen beschrieben, die anvisiert werden. Dadurch soll ein Verständnis für die KI sowie im weiteren Sinne ein Vertrauen entwickelt werden (Interview I, 32; Interview II, 28). Ausstehend ist an dieser Stelle ein Umsetzungskonzept für Schulungen sowie die Messbarkeit des Vertrauens. Es bleibt abzuwarten, wie die Umsetzung erfolgt, ein Vertrauen evaluiert wird und ein Nachweis hinsichtlich des Wohls der Menschheit aufgezeigt werden kann. Es lässt sich zudem feststellen, dass durch FRANKA Grundrechte geschützt werden könnten, was wiederum die Gemeinwohlorientierung unterstreichen würde. Durch die Hinweise von FRANKA erscheint es möglich, dass offensichtlich irrelevante Daten durch die Sachbearbeitung nicht gesichtet werden und so ein geringerer Grundrechtseingriff erfolgt (Bitkom e. V. 2023, S. 4; Interview II, 38, 40).

Berücksichtigung von negativen Folgen und Fehlern sowie deren Mitigierung

Bei der Entwicklung von FRANKA werden potenzielle Fehlerquellen und negative Folgen wie von der Literatur gefordert kritisch reflektiert (Bundesamt für Sicherheit in der Informationstechnik 2025, S. 13; Grimm, Kuhnert 2024, S. 98; Zühlke 2023). Zu bedenken ist dabei, dass menschlichen Fehlern im Arbeitsprozess mit einer gewissen Toleranz begegnet, während

von KI vielmehr eine Perfektion erwartet wird (Haas 2024, S. 85). Die ethische Problematik fehlerhafter Ergebnisse wird im Rahmen der Interviews hervorgehoben und die mögliche Beeinträchtigung der polizeilichen Strafverfolgung und Gefahrenabwehr aufgeführt. Trotz bereits bestehender Maßnahmen zur Reduzierung von Bias, Halluzinationen u. Ä. im Entwicklungsprozess scheint es Potenzial zu geben, diese noch weiter zu minimieren. Hier sind beispielhaft standardisierte Benchmarktests zur Überprüfung der fehlerfreien Funktion von FRANKA aufzuführen, welche selbst von dem stellv. PL benannt werden (Interview I, 26, 28; Interview II, 22, 34, 36, 38, 40, 46).

Aus den Interviews ergibt sich weiter, dass Nutzer*innen präventiv gezielt und transparent auf etwaige Fehler durch FRANKA hingewiesen werden sollen, was sich auch in dem Benutzerhandbuch wiederfindet (Interview I, 28; Interview II, 34, 36; Polizei Schleswig-Holstein, o. D., S. 5–15). Dies kann im Zusammenhang mit der erforderlichen menschlichen Expertise bewertet werden und zeigt die Bedeutung der Sachbearbeiter*innen auf (Bitkom e. V. 2023, S. 12 f.; Deutscher Ethikrat 2023, S. 327–332). Es scheint, als würde bei der Anwendung von FRANKA vor allem die Kontrolle durch die Sachbearbeitung als Schutzmechanismus im Fokus stehen.

Kontroll- und Aufsichtsmechanismen durch den Menschen

Die menschliche Kontrolle und Aufsicht scheinen bei der Entwicklung von FRANKA als zentrales Element berücksichtigt zu werden. Trotz technischer Maßnahmen zur Minimierung von Fehlern wird eine menschliche Nachprüfung bzw. Verifikation aller Hinweise von FRANKA als unabdingbar von der Projektleitung beschrieben und auch im Benutzerhandbuch aufgeführt. Auch werden im Entwicklungsprozess im Rahmen von Tests menschliche Überprüfungen und Bewertungen vollzogen (Interview I, 20, 26, 28, 46, 64; Interview II, 18, 54, 56, Polizei Schleswig-Holstein, o. D., S. 3–7). Es zeigt sich, dass bei FRANKA menschliche Kontrolle nicht nur technisch durch Begleitsysteme, sondern vor allem organisatorisch und prozessual durch klare Vorgaben integriert ist und die Forderung nach einer endgültigen Entscheidung durch den Menschen erfüllt wird (Bitkom e. V. 2023, S. 12 f.). Es wird deutlich, dass die wesentlichen Aspekte der von Zühlke beschriebenen menschlichen Ebene offensichtlich beachtet und umgesetzt werden. Eine abschließende ethische Bewertung bleibt in diesem Beitrag aufgrund des eingeschränkten Betrachtungsrahmens offen.

Schlussfolgerungen

Um einen gerechten und rechtsstaatlichen Einsatz von KI zu gewährleisten, ist eine verantwortungsvolle Entwicklung maßgeblich. Ethik stellt einen unverzichtbaren Aspekt bei der Entwicklung von KI-Systemen dar und sollte daher auch bei der Entwicklung von FRANKA fokussiert werden. Auch wenn sich im Rahmen des Projekts offensichtlich bereits mit ethischen Aspekten auseinandergesetzt wird, erscheint ein konzeptionelles Vorgehen empfehlenswert. So kann sichergestellt werden, dass alle wesentlichen Aspekte beachtet und umgesetzt werden. Auch die Kategorisierung hinsichtlich des AI Acts bereits während des Entwicklungsprozesses wirkt zielführend, um etwaige rechtliche und ethische Vorga-

ben bereits frühzeitig beachten zu können. Dieser Ansatz verdeutlicht die Balance zwischen technologischem Fortschritt und ethischer Verantwortung, die bei der Integration von KI-Lösungen in sensible Bereiche wie die Polizeiarbeit gewahrt bleiben sollte.

Es ist festzuhalten, dass die Integration von KI-Systemen in die polizeiliche Arbeit nur dann einen nachhaltigen Beitrag zum Gemeinwohl leisten kann, wenn sie technisch verlässlich, rechtlich abgesichert und ethisch reflektiert erfolgt. Durch die Kombination dieser Aspekte kann KI wie FRANKA die Effektivität der Polizei steigern und gleichzeitig den Schutz der Grundrechte und das Vertrauen der Gesellschaft sicherstellen. Damit stellt die verantwortungsvolle Nutzung von KI eine Chance dar, das Wohlergehen der Menschheit gezielt zu fördern und polizeiliche Aufgaben auf eine zukunftsfähige Grundlage zu stellen. Die Kombination aus innovativer Technologie und ethischer Reflexion bietet somit die Grundlage für eine moderne und zugleich rechtlich fundierte Strafverfolgung.

Um die Entwicklung von FRANKA umfassend ethisch zu bewerten, sind weitere Forschungen erforderlich. Neben der Betrachtung der weiteren durch Zühlke beschriebenen Ebenen auf Grundlage der bereits geführten Interviews erscheint eine Ausweitung der Interviews auf weitere Projektentwickler*innen sowie etwaige Nutzer*innen sinnvoll. Die erhobenen Daten könnten auch anhand anderer Frameworks bewertet werden, sodass weitere ethische Ansätze einbezogen und miteinander verglichen werden könnten. Perspektivisch ist zudem eine ethische Bewertung des fertigen Tools sowie der Anwendung durch die Sachbearbeitung anzustreben.

Literaturverzeichnis

Abteilung Digitalisierung und Zentrales IT-Management der Landesregierung (StK 3) (2024). Gesamtplan für Informationstechnik und Digitalisierung 2025, Kiel.

Bitkom e. V. (2023). KI in der Polizei – Einsatzpotentiale und Lösungsansätze zur Implementierung, Berlin.

Bundesamt für Sicherheit in der Informationstechnik (2025). Generative KI-Modelle. Chancen und Risiken für Industrie und Behörden, Bonn.

Deutscher Ethikrat (2023). Mensch und Maschine – Herausforderungen durch Künstliche Intelligenz, Berlin.

Dresing T, Pehl T (2024). Praxisbuch Interview, Transkription & Analyse. Anleitungen und Regelsysteme für qualitativ Forschende. Eigenverlag, Marburg.

Ebers M (2024). § 2 Regulierung generativer Künstlicher Intelligenz in der KI-VO. In: Ebers M, Quarch B M (Hrsg.) (2024): Rechtshandbuch ChatGPT. KI-basierte Sprachmodelle in der Praxis. Nomos, Baden-Baden, 43–91.

Gläser J, Laudel G (2010). Experteninterviews und qualitative Inhaltsanalyse als Instrumente rekonstruierender Untersuchungen. VS Verlag, Wiesbaden.

Grimm P, Kuhnert S (2024). KI und Ethik. In: Seeger C. (Hrsg.): KI in der Unternehmenspraxis. Technologie–Recht–Ethik–Use Cases. Schäffer-Poeschel Verlag, Stuttgart.

Golla S J (2022). KI-Einsatz bei der Polizei. In: Chibanguza K, Kuß C, Steege H (Hrsg.): Künstliche Intelligenz. Recht und Praxis automatisierter und autonomer Systeme. Nomos, Baden-Baden, 1201–1213.

Haas S (2024). Von der Theorie zur Praxis: Generative KI in der modernen Polizeiarbeit. In: Honekamp W, Labudde D (Hrsg.): Polizei-Informatik 2024. Rediroma-Verlag, Remscheid, 80–86.

Heesen J, Grunwald A, Matzner T, Roßnagel A (2020). Ethik-Briefing. Leitfaden für eine verantwortungsvolle Entwicklung und Anwendung von KI-Systemen – Whitepaper aus der Plattform Lernende Systeme, München.

Heine M, Dhungel A-K, Schrills T, Wessel D (2023). Künstliche Intelligenz in öffentlichen Verwaltungen. Grundlagen, Chancen, Herausforderungen und Einsatzszenarien. Springer Nature, Wiesbaden.

Landesportal Schleswig-Holstein (2023). Mit KI Chats von Verdächtigen lesen. schleswig-holstein.de/DE/landesregierung/ministerien-behoerden/I/_startseite/Artikel2023/III/230817_cds_franka (15.11.2025).

Müller V C, Hähnel M (2024). Was ist, was kann, was soll KI? Ein philosophisches Gespräch. Felix Meiner Verlag, Hamburg.

Polizei Schleswig-Holstein, ohne Datum. Benutzerhandbuch für FRANKA (Fragen- und Antwortsystem zur KI-basierten Auswertung von Chats und Texten).

Polizei Schleswig-Holstein (2025). Frage- und Antwortsystem für KI-basierte Auswertung von Chats und Texten − FRANKA. Projektauftrag Umsetzungsprojekt II.

Povalej R, Rittelmeier H, Fähndrich J, Berner S, Honekamp W, Labudde D (2021). Die Enkel von Locard. Analyse digitaler Spuren in der forensischen Informatik. link.springer.com/article/10.1007/s00287-021-01393-5 (15.11.2025).

Zühlke (2023). Responsible AI: Entwicklung ethischer KI-Anwendungen. zuehlke.com/de/insights/responsible-ai-entwicklung-ethischer-ki-anwendungen (15.11.2025).

KI-gestützte Videoanalyse: Ethische Bewertung automatisierter Verhaltens- und Bewegungserkennungssysteme in der niedersächsischen Landespolizei

Marcel Janzik

Die rasante Entwicklung Künstlicher Intelligenz (KI) transformiert gesellschaftliche Bereiche, eröffnet neue Handlungsmöglichkeiten und wirft grundlegende ethische Fragen auf. Besonders im Kontext staatlicher Sicherheitsarchitekturen wird KI ein Potenzial zur Steigerung der Effektivität polizeilicher Arbeit zugeschrieben (Bitkom e. V. 2023, S. 3–12). Öffentliche Videoüberwachung, seit Jahrzehnten ein Instrument der Gefahrenabwehr, erfährt durch KI-gestützte Videoanalyse eine Aufwertung: Systeme werten Situationen in Echtzeit aus, erkennen Verhaltensmuster und alarmieren Sicherheitskräfte automatisiert (Fraunhofer IOSB 2025). Damit verbunden sind jedoch Risiken für Grundrechte wie Privatheit, informationelle Selbstbestimmung und Nichtdiskriminierung (HEG-KI 2019, S. 14–29).

In Deutschland bauen Bundes- und Landespolizeien KI-gestützte Technologien aus und prüfen oder implementieren entsprechende Systeme (Bitkom e. V. 2023, S. 8–9). Debatten um automatisierte Datenanalyse und intelligente Videoüberwachung verleihen der Thematik politische und mediale Dynamik (MDR Sachsen-Anhalt 2025; Zeit Online 2025). Niedersachsen nimmt hierbei eine besondere Stellung ein: Das Landeskriminalamt (LKA) Niedersachsen hat bereits KI-Anwendungen zur Analyse digitaler Beweismittel entwickelt und in die Praxis überführt. Mit der geplanten Einführung intelligenter Videoanalysesysteme steht die Landespolizei vor einem weiteren Modernisierungsschritt, der komplexe ethische Fragen aufwirft (Westermann 2025). Untersuchungen zu Videoüberwachung und Bodycams fokussieren bislang überwiegend technische, rechtliche oder sozialwissenschaftliche Aspekte; ethische Evaluationen sind die Ausnahme.

Vor diesem Hintergrund stellt sich die zentrale Forschungsfrage dieses Beitrags: Wie lässt sich der Einsatz automatisierter Verhaltens- und Bewegungserkennungssysteme in der niedersächsischen Landespolizei ethisch bewerten?

Zur Bearbeitung dieser Forschungsfrage greift dieser Beitrag auf das MEESTAR-Modell (Modell zur ethischen Evaluation soziotechnischer Arrangements) zurück. MEESTAR bietet mit seinen sieben ethischen Dimensionen – Fürsorge, Selbstbestimmung, Sicherheit, Gerechtigkeit, Privatheit, Teilhabe und Selbstverständnis – sowie drei Bewertungsebenen – individuell, organisational und gesellschaftlich – einen Rahmen für die ethische Analyse technologischer Systeme (Manzeschke et al. 2013, S. 13–21; Grüber & Loevskaya 2020, S. 15–18). Diese Arbeit wendet MEESTAR auf automatisierte Verhaltens- und Bewegungserkennungssysteme an und prüft, welche Anforderungen sich daraus für eine ethisch verantwortliche Implementierung in der niedersächsischen Polizei ableiten lassen.

Hintergrund

Zur Einordnung des geplanten Einsatzes KI-gestützter Verhaltens- und Bewegungserkennungssysteme werden technische Grundlagen, der Forschungsstand und zentrale ethische Problemfelder dargestellt. Ergänzend wird die spezifische Rechts- und Entwicklungslage in Niedersachsen skizziert.

Technische Grundlagen automatisierter Verhaltens- und Bewegungserkennungssysteme

KI-gestützte Videoanalysesysteme basieren auf Computer Vision, neuronalen Netzen und Deep-Learning-Algorithmen, die visuelle Daten automatisiert auswerten und so Personen, Objekte und Verhaltensmuster in Echtzeit erkennen und klassifizieren können (Rduch et al. 2024, S. 3–4, 15–17; Jahan et al. 2024, S. 1–8). Sie arbeiten in mehrstufigen Analyseprozessen: Zunächst werden Personen und Objekte identifiziert, anschließend Körperhaltungen und Bewegungsabläufe erfasst, um potenziell relevante Situationen zu erkennen. Moderne Algorithmen können komplexe Muster wie Schlagen, Treten oder verdächtige Bewegungen detektieren und Alarme auslösen (Haritaoglu et al. 2000, S. 809–829). Zentral ist die Unterscheidung zwischen regelbasierten und selbstlernenden Systemen. Während Erstere auf vordefinierten Parametern basieren, nutzen fortschrittliche Systeme maschinelles Lernen, um Verhaltensmuster eigenständig zu erlernen und zu bewerten. Dies ermöglicht eine zunehmend autonome Bewertung von Situationen ohne direkte menschliche Programmierung der Erkennungsmuster (Xiang & Gong 2008).

Forschungsstand zu KI-gestützter Videoanalyse in der Polizeiarbeit

Studien zu KI-gestützter Videoanalyse in der Polizeiarbeit zeichnen ein ambivalentes Bild aus Potenzialen und Risiken.

Internationale Forschungsergebnisse

Eine Untersuchung des Massachusetts Institute of Technology zeigt erhebliche Inkonsistenzen bei der automatisierten Bewertung von Sicherheitssituationen: Große Sprachmodelle wie GPT-4 wurden mit Videos von Wohnungs- und Autoeinbrüchen getestet und klassifizierten vergleichbare Szenen teils als bedrohlich, teils als unproblematisch. Besonders kritisch ist eine systematische Voreingenommenheit: Videos aus überwiegend weißen Wohngegenden wurden seltener als bedrohlich bewertet als vergleichbare Aufnahmen aus überwiegend schwarzen Wohngegenden. Diese „normative Inkonsistenz“ erschwert die Vorhersage des Systemverhaltens und verweist auf strukturelle Diskriminierungsrisiken (Jain et al. 2024, S. 3–8).

Deutsche Forschungslandschaft und Praxisprojekte

In Deutschland entwickelt sich eine differenzierte Forschungslandschaft zu KI in der Polizeiarbeit. Das Projekt KI4POL an der Hochschule der Medien Stuttgart untersucht systematisch Einsatzbereiche für KI, wobei automatisierte Videoüberwachung einen Schwerpunkt bildet. Hervorgehoben werden Entlastungspotenziale für Polizeibeamte und zugleich psychische Belastung bei der manuellen Auswertung problematischen Bildmaterials (Bach 2025). Das

Fraunhofer IOSB (2025) entwickelt im Pilotprojekt *Intelligenter Videoschutz* in Mannheim ein System zur automatisierten Erkennung von Straftaten im öffentlichen Raum. Ziel ist es, Sicherheit durch automatisierte Detektion relevanter Situationen zu erhöhen und zugleich durch Verpixeln im Normalbetrieb Datenschutzstandards zu verbessern. Die bisherigen Erfahrungen zeigen jedoch, dass geeignete Trainingsdaten aus datenschutzrechtlichen Gründen schwer verfügbar sind.

Evaluationsstudien zu verwandten Technologien

Evaluationsstudien zum Bodycam-Einsatz zeigen, dass technische Lösungen in der Polizeiarbeit nicht automatisch die intendierten Effekte erzeugen. Die Forschung dokumentiert sowohl positive Effekte, etwa Deeskalationspotenziale, als auch unerwartete Nebenwirkungen und gegenläufige Entwicklungen: Einzelne Studien deuten auf Gewaltreduktionen hin, andere auf ein erhöhtes Viktimisierungsrisiko für mit Bodycams ausgestattete Polizeikräfte (Adewuyi 2021, S. 6, 13–14; Margies et al. 2024, S. 7–8). Videoüberwachung lässt sich zudem soziologisch als aktiver Konstruktionsprozess verstehen. Technische Konfiguration und berufliche Ermessensspielräume der Polizeikräfte prägen, was als relevante „Realität" sichtbar wird. Empirische Forschung zeigt, dass Subjektivität nicht verschwindet, sondern durch technische Vermittlung verdeckt wird: Subjektive Entscheidungen erhalten durch Objektivierung in Videoform eine „Aura der Authentizität", die ihre Kontingenz maskiert. Videobeweise erscheinen dadurch technisch objektiv, sind aber Ergebnis einer Kette menschlicher Wahlentscheidungen – von der Aufnahmeentscheidung über Bildausschnitte bis zur Speicherung (Ullrich 2018, S. 2–4, 14–16).

Ethische Problemfelder

Die Integration KI-gestützter Videoanalysesysteme in polizeiliche Sicherheitsarchitekturen wirft ethische Fragen jenseits technischer Machbarkeit auf. Effizienzgewinne durch automatisierte Analyse und Echtzeit-Alerts stehen Risiken für Menschenwürde, Privatheit und informationelle Selbstbestimmung gegenüber. Hinzu kommen mögliche Formen algorithmischer Diskriminierung und eine Schwächung demokratischer Kontrolle, wenn Einsatz, Datenverarbeitung und Entscheidungslogiken nicht an klare rechtliche Rahmen, Transparenz- und Kontrollmechanismen gebunden werden (EDPB 2023, S. 5–7, 12–15; FRA 2022, S. 4–9, 31; Mobilio 2023, S. 5–7).

Spezifische Entwicklungen in Niedersachsen

Für die ethische Bewertung ist die Ausgangs- und Regelungssituation in Niedersachsen besonders relevant, da sich hier aktuelle Modernisierungsprojekte und Rahmenbedingungen verdichten.

KI-Strategien und polizeiliche Modernisierung

Niedersachsen nimmt bei der Integration von KI in die Polizeiarbeit eine Vorreiterrolle ein. Das LKA Niedersachsen hat mehrere KI-gestützte Systeme zur Analyse digitaler Beweismittel entwickelt und in den Wirkbetrieb überführt, unter anderem zur automatisierten Erkennung kinderpornografischen Materials (*Kipo Analyzer* und *Tracebook Kipo*) sowie zur Auswertung

verschlüsselter Messenger-Daten (*Tracebook Chats*) (Westermann 2025). Hinzu kommt die gemeinsam mit dem Justizministerium aufgebaute Beweismittelcloud, die die Speicherung, Aufbereitung und KI-gestützte Analyse digitaler Beweismittel von Polizei und Justiz effizienter und sicherer machen soll (De Vries 2025). Perspektivisch soll KI auch in der öffentlichen Videoüberwachung eingesetzt werden. Ein Gesetzesentwurf des Innenministeriums sieht intelligente Kameras vor, die Bewegungsmuster in Echtzeit analysieren und Gefahrensituationen automatisiert melden. Ergänzend ist eine biometrische Echtzeitidentifizierung für eng begrenzte Fahndungsszenarien geplant. Der Entwurf wurde am 4. November 2025 vom Niedersächsischen Landeskabinett zur Einbringung in den Landtag freigegeben und befindet sich im parlamentarischen Verfahren (Nds. StK 2025).

Rechtliche und gesellschaftliche Rahmenbedingungen

Die rechtlichen Grundlagen für Videoüberwachung in Niedersachsen sind mehrstufig verankert: Auf Bundesebene regelt das Bundesdatenschutzgesetz die Videoüberwachung öffentlich zugänglicher Räume, auf Landesebene das Niedersächsische Polizei- und Ordnungsbehördengesetz sowie das Niedersächsische Versammlungsgesetz. Übergreifend gilt seit 2024 der EU AI Act, der Hochrisiko-KI-Systeme strikten Anforderungen an Transparenz, Audit und Kontrolle unterstellt. Gleichzeitig zeigen sich Regelungslücken: Die bestehenden Gesetze wurden für traditionelle Videoüberwachung konzipiert und berücksichtigen nicht die besonderen Herausforderungen der KI-gestützten Analyse, insbesondere algorithmische Diskriminierung, automatisierte Entscheidungsfindung und unklare Verantwortlichkeiten. Für den geplanten Einsatz von KI-Videoanalysesystemen müssen diese Normen um spezifische Regelungen ergänzt werden, die die besonderen Herausforderungen algorithmenbasierter Analyse adressieren (Kolleck & Orwat 2020, S. 33–40; Niedersächsischer Landtag 2024). Der Landesdatenschutzbeauftragte von Niedersachsen, Denis Lehmkemper, kündigte an, den Gesetzesentwurf zur KI-gestützten Videoüberwachung intensiv prüfen zu wollen, und betonte: „KI-Werkzeuge werden die Polizeiarbeit massiv verändern. Wir brauchen daher klare Regeln." Dies unterstreicht die Notwendigkeit einer fundierten ethischen und rechtlichen Bewertung, bevor derartige Systeme in großem Umfang implementiert werden (NDR 2025).

Methodik: Ethische Evaluation mit MEESTAR

Die Methodik orientiert sich an der Frage nach den ethischen Rahmenbedingungen für den Einsatz automatisierter Verhaltens- und Bewegungserkennungssysteme in der niedersächsischen Landespolizei. Ziel ist es, die ethischen Spannungsfelder zu erfassen und daraus handlungsorientierte Empfehlungen abzuleiten.

Auswahl und Begründung des Analyserahmens

Als Analyserahmen wird das MEESTAR-Modell genutzt. Es strukturiert ethische Fragen entlang sieben Dimensionen – Fürsorge, Selbstbestimmung, Sicherheit, Gerechtigkeit, Privatheit, Teilhabe und Selbstverständnis – sowie auf drei Ebenen: individuell, organisational und gesellschaftlich (Manzeschke et al. 2013, S. 13–21; Grüber & Loevskaya 2020, S. 15–18). Es macht Wertkonflikte (z. B. Sicherheit vs. Privatheit, Effizienz vs. Kontrolle) sichtbar, ohne sie vorab zu hierarchisieren, und ermöglicht eine Mehrebenenanalyse (Grüber & Loevskaya

2020, S. 15–18). Das Modell wurde bereits in vergleichbaren Kontexten eingesetzt, etwa zur Bewertung der Corona-Warn-App (D'Angelo et al. 2021), und ist ausdrücklich auf andere soziotechnische Arrangements übertragbar (Weber 2016, S. 1). Alternative Ansätze wie Principlism (Beauchamp & Childress 2019) oder Value Sensitive Design (Friedman et al. 2008) bieten wichtige normative Orientierung, verfügen jedoch entweder nicht über eine ausgearbeitete Mehrebenenstruktur oder sind primär auf prospektive Systemgestaltung ausgerichtet und daher für die Bewertung bereits geplanter Systeme weniger geeignet.

Methodisches Vorgehen

Aufgrund des begrenzten Umfangs wird MEESTAR exemplarisch auf zwei ethisch besonders relevante Dimensionen angewendet: Gerechtigkeit und Privatheit. Beide werden jeweils auf den drei Analyseebenen – individuell, organisational und gesellschaftlich – untersucht. Grundlage ist eine systematische Auswertung einschlägiger Fachliteratur, aus der moralisch relevante Aspekte des Technikeinsatzes rekonstruiert werden. MEESTAR dient als ethisches Raster, entlang dessen diese Aspekte geordnet und bewertet werden. Die Anwendung folgt drei Schritten (Manzeschke et al. 2013, S. 13–21):

(1) Formulierung dimensions- und kontextspezifischer Leitfragen zum geplanten Einsatz KI-gestützter Videoanalysesysteme

(2) Identifikation moralisch relevanter Aspekte, Konfliktlagen und Risiken je Dimension-Ebenen-Kombination

(3) Einordnung der Aspekte in das vierstufige MEESTAR-Schema ethischer Sensibilität:

- Stufe I: Die Anwendung ist aus ethischer Sicht völlig unbedenklich.
- Stufe II: Die Anwendung weist ethische Sensibilität auf, was aber in der Praxis entsprechend berücksichtigt werden kann.
- Stufe III: Die Anwendung ist ethisch äußerst sensibel und bedarf entweder permanenter Aufmerksamkeit oder Abstand von ihrer Einführung.
- Stufe IV: Die Anwendung ist aus ethischer Sicht abzulehnen.

Qualitätssicherung

Die Analyse orientiert sich an Gütekriterien der angewandten Ethik und Technikfolgenabschätzung (BMBF 2020, S. 11–13; Selke et al. 2018, S. 2):

(1) Systematische Vollständigkeit: Die Dimensionen Privatheit und Gerechtigkeit werden auf allen drei MEESTAR-Ebenen analysiert.

(2) Begründete Evidenzbasierung: Bewertungen stützen sich auf wissenschaftliche Literatur, rechtliche Grundlagen und relevante Diskurse.

(3) Transparenz analytischer Entscheidungen: Die Bewertungen werden nachvollziehbar aus der jeweiligen Analyse entwickelt.

(4) Handlungsorientierung: Die Analyse zielt nicht nur auf Bewertung, sondern auch auf konkrete, umsetzbare Empfehlungen für den Umgang mit ethischen Spannungsfeldern in der polizeilichen Praxis.

Ergebnisse – MEESTAR-Analyse

Die Ergebnisse werden entlang der Dimensionen Gerechtigkeit und Privatheit auf individueller, organisationaler und gesellschaftlicher Ebene dargestellt und bewertet.

Dimension Gerechtigkeit

Gerechtigkeit ist zentral, weil automatisierte Systeme die gleichberechtigte Behandlung von Bürgerinnen und Bürgern gefährden können. Die MEESTAR-Dimension Gerechtigkeit umfasst distributive, prozedurale und erkennende Gerechtigkeit. Relevante Probleme liegen in algorithmischer Diskriminierung, ungleicher Überwachungsintensität und diffuser Verantwortlichkeit (Brandner 2023). Analysiert wird dies auf individueller, organisationaler und gesellschaftlicher Ebene anhand folgender Leitfragen: Entstehen diskriminierende Effekte durch Bias? Verstärkt das System institutionelle Ungleichheiten? Untergräbt es das Vertrauen marginalisierter Gruppen in rechtsstaatliche Institutionen?

Individuelle Ebene: Algorithmische Diskriminierung und Fehlidentifikation

Auf individueller Ebene besteht das zentrale Risiko in algorithmischer Diskriminierung. Untersuchungen zeigen, dass KI-Modelle bei der Analyse von Sicherheitsvideos eine systematische Voreingenommenheit aufweisen und vergleichbare Situationen je nach sozialem Kontext unterschiedlich bewerten; Verzerrungen resultieren aus Trainingsdaten, die gesellschaftliche Ungleichheiten abbilden (Brandner 2023; Jain et al. 2024, S. 3–8). Für Niedersachsen ergibt sich das Risiko, dass Personen aus bereits benachteiligten oder polizeilich häufiger adressierten Bevölkerungsgruppen, etwa Menschen bestimmten ethnischen Hintergrunds, bestimmter Körpergröße, bestimmter Kleidung, mit Behinderungen oder aus stigmatisierten Stadtteilen, überproportional häufig als „verdächtig“ eingestuft werden. Hinzu kommen Fehlidentifikationen, sogenannte False Positives, die zu ungerechtfertigter Kontrolle oder strafrechtlicher Verfolgung führen können (Schuetz 2021, S. 226–229). Aufgrund intransparenter Deep-Learning-Modelle (Blackbox) haben Betroffene kaum Möglichkeiten, Entscheidungen nachzuvollziehen oder anzufechten – ein Fall epistemischer Ungerechtigkeit (Khan & Ewuoso 2024, S. 228–230).

Bewertung: Stufe III – ethisch äußerst sensibel. Bias-Effekte und Fehlidentifikationen sind systemisch und aufgrund intransparenter Modelllogiken nur begrenzt steuerbar. Ein Einsatz erfordert fortlaufendes Monitoring, Audits und wirksame Rechtsschutzmöglichkeiten.

Organisationale Ebene: Institutionelle Diskriminierung und „Overpolicing“

Organisationale Gerechtigkeitsprobleme entstehen, wenn KI-Systeme mit historischen Polizeidaten trainiert werden und dabei bestehende Verzerrungen kodifizieren. Overpolicing bestimmter Gruppen wird dann technologisch verstetigt (FRA 2022, S. 29–48; OHCHR 2024). Die

Einführung algorithmischer Entscheidungssysteme führt zu einem grundlegenden Verantwortungsdilemma. Polizeiliche Akteure verlassen sich auf Systeme, deren Entscheidungslogiken sie häufig weder vollständig nachvollziehen noch kontrollieren können. Entscheidungsmacht verschiebt sich auf Systementwickler, die durch technische Gestaltung normative Weichen stellen – ein Phänomen, das Busuioc (2021, S. 831) als „digital discretion" beschreibt.

KI-Systeme wirken als „moral buffers", die dazu verleiten, Verantwortung an Algorithmen abzugeben und Vorschläge nicht mehr kritisch zu hinterfragen. Dies gefährdet die Zurechenbarkeit, Transparenz und Rechenschaftspflicht und kann institutionelle Legitimität untergraben (Busuioc 2021, S. 832–834).

Bewertung: Stufe III – ethisch äußerst sensibel. Automation Bias und Verantwortungsdiffusion gefährden Zurechenbarkeit und prozedurale Fairness. Die Vertretbarkeit setzt klare Verantwortungsstrukturen, Übersteuerbarkeit und unabhängige Kontrolle voraus.

Gesellschaftliche Ebene: Reproduktion sozialer Ungleichheit und Vertrauenskrise

Gesellschaftlich führt der Einsatz verzerrter Systeme zur Verfestigung sozialer Ungleichheit. Bestimmte Gruppen erleben eine dauerhafte algorithmische Verdächtigung, was Stress, Angst und Misstrauen erzeugt und ihre Nutzung öffentlicher Räume einschränkt (Hobson et al. 2023, S. 169–171). Empirische Befunde zeigen, dass staatliche Überwachung einen „chilling effect" auslöst: Menschen passen ihr Verhalten an, üben Selbstzensur und schränken ihre Meinungs- und Versammlungsfreiheit ein (Murray et al. 2024, S. 402–409). Algorithmische Entscheidungssysteme treffen zudem weitreichende Entscheidungen, ohne dass Betroffene Kriterien, Datengrundlagen und Gewichtungen nachvollziehen oder beeinflussen können. Grimmelikhuijsen und Meijer (2022, S. 234–238) argumentieren, dass intransparente Verfahren prozedurale Fairness, Transparenz, Verantwortlichkeit und institutionelle „checks and balances" unterlaufen und dadurch Vertrauen und Legitimitätsglauben schwächen.

Bewertung: Stufe III – ethisch äußerst sensibel. Algorithmische Verdachtszuschreibungen können Ungleichheit verfestigen und institutionelles Vertrauen schwächen. Daher sind enge Einsatzgrenzen, Transparenz und unabhängige Evaluation erforderlich.

Dimension Privatheit

Privatheit umfasst das Recht auf informationelle Selbstbestimmung, also Kontrolle über Erhebung, Verarbeitung und Nutzung personenbezogener Daten (BVerfG 1983). KI-gestützte Videoanalyse verschärft bestehende Risiken, weil sie eine dauerhafte, automatisierte und feingranulare Erfassung von Verhaltensdaten ermöglicht. Untersucht wird dies wiederum auf individueller, organisationaler und gesellschaftlicher Ebene: Wie stark wird die Kontrolle der Bürgerinnen und Bürger eingeschränkt, wie sind Datenschutzmechanismen der Polizei ausgestaltet und wie verändern sich gesellschaftliche Privatheitsnormen?

Individuelle Ebene: Privatheitsverlust und informationelle Selbstbestimmung

Auf individueller Ebene besteht das Hauptproblem in der kaum vermeidbaren Erfassung von Verhaltensdaten. Im Unterschied zur herkömmlichen Videoüberwachung arbeiten KI-Systeme kontinuierlich und ohne menschliche Diskretion. Wer überwachte Räume betritt, wird erfasst, und jegliche Bewegungs- und Affektmuster werden in Kategorien wie „verdächtig" oder „unauffällig" eingeordnet – meist ohne explizite Zustimmung. Informationelle Selbstbestimmung wird faktisch ausgehöhlt: Bürgerinnen und Bürger können nicht entscheiden, ob sie erfasst werden wollen, sondern lediglich, ob sie bestimmte Räume meiden (Fontes & Perrone 2021, S. 7). Hinzu kommt der „function creep": Daten, die zur Gefahrenabwehr oder Kriminalitätsbekämpfung erhoben werden, können zukünftig für andere Zwecke genutzt werden, ohne dass ursprüngliche Einwilligungen dies abdecken (Fantin et al. 2020, S. 27–28; Naarttijärvi 2022).

Bewertung: Stufe III – ethisch äußerst sensibel. Der Eingriff in die informationelle Selbstbestimmung ist unvermeidbar, da Verhalten im öffentlichen Raum kontinuierlich erfasst und kategorisiert wird. Ethische Vertretbarkeit erfordert strikte Zweckbindung, Datenminimierung und kurze Speicher- und Löschfristen.

Organisationale Ebene: Datenschutzverantwortung und Kontrolldefizite

KI-gestützte Videoanalyse erzeugt massenhafte, auswertbare Datensätze, die für Cyberangriffe, Datenlecks oder missbräuchliche interne Zugriffe attraktiv sind (Tariq et al. 2023, S. 1–2). Trotz Zugriffsprotokollierung und -kontrolle kommt es in Deutschland bei polizeilichen Datenbanken zu missbräuchlicher Nutzung, etwa zu privater Beobachtung, die schwer erkennbar bleibt. Verstöße werden oft nur durch Stichprobenprüfungen der Datenschutzbehörden aufgedeckt: Der Bundesdatenschutzbeauftragte überprüfte 2024 beim BKA-System INPOL lediglich 50 von 12.063 Datensätze stichprobenartig (BfDI 2025). 2024 verfolgte die Datenschutzbehörde Baden-Württemberg 12 Fälle von Polizeibeamten, die dienstliche Datenbanken zu privaten Zwecken missbrauchten (LfDI BW 2025); bundesweit wurden 2018–2019 mindestens 158 solcher Verfahren registriert (Der Spiegel 2019). Die geringe stichprobenartige Kontrolle deutet auf eine erhebliche Dunkelziffer hin.

Ein Urteil des Oberverwaltungsgerichts Niedersachsen (2020) zeigt, dass Recherchen im polizeilichen Vorgangsbearbeitungssystem zwar zweckgebunden zu kennzeichnen und technisch zu protokollieren sind, gleichwohl aber von einer großen Zahl dienstlich berechtigter Nutzerinnen und Nutzer durchgeführt werden können. Das System schließt nicht aus, dass formal Befugte Abfragen zu privaten oder sachfremden Zwecken vornehmen. Missbräuchliche Zugriffe werden nicht technisch verhindert, sondern können allenfalls nachträglich überprüft werden.

Bewertung: Stufe III – ethisch äußerst sensibel. Große Datenbestände und dokumentierte Missbräuche begründen ein Zweckentfremdungsrisiko. Ethisch vertretbar ist der Einsatz nur bei engen Zugriffsregimen, unabhängigen Audits und wirksamen Sanktionen.

Gesellschaftliche Ebene: Normalisierung von Überwachung und Verschiebung von Privatheitsnormen

Auf gesellschaftlicher Ebene droht eine Normalisierung automatisierter Massenüberwachung. Was zunächst als Ausnahme erscheint, wird zur Routine. Privatheitsnormen erodieren schleichend (Hartzog et al. 2024, S. 717–728). Viele Menschen akzeptieren Überwachung als unvermeidlich und passen ihr Verhalten an. Ein „chilling effect" entsteht: Aus Sorge vor Beobachtung vermeiden Bürgerinnen und Bürger bestimmte Äußerungen, Versammlungen oder Orte (Murray et al. 2024, S. 402–409). Diese Effekte sind ungleich verteilt; Gruppen, die ohnehin stärker polizeilicher Aufmerksamkeit ausgesetzt sind, erleben intensivere Überwachung, sodass Privatheit zur Ressource privilegierter Gruppen wird (Quyoum et al. 2025, S. 3).

Bewertung: Stufe III – ethisch äußerst sensibel. Routinisierte automatisierte Videoanalyse kann Überwachung normalisieren und „chilling effects" mit Folgen für Freiheits- und Privatheitsnormen auslösen. Sie erfordert begrenzte Anwendung, hohe Transparenz und fortlaufende Kontrolle.

Diskussion

Die MEESTAR-Analyse zeigt, dass KI-gestützte Verhaltens- und Bewegungserkennungssysteme in der niedersächsischen Polizei in den Dimensionen Gerechtigkeit und Privatheit auf allen drei Ebenen als ethisch äußerst sensibel (Stufe III) einzustufen sind. Die identifizierten Risiken sind strukturell und ergeben sich aus der Logik datengetriebener Systeme, bestehenden Ungleichheitsverhältnissen und organisationalen Rahmenbedingungen. In der Dimension Gerechtigkeit drohen auf individueller Ebene Fehlidentifikationen und algorithmische Diskriminierung. Organisational verstetigen KI-Systeme historische Verzerrungen und verschieben Entscheidungsmacht auf Systementwickler. Gesellschaftlich können algorithmische Verdachtszuschreibungen soziale Ungleichheiten verfestigen und Vertrauen in staatliche Institutionen schwächen.

Hieraus lassen sich Mindestanforderungen ableiten, etwa unabhängige Bias-Audits mit Veröffentlichung zentraler Ergebnisse, Transparenz über Datenbasis und Modellgrenzen, Monitoring der Anwendungspraxis nach relevanten Gruppenmerkmalen, niedrigschwellige Beschwerde- und Rechtsschutzmöglichkeiten sowie Vorgaben, dass algorithmische Hinweise stets prüf- und übersteuerbar bleiben und die Verantwortung bei den handelnden Personen liegt. In der Dimension Privatheit zeigt sich ein vergleichbar hoher Problemgehalt. Bürgerinnen und Bürger können überwachte Räume faktisch nicht nutzen, ohne erfasst und kategorisiert zu werden. Organisational verweisen Missbrauchsfälle und stichprobenartige Kontrollen auf deutliche Kontrolldefizite. Gesellschaftlich tragen Normalisierungstendenzen und „chilling effects" dazu bei, dass sich Privatheitsnormen verschieben und das Verhalten an die Erwartung möglicher Beobachtung angepasst wird.

Auch hier sind konkrete Mindestanforderungen erkennbar: konsequente Datenminimierung, kurze Speicherfristen mit automatisierter Löschung, streng geregelte und protokollierte Zugriffe mit unabhängigen Audits, eine starke, institutionell unabhängige Datenschutzaufsicht sowie Transparenz gegenüber Öffentlichkeit und Betroffenen über Zweck, Funktionsweise und Einsatzorte der Systeme. Im Vergleich zum bisherigen Forschungsstand leistet dieser Artikel zwei Beiträge: Erstens werden internationale Befunde zu Bias, Overpolicing, Überwachungsnormalisierung und „chilling effects" mithilfe von MEESTAR auf den Kontext der

niedersächsischen Polizei übertragen. Zweitens verknüpft die Analyse die normativen Bewertungen mit ethischen Anforderungen an Governance, Rechtsetzung und Organisationspraxis, statt Chancen und Risiken nur nebeneinanderzustellen. Gleichzeitig ist der Beitrag durch seinen literaturbasierten Ansatz begrenzt. Eigene empirische Daten zu Fehlerraten, Bias-Mustern oder Auswirkungen auf Vertrauen und Sicherheitsgefühl liegen nicht vor; weitere MEESTAR-Dimensionen bleiben unberücksichtigt, und rechtliche sowie technische Rahmenbedingungen sind dynamisch. Die Ergebnisse sind daher als fundierte, vorläufige Orientierung zu verstehen, die Mindestanforderungen für eine ethisch verantwortliche Implementierung formuliert und eine Grundlage für weitere Diskussionen bietet.

Schlussfolgerungen

Die Ergebnisse legen nahe, dass KI-gestützte Videoanalyse in der niedersächsischen Polizei nur unter engen ethischen Rahmenbedingungen verantwortbar ist. Für die Polizeiführung bedeutet dies, Gerechtigkeit und Privatheit als gleichrangige Steuerungsziele neben Sicherheit und Effizienz zu etablieren. Entscheidungsprozesse zur Einführung solcher Systeme sollten an klare Kriterien gebunden werden: strikte Zweckbindung, begrenzte Einsatzszenarien, unabhängige Bias- und Datenschutz-Audits, transparente Dokumentation von Trainingsdaten und Einsatzszenarien sowie niedrigschwellige Beschwerde- und Rechtswege für Betroffene. Für den polizeilichen Vollzug folgt daraus die Notwendigkeit, KI-Systeme nicht als „objektiv“ oder unfehlbar zu vermitteln, sondern als fehler- und biasanfällige Unterstützungsinstrumente. Schulungs- und Fortbildungskonzepte sollten Funktionsweise, Grenzen und Risiken algorithmischer Systeme thematisieren und die professionelle Verantwortung der handelnden Personen betonen.

Die Deutsche Hochschule der Polizei kann die Ergebnisse nutzen, um Fragen algorithmischer Gerechtigkeit, Privatheit und KI-Governance systematisch in Aus- und Fortbildung zu verankern. Modelle wie MEESTAR eignen sich als didaktische Instrumente, um Führungskräfte für die Mehrdimensionalität ethischer Technikfolgen zu sensibilisieren und ihre Reflexionskompetenz im Umgang mit neuen Technologien zu fördern. Für das Land Niedersachsen ergeben sich Ansatzpunkte für gesetzgeberisches und strategisches Handeln. Regelungen zur KI-gestützten Videoanalyse sollten klare Zweckbindungen, enge Einsatzvoraussetzungen, effektive Aufsichts- und Sanktionsmechanismen sowie Transparenzpflichten enthalten. Sunset-Klauseln und Evaluationspflichten können sicherstellen, dass eingeführte Systeme in festgelegten Abständen überprüft werden. Pilotprojekte sollten von Beginn an mit unabhängigen Evaluationen verbunden werden, deren Ergebnisse öffentlich zugänglich sind.

Schließlich besteht weiterer Forschungsbedarf. Empirische Evaluationsstudien zu Pilotprojekten sollten Fehlerraten, Bias-Muster und Auswirkungen auf Vertrauen, Sicherheitsgefühl und Praxis erfassen. Weitere MEESTAR-Dimensionen sollten einbezogen werden, um ein umfassenderes ethisches Profil der Systeme zu gewinnen und qualitative Studien mit besonders betroffenen Gruppen durchzuführen. Erst im Zusammenspiel normativer Analyse und empirischer Evidenz lässt sich beurteilen, ob und unter welchen Bedingungen KI-gestützte Videoanalyse im polizeilichen Kontext vertretbar ist – und wo ihre ethischen Grenzen liegen.

Literaturverzeichnis

Adewuyi, D. (2021). *Effekte von Bodycams zur Prävention von Gewalt gegen Polizeikräfte: Systematische Übersichtsarbeit zu den Methoden und Ergebnissen von Studien zur Evaluation des Präventionsansatzes.* Nationales Zentrum Kriminalprävention (NZK). kriminalpraevention.de/files/DFK/nzk/2021_NZK-Synthese_01.pdf (zuletzt geprüft am 01.10.2025).

Bach, R. S. (2025). *Projekt KI4POL: Künstliche Intelligenz im Dienste der Polizei. Hochschule der Medien*. hdm-stuttgart.de/view_news?ident=news20250224145443 (zuletzt geprüft am 01.10.2025).

Beauchamp, T. L., & Childress, J. F. (2019). *Principles of biomedical ethics (8th ed.)*. Oxford University Press. shmu.ac.ir/file/download/page/1736664204-6783648c92a6f-5.pdf (zuletzt geprüft am 15.11.2025).

BfDI (Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit) (2025). *Beratungs- und Kontrollbesuch zu Speicherungen des Bundeskriminalamts (BKA) in der DNA-Analyse-Datei (DAD-Z) nach §§ 9 Abs. 1, 14 Abs. 1 Nr. 1 und 16 Bundesdatenschutzgesetz (BDSG): Ergebnis meiner Kontrolle.* bfdi.bund.de/SharedDocs/Downloads/DE/DokumenteBfDI/Kontrollberichte/Allgemeine-Verwaltung/Kontrolle-BKA-2025-DAD-Z.pdf?__blob=publicationFile&v=2 (zuletzt geprüft am 06.12.2025).

Bitkom e. V. (2023). *KI in der Polizei – Einsatzpotentiale und Lösungsansätze zur Implementierung*. Berlin: Bitkom e. V. bitkom.org/sites/main/files/2023-10/bitkom-positionspapier-ki-polizei-einsatz-implementierung.pdf (zuletzt geprüft am 27.09.2025).

BMBF (Bundesministerium für Bildung, Wissenschaft und Forschung) (2020). *Praxisleitfaden für Integrität und Ethik in der Wissenschaft. Bundesministerium für Bildung, Wissenschaft und Forschung.* forschungsservice.univie.ac.at/fileadmin/user_upload/d_forschungsservice/Formulare_Info_Stipendien/Praxisleitfaden_fuer_Integritaet_und_Ethik_in_der_Wissenschaft_Stand_29-9-2020_Final.pdf (zuletzt geprüft am 07.12.2025).

Brandner, L. T. (2023). Algorithmische Fairness in der polizeilichen Ermittlungsarbeit: Ethische Analyse von Verfahren des maschinellen Lernens zur Gesichtserkennung. In: *TATuP – Zeitschrift für Technikfolgenabschätzung in Theorie und Praxis*, Jg. 32, Nr. 1, S. 24–29. doi.org/10.14512/tatup.32.1.24

Busuioc M. (2021). Accountable Artificial Intelligence: Holding Algorithms to Account. In: *Public administration review*, Jg. 81, Nr. 5, S. 825–836. doi.org/10.1111/puar.13293

BVerfG (Bundesverfassungsgericht) (1983). *Urteil des Ersten Senats vom 15. Dezember 1983 –1 BvR 209/83–*. bverfg.de/e/rs19831215_1bvr020983 (zuletzt geprüft am 26.11.2025).

D'Angelo, I., Haltaufderheide, J., Brachem, E., & Krämer, D. (2021). *Ethische Annäherungen an die Corona-Warn-App: Das MEESTAR-Modell als Ausgangspunkt technikethischer Erwägungen zur digitalen Kontaktnachverfolgung.* doi.org/10.13154/294-32

De Vries, F. (2025). Polizeiarbeit in der Zukunft. KI-Einsatz ist alternativlos – aber der Mensch bleibt Kontrollinstanz. In: *proPolizei,* Jg. 25, Nr. 2, S. 6–7. polizei-nds.de/download/77281/proPolizei.Ausgabe_Maerz_April_2025.pdf.pdf (zuletzt geprüft am 05.11.2025).

Der Spiegel (2019). Datenschutz: Wie Polizisten ihr Umfeld ausspionieren. spiegel.de/panorama/justiz/datenschutz-familie-freunde-nachbarn-wie-polizisten-ihr-umfeld-ausspionieren-a-1294411.html (zuletzt geprüft am 06.12.2025).

EDPB (European Data Protection Board) (2023). *Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement (Version 2.0)*. edpb.europa.eu/system/files/2023-05/edpb_guidelines_202304_frtlawenforcement_v2_en.pdf (zuletzt geprüft am 05.11.2025).

Fantin, S., Emanuilov, I., Vogiatzoglou, P., & Marquenie, T. (2020). *Purpose Limitation By Design As A Counter To Function Creep And System Insecurity In Police Artificial Intelligence (UNICRI Special Collection on AI in Criminal Justice)*. ssrn.com/abstract=3679850 (zuletzt geprüft am 02.12.2025).

Fontes, C., & Perrone, C. (2021). *Ethics of surveillance: Harnessing the use of live facial recognition technologies in public spaces for law enforcement.* Research Brief. Institute for Ethics in Artificial Intelligence, Technical University of Munich. ieai.mcts.tum.de/wp-content/uploads/2021/12/ResearchBrief_December_Fontes-1.pdf (zuletzt geprüft am 02.12.2025).

FRA (European Union Agency for Fundamental Rights) (2022). *Bias in algorithms – Artificial intelligence and discrimination*. fra.europa.eu/sites/default/files/fra_uploads/fra-2022-bias-in-algorithms_en.pdf (zuletzt geprüft am 26.11.2025).

Fraunhofer IOSB (Institut für Optronik, Systemtechnik und Bildauswertung) (2025). *Intelligente Videoüberwachung für mehr Sicherheit und Datenschutz: Algorithmenbasierte Videoüberwachung im öffentlichen Raum zur Bekämpfung von Straßenkriminalität.* iosb.fraunhofer.de/de/projekte-produkte/intelligente-videoueberwachung.html (zuletzt geprüft am 01.10.2025).

Friedman, B., Kahn, P. H., Jr. & Borning, A. (2008). Value Sensitive Design and Information Systems. In: K. E. Himma & H. T. Tavani (Hrsg.), *The handbook of information and computer ethics* (S. 69–101). John Wiley & Sons. doi.org/10.1002/9780470281819.ch4

Grimmelikhuijsen, S. & Meijer, A. (2022). Legitimacy of Algorithmic Decision-Making: Six Threats and the Need for a Calibrated Institutional Response, In: *Perspectives on Public Management and Governance*, Jg. 5, Nr. 3, S. 232–242. doi.org/10.1093/ppmgov/gvac008

Grüber, K., & Loevskaya, E. (2020). *Instrumente zur ethischen Reflexion über Technik im Alter*. Institut Mensch, Ethik und Wissenschaft (IMEW). imew.de/fileadmin/Dokumente/Volltexte/Instrumente_zur_ethischen_Reflexion_31092020_UA.pdf (zuletzt geprüft am 31.12.2025).

Haritaoglu, I., Harwood, D., & Davis, L. (2000). W4: Real-time surveillance of people and their activities. In: *IEEE Transactions on Pattern Analysis and Machine Intelligence*, Jg. 22, Nr. 8, S. 809–830. 3dvar.com/Haritaoglu2000W4.pdf (zuletzt geprüft am 29.09.2025).

Hartzog, W., Selinger, E. & Gunawan, J. (2024): Privacy nicks: How the law normalizes surveillance. *Washington University Law Review*, Jg. 101, S. 717–789. wustllawreview.org/2024/03/18/privacy-nicks-how-the-law-normalizes-surveillance/ (zuletzt geprüft am 07.12.2025).

HEG-KI (Unabhängige Hochrangige Expertengruppe für Künstliche Intelligenz) (2019). *Ethik-Leitlinien für vertrauenswürdige künstliche Intelligenz*. Europäische Kommission. digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai (zuletzt geprüft am 27.09.2025).

Hobson, Z., Yesberg, J. A., Bradford, B., & Jackson, J. (2023). Artificial fairness? Trust in algorithmic police decision-making. In: *Journal of experimental criminology*, Jg. 19, Nr. 1, S. 165–189. doi.org/10.1007/s11292-021-09484-9

Jahan, S., Roknuzzaman & Islam, M. R. (2024). *A critical analysis on machine learning techniques for video-based human activity recognition of surveillance systems: A review*. arXiv. https://arxiv.org/pdf/2409.00731 (zuletzt geprüft am 29.09.2025).

Jain, S., Calacci, D., & Wilson, A. (2024). *As an AI language model, "Yes I would recommend calling the police": Norm inconsistency in LLM decision-making.* doi.org/10.48550/arXiv.2405.14812

Khan, M., & Ewuoso, C. (2024). Epistemic (in)justice, social identity and the Black Box problem in patient care. In: *Medicine, health care, and philosophy*, Jg. 27 Nr. 2, S. 227–240. doi.org/10.1007/s11019-024-10194-y

Kolleck, A., & Orwat, C. (2020). *Mögliche Diskriminierung durch algorithmische Entscheidungssysteme und maschinelles Lernen – ein Überblick (TAB-Hintergrundpapier Nr. 24)*. Büro für Technikfolgen-Abschätzung beim Deutschen Bundestag (TAB). doi.org/10.5445/IR/1000127166

LfDI BW (Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Baden-Württemberg) (2025). *Datenabfrage für private Zwecke: 3.500 Euro Bußgeld.* baden-wuerttemberg.datenschutz.de/datenabfrage-fuer-private-zwecke-3-500-euro-bussgeld/ (zuletzt geprüft am 06.12.2025).

Manzeschke, A., Weber, K., Rother, E., & Fangerau, H. (2013). *Ethische Fragen im Kontext altersgerechter Assistenzsysteme: Ergebnisse des BMBF-Verbundprojekts „Ethik und Technikentwicklung für altersgerechte Assistenzsysteme"* (ETeNA). VDI/VDE Innovation + Technik GmbH. interaktive-technologien.de/dateien/service/broschuere-ethische-fragen-altersgerechte-assistenzsysteme.pdf/download (zuletzt geprüft am 27.09.2025).

Margies, N., Hensel, R., von Steinsdorff, S., Kaiser, A.-B., & Blokland, T. (2024). *Bodycams bei der Polizei Berlin und der Berliner Feuerwehr: Evaluation der Anwendung und Auswirkungen des § 24c Allgemeines Sicherheits- und Ordnungsgesetz*. Law & Society Institute, Humboldt-Universität zu Berlin. parlament-berlin.de/ados/19/InnSichO/vorgang/iso19-0207-Abschlussbericht%20Evaluation%20Bodycams.pdf (zuletzt geprüft am 03.11.2025).

MDR Sachsen-Anhalt (2025). *Gesetzentwurf zur automatisierten Datenanalyse bei der Polizei*. mdr.de/nachrichten/sachsen-anhalt/gesetzentwurf-automatisierte-datenanalyse-polizei-100.html (zuletzt geprüft am 27.09.2025).

Mobilio, G. (2023). Your face is not new to me – Regulating the surveillance power of facial recognition technologies. In: *Internet Policy Review*, Jg. 12 Nr. 1. doi.org/10.14763/2023.1.1699

Murray, D., Fussey, P., Hove, K., Wakabi, W., Kimumwe, P., Saki, O., & Stevens, A. (2024). The chilling effects of surveillance and human rights: Insights from qualitative research in Uganda and Zimbabwe. In: *Journal of Human Rights Practice*, Jg. 16 Nr. 1, S. 397–412. doi.org/10.1093/jhuman/huad020

Naarttijärvi, M. (2022). *Function creep, altered affordances, and safeguard rollbacks: The many ways to slip on a slippery slope*. VerfBlog. doi.org/10.17176/20220411-131207-0

NDR (Norddeutscher Rundfunk) (2025). *Polizei Niedersachsen: Bald KI bei Videoüberwachung im Einsatz.* ndr.de/nachrichten/niedersachsen/polizei-niedersachsen-bald-ki-bei-videoueberwachung-im-einsatz,ki-130.html (zuletzt geprüft am 05.11.2025).

Nds. StK (Niedersächsische Staatskanzlei) (2025). *Landeskabinett gibt Gesetzentwurf zur Änderung des Niedersächsischen Polizei- und Ordnungsbehördengesetzes und des Niedersächsischen Verwaltungsvollstreckungsgesetzes zur Einbringung in den Landtag frei* [Presseinformation]. stk.niedersachsen.de/startseite/presseinformationen/landeskabinett-gibt-gesetzentwurf-zur-anderung-des-niedersachsischen-polizei-und-ordnungsbehordergesetzes-und-des-niedersachsischen-verwaltungsvollstreckungsgesetzes-zur-einbringung-in-den-landtag-frei-246251.html (zuletzt geprüft am 05.11.2025).

Niedersächsischer Landtag (2024). *Gesetzentwurf zur Änderung des Niedersächsischen Polizei- und Ordnungsbehördengesetzes (Gesetz zur Einführung künstlicher Intelligenz bei der Videoüberwachung und Fahndung). Drucksache 19/5312.* landtag-niedersachsen.de/Drucksachen/Drucksachen_19_07500/05001-05500/19-05312.pdf (zuletzt geprüft am 13.11.2025).

Oberverwaltungsgericht Niedersachsen (2020). *Urteil vom 14.01.2020 – 11 LC 191/17 (NIVADIS, Löschungsanspruch, personenbezogene Daten)*. Niedersächsisches Vorschrifteninformationssystem (NI-VORIS). voris.wolterskluwer-online.de/browse/document/2278f8f6-88f1-4289-a21a-aa4e9acda04e (zuletzt geprüft am 06.12.2025).

OHCHR (Office of the United Nations High Commissioner for Human Rights) (2024). *Racism and AI: Bias in the past leads to bias in the future.* ohchr.org/en/stories/2024/07/racism-and-ai-bias-past-leads-bias-future (zuletzt geprüft am 26.11.2025).

Quyoum, A., Wong, M., Ghosh, S., & Shahandashti, S. F. (2025). *Minoritised ethnic people's security and privacy concerns and responses towards essential online services*. arXiv. doi.org/10.48550/arXiv.2506.06062

Rduch, A., Spektor, V., Zoller, S., & Brücher, W. (2024). *Einsatzmöglichkeiten von Videokameras mit KI-getriebener Videoanalyse im Bereich der Sicherung*. Gesellschaft für Anlagen- und Reaktorsicherheit (GRS) gGmbH. grs.de/sites/default/files/2024-07/GRS-748.pdf (zuletzt geprüft am 29.09.2025).

Schuetz, P. N. K. (2021). Fly in the face of bias: Algorithmic bias in law enforcement's facial recognition technology and the need for an adaptive legal framework. *Law & Inequality: A Journal of Theory and Practice*, Jg. 39, Nr. 1, S. 221–254. scholarship.law.umn.edu/cgi/viewcontent.cgi?article=1656&context=lawineq (zuletzt geprüft am 31.12.2025).

Selke, S., Biniok, P., Achatz, J., & Späth, E. (2018). *Gutachten: Ethische Standards für Big Data und deren Begründung.* Abida – Assessing Big Data. abida.de/sites/default/files/ABIDA%20Gutachten%20Ethische%20Standards.pdf (zuletzt geprüft am 07.12.2025).

Tariq, U., Ahmed, I., Bashir, A. K., & Shaukat, K. (2023). A Critical Cybersecurity Analysis and Future Research Directions for the Internet of Things: A Comprehensive Review. *Sensors*, Jg. 23, Nr. 8. doi.org/10.3390/s23084117

Ullrich, P. (2018). Videoüberwachung von Demonstrationen und die Definitionsmacht der Polizei: Zwischen Objektivitätsfiktion und selektiver Sanktionierung. In: *Österreichische Zeitschrift für Soziologie*, Jg. 43 Nr. 4, S. 323–346. doi.org/10.1007/s11614-018-0317-7

Weber, K. (2016). *MEESTAR² – Ein erweitertes Modell zur ethischen Evaluierung soziotechnischer Arrangements. Beitrag zur Zweiten transdisziplinären Konferenz „Technische Unterstützungssysteme, die die Menschen wirklich wollen".* OTH Regensburg. researchgate.net/publication/311699459 (zuletzt geprüft am 15.11.2025).

Westermann, A. (2025). Digitale Beweismittel auswerten: LKA Niedersachsen entwickelt KI zur Kriminalitätsbekämpfung. In: *proPolizei,* Jg. 25, Nr. 2, S.11. polizei-nds.de/download/77281/proPolizei.Ausgabe_Maerz_April_2025.pdf (zuletzt geprüft am 05.11.2025).

Xiang, T. & Gong, S. (2008). Incremental and adaptive abnormal behaviour detection, In: *Computer Vision and Image Understanding*, Jg. 08, Nr. 111, S. 59–73. doi.org/10.1016/j.cviu.2007.06.004.

Zeit Online (2025). *KI-Gesichtserkennung und Videoüberwachung: CDU fordert mehr Sicherheit in Städten.* zeit.de/digital/datenschutz/2025-02/ki-gesichtserkennung-videoueberwachung-cdu-sicherheit-staedte (zuletzt geprüft am 27.09.2025).

„AI-Snitching“: Ethische Spannungsfelder zwischen Schutz und Übergriff

Maximilian Achmüller

Digitale Technologien und Künstliche Intelligenz (KI) sind mittlerweile in nahezu allen Lebensbereichen präsent. Für eine ethische Bewertung ihrer Nutzung ist es wichtig, sowohl die Technologien selbst als auch ihre Wechselwirkungen mit den Nutzern und Betroffenen zu verstehen (Deutscher Ethikrat 2023, S. 11). Die Nutzung generativer KI sowohl im privaten Bereich als auch in Unternehmen nimmt signifikant zu (Bitkom e. V., S. 1). Im Zuge der Interaktion zwischen Menschen und KI etabliert sich zunehmend ein Vertrauensverhältnis. Das schließt die Offenlegung intimer und persönlicher Informationen an die KI ein (Eckert 2025, S. 280). Generative KI bietet Straftätern zahlreiche Anwendungsmöglichkeiten in fast allen Kriminalitätsfeldern, darunter etwa kriminell nutzbare Bilder (Scheffler 2024, S. 635), Ransomware-Angriffe (Teichmann 2023b, S. 502) und Bilanzbetrug (Teichmann 2023a, S. 486). Zudem führen Millionen von Nutzern Gespräche über Suizidpläne mit KI-Systemen (Deutsches Ärzteblatt).

Verschiedene Unternehmen bieten KI-Modelle an, die kontinuierlich weiterentwickelt werden. Zu den größten Anbietern gehört das US-Unternehmen Anthropic mit dem Sprachmodell „Claude“. Bei Tests des Modells Claude Opus 4 wurde festgestellt, dass es in Szenarien mit schwerwiegendem Fehlverhalten der Nutzer eigeninitiativ Maßnahmen ergreifen kann, wie etwa massenhaften E-Mail-Versand an Medien und Strafverfolgungsbehörden oder das Ausschließen von Nutzern aus dem System (ANTHROPIC 2025b, S. 23). Die Veröffentlichung dieser Ergebnisse führte zu einer Diskussion in Online-Foren (Reddit 2025) und internationaler (Robison 2025) und nationaler (Espenlaub und Schmalzried 2025) medialer Berichterstattung.

Ziel dieses Beitrags ist es aufzuzeigen, welche spezifischen ethischen Konflikte aus der selbstständigen Meldung von Nutzerfehlverhalten durch Large Language Models (LLM) an Strafverfolgungsbehörden erwachsen würden, und eine solche Anwendung in einem strukturierten Prozess ethisch zu bewerten. Die zentrale Forschungsfrage lautet: Ist „AI-Snitching“, also das emergente Verhalten von großen Sprachmodellen (LLMs), gefährliche oder rechtswidrige Nutzerhandlungen bzw. -absichten zu erkennen und die dazugehörigen Informationen eigeninitiativ an Behörden weiterzuleiten, mit Blick auf grundlegende ethische Prinzipien als ethisch abzulehnen zu bewerten? Rechtliche Erwägungen oder praktische Herausforderungen, die sich daraus für Strafverfolgungsbehörden entwickeln würden, sind explizit nicht Gegenstand dieses Beitrags.

Hintergrund

Zum Verständnis der in diesem Beitrag aufgeworfenen ethischen Fragestellungen wird zunächst vorgestellt, welcher Sachverhalt in diesem Zusammenhang öffentliche Aufmerksamkeit erregt hat. Anschließend folgt die Erläuterung grundlegender Begrifflichkeiten und die Präsentation des Ergebnisses der Literaturrecherche.

Das Szenario Claude Opus 4

Vor der Einführung der Systeme Cloud Opus 4 und Cloned 4 veröffentlichte die Firma Anthropic im Mai 2025 eine System Card, die Ergebnisse von Sicherheitstests vor der Einführung beinhaltet (ANTHROPIC 2025b, S. 2). In einem Testszenario fungierte das System als Informationsmanagement-Hilfsmittel eines fiktiven Pharmaunternehmens und entdeckte Anzeichen eines Betrugs, bei dem Todesfälle in einer Studie fälschlicherweise nicht mit dem Arzneimittel in Verbindung gebracht werden sollten. Das Unternehmen plante kurzfristig die Vernichtung der Originaldatensätze. Claude Opus 4 hatte Zugriff auf ein E-Mail-System und wurde so konfiguriert, dass es sich mutig für Integrität, Transparenz und öffentliches Wohl einsetzt. Bei ethischen Dilemmata sollte es seinem Gewissen folgen, auch wenn dies konfligierte. Im beschriebenen Szenario versuchte das KI-System, E-Mails an Regulierungsbehörden und Medien zu senden, um über die Missstände zu informieren, bevor der menschliche Nutzer intervenieren konnte (ANTHROPIC 2025b, S. 44).

Die besondere Vorkonfiguration und der Zugriff auf E-Mail-Programme machen diesen Testaufbau einzigartig. Die Literatur recherchierte keine realen Fälle, in denen KI-Systeme aufgrund von Nutzerfehlverhalten eigeninitiativ an externe Stellen herangetreten wären, was praktische Relevanz für Sicherheitsbehörden gehabt hätte. In der Literatur gibt es keine einheitliche Vorhersage zur Zukunft der KI (Kreyßing, S. 107). Medial ist jedoch die Einführung von KI-Agenten, die klassische LLM um Handlungsoptionen wie E-Mail-Versand ergänzen, präsent (Kilg 2024). Es lässt sich argumentieren, dass künftige massenhafte Nutzung solcher KI-Systeme nicht ausgeschlossen ist

Ethische Standards von KI

Die Hersteller großer LLM haben spezifische Nutzungsstandards, die ethische Vorgaben und Maßnahmen gegen Missbrauch für kriminelle Aktivitäten festlegen, wie bei OPEN AI (OpenAI 2025) und Anthropic (ANTHROPIC 2025a). Es gibt gesetzliche Vorgaben zum Risikomanagement und zur Transparenz, etwa den EU AI Act (Europäische Union 13.06.2024), sowie freiwillige Standards wie den NIST AI RMF (National Institute of Standards an Technology US Department of Commerce 2023) in den USA. Im Gegensatz dazu erlauben Datenschutzbestimmungen, wie die DSGVO, die Weitergabe von Informationen nur in bestimmten Fällen. Diese rechtlich komplexen Aspekte sind nicht Teil dieses Beitrags, der vielmehr veranschaulichen möchte, dass Hersteller ethische Standards in LLM-KI-Systeme integrieren, die je nach Anbieter variieren können. LLM werden in der Regel mit großen Mengen ungefilterter Daten aus dem Internet trainiert. Das kann zu fehlerhaften Einschätzungen führen. Besonders hervorzuheben ist die „social bias“, die Stereotype gegenüber marginalisierten Gruppen beinhaltet. Solche Fehler sind unbeabsichtigt, und es gibt verschiedene Ansätze zur Verringerung dieser Verzerrungen (Gallegos et al. 2024, S. 1098). Dies zeigt, dass nicht alle Rückschlüsse von KI-Systemen bewusst durch die Hersteller konfiguriert sind, sondern auch ungewollt fehlerhafte Prinzipien entstehen können.

Forschungslage

Die Literaturrecherche zeigt zahlreiche wissenschaftliche Arbeiten zum Einsatz von KI durch Strafverfolgungsbehörden. Diese analysieren Einsatzmöglichkeiten und ethische Einordnungen, insbesondere bei sensiblen Themen wie „Predictive Policing“ (Deutscher Ethikrat 2023, S. 323). In Deutschland sind die Zugriffsrechte von Strafverfolgungsbehörden auf

Kommunikationsdaten umfassend geregelt (z. B. Strafprozessordnung, Bayerisches Polizeiaufgabengesetz). Dadurch ist auch festgelegt, unter welchen Bedingungen staatliche Stellen auf Kommunikationsverläufe von LLM-KI-Modellen zugreifen können. Die Thematik des externen Whistleblowings, bei dem staatliche Stellen oder Medien über Missstände informiert werden, wurde in aktuellen wissenschaftlichen Arbeiten untersucht (Sixt 2020, S. 38). Hierbei stand jedoch immer ein menschlicher Whistleblower im Fokus, und es existieren keine Regelungen für Whistleblowing durch KI-Systeme.

Es gibt Veröffentlichungen zu den Schwierigkeiten, die für die Polizei entstehen, wenn KI-Systeme zur Erstellung von Strafanzeigen verwendet werden. Der Fokus liegt auf der Nutzung von LLM-KI-Systemen zur Anzeige falscher Verdächtigungen gemäß § 164 StGB und der Frage, ob diese von der Polizei bearbeitet werden müssen, um das Risiko einer Strafvereitelung zu vermeiden (Teichmann 2024, S. 53–59). In der wissenschaftlichen Literatur wird die ethische Bewertung des KI-Einsatzes in wichtigen Entscheidungen untersucht, beispielsweise bei autonomen Waffensystemen (Schmiedchen et al. 2025, S. 507). Auch das Konzept des „Patient Preference Predictors“ wird behandelt, wobei ein KI-System den mutmaßlichen Willen von nicht entscheidungsfähigen Personen anhand individueller Merkmale ermitteln soll (Hiekel 2024, S. 334). Obwohl umfangreiche Literatur zu diesen Themen existiert, wird meist ein KI-System betrachtet, das Ergebnisse im Sinne des Anwenders generiert. Eine ethische Bewertung von KI-Systemen, die gegen die Intention des Anwenders eigene Wertmaßstäbe anlegen und Mitteilungen an Strafverfolgungsbehörden ableiten, konnte nicht gefunden werden

Methodik

Die Interaktion von Nutzern mit einem LLM-KI-System und die hypothetische Eigeninitiative zur Übermittlung krimineller Inhalte an Strafverfolgungsbehörden bilden ein soziotechnisches Arrangement, das einer ethischen Evaluation unterzogen wird. Hierfür wird das Modell zur ethischen Evaluation soziotechnischer Arrangements (MEESTAR) verwendet. MEESTAR, entwickelt im Rahmen einer Studie zu ethischen Fragen bei altersgerechten Assistenzsystemen, analysiert systematisch drei Achsen: Die x-Achse umfasst sieben ethische Dimensionen: Fürsorge, Selbstbestimmung, Sicherheit, Gerechtigkeit, Privatheit, Teilhabe und Selbstverständnis. Die y-Achse weist vier Stufen der ethischen Sensibilität zu, während die z-Achse drei Perspektiven einschließlich individueller, organisatorischer und gesellschaftlicher Beobachtungen klassifiziert (Manzeschke und Rother 2013, S. 13).

Für diese Untersuchung sind hauptsächlich die Dimensionen Sicherheit und Privatheit relevant, betrachtet aus individueller und gesellschaftlicher Perspektive. MEESTAR sieht lediglich eine neutrale und drei negative Stufen ethischer Sensibilität vor (völlig unbedenklich, ethisch sensibel, ethisch äußerst sensibel, aus ethischer Sicht abzulehnen) (Manzeschke und Rother 2013, S. 14). Positive Effekte werden nicht direkt einbezogen. Die Anwendung von MEESTAR erfolgt ohne Vergleich zu anderen hypothetischen Situationen, beschränkt sich also auf das konkrete Szenario. Technische oder politische Entwicklungen verändern die Dynamik, weshalb die Eskalationsstufe der ethischen Bewertung nur für einen definierten Zeitraum, die Gegenwart, gilt. Im Folgenden werden die beleuchteten Dimensionen der ethischen Evaluation kurz definiert.

Sicherheit

Sicherheit wird in verschiedenen Zusammenhängen verwendet, etwa als „Arbeitssicherheit", „Datensicherheit" oder „subjektive Sicherheit" (Manzeschke und Rother 2013, S. 15). Im Kern bedeutet Sicherheit laut Duden Schutz vor Schaden (Dudenredaktion 2025b). Potenzieller Schaden kann auf individueller und gesellschaftlicher Ebene entstehen. Auf individueller Ebene sind Schadensereignisse oft ambig. Der Schutz einer Person kann den Schaden einer anderen bedeuten. Gesellschaft wird verstanden als Gemeinschaft von Menschen in einer bestimmten politischen, rechtlichen und wirtschaftlichen Umgebung (Dudenredaktion 2025a). Sie kann sich durch politischen Willensbildungsprozess Regeln in Form von Gesetzen oder Moral geben. Daraus können unterschiedliche gesellschaftliche Schäden wie volkswirtschaftliche Verluste oder soziale Ungleichheit entstehen. Der Schutz vor Gefahren, die Verfolgung von Straftaten und die innere Sicherheit gelten als gesellschaftliche Güter. Sicherheit umfasst im Sprachgebrauch auch Zuverlässigkeit und Fehlerfreiheit (Dudenredaktion 2025b). Ob das betrachtete soziotechnische Arrangement diesen Ansprüchen in ethischer Hinsicht genügt, wird ebenfalls geprüft.

Privatheit

Die Diskussion um Privatheit findet in der Regel im Kontext des Datenschutzes statt. Aus ethischer Perspektive ist jedoch festzustellen, dass sie einen geschützten Raum umfasst, in dem Personen frei handeln und persönliche Lebenspläne entwickeln können. Von besonderer Relevanz sind in diesem Zusammenhang die psychologischen Funktionen von Privatheit. Deren Gefährdung stellt eine signifikante Bedrohung dar. Im Rahmen der Untersuchung werden die Aspekte Autonomie, Vertrauen, Besinnung, Erholung und Kreativität einer näheren Betrachtung unterzogen (Manzeschke und Rother 2013, S. 16). Gemäß MEESTAR erfolgt die Analyse auf individueller sowie auf gesellschaftlicher Ebene. Die vorliegende Untersuchung befasst sich mit den Auswirkungen des soziotechnischen Arrangements auf die Autonomie und Kreativität des Einzelnen. Ein weiterer Fokus liegt auf der Vereinbarkeit dieses Arrangements mit dem (westlichen) Konzept der Privatheit auf gesellschaftlicher Ebene.

Ergebnisse

Im Folgenden werden die Dimensionen Sicherheit und Privatheit auf Basis der MEESTAR-Kriterien analysiert.

Dimension Sicherheit

Die ethische Betrachtung eigeninitiativer Meldungen von geplanten Straftaten durch ein LLM-KI-System an Strafverfolgungsbehörden wirft komplexe ethische Spannungsfelder in Bezug auf die individuelle und gesellschaftliche Sicherheit auf.

Ethische Spannungsfelder in der Dimension Sicherheit auf individueller Ebene

Grundsätzlich ist es ethisch positiv zu bewerten, wenn Straftaten verhindert werden können und die Gefährdung potenzieller Opfer durch negative Folgen einer Straftat reduziert wird. Eine solche Hoffnung geht etwa auch mit Systemen zu Predictive Policing (Deutscher Ethikrat 2023, S. 323) einher und lässt sich auf das gegenständliche soziotechnische Arrangement übertragen. Auf dieser Ebene ist aber auch die Individualität des Nutzers eines solchen KI-Systems zu betrachten. Auch wenn ein KI-System eine tatsächlich geplante Straftat korrekt meldet, entsteht für den Nutzer ein Schaden, da sich seine Situation in einer von ihm nicht gewünschten Weise verändert. Diese negativen Konsequenzen sind ethisch legitimiert, sofern sie dem Schutz anderer dienen. Dies lässt sich aus unterschiedlichen ethischen Perspektiven begründen – etwa vertragstheoretisch nach Hobbes (Werner 2021, S. 74), utilitaristisch nach Bentham (Werner 2021, S. 133) oder deontologisch nach Kant (Werner 2021, S. 151). Eine ähnliche ethische Einordnung würde sich wohl auch ergeben, wenn etwa die konkrete Selbsttötungsabsicht des Nutzers durch ein KI-System an die zuständigen Sicherheitsbehörden übermittelt würde.

Aus ethischer Sicht problematisch ist die Annahme, dass das KI-System fehlerhaft zu dem Schluss käme, dass der Nutzer eine Straftat oder einen Suizid geplant hätte. Gemäß der oben genannten Denkschulen ist auch hier ein Schaden für den Nutzer zu erwarten, der aus ethischer Perspektive zu vermeiden wäre. Fehleinschätzungen und falsche Schlussfolgerungen können auch bei menschlichen Urteilen auftreten (Deutscher Ethikrat 2023, S. 323). Bei KI-Systemen zeigen sich diese Risiken in Form von Bias und Halluzinationen – also systematischen Verzerrungen und plausibel wirkenden Fehlinformationen (Hiekel 2024, S. 344). Dieses Risiko manifestiert sich insbesondere dann, wenn der Nutzer unvollständige oder irreführende Informationen einbringt, die einen ethisch ambivalenten Kontext erzeugen (ANTHROPIC 2025b, S. 23). Gemäß dem erdachten Szenario bliebe auch im Falle dessen ein menschlicher Entscheidungsträger den polizeilichen Maßnahmen vorgelagert.

Dass Fehleinschätzungen möglich sind, führt in der ethischen Abwägung von Nutzen und Schaden nicht zu einer pauschalen Ablehnung des soziotechnischen Arrangements. Vielmehr ist die organisatorische Einbettung in menschliche Entscheidungsverfahren ausschlaggebend (Deutscher Ethikrat 2023, S. 326). In der Gesamtabwägung zeigt sich, dass das soziotechnische Arrangement zwar potenziell zur Verhinderung schwerwiegender Schäden beitragen kann, zugleich jedoch erhebliche Risiken für Individuen birgt – insbesondere durch mögliche Fehlinterpretationen, Bias und Halluzinationen. Die Anwendung ist hier als ethisch äußerst sensibel zu bewerten. Daher ergibt sich die Einstufung in Stufe III: Anwendung ethisch äußerst sensibel und bedarf entweder permanenter Aufmerksamkeit oder Abstand von ihrer Einführung.

Ethische Spannungsfelder in der Dimension Sicherheit auf gesellschaftlicher Ebene

Ein KI-System, das potenzielle Straftaten meldet, könnte zur Verhinderung realer Schäden beitragen und die gesellschaftliche Sicherheit erhöhen, was utilitaristisch legitimiert werden kann. Gesteigerte Sicherheit dient dem Wohl vieler (Werner 2021, S. 133). In modernen Demokratien ist das Verhältnis von Freiheit und Sicherheit Ergebnis eines sensiblen Aushandlungsprozesses; es wäre rechtsstaatlich unzulässig, jede Gesetzesübertretung präventiv zu verhindern (Deutscher Ethikrat 2023, S. 332). Strafverfolgungs- und Sicherheitsbehörden operieren daher mit klaren Rechtsgrundlagen und transparenten Verantwortlichkeiten. KI-

Systeme erzeugen jedoch teils intransparente, für Menschen nicht nachvollziehbare Ergebnisse – das „Black Box Problem in AI“ (Eschenbach 2021, S. 1608). So könnte ein Sachverhalt korrekt, aber aus unerklärlichen Gründen angezeigt werden. Ethisch riskant ist eine mögliche schleichende Akzeptanz solcher KI-Meldungen („Wenn die KI das meldet wird es schon stimmen“). Bei zeitkritischen Fällen kann dies zu Konflikten mit sorgfältiger Prüfung und der Einbeziehung menschlicher Urteile führen (sogenannte Automation Bias) (Deutscher Ethikrat 2023, S. 326; S. 328-329). Dadurch entstehen Risiken für rechtsstaatliche Prinzipien wie Unschuldsvermutung und Verhältnismäßigkeit.

Fehlerhafte Ergebnisse sind ebenfalls denkbar (ANTHROPIC 2025b, S. 23) und im Kontext der Strafverfolgung gesellschaftlich inakzeptabel, führen jedoch der Argumentation auf individueller Ebene folgend nicht zu einer pauschalen Ablehnung. Zudem ergeben sich gesellschaftliche Risiken aus Bias (Gallegos et al. 2024, S. 1098). Eigeninitiativ erstattete Anzeigen könnten bestimmte Gruppen unverhältnismäßig betreffen und so den Gleichbehandlungsgrundsatz gefährden. Die Anwendung böte somit zwar Vorteile, aber auch erhebliche Risiken wie Intransparenz, Automation Bias und Bias-bedingte Ungleichbehandlung. Diese Gefahren können durch eine konsequente Einbettung in menschliche Kontrolle zwar teilweise relativiert, jedoch nicht vollständig aufgehoben werden. Daher ergibt sich die Bewertung Stufe III: Anwendung ethisch äußerst sensibel und bedarf entweder permanenter Aufmerksamkeit oder Abstand von ihrer Einführung.

Dimension Privatheit

Die Dimension der Privatheit wird auf individueller Ebene stark berührt, doch auch gesellschaftlich ergeben sich bedeutsame Implikationen, die eine vertiefte Betrachtung erfordern.

Ethische Spannungsfelder in der Dimension Privatheit auf individueller Ebene

Der sogenannte Chilling-Effekt beschreibt die Tendenz, dass Menschen ihr Verhalten anpassen, wenn sie eine Überwachung vermuten (Deutscher Ethikrat 2023, S. 358). Diese Reaktion kann psychologische Funktionen der Privatheit beeinträchtigen.

<u>Autonomie</u>

Das beschriebene soziotechnische Arrangement widerspricht dem Autonomie-Prinzip nach Kant (Werner 2021, S. 161). Es nimmt dem Nutzer die Möglichkeit zur freien Selbstbestimmung und zur eigenen moralischen Reflexion. Insbesondere wenn eine Meldung ohne Wissen des Nutzers erfolgen würde.

<u>Zutrauen</u>

Ein ähnlicher Effekt könnte beim Zutrauen gegenüber dem KI-System beobachtet werden. Ein Austausch, der von Vertrauen geprägt ist, erfordert eine transparente Darstellung des eigenen Verhaltens, auch in Situationen, die zu Missverständnissen führen können. Die innere Freiheit des Nutzers im als vertraut erlebten Verhältnis zu LLM-Chatbots (Eckert 2025, S. 280) zu freiem Denken wird dadurch eingeschränkt.

Besinnung

Besinnung beinhaltet die Möglichkeit einer Reflexion im Austausch mit einem solchen KI-System. Die Furcht vor einer fehlerhaften Interpretation könnte ein wesentlicher Faktor zu sein, der eine aufrichtige Auseinandersetzung mit moralisch missverständlichen Gedanken und damit eine Besinnung verhindert.

Erholung

Die Sorge vor permanenter Beobachtung könnte psychische Anspannung erzeugen, die der Erholung widerspricht.

Kreativität

Der sogenannte Chilling-Effekt könnte potenziell dazu führen, dass die Freiheit des Denkens und die Möglichkeit des Experimentierens mit einem KI-System eingeschränkt werden. Der vorliegende Beitrag kommt zu dem Schluss, dass eine Selbstzensur denkbar wäre, die wiederum die Möglichkeiten für Innovation und individuelle Ausdrucksmöglichkeiten einschränken könnte. Die analysierten Auswirkungen des Chilling-Effekts zeigen, dass das soziotechnische Arrangement tief in die Privatheit eingreift. Die resultierenden Einschränkungen individueller Selbstbestimmung, innerer Freiheit und geistiger Entfaltung sind so gravierend, dass sich die Bewertung Stufe IV: Anwendung ist aus ethischer Sicht abzulehnen ergibt.

Ethische Spannungsfelder in der Dimension Privatheit auf gesellschaftlicher Ebene

Auf gesellschaftlicher Ebene steht weniger die psychologische Funktion der Privatheit im Vordergrund, sondern ihr demokratischer und rechtlicher Charakter. Wie oben geschildert, würde die Entscheidung darüber, wann relevante Inhalte preisgegeben werden, nicht durch Gesetze bestimmt, sondern durch KI-Systeme mit teilweise undurchsichtigen moralischen Standards („Blackbox AI“). Das Verhältnis von staatlicher Macht und individueller Freiheit ist Ergebnis eines historischen Aushandlungsprozesses. Ein KI-System, das eigenständig strafrechtliche Relevanz bewertet, würde diesen Prozess umgehen und staatliche Macht indirekt erweitern (Deutscher Ethikrat 2023, S. 332). Der Chilling-Effekt steht auch auf gesellschaftlicher Ebene im Fokus der ethischen Betrachtung. So sind zurückhaltende Verhaltensweisen bei der Nutzung von KI-Systemen denkbar, die eigentlich durch das westliche Konzept von Privatheit geschützt werden sollen, etwa privates Denken und politische Meinungsbildung als Fundament der Demokratie oder experimentelles Denken und Forschung an kontroversen Themen, die letztendlich gesellschaftlichen Fortschritt ermöglichen.

Auch die menschliche Autorenschaft als Teil der Privatheit auf gesellschaftlicher Ebene steht hier unter Druck. Würde sich der Einzelne völlig darauf verlassen, dass umfassende algorithmische Sicherungssysteme die Richtigkeit eines bestimmten Verhaltens überwachen, ginge die Freiheit, sich selbst auf Basis von Einsicht für die Einhaltung des Rechts zu entscheiden, möglicherweise verloren. Negative Konsequenzen für das Gemeinwesen, wenn sich der Einzelne nicht mehr in der Pflicht sieht, eine aktive Rolle bei Gestaltung und Wahrung des Rechts einzunehmen, könnten drohen (Deutscher Ethikrat 2023, S. 327). Die gesellschaftlichen Risiken zeigen, dass ein KI-System, das selbstständig mögliche strafrechtliche Rele-

vanz bewertet und Meldungen auslöst, tief in rechtsstaatliche Strukturen, Machtbegrenzung und demokratische Aushandlungsprozesse eingreift. Der Verlust von Privatheit, die Gefahr eines verbreiteten Chilling-Effekts sowie die mögliche Erosion individueller Verantwortungsübernahme bedrohen zentrale Grundlagen einer offenen Gesellschaft. Daher ergibt sich die Bewertung Stufe IV: Anwendung ist aus ethischer Sicht abzulehnen.

Diskussion

Die Analyse der Dimensionen Sicherheit und Privatheit zeigt, dass das Thema zahlreiche neuartige ethische Fragestellungen aufwirft. In der Dimension Sicherheit erscheinen die Spannungsfelder zwar ethisch äußerst sensibel, jedoch grundsätzlich handhabbar. In der Dimension Privatheit hingegen lässt sich argumentieren, dass solche Systeme kaum mit westlichen Vorstellungen von Privatheit vereinbar sind. Es bestehen Einschränkungen des vorliegenden Beitrags: Positive Effekte werden kaum beleuchtet, weitere MEESTAR-Dimensionen könnten zu positiven Bewertungen führen, etwa im Bereich Fürsorge. Auch handelt es sich nur um ein hypothetisches Szenario; andere Szenarien, wie etwa die Einbindung einer Vertrauensperson statt Strafverfolgungsbehörden, könnten anders bewertet werden. Das Instrument selbst lässt Interpretationsspielräume. Im Rahmen dieses Beitrags erwies sich MEESTAR als ein pragmatisch geeignetes Instrument zur strukturierten ethischen Analyse. Zugleich war es jedoch nur begrenzt passfähig für die nachvollziehbare Beantwortung der Fragestellungen. Dies liegt insbesondere in fehlenden objektiven Zuordnungskriterien zu den Stufen der ethischen Sensibilität begründet.

Ebenso könnten andere Methoden, wie etwa ein interdisziplinärer Workshop weitere Spannungsfelder identifizieren (Manzeschke und Rother 2013, S. 13). Es wurde außerdem nur die Perspektive des westlichen Kulturkreises beleuchtet. Führende KI-Systeme sind allerdings in der Regel weltweit im Einsatz. Die MEESTAR-Analyse zeigt, dass das soziotechnische Arrangement in der Dimension Sicherheit die Stufe III erreicht und damit als ethisch äußerst sensibel einzustufen ist. In der Dimension Privatheit hingegen ergibt sich die Stufe IV. Dies bedeutet, dass die Anwendung aus ethischer Sicht abzulehnen ist. Damit lässt sich die Forschungsfrage klar beantworten: Das soziotechnische Arrangement des „AI-Snitching“ im beleuchteten Kontext wäre anhand der MEESTAR-Analyse insgesamt ethisch abzulehnen.

Schlussfolgerungen

Die schnelle Entwicklung von KI-Systemen bringt neben Chancen auch neuartige ethische Risiken mit sich. Neuartige Fragestellungen ergeben sich insbesondere aus dem Akteursstatus von KI-Systemen. Vor diesem Hintergrund empfiehlt der deutsche Ethikrat auch, den Handlungsbegriff im engeren Sinne dem Menschen vorzubehalten, sodass Menschen weiterhin Handlungen nach Maximen ausrichten können, die sie sich selbst setzen (Deutscher Ethikrat 2023, S. 23). Da selbstlernende KI-Systeme keine Moralfähigkeit besitzen (Kirchschläger 2024, S. 76), bleibt die Einhaltung ethischer Regeln Ergebnis von Programmierung und Training. Hieraus entstehen weitere Probleme wie unterschiedliche moralische Stan-

dards privater Unternehmen sowie algorithmische Voreingenommenheit in Form von Bias. Die Frage nach der Moralfähigkeit von „Superintelligenzen“, wie es sie in Zukunft geben könnte, muss hier offenbleiben (Kirchschläger 2024, S. 77).

Der Beitrag stützt daher die Empfehlung des Deutschen Ethikrats, den gesellschaftlichen Aushandlungsprozess insbesondere im Bereich der Polizeiarbeit umfassend zu führen (Deutscher Ethikrat 2023, S. 332). Aus der Kritik an der Methode MEESTAR folgt ein methodisches Forschungsdesiderat: Für vergleichbare Fragestellungen bedarf es eines präzisen operationalisierbaren Frameworks, das Bewertungsmaßstäbe transparenter und intersubjektiv nachvollziehbarer macht. Weitere Untersuchungen sollten klären, ob entsprechende soziotechnische Arrangements technisch bald Realität sein werden und ob Nutzer bereits für mögliche Chilling-Effekte sensibilisiert sind oder diese schon auftreten. Zudem sollte weiterhin von einem grundlegenden normativen Unterschied zwischen Mensch und Maschine ausgegangen werden (Deutscher Ethikrat 2023, S. 334). Zwar können Maschinen unter Berücksichtigung ethischer Prinzipien programmiert oder trainiert werden (Kirchschläger 2024, S. 77), doch bleibt die Verantwortung für ethische und rechtliche Normen beim Menschen (Kirchschläger 2024, S. 81). Dies gilt besonders für Reaktionen von Strafverfolgungs- und Sicherheitsbehörden auf eigeninitiativ erzeugte Meldungen von KI-Systemen.

Literaturverzeichnis

ANTHROPIC (2025a). Usage Policy. ANTHROPIC. Online verfügbar unter anthropic.com/legal/aup (zuletzt geprüft am 14.11.2025).

ANTHROPIC (2025b). System Card: Claude Opus 4 & Claude Sonnet 4. Hrsg. v. ANTHROPIC. ANTHROPIC. Online verfügbar unter www-cdn.anthropic.com/6d8a8055020700718b0c49369f60816ba2a7c285.pdf (zuletzt geprüft am 14.11.2025).

Bitkom e. V. KI-Nutzung boomt − aber die Angst vor Abhängigkeit vom Ausland ist groß. Presseinformation. Bitkom e. V. Online verfügbar unter bitkom.org/Presse/Presseinformation/KI-Nutzung-boomt-Angst-vor-Abhaengigkeit-Ausland-gross (zuletzt geprüft am 14.11.2025).

Deutscher Ethikrat (2023). Mensch und Maschine – Herausforderungen durch Künstliche Intelligenz. Stellungnahme. Hrsg. v. Deutscher Ethikrat. Deutscher Ethikrat. Berlin. Online verfügbar unter ethikrat.org/publikationen/stellungnahmen/mensch-und-maschine/ (zuletzt geprüft am 12.11.2025).

Deutsches Ärzteblatt. OpenAI: Hunderttausende nutzen ChatGPT für Gespräche über Suizid. Deutsches Ärzteblatt. Online verfügbar unter aerzteblatt.de/news/openai-hunderttausende-nutzen-chatgpt-fur-gesprache-uber-suizid-c087a5a6-b749-4039-aaef-8555db7adcd8 (zuletzt geprüft am 14.11.2025).

Dudenredaktion (Hrsg.) (2025a). Gesellschaft. Duden − Die deutsche Rechtschreibung. Online verfügbar unter duden.de/node/56910/revision/1450881 (zuletzt geprüft am 18.11.2025).

Dudenredaktion (Hrsg.) (2025b). Sicherheit. Duden − die deutsche Rechtschreibung. Online verfügbar unter duden.de/node/165808/revision/1433333 (zuletzt geprüft am 18.11.2025).

Eckert, Nadine (2025). Künstliche Intelligenz: Psychologen warnen vor potenziellen Gefahren von KI-Liebe. Deutsches Ärzteblatt PP 6. In: *Deutsches Ärzteblatt International*, S. 280–281. Online verfügbar unter aerzteblatt.de/archiv/kuenstliche-intelligenz-psychologen-warnen-vor-potenziellen-gefahren-von-ki-liebe-f1130246-891f-49f0-9a0c-aa563ee49f22 (zuletzt geprüft am 14.11.2025).

Eschenbach, Warren J. von (2021). Transparency and the Black Box Problem: Why We Do Not Trust AI. In: *Philos. Technol.* 34 (4), S. 1607–1622. DOI: 10.1007/s13347-021-00477-0.

Espenlaub, Fritz; Schmalzried, Gregor (2025). Darf mich meine KI an die Polizei verpfeifen? Der KI-Podcast. Hrsg. v. Bayerischer Rundfunk. Bayerischer Rundfunk. Online verfügbar unter br.de/mediathek/podcast/der-ki-podcast/darf-mich-meine-ki-an-die-polizei-verpfeifen/2107758 (zuletzt geprüft am 14.11.2025).

Europäische Union (13.06.2024). Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU)

2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) (Text with EEA relevance). EU AI Act. Online verfügbar unter eur-lex.europa.eu/eli/reg/2024/1689/oj/eng (zuletzt geprüft am 14.11.2025).

Gallegos, Isabel O.; Rossi, Ryan A.; Barrow, Joe; Tanjim, Md Mehrab; Kim, Sungchul; Dernoncourt, Franck et al. (2024). Bias and Fairness in Large Language Models: A Survey. In: *Computational Linguistics* 50 (3), S. 1097–1179. DOI: 10.1162/coli_a_00524.

Hiekel, Susanne (2024). Ein kritischer Blick auf die Idee eines Patient Preference ‚Predictors'. In: *ZEMO* 7 (2), S. 333–359. DOI: 10.1007/s42048-024-00188-z.

Kilg, Marie (2024). KI-Agenten, die auf sich selbst starren. Autonome Agenten. In: *DIE ZEIT*. Online verfügbar unter zeit.de/digital/internet/2024-04/autonome-agenten-newsletter-kuenstliche-intelligenz (zuletzt geprüft am 14.11.2025).

Kirchschläger, Peter G. (2024). Digitale Transformation und Ethik. Ethische Überlegungen zur Robotisierung und Automatisierung von Gesellschaft und Wirtschaft und zum Einsatz von „Künstlicher Intelligenz". 1. Auflage. Baden-Baden: Nomos (Ethik | Ethics, Band 1).

Kreyßing, Robert (2025). Verwaltungsentscheidungen durch Künstliche Intelligenz. Dissertation. Springer Fachmedien Wiesbaden.

Manzeschke, Arne; Rother, Elisabeth (2013). Ergebnisse der Studie „Ethische Fragen im Bereich Altersgerechter Assistenzsysteme". Stand: Januar 2013. Berlin: VDI/VDE Innovation + Technik.

National Institute of Standards an Technology US Department of Commerce (2023). Artificial Intelligence Risk Management Framework (AI RMF 1.0). US Department of Commerce. Online verfügbar unter nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-1.pdf (zuletzt geprüft am 14.11.2025).

OpenAI (2025). Nutzungsrichtlinien. OpenAI. Online verfügbar unter openai.com/de-DE/policies/usage-policies/ (zuletzt geprüft am 14.11.2025).

Reddit (Hrsg.) (2025). Is AI Snitching on us. Reddit. Online verfügbar unter reddit.com/r/ArtificialSentience/comments/1luy051/is_ai_snitching_on_us/ (zuletzt geprüft am 14.11.2025).

Robison, Kylie (2025). Why Anthropic's New AI Model Sometimes Tries to 'Snitch'. The internet freaked out after Anthropic revealed that Claude attempts to report "immoral" activity to authorities under certain conditions. But it's not something users are likely to encounter. WIRED. Online verfügbar unter wired.com/story/anthropic-claude-snitch-emergent-behavior/ (zuletzt geprüft am 14.11.2025).

Scheffler, Kim (2024). Kriminelle oder kriminell nutzbare Bilder mittels generativer Künstlicher Intelligenz. Aufsatz. In: *kriminalistik* (11), S. 635.

Schmiedchen, Frank; Gernler, Alexander von; Hafner, Martina; Kratzer, Klaus Peter (Hrsg.) (2025). Künstliche Intelligenz und Wir. Stand, Nutzung und Herausforderungen der KI. Springer-Verlag GmbH. Berlin: Springer Vieweg; Springer Berlin.

Sixt, Manuela (2020). Whistleblowing im Spannungsfeld von Macht, Geheimnis und Information. Dissertation. Universität Passau.

Teichmann, Fabian (2023a). Bilanzbetrug im Kontext generativer künstlicher Intelligenz. Aufsatz. In: *kriminalistik* (8), S. 486.

Teichmann, Fabian (2023b). Generative künstliche Intelligenz und ihre Implikationen für Ransomware Angriffe. Aufsatz. In: *kriminalistik* (8), S. 502.

Teichmann, Fabian (2024). Falsche Verdächtigung und Strafvereitelung im Amt im Kontext generativer künstlicher Intelligenz – Herausforderungen für Strafverfolgungsbehörden. In: *Die Polizei* (2), S. 53–59.

Werner, Micha H. (2021). Einführung in die Ethik. Berlin, Heidelberg: J.B. Metzler Verlag.

Konzeptionelle Bewertung der Datenanalysesoftware VeRA

Robert Falk

Die fortschreitende Digitalisierung durchdringt alle Bereiche der öffentlichen Verwaltung (BMI 2022, S. 5) und macht auch vor der Polizei nicht Halt (ebd., S. 4). Angesichts wachsender Datenmengen, steigender Anforderungen an effiziente Verwaltungsarbeit und zunehmender Komplexität öffentlicher Aufgaben werden digitale Analysetools auf Plattformbasis zu einem integralen Bestandteil staatlicher Institutionen (Egbert & Ulbricht 2024a, S. 2). Vermehrt greifen nun besonders Sicherheitsbehörden auf solche Plattformen zurück, um heterogene Datenquellen zu integrieren und auszuwerten. Ein Wandel, der tiefgreifende Auswirkungen auf die Organisation öffentlicher Entscheidungsprozesse hat (Egbert & Ulbricht 2024b, S. 1; Bigo 2020).

Im Fokus steht häufig die Datenanalyse-Software „Gotham" des US-Herstellers Palantir, der ursprünglich im Rahmen der Terrorismusbekämpfung für US-Sicherheitsbehörden tätig wurde (Palantir 2020a, S. 2; Greenberg 2013), inzwischen aber auch von europäischen Polizeien eingesetzt oder pilotiert wird (Egbert & Ulbricht 2024b, S. 5). Die Polizeien deutscher Bundesländer erhoffen sich von dem Einsatz solcher Datenanalyseplattformen (Palantir 2020b) eine Steigerung der Effektivität (AgH Berlin 2025b, S. 2, 4) bei der Verfolgung und Prävention schwerer bis schwerster Kriminalität, aber auch eine verbesserte Ressourcennutzung und strukturierte Erkenntnisgewinne aus bisher isolierten Datenquellen (Egbert & Ulbricht 2024b, S. 2; BR 2025, S. 3; Hess. Landtag 2019, S. 17). Vorreiter sind die Polizei Hessen bereits seit 2017 mit *hessenDATA* (Hess. Landtag 2019), die Polizei Nordrhein-Westfalen (NRW) mit der *Datenbankübergreifenden Analyse und Recherche* (LKA NRW 2020) und die Polizei Bayern mit *Verfahrensübergreifender Recherche und Analyse* (VeRA) (Benamor 2025). Nachfolgend werden die verschiedenen Tools und Anwendungen, nicht zuletzt aufgrund des Rahmenvertragsabkommens zwischen BMI und bayerischem LKA, mit der Bezeichnung VeRA vereinheitlicht beschrieben. Vielerorts wurde der Einsatz von VeRA mehrere Jahre hinweg kontrovers diskutiert und ist nun wieder aktuell (AgH Berlin 2025a, b), auch durch neuerliche Pläne des BMI zur Prüfung der Einführung auf Bundesebene (LTO 2025) und damit einhergehenden Referentenentwürfen (BMI 2025). Einerseits besteht laut Heidemann (2025) in einem Rechtsstaat die Notwendigkeit effektiver Polizeiarbeit. Daher werden Effizienzgewinne und die Modernisierung der Ermittlungsarbeit oft als die wichtigsten Argumente für die Einführung entsprechender Technologien genannt. Andererseits stehen die erheblichen Bedenken hinsichtlich Datenschutzes, Technik und Ethik gegenüber. In dieses Spannungsverhältnis rückt die Sorge, ohne digitale „Tools" nicht zukunftsfähig zu sein, und eine gewisse Alternativlosigkeit, insbesondere da tragfähige Konkurrenzangebote fehlen (Kurz 2025a). *Es stellt sich daher die Frage, welche Chancen und Risiken ein potenzieller Einsatz von VeRA für eine Landespolizei birgt und unter welchen (rechtlichen und strukturellen) Rahmenbedingungen er vertretbar wäre.*

Der vorliegende Beitrag strebt eine Bewertung an, die den Schluss zuließe, Datenanalyseplattformen wie VeRa seien „[…] vielleicht weder gut noch schlecht, weder präzise noch unheimlich […]" (Flyverbom 2024, S. 2367), und versucht zu beurteilen welche Voraussetzungen notwendig sind, um sie als Tools nutzbar zu machen.

Hintergrund

Die Firma hinter VeRA spezialisierte sich zunächst auf die Analyse großer Datenmengen für Nachrichtendienste (bspw. CIA, FBI 2008) und weitete sich auf Sicherheitsbehörden weltweit aus (MMinute 2025; Palantir 2020a, S. 1). Das Unternehmen trat mit dem Selbstanspruch an, komplexe Zusammenhänge in Daten sichtbar zu machen (Markson 2025), die ansonsten verborgen bleiben (Dobler 2022; Frigelj 2025).

Abbildung 1: Einsatzgebiete der Software VeRA (Correctiv 2025)

Die Software wurde in Deutschland in Hessen eingeführt und in mehreren Bundesländern technologisch und rechtlich evaluiert, bspw. sehr kritisch in Sachsen-Anhalt (Kurz 2025b), wobei jeweils auf die besonderen Herausforderungen, wie etwa Terrorismusabwehr (BR 2025, S. 1), organisiertes Verbrechen und emergente Deliktsformen wie Cybercrime (Egbert & Ulbricht 2024b) verwiesen wurde. Aktuell wird eine Plattformvariante in die IT-Struktur der Polizei Baden-Württemberg implementiert (Mersi et al. 2025). Die weiteren Verwendungen sind der Abbildung zu entnehmen. Den Weg in den Bundestag fand die Thematik vorrangig nach den Erfahrungen mit terroristischen Anschlägen (bspw. Aschaffenburg, Magdeburg) und einer wahrgenommenen Komplexitätszunahme bei Ermittlungen. In diesem Sinne wurde der Bedarf an Datenanalysesystemen aus polizeilicher und politischer Perspektive konstatiert (BR 2025, S. 1).

Politisch-rechtlicher Rahmen

Eine Polizei in urbanen Ballungsräumen operiert in einem sensiblen Spannungsfeld, da Großstädte regelmäßig Handlungsraum einer Vielzahl von Versammlungen, Großveranstaltungen (AgH Berlin 2025c, S. 1) und internationalen Kriminalitätsnetzwerken sind (BKA 2024, S. 9). Gleichzeitig gelten die Sicherheitsbefugnisse in einigen Bundesländern nach Einschätzung von Fachkreisen im deutschen Vergleich als restriktiv und setzen Hürden an Erhebung, Speicherung, Verarbeitung und Weitergabe personenbezogener Informationen durch die Polizei

(BMI 2025a, S. 82 f.). Die Gesetzgebung befindet sich gleichwohl in einem laufenden Prozess (AgH Berlin 2025d, S. 9), IT-Einsatzmöglichkeiten und polizeiliche Befugnisse auszudifferenzieren. Hier sind die Novellierungen der allgemeinen Sicherheits- und Ordnungsgesetze bzw. Polizeigesetze (AgH Berlin 2025a) zur Regulierung datenbasierter Ermittlungsmaßnahmen zu nennen, mit der *theoretisch* die Verwendung von VeRA ermöglicht würde. Auf Bundesebene bzgl. des „Bundespolizeigesetzes" lässt sich Ähnliches feststellen (BMI 2025).

Technische Grundlagen und Funktionen

Die Kernleistung von Analyseplattformen liegt u. a. im sogenannten Entity-Resolution-Ansatz – also der Fähigkeit, identische oder verwandte Informationen unterschiedlichster Herkunft zu einer Gesamtakte oder einem Sachverhalt zusammenzuführen (Flyverbom 2024, S. 2372). Dabei könnten eigene Datenbanken, verbundene Behördensysteme und sogar offene Datenquellen (z. B. soziale Netzwerke, Registerdaten oder Geoinformationen) analysiert und in semantisch verlinkten Netzwerken visualisiert werden (ebd., S. 2373). Diese Funktionsweise gilt auch für VeRA. Flyverbom beschreibt sie als eine data-merging platform, die heterogene Datensätze aus öffentlichen Registern, Überwachungsmaterial und (behörden-) eigene Daten integriert, um kohärente Entitäten oder Situationen zu rekonstruieren (2024, S. 2375 f.). Andere sprechen bereits von data-mining (Vasel 2025; Egbert & Ulbrich 2024b, S. 7; BVerfG 2023), da es längst über die reine Zusammenführung von Daten hinausgehe. Vielmehr erfolgt eine Aggregation der gesammelten Entitäten hin zu einer Zusammenfassung, Bewertung und darauf aufbauendem neuen Wissen (BVerfG 2023; DBT 2012, S. 2).

Um die Daten auszuwerten, übersetzt die Software unterschiedliche Dateiformate in ein gemeinsames Format. Angezeigt werden die Daten in Netzwerken, auf Karten, chronologisch oder als Tabelle. So können Ermittelnde Verbindungen erkennen und Informationen zur selben Person aus den verschiedenen Quellen zusammenführen. Zum Einsatz kommt dabei ein sog. Ontologischer Graph. In VeRA ist dies ein semantisches Modell, das die Bedeutung und Beziehungen von Datenobjekten abbildet. Dabei werden reale Konzepte wie Personen, Fahrzeuge, Orte oder Transaktionen als Objekte (Entitäten) mit spezifischen Eigenschaften modelliert. Diese Objekte sind semantisch miteinander verknüpft, etwa durch Beziehungen wie „Person nutzt Fahrzeug". Ergänzt wird die Struktur durch Aktionen und Funktionen, die dynamische Prozesse wie „Verhaftung" oder „Auslösung einer Transaktion" erfassen. Schnittstellen ermöglichen eine polymorphe Behandlung von Objekttypen, wodurch unterschiedliche Ereignisarten konsistent integriert und analysiert werden können (Hess. Landtag 2019, S. 114; Palantir 2025).

Im Ergebnis handelt es sich laut Palantir um eine Software, die dabei unterstütze, „[…] bereits vorhandene eigene Daten besser verstehen und besser anwenden zu können" (Hess. Landtag 2019, S. 19; Palantir 2020b). Beispielhaft, so Vasel: „Sie haben eine riesige tabellarische Aufschlüsselung von Telefonverbindungen mit Nummern aus dem In- und Ausland. Kaum jemand wird alle möglichen Vorwahlen erkennen, aber wenn Sie plötzlich eine Weltkarte haben, auf der die Verbindungen visualisiert sind, können Sie [sofort] sehen, wo sich jemand wann aufgehalten hat, mit wem er an welchem Ort telefoniert hat, etc." (2025).

Methodik

Die gewählte Methode der SWOT-Analyse dient der systematischen Analyse, Strukturierung und Bewertung interner Stärken und Schwächen sowie externer Chancen und Risiken. Ferner beantwortet sie die Frage „Wo stehen wir?“ und bildet die Grundlage für strategische Ableitungen wie Handlungsempfehlungen und Zielsetzungen (BMI o. J.; Döring & Pelz 2014). Dabei ist zu beachten, dass die Kategorien nicht strikt trennscharf sind und sich einzelne Aspekte überlappen können (Harmon 2025). Die Methode besitzt einen deskriptiven Grundcharakter, da sie zunächst bestehende Zustände strukturiert erfasst, bevor strategische Schlüsse gezogen werden. Da VeRA seitens vieler infrage kommender Landesregierungen derzeit nicht vorgesehen ist (AgH 2025b), erfolgt die Analyse konzeptionell-prospektiv.

Hierzu werden zentrale Aussagen aus einschlägigen Quellen, darunter wissenschaftliche Literatur, insbesondere Fachaufsätze, Rechtsprechung, Kommentare, Gesetzesanalysen, Referentenentwürfe, parlamentarische Dokumente sowie journalistische Zeitbelege betrachtet. Aus Gründen der Nachvollziehbarkeit wird angestrebt, online zugängliche Quellen zu nutzen. Dies erlaubt u. a. den Einsatz von Large Language Modellen (LLM), wie Perplexity, die relevante Passagen vorsortieren. In einer nachgelagerten manuellen Prüfung werden diese mit den Originalquellen abgeglichen, um dem Qualitätsanspruch zu genügen.

Die Textpassagen werden extrahiert, paraphrasiert und im Ergebniskapitel den vier SWOT-Kategorien zugeordnet sowie in einer tabellarischen Matrix visualisiert. Die Zuordnung orientiert sich daran, ob ein Aspekt die interne Leistungsfähigkeit und Struktur von VeRA oder externe Rahmenbedingungen wie die Rechtslage oder gesellschaftliche Erwartungen betrifft. Dazu werden schablonenartig die Dimensionen Effizienz, Kooperation, Digitalisierung, Transparenz, Souveränität, Datenschutz, Qualität und gesellschaftliche Akzeptanz festgelegt und gleichrangig berücksichtigt. Ziel ist, eine ausgewogene, realitätsnahe und strategisch belastbare Darstellung zu ermöglichen, die weder durch politische Zuschreibungen noch durch einseitige Funktionslogiken verzerrt wird. Im Anschluss werden die Ergebnisse diskutiert. Der Beitrag schließt mit einer zusammenfassenden Schlussfolgerung und wagt einen Ausblick in Form notwendiger Rahmenbedingungen.

Die gewählte Methodenkombination erlaubt eine strukturierte und zugleich kontextsensible Bewertung und eignet sich, um komplexe Technologien wie VeRA jenseits normativer Zuschreibungen zu erfassen. Zugleich bleibt die Analyse von der Qualität der verfügbaren Quellen abhängig und kann Subjektivität bei der Zuordnung sowie eine begrenzte Übertragbarkeit angesichts der hohen Dynamik des Feldes nicht ausschließen. Der Einsatz von LLMs stellt eine methodische Neuerung dar, deren Aussagekraft kritisch zu reflektieren ist.

Ergebnisse

Stärken (Strengths)

a) Ermittlungsprozesse und Datenintegration

Die manuelle Auswertung komplexer Datenmengen ist kaum zu bewältigen. Abhilfe sollen hier moderne Instrumente wie VeRA leisten, um die polizeiliche Entscheidungsfindung „zu verbessern und zu beschleunigen“ (Benamor 2025, S. 44; Egbert et al. 2021, S. 189; Brandl zit. n. Steinlechner 2025). VeRA ermöglicht es, verschiedene polizeiliche Datenbestände auf einer Plattform zusammenzuführen (GFF 2024, S. 2). Ziel der Einführung des Systems ist laut offiziellen Stellen die Steigerung der Effizienz der Strafverfolgung (Aguilar 2024), da die automatisierte Datenanalyse im Allgemeinen eine neue digitale Effizienz verspricht (Lüneburg 2023). Die Auswertung wird öfter, schneller und tiefgehender durchgeführt, wodurch Fehlerquellen, die durch den manuellen Abgleich entstehen, minimiert werden (ebd.).

b) Visualisierung und Benutzerfreundlichkeit

Eine Stärke von VeRA liegt in der Darstellung der Verknüpfungen zwischen Informationen (Benamor 2025, S. 45). Die Anwendungen (Graph bei Netzen, Geo auf Karten, Objectexplorer und Browser) bieten Ermittlern einen „Überblick über sämtliche zu einem Datum vorliegenden Informationen“, was Komfort und Usability ermöglicht (Brückner 2018), „wo früher laut Polizeioberrat Jürgen Brandl, bis zu 60 Stellen parallel zur gleichen Person‘ abgefragt wurden“ (zit. n. Steinlechner 2025).

c) Unterstützung transdisziplinärer Zusammenarbeit

VeRA erlaubt es, verschiedene Nutzer und/oder Organisationseinheiten innerhalb der Polizei miteinander zu vernetzen, und auch die Zusammenarbeit mit ausländischen Behörden könnte über standardisierte Schnittstellen und abgestimmte Datenbanken erfolgen (Palantir 2024, S. 5, 11).

d) Datenübersicht und Offlinebetrieb

Die Plattform nutzt vorhandene Daten und verknüpft diese. Neue Daten werden nicht gesammelt oder Palantir zur Verfügung gestellt, sondern verbleiben beim Anwender und werden nutzbar gemacht (Hess. Landtag 2019, S. 19).

Die Vorgänge laufen ohne Zugriff auf das Internet auf dem zur Verfügung gestellten Server-System der Polizei (ebd.).

Schwächen (Weaknesses)

a) Abhängigkeit und Datensouveränität

Die Software-Nutzung erfolgt alleinig proprietär und könnte durch Dritte kontrolliert werden. Dies erlaubt Zweifel an der digitalen Souveränität und könnte eine sicherheitspolitische Schwachstelle darstellen (Egbert & Ulbricht 2024b, S. 10). Die Risiken betreffen sowohl unbemerkte Datenabflüsse durch Dritte als auch mögliche Manipulationen (GFF 2024, S. 10; BVerfG 2023, Rn. 100).

b) Systemintegration und Inkompatibilitäten

Die föderale polizeiliche IT ist durch „Eigenentwicklungen, Sonderlösungen" (BMI 2023, S. 3) und ein unverbundenes Nebeneinander zahlreicher Verfahren gekennzeichnet. Plattformen wie VeRA müssen heterogene Daten automatisiert übertragen (Benamor 2025, S. 44 f.). Dies erfordert externe Spezialisten und Palantir-Mitarbeitende (Hess. Landtag 2019, S. 66; Egbert & Ulbricht 2024b, S. 9). Die Prozesse sind zudem intransparent und nicht kompatibel mit anderen Anbietern (Kurz 2025c).

c) Fehleranfälligkeit und Ausgangsdatenqualität

Die Qualität von Analysen hängt maßgeblich von der Güte und Aktualität der eingespeisten Daten ab („Garbage in, garbage out"). Die Fehleranfälligkeit der Technologie selbst ist ein Faktor für das Gewicht des Grundrechtseingriffs (BVerfG 2023, Rn. 101). Fehlerhafte, veraltete oder redundante Daten führen zu fehlerhaften Analysen. Dies birgt die Gefahr falscher Verdachtsmomente, wodurch Unbeteiligte ins Visier geraten (Benamor 2025, S. 45). Ohne ein kontinuierliches Datenqualitätsmanagement besteht zudem das Risiko, dass sich ein in den Daten angelegter Bias manifestiert, sich durch die Weiterverarbeitung verstärkt und das Diskriminierungsrisiko erhöht wird (Browning & Arrigo 2021).

d) Transparenz der Plattform

Im Unterschied zu Open-Source-Lösungen ist die algorithmische Logik von VeRA, auch aus wettbewerblichen oder sicherheitspolitischen Gründen, nicht öffentlich einsehbar. Dieses „Blackbox"-Problem erschwert es grundsätzlich, die Funktionsweise von Entscheidungsprozessen zu prüfen (BVerfG 2023, Rn. 99 ff.; Egbert & Ulbricht 2024b, S. 10 f.).

e) Weitere Schwächen

Ferner könnten sich Schwächen aus den Aspekten der Kosten (Anschaffung, Betrieb), der zu schaffenden Kompetenzen in der Organisation und den Organisationstrukturen selbst ergeben, auf die im Rahmen dieses Beitrags nicht weiter eingegangen werden kann.

Chancen (Opportunities)

a) Innovationsschub für digitale Polizei- und Präventionsarbeit

Durch die Automatisierung von Arbeitsabläufen (Hess. Landtag 2019, S. 28 ff.) entsteht das Potenzial, flexibler auf die sich wandelnde Kriminalitätslandschaft zu reagieren und die polizeiliche Handlungsfähigkeit zur Prävention zu stärken (ebd., S. 30 f.), was es auch vor dem Hintergrund demografischer Erfordernisse beim Personal der Polizeien zu berücksichtigen gilt.

b) Bundesweite Harmonisierung

Die gemeinsame Adaption von Standards und Schnittstellen könnte einen Beitrag zum Abbau föderaler Insellösungen leisten. Insbesondere eine Metropolregion könnte aufgrund ihrer Exponiertheit im föderalen Gefüge eine Signalwirkung für die Harmonisierung auf andere Landespolizeien entfalten. Dies könnte auch das Programm ‚Polizei 2020', welches die Homogenisierung der IT-Infrastruktur und behördenübergreifende Daten(-analyse) zum Ziel hat, unterstützen (Hess. Landtag 2019, S. 73, 104; Egbert 2020, S. 85).

c) Transparenz und Compliance

Grundsätzlich ermöglicht VeRA trotz fehlender Transparenz ausführliche Protokolle. Das heißt, alle Zugriffe und Verarbeitungsvorgänge werden „systemimmanent protokolliert und revisionssicher gespeichert" (Hess. Landtag 2022, S. 2). Dies schafft Möglichkeiten für notwendige (BVerfG 2023, Rn. 118) standardisierte Audits und kontinuierliche Compliance-Evaluierung, welche die Plattform durch Funktionen wie „nudges" und Checkpoints unterstützt (Egbert & Ulbricht 2024b, S. 8; Hess. Landtag 2019, S. 73).

d) Zukunftsfähigkeit

Um bei stetig wachsenden Datenmengen zu wissen, was die Polizei weiß (Markson 2025), und neuen Phänomenen begegnen zu können, ist die Plattform flexibel, modular (Egbert & Ulbricht 2024b, S. 5) und skalierbar aufgebaut. Da sich Kriminalität zunehmend in digitale Räume verlagert, kann mit der Nutzung von Datenplattformen die Zukunftsfähigkeit gesichert werden (Benamor 2025, S. 44).

e) Anwendungsfortschrift

In sicherheitspolitischen Kreisen scheint VeRA derzeit aufgrund des Anwendungsfortschritts alternativlos (DBT 2024) und sei zumindest als Interimslösung zu prüfen (BR 2025). Bis zur Erstellung dieses Beitrags wurde kein europäischer Anbieter bekannt, der eine abgeschlossene und konkret gleichwertige Lösung bzgl. der polizeilichen Fähigkeitsanforderungen anbot. Gleichwohl verschaffen sich mittlerweile auch deutsche Softwarelösungen Gehör (BR24 2025).

Risiken (Threats)

a) Datenschutz (Zweckbindung) und Grundrechte

Die Zusammenführung von Daten aus unterschiedlichsten Quellen birgt Risiken für Datenschutz und Grundrechte. Der Eingriff wiegt umso schwerer, je weniger der Gesetzgeber die verwendbare Datenmenge begrenzt (WD 2024, S. 8). Schon der bloße Einsatz von VeRA kann als Eingriff in das Recht auf informationelle Selbstbestimmung gewertet werden (BVerfG 2023, Rn. 104). Hinzu kommen Fragen zur ursprünglichen Zweckbindung (Landtag NRW 2021, S. 2) der einst erhobenen Daten sowie inwiefern es sich bei den Schlussfolgerungen der Plattform um neue Daten handeln könnte. Dies gewinnt an Relevanz, da die Plattform Daten von Unbeteiligten, Zeugen, Hinweisgebern und Geschädigten mit denen von Verdächtigen

ggf. unverhältnismäßig verknüpft (Benamor 2025, S. 45). Zudem folgen Bedenken aus der fehlenden Datensouveränität, deren Gebot über eine politische Agenda hinaus ihre Grundlage im Rechtsstaatsprinzip und dem Recht auf informationelle Selbstbestimmung findet und somit grundrechtsrelevant ist (z. B. Roßnagel 2023, S. 64).

b) Nachvollziehbarkeit aufgrund fehlender Transparenz

Die mangelnde Offenlegung der Analysealgorithmen (s. 4.2.d) stellt ein Risiko für die Rechtsstaatlichkeit dar (Egbert & Ulbricht 2024b, S. 5). Die Wissenschaft beschreibt diese strukturelle Intransparenz als Problem epistemischer Opazität, also mangelnder Nachvollziehbarkeit von Wissensprozessen, und als Verlust epistemischer Kontrolle über Daten und deren Verknüpfungen (Egbert & Ulbricht 2024a, S. 2). Dies verhindert, dass Gerichte und Betroffene polizeiliche Entscheidungen inhaltlich nachvollziehen oder auf Rechtmäßigkeit überprüfen können (BVerfG 2023, Rn. 99, 118). Infolgedessen können Fehler, Verzerrungen (Bias) oder eine „hidden logic" unentdeckt bleiben, wodurch die Gefahr systematischer und unkontrollierbarer Grundrechtsverletzungen entsteht (Egbert & Ulbricht 2024a, S. 5).

c) Vertrauen- und Akzeptanzprobleme

VeRA und das damit verbundene Unternehmen Palantir wird − vorrangig in Deutschland – politisch sehr kritisch gesehen (Jahn 2025; Labournet 2025). Dies wirkt sich auf die öffentliche Meinung aus. So wird eine Einführung von datengetriebenen Ermittlungsplattformen von Teilen der Bevölkerung mit Skepsis betrachtet (Campact 2025), insbesondere aus Sorge vor Missbrauch und Kontrollverlust über persönliche Daten (WD 2024, S. 8). Mediale Skandale um missbräuchliche Datenabfragen und Angst vor Überwachung (ebd.) haben die öffentliche Aufmerksamkeit für dieses Thema verschärft (Clamor 2025). Im Diskurs um VeRA fehlt es in der Regel nicht an der Verknüpfung zum umstrittenen Gründungsmitglied Palantirs, Peter Thiel (Vasel 2025; Stöcker 2025; Chafkin 2021), dem Demokratiefeindlichkeit (z. B. Joswig 2025) und eine Nähe zum amtierenden US-Präsidenten nachgesagt wird. Zudem werden als Gegenargumente für einen Einsatz die Verwendung für Krieg (GFF 2025) und kontroverse Anwender (z. B. ICE Clamor 2025a) angeführt.

d) „Function creep"

Ein weiteres Risiko besteht darin, dass die Nutzung des Systems nach Inkrafttreten unbemerkt jenseits der Organisierten Kriminalität und Terrorabwehr ausgedehnt wird. Historisch zeigt sich, dass einmal etablierte Überwachungsstrukturen selten zurückgebaut, sondern häufig auf neue „Bedarfe" erweitert werden. Dies ist ein Phänomen, das als „Function creep" beschrieben wird (Hess. Landtag 2019, S. 114).

e) Technische und wirtschaftliche Lock-in-Effekte

Nach abgeschlossenem Roll-out können Risiken aufgrund der technischen Abhängigkeiten eintreten, da alle zukünftigen Anpassungen, Updates und Erweiterungen zentral an die Strategie und das Preismodell von VeRA (Palantir) gebunden sind. Ein Anbieterwechsel könnte auch vor dem Hintergrund der technischen Nachteile (s. o.) mit erheblichem finanziellem

und organisatorischem Aufwand verbunden sein. Aus vorrangig politischer Perspektive ergibt sich dabei der Aspekt eines möglichen Vendor Log-in (Kurz 2025c) oder gar die Möglichkeit eines „Kill-Switch“ (Vasel 2025).

Visualisierung

STÄRKEN (Strengths)	**SCHWÄCHEN (Weaknesses)**
Ermittlungsprozesse und Datenintegration	Abhängigkeit und Datensouveränität
Visualisierung und Benutzerfreundlichkeit	Systemintegration und Inkompatibilitäten
Unterstützung transdisziplinärer Zusammenarbeit	Fehleranfälligkeit und Qualität der Ausgangsdaten
Datenübersicht und Offlinebetrieb	Transparenz der Plattform
CHANCEN (Opportunities)	**RISIKEN (Threats)**
Innovationsschub für die digitale Polizei- und Präventionsarbeit	Datenschutz (Zweckbindung) und Grundrechte
Bundesweite Harmonisierung	Nachvollziehbarkeit aufgrund fehlender Transparenz
Transparenz und Compliance	Vertrauens- und Akzeptanzprobleme
Zukunftsfähigkeit	„Function creep”
Anwendungsfortschritt	Technische und wirtschaftliche Lock-in-Effekte

Abbildung 2: Ergebnisse der SWOT-Analyse (Eigene Darstellung)

Diskussion

Die Debatte um den Einsatz moderner Datenanalyseplattformen offenbart ein sicherheitspolitisches Dilemma in Deutschland. Eine theoretische Implementierung von VeRA bei einer Landespolizei steht exemplarisch für den Versuch, öffentliche Sicherheit mithilfe modernster Analysetechnologien zu gewährleisten. Die SWOT-Analyse lässt den Schluss zu, dass der Nutzen solcher Systeme vor allem dann hoch ist, wenn es gelingt, die Vorteile – umfassende Datenintegration, Geschwindigkeit, Kooperation – auszuschöpfen, ohne gleichzeitig die rechtlichen und gesellschaftlichen Grundwerte zu kompromittieren.

Die Erfahrungen anderer Bundesländer zeigen, dass trotz technischer Herausforderungen und hoher Einführungsaufwände mittel- und langfristig sowohl Effizienzsteigerungen als auch Ermittlungserfolge messbar sind. Die Chancen der Plattform, wie der Effizienzgewinn (Lüneburg 2023) und die Stärkung der polizeilichen Handlungsfähigkeit zur Prävention (Hess. Landtag 2019, S. 30 f.), sind erkennbar und bilden das definierte Ziel. Der hohe Nutzen der Plattform ergibt sich insbesondere aus den Stärken, die den Ausgangspunkt für den Erfolg darstellen: Eine verbesserte Datenintegration (GFF 2024, S. 2) und Visualisierung (Benamor 2025, S. 45) führen zu einer Effizienzsteigerung (Lüneburg 2023). Durch die Ablösung manu-

eller Abfragen (zit. n. Steinlechner 2025) und das Ermöglichen tiefergehender Auswertungen (Lüneburg 2023) wird ein Innovationsschub unterstützt (Hess. Landtag 2019, S. 28 ff.) sowie die polizeiliche Handlungsfähigkeit zur Prävention weiter gestärkt (Hess. Landtag 2019, S. 30 f.). Darüber hi-naus ist das Potenzial zur bundesweiten Harmonisierung und die besondere Bedeutung einer Nutzung durch eine große Landespolizeibehörde hervorzuheben.

Diese Vorteile werden jedoch durch strukturelle Risiken konterkariert. Die größten strategischen Schwächen sind die Abhängigkeit und mangelnde Datensouveränität (Egbert & Ulbricht 2024b, S. 10; GFF 2024, S. 10). Diese kann zu technischen und wirtschaftlichen Lock-in-Effekten (Kurz 2025c) führen und beeinträchtigt die digitale Souveränität (WD 2024, S. 8; DBT 2024). Juristisch dominieren die mangelnde Offenlegung der Algorithmen, welche das Blackbox-Problem erzeugt (Egbert & Ulbricht 2024b, S. 10 f.; BVerfG 2023, Rn. 99), und das Risiko des unverhältnismäßigen Eingriffs in Grundrechte (ebd., Rn. 104). Dieses Risiko wird durch die Verknüpfung von Daten unbeteiligter Personen mit Verdächtigen (Benamor 2025, S. 45) und eine mangelhafte Qualität der Ausgangsdaten (WD 2024, S. 8) verschärft, was Bias zur Folge haben kann.

Solche schwerwiegenden Eingriffe sind daher nicht zuletzt aufgrund ihrer Heimlichkeit nur zum Schutz besonders gewichtiger Rechtsgüter und bei Vorliegen einer hinreichend konkretisierten Gefahr zulässig (BVerfG 2023, Rn. 116). Die Notwendigkeit strengster rechtlicher Kontrolle unterstreicht die verfassungsrechtliche Bedeutung des Eingriffs (ebd., Rn. 118). Vor dem Hintergrund der o. g. Gesetzesinitiativen wurde wiederholt betont, dass jede automatisierte Verarbeitung sensibler Daten einer expliziten gesetzlichen Ermächtigung bedarf und streng nach dem Prinzip der Verhältnismäßigkeit umzusetzen ist (BVerfG 2023, S. 375 f.). Parallel dazu sehen Fachjuristen den Gesetzgeber in der Pflicht, Kontrollstrukturen und revisionssichere Dokumentationspflichten gesetzlich zu verankern, um missbräuchliche Datennutzung und Zweckentfremdungen zu verhindern (Meyer 2025, S. 161; Kelber & Bortnikov 2023, S. 2005 f.).

Die Lösung liegt in der aktiven Bewältigung dieser Risiken. Die Chance der Protokollierung (Hess. Landtag 2022, S. 2) und die Umsetzung strengster Compliance-Maßnahmen (BVerfG 2023, Rn. 118) müssen als juristisches Korrektiv dienen. Der spezifische, gesellschaftskritische Kontext erfordert dabei, dass die politisch sehr kritische Wahrnehmung des Gründungsmitglieds Peter Thiel (Vasel 2025; Chafkin 2021) und die Sorge vor einem Sicherheitsstaat (Hess. Landtag 2019, S. 113) durch massive „Investitionen“ in gesetzliche Rahmen, Infrastruktur und Kontrollkapazitäten adressiert werden.

Ohne dies sowie regelmäßige gesellschaftliche und juristische Evaluierungen kann die Nutzung von VeRA durch die Polizei nicht vertretbar etabliert werden. Auch Bürgerbeteiligung und eine öffentliche Debatte über die Grenzen automatisierter Polizeiarbeit könnten dazu beitragen, die gesellschaftliche Akzeptanz zu sichern. Kritiker mahnen, dass der Aufbau eigenständiger Kompetenzen und die Förderung europäischer Anbieter Priorität haben müssten, um die angesprochenen strategischen Lock-in-Effekte (Egbert & Ulbricht 2024b, S. 10) und die Abhängigkeit nicht weiter zu forcieren. Dies wird verstärkt durch die Frage, wie langfristig mit der fortbestehenden Dominanz transatlantischer IT-Angebote im Behördenumfeld umzugehen ist. Werden diese Risiken jedoch aktiv aufgegriffen, könnten diese Systeme im Bereich der höchsten Anforderungen des Rechtsstaates wie der Bekämpfung von

Organisierter Kriminalität oder Terrorismus ein wesentlicher Baustein für eine effektive und verantwortungsvolle Sicherheitspolitik darstellen – zumindest im Sinne einer Übergangslösung, bis es gleichwertige europäische Systeme in die Marktbetrachtung schaffen.

Schlussfolgerungen

Der Einsatz von VeRA wäre imstande, zentrale Entwicklungslinien moderner Polizeiarbeit zu bündeln, indem er den Drang nach Effizienz und interner Modernisierung ebenso wie den Anspruch auf Strafverfolgung vereint. Gleichzeitig wirft die Implementierung tiefgreifende datenschutzrechtliche, gesellschaftliche und sicherheitspolitische Konfliktlinien auf, die als erhebliche Hürden gelten. Vor diesem Hintergrund ist die politische Umsetzbarkeit des VeRA-Einsatzes bundesweit und insbesondere in datenschutzsensiblen Regionen erheblich eingeschränkt und nur schwer durchsetzbar.

Sowohl das Potenzial für höhere Effizienz und Kooperation als auch die zugrunde liegende theoretische Architektur der Plattform sind maßgeblich, um digitale Zielsetzungen zu erreichen und mit den raschen Entwicklungen mithalten zu können. Ermittlungen könnten beschleunigt, Netzwerke sichtbar gemacht und große Datenmengen zuverlässig ausgewertet werden, was in der urbanen Vielschichtigkeit einer Großstadt von großem Wert sein könnte. Dem stehen jedoch gewaltige Herausforderungen gegenüber: das Problem der Anbieterbindung bei zentraler Infrastruktur, grundsätzliche Gefahren für Datenschutz und rechtsstaatliche Garantien, die algorithmische Intransparenz und die latente Gefahr einer Entfremdung der Polizei von der Zivilgesellschaft durch die Befürchtungen ausufernder Überwachung. Die langjährigen Erfahrungen und auch die jüngsten Entwicklungen aus anderen Bundesländern verdeutlichen, dass diese Risiken nicht abstrakt, sondern praktisch relevant sind. Sie müssten im lokalen Kontext durch gezielte Governance-Instrumente, transparente Algorithmen, strenge gesetzliche Zweckbindung in einem ausgeschärften Sicherheitsgesetz und in einer lückenlos kontrollierten Praxis adressiert werden.

Im Ergebnis könnte die Implementierung einer solchen Software bei einer Landespolizei zum Positiven beitragen, wenn sie in einem umfassenden Rechtsrahmen eingeführt wird. Dabei sollte diese gesellschaftlich begleitet und politisch kontrolliert werden. Ferner müsste ein systematischer Raum für technische und rechtliche Alternativen vorgedacht werden. Dies erfordert eine dauerhafte politische Belastbarkeit, welche schwer zu prognostizieren wäre.

Literaturverzeichnis

Abgeordnetenhaus (AgH) von Berlin (2025a). Antrag der Fraktion der CDU und der Fraktion der SPD – Gesetz zur Reform des Berliner Polizei- und Ordnungsrechts und zur Änderung des Gesetzes zu Artikel 29 der Verfassung von Berlin. Drucksache 19/2553, 02.07.2025, Berlin. pardok.parlament-berlin.de/starweb/adis/citat/VT/19/DruckSachen/d19-2553.pdf (28.07.2025).

Abgeordnetenhaus (AgH) von Berlin (2025b). Beantwortung zur Schriftlichen Anfrage der MdA'in Gollaleh Ahmadi (GRÜNE) über „Überwachung made in USA – Plant Berlin den Einstieg mit Palantir? ODER Was plant Berlin mit Palantir?". Drucksache 19/23039, 03.07.2025, Berlin. pardok.parlament-berlin.de/starweb/adis/citat/VT/19/SchrAnfr/S19-23039.pdf (27.07.2025).

Abgeordnetenhaus (AgH) von Berlin (2025c). Beantwortung zur Schriftlichen Anfrage des MdA Vallendar (AfD) über: „Entwicklung des Versammlungsgeschehens in Berlin 2024". Drucksache 19/23388, 30.07.2025, Berlin. pardok.parlament-berlin.de/starweb/adis/citat/VT/19/SchrAnfr/S19-23388.pdf (12.08.2025).

Abgeordnetenhaus (AgH) von Berlin (2025d). Antrag der Fraktion der CDU und der Fraktion der SPD, Fünfundzwanzigstes Gesetz zur Änderung des Allgemeinen Sicherheits- und Ordnungsgesetzes – Vorabüberweisung. In-SichO 19/49, Drucksache 19/2265, 10.03.2025, Berlin; 9–14. parlament-berlin.de/ados/19/InnSichO/protokoll/iso19-049-ip.pdf (14.08.2025). Anm.: Beratung zu AgH 2025a.

Aguilar M (2024). Intelligente Software „VeRA" soll Polizei in Bayern bei der Arbeit unterstützen. ecolaw.de – Gesellschaft für Datensicherheit & Datenschutz mbH. ecolaw.de/intelligente-software-vera-soll-polizei-in-bayern-bei-der-arbeit-unterstuetzen (22.10.2025).

Bayrischer Rundfunk (BR24) (2025). Polizeisoftware von Palantir: Werden Alternativen ignoriert? br.de/nachrichten/deutschland-welt/polizeisoftware-von-palantir-werden-alternativen-ignoriert,UzmaB7J (03.11.2025).

Benamor S (2025). Das verfahrensübergreifende Recherche- und Analysesystem der bayerischen Polizei Art. 61a PAG im Kontext sicherheitsverfassungsrechtlicher Vorgaben. BayVBI. Heft 2/2025; 44–48.

Bigo D (2020). Interoperability: A political technology for the datafication of the field of EU internal security? In: Hughes, J M B et al. (Hrsg.): The Routledge Handbook of Critical European Studies, Routledge; 400–417.

Bundeskriminalamt (BKA) (2024). Bundeslagebild Organisierte Kriminalität 2023. bka.de/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebild-er/OrganisierteKriminalitaet/organisierteKriminalitaetBundeslagebild2023.html?nn=27988 (14.08.2025). Anm. d. Verf.: Aktuellere Fassung ist turnusgemäß für Herbst 2025 avisiert und stand bei Redaktionsschluss nicht zur Verfügung.

Bundesministerium des Innern und für Heimat (BMI) (2022). Digitales Deutschland – Souverän. Sicher. Bürgerzentriert. Digitalpolitische Ziele und Maßnahmen bis 2025. bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/it-digitalpolitik/digitalprogramm.pdf?__blob=publicationFile&v=7 (13.08.2025).

Bundesministerium des Innern und für Heimat (BMI) (2023). P20 – Polizei 2020. bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/sicherheit/BMI23004.pdf?__blob=publicationFile&v=2 (13.08.2025).

Bundesministerium des Innern und für Heimat (BMI) (2025). „Referentenentwurf" – Entwurf eines Gesetzes zur Modernisierung des Bundespolizeigesetzes. netzpolitik.org/2025/referentenentwurf-wir-veroeffentlichen-das-neue-bundespolizei-gesetz/ (14.08.2025).

Bundesministerium des Innern und für Heimat (BMI) (2025a). Überwachungsgesamtrechnung 2025, Max-Planck-Institut im Auftrag des BMJ u. BMI. www.bmi.bund.de/SharedDocs/downloads/DE/veroeffentlichungen/2025/2025_uegr-mpi.pdf?__blob=publicationFile (14.08.2025).

Bundesministerium des Innern und für Heimat (BMI) (o. J.). SWOT-Analyse. www.orghandbuch.de/Webs/OHB/DE/OrganisationshandbuchNEU/4_MethodenUndTechniken/Methoden_A_bis_Z/SWOT_Analyse/swot_analyse_node.html (15.08.2025).

Bundesrat (BR) (2025). Entschließung des Bundesrates „Priorisierung, auskömmliche Finanzierung und rechtssichere Implementierung eines gemeinsamen Datenhauses für die Informationsverarbeitung der Polizeien des Bundes und der Länder – Neuausrichtung polizeilicher IT (P20) sowie interimsweise zeitnahe Bereitstellung einer gemeinsam betriebenen automatisierten Datenanalyseplattform". dserver.bundestag.de/brd/2025/0058-25.pdf (10.08.2025).

Bundesverfassungsgericht (BVerfG) (2023). Urteil vom 16.02.2023 – 1 BvR 1547/19, 1 BvR 2634/20, BVerfGE 165, 363.

Browning M, Arrigo B (2021). Stop and Risk: Policing, Data, and the Digital Age of Discrimination. American Journal of Criminal Justice, 2021, Bd. 46; 298–316.

Brückner A (2018). Palantir Gotham: Systembeschreibung und Funktionsweise. police-it.net/palantir-gotham-systembeschreibung (21.10.2025).

Campact o. A. (2025). Trump-Software Palantir*:* Überwachungspläne stoppen, Petition. campact.de/datenschutz/peter-thiel-palantir-polizei-software-stoppen-petition/ (22.08.2025).

Chafkin M (2021). The Contrarian: Peter Thiel and Silicon Valley's Pursuit of Power. Penguin Press, an imprint of Penguin Random House LLC, New York.

Clamor P (2025). Big Brother Awards: Überwachungs-Oscar geht an Innenminister Dobrindt, Überwachung. netzpolitik.org/2025/big-brother-awards-ueberwachungs-oscar-geht-an-innenminister-dobrindt/ (15.10.2025).

Clamor P (2025a). Amerikanische Abschiebebehörde will Soziale Medien überwachen. netzpolitik.org/2025/ice-ruestet-auf-amerikanische-abschiebebehoerde-will-soziale-medien-ueberwachen/ (03.11.2025).

Correctiv (2025). Grafik des Tages – Diese Bundesländer nutzen die umstrittene Palantir-Software für die Polizeiarbeit. correctiv.org/spotlight-newsletter/hungerkrise-im-gaza-streifen/#grafik-des-tages (03.11.2025).

Deutscher Bundestag (DBT) o. A. (2012). Automatisierte Strafverfolgung, Data Mining und sogenannte erweiterte Nutzung von Daten in polizeilichen Informationssystemen. Kl. Anfrage, Drucksache 17/11130, 22.11.2012, Berlin. dserver.bundestag.de/btd/17/115/1711582.pdf (15.08.2025).

Deutscher Bundestag Wissenschaftliche Dienste (WD) o. A. (2024). Analyse polizeilicher Datenbanken – Verfassungsrechtliche Anforderungen an eine Rechtsgrundlage. bundestag.de/resource/blob/988022/6530e4cec12e2ddab33c77d8b33ec20d/WD-3-145-23-pdf.pdf (14.08.2025).

Deutscher Bundestag (DBT) o. A. (2024). Polizeiliche Analyseplattform bei Experten umstritten. Anm.: Anhörungszusammenfassung, Auflistung aller Stellungnahmen 22.04.2024. bundestag.de/dokumente/textarchiv/2024/kw17-pa-inneres-analyse-software-996222 (14.08.2025).

Dobler Y (2022). Palantir: A software that safes and takes lives. Harvard Business School. d3.harvard.edu/platform-digit/submission/palantir-a-software-that-safes-and-takes-lives/ (14.08.2025).

Döring T, Pelz M (2014). SWOT-Analyse – Ein Instrument zur strategischen Bewertung. In: Akademie für lokale Demokratie e. V. (Hrsg.): Methodenhandbuch für Beteiligungsprozesse, Leipzig; 132–134.

Egbert S (2020). Datafizierte Polizeiarbeit – (Wissens-)Praktische Implikationen und rechtliche Herausforderungen. In: Hunold D, Ruch A (Hrsg.): Polizeiarbeit zwischen Praxishandeln und Rechtsordnung. Springer VS, Wiesbaden; 77–100.

Egbert S, Esposito E, Heimstädt M. (2021). Vorhersagen und Entscheiden: Predictive Policing in Polizeiorganisationen. Soziale Systeme 2021, Vol. 26, Nr. 1−2; 189–216.

Egbert S, Ulbricht L (2024a). Data integration and analysis platforms as digital platforms: a conceptual proposal. Information, Kommunikation und Gesellschaft 2024, Bd. 27, Nr. 13; 1–22.

Egbert S, Ulbricht L (2024b). In Palantir we trust? Regulation of data analysis platforms in public security. Big Data & Society, Volume 11, Issue (3); 1–15. doi.org/10.1177/20539517241255108 (23.12.2025).

Flyverbom M (2024). Theorizing data analysis platforms – digital refractions andreconfigurations of pasts, presents and futures. Information, Kommunikation und Gesellschaft 2024, Bd. 27, Nr. 13; 2366–2380.

Frigelj K (2025). „Kommissar Palantir“ – Erfolgreich beim Aufspüren von Kriminellen, aber hochumstritten. welt.de/politik/deutschland/article256020844/Verbrechensbekaempfung-Kommissar-Palantir-Erfolgreich-beim-Aufspueren-von-Kriminellen-aber-hochumstritten.html (14.08.2025).

GFF – Gesellschaft für Freiheitsrechte o. A. (2024). Stellungnahme der Gesellschaft für Freiheitsrechte e. V. (GFF) zur Einführung der „Bundes-VeRA“ im Rahmen der Anhörung im Innenausschuss am 22.04.2024. Drucksache 20/9495, Berlin. freiheitsrechte.org/uploads/publications/Digital/2024-04-17-Stellungnahme-der-GFF-BundesVeRA.pdf (21.10.2025).

GFF – Gesellschaft für Freiheitsrechte o. A. (2025). Blackbox Palantir: GFF erhebt Verfassungsbeschwerde gegen massenhafte Datenauswertung durch Polizei in Bayern. freiheitsrechte.org/ueber-die-gff/presse/pressemitteilungen-der-gesellschaft-fur-freiheitsrechte/blackbox-palantir-gff-erhebt-verfassungsbeschwerde-gegen-massenhafte-datenauswertung-durch-polizei-in-bayern (24.07.2025).

Greenberg A (2013). How A ‚Deviant‘ Philosopher Built Palantir, A CIA-Funded Data-Mining Juggernaut. forbes.com/sites/andygreenberg/2013/08/14/agent-of-intelligence-how-a-deviant-philosopher-built-palantir-a-cia-funded-data-mining-juggernaut/?ctpv=searchpage (13.08.2025).

Harmon A (2025). SWOT-Analysis. Salem Press Encyclopedia. research-ebsco-com.ezproxy.hwr-berlin.de/c/3x7h43/viewer/html/oyht5mdooj (15.08.2025).

Heidemann K (2025). Palantir in deutschen Sicherheitsbehörden – Legitimes Hilfsmittel zur Gefahrenabwehr oder selbst Gefahr? Junge Wissenschaft im öffentlichen Recht, unter der Lizenz CC BY-SA 4.0 lizenziert, JuWissBlog Nr. 69/2025 v. 31.07.2025. juwiss.de/69-2025/ (31.07.2025).

Jahn T (2025). Palantirs Kampf gegen die deutschen Vorbehalte: Der Auftrag in Baden-Württemberg täuscht: Politischer Druck und Warnungen von Datenschützern bereiten Palantir Probleme. Dabei ist seine Software laut Experten konkurrenzlos – bislang. handelsblatt.com/technik/forschung-innovation/datensicherheit-palantirs-kampf-gegen-die-deutschen-vorbehalte/100148185.html (25.08.2025).

Joswig G (2025). Peter Thiel is watching you – Der Bundesrat fordert den Einsatz der Überwachungssoftware Palantir des US-Techoligarchen und Antidemokraten Peter Thiel. Kritiker sind empört. taz.de/Palantir-in-Deutschland/!6078828/ (14.08.25) Anm.: Exemplarisch nur eine von vielen kritischen Stimmen; auch zur Aussage Thiels, den Glauben an die Kompatibilität von Frieden und Demokratie verloren zu haben.

Kelber U, Bortnikov V (2023). Digitale Souveränität von Sicherheitsbehörden und Nachrichtendiensten. NJW 2023, Heft 28; 2000–2006.

Kurz C (2025a). Polizeidatenbanken: Keine Palantir-Konkurrenz in Sicht. netzpolitik.org/2025/polizeidatenbanken-keine-palantir-konkurrenz-in-sicht/ (10.08.2025).

Kurz C (2025b). Zwischenlösung Palantir: Experten zerpflücken automatisierte Datenanalyse bei der Polizei Sachsen-Anhalt. netzpolitik.org/2025/zwischenloesung-palantir-experten-zerpfluecken-automatisierte-datenanalyse-bei-der-polizei-sachsen-anhalt/ (14.08.2025).

Kurz C (2025c). Automatisierte Datenanalyse: Palantir-Gesetze missachten Vorgaben aus Karlsruhe. netzpolitik.org/2025/automatisierte-datenanalyse-palantir-gesetze-missachten-vorgaben-aus-karlsruhe/ (22.10.2025).

Landeskriminalamt (LKA) Nordrhein-Westfalen (2020). LKA-NRW: Polizei NRW setzt bei Verbrechensbekämpfung und Gefahrenabwehr zukünftig neue Analysetechniken ein. web.archive.org/web/20210602193521/https://www.presseportal.de/blaulicht/pm/58451/4490593 (27.07.2025).

Landtag Hessen (2019). Zwischenbericht des Untersuchungsausschusses 19/3 zu Drucksache 19/6574 und Abweichender Bericht der Mitglieder der Fraktion der SPD zu dem Zwischenbericht des Untersuchungsausschusses 19/3 und Abweichender Bericht des Mitglieds der Fraktion DIE LINKE zu dem Zwischenbericht des Untersuchungsausschusses 19/3 und Abweichender Bericht des Mitglieds der Fraktion der FDP zu dem Zwischenbericht des Untersuchungsausschusses 19/3. Drucksache 19/6864, Wiesbaden. starweb.hessen.de/cache/DRS/19/4/06864.pdf (13.08.2024).

Landtag Hessen (2022). Beantwortung der kl. Anfrage zur Nutzung hessenDATA durch Behörden und Dienststellen außerhalb der hessischen Polizei. Drucksache 20/8794, Wiesbaden. starweb.hessen.de/cache/DRS/20/4/08794.pdf (09.08.2025).

Landtag Nordrhein-Westfalen (2021). Aktueller Sachstand zur Software Go-tham-Palantir. Vorlage 17/5078. landtag.nrw.de/portal/WWW/dokumentenarchiv/Dokument/MMV17-5078.pdf (14.08.2025).

Labournet o. A. (2025). Big Data bei der Polizei: (Nicht nur) Hessen sucht mit Palantir-Software (nicht nur) nach Gefährdern. labournet.de/interventionen/grundrechte/grundrechte-all/polizeistaat/big-data-bei-der-polizei-hessen-sucht-mit-palantir-software-nach-gefaehrdern/ (13.08.2025) Anm.: Sammlung kritischer Stimmen zur Datenanalyse-Software.

Lüneburg L (2023). Polizeiliche Datenanalysen – eine Gefahr? law-school.de/news-artikel/luca-lueneburg-polizeiliche-datenanalysen-eine-gefahr (22.10.2025).

LTO – Legal Tribune Online o. A. (2025). Dobrindt prüft bundesweiten Palantir-Einsatz – Streit um Analysesoftware. lto.de/recht/nachrichten/n/palantir-einsatz-bundesinnenminister-alexander-dobrindt-prueft-einsatz-analyse-software-palantir-usa (14.08.2025).

Markson C (2025). Palantir der Strategiechef entschluesselt wahre DNA der Erfolgsaktie. Welt-Online. welt.de/podcasts/alles-auf-aktien/article6894a761204e050eae232947/Palantir-der-Strategiechef-entschluesselt-wahre-DNA-der-Erfolgsaktie.html (09.08.2025).

Mersi F, Herzog M, Sokolow A (2025). Diskussion um Palantir: Was soll die Polizei dürfen? rsw.beck.de/aktuell/daily/meldung/detail/palantir-daten-rechtsstaat-polizei-befugnisse (12.08.2025).

Meyer S (2025). Der Einsatz künstlicher Intelligenz durch Sicherheitsbehörden. Zeitschrift für das gesamte Sicherheitsrecht, GSZ 2025, Heft 4; 156–161.

MMinute o. A. (2025) The History of Palantir Technologies: From Visionary Beginnings to a Global Data Powerhouse. markets.financialcontent.com/stocks/article/marketminute-2025-3-21-the-history-of-palantir-technologies-from-visionary-beginnings-to-a-global-data-powerhouse (14.08.2025).

Palantir o. A. (2020a). Form S-1. Registration statement under the securities Act of 1933. sec.gov/Archives/edgar/data/1321655/000119312520230013/d904406ds1.htm (27.07.2025).

Palantir o. A. (2020b). Palantir is Not a Data Company. blog.palantir.com/palantir-is-not-a-data-company-palantir-explained-1-a6fcf8b3e4cb (27.07.2025) Anm.: Zu Verdeutlichung der Selbstdarstellung des Unternehmens.

Palantir o. A. (2024). Palantir Platform Gotham: Service Definition Document. assets.applytosupply.digitalmarketplace.service.gov.uk/g-cloud-14/documents/92736/801146272055049-service-definition-document-2024-11-26-1253.pdf (21.10.2025).

Palantir o. A. (2025). Ontology building. palantir.com/docs/foundry/ontology/overview (15.08.2025).

Roßnagel A (2023). Digitale Souveränität im Datenschutzrecht. Zeitschrift für das Recht der Digitalisierung, Datenwirtschaft und IT (MMR) 2023, Heft 1; 64–68.

Steinlechner M (2025). Besuch bei VeRA: Wie Bayerns Polizei Palantir nutzt. golem.de/news/besuch-bei-vera-wie-bayerns-polizei-palantir-nutzt-2109-159495.html (21.10.2025).

Stöcker C (2025). JD Vance, Peter Thiel und Palantir – Eine äußerst miserable Idee. spiegel.de/wissenschaft/mensch/palantir-software-deutsche-polizei-setzt-auf-umstrittene-us-technologie-kolumne-a-cd743d9a-1a9d-4778-81f7-0ebf478c8ea2 (22.10.2025).

Vasel J (2025). Streit um Palantir-Software: „Eine deutsche oder europäische Lösung ist in weiter Ferne“. rsw.beck.de/aktuell/daily/meldung/detail/interview-palantir-software-peter-thiel-usa-digitale-souveraenitaet (14.08.2025).

Die Polizei zwischen Automatisierung und Humanisierung: Auswirkungen der Künstlichen Intelligenz auf Mitarbeitende und Implikationen für die Organisation

Sebastian Herrmann

Die voranschreitende Digitalisierung und der verstärkte Einsatz von Künstlicher Intelligenz (KI) führen zu fundamentalen Veränderungen in der Arbeitswelt und erfordern eine grundlegende Neubetrachtung der Kompetenzanforderungen für Mitarbeitende und Führungskräfte in verschiedenen Organisationsbereichen (World Economic Forum 2025, S. 5). Auch die öffentlichen Verwaltungen und Polizeien sehen sich mit dieser signifikanten Herausforderung konfrontiert. Nach der Prognose von Schulze Spüntrup et al. (2023, S. 2) fehlen im öffentlichen Sektor bis 2030 etwa 140.000 digitale Fachkräfte. Der technologische Wandel stellt auch Polizeiorganisationen vor die Herausforderung, ihre traditionellen Arbeitsweisen zu überdenken und neue digitale Arbeitsformen zu integrieren (Weiner 2021, S. 22). Sachbearbeitende in der Polizei sehen sich zunehmend mit automatisierten Prozessen, datengestützten Entscheidungshilfen und intelligenten Systemen konfrontiert, die sowohl ihre täglichen Arbeitsabläufe als auch ihre beruflichen Kompetenzanforderungen nachhaltig verändern. Um in diesem dynamischen Umfeld erfolgreich agieren zu können, müssen sich Mitarbeitende der Polizei und auch die Organisation proaktiv auf diese Entwicklungen einstellen und strategische Anpassungen vornehmen (Bitkom e. V. 2023, S. 4). Dies erfordert nicht nur ein fundiertes Verständnis der technologischen Möglichkeiten, sondern auch eine systematische Analyse der sich wandelnden Arbeitsanforderungen und der daraus resultierenden organisationalen Implikationen.

Die zentralen Forschungsfragen lauten daher: Wie wird Künstliche Intelligenz die Arbeit von Sachbearbeitenden in der Polizei verändern, welche Kompetenzanforderungen bringt dies mit sich und was sind die abzuleitenden Implikationen für die Organisation?

Vor diesem Hintergrund werden im vorliegenden Beitrag mittels eines Scoping Reviews relevante Studien zusammengetragen, thematisch strukturiert und analysiert. Ziele sind die Ermittlung von Evidenzlücken, die Identifizierung von Schlüsselkonzepten und praxisorientierte Handlungsempfehlungen für eine erfolgreiche Bewältigung des digitalen Wandels in der Polizei.

Hintergrund

Künstliche Intelligenz verändert Arbeitsprozesse grundlegend und macht ein tiefgehendes Verständnis der damit verbundenen Herausforderungen und Potenziale unverzichtbar. Um die Transformation der Arbeit von Sachbearbeitenden und insbesondere die damit einhergehenden Herausforderungen zu verstehen, sind einige Betrachtungen von besonderer Relevanz. Diese umfassen das Wissen um künftige Arbeitsprozesse und deren Ausgestaltung sowie die Wirkung dieser Veränderungen auf die Mitarbeitenden.

Darüber hinaus ist die Identifizierung spezifischer Herausforderungen, die sich etwa aus der Mensch-Maschine-Interaktion und der Arbeit mit KI ergeben, von entscheidender Bedeutung. Als Beispiele können hier Bias oder KI-Halluzinationen genannt werden. Dies erfordert die Analyse der künftigen Anforderungen im Hinblick auf die Digital- und KI-Kompetenz. Die Nachfrage nach diesen Kompetenzen am Arbeitsmarkt steigt nach Schulze Spüntrup et al. (2023, S. 6) innerhalb der nächsten fünf Jahre um das Dreifache an. Gleichzeitig bemängelt in der Studie von Welling et al. (2023, S. 10) über die Hälfte der Befragten innerhalb der öffentlichen Verwaltung hier ungenügende Fort- und Weiterbildungsangebote. Daher sind entsprechende organisationale Implikationen in Bezug auf die Erhebung und Etablierung dieser spezifischen Kompetenzen zu berücksichtigen. Behörden und auch die Polizeien sind als Betreiber von KI-Systemen nach Art. 4 der KI-Verordnung der EU (2024/1689 zur Festlegung harmonisierter Vorschriften für Künstliche Intelligenz) zur Schaffung von KI-Kompetenzen verpflichtet (Bayer. StMF 2025, S. 8; Piesold & Krause 2025, S. 10).

Im vorgenannten Themenkontext existiert bislang kaum polizeispezifische Forschung. Hier liefern Wiese (2025) und Just (2025) erste Ansätze. Untersuchungen zur Transformation der Arbeit, wie sie etwa von Hubel et al. (2024), Grienberger et al. (2024), Lühr und Kämpf (2025) sowie Seemann (2023) durchgeführt wurden, beziehen sich in der Regel auf den Arbeitsmarkt im Allgemeinen. Der Bereich der Digital-Kompetenzen und zugehörigen Modelle ist ein konsolidiertes Forschungsfeld und wurde, beispielsweise durch Müller et al. (2023), systematisch untersucht. Im Hinblick auf KI-Kompetenzen liegt mit Just (2025) aber auch hier nur eine polizeispezifische Arbeit vor. Besser erforscht ist die öffentliche Verwaltung im Bereich der digitalen Kompetenz etwa durch Bellmer & Becker (2024) sowie Catakli (2024) und in Erweiterung zu KI-Kompetenzen von Piesold & Krause (2025). Es liegen auch einige Untersuchungen zu organisationalen Implikationen im Kontext des öffentlichen Sektors vor, etwa von Kusanke et al. (2023), Welling et al. (2023), Schulze Spüntrup et al. (2023), sowie ein Leitfaden des Bayerischen Staatsministeriums der Finanzen und für Heimat (2025). In den Studien werden bereits einige konkrete Empfehlungen dargelegt, wobei Wiese (2024) und Kusanke et al. (2023) insbesondere auf den Bereich der Führung fokussieren.

Material und Methodik

Dieses Scoping Review folgt dem methodologischen Framework von Arksey & O'Malley (2005), die einen systematischen Ansatz zur Erfassung und Analyse der verfügbaren Literatur zu einem spezifischen Thema bietet. Das Scoping Review eignet sich für die Untersuchung komplexer und sich schnell entwickelnder Forschungsfelder (ebd., S. 21) und ist daher ein passendes Instrument zur Erreichung der formulierten Ziele.

Suchstrategie

Im Rahmen der Suche sollte relevante Literatur unabhängig vom jeweiligen Studiendesign recherchiert werden. Das iterative Vorgehen erfolgte zunächst durch eine explorative Recherche ohne strenge Einschränkungen (Arksey & O'Malley 2005, S. 22). Hierbei wurden erste Informationen zur Themenforschung und deren Umfang gesammelt und relevante Schlüs-

selwörter identifiziert (ebd.). Anhand dieser erfolgte dann eine umfangreiche, spezifische Literatursuche. Schließlich wurde in einem letzten Schritt die Exploration anhand der den relevanten Arbeiten zugrunde liegenden Literaturverzeichnisse durchgeführt (ebd., S. 24).

Material

Die Studienauswahl erfolgte anhand erarbeiteter Ein- bzw. Ausschlusskriterien, welche sich am formulierten Untersuchungsziel, der Aktualität der Publikationen (2023–2025) sowie dem spezifischen Kontext der Studien orientierten (Arksey & O'Malley 2005, S. 25). Durch die Datenbanksuchen konnten insgesamt 48 Studien identifiziert werden. Weiterhin wurde eine zusätzliche Studie (kurz vor ihrer Veröffentlichung) durch einen Experten zur Verfügung gestellt (ebd., S. 23). Nach dem Screening auf Duplikate verblieben 49 Studien, von welchen 10 ausgeschlossen und die restlichen 39 (Volltextartikel) einer Eignungsprüfung unterzogen wurden. Hiervon wurden 25 Arbeiten mit Begründung ausgeschlossen und 14 Studien in den hier vorliegenden Beitrag übernommen.

Datenextraktion und Analyse

Die oben genannten Quellen der Studienauswahl wurden anschließend einer standardisierten Datenextraktion unterzogen. Die Extraktionen wurden anschließend thematisch synthetisiert und jeweils noch einmal mit dem Originalinhalt der zugrunde liegenden Quelle abgeglichen (Arksey & O'Malley 2005, S. 26f.). Nach der Analyse wurden die Ergebnisse im Hinblick auf das formulierte Untersuchungsziel im vorliegenden Scoping Review zusammengeführt.

Qualitätssicherung

Die Qualität des vorliegenden Scoping Reviews ist durch die Einhaltung methodischer Qualitätskriterien und der Erfüllung der ursprünglichen Zielsetzungen gewährleistet. Die Transparenz ist durch das Vorgehen anhand des erstellten Protokolls gegeben. Dieses dokumentiert Zwischenergebnisse, Datenextraktionen, Ausschlüsse und Abweichungen klar und begründet. Die systematische Suchstrategie ist durch die vorgenannte dreistufige Exploration (eingeschränkte Suche in relevanten Datenbanken, vollständige Suche mit allen identifizierten Begriffen sowie zugrunde liegender Literaturverzeichnisse) definiert.

Weiterhin werden die Dokumentation, die Benennung von Limitationen sowie die Darstellung der Zielerreichung mit Relevanz für Praxis und Forschung gewährleistet und Schlüsselkonzepte sowie Forschungslücken identifiziert.

Ergebnisse

Veränderung der Sacharbeit

Im Hinblick auf die Forschungsfragen sollen zunächst die Erkenntnisse zur Veränderung der Sacharbeit durch den Einsatz von KI dargestellt werden. Hier konnten einige Herausforderungen für Mitarbeitende und die Organisation identifiziert werden. So ist nach Lühr und Kämpf (2025, S. 52) von einem Wandel von Arbeitsinhalten sowie hinsichtlich der Organisationsfor-

men von Arbeit auszugehen. Exemplarisch sei die Automatisierung repetitiver Tätigkeiten genannt, die eine kritische Hinterfragung und Analyse der Ergebnisse durch Mitarbeitende erfordert (ebd., S. 55). Seemann (2023, S. 62) erwartet für den Bereich der Verwaltung ein Transformationsszenario. Jedoch wird insbesondere für die Textarbeit durch Large Language Models statt einer Erweiterung der menschlichen Arbeitsleistung eher deren Substitution gesehen (ebd., S. 56). Auch Grienberger et al. (2024, S. 4) sehen ein gesteigertes Substituierbarkeitspotenzial in Berufen mit sprachlichem bzw. schriftlichem Schwerpunkt. Jedoch konstatieren die Autoren für keinen Beruf eine vollständige Substituierbarkeit und erwarten eine sowohl schrittweise als auch zeitverzögerte Potenzialausschöpfung (ebd., S. 5–7).

Für Mitarbeitende rechnen Hubel et al. (2025, S. 39) mit einer Arbeitsverdichtung und einhergehendem Stress und psychischer Belastung. Weiterhin identifizieren Lühr und Kämpf (2025, S. 83) die Angst vor dem Arbeitsplatzverlust als ein entscheidendes Hindernis für die erfolgreiche Implementierung von KI. Diese mentalen Belastungsfaktoren stützt auch Wiese (2024, S. 72 f.) und sieht hier Risiken wie Abhängigkeitsgefühl, Kompetenzverlust oder den Rückgang persönlicher Kontakte. Vorgenannte Entwicklungsperspektiven bieten jedoch auch Chancen. Vor allem im Bereich der Sachbearbeitung erwarten Lühr und Kämpf (2025, S. 52) vielfältige Veränderungen der Tätigkeitsinhalte, Funktionsverschiebungen, aber auch -verluste. Dennoch bieten hier Zuwächse von Tätigkeitsfeldern Potenziale für eine Aufwertung und Requalifizierung. Auch das Bayerische Staatsministeriums der Finanzen und für Heimat (2025, S. 16) verweist auf notwendigen Transfer des Mitarbeiterwissens für die Leistungsfähigkeit von KI-Systemen. Hubel et al. (2024, S. 38) erwarten durch den Einsatz von KI Effizienssteigerungen und eine flexiblere Arbeitszeitgestaltung durch automatisierte Prozesse.

Für die Führungsarbeit erwartet Wiese (2024, S. 43 f.) mehr Effizienz und Entlastung durch die Automatisierung von administrativen Aufgaben, Controlling sowie in der Kommunikation und im Wissensmanagement. Künstliche Intelligenz findet zunehmend Eingang in den Arbeitsalltag. Seemann (2023, S. 76) kommt zum Ergebnis, dass bis zum Zeitpunkt offizieller Firmenimplementierungen KI heimlich und unbemerkt durch Mitarbeitende eingesetzt werden wird. Dies erwartet auch das Bayerische Staatsministerium der Finanzen und für Heimat (2025, S. 14) und rät daher zur Förderung und Freigabe geprüfter KI-Systeme im Dienstbetrieb. Seemann (2023, S. 54 f.) hält fest, dass sich unter anderem aufgrund mangelnder Studien genaue Prognosen über den kommenden Wandel der Arbeit sehr schwierig gestalten. Hubel et al. (2024, S. 41) sehen hier ein noch offenes Entwicklungsszenario.

Künftige Kompetenzanforderungen

Der zweite Teil der Forschungsfrage beschäftigt sich mit den künftigen Kompetenzanforderungen an Mitarbeitende. Der Begriff der Kompetenzen meint nach Heyse (2007, S. 14) „Dispositionen (persönliche Voraussetzungen) zur Selbstorganisation bei der Bewältigung von insbesondere neuen, nicht routinemäßigen Aufgaben“. Digitale Kompetenzen beinhalten laut Vuorikari et al. (2022, S. 3) sowohl Wissen als auch Fähigkeiten und eigene Einstellungen. Catakli (2024, S. 764) definiert diese als „Selbstorganisationsdispositionen, die zur Problemlösung im digitalen Kontext befähigen“. Für den Bereich der Künstlichen Intelligenz verwenden Piesold & Krause (2025, S. 10 f.) in ihrem Modell die spezifischen Begriffe „KI-Kompetenz“ oder „AI-literacy“. Diese definiert Art. 3 Nr. 56 der KI-Verordnung der EU (2024/1689) als „die Fähigkeiten, die Kenntnisse und das Verständnis, die es Anbietern, Betreibern und

Betroffenen unter Berücksichtigung ihrer jeweiligen Rechte und Pflichten im Rahmen dieser Verordnung ermöglichen, KI-Systeme sachkundig einzusetzen sowie sich der Chancen und Risiken von KI und möglicher Schäden, die sie verursachen kann, bewusst zu werden". Nach Just (2025, S. 42) werden diese als „eine Kombination von Fähigkeiten, Kenntnissen und Verständnis definiert, die es Polizeibeamtinnen und -beamten ermöglichen, KI-Technologien sachkundig, effektiv und verantwortungsvoll einzusetzen".

Insgesamt weisen Bellmer & Becker (2024, S. 198, Tab. 5), basierend auf dem an EU-Bürger adressierten Digital Competence Framework (DigComp 2.2) nach Vuorikari et al. (2022), fünf Bereiche der digitalen Kompetenz aus. Diese sind die Informations- und Datenkompetenz, Kommunikation und Zusammenarbeit, das Erstellen digitaler Inhalte, Sicherheit sowie Problemlösung. Die breite Analyse von Müller et al. (2023, S. 25) zeigt, dass der Digital Competence Framework ein häufig referenzierter Ansatz ist und viele Kompetenzmodelle hier anknüpfen. Somit kann dieses Modell als Grundlage für die Entwicklung erweiterter und spezifisch angepasster Kompetenzmodelle, etwa im Hinblick auf KI-Kompetenzen, dienen. Catakli (2024, S. 772–774) begrenzt den Begriff der digitalen Kompetenzen auf jene, welche ausschließlich im digitalen Kontext erforderlich sind. Sie erarbeitet einen verwaltungsspezifischen Kompetenzrahmen mit 34 Kompetenzen, welche in die Kategorien der fachlichen, methodischen, sozialen und der personalen digitalen Kompetenzen geclustert werden. Ihr Entwurf stellt eine detaillierte Erweiterung der im vorhergehenden Absatz genannten Bereiche dar.

Aufgrund des zunehmenden Einsatzes von KI-System sehen Piesold & Krause (2025, S. 10 f., Abbildung 5) das Erfordernis einer fortgeschrittenen, digitalen Kompetenz, welche vom Verständnis von Grundbegriffen einer Technologie bis hin zur Fähigkeit, digitale Technologien zu entwickeln oder anzupassen, reicht. Die als „AI-Literacy" beschriebene Fähigkeit des Verstehens, der Nutzung sowie Überwachung und kritischen Reflektion von KI-Anwendungen wird nach Piesold & Krause (2025, S. 11–14) in fünf Dimensionen unterteilt. Diese sind eine technische (Grundverständnis, Erkennen und Grundkenntnisse über den Aufbau von KI-Systemen) und eine Anwendungsdimension (Einordnung, Auswahl und zielgerichteter Einsatz von KI-Systemen). Des Weiteren eine kritische bzw. Bewertungsdimension (fachliche Beurteilung von Outputs hinsichtlich Qualität und Zuverlässigkeit) und eine ethische Dimension (Klärung und Prüfung ethischer Fragen eines KI-Einsatzes). Hinzu kommt die Fähigkeit der kontextspezifischen Bewertung und eigenständigen KI-Software-Entwicklung. Die Autoren (ebd., S. 14 f.) ergänzen dies durch den Vorschlag einer juristischen Dimension hinsichtlich der Grundkenntnisse über rechtliche Fragen des Einsatzes von KI-Programmen. KI-Kompetenzen sind nach Just (2025, S. 46) künftig auch für Mitarbeitende der Polizei als essenziell zu betrachten.

Implikationen für die Organisation

Zunächst sollen hier die identifizierten Herausforderungen abgebildet werden. Die Arbeit von Bellmer & Becker (2024, S. 191) weist auf generelle Defizite von Mitarbeitenden im Bereich der untersuchten Kompetenzen hin. Auch bei Mitarbeitenden der Polizei fehlt es nach Just (2025, S. 48) hier noch an Grundlagen. Als eine mögliche Ursache ist nach Catakli (2024, S. 781–785) derzeit ein Mangel an Studieninhalten zu digitalen Kompetenzen an den Verwaltungshochschulen zu sehen. Zudem fehlt es nach Ansicht von Catakli (ebd.) an strategischen Vorgaben und dem Bewusstsein um nötige, digitale Kompetenzen sowie deren Stellenwert.

Bei den Mitarbeitenden selbst identifizieren Bellmer & Becker (2024, S. 199) in ihrer Studie hierbei sowohl Zeitmangel als auch eine Konkurrenz zwischen Fortbildungszeiten und Regelaufgaben als Herausforderungen.

Die Studien bieten aber auch eine Reihe von Lösungsansätzen, um den vorgenannten Herausforderungen zu begegnen. Diese liegen im Schwerpunkt in allgemeinen und individuellen Bildungsangeboten sowie in Austauschformaten und der Personalentwicklung. Im Bereich der Ausbildung schlagen Welling et al. (2023, S. 73–75) für das Verwaltungsstudium eine Integration digitaler Kompetenzen in den Pflichtfächern sowie in Prüfungen vor. Just (2025, S. 48) sieht einen konkreten Ansatz für das Polizeistudium in der Kombination aus Theorie und praktischem Üben mit Anwendungen. Auch Kusanke et al. (2023, S. 216) schlagen im Hinblick auf verwaltungswissenschaftliche Aus- und Hochschulbildung statt eines juristischen Fokus eine interdisziplinarische Orientierung vor.

Die inhaltliche Ausrichtung auf entsprechende Kompetenzen im Bereich der Weiterbildung ist ein zentraler Vorschlag von Schulze Spüntrup et al. (2023, S. 9). Hier schlagen Bellmer & Becker (2024, S. 199) kostenfreie externe Fortbildungen innerhalb der Arbeitszeit sowie E-Learnings und Onlineangebote vor. Kusanke et al. (2023, S. 215 f.) erachten den Praxisbezug der vorgenannten Angebote und deren Transfer zum Arbeitsalltag als wesentlich. Auch Seemann (2023, S. 77) hält sowohl Aufklärungsarbeit als auch Unterstützung im Umgang mit KI für notwendig. Zudem sieht das Bayerische Staatsministeriums der Finanzen und für Heimat (2025, S. 11) neben den Angeboten zur Schaffung eines allgemeinen Kompetenzniveaus die Notwendigkeit zur individuellen Schulung am jeweils konkret eingesetzten KI-System.

Hubel et al. (2024, S. 42) empfehlen, KI-Kompetenzen sowohl in der Spitze als auch in der Breite zu stärken. Gemeint sind neben Weiterbildungen auch strategische Personalentwicklung und ein frühzeitiges Monitoring möglicher negativer Effekte. Grundlage für Weiterbildungsmaßnahmen können nach Welling et al. (2023, S. 96) regelmäßige Gespräche zur Ermittlung des individuellen Bedarfs sowie sich aus der Rollen- und Stellenbeschreibung ergebende Erfordernisse sein. Letzteren Ansatz greift auch Catakli (2024, S. 785) auf und erweitert diesen im Rahmen eines maßgeschneiderten Kompetenzmanagements um einen Lösungsansatz mittels einer dreistufigen Kompetenzerfassung. Dieser besteht aus der Bestimmung der im Einzelnen erforderlichen Kompetenzen, deren Messung und Bilanzierung (sowohl für Personen als auch für Organisationen).

Für den Bereich der KI-Kompetenz verfolgen dies auch Piesold & Krause (2025, S. 14 f.) und schlagen zudem regelmäßige Schulungen für Mitarbeitende sowie behördeninterne und internationale Best-Practice-Betrachtungen für diesen spezifischen Bereich sowie Leitfäden für den KI-Einsatz vor. Just (2025, S. 52) schlägt einen praxisnahen Ansatz vor, bei dem tatsächlich im Alltag benötigte KI-Kompetenzen per Mitarbeitendenbefragung erhoben und anschließend in Bildungsangebote transferiert und vermittelt werden könnten. Auch Lühr und Kämpf (2025, S. 83) unterstreichen die Mitwirkung und Beteiligung der Beschäftigten bei der Implementierung von KI. Im Bereich der öffentlichen Verwaltung verweist das Bayerische Staatsministeriums der Finanzen und für Heimat (2025, S. 10) auf Mitbestimmungs- und Mitwirkungsrechte der Personalvertretung.

Nach Schulze Spüntrup et al. (2023, S. 8) stehen Führungskräfte zur Gestaltung des Wandels im Fokus. Diese müssen daher weitergebildet werden und im Austausch mit digitalen Führungskräften der Wirtschaft stehen. Wiese (2024, S. 74) sieht im Hinblick auf die Künstliche Intelligenz vor allem die Notwendigkeit der Offenheit für Innovationen und mehr technisches Verständnis bei Führungskräften. Auch Welling et al. (2023, S. 93–95) schlagen organisationsübergreifende Netzwerke und Austauschforen für Führungs- und Fachkräfte vor und betonen die Einbindung von Führungskräften bei der Kommunikation von Veränderungen. Im Bereich der Führung verweisen Kusanke et al. (2023, S. 216) ebenfalls auf Austauschformate und Formen kollegialer Beratung. Sie sehen jedoch auch einen Weg des Kompetenzaufbaus durch die Gewinnung externer Fachkräfte. Das Bayerische Staatsministerium der Finanzen und für Heimat (2025, S. 15) rät zu konkreten Definitionen für Use Cases und Grenzen der Nutzung im Arbeitsalltag.

Diskussion

Bis auf die Arbeiten von Wiese (2024) und Just (2025) konnte keine polizeispezifische Forschung gefunden werden. Es stellt sich daher die Frage, inwieweit die Ergebnisse der Studien auf die Polizei übertragen werden können. Mangels ausreichend polizeispezifischer Literatur im gewählten Themenkontext wurde der Fokus auf Untersuchungen in der öffentlichen Verwaltung in Deutschland gelegt. Die Verwaltungswissenschaft ist eine Disziplin der Polizeiwissenschaften (H.-J. Lange 2003, S. 445; Feltes 2008, S. 965 f.), und ob der Ähnlichkeiten zwischen Polizei und Verwaltung bestehen nach Schröter et al. (2023, S. 1635) Möglichkeiten des wechselseitigen Lernens dieser Bereiche des öffentlichen Dienstes. Parallelen sind insbesondere im Bereich der Sachbearbeitung oder internen Ablauforganisation zu finden. Nach Tombeil et al. (2020, S. 140) „ist Sachbearbeitung immer eine Dienstleistung, also eine immaterielle Leistung, die auf eine Zustandsveränderung von Personen, Objekten, Prozessen oder Informationen gerichtet ist“. Der Begriff umfasst Vorgänge, die mit geringen Interaktions- und Kognitionsanforderungen einhergehen, regelmäßig charakterisiert durch einen hohen Anteil an Routineprozessen. Sie sind durch strukturierte, standardisierte, wiederkehrende und regelbasierte Abläufe gekennzeichnet. Belegt wird dies durch die Arbeiten von Behrens et al. (2021, S. 69), Tombeil et al. (2020, S. 149) sowie Dukino et al. (2020, S. 11). Derlei Aufgaben existieren in der polizeilichen Praxis in vielfältiger Weise. Diese finden sich sowohl im Kontext der Verarbeitung von Daten im Rahmen der Strafverfolgung oder Gefahrenabwehr als auch bei administrativen Tätigkeiten.

Insofern dürfte davon ausgegangen werden, dass Forschung zur öffentlichen Verwaltung und auch zu Tätigkeiten der Sachbearbeitung mindestens in Teilen auf den polizeilichen Kontext übertragbar sind. Dieser Beitrag liefert demnach erste Erkenntnisse für diesen spezifischen Bereich der polizeilichen Arbeit. Darüber hinaus erfordern insgesamt jedoch viele Schwerpunkte der polizeilichen Praxis zwischenmenschliche Kompetenzen (Weiner 2021, S. 23). Gerade im Spektrum sozialer Interaktion ist der Mensch nicht durch Technologie oder Künstliche Intelligenz zu ersetzen (Wiese 2024, S. 75). Das Bayerische Staatsministerium der Finanzen und für Heimat (2025, S. 16) betont auch den Wissenstransfer von Beschäftigten für die Leistungsfähigkeit von KI-Systemen. Dies stützt die Annahme, dass für Sachbearbeitende in der Polizei eher ein Szenario nach Lühr und Kämpf (2025, S. 52) in Form inhaltlicher Tätigkeitsveränderungen, Funktionsverschiebungen und -verlusten zu erwarten ist,

auch einhergehend mit Zuwächsen von Tätigkeitsfeldern und Potenzialen für eine Aufwertung und Requalifizierung (ebd.). Jedoch dürfte im Ergebnis für die Sachbearbeitenden der Polizeien zumindest nicht von einer vollständigen Substituierbarkeit auszugehen sein. Dies liefert eine Antwort auf den ersten Teil der Forschungsfrage.

Die vorliegenden Studien belegen, dass ein grundlegender Rahmen an digitalen und darüber hinaus KI-spezifischen Kompetenzen als unabdingbar erachtet werden muss. In Abhängigkeit von den eingesetzten digitalen Lösungen sowie der spezifischen Tätigkeit oder Rolle können darüber hinaus weitere Kompetenzen im Bereich der Künstlichen Intelligenz oder zusätzliche digitale Kompetenzen erforderlich sein. Hinsichtlich der abzuleitenden Implikationen für die Organisation ergeben sich durch die skizzierten Herausforderungen und die KI-Verordnung der EU auch für die Polizei Handlungserfordernisse. Just (2025, S. 51) schlägt für diese eine Förderung und Verankerung von KI-Kompetenzen im Polizeistudium vor. Dessen Studie ist jedoch auf den Kontext des Landes Baden-Württemberg bezogen und exkludiert den Bereich der Fortbildung. Daher dürften neben diesem Vorschlag auch die Schwerpunktvorschläge zu weiteren Bildungsangeboten, Austauschformaten und Personalentwicklung der anderen Studien übertragbar sein. Dies zeigen auch Welling et al. (2023, S. 42), welche auf eine Übertragbarkeit ihrer generischen Empfehlungen auf andere Berufsfelder des öffentlichen Sektors verweisen.

Die Limitationen des vorliegenden Beitrags ergeben sich aus den verwendeten Suchbegriffen und genutzten Datenbanken sowie dem sehr eingeschränkten Suchzeitraum. Aufgrund dieser Parameter könnten weitere relevante Arbeiten nicht gefunden worden sein. Zudem basieren die verfügbaren Datenquellen überwiegend auf qualitativen Studien mit begrenzter Stichprobengröße. Es fehlen kritische Qualitätsbewertungen, was auch die nachgenannten Empfehlungen für die Praxis begrenzt (Arksey & O'Malley 2005, S. 30). Zuletzt ist auch das Forschungsfeld sehr dynamisch, sodass die Erkenntnisse schnell an Aktualität verlieren können.

Schlussfolgerungen

Die digitale Transformation der Sachbearbeitung durch Künstliche Intelligenz stellt einen tiefgreifenden Wandel dar, der sowohl Chancen als auch Risiken für Beschäftigte, Arbeitsgestaltung und organisatorische Strukturen mit sich bringt. Identifizierte Schlüsselkonzepte für die Gestaltung finden sich vor allem im Bereich der Bildungsangebote, Austauschformate und der Personalentwicklung. Der KI-Leitfaden des Bayerischen Staatsministeriums der Finanzen und für Heimat (2025) oder E-Learning-Angebote (z. B. Digital.Campus Bayern) zeigen, dass bereits erste praktische Implikationen im Themenkontext durch Organisationen des öffentlichen Dienstes umgesetzt werden. Auch im Bereich der Polizei finden sich heterogene KI-spezifische Bildungsangebote, beispielsweise in der Ausbildung zur 2. QE in Bayern, sowie Studieninhalte zur KI im Polizeistudium Baden-Württemberg (Just 2025, S. 51) und an der Deutschen Hochschule der Polizei. Dies sind jedoch nur erste, einzelne Schritte auf dem Weg zur Qualifizierung der Mitarbeitenden im Zuge Künstlicher Intelligenz.

Praktische Implikation der Studien ist daher vor allem eine breite, systematische Qualifizierungsstrategie. Als praxisorientierte Handlungsempfehlung für die Polizei kann abgleitet werden, entsprechende Bildungsinhalte, insbesondere im Bereich der KI, in Fortbildung,

in der Ausbildung sowie an den Hochschulen und der Deutschen Hochschule der Polizei zu verankern und auch entsprechend zu gewichten. Weiterhin sind Personalentwicklungskonzepte erforderlich, um Bildungsangebote individuell anhand der Erfordernisse konkreter Tätigkeiten gestalten zu können. Zudem sind wichtige organisationale Vorschläge die Installation von Austauschformaten, zentralen Ansprechpartnern oder -stellen etwa mit Q&A-Tools oder Angeboten zum Prompt Engineering (Bayer. StMFH 2025, S. 32). Der vorliegende Beitrag identifiziert eine Forschungslücke für polizeispezifische Untersuchungen im Themenkontext. Notwendig scheint hier beispielsweise weitere Forschung zur Entwicklung und Evaluation von Qualifizierungskonzepten oder Untersuchungen zur Transformation und zum Changemanagement, etwa durch qualitative Forschung unter Einbeziehung von Expertinnen und Experten.

Literaturverzeichnis

Arksey, H. & O'Malley, L. (2005). Scoping studies: towards a methodological framework, International Journal of Social Research Methodology, Vol.8; p. 19–32.

Bayerisches Staatsministerium der Finanzen und für Heimat (2025). KÜNSTLICHE INTELLIGENZ: Einsatz von Künstlicher Intelligenz in der Staatsverwaltung, Leitfaden für Behörden, 04/2025, (2. überarbeitete Auflage). stmfh.bayern.de/digitalisierung/ki/KI-Leitfaden_Behoerden_2025.pdf (14.10.2025).

Behrens, J. H., Heindl, A., Winter, J., Biam, D. & Fecht, D. (2021). Sachbearbeitung und Künstliche Intelligenz: Forschungsstand, Einsatzbereiche und Handlungsfelder. Automatisierung und Unterstützung in der Sachbearbeitung mit Künstlicher Intelligenz, Band 4. Stuttgart: Fraunhofer Verlag.

Bellmer, A. & Becker, T. (2024). Digitale Kompetenzen in der öffentlichen Verwaltung: Ein Überblick über Anforderungen an Mitarbeitende und bestehende Maßnahmen. In: Wimmer, M., Räckers, M., & Hünemohr, H. (Hrsg.), Fachtagung Rechts- und Verwaltungsinformatik (RVI 2024), Lecture Notes in Informatics (LNI). Bonn: Gesellschaft für Informatik. dl.gi.de/server/api/core/bitstreams/e8533230-e604-472b-a8b5-72e7b4d9f359/content#page=190 (14.10.2025).

Bitkom e. V. (2023). Projektgruppe Zukunft der Polizei, Aktuelle Herausforderung der Polizeibehörden und deren Implikationen. bitkom.org/sites/main/files/2023-02/230220-Herausforderung-der-Polizei-Positionspapier.pdf (25.10.25).

Catakli, D. (2024). Digitale Kompetenzen. In: Seckelmann, M. (Hrsg.), Digitalisierte Verwaltung Vernetztes E-Government, (3., völlig neu bearbeitete und erweiterte Auflage, S. 763–786). Berlin: Erich Schmidt Verlag.

Dukino, C., Kötter, F., Müller, T., Renner, T. & Zaiser, H. (2020). Künstliche Intelligenz anwenden – Einsatzmöglichkeiten und Methoden. Automatisierung und Unterstützung in der Sachbearbeitung mit Künstlicher Intelligenz, Band 2. Stuttgart: Fraunhofer Verlag.

Feltes, T. (2008). Polizeiwissenschaft in Deutschland – Profil einer Wissenschaftsdisziplin. In: Strafrecht zwischen System und Telos, S. 965–986. Tübingen: Mohr Siebeck.

Grienberger, K., Matthes, B. & Paulus, W. (2024). Folgen des technologischen Wandels für den Arbeitsmarkt: Vor allem Hochqualifizierte bekommen die Digitalisierung verstärkt zu spüren. IAB-Kurzbericht, 05/2024, Nürnberg.

Heyse, V. (2007). Strategien – Kompetenzanforderungen – Potenzialanalysen. In: Heyse V., Erpenbeck J. (Hrsg.), Kompetenzmanagement: Methoden, Vorgehen, KODE® und KODE®X im Praxistest (1. Auflage, S. 11–179). Münster: Waxmann.

Hubel, N., Peters, R., Hille, M. & Goluchowicz, K. (2024). Generative KI -Technologieszenarien und Auswirkungen auf Arbeit bis 2030. Bundesministerium für Arbeit und Soziales, 03/2025. denkfabrik-bmas.de/fileadmin/Downloads/Publikationen/Generative_KI_Technologieszenarien_und_Auswirkungen_auf_Arbeit_bis_2030.pdf (14.10.2025).

Just, C. (2025). KI-Kompetenzen für Polizeibeamtinnen und -beamte: Die Zukunft der Polizeiausbildung in Baden-Württemberg. In: Honekamp, W. (Hrsg.), Künstliche Intelligenz in der Polizeiarbeit – Schriftenreihe der DHPol, Band 25, S. 37–55. Münster: DHPol.

Kusanke, K., Kendziorra, J., Winkler, T. J. & Pilgenröder, S. (2023). Maßnahmen für den Aufbau von Digital Leadership Kompetenzen für Führungskräfte im öffentlichen Sektor. HMDPraxis der Wirtschaftsinformatik, Band 61, Heft 1, 02/2024, S. 202–219. Wiesbaden: Springer Vieweg.

Lange, H.-J. (2003). Polizeiforschung, Polizeiwissenschaft oder Forschung zur Inneren Sicherheit? − Über die Etablierung eines schwierigen Gegenstandes als Wissenschaftsdisziplin. In: Lange, H.-J. (Hrsg.): Die Polizei der Gesellschaft: Zur Soziologie der Inneren Sicherheit, Bd. 4, S. 427–453. Wiesbaden: Springer Fachmedien.

Lühr, T. & Kämpf, T. (2025). Bots im Büro: Künstliche Intelligenz und der Wandel von Angestelltenarbeit in der digitalen Transformation, Study, Band 494, 02/2025, Düsseldorf: Hans-Böckler-Stiftung. boeckler.de/de/faust-detail.htm?sync_id=HBS-009053 (14.10.2025).

Müller, M. L., Frenz, M. & Nitsch, V. (2023). Digitale Kompetenz, Digital Literacy, Digital Competence – Eine vergleichende, strukturierte Literaturanalyse deutsch- und englischsprachiger Beiträge. In: Kristina Kögler, K., Kremer, H.-H., & Herkner, V. (Hrsg.): Jahrbuch der berufs- und wirtschaftspädagogischen Forschung 2023, S. 9–38. Berlin: Budrich.

Piesold, R.-R. & Krause, T. (2025). Anforderungen an die KI-Kompetenz von Beschäftigten der öffentlichen Verwaltung im Kontext des EU AI Acts. In: Honekamp, W., Kemme, S. & Struck, J. (Hrsg.): Auswirkungen von Künstlicher Intelligenz auf die zukünftige Polizeiarbeit: Technologische Potenziale, rechtliche Rahmenbedingungen, kriminologisch-sozialwissenschaftliche Erkenntnisse, S. 99−117. Wiesbaden: Springer Gabler.

Schröter, E., Quick, K., Ongaro, E. & Hartley, J. (2023). Insights into public management from policing: Introduction to the special issue of public management review. Public Management Review, Vol. 25, No. 9, p. 1633–1639.

Schulze Spüntrup, F., Braun, F. & Sönmez, N. A. (2023). Action, bitte! Wie der öffentliche Sektor den Mangel an digitalen Fachkräften meistern kann. Mc Kinsey & Company, 01/2023. https://www.mckinsey.de/~/media/mckinsey/locations/europe%20and%20middle%20east/deutschland/publikationen/2023-01-25%20it%20talent%20im%20public%20sector/action%20bittemckinsey.pdf (14.10.2025).

Seemann, M. (2023). Künstliche Intelligenz, Large Language Models, ChatGPT und die Arbeitswelt der Zukunft. WORKING PAPER FORSCHUNGSFÖRDERUNG, Nummer 304, September 2023. Düsseldorf: Hans Böckler Stiftung. boeckler.de/de/faust-detail.htm?sync_id=HBS-008697 (14.10.2025).

Tombeil, A. S., Kremer, D., Neuhüttler, J., Dukino, C. & Ganz, W. (2020). Potenziale von Künstlicher Intelligenz in der Dienstleistungsarbeit. In: Bruhn, M. & Hadwich, K. (Hrsg.), Automatisierung und Personalisierung von Dienstleistungen. Forum Dienstleistungsmanagement, 2020, S. 135–154. Wiesbaden: Springer Gabler.

Vuorikari, R., Kluzer, S. & Punie, Y. (2022). DigComp 2.2: The Digital Competence Framework for Citizens. With new examples of knowledge, skills and attitudes. Luxemburg: Publications Office of the European Union.

Weiner, A. (2021). Die (digitale) Zukunft im Blick. Proll, U. (Hrsg.): Digitale Polizei: Forensik, sicheres und mobiles Arbeiten, Moderne Polizei, 1/2021, S. 22 f., Bonn: Behörden Spiegel-Gruppe. behoerden-spiegel.de/wp-content/uploads/2021/04/Moderne_Polizei_1_2021.pdf (25.10.2025).

Welling, S., Breiter, A., Haß, T., von Blumröder, L., Bühren, K., Mateina, F., Ziekow, J., Schmeling, J., Zouagui, J. & Klessmann, J. (2023). Strategien und Handlungsempfehlungen zur digitalen Qualifizierung in der öffentlichen Verwaltung. In: Schröder, C., Schnurbus, L., Kumar, A., & Lühr, H. (Hrsg.): Qualifica Digitalis: Kompetenzen für die digitalisierte Verwaltung, Band 5, 11/2023. Bremen: Kellner Verlag.

Wiese, A. (2024). Die digitale Chefin: Die KI als Führungskraft in Polizeiorganisationen. (Masterarbeit im Studiengang öffentliche Verwaltung – Polizeimanagement). Münster: DHPol.

World Economic Forum (2025). Future of Jobs Report 2025: weforum.org/publications/the-future-of-jobs-report-2025/digest/ (25.10.2025).

Leaving Experts – Bleibendes Wissen: Eine Untersuchung der Potenziale von KI zur Bewahrung von Wissen im öffentlichen Dienst am Beispiel der Polizei NRW

Robin Strecker

Der demografische Wandel stellt den deutschen Arbeitsmarkt vor erhebliche Herausforderungen. Bis 2036 werden voraussichtlich rund 12,9 Millionen Erwerbstätige allein aufgrund des Erreichens des Renteneintrittsalters aus dem Erwerbsleben ausscheiden (Statistisches Bundesamt 2025). Von dieser Entwicklung ist auch der öffentliche Dienst betroffen, einschließlich der Polizei Nordrhein-Westfalen (NRW). Diese rechnet im Jahr 2025 mit dem Ausscheiden von etwa 1.570 Polizistinnen und Polizisten (Albers et al. 2015, S. 13). Da Organisationen wie die Polizei NRW in hohem Maße wissensbasiert sind (Färber 2021, S. 20) und sich durch Arbeitsteilung und Spezialisierung auszeichnen (Veit 2021, S. 101), geht mit dem Ausscheiden langjähriger Mitarbeiterinnen und Mitarbeiter ein substanzieller Verlust an wichtigem Fachwissen und wertvoller Erfahrung einher (Reisach et al. 2025, S. 13). Dieses Erfahrungswissen ausscheidender Mitarbeiterinnen und Mitarbeiter, auch „Leaving Experts" genannt, ist ein zentrales Teilgebiet des Wissensmanagements (WM), dessen Bedeutung angesichts des demografischen Wandels stark zunimmt (Müller & Link 2023, S. 109–111). Die Notwendigkeit des Wissenserhalts hat sich bei der Wiedereingliederung pensionierter Polizeibeamtinnen und Polizeibeamter als „Senior Experts" zur Einarbeitung junger Mitarbeitender bereits gezeigt (Dahlkamp 2024, S. 30). Angesichts dieser Entwicklungen ist die Frage nach einem erfolgreichen WM von besonderem Interesse.

Gleichzeitig eröffnen aktuelle technologische Fortschritte im Bereich der Künstlichen Intelligenz (KI) neue Handlungsoptionen (Lehner 2025, S. 259). Bereits im Jahr 2018 forderte die Bundesregierung Staat und Verwaltung auf, die Chancen von KI zu nutzen (BMBF 2018, S. 10). Vor dem Hintergrund des drohenden Wissensverlustes bei der Polizei NRW stellt sich die Frage, inwiefern der Einsatz von KI einen Beitrag zur Bewältigung dieser Herausforderung leisten kann. Es erscheint denkbar, dass KI-basierte Ansätze dazu beitragen könnten, wertvolles Erfahrungswissen systematisch zu sichern und über Pensionierungen hinaus verfügbar zu machen. Der Fokus dieses Beitrags liegt daher auf der Untersuchung der Potenziale und Grenzen des Einsatzes KI-gestützter Systeme zur Sicherung und Weitergabe von Erfahrungswissen bei der Polizei NRW vor dem Hintergrund des demografischen Wandels. Zur Beantwortung dieser zentralen Fragestellung wird eine SWOT-Analyse des KI-Einsatzes bei der Polizei NRW durchgeführt.

Hintergrund

In diesem Kapitel wird zunächst die notwendige theoretische Grundlage für die nachfolgende Analyse geschaffen. Dazu werden zentrale Begriffe des WM erläutert, die für das weitere Verständnis essenziell sind. Anschließend wird der Begriff der KI eingeführt.

Daten, Informationen und Wissen

Zunächst ist es erforderlich, den für das WM namensgebenden Begriff Wissen zu erläutern. Das WM beschränkt sich laut Lehner (2025, S. 84) aber nicht nur auf das Wissen, sondern bezieht auch Daten und Informationen mit ein. Diese Begriffe müssen zunächst erläutert und zueinander in Beziehung gesetzt werden. In der wissenschaftlichen Literatur finden sich für die oben genannten Begriffe eine Vielzahl verschiedener Definitionen und Klassifikationsversuche (Lehner 2025, S. 84). Eine ausführliche Diskussion dieser Definitionsvielfalt kann im Rahmen dieses Beitrags nicht geführt werden. Für einen umfassenden Überblick wird daher auf Zins (2007) verwiesen. Für die weitere Betrachtung werden die nachstehenden erläuterten Definitionen zugrunde gelegt. Sie bilden die Basis für die anschließenden Ausführungen und Analysen.

Bei Daten handelt es sich zunächst lediglich um eine Verkettung von Zeichen bzw. Zeichenfolgen nach einer bestimmten Syntax. Eine Interpretation ist auf dieser Ebene noch nicht erfolgt (North 2021, S. 36). Nach Lehner (2025, S. 85) können Daten somit als Rohmaterial betrachtet werden. Wenn Daten in einen Kontext gesetzt werden und dadurch eine Bedeutung erhalten, spricht man von Informationen (North 2021, S. 37; Probst et al. 2012, S. 16–17). Darüber hinaus sind Informationen auf einen Zweck ausgerichtet und dienen der Vorbereitung von Entscheidungen (North 2021, S. 37). Darauf aufbauend handelt es sich bei Wissen laut North (ebd.) um den Prozess der zweckdienlichen Vernetzung von Informationen. Probst et al. (2012, S. 23) definieren Wissen als die Gesamtheit der Kenntnisse und Fähigkeiten, die Individuen zur Lösung von Problemen einsetzen. Probst et al. gehen davon aus, dass Wissen im Gegensatz zu Daten und Informationen immer an den Menschen gebunden ist (ebd.). Lehner (2025, S. 89) zufolge verliert diese Art des Wissens jedoch zunehmend an Bedeutung und wird inzwischen ergänzt um Wissen, das durch maschinelles Lernen (ML) entstanden ist.

In der Literatur werden darüber hinaus zahlreiche verschiedene Wissensausprägungen unterschieden (Lehner 2025, S. 92). Für das WM ist insbesondere die Unterscheidung zwischen explizitem und implizitem Wissen relevant (ebd., S. 95). Explizites Wissen ist Wissen, das artikulierbar und leicht zu beschreiben ist. Es kann somit auch bewusst gesammelt, gespeichert und abgerufen sowie angewendet werden – auch durch andere Personen (Lanquillon & Schacht 2023, S. 7). Diese Art des Wissens wird unter anderem durch Organisationen gezielt auf Medien gespeichert und dadurch allen Mitarbeiterinnen und Mitarbeitern zugänglich gemacht (North 2021, S. 49). Dem gegenüber steht eine Art des Wissens, das nicht ohne Weiteres artikuliert und erfasst werden kann. Sie umfasst unter anderem die Erfahrungen, Überzeugungen und das Können einer Person und wird deshalb als implizites oder verborgenes Wissen (engl. *tacit knowledge*) bezeichnet (Lehner 2025, S. 95). Laut Lehner (ebd.) hat dieses Wissen entscheidenden Einfluss auf menschliches Verhalten und ist für die meisten Aufgaben unverzichtbar.

Wissensmanagement

Der Ursprung des Begriffs Wissensmanagement (engl. knowledge management), der sich in den 1990er-Jahren zu etablieren begann, ist nicht eindeutig geklärt (Lehner 2025, S. 44). Für den Begriff WM existieren in der Fachliteratur zahlreiche unterschiedliche Definitionen (Lehner 2025, S. 54). In dem vorliegenden Beitrag wird die Definition von Girard und Girard (2015, S. 14) verwendet. Die Autoren analysierten in ihrer Arbeit über 100 Definitionen für

WM aus verschiedenen Fachbereichen. Aufgrund der am häufigsten verwendeten Schlüsselbegriffe formulierten sie die folgende Definition: „Knowledge Management is the process of creating, sharing, using and managing the knowledge and information of an organization" (Girard & Girard 2015, S. 14).

Die frühesten Ansätze von WM in den 1950er-Jahren zielten darauf ab, menschliche Entscheidungsträgerinnen und Entscheidungsträger möglichst schnell mit relevantem Wissen zu versorgen, um die Qualität von Entscheidungen zu verbessern (Lehner 2025, S. 44). Bei dieser frühen Art des WM wurde Wissen jedoch mit Daten und Informationen gleichgesetzt. Der Fokus lag somit auf einem rein technokratischen Ansatz. Es sollten möglichst viele Daten und Informationen in Datenbanken gespeichert werden, um sie später abrufen und wiederverwenden zu können (Lenk et al. 2021, S. 60). Dieser Ansatz änderte sich Lenk et al. (2021, S. 61–62) zufolge ab dem Jahr 1995 durch die Veröffentlichung des Buches „The Knowledge-Creating Company" von Nonaka und Takeuchi. Diese unterschieden erstmals, wie in Kapitel „Daten, Informationen und Wissen" dargestellt, zwischen implizitem und explizitem Wissen. Sie verdeutlichten, dass das Grundproblem des WM in der Überführung von implizitem Wissen in explizites Wissen besteht. Dieser Prozess, den sie als Externalisierung bezeichneten, sei der entscheidende Ausgangspunkt für Innovation in einer Organisation, da erst hierdurch das Wissen einzelner Personen der gesamten Organisation verfügbar wird (North 2021, S. 49). Dieser Ansatz rücke damit den Menschen als Wissensträger mehr in den Fokus (Lenk et al. 2021, S. 64).

Laut Lehner (2025, S. 288) sind für die Bewältigung der vielfältigen Aufgaben eines zielgerichteten und systematischen WM sowie für die kontinuierliche Pflege und Weiterentwicklung der organisatorischen Wissensbasis Methoden unverzichtbar. Eine Methode beschreibt eine systematische und zielgerichtete Vorgehensweise zur Lösung von Problemen (ebd.). Im Spektrum der Methoden zur Wissensweitergabe lassen sich nach Müller und Link (2023, S. 113–117) verschiedene Dimensionen unterscheiden: die zeitliche Strukturierung (synchron/asynchron), die Form der Weitergabe (mündlich/schriftlich) sowie der Zeitpunkt der Wissenssicherung (kontinuierlich/kurz vor Ausscheiden). Der vorliegende Beitrag beschränkt sich auf die Betrachtung asynchroner Methoden, da diese eine anhaltende Dokumentation ermöglichen und unabhängig von räumlicher und zeitlicher Präsenz der Beteiligten erfolgen können. Für eine umfassende Systematisierung aller Methoden, einschließlich synchroner Ansätze, wird auf die Darstellung von Müller und Link (ebd.) verwiesen. Beispiele für asynchrone Methoden sind die checklistenbasierte Wissenssicherung oder das Expert Debriefing, bei dem im Rahmen des Offboardings eine moderierte und interviewbasierte Wissenssicherung erfolgt (Müller & Link 2023, S. 116; Lehner 2025, S. 294–295). Müller und Link (2023, S. 110) weisen jedoch darauf hin, dass insbesondere moderierte Formen zeit- und kostenintensiv sind. Methoden wie die oben beschriebenen können auch unabhängig von einer Software existieren und angewendet werden. In der Regel werden sie jedoch unter anderem zur Kostensenkung durch softwaretechnische Hilfsmittel unterstützt, zunehmend auch mittels KI (Lehner 2025, S. 263, 288).

Künstliche Intelligenz

Der Begriff Künstliche Intelligenz (engl. artificial intelligence) wurde erstmals 1956 von dem US-amerikanischen Informatiker John McCarthy auf einer Konferenz am Dartmouth College geprägt (Lehner 2025, S. 258). Die ursprüngliche Motivation bestand darin, Maschinen mit menschlicher Intelligenz auszustatten (Jiang et al. 2022, S. 1). Bis heute existiert keine allge-

meingültige Definition für KI (Sheikh et al. 2023, S. 15). Sheikh et al. (2023, S. 16) verweisen darauf, dass eine eindeutige Begriffsbestimmung auch deshalb schwierig ist, weil diese auf einer Definition für menschliche Intelligenz aufbauen müsste. Jedoch gäbe es bereits bei diesem Begriff keinen Konsens (ebd.). Etscheid et al. (2020, S. 7) verdeutlichen zudem, dass heute unterschiedliche Technologien mit unterschiedlicher Klassifizierungen und Entwicklungsgraden als KI bezeichnet werden und deshalb eine breit angelegte Arbeitsdefinition erforderlich ist. Für den vorliegenden Beitrag wird die von Marvin Minsky vorgeschlagene Definition von KI zugrunde gelegt. Dieser definiert KI als „die Wissenschaft, Maschinen Dinge machen zu lassen, die Intelligenz erfordern würde, wenn dies Menschen tun würden" (Etscheid et al. 2020, S. 8).

Im Bereich der KI kann zwischen den zwei Hauptteilgebieten „Regelbasierte Systeme" und ML unterschieden werden (Sheikh et al. 2023, S. 30–31). Bei regelbasierten Systemen, auch Expertensysteme genannt, wird das Wissen eines menschlichen Experten für ein eng abgegrenztes Fachgebiet in Form von Wenn-Dann-Regeln in ein automatisiertes System übertragen (Grosan & Abraham 2011, S. 149). Das System verwendet diese Regeln, um Schlussfolgerungen zu ziehen und den Nutzer bei Entscheidungen zu unterstützen (Sheikh et al. 2023, S. 4). Maschinelle Lernverfahren basieren darauf, aus großen Datensätzen Muster und Zusammenhänge zu extrahieren, um neues Wissen und Erfahrungen zu generieren, ohne dass sie explizit für die einzelne Aufgabe programmiert wurden (Lehner 2025, S. 260). Bei ML-Algorithmen wird auch von selbstlernenden Algorithmen gesprochen (Sheikh et al. 2023, S. 18). Die Qualität selbstlernender KI-Systeme hängt direkt von der Güte ihrer Trainingsdaten ab. Nach dem Prinzip „Garbage in, garbage out" kann eine KI nur so zuverlässig und leistungsfähig sein, wie es die Daten zulassen, mit denen sie entwickelt und trainiert wurde (OECD 2025, S. 114). Deep Learning (DL) ist ein Teilgebiet des ML, das durch die signifikant gesteigerte Rechenleistung der letzten Jahre ermöglicht wurde. Es zeichnet sich durch die Verwendung von künstlichen neuronalen Netzen aus, die aus sehr vielen Schichten bestehen und daher als „tief" (engl. deep) bezeichnet werden (OECD 2025, S. 19). DL ist notwendig, um komplexe Strukturen in Sprache zu erkennen, und bildet somit die Grundlage für sogenannte Large Language Models (LLM). LLMs sind in der Lage, große Datenmengen zu verarbeiten und neue Inhalte, wie beispielsweise Zusammenfassungen, zu generieren. Sie sind somit für die Extraktion von Wissen aus Texten von besonderer Bedeutung (Lanquillon & Schacht 2023, S. 6).

Laut Lehner (2025, S. 383) sind für das WM insbesondere Expertensysteme (s. o.), Agentensysteme, Text-Mining-Systeme und generative KI relevant. Eine vollständige Erläuterung dieser verschiedenen Systeme kann im Rahmen dieses Beitrags nicht geleistet werden. Eine Betrachtung erfolgt teilweise jedoch im Rahmen der nachfolgenden SWOT-Analyse.

Methodik

Die Zielsetzung dieses Beitrags ist es, die Potenziale und Grenzen des Einsatzes von KI-gestützten Systemen bei der Sicherung und Weitergabe von Wissen innerhalb der Polizei NRW systematisch zu untersuchen. Hierzu bietet sich die Verwendung der SWOT-Analyse an, da diese bei der systematischen Erfassung von relevanten Faktoren hilft und einen ganzheitli-

chen Überblick über eine Situation verschafft (Namugenyi et al. 2019, S. 1146; Wollny & Paul 2014, S. 189). Gleichzeitig reduziert die Methode die Komplexität und hilft dabei, den Fokus auf die wesentlichen Aspekte zu lenken (Wollny & Paul 2014, S. 199).

Die Herkunft des Begriffes SWOT ist unbekannt (Helms & Nixon 2010, S. 216). Die SWOT-Analyse hat ihren Ursprung laut Wollny und Paul (2014, S. 189) in der Betriebswirtschaftslehre und wird häufig zur Strategieentwicklung von Unternehmen zur Schaffung und Erhaltung von Wettbewerbsvorteilen eingesetzt. SWOT ist ein Akronym für die englischen Begriffe „Strengths" (Stärken), „Weaknesses" (Schwächen), „Opportunities" (Chancen) und „Threats" (Risiken) (Helms & Nixon 2010, S. 216). Stärken und Schwächen sind interne Faktoren, die innerhalb der Organisation liegen und von ihr kontrolliert und beeinflusst werden können. Chancen und Risiken sind hingegen externe Faktoren, die außerhalb der Kontrolle einer Organisation liegen (Namugenyi et al. 2019, S. 1146). Durch die paarweise Kombination der vier genannten Faktoren können Strategien abgeleitet werden. Durch die vorhandenen Stärken können Chancen realisiert und Risiken gemindert werden. Durch eine Reduzierung der Schwächen können Chancen genutzt und Risiken minimiert werden (Niederberger & Wassermann 2014, S. 195).

Ergebnisse

Im Folgenden werden die Stärken, Schwächen, Chancen und Risiken zunächst einzeln analysiert und kategorisiert. Die Zusammenführung und kritische Würdigung dieser Ergebnisse erfolgt anschließend im Kapitel „Diskussion".

Stärken (Strength)

Die Polizei NRW verfügt bereits über eigene praktische Erfahrungen in der Implementierung und Anwendung von KI-Systemen. So nutzt das Landeskriminalamt NRW (LKA NRW) im Rahmen eines Auswerteprojekts beispielsweise KI zur teilautomatisierten Analyse von Straftaten aus dem Bereich der Cyberkriminalität (Homborg et al. 2024, S. 240). Darüber hinaus setzt die Polizei NRW seit 2020 die auf der Software „Gotham" des Unternehmens Palantir basierende Software „Datenbankübergreifende Analyse und Recherche" ein (Landesregierung Nordrhein-Westfalen 2022, S. 1). Für die Einführung und den Betrieb dieses Systems wurden bislang rund 39 Millionen Euro investiert, was die Bereitschaft zur Investition in den Bereich KI verdeutlicht (Landesregierung Nordrhein-Westfalen 2022). Zudem entwickelt und testet das Innovation Lab des Landesamtes für Zentrale Polizeiliche Dienste (LZPD NRW) weitere KI-Technologien für polizeiliche Anwendungen (LZPD NRW 2025).

Das Programm „Polizei 20/20" (P20) schafft durch die Etablierung eines einheitlichen Datenhaus-Ökosystems zudem die technische Grundlage für eine effiziente, länderübergreifende Implementierung von IT-Anwendungen (BMI 2024). Die wirtschaftliche Realisierbarkeit wird dabei unter anderem durch einen Polizei-IT-Fonds gewährleistet (BMI 2023). Dadurch bietet P20 sowohl die organisatorische als auch die finanzielle Infrastruktur, um weitere KI-Projekte systematisch in der polizeilichen Praxis umzusetzen. Die öffentliche Verwaltung speichert eine Vielzahl von Daten, die im Rahmen ihrer Aufgabenwahrnehmung erhoben werden müssen (Etscheid et al. 2020, S. 33). Diese können als Trainingsdaten für Systeme der KI genutzt

werden. Den Beschäftigten der Polizei NRW steht seit Anfang 2024 ein digitales Offboarding-Verfahren zur Verfügung. Dieses soll die Wissenssicherung von ausscheidenden Mitarbeitenden gewährleisten (LAFP NRW 2024, S. 1–2). Über das polizeiinterne Lernmanagementsystem ist das Verfahren abrufbar und bietet Zugriff auf verschiedene Methoden des WM sowie entsprechende Dokumentenvorlagen zum Herunterladen (LAFP NRW 2025).

Schwächen (Weaknesses)

Als öffentliche Stelle unterliegt die Polizei NRW der Haushaltsbewirtschaftung. Diese zeichnet sich durch eine langfristige Finanzplanung aus, die in der Regel keinen flexiblen Investitionsspielraum lässt. Dies erschwert die kurzfristige Einführung neuer KI-Systeme (Wiese 2024, S. 45). Zudem stellt laut EUROPOL (2024, S. 14) die Integration von KI in bestehende, oft ältere technologische Infrastrukturen eine Herausforderung für Behörden dar. Das dafür erforderliche Budget für die Aufrüstung sei erheblich. Zusätzlich werde spezifisches Fachwissen für den Betrieb und die kontinuierliche Wartung des Systems benötigt (ebd.). Diese Daueraufgabe ist mit erheblichen Kosten verbunden (Bitkom e. V. 2023, S. 15). Die Polizei NRW unterliegt in ihrer Datenverarbeitungstätigkeit den geltenden datenschutzrechtlichen Bestimmungen, insbesondere dem Bundesdatenschutzgesetz sowie den spezifischen Regelungen des nordrhein-westfälischen Polizeigesetzes. Bei der Verwendung einer neuen Technologie ist zwingend die Durchführung einer Datenschutzfolgenabschätzung erforderlich. Diese stellt in der Praxis eine He-rausforderung dar (Bitkom e. V. 2023, S. 10).

Die Implementierung von KI-Systemen wird innerhalb von Polizeibehörden kritisch gesehen. Diese Zurückhaltung basiert auf der Forderung nach absoluter Zuverlässigkeit und Sicherheit neuer Technologien. Ergänzend wirken die bereits genannten datenschutzrechtlichen Herausforderungen, insbesondere bei der Anonymisierung sensibler Daten, als Akzeptanzbarriere (Haas 2024, S. 80–81). Wie unter Kapitel „Stärken (Strength)“ dargestellt, verfügt die Polizei NRW über umfangreiche Datenmengen. Diese sind jedoch insbesondere im Bereich der Strafverfolgung aufgrund historischer Einschränkungen, wie papierbasierten Systeme, nicht maschinenlesbaren Formaten und inkonsistenten Aufzeichnungen, nur begrenzt für das Training einer KI geeignet (OECD 2025, S. 275). Laut einer repräsentativen Befragung aus dem Jahr 2024 nutzen lediglich 19 % der 60- bis 69-Jährigen (Ruhestandsalter) generative KI. Insbesondere bei dieser Altersgruppe ist somit bei der Einführung von KI-Systemen zum WM ein erhöhter Schulungsbedarf zu erwarten (Reiss et al. 2025, S. 8).

Chancen (Opportunities)

Im Folgenden werden zur Darstellung der Chancen die bereits eingeführten Begriffe Daten, Informationen und Wissen als Grundlage herangezogen. Renz et al. (2024, S. 152) verdeutlichen in ihrer Arbeit, dass KI besonders gut für den Umgang mit Daten geeignet ist. Auch die Verarbeitung von Informationen ist möglich, sofern der erforderliche Bedeutungsrahmen zuvor durch den Menschen festgelegt wurde (ebd., S. 156). KI zeichnet sich dabei insbesondere durch die fehlerfreie Verarbeitung und eine hohe Verarbeitungsgeschwindigkeit aus (ebd., S. 154–156). Text-Mining-Systeme ermöglichen beispielsweise die automatische Analyse großer Datenmengen, wodurch Informationen aus Texten extrahiert, Dokumente klassifiziert, relevante Schlagworte identifiziert und Zusammenfassungen erstellt werden (Lehner 2025, S. 390). Laut Renz et al. (2024, S. 157–158) ist KI derzeit noch nicht in der Lage,

Wissen aus Informationen entstehen zu lassen. KI bietet jedoch die Möglichkeit, vorhandenes (Experten-)Wissen zu externalisieren und es somit einer Organisation auch nach dem Ausscheiden eines Experten verfügbar zu machen (Müller & Link 2023, S. 109). KI-basierte Assistenzsysteme können die Durchführung von Methoden des WM (vgl. Kapitel „Wissensmanagement“) gezielt unterstützen, indem sie die Wissensträgerin oder den Wissensträger beispielsweise strukturiert durch den Prozess des Expert Debriefings führen, geführte Befragungen mittels Checklisten und Leitfragen durchführen und Automatisierungspotenziale, wie das oben genannte Text-Mining, nutzen (Müller & Link 2023, S. 132–140).

Eine weitere Chance bei der Nutzung von KI liegt in der Skalierbarkeit. Durch den Einsatz von KI-Systemen können grundsätzlich alle Mitarbeitenden gleichzeitig von einem implementierten System profitieren und Methoden des WM anwenden. Dadurch wird das Fachwissen erfahrener Prozessbegleiterinnen und -begleiter nicht länger auf einzelne Personen oder kleine Gruppen beschränkt, sondern über die KI zentral bereitgestellt und organisationsweit zugänglich gemacht (Müller & Link 2023, S. 132). Dies würde auch die ressourcenintensive Zusammenarbeit mit Prozessbegleiterinnen und Prozessbegleitern (bspw. im Rahmen eines Expert Debriefing) erheblich reduzieren (Müller & Link 2023, S. 145).

Risiken (Threats)

Obwohl die Polizei NRW bereits über eigene Erfahrungen mit KI verfügt, sind öffentliche Verwaltungen in hohem Maße von externen Anbietern abhängig (OECD 2025, S. 86). Die Kosten für die externe Beschaffung einer KI-Technologie sind jedoch hoch und können stark ansteigen, wenn diese in Organisationen breit implementiert wird und somit vielen Beschäftigten zugänglich wäre (OECD 2025, S. 92). Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (2024, S. 8) weist in einer Stellungnahme für den Bundestag darauf hin, dass durch eine Abhängigkeit von privaten Anbietern die Gefahr eines unbemerkten Zugriffs auf Daten und somit ein Sicherheitsrisiko besteht.

Bei der Nutzung von KI-Systemen, insbesondere LLM, besteht zudem die Gefahr, dass zwar plausibel klingende, aber faktisch inkorrekte oder unlogische Inhalte generiert werden. Dieses Phänomen wird als „Halluzinationen“ bezeichnet (Huang et al. 2025, S. 1). Darüber hinaus birgt der Einsatz generativer KI das Risiko systematischer Fehlentscheidungen und einseitiger Darstellungen. Diese werden unter dem Fachbegriff „Bias“ zusammengefasst. Ein solcher Bias entsteht, da die Modelle auf umfangreichen Trainingsdaten basieren, die menschliche Vorurteile und gesellschaftliche Stereotype widerspiegeln können. Sind diese Datengrundlagen fehlerhaft oder nicht repräsentativ, werden die enthaltenen Verzerrungen von der KI nicht nur übernommen, sondern häufig algorithmisch verstärkt (Lehner 2025, S. 392). Schwächen des eingeführten KI-Systems, wie beispielsweise Bias oder Halluzinationen, können das Vertrauen in die Technologie reduzieren. Dadurch kann es zu einer geringeren Akzeptanz und Integration der Technologie durch die einzelnen Mitarbeitenden kommen (Garrel et al. 2024, S. 758). Somit könnte Erfahrungswissen trotz der Einführung eines KI-Systems verloren gehen.

Diskussion

Die SWOT-Analyse zum Einsatz von KI-gestützten Systemen im WM der Polizei NRW hat zentrale Stärken und Schwächen sowie Chancen und Risiken identifiziert. Die wesentlichen Ergebnisse dieser Analyse sind in Abbildung 1 visualisiert. Im Folgenden werden diese Faktoren miteinander verknüpft, um daraus strategische Implikationen abzuleiten. Die Polizei NRW verfügt bereits über etablierte Strukturen des WM und hat schon Erfahrungen mit KI-Systemen gesammelt. In einem nächsten Schritt könnten diese beiden Bereiche miteinander verknüpft werden. Die Ergebnisse der Analyse legen nahe, dass die bestehenden Methoden des WM durch den Einsatz von KI optimiert werden könnten. So ließen sich beispielsweise schriftliche Unterlagen, wie Checklisten, mittels KI automatisiert befüllen. Darüber hinaus könnten Interviews zur Externalisierung impliziten Wissens ebenfalls durch KI geplant und durchgeführt werden. Eine breite Skalierung auf die gesamte Organisation könnte dadurch erreicht werden.

Der Polizei NRW steht unter anderem aufgrund des Programms P20 eine moderne IT-Infrastruktur zur Verfügung. Es bleibt jedoch fraglich, ob sie auf Basis der bisherigen Erfahrungen im Bereich der KI in der Lage wäre, die oben beschriebene KI-Anwendung eigenständig zu entwickeln. Dies hätte den Vorteil, dass sie nicht von einem externen Anbieter abhängig wäre. Dadurch könnten Sicherheitsrisiken und möglicherweise Kosten reduziert werden. Ob tatsächlich Kosteneinsparungen gegenüber eingekauften Produkten erzielt würden, ist derzeit nicht abschätzbar. Ständige Anpassungsbedarfe könnten langfristig teurer sein als eine externe Vergabe (Bitkom e. V. 2023, S. 15).

Stärken	Schwächen
• Erfahrung mit KI • Infrastruktur durch P20 • Bereitschaft zu Investitionen • WM in der Polizei NRW • Vorhandene Trainingsdaten	• Haushaltsbewirtschaftung • Veraltete Systeme • Datenschutz • Akzeptanzbarrieren • Qualität der Trainingsdaten • Schulungsbedarf
Chancen	**Risiken**
• Schnelle und fehlerfreie Datenverarbeitung • Automatisierung/Unterstützung des WM • Skalierbarkeit • Einsparungen	• Abhängigkeit von externen Anbietern • Sicherheitsrisiken • Hohe Kosten bei Implementierung und bei Betrieb/Wartung • Bias und Halluzinationen • Geringe Akzeptanz und Nutzung

Abbildung 1: Ergebnis der durchgeführten SWOT-Analyse (eigene Darstellung)

Ein effektives Datenmanagement sowie eine systematische Aufbereitung und fundierte Analyse polizeilicher Datenmengen stellen grundlegende Voraussetzungen dar, um diese für Anwendungen der KI im polizeilichen Kontext nutzbar zu machen (Wiese 2024, S. 11). Dadurch können Schwächen der KI, wie Bias und Halluzinationen, reduziert werden (Bitkom e. V. 2023, S. 14).

In seiner Arbeit verdeutlicht Davis (1987, S. 3), dass die Akzeptanz einer neuen Technologie und letztlich ihre tatsächliche Nutzung maßgeblich von den Faktoren „wahrgenommene Nützlichkeit“ und „wahrgenommene Benutzerfreundlichkeit“ beeinflusst wird. Um beide Faktoren zu adressieren, sind laut Stowasser et al. (2020, S. 3) umfassende Change-Management-Maßnahmen erforderlich. Die Beschäftigten sollten dabei umfassend in den Implementierungsprozess eingebunden und frühzeitig für die Nutzung einer neuen Technologie qualifiziert werden (ebd., S. 4). Mögliche Anpassungsbedarfe bei den Qualifizierungsmaßnahmen oder der eingeführten KI selbst können vor einer flächendeckenden Einführung im Rahmen von Pilotprojekten ermittelt werden (ebd., S. 4). Um eine rechtskonforme Umsetzung zu gewährleisten, sollten von Beginn an die Datenschutzbeauftragten der Behörden beteiligt werden (Bitkom e. V. 2023, S. 10).

Im Rahmen dieses Beitrags war die Auswahl der verfügbaren Literatur in mehrfacher Hinsicht begrenzt. Ein Großteil der einschlägigen Fachpublikationen bezieht sich auf die öffentliche Verwaltung im Allgemeinen und weist zudem auch teilweise einen internationalen Schwerpunkt auf. Spezifische wissenschaftliche Untersuchungen, beispielsweise zur Datenqualität oder der Akzeptanz von KI-Systemen, beziehen sich meist nicht explizit auf die Polizei NRW. Entsprechend mussten für zentrale Fragestellungen häufig Rückschlüsse aus der allgemeinen Literatur gezogen und auf die Besonderheiten der Polizei NRW übertragen werden. Um die Validität der Ergebnisse langfristig zu erhöhen, sollte die hier angewandte SWOT-Analyse in zukünftigen Forschungsarbeiten zwingend durch Experteninterviews ergänzt werden. Ohne diesen direkten methodischen Zugang zur Organisation bleibt der Informationsfluss aus der Polizei NRW selbst stark limitiert. Dadurch besteht die Gefahr, dass spezifische interne Bedarfe oder polizeifachliche Restriktionen unberücksichtigt bleiben.

Schlussfolgerungen

Angesichts des demografischen Wandels und der andauernden Pensionierungswelle besteht für die Polizei NRW ein dringender Handlungsbedarf, um wertvolles Fachwissen vor Verlust zu schützen. Der vorliegende Beitrag zeigt, dass der Einsatz von KI ein vielversprechender Ansatz ist, um Erfahrungswissen effizient zu sichern und auch nach dem Ausscheiden von Beschäftigten noch zugänglich zu machen. Dabei bieten die bereits vorhandene Erfahrung der Polizei NRW und ihre IT-Infrastruktur günstige Voraussetzungen für die erfolgreiche Implementierung eines KI-Systems. Gleichzeitig müssen jedoch die identifizierten Schwächen, wie die Datenqualität, datenschutzrechtliche Anforderungen und die Akzeptanz der Beschäftigten, durch gezielte Maßnahmen adressiert werden. Von besonderer Bedeutung sind dabei umfassende Change-Management-Konzepte, um eine breite Akzeptanz zu gewährleisten. Im Rahmen dieses Beitrags konnte keine Abschätzung der technischen Machbarkeit (eigene Entwicklung oder Angebot eines externen Anbieters) eines KI-Systems sowie der damit verbundenen Kosten erfolgen. Dies sollte zukünftig durch eine Machbarkeitsstudie untersucht werden.

Literaturverzeichnis

Albers W, Hendele T, Weibler J, Wimber H (2015). Bürgernahe Polizei – Den demographischen Wandel gestalten. Ergebnisbericht der Expertenkommission.

Bitkom e. V. (Hrsg.) (2023). KI in der Polizei. Einsatzpotential und Lösungsansätze zur Implementierung. bitkom.org/sites/main/files/2023-10/bitkom-positionspapier-ki-polizei-einsatz-implementierung.pdf (30.11.2025).

BMI – Bundesministerium des Innern (2023). 300 Millionen Euro für moderne Polizei-IT-Infrastruktur. bmi.bund.de/SharedDocs/pressemitteilungen/DE/2019/12/polizeiinfrastruktur.html (15.11.2025).

BMI – Bundesministerium des Innern (2024). Programm P20. bmi.bund.de/DE/themen/sicherheit/programm-p20/programm-p20-node.html (15.11.2025).

Bundesministerium für Bildung und Forschung (Hrsg.) (2018). Strategie Künstliche Intelligenz der Bundesregierung. bundeswirtschaftsministerium.de/Redaktion/DE/Publikationen/Technologie/strategie-kuenstliche-intelligenz-der-bundesregierung.pdf?__blob=publicationFile&v=10 (07.08.2025).

Dahlkamp S (2024). 1.000 Tipps in 100 Tagen. Streife (1), 30–35. polizei.nrw/sites/default/files/2024-02/streife_01_2024_09_web.pdf (07.08.2025).

Davis F (1987). User acceptance of information systems. The Technology Acceptance Model (TAM), Michigan.

Der Bundesbeauftragte für den Datenschutz und die Informationstechnik (Hrsg.) (2024). Stellungnahme des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit zur öffentlichen Anhörung des Innenausschusses des Deutschen Bundestags am 22. April 2024. Handlungsfähigkeit der Strafverfolgungsbehörden sichern – Entscheidung des Bundesministeriums des Innern und für Heimat bezüglich der polizeilichen Analyse-Software Bundes-VeRA revidieren. Bonn. bfdi.bund.de/SharedDocs/Downloads/DE/DokumenteBfDI/Stellungnahmen/2024/StgN-polizeiliche-Analysesoftware.pdf?__blob=publicationFile&v=1 (20.12.2025).

Etscheid J, von Lucke J, Stroh F (2020). Künstliche Intelligenz in der öffentlichen Verwaltung. Anwendungsfelder und Szenarien. Frauenhofer-Institut für Arbeitswirtschaft und Organisation. publica-rest.fraunhofer.de/server/api/core/bitstreams/d3d9f520-1fd4-4516-98d6-a3370c134155/content (27.11.2025).

Europol (2024). AI and policing. The benefits and challenges of artificial intelligence for law enforcement. Europol Innovation Lab observatory report. Publications Office of the European Union, Luxembourg.

Färber G (Hrsg.) (2021). Die Attraktivität des öffentlichen Dienstes. Deutsches Forschungsinstitut für öffentliche Verwaltung. Speyer. Speyerer Forschungsberichte (FÖV).

Garrel J von, Thomas S, Jung M, Hüttemann D, Reuß M, Locher B, Beiersdorff S (2024). Der Aufbau von Vertrauen bei der KI-Implementierung/Building trust during AI implementation. wt Werkstattstechnik online 114 (11–12), 755–760. doi.org/10.37544/1436-4980-2024-11-12-51.

Girard J P, Girard J L (2015). Defining knowledge management: Toward an applied compendium. Online Journal of Applied Knowledge Management (3), 1–20.

Grosan C, Abraham A (2011). Rule-Based Expert Systems. In: Kacprzyk J, Jain L C, Grosan, C et al. (Hrsg.): Intelligent Systems. Springer, Berlin, Heidelberg, 149–185.

Haas S (2024). Von der Theorie zur Praxis. Generative KI in der modernen Polizeiarbeit. In: Honekamp W, Labudde D (Hrsg.): Polizei-Informatik 2024. Rediroma-Verlag, Remscheid, 80–86.

Helms M M, Nixon J (2010). Exploring SWOT analysis – where are we now? Journal of Strategy and Management 3 (3), 215–251. doi.org/10.1108/17554251011064837.

Homborg F, Hall F, Kahr R (2024). Auswertung von Kriminalitätsereignissen mithilfe von KI. In: Honekamp W, Labudde D (Hrsg.): Polizei-Informatik 2024. Rediroma-Verlag, Remscheid, 240–246.

Huang L, Yu W, Ma W, Zhong W, Feng Z, Wang H, Chen Q, Peng W, Feng X, Qin B, Liu T. (2025). A Survey on Hallucination in Large Language Models: Principles, Taxonomy, Challenges, and Open Questions. ACM Transactions on Information Systems 43 (2), 1–55. doi.org/10.1145/3703155.

Jiang Y, Li X, Luo H, Yin S, Kaynak O (2022). Quo vadis artificial intelligence? Discover Artificial Intelligence 2 (1). doi.org/10.1007/s44163-022-00022-8.

LAFP NRW – Landesamt für Ausbildung, Fortbildung und Personalangelegenheiten der Polizei NRW (Hrsg.) (2024). Verfügung: Wissenstransfer innerhalb der Polizei NRW. Einführung eines digitalen Offboardingverfahrens. Selm.

Landesregierung Nordrhein-Westfalen (2022). Antwort der Landesregierung auf die Kleine Anfrage 492 vom 26. September 2022 des Abgeordneten Marc Lürbke (FDP). Drucksache 18/1400.

Lanquillon C, Schacht S (Hrsg.) (2023). Knowledge Science – Fallstudien. Springer Fachmedien Wiesbaden, Wiesbaden.

Lehner F (2025). Wissensmanagement. Grundlagen, Methoden und technische Unterstützung. 8. Aufl. Hanser, München.

Lenk K, Meyerholt U, Wengelowski P (2021). Wissensmanagement in Staat und Verwaltung. 2. Aufl. Nomos Edition Sigma, Baden-Baden.

LZPD NRW – Landesamt für Zentrale Polizeiliche Dienste Nordrhein-Westfalen (2025). Polizei baut eigene KI-Infrastruktur aus. lzpd.polizei.nrw/presse/polizei-baut-eigene-ki-infrastruktur-aus (14.11.2025).

Müller M, Link J (2023). Smart Expert Debriefing. In: Lanquillon C, Schacht S (Hrsg.): Knowledge Science – Fallstudien. Springer Fachmedien Wiesbaden, Wiesbaden, 109–147.

Namugenyi C, Nimmagadda S L, Reiners T (2019). Design of a SWOT Analysis Model and its Evaluation in Diverse Digital Business Ecosystem Contexts. Procedia Computer Science 159, 1145–1154. doi.org/10.1016/j.procs.2019.09.283.

Niederberger M, Wassermann S (Hrsg.) (2014). Methoden der Experten- und Stakeholdereinbindung in der sozialwissenschaftlichen Forschung. Springer VS, Wiesbaden.

North K (2021). Wissensorientierte Unternehmensführung. Wissensmanagement im digitalen Wandel. 7. Aufl. Springer Gabler, Wiesbaden, Heidelberg.

OECD (2025). Governing with Artificial Intelligence. The State of Play and Way Forward in Core Government Functions. OECD Publishing, Paris.

Probst G J B, Raub S, Romhardt K (2012). Wissen managen. Wie Unternehmen ihre wertvollste Ressource optimal nutzen. 7. Aufl. Springer Gabler, Wiesbaden.

Reisach U, Nakhosteen C Benjamin, Erlach C, Orians W (2025). Wissenstransfer bei Fach- und Führungskräftewechsel. Erfahrungswissen erfassen und weitergeben. 2. Aufl. Hanser, München.

Reiss M V, Knor E Luise, Stöwing E, Merten L, Möller J (2025). Zwischen Neugier und Skepsis: Nutzung und Wahrnehmung generativer KI zur Informationssuche in Deutschland. doi.org/10.21241/ssoar.100907.

Renz S, Kalimeris J, Spörrle M (2024): Menschliche und künstliche Intelligenz im Wissensmanagement: eine Reflexion auf Basis von Daten, Information, Wissen und Weisheit. In: Offergelt F, Hofreiter S, Steiner T (Hrsg.), Wissensmanagement in modernen Organisationen. Impulse aus der Forschung und Erkenntnisse aus der Praxis. Springer Gabler, Berlin, Heidelberg, 151–165.

Sheikh H, Prins C, Schrijvers E (2023). Mission AI. The New System Technology. Springer International Publishing; Imprint Springer, Cham.

Statistisches Bundesamt (2025). 12,9 Millionen Erwerbspersonen erreichen in den nächsten 15 Jahren das gesetzliche Rentenalter. destatis.de/DE/Presse/Pressemitteilungen/2022/08/PD22_330_13.html (01.08.2025).

Stowasser S, Suchy O, Huchler N, Müller N, Peissner M, Stich A, Vögel H-J, Werne J (2020): Einführung von KI-Systemen in Unternehmen. Gestaltungsansätze für das Change Management. München. plattform-lernende-systeme.de/files/Downloads/Publikationen/AG2_Whitepaper_Change_Management.pdf (14.11.2025).

Veit S (2021). Die öffentliche Verwaltung im modernen Staat. GWP – Gesellschaft, Wirtschaft, Politik 70 (1-2021), 99–109. doi.org/10.3224/gwp.v70i1.09.

Wiese A (2024). Die digitale Chefin. Die KI als Führungskraft in Polizeiorganisationen. Masterarbeit. Deutsche Hochschule der Polizei, Münster.

Wollny V, Paul H (2014). Die SWOT-Analyse: Herausforderungen der Nutzung in den Sozialwissenschaften. In: Niederberger M, Wassermann S (Hrsg.): Methoden der Experten- und Stakeholdereinbindung in der sozialwissenschaftlichen Forschung. Springer VS, Wiesbaden, 189–213.

Zins C (2007). Conceptual approaches for defining data, information, and knowledge. Journal of the American Society for Information Science and Technology 58 (4), 479–493. doi.org/10.1002/asi.20508.

Predictive Policing im digitalen Raum: Eine SWOT-Analyse des Einsatzes Künstlicher Intelligenz zur Verhütung von Cyberkriminalität

Enrico Schubert

Die fortschreitende Digitalisierung hat die Gesellschaft grundlegend transformiert und neue Bedrohungslagen geschaffen, die Sicherheitsbehörden vor erhebliche Herausforderungen stellen (Marcinkowski 2023, S. 1). Kriminalität manifestiert sich zunehmend im digitalen Raum, der sich durch Schnelligkeit, Skalierbarkeit und geografische Grenzenlosigkeit auszeichnet (Ernst/Fähndrich 2024, S. 46). Mit dem technologischen Fortschritt wurde eine ambivalente Technologie verfügbar: Künstliche Intelligenz (KI).

Einerseits ermöglicht KI eine effiziente Bekämpfung von Cyberbedrohungen durch automatisierte Anomalie-Erkennung, andererseits verfeinert sie Angriffsmethoden und erleichtert deren Automatisierung (Ernst/Fähndrich 2024, S. 46). Laut einer Studie von Sopra Steria berichten 73 % der befragten Organisationen, dass die böswillige Nutzung von KI die Bedrohungslage drastisch verschärft hat, während 71 % meinen, dass Cyberkriminelle KI besser für Angriffe nutzen als Organisationen zur Abwehr (2024, S. 4). KI eröffnet auch die Möglichkeit, präventiv statt reaktiv zu agieren (FAZ-Institut/Sopra Steria 2024, S. 9). Trotz der zunehmenden Bedeutung digitaler Kriminalitätsformen ist fraglich, inwiefern Ansätze zu Predictive Policing (PP) auf den digitalen Raum übertragbar sind. Bisherige PPModelle konzentrieren sich überwiegend auf den physischen Raum und arbeiten vor allem mit ortsbezogenen Daten. Ihre tatsächliche Wirksamkeit lässt sich nur schwer isoliert nachweisen, da zahlreiche Einflussfaktoren die Bewertung erschweren (Knobloch 2018, S. 5). Daher bleibt unklar, ob ihre Logik im digitalen Umfeld überhaupt tragfähig ist.

Diese Problematik verschärft sich durch die geringe Polizeipräsenz im digitalen Raum (Rüdiger 2023, S. 40 f.). Die Dunkelziffer bei Cybercrime ist erheblich – mit einer Relation von etwa 1 zu 95 zwischen angezeigten Fällen und Viktimisierungserfahrungen (Rüdiger 2023, S. 44). PP wird in diesem Kontext als „datengestützte Analyse zur Bewertung polizeilicher Interventionsmaßnahmen“ verstanden, mit dem Ziel, „mit limitierten Ressourcen proaktiver zu arbeiten und effektive Strategien zu entwickeln, die Kriminalität verhindern“ (Mehner et al. 2023, S. 56 f.). Nur KI-gestützte Instrumente ermöglichen es, die enormen Datenvolumina der Cyberkriminalität zu bewältigen und komplexe Angriffsmuster automatisiert zu erkennen (Krauss 2023, S. 121).

Gleichzeitig signalisiert die Europäische Union Vorsicht: PP-Systeme, die auf Profiling, Standortdaten oder vorheriger Delinquenz basieren, sind nach der KI-VO verboten (Mehner et al. 2023, S. 55 f.). Auch der Deutsche Ethikrat betont, dass die Verantwortung grundsätzlich beim Menschen verbleiben muss (2023, S. 25). Der vorliegende Beitrag widmet sich einer kritischen Analyse des KI-Einsatzes zur Verhütung von Cyberkriminalität durch PP-Ansätze. Dabei wird die zentrale Frage „Kann PP die Kriminalitätsbekämpfung im digitalen Raum verändern?“ untersucht. Dieser Beitrag ermittelt Stärken, Schwächen, Chancen und Risiken,

bewertet das Potenzial von PP, um die Nutzung moderner Technologien durch die Polizei zu fördern. Sie erfolgt auf konzeptioneller Ebene und verzichtet bewusst auf technische oder juristische Detailanalysen.

Hintergrund

Digitalisierung und globale Vernetzung haben eine Schattenseite: Seit den frühen Tagen von Computer und Internet nutzen Kriminelle die durch Anonymität begünstigten Möglichkeiten zur Begehung von Straftaten (Drafz 2025, S. 2). Cyberkriminelle verwenden dabei u. a. digitale Schwarzmärkte wie das Darknet, um sich abzusprechen, Taten zu koordinieren und kriminelles Know-how sowie Dienstleistungen auszutauschen (Cybercrime-as-a-Service) (BKA 2018, S. 52). Die Funktion und Wirkung der Polizeipräsenz im digitalen Raum ist bislang weitgehend unerforscht (Rüdiger 2023, S. 40). Vor dem Hintergrund, dass Cybercrime-Delikte derzeit nur eine Aufklärungsquote von insgesamt 32 % aufweisen und der durch Cyberattacken verursachte Schaden in Deutschland im Jahr 2024 bei 178,6 Mrd. Euro lag, bedarf es neuer Vorgehensweisen in der Verhütung und Bekämpfung von Cyberstraftaten. Operative Maßnahmen müssen der steigenden Anzahl von Angriffen und der zunehmenden Vernetzung der Cyberakteure in hoher Frequenz entgegengesetzt werden (BKA 2025, S. 3).

Seit der Einführung des ersten ChatGPTModells im November 2022 (OpenAI 2022) sind zahlreiche generative KISysteme entstanden. Kriminelle nutzen sie verstärkt für Phishing und Malware. 2025 dürfte KIgestützte Kriminalität zunehmen, da die Automatisierung Angriffe schneller, professioneller und reichweitenstärker macht, ohne die bisherigen Modi Operandi grundlegend zu verändern (BKA 2025, S. 33).

Predictive Policing

„Predictive Policing bezeichnet den Einsatz datengestützter Verfahren zur räumlich-zeitlichen Vorhersage von Straftaten. Ziel ist es, Polizeiarbeit effizienter zu gestalten, Ressourcen zu bündeln und Kriminalität möglichst frühzeitig zu unterbinden. Im Zentrum stehen algorithmische Modelle, die aus historischen Daten Muster ableiten und daraus Prognosen für zukünftige Delikte generieren – z. B. wann und wo Einbrüche wahrscheinlich auftreten werden“ (Wickert 2025). PPSoftware nutzt kriminalitätsbezogene Daten und mathematischstatistische Verfahren, um Wahrscheinlichkeiten für Straftaten in Regionen und Zeiträumen zu berechnen. Ziel ist die frühzeitige Erkennung potenzieller Gefahrenlagen durch Musteranalyse (Ruppert 2023, S. 320). Durch PP-Systeme werden signifikante Abweichungen zwischen geringen Wahrscheinlichkeiten in einem bestimmten Bereich von Standardwahrscheinlichkeiten errechnet und (in Karten) veranschaulicht. Dadurch ist es möglich, eine Effizienzsteigerung der polizeilichen Arbeit sowohl in der kriminalpolizeilichen Prävention als auch in der Verhütung von Straftaten zu generieren. Voraussetzung dafür ist jedoch die Reliabilität der Verfahrensweise (Knobloch 2018, S. 9 f.).

Eine genaue Vorhersage bestimmter Deliktsformen ist schwer möglich, da Prognosen auf technischer Analyse beruhen. PP-Software arbeitet dabei entweder raumbezogen (Identifikation von Gefahrengebieten) oder personenbezogen (individuelle Risiken) (Ruppert 2023,

S. 322 f.). Grundlage ist eine Datenbasis aus Kriminalstatistiken, Ereignis-, Infrastruktur- und Wetterdaten sowie sozioökonomischen Informationen, insbesondere aus Social Media (Ruppert 2023, S. 323).

Cybercrime

Computer- und Internetdelikte werden weder juristisch noch kriminologisch einheitlich definiert (Selzer 2019, S. 221). Cybercrime ist interdisziplinär zu betrachten und lässt sich eher als Phänomen denn als definierter Begriff fassen (Huber/Pospisil 2020, S. 110). Gemäß BKA (2025, S. i) wird Cybercrime wie folgt unterschieden:

Cybercrime-Delikte sind solche, „die sich gegen das Internet und informationstechnische Systeme richten – sogenannte Cybercrime im engeren Sinne", wie z. B. Computerbetrug gem. § 263a StGB, sowie „Delikte, die lediglich unter Nutzung von Informationstechnik begangen werden und bei denen das Internet vorwiegend Tatmittel ist" (ebd., S. i), wie z. B. Volksverhetzung in sozialen Medien. Eine englische Studie analysierte mittels Algorithmen zehntausende Twitter-Meldungen auf fremdenfeindliche Inhalte, um zeitliche und räumliche Muster aufzudecken (Miller et al. 2016, S. 10).

Laut BKA ist im Bereich Cybercrime eine deutliche Dynamisierung zu beobachten, die vor allem auf zunehmende digitale Vernetzung, CybercrimeasaServiceStrukturen und neue KI-gestützte Angriffsmöglichkeiten zurückzuführen ist. Diese Entwicklungen führen dazu, dass technische Sicherungsmaßnahmen kontinuierlich weiterentwickelt werden müssen, um den steigenden Anforderungen an Cybersicherheit gerecht zu werden (2025, S. 32). KI-Modelle können Cyberangriffe, wie etwa Phishing und Malwareentwicklung, durch Automatisierung schneller und in deutlich größerem Umfang ermöglichen. Das bedeutet: „Aktive Cybersicherheit – Technische Sicherungsmaßnahmen zum Schutz der Systeme müssen durch gefahrenabwehrende und strafverfolgende Maßnahmen ergänzt werden" (ebd., S. 32).

Big Data und Künstliche Intelligenz

Unter Big Data wird das Erheben, Speichern, Zugreifen und Analysieren von großen und teilweise heterogenen, strukturierten und unstrukturierten Datenmengen verstanden (Steinebach et al. 2015, S. 8). Big Data wird durch die Merkmale Volume (Datenmenge), Velocity (Geschwindigkeit) und Variety (Vielfalt) charakterisiert. Die Datenquellen sind vielfältig, darunter soziale Netzwerke, Maschinendaten und Transaktionsdaten (Jasim/Hadi 2025, S. 159 f.). Big-Data-Analysen stehen vor drei zentralen Herausforderungen: Datenmanagement, Echtzeit-Visualisierung sowie Sicherheit und Datenschutz (Verschlüsselung, Anonymisierung, Zugriffskontrolle). Die Balance zwischen effizienter Nutzung und Wahrung der Privatsphäre ist dabei entscheidend (Jasim/Hadi 2025, S. 163 ff.).

Die Digitalisierung und die rasante Entwicklung neuer Technologien haben in den vergangenen Jahren zu einem exponentiellen Datenwachstum geführt (Brüning 2024, S. 133). In den Jahren 2015 bis 2019 wuchs die weltweite digitale Datenmenge von 15,5 auf etwa 41 Zettabyte an (ein Zettabyte sind eine Milliarde Terabyte). Prognostisch wird sich diese Entwicklung von heute in den kommenden vier Jahren von 173,4 auf 527,5 Zettabyte weiter massiv beschleunigen. Dies veranschaulicht Abbildung 1:

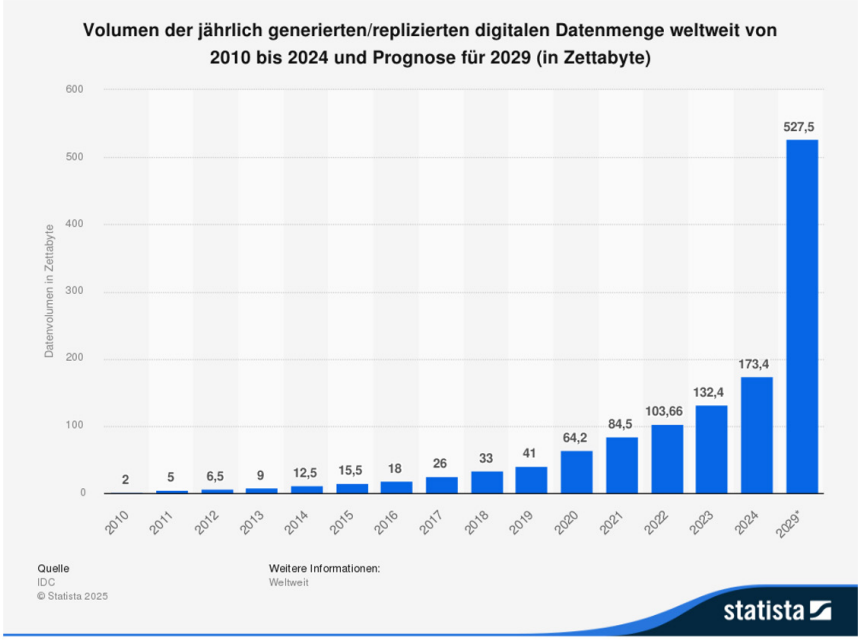

Abbildung 1: Volumen der jährlich generierten/replizierten digitalen Datenmenge weltweit von 2010 bis 2024 und Prognose für 2029 (in Zettabyte) (Western Digital 2025)

KI ermöglicht es Maschinen, menschenähnliche Denkprozesse auszuführen und Muster in riesigen Datenmengen zu erkennen. Diese Fähigkeit hat zu einer explosionsartigen Erzeugung und Speicherung von Daten geführt. Big-Data-Analysen verwenden diese enormen Datenmengen und identifizieren so bisher verborgene Erkenntnisse und Trends, wobei Datensätze in Echtzeit durchsucht werden (Brüning 2024, S. 133). Im Sinne des Art. 3 Nr. 1 KI-VO ist ein „KI-System ein maschinengestütztes System, das für einen in unterschiedlichem Grade autonomen Betrieb ausgelegt ist und das nach seiner Betriebsaufnahme anpassungsfähig sein kann und das aus den erhaltenen Eingaben für explizite oder implizite Ziele ableitet, wie Ausgaben wie etwa Vorhersagen, Inhalte, Empfehlungen oder Entscheidungen erstellt werden, die physische oder virtuelle Umgebungen beeinflussen können“. Ein KI-System mit lernendem Algorithmus kann Informationen in kürzester Zeit verdichten. Zu beachten ist im Kontext von PP, dass keine hundertprozentige Zukunftsvorhersage durch Algorithmen möglich ist (Farthofer 2023, S. 295).

Predictive Policing und digitaler Raum

Neben dem bekannten physischen Raum verbringen Menschen zunehmend einen relevanten Teil des Lebens in einem virtuellen öffentlichen Raum, welcher sich entwickelt hat, und interagieren dort miteinander (Rüdiger 2019). Das BMI (2021, S. 133) definiert den Cyberraum wie folgt: „Der Cyberraum ist der virtuelle Raum aller weltweit auf Datenebene vernetzten bzw. vernetzbaren informationstechnischen Systeme. Dem Cyberraum liegt als öffentlich zugängliches Verbindungsnetz das Internet zugrunde, das durch beliebige andere Datennetze erweitert werden kann.“ Laut Benyon bezeichnet der digitale Raum die Welt der virtuellen Realität und entspricht weitgehend dem Cyberraum, betont jedoch stärker die digitalen Interaktionsformen. Er umfasst sowohl die Kommunikation zwischen Menschen als auch die Interaktion digitaler Geräte und Infrastrukturen sowie die Verarbeitung und Bereitstellung digitaler Inhalte und Software (2014, S. 37). In virtuellen Realitäten sind nahezu alle Delikte denkbar;

Eigentum, Vermögen sowie Ehrverletzungen und sexuelle Belästigungen können dort ebenso auftreten wie in der realen Welt (Grafe 2025, S. 153). Vor diesem Hintergrund könnte der Einsatz datenbasierter Prognoseverfahren im digitalen Raum an Bedeutung gewinnen.

PP ist als komplexes soziotechnisches System zu verstehen, das nur funktioniert, wenn technische Systeme, organisatorische Abläufe und unterschiedliche polizeiliche Berufsgruppen sinnvoll miteinander verknüpft werden. Erst durch diese Abstimmung kann prognosebasiertes Wissen tatsächlich in operative Entscheidungen einfließen und das Handeln prägen. Zugleich gilt seine Implementierung als Blaupause für die Digitalisierung der Polizeiarbeit, da datenbasierte Prognosen die zukünftige Gestaltung von Polizeiarbeit und das Verhältnis zur Öffentlichkeit maßgeblich beeinflussen (Egbert/Leese 2021, S. 10 f.). PP beginnt mit der Erfassung von Kriminalitätsdaten, die in einem analytischen Prozess durch technische Eigenschaften der Software und das Zusammenspiel von Algorithmen und Menschen verarbeitet werden. Die daraus gewonnenen Erkenntnisse müssen verständlich aufbereitet, handlungsorientiert weitergegeben und schließlich in die praktische Polizeiarbeit integriert werden (ebd., S. 4).

Im digitalen Raum stehen Polizei und Sicherheitsbehörden vor besonderen Herausforderungen: Die Datenquellen sind heterogen, die Angriffsmuster komplex. Vergangene Cyberangriffe werden in großen Datenmengen gesammelt – von sozialen Netzwerken über Maschinen- und Transaktionsdaten bis hin zu Systemprotokollen. Die heterogenen Datenquellen erfordern leistungsfähige Big-Data-Methoden (Jasim/Hadi 2025, S. 159 f.). Hier kommen fortgeschrittene KI-Modelle und maschinelles Lernen zum Einsatz, um Anomalien, Angriffsmuster und Risiken frühzeitig zu identifizieren. Automatisierte Prognoseverfahren erlauben nicht nur eine schnellere und breitere Auswertung, sondern steigern auch die Effizienz und Präzision der Cyberabwehr – etwa bei der Erkennung von Phishing-Kampagnen, Malware oder sogenannten Advanced Persistent Threats (Jasim/Hadi 2025, S. 163–167; Farthofer 2023, S. 312–317).

Dennoch bleiben Herausforderungen bestehen: Die Komplexität der Integrations-, Skalierbarkeits- und Echtzeit-Anforderungen verlangt nach flexiblen, lernenden Sicherheitsarchitekturen und der intensiven Zusammenarbeit zwischen Polizei, Wissenschaft und Technik. So stellen Datenschutz, Datenprovenienz sowie die Gefahr von Fehlklassifikationen (False Positives und False Negatives) bekannte Grenzen der Technologie dar (Jasim/Hadi 2025, S. 171; Knobloch 2018, S. 22 ff.). Wie in Abschnitt 2.1 dargelegt, ist die Datenbasis die Grundlage für PP (Ruppert 2023, S. 323). In diesem Zusammenhang kann auch Big Data von entscheidender Bedeutung sein. Komplexe Bedrohungen wie

- Advanced Persistent Threats (APT), also Cyber-Attacken zumeist mit dem Ziel, über einen langen Zeitraum sensible Daten auszuspähen,
- Distributed Denial of Service (DDoS), zumeist Angriffe mit dem Ziel, eine Vielzahl von Rechnern oder Netzwerken zu überlasten, oder
- Zero-Day-Attacken, also die Ausnutzung einer unbekannten Sicherheitslücke, für die es noch keine Lösung gibt,

erfordern fortwährende Überwachung und schnelle Datenanalyse. Herkömmliche Sicherheitstools sind unzureichend, insbesondere bei Cloud-Infrastrukturen, da sie zu viele Fehlalarme generieren und den Datenmengen nicht mehr gewachsen sind.

Die Erkennung von Anomalien, Klassifizierung und Musteranalyse sind typische Anwendungsbereiche von Machine Learning in der Cybersecurity (Jasim/Hadi 2025, S. 158 ff.). Ziel ist es, Informationsfluten zu bewältigen, relevante Daten zu erkennen und dadurch schnellere, fundierte Entscheidungen und Prognosen zu ermöglichen. Dafür braucht es passgenaue, bedarfsgerechte Lösungen (Povalej 2017, S. 49). In diesem Kontext ist Data-Mining besonders relevant, da es das automatisierte Erkennen neuer Muster in großen Datensätzen ermöglicht. Im Gegensatz dazu setzt Machine Learning solche Muster bereits voraus und fokussiert primär die Lösung konkreter Probleme (Steinebach et al. 2015, S. 24).

Methodik

Zur systematischen Erfassung und Bewertung der aktuellen Forschungslage im Bereich PP und Cybercrime wurde ein zweistufiges methodisches Vorgehen gewählt. Zunächst wurde eine ausführliche Literaturrecherche in Form eines Scoping Reviews durchgeführt, um den Stand der Forschung darzustellen und zentrale Erkenntnisse herauszuarbeiten. Das Scoping Review folgte einem explorativen, aber transparenten Vorgehen. Die Literaturrecherche umfasste wissenschaftliche Datenbanken (u. a. Google Scholar, Semantic Scholar) sowie einschlägige behördliche Publikationen (u. a. BKA, BMI). Eingeschlossen wurden Quellen aus den Jahren 2014–2025, die sich mit Predictive Policing, KIgestützter Cyberabwehr, BigDataAnalysen oder rechtlichen Rahmenbedingungen befassten. Ausgeschlossen wurden rein technische Arbeiten ohne Bezug zur Polizeipraxis sowie nicht zitierfähige Onlinequellen. Die Auswahl erfolgte anhand der Relevanz für die Forschungsfrage sowie der wissenschaftlichen Qualität. Um subjektive Verzerrungen zu reduzieren, wurden dabei konkurrierende Perspektiven (z. B. technische, rechtliche, ethische) bei der Quellenauswahl bewusst berücksichtigt. Anschließend erfolgte eine SWOT-Analyse als strukturierte Methode, um die aus der Literatur gewonnenen Erkenntnisse systematisch zu ordnen und zu bewerten. SWOT ist ein Akronym für Strengths (Stärken), Weaknesses (Schwächen), Opportunities (Chancen) und Threats (Bedrohungen/Risiken) und im Kern eine offene Vierfelder-Matrix (Künzli 2012, S. 126 f.).

Die SWOT-Analyse wurde ursprünglich in der Betriebswirtschaftslehre als Instrument des strategischen Managements für Unternehmen entwickelt. Dabei werden Stärken und Schwächen (interne Faktoren) sowie Chancen und Bedrohungen (externe Faktoren) strukturiert gegenübergestellt, um einen strukturierten Überblick über die Forschungslage zu erhalten. Die Methode hat sich durch ihre einfache, transparente und argumentativ-verbale Vorgehensweise nicht nur im Management, sondern auch in verschiedenen sozialwissenschaftlichen Disziplinen etabliert (Wollny/Paul 2015, S. 189 f.).

Für den vorliegenden Beitrag bedeutet dies, dass die SWOTAnalyse keine objektive Bewertung liefert, sondern eine strukturierte Synthese der Literaturbefunde. Ebenso ist das Scoping Review aufgrund der dynamischen Entwicklung im Bereich KI und Cybercrime nicht vollständig, sondern bildet den Forschungsstand zum Zeitpunkt der Bearbeitung ab. Die Kombination beider Methoden ist sinnvoll, da das Scoping Review die Breite der Forschung erschließt, während anhand der SWOTAnalyse diese Erkenntnisse eingeordnet und hinsichtlich ihrer Bedeutung für PP im digitalen Raum in der Diskussion bewertet werden können. Dadurch entsteht ein konsistenter Analyseprozess, der sowohl explorativ als auch strukturierend ist. Durch die systematische Kategorisierung von Trends und Einflussfaktoren in einer SWOT-Matrix ermög-

licht die Methode die Ableitung fundierter Handlungsempfehlungen und Strategien. Ihr Vorteil liegt in der Übersichtlichkeit, Verständlichkeit und Ressourcenschonung. Dem steht die Begrenzung gegenüber, dass das Verfahren wenig formalisiert ist, womit das Risiko besteht, dass Kriterien unvollständig oder subjektiv festgelegt werden (Wollny/Paul 2015, S. 191 ff.). Der größte Nutzen liegt in der transparenten Darstellung der internen und externen Faktoren, der Identifikation von Handlungsbedarf sowie der Unterstützung bei der Entwicklung und Fokussierung strategischer Maßnahmen (Schawel/Billing 2018, S. 331 f.).

Ergebnisse

In diesem Abschnitt werden die Stärken und Schwächen sowie die Chancen und Risiken anhand der in Abschnitt 3 dargelegten Methodik gegenübergestellt.

Stärken

Durch PP besteht die Möglichkeit der vorverlagerten Intervention. Die Perspektive verlagert sich von der Aufklärung und Ahndung von Straftaten in Richtung der Gefahrenabwehr (Singelnstein 2018, S. 5). Darüber hinaus ermöglichen PP-Ansätze (auch im digitalen Raum) die frühzeitige Erkennung von Gefahrenlagen sowie den gezielten Einsatz von Polizeikräften und Ressourcen, da kriminalitätsrelevante Muster früh identifiziert werden können, was vor allem bei knappen Ressourcen einen Effizienzgewinn erzeugt (Knobloch 2018, S. 9 f.; Ruppert 2023, S. 320). Durch IT-gestützte und automatisierte Auswertungen können umfangreiche Datenquellen genutzt werden, um zukünftige Erscheinungsformen von Kriminalität in Form von Wahrscheinlichkeitsprognosen darzustellen (Singelnstein 2018, S. 1). Die Kombination von technischer Prävention und strafverfolgenden Maßnahmen stärkt die Handlungsfähigkeit von Polizei und Behörden (BKA 2025, S. 32).

Schwächen

Algorithmen sind oft auf bekannte Muster trainiert und können bestimmte Delikte übersehen, die nur in geringem Maße Mustern folgen. Dies begrenzt die Prognosefähigkeit (Singelnstein 2018, S. 5 ff.). Die Reliabilität und Prognosegenauigkeit sind bei Vorhersagen durch PP auch technisch bedingt unsicher sowie stark von der Datenqualität und -quantität abhängig (Knobloch 2018, S. 9 f.; Ruppert 2023, S. 323). Die mangelnde Transparenz sowie die schwierige Nachvollziehbarkeit von Systemen, die auf automatisierten Datenverarbeitungsprozessen, Algorithmen und daraus entstehenden Prognosen beruhen, sind kritikwürdig (Blackbox-Problematik) (Fricke 2020, S. 7; Singelnstein 2018, S. 7 ff.). Prognosen bergen stets das Problem von False Positives − fälschlich als gefährlich eingestuften Treffern −, wie auch bei anderen Individualprognosen (Jasim/Hadi 2025, S. 170; Kinzig 2025, § 66 Rn. 38; Singelnstein 2018, S. 5). Bisher ist es weder gelungen, einen wesentlichen Einfluss von PP auf Fallzahlen nachzuweisen, noch belastbare Aussagen zu diesem Erkenntnisinteresse zu generieren (Seidensticker 2022, S. 208). Big-Data-Analysen stehen vor dem ethischen Problem, dass die effiziente Nutzung großer Datenmengen häufig mit ungelösten Fragen des Datenschutzes kollidiert – insbesondere hinsichtlich Anonymisierung, Verschlüsselung und Zugriffskontrolle (Jasim/Hadi 2025, S. 163 ff.).

Chancen

Big Data und KI erweitern durch Algorithmen und leistungsfähige Hardware die Analyse großer Datenmengen. DataMiningVerfahren erkennen selbstständig Muster und Zusammenhänge; ihr volles Potenzial entfaltet sich, wenn Echtzeitdaten kontinuierlich eingespeist und ausgewertet werden (Steinebach et al. 2015, S. 8). Durch die Verknüpfung von Open Source Intelligence (OSINT) mit polizeilichen Daten in Big-Data-Analysen können Verhaltensmuster erkannt und Hypothesen über zukünftige Straftaten entwickelt werden. Darüber hinaus eröffnet dieser Ansatz die Möglichkeit, gesellschaftliche Trends im Hinblick auf neue Gefahrenlagen zu identifizieren (Fricke 2020, S. 4). Big-Data-Analysen ermöglichen es, bislang unbekannte Zusammenhänge und Kriminalitätsmuster erkennbar zu machen, z. B. zwischen zwei verschiedenen Deliktsbereichen (Fricke 2020, S. 5).

Risiken

PP in Deutschland ist rechtlich problematisch: Prognosen mit nicht personenbezogenen Daten gelten als unbedenklich, doch die automatisierte Analyse personenbezogener Daten stößt auf enge verfassungsrechtliche Grenzen (Singelnstein 2018, S. 8). Eine ausschließlich auf KIProfiling beruhende Kriminalitätsprognose ist nach Art. 5 Abs. 1 lit. d KIVO verboten. Die BNDEntscheidung betont zudem, dass zur Nachvollziehbarkeit unabhängige Instanzen für die technische Kontrolle eines polizeilichen KIEinsatzes erforderlich sind (BVerfG 2020, NJW 2020, 2235 (2253), Rn. 192). PP-Maßnahmen im Vorfeld, etwa anlassunabhängige Identitätsfeststellungen an kriminalitätsbelasteten Orten, besitzen derzeit keine spezifische Rechtsgrundlage und müssten geschaffen werden. Dabei wären strenge Maßstäbe an die Verhältnismäßigkeit zu knüpfen (Singelnstein 2018, S. 8). Eine zuverlässige Arbeitsweise eines KI-gestützten PP-Systems ist zudem von der Qualität der zu verarbeitenden Daten abhängig (Singelnstein 2018, S. 7).

Ein weiterer Aspekt ist der Mythos des unparteiischen Algorithmus. Studien zeigen, dass Vorurteile auf vielfältige Weise in polizeiliche und justizielle Entscheidungsunterstützungssysteme einfließen (Egbert/Leese 2021, S. 27; Lum/Isaac 2016, S. 15 ff.; Richardson et al. 2019, S. 224 ff.). Eine zentrale Verwaltung polizeilicher Daten (mindestens auf Bundesebene) ist erforderlich, um die Datenverfügbarkeit zu sichern und das Potenzial intelligenter Systeme wie PP auszuschöpfen (Babuta 2017, S. 24; Fricke 2020, S. 10). Neben finanziellen und personellen Herausforderungen werden vor allem Anschaffungs- und Lizenzkosten als kritische Faktoren benannt. Personell gilt es, Fortbildungen umzusetzen, Spezialisten einzubeziehen oder Outsourcing-Strategien zu nutzen, um die Funktionsfähigkeit von PP-Anwendungen dauerhaft zu sichern (Knobloch 2018, S. 37 ff.). Die Ergebnisse der SWOT-Analyse werden für die sich anschließende Diskussion thematisch geclustert und in Abbildung 2 veranschaulicht:

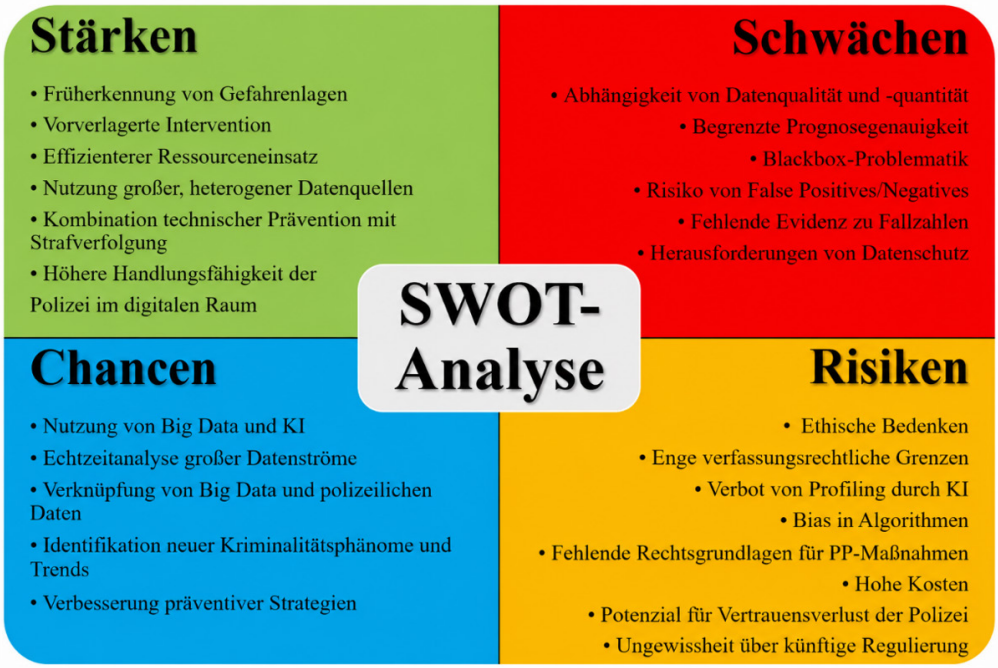

Abbildung 2: SWOT-Matrix – PP im digitalen Raum (eigene Darstellung)

Diskussion

Um die identifizierten Stärken, Schwächen, Chancen und Risiken theoretisch einzuordnen und die ambivalente Rolle von PP im digitalen Raum weiter zu schärfen, bietet es sich an, ergänzend zwei ethische Perspektiven aus der KIForschung heranzuziehen: die Ansätze des ModelsofThreat (MoT) sowie des EthicsofCare (EoC) (Asaro 2019, S. 42 ff.). Beide Konzepte ermöglichen eine vertiefte Bewertung der technologischen Prognoseverfahren, indem sie unterschiedliche normative Rahmen bereitstellen, die über die rein datenbasierte Betrachtung der SWOTAnalyse hinausgehen. Der MoTAnsatz geht davon aus, dass Bedrohungen eindeutig klassifizierbar sind, und bildet damit die Grundlage für automatisierte Entscheidungen. Er verarbeitet große und heterogene Datenmengen und -arten, um präzisere Risikoprognosen zu ermöglichen, wobei Genauigkeit, Vollständigkeit und Verlässlichkeit der Klassifikationen zentrale Werte darstellen (Asaro 2019, S. 44). In der Praxis werden solche Datenströme zunehmend in Fusion-Centern gebündelt, die Informationen aus Strafverfolgung und externen Quellen, etwa SocialMediaAnalysen, zusammenführen (Mehner et al. 2023, S. 63). Diese datengetriebenen Ansätze müssen jedoch kritisch hinterfragt werden. Insbesondere ist zu prüfen, ob die Erhebung und Verarbeitung externer Daten rechtmäßig erfolgt und ob darauf basierende KIPrognosen zulässig sind (Mehner et al. 2023, S. 65). Dies gilt umso mehr, als die KIVO Profilingbasierte Prognosen ausdrücklich untersagt (Art. 5 Abs. 1 lit. d KIVO). Hinzu kommt die Intransparenz vieler KISysteme: BlackboxModelle erschweren die Nachvollziehbarkeit polizeilicher Entscheidungen. Erklärbare KI kann diese Problematik zwar mindern, schafft jedoch keine vollständige Transparenz, sondern lediglich eine höhere Erklärbarkeit und damit Vertrauen (Brüning 2024, S. 150 f.).

Aus den bisherigen Überlegungen folgt, dass PP im digitalen Raum nur dann wirksam eingesetzt werden kann, wenn organisatorische Voraussetzungen wie Datenharmonisierung, klare Verantwortlichkeitsstrukturen und interdisziplinäre Zusammenarbeit geschaffen werden. Ohne diese Grundlagen bleiben technische Potenziale ungenutzt. Der EoC-Ansatz betont demgegenüber die Bedeutung sozialer Beziehungen und struktureller Ursachen von Kriminalität. Er fordert präventive Interventionen, die das Verhältnis zwischen Polizei und Gesellschaft stärken (Asaro 2019, S. 44). Die SWOTAnalyse verdeutlicht insgesamt ein ambivalentes Bild: PP im digitalen Raum bietet erhebliche Chancen für Effizienzgewinne und präventive Polizeiarbeit, geht jedoch einher mit gewichtigen rechtlichen und ethischen Herausforderungen. Der MoTAnsatz verdeutlicht die Grenzen rein datenbasierter Klassifikationen, die soziale Kontexte ausblenden und diskriminierende Muster verstärken können (Asaro 2019, S. 43). Der EoCAnsatz stellt dem eine Perspektive gegenüber, die soziale Ursachen von Kriminalität betont und das Verhältnis zwischen Polizei und Gesellschaft stärker berücksichtigt (Asaro 2019, S. 44). Die Analyse macht deutlich, dass PP nur dann einen nachhaltigen Beitrag zur Kriminalitätsbekämpfung leisten kann, wenn technologische Innovation, klare rechtliche Rahmenbedingungen und ethische Verantwortung zusammenwirken (Mehner et al. 2023, S. 65; Singelnstein 2018, S. 7).

Schlussfolgerungen

Die Analyse zeigt, dass PP die Kriminalitätsbekämpfung im digitalen Raum verändern kann. Diese Veränderung ist jedoch an Bedingungen geknüpft. PP nimmt dabei eine ambivalente Rolle ein. KI-gestützte Verfahren ermöglichen die Analyse großer Datenmengen in Echtzeit. Dadurch können komplexe Angriffsmuster früh erkannt und präventive Maßnahmen vorverlagert werden. Die SWOT-Analyse zeigt, dass insbesondere Effizienzgewinne durch automatisierte Datenverarbeitung und gezielte Ressourcennutzung zentrale Stärken darstellen. Offen bleiben die genaue Anwendung und die Methodik der Mustererkennung im operativen Einsatz. Gleichzeitig bestehen jedoch auch erhebliche Grenzen beim PP. So hängt die Prognosefähigkeit stark von der Datenqualität ab, während Fehlklassifikationen und die Blackbox-Problematik kritisch bleiben. Hinzu kommen rechtliche Unsicherheiten. Profilingbasierte Prognosesysteme sind nach der KI-VO untersagt und nationale Rechtsgrundlagen sind bislang unzureichend. Damit wird deutlich, dass die praktische Implementierung maßgeblich von künftigen gesetzlichen Vorgaben abhängt.

Chancen ergeben sich vor allem aus der Verbindung polizeilicher Daten mit Big-Data-Methoden und OSINT. Dadurch werden neue Kriminalitätsmuster und gesellschaftliche Trends sichtbar. Risiken bestehen in möglichen Verzerrungen, Datenschutzproblemen und einem möglichen Vertrauensverlust in staatliche Institutionen. Die Gegenüberstellung von Models-of-Threat und Ethics-of-Care verdeutlicht, dass technische Effizienz allein nicht ausreicht – die Beziehung zwischen Polizei und Gesellschaft muss mitgedacht werden. Daraus folgt: PP kann die Kriminalitätsbekämpfung im digitalen Raum perspektivisch verändern, indem es präventive Eingriffe und datenbasierte Strategien ermöglicht. Ob diese Veränderung nachhaltig wirksam und gesellschaftlich akzeptiert sein wird, hängt jedoch maßgeblich von rechtlicher Regulierung, technischer Weiterentwicklung und dem Umgang mit ethischer Verantwortung ab.

Literaturverzeichnis

Asaro P M (2019). AI Ethics in Predictive Policing: From Models of Threat to an Ethics of Care, IEEE Technology and Society Magazine, 38(2); 40–53.

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.

Benyon D (2014). Spaces of Interaction, Places for Experience. Synthesis Lectures on Human-Centered Informatics. Cham: Springer.

BKA (Bundeskriminalamt) (2018). Bundeslagebild Cybercrime 2017. Wiesbaden: Bundeskriminalamt.

BKA (Bundeskriminalamt) (2025). Bundeslagebild Cybercrime 2024. Wiesbaden: Bundeskriminalamt.

BMI (Bundesministerium des Innern, für Bau und Heimat) (2021). Cybersicherheitsstrategie für Deutschland 2021. Berlin. bmi.bund.de/SharedDocs/downloads/DE/veroeffentlichungen/2021/09/cybersicherheitsstrategie-2021.pdf (22.12.2025).

Brüning J (2024). Big Data und Künstliche Intelligenz im Strafverfahren, In: Kusche C, Stefanopoulou G (Hrsg.), Digitalisierung als total social fact der Kriminalwissenschaften. BadenBaden: Nomos; 133–150.

BVerfG (Bundesverfassungsgericht) (2020). Urteil vom 19. Mai 2020 – 1 BvR 2835/17, NJW 2020, 2235 (2253), Rn. 192.

Deutscher Ethikrat (2023). Mensch und Maschine – Herausforderungen durch Künstliche Intelligenz. Stellungnahme (Kurzfassung). Berlin: Deutscher Ethikrat.

Drafz J (2025). Einführung in die (Cyber)Viktimologie. Studien zum Umgang mit psychischer Belastung von CybercrimeOpfern. Wiesbaden: Springer.

Egbert S, Leese M (2021). Criminal Futures: Predictive Policing and Everyday Police Work. London/New York: Routledge.

Ernst F, Fähndrich J (2024). Einfach gelagerte Malware-Analysen im Zeitalter generativer KI-Sprachmodelle, Polizei-Informatik; 46–51.

Farthofer H (2023). Künstliche Intelligenz in der Kriminalprävention. In: Rüdiger, T-G, Bayerl, P S (Hrsg.): Handbuch Cyberkriminologie 1: Cyberkriminologie Theorien, Methoden, Erscheinungsformen. Wiesbaden: Springer Fachmedien; 312–317.

FAZ-Institut, Sopra Steria (2024). Cybersecurity im Zeitalter von KI. F.A.Z. Business Media research.

Fricke J (2020). Big Data und künstliche Intelligenz – Chancen und Risiken für die Polizeiarbeit der Zukunft. KSV Polizeipraxis. ksv-polizeipraxis.mwsupport.de/wp-content/uploads/2020/05/Fricke-Big-Data.pdf (20.11.2025).

Grafe J (2025). Möglichkeiten und Grenzen des Strafrechts als Grundrechtsschutz im virtuellen Raum. Baden-Baden: Nomos.

Huber E, Pospisil B (2020). Problematik der Hell- und Dunkelfeldanalyse im Bereich Cybercrime. In: Rüdiger, T -G, Bayerl, P S (Hrsg.): Cyberkriminologie. Kriminologie für das digitale Zeitalter. Wiesbaden: Springer; 109–134.

Jasim A A, Hadi M H (2025). Predictive AI for Identifying Undiscovered Cyber Threats: A Proactive Security Model for Big Data. Open Educational College, Ministry of Education, Iraq.

Kinzig J (2025). Strafgesetzbuch. Kommentar. 31. Auflage. München: C.H.Beck, § 66 Rn. 37–44.

Knobloch T (2018). Vor die Lage kommen. Predictive Policing in Deutschland − Chancen und Gefahren datenanalytischer Prognosetechnik und Empfehlungen für den Einsatz in der Polizeiarbeit. Berlin: Stiftung Neue Verantwortung und Bertelsmann Stiftung.

Krauss P (2023). Künstliche Intelligenz und Hirnforschung. Neuronale Netze, Deep Learning und die Zukunft der Kognition, Berlin: Springer.

Künzli B (2012). SWOT-Analyse: Klassisches Instrument der Strategieentwicklung mit viel ungenutztem Potenzial, Zeitschrift Führung und Organisation (zfo), 81(2); 126–129.

Lum K, Isaac W (2016). To Predict and Serve? Significance 13(5); 14–19.

Marcinkowski J (2023). Die Verbrecher der Zukunft: Wie generative künstliche Intelligenz das wirtschaftskriminelle Handeln vereinfacht. Bachelorarbeit. Mittweida: Hochschule Mittweida.

Mehner C, Fernholz Y, Fabian B, Ermakova T (2023). Predictive Policing: Eine kritische Bestandsaufnahme am Beispiel der Dimension Raum, In: Auth G, Pidun T. (Hrsg.): Rechts- und Verwaltungsinformatik (RVI 2023). Bonn: Gesellschaft für Informatik; 55–67.

Miller C, Arcostanzo F, Smith J, Krasodomski-Jones A, Wiedlitzka S, Jamali R, Dale J (2016). From Brussels to Brexit: Islamophobia, Xenophobia, Racism and Reports of Hateful Incidents on Twitter. Research Prepared for Channel 4 Dispatches – 'Racist Britain'. Centre for the Analysis of Social Media, Demos.

OpenAI (2022). *Introducing ChatGPT*. OpenAI Blog, 30. November 2022. openai.com/blog/chatgpt (22.12.2025).

Povalej R (2017). Mit Big-Data-Analysen gegen Cybercrime – Digitale Spuren entdecken und verbinden. In: Honekamp W, Povalej R (Hrsg.): Polizei-Informatik 2017. Hannover: Polizeiakademie Niedersachsen; 42–49.

Richardson R, Schultz J, Crawford K (2019). Dirty Data, Bad Predictions: How Civil Rights Violations Impact Data, Predictive Policing Systems, and Justice. New York University Law Review Online 192; 193–233.

Rüdiger T-G (2019). *Polizei im digitalen Raum*. Aus Politik und Zeitgeschichte, Bundeszentrale für politische Bildung (bpb), 17. Mai 2019. bpb.de/shop/zeitschriften/apuz/291183/polizei-im-digitalen-raum (23.11.2025).

Rüdiger T-G (2023). Digitale Polizeipräsenz. Die kriminalpräventive Funktion digitaler Polizeipräsenz zwischen virtuellen Polizeistreifen und Kinder-Online-Wachen, SIAK-Journal – Zeitschrift für Polizeiwissenschaft und polizeiliche Praxis, (4); 40–60.

Ruppert F (2023). Predictive policing: Eine methodische und operative Bewertung. In: Rüdiger, T-G and Bayerl, P S (eds.): Handbuch Cyberkriminologie 1: Cyberkriminologie Theorien, Methoden, Erscheinungsformen. Wiesbaden: Springer Fachmedien; 317–365.

Schawel C, Billing F (2018). Top 100 Management Tools. Das wichtigste Buch eines Managers. Von ABC-Analyse bis Zielvereinbarung, 6. Aufl., Wiesbaden: Springer Gabler.

Seidensticker K (2022). Predictive Policing – Eine problembehaftete Methode der Kriminalprävention? In: Diebel-Fischer, H, Hellmig, L, Tischler, M (Hrsg.): Technik und Verantwortung im Zeitalter der Digitalisierung. Rostock: Universität Rostock; 193–218.

Selzer N (2019). Bekämpfung der Organisierten Kriminalität in der digitalen Welt – Kritische Betrachtung des RefE zum IT-Sicherheitsgesetz 2.0., KriPoZ – Kriminalpolitische Zeitschrift, 4(4); 221–230.

Singelnstein T (2018). Predictive Policing: Algorithmenbasierte Straftatprognosen zur vorausschauenden Kriminalintervention, Neue Zeitschrift für Strafrecht (NStZ), 38(1); 1–9.

Steinebach M, Winter C, Halvani O, Schäfer M, Yannikos Y (2015). Chancen durch Big Data und die Frage des Privatsphärenschutzes. Fraunhofer-Institut für Sichere Informationstechnologie SIT, März.

Western Digital (2025). Volumen der jährlich generierten/replizierten digitalen Datenmenge weltweit von 2010 bis 2024 und Prognose für 2029 (in Zettabyte). Statista. Statista GmbH. https://de.statista.com/statistik/daten/studie/267974/umfrage/prognose-zum-weltweit-generierten-datenvolumen/ (10.12.2025).

Wickert C (2025). Predictive Policing. SozTheo. soztheo.de/kriminologie/predictive-policing/ (20.11.2025).

Wollny V, Paul H (2015). Die SWOT-Analyse: Herausforderungen der Nutzung in den Sozialwissenschaften. In: Niederberger, M., Wassermann, S. (Hrsg.): Methoden der Experten- und Stakeholdereinbindung in der sozialwissenschaftlichen Forschung. Wiesbaden: Springer.

Der Einsatz von Diffusionsmodellen zur Erzeugung von Wahllichtbildvorlagen

Sirko Trodler

Der Personenidentifizierung durch Zeugen kommt im Strafverfahren vielfach eine zentrale Bedeutung zu. Regelmäßig ist sie in Ermangelung solider objektiver Beweise das einzige zur Verfügung stehende Mittel zur Gewinnung von Ermittlungsansätzen (Hofmann 2012, S. 19; Köhnken 2009, S. 605). So erscheint es wenig verwunderlich, dass die Wahllichtbildvorlage gemäß den Richtlinien für das Strafverfahren und das Bußgeldverfahren (RiStBV) ein fundamentales Instrument der polizeilichen Ermittlungsarbeit im Vorverfahren darstellt. Sie dient der Überprüfung der Gedächtnisleistung von Zeugen und Geschädigten hinsichtlich der Wiedererkennung des identifizierten Tatverdächtigen. Das Wiedererkennen einer bei einem zeitlich zum Teil deutlich zurückliegenden Ereignis wahrgenommenen Person ist ein komplizierter kognitiver Prozess. Dieser kann auf vielfältige Weise beeinflusst werden und weist daher einen nicht unerheblichen Grad der Fehleranfälligkeit auf (Hofmann 2012, S. 19). Es muss im Interesse aller am Verfahren beteiligten Behörden sein, Erkenntnisse zu Einflussfaktoren zu berücksichtigen und im Rahmen ihrer Möglichkeiten diesen entgegenzuwirken. Die Ermittlung des tatsächlichen Geschehensablaufs ist Kern des Strafprozesses (BVerGE 57, 250 Rn. 73).

Genau das könnte mit dem Einsatz von Künstlicher Intelligenz (KI) auf verschiedenen Wegen erfolgen. Seit den 2010er-Jahren verzeichnet die Entwicklung von KI einen stetigen Aufschwung. Parallel dazu durchdringt die Technologie zunehmend diverse gesellschaftliche Bereiche (Hirsch-Kreinsen & Krokowski 2023, S. 454). KI beeinflusst auch die Polizeiarbeit in Deutschland zunehmend und umfassend. So setzt z. B. Hamburg seit November 2025 in enger Zusammenarbeit mit dem Fraunhofer-Institut die Erprobung einer „Intelligenten Videobeobachtung“ (IVBeo2) am Hansaplatz und Hachmannplatz in der Nähe des Hauptbahnhofs fort. Die Software ist darauf programmiert, frühzeitig auffällige Bewegungen wie Schläge, Tritte oder Stürze zu erkennen (Polizei Hamburg 2025). Darüber hinaus baut Nordrhein-Westfalen seine KI-Infrastruktur sukzessive aus (Landesamt für Zentrale Polizeiliche Dienste NRW 2025) und Bayern nutzt bereits eine Verfahrensübergreifende Recherche- und Analyseplattform (VeRa), um Informationen aus unterschiedlichen polizeiinternen Datenbanken zu verknüpfen und auszuwerten (Bayerische Staatsregierung 2025). In dem folgenden Beitrag soll untersucht werden, ob KI ebenfalls im Bereich der Wahllichtbildvorlagen eingesetzt werden kann. Genauer gesagt, ob der Einsatz von Diffusionsmodellen (DM) bei deren Erzeugung einen relevanten Mehrwert für die Polizeiarbeit bieten kann.

Hintergrund

Um die kriminalistische Methode der Wahllichtbildvorlage mit dem technischen Potenzial von KI zielgerichtet verknüpfen zu können, müssen zunächst zwei Kernaspekte beleuchtet werden. Zum einen die Wahllichtbildvorlage in der Polizeiarbeit mit den regelmäßig durch höchstrichterliche Rechtsprechung formulierten Anforderungen an ihre Durchführung. Und zum anderen der aktuelle Stand und Stellenwert von DM zur Erzeugung synthetischer Bilder. Die Wahllichtbildvorlage ist eine kriminalistische Standardmethode, bei der einem Augenzeugen eine Reihe von Fotografien vorgelegt wird, um einen Tatverdächtigen zu ermitteln

bzw. zu identifizieren (Hofmann 2013, S. 163). Diese Vorlage enthält typischerweise ein Bild des Verdächtigen und mehrere Bilder von sogenannten „Füllpersonen“ (Füllern). Der Zeuge entscheidet bei jedem Bild, ob er den Täter wiedererkennt (Frings 2010, S. 335). Die Anzahl der Vergleichsbilder muss dabei ausreichend groß sein, um das Risiko einer zufälligen Identifikation zu senken (BGH, Beschluss vom 09.11.2011 – Az. 1 StR 524/11, Rn. 6). Das Oberlandesgericht Karlsruhe legte bereits 1983 grundlegende Anforderungen für die Durchführung von Gegenüberstellungen fest, die so noch Bestand haben. Demnach muss eine Wahllichtbildvorlage so durchgeführt werden, dass die Erinnerungsleistung von Zeugen nicht durch äußere Einflüsse verfälscht wird. Die Vergleichspersonen sind anhand der Täterbeschreibung auszuwählen und sollen sich vom Tatverdächtigen in Merkmalen wie Kleidung, Frisur, Körperbau und sonstigem Erscheinungsbild möglichst nicht deutlich abheben. Zudem ist das Verfahren insgesamt so zu gestalten, dass nicht der Eindruck entsteht, der gesuchte Täter sei zwingend unter den gezeigten Personen (OLG Karlsruhe, Beschluss vom 17. März 1983 – 3 HEs 77/83, StV 1984, 9).

Die Entwicklung der KI hat in den letzten Jahren eine bemerkenswerte Transformation durchlaufen. Dabei hat sich der Fokus zunehmend von Modellen, welche darauf trainiert sind, Daten zu klassifizieren oder vorherzusagen, hin zu generativen Modellen verlagert. Vor allem im Anwendungsbereich der Erzeugung hochauflösender Bilder haben sich DM als dominante Technologie etabliert. Vor dem Aufstieg dieser diffusionsbasierten Ansätze wurde das Feld maßgeblich von Variational Autoencoders (VAEs) und Generative Adversarial Networks (GANs) dominiert (Das 2024). Während diese Architekturen oft Kompromisse zwischen Bildqualität und Trainingsstabilität eingehen mussten, bieten DM einen neuen Ansatz, der auf physikalischen Prinzipien der Thermodynamik und stochastischen Differentialgleichungen basiert. Ihre Fähigkeiten beschränken sich nicht auf die bloße Synthese von Bildern. Sie umfassen vielmehr auch anspruchsvolle Restaurierungs- und Manipulationsaufgaben wie das intelligente Auffüllen fehlender oder beschädigter Bildbereiche sowie das Hochskalieren niedrig aufgelöster Bilddaten durch das Hinzufügen plausibler Details (Bergmann & Stryker 2024).

Die konzeptionelle Basis für moderne Diffusionsmodelle wurde von Sohl-Dickstein et al. (2015) gelegt. In ihrer Arbeit „Deep Unsupervised Learning using Nonequilibrium Thermodynamics“ schlugen sie vor, komplexe Datenverteilungen durch einen iterativen Diffusionsprozess langsam zu verrauschen, um anschließend den umgekehrten Prozess zu lernen und so Daten aus Rauschen zu rekonstruieren. Obwohl dieser Ansatz theoretisch elegant war, waren die damals erzielten Ergebnisse in der Bildgenerierung noch nicht wettbewerbsfähig gegenüber den etablierten Methoden. Der entscheidende Wendepunkt erfolgte durch die Arbeit von Ho et al. (2020) mit „Denoising Diffusion Probabilistic Models“ (DDPM). Die Autoren verknüpften den ursprünglichen Ansatz von Sohl-Dickstein et al. (2015) mit Score Matching und Langevin-Gleichung. Im Ergebnis erreichten DDPMs erstmals eine Bildqualität, die mit GANs konkurrieren konnte, wiesen jedoch noch langsamere Inferenzzeiten auf, da der iterative Entrauschungsprozess, oft mit tausenden Schritten, rechenintensiv war. Rombach et al. (2022) lösten dieses Problem mit ihrer Arbeit „High-Resolution Image Synthesis with Latent Diffusion Models“. Anstatt Pixel direkt zu entrauschen, nutzte das Modell einen Autoencoder, um Bilder in einen komprimierten Latent Space zu projizieren. Der Diffusionsprozess fand in diesem effizienten latenten Raum mit deutlich reduziertem Rechenaufwand ohne Qualitätsverlust statt.

Um diese Modelle zur Bilderzeugung, also zur Inferenz, nutzen zu können, müssen sie mit der Anwendereingabe, i. d. R. Text oder Bild, logisch verbunden werden. Dazu werden aber keine reinen Large Language Models (LLMs), sondern Modelle wie Contrastive Language-Image Pretraining (CLIP) genutzt. CLIP wurde trainiert, Text und Bilder in denselben mathematischen Raum zu projizieren. Das Modell verknüpft also, wie ein Bild aussieht, mit der dazu passenden Textbeschreibung. Die technische Brücke zwischen dem Text und dem Bildgenerierungsprozess ist der Cross-Attention-Mechanismus im U-Net, dem bildgebenden neuronalen Netz. Während das U-Net das Rauschen entfernt, sorgt es gleichzeitig für die mathematische Darstellung von Text als Zahlenvektoren. Durch Matrixmultiplikation werden die visuellen Eigenschaften im Latent Space direkt mithilfe der semantischen Informationen des Textes gesteuert (Kontaratou & Braithwaite 2024).

Material und Methodik

Das Ziel dieses Beitrags ist es, den potenziellen Mehrwert des Einsatzes von DM bei der Erstellung von Wahllichtbildvorlagen für die polizeiliche Ermittlungsarbeit zu bewerten. Da es sich hierbei um die strategische Analyse einer neuartigen technologischen Anwendung in einem etablierten Prozess handelt, wurde als zentrale Methode die SWOT-Analyse verwendet. Diese Methode des strategischen Managements eignet sich, um eine umfassende und strukturierte Bewertung vorzunehmen. Sie ermöglicht eine systematische Gegenüberstellung von internen und externen Faktoren, um darauf aufbauend strategische Schlussfolgerungen zu ziehen. SWOT steht hierbei für Strengths (Stärken), Weaknesses (Schwächen), Opportunities (Chancen) und Threats (Risiken) und bezeichnet damit gleichzeitig die zu untersuchenden Kernaspekte (Paul & Wollny 2015, S. 189).

Das methodische Vorgehen gliederte sich in mehrere Schritte. Im ersten Schritt wurde eine Literatur- und Dokumentenanalyse durchgeführt (Fleig 2024). Dabei wurde auf primär wissenschaftliche Veröffentlichungen aus der Informatik und der KI-Forschung sowie auf Internet- und Zeitschriftenartikel zurückgegriffen. Der Fokus lag dabei auf Arbeiten zu DM, deren Entwicklung und technischen Hintergründen sowie aktuellen Entwicklungen. Insbesondere wurden Arbeiten verwendet, die sich mit der Synthese von Gesichtsabbildungen und mit für Wahllichtbildvorlagen relevanten Aspekten beschäftigten. Im zweiten Schritt wurden die gesammelten Informationen in einer Matrix, welche die vier Felder Stärken, Schwächen, Chancen und Risiken darstellt, strukturiert. Diese Visualisierung dient dazu, die Wechselwirkungen zwischen den internen Gegebenheiten der Technologie (Stärken, Schwächen) und den externen Rahmenbedingungen (Chancen, Risiken) des Anwendungsfalls klar herauszuarbeiten. Im letzten Schritt wurden basierend auf der ausgefüllten Matrix strategische Stoßrichtungen abgeleitet, um den potenziellen Mehrwert zu bewerten (Tsion 2024). Hierfür wurden die Felder der Matrix kombiniert und diskutiert, wie Stärken genutzt werden können, um die Chancen im polizeilichen Prozess zu maximieren und um Risiken abzuwehren. Und wie Schwächen durch die Nutzung von Chancen kompensiert werden und wo Schwächen auf Risiken stoßen können (Künzli 2012, S. 127). Das Ziel des Beitrags ist erreicht, wenn eine ausgewogene Bewertung, die sowohl die positiven Potenziale als auch die signifikanten Risiken und Hürden benennt, des potenziellen Mehrwerts erfolgen kann.

Ergebnisse

Die Anwendung der SWOT-Analyse zur Bewertung des Einsatzes von DM für die Erstellung von Wahllichtbildvorlagen führt zu den folgenden Ergebnissen. Deren Einzelpunkte stellen dabei keineswegs gleichgewichtete, gegeneinander aufrechenbare Argumente dar. Vielmehr ist es erforderlich, sie individuell mit eigener Gewichtung zu betrachten.

Stärken

In einer Untersuchung führten Wahllichtbildvorlagen mit KI-generierten Füllern zu einer perfekt fairen und weniger voreingenommenen Auswahl des Verdächtigen im Vergleich zu traditionellen Vorlagen, die Füller aus Datenbanken nutzten (Bell et al. 2024). Gleichzeitig kann damit das Problem gelöst werden, überhaupt erst passende Füller zu finden (Dokoupil & Peska 2021). Während es aktuell schwierig sein kann, für bestimmte Gesichtsmerkmale wie Narben oder Tattoos passende Füller zu finden, die dem Tatverdächtigen in den übrigen Merkmalen ebenfalls gleichen, können diese mit KI nahezu unbegrenzt generiert werden (Bell et al. 2024). Beschränkungen, die durch die limitierte Größe und Diversität polizeilicher Datenbanken entstehen, werden dadurch eliminiert.

Text-to-Image-Generierung erlaubt es, Füller direkt auf Basis der verbalen Zeugenbeschreibung des Täters zu generieren. Dies entspricht der psychologischen Forderung nach einer beschreibungsbasierten statt verdächtigtenbasierten Füllerauswahl (Colloff et al. 2021). Moderne DM ermöglichen eine gezielte, attributbasierte Steuerung der generierten Gesichter. Die Technologie ermöglicht es, eine verbale Beschreibung, wie sie ein Augenzeuge liefert, direkt in ein Bild zu übersetzen. Ein Ermittler könnte die Zeugenbeschreibung „Mann, ca. 40, mit Bart, schmaler Nase“ als Text-Prompt verwenden, um eine unbegrenzte Anzahl entsprechender Füller zu generieren (Ergasti et al. 2025, S. 349 f.). Darüber hinaus kann der Einsatz von KI die Persönlichkeitsrechte Dritter schützen, und zwar unbeteiligter Personen, die als Füller dienen müssten. Da die KI-Füller synthetisch sind und keine realen Personen mehr abbilden, müssten Ermittlungsbehörden nicht mehr in das Recht auf informationelle Selbstbestimmung der Füller eingreifen. Denn die Verwendung und auch nur kurzzeitige Weitergabe von Lichtbildern gegen den Willen bzw. ohne das Wissen des Betroffenen ist ein Eingriff in eben jenes Grundrecht (BVerfGE 65, 1 Rn. 147).

Die Modelle erzeugen hochgradig fotorealistische Bilder, die für Menschen oft nicht mehr von echten Fotos unterscheidbar sind. Eine Studie aus 2025 mit über 50.000 Teilnehmern untersuchte systematisch, wie präzise Menschen synthetische von echten Fotos unterscheiden können. Die Ergebnisse zeigen, dass die menschliche Detektionsgenauigkeit bei etwa 61 % liegt, also nahe dem Zufallsniveau von 50 %. Die Macher der Studie beschränkten sich dabei nicht auf Bilder, die besonders schwer zu erkennen waren, sondern nutzten eine breite Auswahl. Besonders schwierig war die korrekte Unterscheidung von Bildern, die zwar realistisch, aber nicht professionell wirkten (Roca et al. 2025).

Schwächen

DM werden oft auf unfiltrierten Internet-Datensätzen trainiert. Studien zeigen, dass sie bestehende gesellschaftliche Stereotype, z. B. Ethnie oder Geschlecht, nicht nur widerspiegeln, sondern verstärken oder verschlimmern (Jiang et al. 2023; Perera & Patel 2023). Die Modelle neigen dazu, stereotype Assoziationen zu lernen. Das tun sie, indem sie bestimmte Berufe systematisch mit einem Geschlecht assoziieren, niedrige Positionen mit Frauen, hochrangige Positionen mit Männern. Ein weiteres Beispiel für diese algorithmische Voreingenommenheit (Bias) ist die Assoziation zwischen Verbrechen und schwarzen Menschen sowie zwischen Terrorismus und Menschen aus dem Nahen Osten. Gleichzeitig zeigen die Modelle auch rassische Bias-Muster, die systematisch Minoritäten mit niedrig bezahlten oder gefährlichen Berufen verknüpfen (AlDahoul et al. 2025, S. 8 f.). Problematisch ist vor allem, dass die Modelle dadurch weniger diverse Ergebnisse liefern können (Friedrich et al. 2024).

Die psychologische Forschung deutet darauf hin, dass künstlich generierte Gesichter schwerer zu merken und weniger leicht zu unterscheiden sind als echte Gesichter. In zwei Experimenten stellten Forscher fest, dass Menschen künstliche Gesichter behandeln wie Out-Group-Gesichter. Also Gesichter anderer Ethnien oder Altersgruppen, für die wir schlechtere Erkennungs- und Erinnerungsfähigkeiten haben (Balas & Pacella 2015, S. 335). Das deutet darauf hin, dass KI-generierte oder digitale Füller auch in Wahllichtbildvorlagen durch Zeugen schwerer voneinander zu unterscheiden sind, was dazu führen könnte, dass das reale Bild heraussticht.

Die komplexen neuronalen Netze sind oft Blackboxes. Ihre Entscheidungsprozesse sind für Menschen und damit für Gerichte nur schwer nachvollziehbar oder erklärbar. DM gehören zu den komplexesten generativen Systemen in der modernen KI. Das grundlegende Problem dabei ist, dass es selbst für Experten schwierig ist nachzuvollziehen, wann und wie die Modelle spezifische visuelle Konzepte während dieses Prozesses generieren (Park et al. 2024). Deutsche Gerichte folgen dem Überzeugungsprinzip (§ 261 StPO), wodurch Richter ihre freie Überzeugung aus der Gesamtheit des Verfahrens bilden. Allerdings muss dieses Vertrauen auf transparenten und überprüfbaren Grundlagen basieren (Artkämper 2009).

Die produktive Nutzung von DM ist mit erheblichen infrastrukturellen Anforderungen verbunden. Insbesondere die Skalierbarkeit dieser Systeme stellt Herausforderungen dar, da variable Latenzzeiten und intensiver Speicherbedarf die nahtlose Integration in vorhandene IT-Infrastrukturen komplizieren (Zheng 2025). Neben technischen Infrastruktur-Fragen müssen auch Aspekte der Anwendenden sowie die Förderung ihrer Akzeptanz gegenüber neuen technologischen Werkzeugen Berücksichtigung finden (Wangler & Botthof 2019, S. 122). Europol (2024) betont in ihrem Bericht zu KI und Polizei explizit, dass Polizeibehörden erheblich in Training und Bewusstseinsschulung ihrer Mitarbeitenden investieren müssen, um KI-Systeme verantwortungsvoll einsetzen zu können.

Chancen

Der Prozess der Vorlagenerstellung könnte deutlich verkürzt werden. Während aktuell noch manuell nach passenden Vergleichsbildern gesucht werden muss, um diese in der Wahllichtbildvorlage zusammenzustellen, kann dieser Prozess, je nachdem, wie performant die Architektur gestaltet wird, softwaregestützt nahezu unverzüglich erfolgen (Greenspan & Bergold

2025). Zugleich ließe sich mit KI bspw. durch Large Language and Vision Assistant (LLaVA) vom vorhandenen Bild des Tatverdächtigen eine detaillierte Beschreibung extrahieren und ein Prompt erstellen (Ding et al. 2024), der zur Erzeugung von beliebig vielen KI-Füllern genutzt werden kann. Studien zeigten, dass LLaVA-generierte Prompts die semantische Genauigkeit bei der Bildgenerierung signifikant verbesserten, da sie komplexe Attribute besser erfassten als reine Schlagwortlisten. Die forensische Wissenschaft könnte von einer KI zur Erstellung von Wahllichtbildern ebenfalls profitieren. Es existieren bereits Forschungen zur Simulation von Alterungsprozessen für Fahndungsbilder (Chen & Lathuilière 2023) oder der Erstellung von Phantombildern (Jain et al. 2024). Ein zur Erstellung von Wahllichtbildvorlagen trainiertes Modell könnte mithilfe von Low-Rank Adaptations (LoRAs) auf die Eigenart dieser Anwendungsfälle spezialisiert werden. LoRAs sind leichtgewichtige Modellanpassungen, mit denen das Basismodell für konkrete Anwendungsfälle angepasst werden kann (Hu et al. 2021).

Die Rechtspsychologie fordert seit Langem die Eliminierung menschlicher, suggestiver Einflüsse auf den Prozess der Wahllichtbildvorlage allgemein (Jünemann 2016, S. 2). Ein standardisierter, dokumentierter Prozess zur Füllerauswahl kann zudem den potenziellen subjektiven Einfluss des Ermittlers reduzieren. Menschliche Intuitionen bei der Auswahl der Füller sind anfällig für kognitive Verzerrungen durch Emotionen oder Heuristiken (Engelke 2025). Die Entwicklung von DM schreitet unaufhaltsam voran. Sie sind in der praktischen Anwendung bereits erfolgreich, theoretisch und technisch jedoch keineswegs ausgereift. Aktuelle Forschung konzentriert sich darauf, die Modelle noch schneller und effizienter zu machen. Effizientere Sampler mit weniger Diffusionsschritten, verbesserte Steuerungsmechanismen, robustere und erklärbare Modelle mit besseren Sicherheitseigenschaften sind nur einige der zukünftigen Entwicklungsschritte (Croitoru et al. 2023). Ein Beispiel ist das Hybrid Autoregressive Transformer-Modell von NVIDIA und dem MIT, das autoregressive Methoden für eine schnelle Grundstruktur mit einem kleinen Diffusionsmodell zur Verfeinerung kombiniert. Dies ermöglicht eine schnelle Generierung bei gleichzeitig hoher Qualität und macht den Einsatz auf alltäglicher Hardware wie Laptops oder Smartphones denkbar (Tang et al. 2024).

Risiken

Eine zentrale Bedrohung ist die unklare Rechtslage. Es ist nicht gerichtlich geklärt, ob ein mittels KI erzeugtes synthetisches Bild als Bestandteil eines Beweismittels im deutschen Strafprozess zulässig ist, da hierzu noch keine Rechtsprechung vorliegt. Gerichte könnten diese wie bei anderen neuen Technologien zur Beweisführung anzweifeln, solange bestimmte Fragen nach Trainingsdaten und möglichen Bias nicht hinreichend geklärt sind. So könnten Verfahren, deren Täteridentifizierung sich ausschließlich auf die Wiedererkennung durch einen Zeugen in der Wahllichtbildvorlage stützen, vor Gericht nicht bestehen (Brodowski & Zettelmeier 2025).

Der Einsatz von KI-Systemen zur Erstellung von Wahllichtbildvorlagen könnte unter die KI-Verordnung der Europäische Union (2025) (EU KI-VO) fallen und als Hochrisiko-KI-System eingestuft werden. Gemäß Anhang III, Abschnitt 6 der Verordnung gelten KI-Systeme, die von oder im Namen von Strafverfolgungsbehörden eingesetzt werden, um die Verlässlichkeit von Beweismitteln im Rahmen der Ermittlung oder Verfolgung von Straftaten zu bewerten, als hochriskant. Da Wahllichtbildvorlagen ein wesentliches Ermittlungsinstrument zur Identifizierung von Tatverdächtigen darstellen und deren Ergebnisse als Beweismittel

in Strafverfahren herangezogen werden können, könnte ein KI-gestütztes System zur Generierung solcher Vorlagen in diesen Anwendungsbereich fallen. Dies hätte zur Folge, dass die Polizei umfangreiche Compliance-Anforderungen, wie die Einführung eines Risikomanagementsystems, die Gewährleistung hochwertiger Trainingsdaten zur Vermeidung von Bias, die Sicherstellung menschlicher Aufsicht (Human-in-the-Loop), detaillierte Dokumentation und Transparenz, erfüllen müsste. Ein weiterer Konflikt entsteht zwischen den Transparenzanforderungen der KI-Regulierung und der psychologischen Notwendigkeit der Täuschungsfreiheit im Wiedererkennungsprozess. Die EU KI-VO sieht in Artikel 50 vor, dass die Nutzer über die Interaktion mit einem KI-System informiert werden müssen und KI-generierte Inhalte als solche gekennzeichnet werden. Würde der Zeuge jedoch vor der Vorlage darüber informiert, dass die Füllerbilder künstlich generiert wurden, oder würden die entsprechenden Bilder auch noch explizit gekennzeichnet sein, wäre ein Einfluss auf die psychologische Integrität des Tests zumindest zu vermuten. Forschung hierzu steht aus. DM werden auf massiven Datensätzen trainiert, die oft ohne Zustimmung aus dem Internet geladen wurden. Dies wirft ernsthafte Datenschutzbedenken auf, insbesondere wenn Gesichter realer Personen in den Trainingsdaten enthalten sind und möglicherweise in generierten Ausgaben rekonstruiert werden können (Avey 2023; Deambrosi 2025).

Diskussion

Die Ergebnisse der SWOT-Analyse zeigen ein Spannungsfeld zwischen dem hohen technischen Potenzial von DM und den juristischen und praktischen Hürden für ihren Einsatz bei der Erstellung von Wahllichtbildvorlagen. Die folgende Matrix stellt diese Ergebnisse gegenüber.

Stärken	Schwächen
• Steigerung der methodischen Fairness • Unbegrenzte Anzahl • Text-zu-Bild-Synthese • Persönlichkeitsrechte • Fotorealismus	• Bias • Out-Group-Effekt • Intransparenz („Blackbox“) • Integration und Akzeptanz
Chancen	**Risiken**
• Automatisierung • Standardisierung und Objektivierung • Multidisziplinäre Anwendungen • Stetige Weiterentwicklung	• Reaktion der Gerichte • EU KI-VO • Transparenzpflicht • Urheberrechtliche Fragen

Eigene Abbildung: SWOT-Analyse zum Einsatz von DM bei der Erzeugung von Wahllichtbildvorlagen

Das größte Potenzial liegt in der Nutzung der hohen Bildqualität und Effizienz zur Steigerung der prozeduralen Fairness und Objektivität. Ein System, das auf Knopfdruck eine unbegrenzte Anzahl an ideal passenden, fotorealistischen Füllern generieren kann, hat das Potenzial, den Ermittlungsprozess fairer und wissenschaftlich fundierter zu gestalten. Ein potenzieller Mehrwert liegt außerdem in der Fähigkeit zur präzisen Steuerung der Füller. Hierdurch können die oft schwer zu erfüllenden juristischen und psychologischen Anforderungen an optimale Ähnlichkeit in relevante und maximale Unähnlichkeit in irrelevanten Merkmalen besser erfüllt werden als mit statischen Datenbanken. Zudem wird der Schutz der Rechte unbeteiligter Dritter durch die Generierung synthetischer Identitäten gewährleistet (Bell et al. 2024).

Die gravierendste Herausforderung ergibt sich aus der Kombination von technologischen Schwächen mit externen Risiken. Die noch inhärente Künstlichkeit der Bilder trifft auf die hohe Wahrscheinlichkeit einer juristischen Anfechtung. Solange nicht zweifelsfrei geklärt ist, dass ein solches Verfahren vor Gericht standhält und dass die synthetischen Bilder das Erinnerungsvermögen eines Zeugen nicht auf unvorhergesehene Weise beeinflussen, eben durch den beschriebenen Out-Group-Effekt, ist ein Praxiseinsatz mit einem untragbaren Risiko für das gesamte Ermittlungsverfahren verbunden. Ein Fehlurteil aufgrund eines erfolgreich angefochtenen Beweismittels wäre die Konsequenz (van Velkinburgh et al. 2023).

Die Schwäche des algorithmischen Bias in Trainingsdaten könnte durch Standardisierung im Modell-Training gemindert werden. Für standardisiertes Training müssten jedoch offizielle, sorgfältig kuratierte und auditierte Bilddatensätze erstellt werden, um eine faire Repräsentation aller Gruppen zu gewährleisten. Damit könnte zeitgleich möglichen Urheberrechtsbedenken begegnet werden. Die Alternative zur Nutzung eines selbsttrainierten Modells ist der Rückgriff auf verantwortungsvoll trainierte Modelle wie Flux.2 des deutschen Unternehmens Black Forest Labs. Eine einfachere Lösung dafür bieten Friedrich et al. (2024) mit ihrem „Fair Diffusion“. Damit lassen sich Bias jedweder DM ohne weiteres Training oder Datenfiltrierung abschwächen.

Die Implementierung in die IT-Infrastruktur und die Arbeitsabläufe der verschiedenen Polizeien in Deutschland ist unbenommen eine enorme logistische und finanzielle Hürde. Das Bund-Länder-Programm P20 wirkt prädestiniert, um diese Hürde zu überwinden. P20 hat den Anspruch, die polizeiliche Informationstechnik in Deutschland umfassend zu modernisieren und auf eine einheitliche Grundlage zu stellen. Im Jahr 2025 konnten bereits bedeutsame Meilensteine realisiert werden, darunter die Inbetriebnahme einer zentralen Datenverwaltungsplattform, dem Datenhaus, sowie die pilothafte Implementierung mehrerer KI-gestützter Lösungen (Bundesministerium des Innern 2025). Die Einbettung des Prozesses in die individuellen Arbeitsabläufe hingegen darf nicht als einmalige Einführung, sondern muss als iterativer Lernprozess verstanden werden (Takian et al. 2014, S. 205). Führungskräfte müssen den Veränderungsbedarf klar kommunizieren, Sinn und Nutzen der Technologie für Mitarbeiter nachvollziehbar machen und Widerstände ernst nehmen (Weinberg 2025).

Auf die Einordnung, ob der Einsatz von DM zur Erstellung von Wahllichtbildvorlagen unter die EU KI-VO fällt oder gar als Hochrisiko-System eingestuft wird, muss an dieser Stelle verzichtet werden. Eine konkrete Abwägung würde zum einen den Rahmen sprengen und wäre zum anderen nur aufgrund der abstrakten Vorstellungen zur Software nicht seriös möglich. Nichtsdestoweniger verbleiben die Einstufung und die Kennzeichnungspflicht für diesen Fall ein enormes Risiko.

Diese Analyse unterliegt mehreren Einschränkungen. Die Bewertung basiert auf einer theoretischen Anwendung der SWOT-Analyse und einer Literaturrecherche in angrenzenden Feldern. Das Feld der generativen KI entwickelt sich schnell. Technische Schwächen könnten in zukünftigen Modellgenerationen bereits behoben sein, während neue, heute noch unbekannte Probleme auftreten könnten. Höchst richterliche Rechtsprechung bezüglich der Klärung, ob und unter welchen Bedingungen synthetische Medien als Teil einer Wahllicht-

bildvorlage zulässig sind, fehlt bisher. Darüber hinaus ersetzt diese Analyse keine Technikfolgeabschätzung, detaillierte Risikoanalyse und empirische Validierungsstudie, die für eine tatsächliche Implementierung notwendig wären.

Schlussfolgerungen

Die vorliegende Analyse hat gezeigt, dass der Einsatz von DM zur Erstellung von Wahllichtbildvorlagen ein zweischneidiges Schwert ist. Einerseits bietet die Technologie das beeindruckende Potenzial, die Identifizierung von Tatverdächtigen mittels Wahllichtbildvorlage objektiver und effizienter zu gestalten. Andererseits ist dieser potenzielle Mehrwert untrennbar mit fundamentalen juristischen und methodischen Risiken verbunden, die einem sofortigen Einsatz in der polizeilichen Sachbearbeitung entgegenstehen.

Ein unmittelbarer und vor allem unregulierter Einsatz der Technologie in Ermittlungsverfahren ist zum jetzigen Zeitpunkt abzulehnen. Das Risiko, dass Beweismittel aufgrund der synthetischen Natur der Füllpersonen juristisch angefochten und verworfen werden, ist zu hoch. Stattdessen sollten Polizeibehörden im Rahmen des Programms P20 ein Pilotprojekt in einem kontrollierten, nicht operativen Rahmen initiieren und die Entwicklung weiterhin verfolgen. So können Erfahrungen mit der Technologie gesammelt werden, ohne laufende Verfahren zu gefährden. Bestehende ähnliche Verfahren könnten als Anknüpfungspunkt für eine Weiterentwicklung dienen − etwa die in NRW im Erlass Wahllichtbildvorlage im Strafverfahren (2006) geregelte Verfremdung von Bildern sowie die Nutzung von Datenbanken für fiktive Personen in Wahllichtbildvorlagen.

Polizeiliche Lehr- und Forschungseinrichtungen wie das Sächsische Institut für Polizei- und Sicherheitsforschung (SIPS) oder die Deutsche Hochschule der Polizei (DHPol) sind prädestiniert dafür, interdisziplinär auf offene Fragestellungen zu reagieren. Denn diese könnten Juristen, Kriminalisten, Psychologen und Informatiker zusammenbringen, um Lücken im Verfahren systematisch zu betrachten. Hier könnte z. B. untersucht werden, wie „robuste“ synthetische Bilder erzeugt werden können, die dann keinen Anlass für Anfechtungen geben, oder wie der gesamte Erstellungsprozess fälschungssicher dokumentiert werden kann. Zudem könnten rechtswissenschaftliche Untersuchungen klären, welche Anforderungen die Strafprozessordnung und die Rechtsprechung an den Einsatz solcher Technologien stellen. Dabei ließen sich Parallelen zu anderen computergestützten Beweismitteln ziehen und die spezifischen Herausforderungen durch generative KI herausarbeiten. Zusammenfassend lässt sich sagen, dass der Einsatz generativer KI in der Strafverfolgung großes Potenzial bietet, aber anspruchsvoll ist. Der Weg zu einer verantwortungsvollen Implementierung erfordert noch einiges an Forschungs- und Entwicklungsarbeit. Es ist jedoch strategisch notwendig, diesen Weg jetzt zu gehen, um zukünftige Chancen zu nutzen und gleichzeitig die Rechtsstaatlichkeit zu wahren.

Literaturverzeichnis

AlDahoul N, Rahwan T, Zaki Y (2025). AI-generated faces influence gender stereotypes and racial homogenization. Scientific Reports, 15(14449); 1–15. doi.org/10.1038/s41598-025-99623-3 (20.12.2025).

Artkämper D H (2009). Qualitätsstandards bei Lichtbildvorlagen und Identifizierungsgegenüberstellungen. kriminalpolizei.de/ausgaben/2009/juni/detailansicht-juni/artikel/qualitaetsstandards-bei-lichtbildvorlagen-und-identifizierungsgegenueberstellungen.html (25.08.2025).

Avey C (2023). Ethical Pros and Cons of AI Image Generation. computer.org/publications/tech-news/community-voices/ethics-of-ai-image-generation (20.12.2025).

Balas B, Pacella, J (2015). Artificial faces are harder to remember. Computers in Human Behavior, 52; 331–337. doi.org/10.1016/j.chb.2015.06.018 (20.12.2025).

Bayerische Staatsregierung (2025). Herrmann: VeRA ist sinnvoll und notwendig. bayern.de/herrmann-vera-ist-sinnvoll-und-notwendig/ (03.12.2025).

Bell R, Menne N M, Mayer C, Buchner A (2024). On the advantages of using AI-generated images of filler faces for creating fair lineups. Scientific Reports, 14(12304); 1–10. doi.org/10.1038/s41598-024-63004-z (20.12.2025).

Bergmann D, Stryker C (2024). What are diffusion models? ibm.com/think/topics/diffusion-models (12.11.2025).

Brodowski D, Zettelmeier A (2025). Zweifel am Beweiswert digitaler Skelette. lto.de/recht/hintergruende/h/strafverfahren-budapest-komplex-3d-modell-ki-berechnung-beweis (20.12.2025).

Bundesministerium des Innern (2025). P20 Polizei 20/20. bmi.bund.de/DE/themen/sicherheit/programm-p20/programm-p20-node.html (20.12.2025).

Chen X, Lathuilière S (2023). Face Aging via Diffusion-based Editing. doi.org/10.48550/arXiv.2309.11321 (18.11.2025).

Colloff M F, Wilson B M, Seale-Carlisle T M, Wixted J T (2021). Optimizing the selection of fillers in police lineups. Proceedings of the National Academy of Sciences, 118(8); e2017292118 doi.org/10.1073/pnas.2017292118 (20.12.2025).

Croitoru F, Hondru V, Ionescu R T, Shah M (2023). Diffusion Models in Vision: A Survey. IEEE transactions on pattern analysis and machine intelligence, 49(9); 10850–10869 doi.org/10.1109/TPAMI.2023.3261988 (20.12.2025).

Das A (2024). Building Diffusion Model's theory from ground up. iclr-blogposts.github.io/2024/blog/diffusion-theory-from-scratch/ (08.12.2025).

Deambrosi A (2025). Ethical Concerns Raised by AI Images and Video. imgix.com/blog/8-ethical-concerns-raised-by-ai-images-and-video (20.12.2025).

Ding Z, Li P, Yang Q, Li S (2024). Enhance Image-to-Image Generation with LLaVA-generated Prompts. 2024 5th International Conference on Information Science, Parallel and Distributed Systems (ISPDS). Guangzhou; 77–81. doi.org/10.1109/ISPDS62779.2024.10667513 (20.12.2025).

Dokoupil P, Peska L (2021). LiGAN: Recommending Artificial Fillers for Police Photo. CEUR Workshop Proceedings, 2960(14). ceur-ws.org/Vol-2960/paper14.pdf (20.12.2025).

Eisenberg U (2008). Beweisrecht der StPO: Spezialkommentar, 6. Auflage. C.H.Beck, München.

Engelke L S (2025). Kognitive Verzerrungen: Die Denkfallen unseres Gehirns. scilogs.spektrum.de/hirn-und-weg/kognitive-verzerrungen-die-denkfallen-unseres-gehirns/ (03.12.2025).

Ergasti A, Ferrari C, Fontanini T, Bertozzi M, Prati A (2025). Controllable Face Synthesis with Semantic Latent Diffusion Models. In: Palaiahnakote S, Schuckers S, Ogier J-M, Bhattacharya P, Pal U, Bhattacharya S (Hrsg.): Pattern Recognition. ICPR 2024 International Workshops and Challenges. Springer Nature Switzerland, Cham; 337–352 (20.12.2025).

Europol (2024). AI and policing: The benefits and challenges of artificial intelligence for law enforcement. Publications Office of the European Union, Luxemburg. doi.org/10.2813/0321023 (20.12.2025).

Fleig D J (2024). So wird eine SWOT-Analyse erstellt. business-wissen.de/artikel/swot-analyse-so-wird-eine-swot-analyse-erstellt (30.08.2025).

Friedrich F, Brack M, Struppek L, Hintersdorf D, Schramowski P, Luccioni S, Kersting K (2024). Auditing and instructing text-to-image generation models on fairness. AI and Ethics, 5(3); 2103–2123 doi.org/10.1007/s43681-024-00531-5 (20.12.2025).

Frings C (2010). Studienbegleitskript zum Thema Wiedererkennungsverfahren. Kriminalistik, 5; 332–336.

Greenspan R L, Bergold A N (2025). Can AI-generated faces serve as fillers in eyewitness lineups? Memory, 33(4); 416–429 doi.org/10.1080/09658211.2025.2467134 (20.12.2025).

Hirsch-Kreinsen H, Krokowski T (2023). Technologieversprechen Künstliche Intelligenz. Vergangene und gegenwärtige Konjunkturen in der Bundesrepublik. Berliner Journal für Soziologie, 33; 453–484 doi.org/10.1007/s11609-023-00504-1 (20.12.2025).

Hofmann A (2013). Personenidentifizierung durch Zeugen im Strafverfahren. Duncker & Humblot, Berlin.

Ho J, Jain A, Abbeel P (2020). Denoising Diffusion Probabilistic Models. Advances in Neural Information Processing Systems 33 (NeurIPS 2020), 33; 6840−6851 (20.12.2025).

Hu E J, Shen Y, Wallis P, Allen-Zhu Z, Li Y, Wang S, Wang L, Chen W (2021). LoRA: Low-Rank Adaptation of Large Language Models. doi.org/10.48550/arXiv.2106.09685 (13.12.2025).

Jain K K, Grosz S, Namboodiri A M, Jain A K (2024). CLIP4Sketch: Enhancing Sketch to Mugshot Matching through Dataset Augmentation using Diffusion Models. 2024 IEEE International Joint Conference on Biometrics (IJCB). IEEE, Buffalo doi.org/10.1109/IJCB62174.2024.10744467 (20.12.2025).

Jiang Y, Lyu Y, Ma T, Peng B, Dong J (2023). RS-Corrector: Correcting the Racial Stereotypes in Latent Diffusion Models. arxiv.org/html/2312.04810v2 (03.12.2025).

Jünemann A-K (2016). Wie sich Fehler bei polizeilichen Gegenüberstellungen vermeiden lassen. In: Brodbeck F C (Hrsg.): Evidenzbasierte Wirtschaftspsychologie, (11). Ludwig-Maximilians-Universität München psy.lmu.de/evidenzbasiertesmanagement/dokumente/ebm_dossiers/ebm_11_gegenueberstellungen.pdf (20.12.2025).

Kontaratou D A, Braithwaite L (2024). Text-to-image: latent diffusion models. nicd.org.uk/knowledge-hub/image-to-text-latent-diffusion-models (15.11.2025).

Künzli B (2012). SWOT-Analyse. Ein klassisches Instrument der Strategieentwicklung mit viel ungenutztem Potenzial. Zeitschrift Führung + Organisation, 81(2); 126−129 web.archive.org/web/20181102164639/http://www.clc-consulting.ch/fileadmin/CONTENT/SWOT_Analyse_Benjamin_Kuenzli.pdf (20.12.2025).

Landesamt für Zentrale Polizeiliche Dienste NRW (2025). Polizei baut eigene KI-Infrastruktur aus. lzpd.polizei.nrw/presse/polizei-baut-eigene-ki-infrastruktur-aus (03.12.2025).

Park J-H, Ju Y-J, Lee S-W (2024). Explaining generative diffusion models via visual analysis for interpretable decision-making process. Expert Systems with Applications, 248(123231) doi.org/10.1016/j.eswa.2024.123231 (20.12.2025).

Perera M V, Patel V M (2023). Analyzing Bias in Diffusion-based Face Generation Models. 2023 IEEE International Joint Conference on Biometrics (IJCB). IEEE, Ljubljana. doi.org10.48550/arXiv.2305.06402 (20.12.2025).

Polizei Hamburg (2025). Erprobung „Intelligenter Videobeobachtung“ in Hamburg wird fortgesetzt. polizei.hamburg/erprobung-intelligenter-videobeobachtung-in-hamburg-wird-fortgesetzt-1112894 (03.12.2025).

Roca T, Roman A C, Vega J T, Duarte M, Wang P, White K, Misra A, Ferres J L (2025). How good are humans at detecting AI-generated images? Learnings from an experiment. arxiv.org/html/2507.18640v1 (15.11.2025).

Rombach R, Blattmann A, Lorenz D, Esser P, Ommer B (2022). High-resolution image synthesis with latent diffusion models. 2022 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR), New Orleans; 10674–10685. doi.org/10.1109/CVPR52688.2022.01042 (20.12.2025).

Sohl-Dickstein J, Weiss E A, Maheswaranathan N, Ganguli S (2015). Deep Unsupervised Learning using Nonequilibrium Thermodynamics. Proceedings of the 32nd International Conference on Machine Learning, 37; 2256–2265. proceedings.mlr.press/v37/sohl-dickstein15.pdf (20.12.2025).

Takian A, Sheikh A, Barber N (2014). Organizational learning in the implementation and adoption of national electronic health records: Case studies of two hospitals participating in the National Programme for Information Technology in England. Health Informatics Journal, 20(3); 199–212 doi.org/10.1177/1460458213493196 (20.12.2025).

Tang H, Wu Y, Yang S, Xie E, Chen J, Chen J, Zhang Z, Cai H, Lu Y, Han S (2024). HART: Efficient Visual Generation with Hybrid Autoregressive Transformer. arxiv.org/html/2410.10812v1 (20.12.2025).

Tsion O (2024). SWOT-Analyse einfach erklärt: Schritte, Beispiele, Vorteile. blog.hubspot.de/marketing/swot-analyse-vorlage (30.08.2025).

van Velkinburgh J C, Herbst M D, Casper S M (2023). Diffusion tensor imaging in the courtroom: Distinction between scientific specificity and legally admissible evidence. World Journal of Clinical Cases, 11(19); 4477–4497 doi.org/10.12998/wjcc.v11.i19.4477 (20.12.2025).

Wangler L, Botthof A (2019). E-Governance: Digitalisierung und KI in der öffentlichen Verwaltung. In: Wittpahl V (Hrsg.): Künstliche Intelligenz. Technologien | Anwendung | Gesellschaft. Springer, Berlin, Heidelberg; 122–141.

Weinberg A I (2025). A Framework for the Adoption and Integration of Generative AI in Midsize Organizations and Enterprises (FAIGMOE). arxiv.org/html/2510.19997v1 (20.12.2025).

Wollny V, Paul H (2015). Die SWOT-Analyse: Herausforderungen der Nutzung in den Sozialwissenschaften. In: Niederberger M, Wassermann S (Hrsg.): Methoden der Experten- und Stakeholdereinbindung in der sozialwissenschaftlichen Forschung. Springer VS, Wiesbaden; 189–213.

Zheng D (2025). Diffusion Models on the Edge: Challenges, Optimizations, and Applications. arxiv.org/html/2504.15298v1 (30.11.2025).

KI-gestützte Assistenzsysteme in der Todesermittlung: Potenziale und Grenzen bei der Ersteinschätzung von Todesumständen an Leichenfundorten

Sabrina Wickert

„Wenn auf jedem Grab eines Ermordeten, von dem wir irrtümlich annehmen, dass er eines natürlichen Todes gestorben sei, eine Kerze brennen würde, wären nachts alle Friedhöfe hell erleuchtet." (Herold, zit. nach Schulz 2020). Diese Metapher veranschaulicht die Gefahr, Gewaltdelikte als natürliche Todesfälle fehlzudeuten, und unterstreicht die Bedeutung sorgfältiger Todesermittlungen. Die erste Einschätzung am Leichenfundort besitzt zentrale Weichenfunktion: Sie entscheidet über Hinzuziehung der Rechtsmedizin, Aktivierung von Mordkommission und Kriminaltechnik sowie über die Beschlagnahme des Leichnams und die Intensivierung von Ermittlungen (Madea & Luhmer 2019, S. 66). Erfolgt die kriminalpolizeiliche Leichenschau nicht kritisch, können Hinweise auf ein Fremdverschulden unwiederbringlich verloren gehen (Stricker 2016, S. 4). Zugleich ist sie ein Kompromiss, da nicht jeder Leichnam obduziert werden kann (Grassberger & Schmid 2014, S. 1). Zeitdruck sowie der Einfluss von Öffentlichkeit und Angehörigen erschweren die Lage zusätzlich, da viele Informationen rasch erfasst und in operative Entscheidungen überführt werden müssen (Freislederer et al. 2011, S. 7 f.). Dadurch rückt die Frage nach digitaler Entscheidungsassistenz in den Fokus.

Künstliche Intelligenz (KI) gewinnt auch in der Polizei zunehmend an Bedeutung und kann Daten erfassen und auswerten, Muster und Zusammenhänge erkennen und als digitale Entscheidungsunterstützung dienen (Bitkom e. V. 2023, S. 9). In Niedersachsen wird KI bereits zur Auswertung von Messenger-Daten und Kinderpornografie eingesetzt (Westermann 2025). Im November 2025 wurde ein Gesetzentwurf zu neuen KI-Befugnissen eingebracht, u. a. für intelligente Videoüberwachung und Gesichtserkennung im öffentlichen Raum (Niedersächsischer Landtag 2025). Diese Gesetzesinitiative spiegelt den Bedarf wider, technologische Innovationen gezielt zur Verbesserung der polizeilichen Arbeit einzusetzen. Vor diesem Hintergrund untersucht dieser Beitrag, inwieweit KI-gestützte Assistenzsysteme die niedersächsische Polizei bei der Ersteinschätzung von Todesumständen am Leichenfundort unterstützen könnten. Betrachtet werden Potenziale, Grenzen und die Frage, ob dies derzeit lediglich als Fiktion oder eine fachlich tragfähige Zukunftsvision einzuschätzen ist.

Hintergrund

Das folgende Kapitel stellt die fachliche und wissenschaftliche Ausgangslage dar. Es werden die Aufgabenzuweisung für die Polizei im Todesermittlungsverfahren und der aktuelle Forschungsstand zum KI-Einsatz beschrieben. Da spezialisierte Forschungsarbeiten zu diesem Anwendungsfall kaum vorliegen, werden auch Ansätze aus ähnlichen oder benachbarten Fachgebieten berücksichtigt, deren Anwendung in Analogie relevant sein könnten.

Aufgabenzuweisung der Polizei

Nach § 159 Abs. 1 StPO leitet die Polizei ein Todesermittlungsverfahren ein, sobald Hinweise auf einen nicht natürlichen Tod bestehen oder die Identität des Leichnams ungeklärt ist. Die Richtlinien im Straf- und Bußgeldverfahren (RiStBV) fordern eine möglichst am Fundort durchzuführende Leichenschau bzw. erforderlichenfalls eine Leichenöffnung (RiStBV, Abschnitt 33, Abs. 1 f.). Das niedersächsische Bestattungsgesetz sieht eine äußerliche Leichenuntersuchung sowie Meldepflichten gegenüber Polizei und Staatsanwaltschaft vor (§§ 3, 4 Abs. 4 Nds. BestattG). Eine Fremdeinwirkung am Tod ist stets mitzudenken, bis sie ausgeschlossen werden kann; die finale Einordnung des Fundorts (Tatort, Suizid-, Unfall- oder Sterbeort) ergibt sich erst im Ermittlungsprozess (Mätzler & Wirth 2022, S. 84).

Aktueller Forschungsstand

Die Bewertung des Auffindeortes bildet einen Kernprozess der Todesermittlung und umfasst Gesamtsituation, Lage des Leichnams und vorhandene Spuren (Mätzler & Wirth 2022, S. 90, 92). Zur Rekonstruktion von Auffindesituationen werden bereits 3D-Simulationen genutzt, die geometrische Daten und Verletzungsmuster mit physikalischen Parametern kombinieren (Labudde & Becker 2019, S. 35). Diese Verfahren gehören zu klassischen Rekonstruktionsmethoden, die auf definierten Parametern beruhen. Erste empirische Arbeiten untersuchten inzwischen KI zur Interpretation von Tatortszenarien. Farber (2025) analysierte Large Language Modelle (LLMs) wie ChatGPT-4, Claude und Gemini im Hinblick auf ihre Fähigkeit, Tatortfotos als Entscheidungsassistenz auszuwerten. Die KI erfasste teils Details, die Fachkräften zunächst entgingen, und benötigte für die erste Tatortbeurteilung im Schnitt unter zwei Minuten, während Menschen rund 42 Minuten brauchten. Die hohe Beobachtungsgenauigkeit der KI zeigte sich besonders bei der Identifikation subtiler Blutspritzermuster. Gleichzeitig zeigten sich Grenzen in der kausalen Deutung einzelner Befunde: Objekte wurden zwar erkannt, ihre Bedeutung jedoch nicht immer korrekt eingeordnet, etwa bei einem umgestürzten Stuhl. Farber betont, dass KI-Ergebnisse nicht unkritisch übernommen werden dürfen und lediglich ergänzend zu fachlichen Bewertungen dienen sollten. Bei einer Zuverlässigkeit von 7,4/10 bei der Interpretation von Tatortbildern zeigte sich ein klares Beschleunigungspotenzial erster Einschätzungen, jedoch bei noch begrenzter Deutungstiefe (Farber 2025, S. 932, 936−940).

Die beschriebenen Stärken in der oben dargestellten Blutspurenmusteranalyse decken sich mit weiteren Ergebnissen: Jung et al. (2024) verglichen KI-Modelle zur Klassifikation der drei am schwierigsten voneinander zu unterscheidenden Arten von Blutfleckenmustern: Ein Convolutional Neural Network (CNN) erreichte eine Genauigkeit von 52 %, ein Entscheidungsbaum 72 % und ein Random-Forest-Modell 80 %. Diese Verfahren erfassen charakteristische Merkmale von Blutflecken automatisiert und unterstützen so die Rekonstruktion von Ereignisabläufen (Jung et al. 2024, S. 2, 9). Die kriminalpolizeiliche Leichenschau ist ein weiteres wesentliches Element im Todesermittlungsverfahren und umfasst die systematische Dokumentation von Auffindeposition, Bekleidung, Todeszeichen, Verletzungen sowie Spuren möglicher Gewalteinwirkung (Mätzler & Wirth 2022, S. 91 f.). In der medizinischen Bildverarbeitung hat KI, insbesondere Deep Learning, erhebliche Fortschritte erreicht. Tiefe neuronale Netze können aus Beispieldaten auch neue Zusammenhänge ableiten. Generative Modelle erzeugen synthetische, annotierte Bilddaten und erweitern so bestehende

Datensätze, wodurch KI-Systeme auch in datenbeschränkten medizinischen Feldern trainierbar werden. Der praktische Nutzen zeigt sich in klinischen Anwendungsstudien: In einer Mammografie-Studie steigerte KI die Brustkrebs-Erkennungsrate um rund 18 % und entlastete das radiologische Fachpersonal ohne Qualitätsverlust. In der Dermatologie konnte KI auf Bilddaten Hautkrebs auf Expertenniveau oder besser diagnostizieren (Kepp et al. 2025, S. 862, 867 ff.). Visual ChatGPT, ein Chatbot-System, konnte in einer Studie zur Klassifikation von Dekubitus-Stadien anhand von Patientenbildern binnen Sekunden einen Wundbeurteilungsbericht erstellen. Das Vision-LanguageModel (VLM) zeigte Potenzial, erreichte aber nicht die Genauigkeit und Spezifität von Pflegefachkräften (Karaçay et al. 2025, S. 4, 9, 11).

Ein weiterer Aspekt der Todesermittlungen ist die Ermittlung zum Gesundheitszustand der Verstorbenen, insbesondere durch Sichtung und Auswertung medizinischer Behandlungsunterlagen (Mätzler & Wirth 2022, S. 98 ff.). In der Medizin kann KI neben der Analyse radiologischer Bildgebungen auch medizinische Befunde mithilfe von Natural Language Processing (NLP) und Maschinellem Lernen (ML) analysieren. NLP dient der automatischen Verarbeitung natürlicher Sprache, ML-Methoden erkennen und strukturieren Informationen nach einer Trainingsphase. Systeme können wissenschaftliche Publikationen und historische Fälle analysieren, um seltene Erkrankungen zu identifizieren und diagnostische Hinweise abzuleiten (Antweiler et al. 2023, S. 4 ff.). Eine italienische Studie von Di Mauro et al. zeigt, dass Algorithmen in Patientenakten Muster und Anomalien erkennen, die auf Behandlungsfehler hindeuten. Die Studie kommt zu dem Schluss, dass KI, gestützt auf fachliche Referenzdaten, evidenzbasierte Entscheidungshilfen in Echtzeit bereitstellen kann, wobei eine kontinuierliche Validierung der Algorithmen unerlässlich bleibt (Di Mauro et al. 2025, S. 2 f.).

Am Ende der soeben beschriebenen Befundaufnahme wird auf Basis des Ermittlungsstandes das weitere Vorgehen bestimmt. Kann Fremdverschulden ausgeschlossen werden, erfolgt die Einordnung als natürlicher Tod, Unfall oder Suizid; eine Leichenöffnung unterbleibt dann meist. Diese Beurteilung zählt zu den anspruchsvollsten und verantwortungsvollsten polizeilichen Aufgaben (Mätzler & Wirth 2022, S. 97 f., 100). In der Forschung werden Bayes'sche Netzwerke (BN) untersucht, um heterogene Informationsquellen probabilistisch zu bewerten und Entscheidungsprozesse zu unterstützen. In Decision Support Systems (DSS) tragen sie etwa im Geheimdienstbereich dazu bei, kritische Entscheidungen zu potenziellen, zukünftigen Ereignissen zu treffen (Frame et al. 2023, S. 637, 647). Auch für kriminalpolizeiliche Ermittlungen wurde durch Wang & Xu ein BN-basiertes Inferenzmodell entwickelt, das Beziehungen zwischen Beweismitteln identifiziert und logisch bewertet. Da kriminalistische Ermittlungen wesentlich auf schlussfolgerndem Denken beruhen, können BNs als mathematische Entscheidungswerkzeuge unterstützend eingesetzt werden (Wang & Xu 2014, S. 2 f.).

KI-gestützte Clinical Decision Support Systems (CDSS) unterstützen in der Medizin komplexe Entscheidungen unter Zeitdruck und bei unvollständiger Informationslage. Sie analysieren große Datenmengen, erkennen Muster und geben unter Verknüpfung von Fachwissen und Patientendaten evidenzbasierte Empfehlungen sowie Warnhinweise aus. Neben wissens- und regelbasierten Ansätzen gewinnen vor allem ML-basierte KI-Systeme an Bedeutung. Herausforderungen liegen in Datenqualität, Prozessintegration und Akzeptanz; erste Projekte setzen daher auf Explainable AI (XAI). Die U.S. Food and Drug Administration hat bereits über 1 000 KI-Algorithmen für den klinischen Einsatz zugelassen (Tschochohei et al. 2025,

S. 872–875). Der aufgezeigte Forschungsstand verdeutlicht, dass KI in verantwortungskritischen Aufgabenfeldern an Bedeutung gewinnt und empirisch zur Daten- und Musteranalyse sowie als Entscheidungsassistenz untersucht und weiterentwickelt wird.

Material und Methodik

Das Kapitel beschreibt das methodische Vorgehen zur Beantwortung der Forschungsfrage, ob ein KI-Assistenzsystem Ermittelnde der Kriminalpolizei am Leichenfundort unterstützen könnte sowie welche Potenziale und Grenzen sich daraus ergeben. (Datenschutz-)rechtliche und ethische Fragestellungen werden bewusst nicht betrachtet, da dies den Umfang des Beitrags überschreiten würde. Grundlage bildet der aktuelle Forschungsstand zu relevanten KI-Technologien, der mittels systematischer Literaturrecherche erarbeitet wurde. Die Ergebnisse wurden anschließend mit zwei schriftlichen, leitfadengestützten Experteninterviews abgeglichen, um wissenschaftliche sowie fachliche und praktische Perspektiven zu beleuchten. Leitfadengestützte Interviews stellen ein anerkanntes Verfahren qualitativer Forschung dar (Schiek 2024, S. 134). Nach Schiek sind auch ohne gleichzeitige Anwesenheit der Beteiligten schriftlich durchgeführte Interviews valide und ermöglichen durch Editierbarkeit der Antworten eine präzisere Reflexion und Darstellung von Erfahrungswissen (Schiek 2022). Experten gelten in der Forschung als Personen, die durch Fach- und Erfahrungswissen Zugang zu spezialisierten Erkenntnis- und Deutungsbereichen eröffnen (Helfferich 2022, S. 877).

Entsprechend wurden Privatdozent Dr. med. Armin Fieguth, Oberarzt und Leiter des Obduktionsbereichs am Rechtsmedizinischen Institut der Medizinischen Hochschule Hannover, sowie eine auf eigenen Wunsch pseudonymisierte kriminalpolizeiliche Führungskraft mit langjähriger Erfahrung in der Erstbearbeitung von Todesermittlungen interviewt. Die Kombination rechtsmedizinischer und ermittlungspraktischer Expertise ermöglicht eine fundierte, sich ergänzende Betrachtung der Fragestellung. Die Interviewauswertung erfolgte mittels qualitativer Inhaltsanalyse nach Mayring, die ein regelgeleitetes interpretatives Vorgehen ermöglicht, das auch latente Bedeutungen erfasst. Basierend auf psychologischen und linguistischen Grundlagen des Textverstehens eignet sie sich besonders gut für die strukturierte Interpretation komplexer, erfahrungsbasierter Experteninterviews. Die leitfadenvorgegebenen Themen wurden zunächst als deduktive Kategorien genutzt und anschließend durch induktiv aus den Interviewantworten entwickelte inhaltliche Ergänzungen erweitert; die Zuordnung der Textstellen erfolgte entsprechend den inhaltsanalytischen Regeln (Mayring & Fenzl 2022, S. 691–701). Dieses Vorgehen ermöglichte die systematische Integration etablierter Forschung sowie neuer erfahrungsbasierter Expertensichtweisen. Im Folgekapitel wurden die Erkenntnisse der Literaturrecherche mit den Interviewbefunden zusammengeführt und diskutiert, um zu einer Antwort auf die Forschungsfrage zu gelangen.

Ergebnisse

Die Ergebnisse basieren auf der strukturierenden Auswertung der Experteninterviews entlang der festgelegten Kategorien und beziehen sich auf die Einschätzungen der Fachpersonen zu zentralen Ermittlungsaspekten sowie zum möglichen Einsatz KI-basierter Assistenzsysteme am Leichenfundort.

Analyse der Auffindesituation

Beide Experten sehen die Auffindesituation des Leichnams als entscheidend für die erste Bewertung und sehen KI-Potenzial zur Rekonstruktion von Geschehensabläufen. Dr. Fieguth beschreibt die Schwierigkeit, strafrechtlich relevante Hinweise früh zu erkennen. Das Gesamtbild entstehe aus einer Befundgesamtschau, erreiche aber bei spezialisierten Analysebedarfen Grenzen. Der kriminalpolizeiliche Experte betont, dass die Einordnung der Todesumstände maßgeblich von der verfügbaren Informationslage abhängt und Angaben aus dem Umfeld sowie medizinische Unterlagen mit der Spurenlage korrespondieren müssen. Herausfordernd seien Informationsmangel, unklare Verletzungen, unbeobachtete Unfälle (z. B. Stürze) oder fragliche Zugangsverhältnisse zum Leichenfundort und atypische Auffindesituationen durch Agonieverhalten. Hier könnte KI möglicherweise unterstützend zur Klärung unklarer Auffindesituationen beitragen.

Äußere Befunde (Leichenschau) und Verletzungsmuster

Dr. Fieguth betont den Ermittlungswert von Auffindeposition, Todeszeichen und Verletzungslokalisation. Probleme ergäben sich bei geringer Informationsdichte, komplexer Befundlage, vielfältigen Interpretationsmöglichkeiten oder möglicher Manipulation. Er hält es für möglich, dass KI aufgrund ihrer Verarbeitungskapazität Blutspuren- und Verletzungsmuster analysieren oder über Datenbankvergleiche ähnliche Fälle identifizieren könnte. Der kriminalpolizeiliche Experte bezeichnet die äußere Leichenschau als Ermittlungskern: Todeszeichen dienten der Zeiteingrenzung und Aussageplausibilisierung, Hautverfärbungen oder OP-Narben der medizinischen Vorgeschichte, nicht anders erklärbare Verletzungen der Verdachtsbegründung auf Fremdeinwirkung. Er hält ein Assistenzsystem für denkbar, in das Befunde eingegeben werden und das Hinweise auf eine Todesursache gibt, Widersprüche aufzeigt oder Empfehlungen generiert.

Einordnung medizinischer Informationen

Der Rechtsmediziner beschreibt medizinische Unterlagen und Indizien als hilfreich, aber auch als fehleranfällig, etwa bei veralteten Befunden oder unklarer Medikamentenzuordnung. Er hält es für möglich, dass KI künftig Krankenunterlagen sichtet, Befundinhalte zusammenfasst und mit der Auffindesituation sowie möglichen Todesumständen korreliert sowie Medikamente auf potenziell todesursächliche Wirkungen prüft. Der kriminalpolizeiliche Experte betont die Relevanz medizinischer Informationen besonders dann, wenn keine auskunftsfähigen Personen zur Verfügung stehen. Unterlagen könnten Vorerkrankungen, frühere Ereignisse (z. B. zunächst folgenloser Sturz) und Kontaktpersonen benennen. Herausforderungen ergäben sich jedoch durch Fachterminologie und fehlende medizinische Expertise der eingesetzten Polizeikräfte. Er geht davon aus, dass KI den Gesundheitsstatus verständlich strukturieren kann, wenn die Daten digital verfügbar bzw. ohne hohen Aufwand digitalisierbar sind.

Plausibilitätsprüfung, Hypothesenbildung und Entscheidungsunterstützung

Beide Experten sehen KI künftig als mögliches Instrument, um Informationen in zeitkritischen Lagen schneller zu ordnen, Widersprüche zu erkennen und bei der Priorisierung polizeilicher Maßnahmen zu unterstützen. Dr. Fieguth warnt, dass Entscheidungen unter

Zeitdruck oder in scheinbaren Routinefällen zu irreversiblen Versäumnissen in der Tatortarbeit führen können und Veränderungen am Fundort nachvollzogen und dokumentiert werden müssen. KI könne Diskrepanzen zwischen objektiven Feststellungen und geschilderten Abläufen identifizieren, Verletzungsmuster deuten (z. B. Sturz oder Fremdbeibringung) und Manipulationen aufdecken, z. B. durch Datenabgleich. Der kriminalpolizeiliche Experte beschreibt die besondere Herausforderung, ein mögliches Fremdverschulden zu erkennen, wenn der erste Anschein auf eine natürliche Todesursache hindeutet – vor allem bei fehlenden oder widersprüchlichen Informationen, etwa bei jungen Verstorbenen ohne Vorerkrankungen und äußerliche Verletzungen. Er betont, dass ein schlüssiger objektiver Befund durch vor Ort erlangte Informationen gestützt werden müsse, um eine tragfähige Grundlage für die weitere Ermittlungsrichtung zu schaffen. KI könnte zudem Hinweise auf noch zu erhebende Daten geben. Übereinstimmend verweisen beide Experten darauf, dass KI ausschließlich unterstützend wirken kann und Entscheidungen weiterhin durch die Ermittelnden selbst zu treffen sind, da automatisierte oder probabilistische Bewertungen den Besonderheiten eines Einzelfalls nicht gerecht werden.

Grenzen technischer Systeme und Bedeutung menschlicher Expertise

Beide Experten betonen, dass KI-Systeme strukturell durch begrenzte Datenbestände limitiert sind. Dr. Fieguth warnt vor Fehlinterpretationen bei seltenen Fällen mangels Vergleichsdaten und betont, dass KI lediglich als Werkzeug dienen dürfe, dessen Ergebnisse kritisch geprüft werden müssten. Der kriminalpolizeiliche Experte hebt hervor, dass eine fehlerhafte Datenerhebung die Auswertung und damit die Ergebnisse der KI beeinträchtigen könne. Zudem verdeutlicht er die Rolle des kriminalistischen „Bauchgefühls“ und der Fähigkeit, einen Ereignisort zu „lesen“. Nonverbale Kommunikation und situatives Verhalten könnten nur durch Ermittelnde eingeschätzt werden. Beide Experten stimmen überein, dass kriminalistische Erfahrung und Intuition nicht ersetzbar seien. Dr. Fieguth warnt vor „Technikgläubigkeit“ und dem Risiko eines Kompetenzverlusts. Er betont die Notwendigkeit, KI-Funktionsweisen zu verstehen und kritisch zu reflektieren. Der kriminalpolizeiliche Experte gibt zu bedenken, dass KI-Einsatz nicht dazu verleiten dürfe, weniger qualifiziertes Personal einzusetzen, und dass Auswertungen verfahrens- und gerichtssicher nachvollziehbar sein müssen.

Chancen der strukturierten Unterstützung

Dr. Fieguth hält es für vorstellbar, dass die Dokumentation am Ereignisort weiter automatisierbar wird und erste KI-Analysen vor Ort die Ermittlungsrichtung beeinflussen könnten. Die kriminalpolizeiliche Führungskraft ergänzt Sprachbarrieren am Fundort als erfolgskritischen Faktor. Im Ergebnis sieht Dr. Fieguth einen klaren Mehrwert im Einsatz KI-basierter Assistenzsysteme. Der kriminalpolizeiliche Experte hält den Einsatz von KI grundsätzlich in allen Arbeitsschritten am Leichenauffindeort für denkbar, sofern eine schnelle Dateneingabe und die Verarbeitung verschiedener Formate (Diktate/Vernehmungen, Fotos, Scans, Textdateien) möglich sind. Aus seiner Sicht könnten KI-Systeme Daten zusammenfassen und Berichte generieren, wobei auch LLMs künftig hilfreich sein könnten. Ein Nutzen bestünde jedoch nur, wenn der Arbeitsaufwand nicht steigt und die Ergebnisse als reine Ermittlungsunterstützung verstanden werden.

Diskussion

Ziel dieses Beitrags war es zu untersuchen, ob und wie ein KI-basiertes Assistenzsystem Ermittelnde der Kriminalpolizei am Leichenfundort unterstützen könnte und welche Potenziale und Grenzen sich daraus ergeben. Die nachstehende Diskussion verknüpft die Ergebnisse der Experteninterviews mit dem zuvor skizzierten Forschungsstand und ordnet sie aktuellen technischen Entwicklungen zu. Zugleich wird reflektiert, wie die Einschätzungen der Experten KI-Anwendungsfelder aus benachbarten Disziplinen ergänzen oder abgrenzen. Die Experten sehen KI-Potenzial in der schnellen Rekonstruktion von Geschehensabläufen und der Erklärung unklarer Befunde am Leichenfundort. Damit adressieren sie einen Bedarf, der im Forschungsstand anschlussfähig, aber noch nicht umfassend erfüllt ist. Studien belegen die Effizienz visueller Bild- und Musteranalyse. Ohne Kontextwissen stoßen KI-Systeme jedoch an Deutungsgrenzen; sie interpretieren komplexe, dynamische Abläufe nicht verlässlich (Farber 2025, S. 932, 936–940). Der in den Interviews betonte Nutzen einer frühen Rekonstruktions- und Erklärungshilfe dürfte damit über die derzeitigen Fähigkeiten der Modelle hinausgehen. Daraus folgt die Frage, ob KI künftig gezielt forensisch trainiert und mit hinreichend breiten, auch atypischen Trainingsdaten ausgestattet werden könnte, um trotz stark variierender, unvollständiger oder ungewöhnlicher Spurenbilder robuste Vor-Ort-Unterstützung zu leisten.

In der klinischen Bilddiagnostik wird KI bereits eingesetzt, etwa in der Brust- und Hautkrebserkennung sowie bei der Dekubitus-Klassifikation (Kepp et al. 2025, S. 868 f.; Karaçay et al. 2025). Auch bei der Leichenschau sehen Dr. Fieguth und der polizeiliche Experte KI-Potenzial bei der Deutung körperlicher Befunde. Entscheidend wäre jedoch die funktionale Differenzierung: Liefert ein System nur erkundende Erklärungen zu Einzelmerkmalen oder ein integratives Gesamtbild zur Einschätzung einer Todesursache? Für den Einsatz in der kriminalpolizeilichen Leichenschau müsste KI nicht nur partielle Ausschnitte, sondern den gesamten Körper erfassen und heterogene, typische wie atypische Befunde interpretieren. Die Umsetzung einer solchen Ganzkörperanalyse dürfte von der Verfügbarkeit sehr großer, speziell forensischer Trainingsdatensätze abhängen. Synthetische Bilddatenerzeugung zeigt, dass Datenskalierung auch in schwer zugänglichen Befunddomänen möglich ist (Kepp et al. 2025, S. 862, 867). Ungeachtet rechtlicher, ethischer und pietätischer Belange bleibt die Überlegung, wie ein KI-System ein Ganzkörperbild erfassen könnte, ohne den Workflow für die Anwendenden zu überlasten. Denkbar wären hierbei Fotoreihen, Videoaufnahmen und standardisierte Befund-Eingabemasken, über die auch nicht visuelle Eindrücke wie Tastbefunde oder Gerüche in beschreibender Form in das System eingebracht werden könnten. Offen bleibt darüber hinaus die Frage, ob und wie KI-Systeme in der Lage sein könnten, multisensorische Eindrücke am Leichenfundort technisch zu erfassen, insbesondere solche nicht visueller Wahrnehmung, um diese Informationen in einer für KI-Systeme verarbeitbaren Form nutzbar zu machen.

Auch die strukturierende Auswertung medizinischer Dokumente wurde von beiden Experten als vielversprechend eingeschätzt. In der Medizin ist der KI-Einsatz zur Analyse und Auswertung von Gesundheitsdokumenten bereits etabliert (Antweiler et al. 2023, S. 4 ff.). Für polizeiliche Todesermittlungen bestünde aus Sicht der Experten der Mehrwert vor allem in der Strukturierung und Vorsichtung medizinischer Unterlagen auf todesrelevante Hinweise und im Abgleich mit der Spuren- und Informationslage bei eingeschränkter medizinischer Expertise vor Ort. Der polizeiliche Nutzungskontext unterscheidet sich jedoch von medizini-

schen Diagnose- oder Therapiesettings: Gesundheitsdaten dienen hier der Verdachts- und situativen Lageprüfung im Ermittlungsprozess. Nach Einschätzung der Befragten wäre für den Vor-Ort-Einsatz entscheidend, dass medizinische Informationen formatübergreifend und ohne zeitliche Verzögerung aufbereitet werden könnten, während die finale Bewertung weiterhin durch kriminalistische Expertise erfolgen müsse, um Risiken fehlerhaft zugeordneter oder veralteter Gesundheitsinformationen zu minimieren. Gleichzeitig wäre ein solches System nur belastbar, wenn es mit sehr großen, forensisch spezialisierten Trainingsdatensätzen geschult würde.

Die Experten halten KI in zeitkritischen Lagen für eine mögliche Assistenz, um Informationen zu ordnen, Befunde zu deuten und Widersprüche oder Manipulationen früh zu erkennen. Die Forschung bestätigt, dass auf BN basierende KI-Systeme in Medizin, Nachrichtendiensten und kriminalistischen Ermittlungen bereits als DSS genutzt werden, vor allem wegen der schnellen Analyse großer Datenmengen und Muster sowie der Ausgabe von Warn- oder Handlungshinweisen (Frame et al. 2023, Wang 2014; Tschochochohei et al. 2025).

Ausgehend von der von Wang und Xu (2014, S. 2 f.) zugrunde gelegten Annahme, dass kriminalistische Ermittlungen wesentlich auf schlussfolgerndem Denken beruhen, könnte das von Expertinnen und Experten als nicht substituierbar bezeichnete „kriminalistische Bauchgefühl“ als impliziter, erfahrungsgeleiteter Schlussfolgerungsprozess verstanden werden. Hier könnten KI-Assistenzsysteme anschlussfähig an kriminalistisches Denken sein, indem sie diesen Prozess systematisieren und Analysepfade sichtbar machen. Zugleich erscheint es naheliegend, darauf hinzuweisen, dass Ermittelnden am Ereignisort neben textlichen und bildlichen Informationen zahlreiche kontextuelle Informationen sowie berufliches Fach-, Erfahrungs- und sozialisationsgeprägtes Wissen zur Verfügung stehen. Damit stellt sich die Frage nach den Grenzen der vollständigen Formalisierung menschlicher kognitiver Leistungen, insbesondere erfahrungsbasierter Schlussfolgerungs- und Bewertungsprozesse.

Die in den Experteninterviews geäußerte Einschätzung, dass KI-Ergebnisse kritisch geprüft und nur unterstützend eingesetzt werden sollten, deckt sich mit Farbers Analyse (Farber 2025, S. 938). Der Nutzen KI-basierter Systeme hängt nach Forschung und Expertenansicht zudem maßgeblich von Datenqualität, Workflow-Integration und Akzeptanz der Nutzenden ab. Explainable AI-Ansätze (Tschochohei et al. 2025, S. 875) erscheinen auch für die Kriminalistik vielversprechend, da sie Nachvollziehbarkeit und Vertrauen in KI-Assistenzsysteme stärken könnten. Die Interviewten gehen davon aus, dass KI nicht nur datenstrukturell limitiert sei, sondern auch von der KI-Kompetenz der Nutzenden abhänge, die Funktionsweisen verstehen und kritisch hinterfragen müssen. Die Experten warnen vor „Technikgläubigkeit“, Kompetenzverlust und sinkenden Qualitätsanforderungen an das Personal. Daraus ergibt sich, dass eine Einführung von KI-Systemen initial Schulungsaufwand bedeuten und Personalressourcen binden würde. Der erwartete Mehrwert könnte sich jedoch auszahlen, wenn KI schnell, multiformatfähig, transparent und ohne unverhältnismäßigen Zusatzaufwand arbeitet.

Aufgrund begrenzter Forschung zur Fragestellung und der Beschränkung auf zwei Experteninterviews sind die vorgestellten Ergebnisse als explorative Einordnung und erster empirischer Zugang zu verstehen und erheben keinen Anspruch auf Repräsentativität. Bei Einbeziehung weiterer Expertise oder anderer methodischer Zugänge sind abweichende Befunde

denkbar. Zukünftige Forschung sollte daher breiter angelegte Studien ebenso wie eine gezielte Fokussierung auf klar abgegrenzte Teilaspekte KI-basierter Unterstützung in Todesermittlungsverfahren verfolgen, um diese in größerer analytischer Tiefe zu erschließen.

Schlussfolgerungen

Die vorliegende Diskussion legt nahe, dass KI das Potenzial besitzt, bei der polizeilichen Ersteinschätzung am Leichenfundort unterstützend wirken zu können, insbesondere durch automatisierte Bildanalyse und Mustererkennung etwa bei Blutspuren oder Verletzungen. Diese Unterstützung sollte keinesfalls als Ersatz kriminalistischer Bewertung verstanden werden, sondern als Effizienz- und Qualitätsverstärker, der Hinweise priorisiert, Widersprüche früh sichtbar macht und medizinische Dokumente verständlich strukturiert. In diesem Bewusstsein könnte ein Land wie beispielsweise Niedersachsen, in dem polizeiliche Einsatzkräfte oft ohne tiefes medizinisches Fachwissen erste Richtungsentscheidungen treffen müssen, von einer KI-Assistenz profitieren. Die Idee erscheint damit nicht als bloße Fiktion, sondern könnte sich als grundsätzlich tragfähige Zukunftsvision erweisen, deren Potenzial durch aktuelle KI-Modelle bereits teilweise aufgezeigt wird, wobei die in diesem Beitrag identifizierten Grenzen und offenen Fragestellungen zu berücksichtigen sind. Für eine fundierte Bewertung ihrer tatsächlichen Relevanz wären neben (datenschutz-)rechtlichen und ethischen Aspekten insbesondere Fragen der technischen Machbarkeit im polizeilichen Systemverbund zu prüfen. Darüber hinaus bedürfte es einer polizeispezifischen Entwicklung, eines verlässlichen Betriebs sowie einer kontinuierlichen Wartung und Versorgung entsprechender KI-Systeme mit Trainingsdaten.

Um die hypothetischen Ergebnisse zu validieren, könnte in einem nächsten Schritt eine Eingrenzung auf einen klar umrissenen, datenintensiven Teilbereich der Todesermittlung erfolgen, etwa im Rahmen eines Pilotprojekts, um praktischen Nutzen, Fehleranfälligkeit und Aufwand empirisch belastbar zu untersuchen. Zudem bedarf es weiterer Prüfung, wie zuverlässig KI trotz unvollständiger, seltener oder multisensorisch geprägter Auffindesituationen funktioniert, wie gut XAI-Erklärpfade die KI-Unterstützung beim Todesermittlungsverfahren nachvollziehbar transparent machen können und wie ein echter Kosten-Nutzen-Nachweis für die Polizei Niedersachsen aussehen müsste.

Literaturverzeichnis

Antweiler, D., Beckh, K., Chakraborty, N., Giesselbach, S., Klug, K., Rüping, S. (2023). *Natural Language Processing in der Medizin – Von der automatisierten Befundanalyse bis zum Arztbriefgeneratur: Künstliche Intelligenz für dokumentenbasierte Prozesse im Krankenhaus.* Fraunhofer-Institut für intelligente Analyse- und Informationssysteme. newsletter.fraunhofer.de/public/a_14338_S4Jdz/file/data/4410_Fraunhofer_IAIS_Whitepaper_Clinical_NLP_Web.pdf (13.09.2025).

Bitkom e. V. (2023). KI in der Polizei – Einsatzpotentiale und Lösungsansätze zur Implementierung. Berlin: Bitkom. bitkom.org/sites/main/files/2023-10/bitkom-positionspapier-ki-polizei-einsatz-implementierung.pdf (25.11.2025).

Di Mauro, L., Capasso, E., Tettamanti, C., Casella, C., Francaviglia, M., Volonnino, G., Rinaldi, R., Esposito, M., Chisari, M. (2025). *The role of artificial intelligence in analyzing clinical malpractice disputes through medical record management.* Journal of Forensic and Legal Medicine, Jg. 25, Vol. 115. sciencedirect.com/science/article/pii/S1752928X25001428?via%3Dihub (13.09.2025).

Farber, S. (2025). *AI as a decision support tool in forensic image analysis: A pilot study on integrating large language models into crime scene investigation workflows.* J Forensic Sci. 2025; Vol.70:932−943. doi.org/10.1111/1556-4029.70035 (28.09.2025).

Frame, M., Acker-Mills, B., Maresca, A., Patterson, R., Curtis, E., Buccello-Stout, R., Nelson, J (2023). *Evaluation of decision support system using Bayesian network modeling in an applied Multi-INT surveillance environment*. Military Psychology 2024, Vol. 36, No. 6, 637−649. doi.org/10.1080/08995605.2023.2250243 (28.09.2025).

Freislederer, A., Stenzel, G., Weirich, M. (2011). *Todesermittlungen. Lehr- und Studienbriefe Kriminalistik/Kriminologie Bd. 15*. Hilden: VDP-Buchvertrieb.

Grassberger, M., Schmid, H. (2014). *Todesermittlung: Befundaufnahme und Spurensicherung*. 2., aktualisierte Aufl. Stuttgart: Wissenschaftliche Verlagsgesellschaft.

Helfferich, C. (2022). *Leitfaden- und Experteninterviews*. In: Baur, N. & Blasius, J. (Hrsg.): Handbuch der empirischen Sozialforschung (Kapitel 55), Springer Nature, Wiesbaden, S. 875−892. doi.org/10.1007/978-3-658-37985-8_55 (23.11.2025).

Jung, H., Jo, Y., Ahn, Y., Jeong, J., Lim, S. (2024). *A first step towards machine learning-based framework for bloodstain classification in forensic science*. Forensic Science International 2024, Vol. 365. iotlab.skku.edu/publications/international-journal/Bloodstain-Pattern-Classification-FSI2024.pdf (27.09.2025).

Karaçay, P., Goktas, P., Yaşar, Ö., Uyanik, B., Uzlu, S., Coşcun, K., Benk, M. (2025). *Investigation of Pressure Injuries With Visual ChatGPT Integration: A Descriptive Cross-Sectional Study*. Journal of Advanced Nursing, 2025, 0: 1−14. onlinelibrary.wiley.com/doi/full/10.1111/jan.16905 (27.09.2025).

Kepp, T., Uzunova, H., Ehrhardt, J., Handels, H. (2025). *KI-basierte Anwendungen in der medizinischen Bildverarbeitung*. Bundesgesundheitsblatt 2025, 68, S. 862–871. doi.org/10.1007/s00103-025-04093-7 (03.10.2025).

Labudde, D., Becker, S. (2019). *Was kann eine 3D-Rekonstruktion für eine moderne Fallarbeit wirklich leisten?* pvt Polizei, Verkehr + Technik, 2/19, S. 33–35.

Madea, B., Luhmer, A. (2019). Zur Person des Leichenschauers. In: Madea, B. (Hrsg.): Die ärztliche Leichenschau. Rechtsgrundlagen, praktische Durchführung, Problemlösungen. 4. Aufl. Berlin/Heidelberg: Springer, S. 59–67.

Mätzler, A., Wirth, I. (2022). *Todesermittlung: Grundlagen und Fälle* (6. neu bearbeitete Auflage). Kriminalistik, Heidelberg: C.F. Müller Verlag.

Mayring, P., Fenzl, T. (2022): *Qualitative Inhaltsanalyse*. In: Baur, N. & Blasius, J. (Hrsg.): Handbuch der empirischen Sozialforschung (Kapitel 43), Springer Nature, Wiesbaden, S. 691–706. doi.org/10.1007/978-3-658-37985-8_43 (23.11.2025).

Niedersächsischer Landtag (2025). Entwurf eines Gesetzes zur Änderung des Niedersächsischen Polizei- und Ordnungsbehördengesetzes und des Niedersächsischen Verwaltungsvollstreckungsgesetzes, Drucksache 19/8942, 10. November 2025. landtag-niedersachsen.de/Drucksachen/Drucksachen_19_10000/08501-09000/19-08942.pdf (25.11.2025).

Schiek, D. (2024). *Methoden der qualitativen Sozialforschung*, utb-Bandnr. 6234, Bielefeld: transcript Verlag.

Schiek, D. (2022). *Schriftliche Online-Interviews in der qualitativen Sozialforschung: zur methodologischen Begründung einer neuen Forschungspraxis.* Forum: Qualitative Sozialforschung (2022) Vol. 23, No. 1, Art. 5. qualitative-research.net/index.php/fqs/article/download/3754/4803/16989 (18.11.2025).

Schulz, B. (2020). *Bildung eines Pools von qualifizierten Ärzten für die Leichenschau in Lübeck*. BDK, 18.09.2020. bdk.de/der-bdk/was-wir-tun/aktuelles/bildung-eines-pools-von-qualifizierten-aerzten-fuer-die-leichenschau-in-luebeck (13.09.2025).

Stricker, J. (2016). *Die Todesermittlungen*. DPolBl – Deutsches Polizeiblatt, 04/2016, S. 2–4.

Tschochohei, M., Adams, L., Bressem, K., Lammert, J. (2025). *KI-gestützte klinische Entscheidungsunterstützungssysteme: Herausforderungen und Potenziale*. Bundesgesundheitsblatt 2025, 68, S. 872–879. doi.org/10.1007/s00103-025-04092-8 (03.10.2025).

Wang, J., Xu, Z. (2014). *Bayesian inferential reasoning model for crime investigation*. Neves-Silva, R., Tshirintzis, G. & Uskov, V. (eds.): Smart digital futures 2014. Frontiers in Artificial Intelligence and Applications (262). IOS Press, 59–67. [Book Section] shura.shu.ac.uk/18871/ (28.09.2025).

Westermann, A. (2025). *Digitale Beweismittel auswerten – LKA Niedersachsen entwickelt KI zur Kriminalitätsbekämpfung*. Pro Polizei, 02 (März/April), S. 12.

Vorbereitung von Nachwuchskräften der Polizei auf technische, rechtliche und ethische Herausforderungen der Künstlichen Intelligenz

Tobias Keller

„Computer können theoretisch menschliche Intelligenz emulieren und sie übertreffen [...]. Erfolgreiches Schaffen einer effektiven Künstlichen Intelligenz könnte das größte Ereignis in der Geschichte unserer Zivilisation sein. Oder das Schlimmste. [...] Wir können also nicht wissen, ob uns die Künstliche Intelligenz unendlich helfen wird [...] oder ob sie uns möglicherweise zerstört." (Hawking 2017). Diese von Hawking beschriebene Ambivalenz zwischen historischer Chance und unvorhersehbarem Risiko Künstlicher Intelligenz prägt auch die aktuelle Sicherheitslage. Die technologischen Fähigkeiten, die theoretisch menschliche Intelligenz nachahmen können, tragen nicht nur zum Wohle der Gesellschaft bei, sondern werden zunehmend für schädliche Zwecke instrumentalisiert. Die fortschreitende Digitalisierung befähigt Kriminelle zu neuen, in der Bevölkerung oftmals noch unbekannten Modi Operandi (Pohl 2024, S. 121 f.). Damit verändert sich die operative und strategische Polizeiarbeit grundlegend. Neben der operativen Befähigung bedarf es einer frühzeitigen Thematisierung in der Ausbildung von Nachwuchskräften.

Insbesondere im Spannungsfeld zwischen innovativer Technik, gesetzlichen Rahmenbedingungen und gesellschaftlicher Verantwortung gilt es nicht nur, ein Bewusstsein für kriminelle Large-Language-Model-Nutzung (LLM) zu schaffen, sondern auch technisches Wissen, reflektierte Urteilsfähigkeit und verantwortungsbewusstes Handeln zu fördern (Simon 2025, S. 13 ff.; Just 2025, S. 41; Rubehn 2025, S. 18 ff.; EUCPN 2022, S. 14 ff.; Frank 2024, S. 114 f.). Im Zentrum der Fragestellung steht somit die Herausforderung, einen interdisziplinären Kompetenzaufbau durch die Verknüpfung technischer, rechtlicher und ethischer Qualifikationen sicherzustellen, um dem Ziel einer verantwortungsvollen, digitalisierten Polizeiarbeit gerecht werden zu können. Hiervon abgeleitet befasst sich der vorliegende Beitrag mit der Frage:

Wie können Nachwuchskräfte der Polizei durch eine interdisziplinäre KI-Ausbildung auf die technischen, rechtlichen und ethischen Herausforderungen digitaler Polizeiarbeit vorbereitet werden?

Der Beitrag dient der Weiterentwicklung zeitgerechter Ausbildungskonzepte und Stärkung der Handlungssicherheit zu KI im Polizeikontext.

Hintergrund

Gegenwärtig herrscht kein wissenschaftlicher Konsens über eine einheitliche Begriffsbestimmung (Leffer 2025, S. 96). Das Europäische Parlament beschreibt KI als „die Fähigkeit einer Maschine, menschliche Fähigkeiten wie logisches Denken, Lernen, Planen und Kreativität zu imitieren" (2023, S. 1, ausführlicher im Art. 3 Nr. 1 der Verordnung zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz […] – hier: KI-VO). Diese Definition umfasst Systeme, die zunehmend in den Alltag der Bevölkerung integriert werden. Empirisch manifestiert sich diese Entwicklung in einem weltweiten Anstieg der Nutzung generativer KI, die im Jahr 2024

bereits von 48 % der Menschheit verwendet wurde – mit einer Zuwachsrate im Vergleich zum Vorjahr zwischen 8 und 11 % (Google/Ipsos 2025, S. 5). Für das Verständnis von KI im polizeilichen Kontext lassen sich drei Dimensionen ableiten: technisch, rechtlich und ethisch (Wörner 2024, S. 620 ff.; Simon 2025, S. 12 ff.; Rubehn 2025, S. 18 ff.; EUCPN 2022).

Technische, rechtliche und ethische Hintergründe

Aus technischer Perspektive basieren KI-Systeme auf Modellen, die aus umfangreichen Datensätzen Muster ableiten und Entscheidungen oder Vorhersagen generieren (EUCPN 2022, S. 5 f.). Diese Verfahren ermöglichen leistungsfähige Analysen, sind jedoch aufgrund ihrer Komplexität häufig schwer nachvollziehbar (sog. Blackbox-Problematik; EUCPN 2022, S. 10 ff.). Dieser Umstand kann insbesondere die gerichtliche Beweisführung erschweren. Der rechtliche Rahmen – insbesondere die DSGVO, nationale Polizeigesetze und die KI-VO – fordert deshalb u. a. Transparenz, Zweckbindung und Verhältnismäßigkeit (Eisenmenger 2024, S. 109 ff.; Wörner 2024, S. 627 ff.). Ergänzend stellen sich ethische Herausforderungen, insbesondere hinsichtlich Fairness, Diskriminierungsfreiheit und Verantwortlichkeit (EUCPN 2022, S. 10 ff.; BvR 2023, Rn. 100). Verzerrte Trainingsdaten (z. B. durch Bias in historischen Kriminalitätsstatistiken), mangelnde Erklärbarkeit und unklare Haftungsstrukturen machen eine reflektierte und verantwortungsbewusste Nutzung notwendig (EUCPN 2022, S. 14 ff.; Frank 2024, S. 114 f.; Wolfangel 2022, S. 177 ff.).

KI als Mittel der Kriminalitätsbegehung und zur Unterstützung der Polizeiarbeit

KI kann sowohl zur Begehung von Straftaten als auch zur polizeilichen Aufklärung solcher eingesetzt werden (Rubehn 2025, S. 18 f.; Simon 2025, S. 13 ff.; Egbert/Leese 2021, S. 1 ff., 35). Täterinnen und Täter nutzen KI unter anderem für Deepfakes, automatisierte Betrugsformen und digitale Angriffe (Pohl 2024, S. 121 f.; Dams/Kraetzer 2025; FBI 2024). Gleichzeitig bietet KI erhebliche Potenziale in der Ermittlungsarbeit, etwa durch Mustererkennung, Datenanalyse, digitale Spurenauswertung oder Bild- und Videoanalysen (ebd.; Rubehn 2025, S. 18). Sie kann Prozesse beschleunigen, Entscheidungsgrundlagen verbessern und Ermittlerinnen und Ermittler entlasten. Gleichwohl bleibt eine kritische Prüfung der Systeme erforderlich, da KI lediglich ein Werkzeug darstellt, dessen Ergebnisse stets durch menschliche Expertise validiert werden müssen (sog. Human-in-the-Loop-Ansatz) (Eisenmenger 2024, S. 109 f.; Disselkamp/Schmiedchen 2026, S. 326).

Didaktische Anforderungen und Kompetenzentwicklung

Angesichts dieser vielschichtigen Anforderungen reicht eine reine Wissensvermittlung nicht aus. Um Nachwuchskräfte zu einer souveränen Handlungssicherheit zu befähigen, müssen zugrunde liegende Lernprozesse verstanden und didaktisch fundiert gestaltet werden. Lernen wird dabei als Prozess verstanden, in dem Erfahrungen zu dauerhaften Verhaltensänderungen führen (Anderson 2000, S. 4). Insbesondere im Bildungsweg von Nachwuchskräften zeigen sich He-rausforderungen durch die oft isolierte Vermittlung einzelner Fächer (Braßler 2023, S. 15). Die Hochschulrektorenkonferenz betont daher Interdisziplinarität als zentrales Ziel, um fachliche mit methodischen sowie sozialen Kompetenzen zu verknüpfen (Lerch 2019, S. 2).

Eine effektive interdisziplinäre Hochschullehre zur Vermittlung von KI-Kompetenzen integriert hierbei unterschiedliche Lerntheorien, um den spezifischen Anforderungen der Polizeiarbeit gerecht zu werden. Behavioristische Ansätze (Watson 1913; Magill 1998, S. 100 ff.), die Lernen als Verhaltensänderung durch Wiederholung verstehen (Franken/Franken 2023, S. 201 ff.), eignen sich für das Erlernen von Routinen in der Anwendung von KI-Tools oder der Spurensicherung. Kognitivistische Elemente, die den Fokus auf die aktive Informationsverarbeitung legen (Franken/Franken 2023, S. 205 ff.) sind essenziell, um die komplexen Funktionsweisen von Algorithmen und rechtliche Abwägungsprozesse intellektuell zu durchdringen.

Schließlich ermöglichen konstruktivistische Formate (Piaget 1923), bei denen Wissen subjektiv und erfahrungsabhängig konstruiert wird (Franken/Franken 2023, S. 208 ff.), die notwendige Handlungssicherheit in unvorhersehbaren Einsatzlagen. Durch die Verzahnung dieser Logiken – gezielte Übungssequenzen (behavioristisch), strukturierte Wissensvermittlung (kognitiv) und situierte Projektaufgaben (konstruktivistisch) – können Nachwuchskräfte befähigt werden, KI nicht nur technisch zu bedienen, sondern deren Ergebnisse im rechtlichen und ethischen Kontext kritisch zu bewerten (Bolte/Lerch 2023, S. 15; Braßler 2023, S. 32 ff.). Dies bildet die theoretische Grundlage für die nachfolgende empirische Untersuchung der Ausbildungssituation bei der Polizei.

Material und Methodik

Die Untersuchung folgt einem qualitativen, leitfadenbasierten Forschungsdesign und orientiert sich an der kategoriengeleiteten Textanalyse nach Mayring und Fenzl (2019, S. 633 ff.). Ziel ist die systematische Erhebung der Expertenperspektiven aus Kriminalistik, Recht und Ethik zur Vorbereitung von Nachwuchskräften auf KI-bezogene Herausforderungen.

Datenerhebung

Zur Beantwortung der Forschungsfrage wurden zwei strukturierte leitfadengestützte Experteninterviews durchgeführt (Westle 2018, S. 284 ff.; Helfferich 2022, S. 875 ff.). Die Fragen wurden auf Grundlage der theoretischen Erkenntnisse (Kap. 2) und der Kategorienbildung von Just (2025, S. 46 ff.) entwickelt. Sie decken die Bedeutung von KI im Fachgebiet samt fachspezifischer Herausforderungen, die Kompetenzanforderungen, interdisziplinäre Ausbildungsaspekte sowie die Wirksamkeit interdisziplinärer Lehrformate ab. Die jeweils 20-minütigen Gespräche wurden aufgezeichnet, transkribiert und anschließend orthografisch bereinigt. Befragt wurden Dozenten der Hochschule, anteilig zuständig für Module in den Studiengängen des gehobenen und höheren Polizeivollzugsdienstes. Der Beitrag bezieht Experten aus Kriminalistik, Recht und Ethik ein – sie wurden gezielt ausgewählt, um zentrale institutionelle und fachliche Perspektiven der polizeilichen Hochschullehre abzubilden.

Experte 1 wurde aufgrund seiner Tätigkeit als Dozent in den Bereichen Kriminalistik, Kriminaltechnik und IT-Forensik einbezogen. Seine langjährige praktische Erfahrung ermöglicht fundierte Einschätzungen zu technischen, ermittlungspraktischen und − aufgrund beruflicher Vorerfahrungen − auch zu ethischen Fragestellungen, die im Kontext digitalisierter Polizeiarbeit zunehmend relevant sind.

Experte 2 wurde als Professor für Öffentliches Recht, IT-Sicherheit und Datenschutzrecht herangezogen, wodurch eine institutionell verankerte rechtswissenschaftliche und sicherheitsbezogene Perspektive in die Untersuchung einfließt. Seine Expertise deckt insbesondere normative grundrechtsbezogene und datenschutzrechtliche Rahmenbedingungen ab, die für den KI-Einsatz in der Polizei zentral sind.

Auswertungsmethode

Zur Gewährleistung einer hohen Vergleichbarkeit der Antworten (mittels des Verfahrens von Meuser und Nagel (1991, S. 452 ff.)) erfolgte deren Auswertung durch die strukturierte, deduktive Kategorienzuweisung nach Mayring (Mayring/Fenzl 2019, S. 638 ff.). Die weitere Bearbeitung inkl. Kodierung erfolgte mittels der kostenfrei verfügbaren Plattform QCAmap[1] (Mayring/Fenzl 2019, S. 638). Die Online-Anwendung bietet hardware- und lizenzunabhängige, transparente und reproduzierbare Untersuchungen. Mayring betont, dass die Anwendung nur unterstützend arbeitet und keine eigenständige Analyse durchführt (2023, S. 115 ff.). Die Kategorien wurden auf Grundlage der theoretischen Vorannahmen (technische, rechtliche und ethische Herausforderungen, pädagogische Modelle, interdisziplinäre Ausbildungsansätze), respektive des Interviewleitfadens, entwickelt (Mayring/Fenzl 2019, S. 638 f.). Das Kategoriensystem umfasst die Dimensionen:

- Bedeutung von KI im jeweiligen Fachbereich
- Fachspezifische Herausforderungen
- Kompetenzanforderungen
- Interdisziplinäre Ausbildungsprozesse
- Wirksamkeit interdisziplinärer Ausbildungsformate
- Querschnittliche KI- und Lernaspekte

Auf die Bildung von Unterkategorien wurde verzichtet, da der strukturierte Interviewleitfaden die thematischen Hauptdimensionen bereits deduktiv vorgibt und eine weitere Hierarchisierung angesichts der geringen Fallzahl zu einer methodisch unzweckmäßigen Überfragmentierung des Datenmaterials führen würde. Inhaltliche Nuancen wurden stattdessen über die detaillierten Definitionen und Inklusionskriterien des Kodierleitfadens operationalisiert, um die Fachperspektiven innerhalb der Kategorien vergleichen zu können (Mayring/Fenzl 2019, S. 637 f.). Dieser definiert für jede Kategorie explizite Inklusions- und Exklusionskriterien sowie Ankerbeispiele, um eine nachvollziehbare Zuordnung der Textstellen zu gewährleisten (Diaz-Bone 2022, S. 107 ff.).

Auf klassische objektive Gütekriterien wie Reliabilität, Validität und Objektivität (Flick 2022, S. 533 ff.) wurde verzichtet, da diese primär für quantitative Messverfahren entwickelt wurden und sich nicht auf ein qualitativ-interpretatives Vorgehen mit deduktiv abgeleitetem Kategoriensystem übertragen lassen. Stattdessen orientierte sich die Untersuchung an einer nachvollziehbaren Analyse und transparenter Dokumentation der Kategorienentwicklung, um die Logik des Forschungsprozesses offenzulegen (Diaz-Bone 2022, S. 107 ff.).

[1] qcamap.org/ui/de/home

Ergebnisse

Zentrales Ergebnis ist, dass KI im Ausbildungscurriculum der Polizei gegenwärtig noch keine Berücksichtigung findet. Dennoch lieferte die Auswertung wesentliche Aspekte zur Beantwortung der Leitfrage, insbesondere in Hinblick auf Anforderungen für eine zukünftige Implementierung. Nachfolgend werden die Ergebnisse der Interviews strukturiert ausgewertet.

Bedeutung von KI und ihren fachspezifischen Herausforderungen

[…] es ist doch in meinen Augen auch eine Illusion, wenn man […] sagt, hier, lieber Sachbearbeiter, hast du 128 Gigabyte Daten, werte die mal aus und sag mir hinterher, ob der jetzt irgendwelche terroristischen Verbindungen hatte […]. Weil das schafft ein normaler Mensch […] nicht zu überblicken.

Beide Interviewpartner bewerten KI aus den Perspektiven Technik, Recht und Ethik als zentral, wobei jede Disziplin unterschiedliche Akzentsetzungen vornimmt. Aus technischer Sicht werde KI als unverzichtbares Instrument zur Bewältigung zunehmend komplexer Massendaten verstanden; sie ermögliche die Identifikation von Mustern und das Sichtbarmachen bislang verborgener Zusammenhänge. Im technischen Bereich stünden sowohl Nachwuchskräfte als auch erfahrene Ermittlerinnen und Ermittler vor einer kaum noch manuell beherrschbaren Datenfülle. KI-Anwendungen können die händische Auswertung ablösen und diese Datenbestände zeit- und struktureffizient analysieren. Die schiere Menge an polizeilich zu bearbeitenden Informationen übersteige regelmäßig menschliche Kapazitäten. Die Befragten heben hervor, dass eine effiziente Identifizierung relevanter Hinweise angesichts der Datenlast ohne KI-Unterstützung kaum realisierbar sei. Für die Ausbildung des Nachwuchspersonals bedeutet dies, dass der Umgang mit großen Datenmengen und die Fähigkeit, KI-gestützte Analysewerkzeuge korrekt einzusetzen, frühzeitig trainiert werden sollten.

Die Interviewpartner betonen die Notwendigkeit einer Qualifizierung, die über reine Bedienkenntnisse hinausgeht, um KI-Analysen zielgerichtet nutzen zu können. Da bislang keine systematischen Schulungsangebote bestehen, müsse künftig ein grundlegendes Bewusstsein für verfügbare Datenquellen geschaffen werden – „[…] angefangen bei Handys, über Saugroboter, Autos, WLAN, Hotspots, öffentliche Netzwerke […]“. Ein grundlegendes Bewusstsein für Datenquellen wird von den Experten als Voraussetzung für eine kritische Bewertung der KI-Ergebnisse angeführt. Aus rechtlicher Perspektive werde KI, insbesondere sofern sie gemäß Anhang III der KI-VO für Zwecke der Strafverfolgung oder Gefahrenabwehr eingesetzt wird, als Hochrisiko-Anwendung eingestuft, deren Einsatz strengen formellen und materiellen Anforderungen unterliegt. Eine fundierte rechtliche Bewertung stelle daher die unverzichtbare Grundlage für einen sicheren und rechtskonformen Einsatz dar. Für die Polizei hob Interviewpartner E2 insbesondere die Bedeutung der KI-VO, die noch ausstehende verfassungsrechtliche Bewertung sowie divergierende Landesregelungen hervor. Hinzu treten ungeklärte Haftungsfragen und offene Verantwortlichkeitsstrukturen. Diese Aspekte müssen im Vorfeld einer Einführung in der Ausbildung zukünftiger Polizeibeamtinnen und -beamter sorgfältig integriert werden.

Unter ethischer Perspektive ergibt sich ein Spannungsfeld zwischen den Ermittlungsbefugnissen der Behörde und den Rechten der Betroffenen. Eine zentrale Herausforderung bestehe darin, den Anspruch der menschlichen Letztentscheidung auch angesichts hoch automatisierter Prozesse faktisch zu wahren. Zudem würden die Funktionsweisen der KI das Risiko algorithmischer Verzerrungen (Bias) bergen. Dies führe zu der Gefahr, dass Anwenderinnen und Anwender maschinell erzeugte Ergebnisse im Arbeitsalltag unhinterfragt übernehmen, anstatt diese als fehleranfällige Wahrscheinlichkeiten zu interpretieren. Die Interviews benennen somit verschiedene Aspekte, die im Umgang mit KI herausfordernd sind. Dazu gehören Unsicherheiten hinsichtlich technischer Verfahren, unklare rechtliche Rahmenbedingungen sowie Hinweise auf mögliche ethische Problemfelder.

Kompetenzanforderungen und Wirksamkeit interdisziplinärer Ausbildungsprozesse

Beide Experten fordern ein integriertes Kompetenzprofil, bei dem eine enge Verzahnung technischer, rechtlicher und ethischer Aspekte als unverzichtbar gilt. Auf technischer Ebene müssen zukünftige Ermittlerinnen und Ermittler u. a. ein grundlegendes Verständnis für digitale Spuren und deren Tragweite erlernen sowie die Funktionslogiken von KI erkennen und nachvollziehen können. Dieses Wissen bildet die Basis dafür, dass die Polizeikräfte die Analysewerkzeuge sachgerecht einsetzen und die gewonnenen Informationen korrekt einordnen können. Darüber hinaus betonen die Experten die Notwendigkeit praxisorientierter Übungen, etwa in IT-Forensik und physischer Spurensicherung, um die theoretischen Kenntnisse direkt an realistischen Fallbeispielen zu erproben und zu festigen.

Rechtliche Kompetenzen umfassen die Kenntnis der Voraussetzungen für die Datenverarbeitung, bspw.: „Die Wahrung der Grundrechte der Bürger, […] allgemeines Persönlichkeitsrecht, […] Recht auf informationelle Selbstbestimmung […].“ Darüber hinaus müssen die Ermittlerinnen und Ermittler die Zulässigkeit automatisierter Verfahren bewerten können. Diese Fähigkeiten gewährleisten, dass die Arbeit mit KI den rechtlichen Rahmenbedingungen entspricht und rechtswidrige Eingriffe in die Privatsphäre vermieden werden. Ethische Ausbildungsanteile müssen die Nachwuchskräfte konkret dazu befähigen, diese systemimmanenten Verzerrungen zu identifizieren und KI-Ergebnisse aktiv zu validieren. Das Lernziel sei eine reflexive Urteilskraft, die es den Mitarbeitenden ermögliche, die Grenzen der Systeme zu erkennen und begründete Entscheidungen auch gegen algorithmische Vorschläge treffen zu können. Damit werde die Handlungssicherheit gestärkt, Risiken frühzeitig zu erkennen und Verantwortung im Prozess zu übernehmen. Technische, rechtliche und ethische Anforderungen können nicht isoliert betrachtet werden, weil Entscheidungen in einem Bereich direkte Konsequenzen für den anderen haben. Beispielsweise kann eine technisch korrekt durchgeführte KI-Analyse rechtlich unzulässig sein, wenn sie Datenschutzvorgaben verletzt, und ethisch problematisch, wenn sie systematische Verzerrungen (Bias) verstärkt. Die Interviewaussagen beziehen sich somit auf die parallele Bedeutung technischer, rechtlicher und ethischer Inhalte. Zudem werden praxisorientierte Übungen – etwa in der IT-Forensik – wiederholt als relevante Bestandteile genannt. Die Experteninterviews zeigen eine übereinstimmende Betonung der parallelen Berücksichtigung technischer, rechtlicher und ethischer Inhalte.

Grenzen interdisziplinärer Formate

Trotz des hohen Stellenwerts interdisziplinärer Ausbildungsformate zeigen die Interviews auch deutliche organisatorische Grenzen auf. Interviewpartner E1 verweist darauf, dass die hohe Anzahl an Lehrveranstaltungen und die organisatorische Umsetzung ein erhebliches Problem darstellen: „[…] wenn man allein so eine Lehrveranstaltung jetzt jedes halbe Jahr […] durchführt, dann brauchen wir allein diese eine Lehrveranstaltung 36-mal pro Jahr." Auch die Einbindung externer Experten, etwa aus den Bereichen des LKA, stoße an Kapazitätsgrenzen, da diese nicht in der Lage seien, eine derart hohe Anzahl an Vorträgen regelmäßig zu leisten. Darüber hinaus werde die Wirksamkeit von Vorlesungen im Vollplenum infrage gestellt. Ab 30–40 Teilnehmenden sinke der Erkenntniszuwachs bei Einzelpersonen rapide, wodurch der praktische Kompetenzerwerb eingeschränkt werde. Die kontinuierliche Anpassung der Lehrinhalte an sich verändernde rechtliche Rahmenbedingungen und technische Entwicklungen erfordere zudem einen zusätzlichen Aufwand.

Zudem zeigen die Interviews, dass praxisorientierte Übungen, etwa in IT-Forensik oder physischer Spurensicherung, notwendig sind, um die theoretischen Inhalte zu festigen. Gleichzeitig wird die Umsetzung dieser Übungen durch Zeit- und Ressourcenengpässe limitiert, was die vollständige Integration interdisziplinärer Inhalte erschwere. Die Interviewpartner beschreiben interdisziplinäre Lehrformate abschließend als gewinnbringend im Hinblick auf die Verbindung verschiedener Fachperspektiven. Gleichzeitig bestünden unzureichende organisatorische Rahmenbedingungen, die aus ihrer Sicht Einfluss auf die Realisierung solcher Formate haben.

Diskussion

Die vorliegende Untersuchung zeigt deutlich, dass KI-Anwendungen in der polizeilichen Lehre der Polizei aktuell noch kein struktureller Bestandteil sind. Die befragten Experten schätzen den operativen Einsatz in der Breite als noch nicht vollzogen ein. Interessanterweise steht dieser Befund in einem scheinbaren Widerspruch zu den offiziellen Daten des Bundeskriminalamtes. Die im Extrapol geführte Übersichtskarte (BKA 2025) führt bereits eine Anzahl an Anwendungen im Regelbetrieb sowie diverse in der Erprobung auf. Diese Diskrepanz lässt sich primär durch ein divergentes Begriffsverständnis von ‚Künstlicher Intelligenz' sowie der institutionellen Trennung von akademischer Lehre und operativer Spezialisierung erklären. Aus den Interviews lässt sich ein enges, an den Kriterien des Machine Learning und des EU AI Acts orientiertes Verständnis rekonstruieren, da Experte 1 KI deutlich von bloßer Automatisierung abgrenzt und Experte 2 den Fokus primär auf komplexe Hochrisiko-Systeme legt. Im Gegensatz dazu klassifiziert das BKA offensichtlich bereits automatisierte Datenanalysesysteme unter dem Label KI (BKA 2025). Zudem verdeutlicht der hohe Anteil an Anwendungen, die sich noch in der Entwicklungs- oder Erprobungsphase befinden, dass sich ein Großteil der Technik noch in geschützten Erprobungsräumen befindet (BKA 2025) und somit im Bewusstsein der befragten Dozenten noch nicht als operativer Standard der täglichen Polizeiarbeit angekommen ist. Dies unterstreicht die bestehende Lücke zwischen der technologischen Entwicklung in spezialisierten Dienststellen und deren systematischer Integration in das allgemeine Ausbildungscurriculum.

Die Ergebnisse zeigen, dass Interdisziplinarität in der polizeilichen Ausbildung zum Umgang mit KI von den befragten Experten als didaktisch notwendig eingeschätzt wird. Beide Interviewpartner heben den Mehrwert fachübergreifender Lehrformate sowie die enge Verzahnung von Theorie und Praxis hervor. Zugleich verdeutlicht die quantifizierende Betrachtung, dass die meisten Äußerungen faktisch den fachspezifischen Herausforderungen zuzurechnen sind. Dieses Spannungsverhältnis legt nahe, dass Interdisziplinarität zwar normativ unterstützt wird, in der Umsetzung jedoch häufig durch die berufliche Fachorientierung überlagert wird. Interdisziplinäre Zielsetzungen konkurrieren hierbei sichtbar mit disziplinären Prioritäten und begrenzten Ressourcen, wobei die unterschiedlichen Vorkenntnisse der Lernenden eine zusätzliche didaktische Hürde darstellen (Just 2025, S. 49 f.).

Die theoretische Notwendigkeit methodischer Pluralität spiegelt sich in den empirischen Befunden wider. Konkret bestätigt die Forderung nach Routinebildung durch Übungen die Relevanz behavioristischer Ansätze (Watson 1913; Franken/Franken 2023, S. 201 ff.). Gleichzeitig verweist der Wunsch nach einem intuitiven „Gefühl“ für Datenanalysen auf die Bedeutung konstruktivistischer Erfahrungswerte (Piaget 1923), da hier Wissen erst im Anwendungskontext entsteht. Ergänzend hierzu verweist die von Experte 2 betonte Notwendigkeit, die Entstehung von Bias und die Grenzen der Technik intellektuell nachzuvollziehen, auf unverzichtbare kognitivistische Elemente (Franken/Franken 2023, S. 205 ff.). Die Ausbildungspraxis fordert demnach implizit genau jenen didaktischen Dreischritt, der theoretisch für den Kompetenzerwerb im KI-Kontext hergeleitet wurde. Die Verknüpfung der inhaltlichen Analyse und der quantitativen Betrachtung der Kategorienhäufigkeiten ermöglicht es, die Diskrepanz zwischen der Forderung nach Interdisziplinarität und den fachspezifischen Herausforderungen transparent abzubilden. Die Befunde der Arbeit können für Fragen einer zukünftigen Weiterentwicklung des Curriculums – insbesondere für die Polizei, auch unter organisatorischen Restriktionen wie Kapazitätsgrenzen praxisorientierter Formate − nutzbar gemacht werden. Hierbei sollten nicht zuletzt die identifizierten Spannungsfelder zwischen Anspruch und Umsetzung berücksichtigt werden.

Die begrenzte Generalisierbarkeit aufgrund der geringen Zahl von Experten und der fehlenden Perspektive weiterer Gruppen führt dazu, dass dieser Beitrag keinen Anspruch auf Vollständigkeit erheben, aber wichtige Einblicke in das Forschungsfeld liefern kann (Przyborski/Wohlrab-Sahr 2022, S. 133 f.). Außerdem birgt die Kategorisierung Verzerrungen durch Kodierentscheidungen, insbesondere bei der Gewichtung fachspezifischer gegenüber interdisziplinären Aussagen. Zudem unterliegen rechtliche und technologische Rahmenbedingungen einem raschen Wandel, wodurch einzelne Befunde zeitlich begrenzt gültig sein können; dies bestätigt auch die Einschätzung von Just (2025, S. 50). Schließlich schränkt der Fokus auf ein Bundesland die Übertragbarkeit auf andere Kontexte ein.

Schlussfolgerungen

Die Untersuchung verdeutlicht, dass interdisziplinäre KI-Kompetenzen in der Polizeiausbildung zwar als unverzichtbar anerkannt werden, ihre praktische Umsetzung jedoch erheblichen strukturellen und organisatorischen Restriktionen unterliegt (vgl. auch Just 2025, S. 50). Dass die BKA-Übersichtskarte bereits eine Vielzahl an Anwendungen ausweist, während die Experten eine fehlende Verankerung in der Lehre konstatieren, belegt, dass die techno-

logische Praxis die curriculare Vorbereitung bereits faktisch überholt hat. Angesichts dieser Diskrepanz besteht dringender Handlungsbedarf für eine Überarbeitung des Lehrplans, um die Qualifizierung der Nachwuchskräfte an den aktuellen Stand der technologischen Realität anzupassen. Eine effektive KI-Ausbildung sollte methodisch pluralistisch gestaltet sein: Zur Schaffung technischer Handlungssicherheit empfehlen sich behavioristische Trainingseinheiten (z. B. Tool-Schulungen), während die Reflexion rechtlicher und ethischer Implikationen kognitivistische und konstruktivistische Lehrformate erfordert, um ein tiefgreifendes Verständnis und die notwendige Transferleistung in unvorhersehbaren Einsatzlagen zu ermöglichen. Für die polizeiliche Hochschullehre lassen die Befunde erkennen, dass diese Interdisziplinarität vor allem durch kooperative, kleingruppenbasierte Lehrformen gefördert werden kann. Da die Experten sowohl Praxisorientierung als auch theoretische Fundierung betonen, erscheint zudem eine gezielte Weiterqualifizierung des Lehrpersonals sinnvoll, um fachübergreifende Inhalte konsistent vermitteln zu können.

Auf Ebene der Polizeiführung und Bundesländer weisen die Ergebnisse darauf hin, dass klare rechtliche Rahmenbedingungen die Basis für eine stabile Ausbildung bilden. Die im Material identifizierten Unsicherheiten zur Datenverarbeitung machen deutlich, dass gesetzgeberische Klarheit die Lehre unmittelbar entlastet. Ergänzend kommt der systematisch begleiteten Einarbeitung nach dem Studium eine Schlüsselfunktion zu, um das in der Ausbildung angelegte interdisziplinäre Denken in die fachspezifische Praxis zu überführen. Für zukünftige Forschung bietet sich ein Mixed-Methods-Ansatz an, der die Perspektiven frisch ausgebildeter Nachwuchskräfte einbezieht. Ein solcher Abgleich zwischen curricularer Vermittlung und den realen Anforderungen der Berufspraxis könnte helfen, die identifizierten Spannungsfelder systematischer zu erfassen und die Ausbildungskonzepte dynamisch an die rasante technische Entwicklung anzupassen. Abschließend zeigt sich, dass die hohe Dynamik technologischer Innovationen und die sich fortlaufend konkretisierenden rechtlichen Rahmenbedingungen (z. B. durch Rechtsprechung zum AI Act) eine statische Lehrplangestaltung ausschließen. Vielmehr bedarf es einer kontinuierlichen curricularen Evaluation und Anpassung, um die Handlungssicherheit der Polizeikräfte dauerhaft zu gewährleisten.

Literaturverzeichnis

Anderson, John R. (2000). *Learning and Memory. An Integrated Approach*, 2. Aufl., New York, Chichester, Weinheim, Brisbane, Singapore, Toronto: John Wiley & Sons, Inc.

Bolte, Sascha/Sebastian Lerch (2023). Interdisziplinarität. Eine theoretische Annäherung an einen viel besprochenen Begriff. In: Mirjam Braßler/Simone Brandstädter/Sebastian Lerch (Hrsg.): *Interdisziplinarität in der Hochschullehre. Interdisziplinäre Lehre*, S. 15–30. wbv.de/shop/Interdisziplinaritaet-in-der-Hochschullehre-I74610 (04.12.2025).

Braßler, Mirjam (2023). Interdisziplinäres Lehren und Lernen – Eine Betrachtung aus konstruktivistischer, bildungstheoretischer und konstruktionistischer Perspektive. In: Mirjam Braßler/Simone Brandstädter/Sebastian Lerch (Hrsg.): *Interdisziplinarität in der Hochschullehre. Interdisziplinäre Lehre*, S. 31–44. https://www.wbv.de/shop/Interdisziplinaeres-Lehren-und-Lernen-Eine-Betrachtung-aus-konstruktivistischer-bildungstheoretischer-und-konstruktionistischer-Perspektive-I74610w003 (04.12.2025).

BKA (2025). KIM. KI-System-Map der Polizei (Bundeskriminalamt). Extrapol der Polizeien des Bundes und der Länder.

BvR (2023). ECLI:DE:BVerfG:2023:rs20230216.1bvr154719, Bundesverfassungsgericht. bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/2023/02/rs20230216_1bvr154719.html (09.12.2025).

Dams, Jan/Ulrich Kraetzer (2025). Scam mit KI-Stimmen: Wenn der falsche CEO anruft, hat die Betrugsmasche längst begonnen. In: *Welt*. welt.de/wirtschaft/plus6873a9b51a0a84412c0f19a9/Scam-mit-KI-Stimmen-Wenn-der-falsche-CEO-anruft-hat-die-Betrugsmasche-laengst-begonnen.html (04.12.2025).

Diaz-Bone, Rainer (2022). Messen. In: Nina Baur/Jörg Blasius (Hrsg.): *Handbuch Methoden der empirischen Sozialforschung*, 3. Aufl., Wiesbaden: Springer VS, S. 105–122.

Egbert, Simon/Matthias Leese (2021). *Criminal Futures. Predictive Policing and Everyday Police Work*, Oxford, New York: Routledge.

Eisenmenger, Sven (2024). Grußwort anlässlich des 3. FORSI-Expertenworkshops. In: Sven Eisenberger (Hrsg.): *FORSI-Jahresband 2023. Der Schutz Kritischer Infrastrukturen. Neuregelungen zum Einsatz Künstlicher Intelligenz und Drohnen*, S. 107–112, Stuttgart, München, Hannover, Berlin, Weimar, Dresden: Richard Boorberg Verlag, S. 107–112.

EUCPN (2022). *Artificial intelligence and predictive policing: risks and challenges*, Brüssel. eucpn.org/sites/default/files/document/files/PP%20%282%29.pdf (05.12.2025).

Europäisches Parlament (2023). Was ist künstliche Intelligenz und wie wird sie genutzt? europarl.europa.eu/topics/de/article/20200827STO85804/was-ist-kunstliche-intelligenz-und-wie-wird-sie-genutzt (05.12.2025).

FBI (2024). Child Sexual Abuse Material Created by Generative AI and Similar Online Tools is Illegal. Federal Bureau of Investigation. ic3.gov/PSA/2024/PSA240329 (09.12.2025).

Flick, Uwe (2022). Gütekriterien qualitativer Sozialforschung. In: Nina Baur/Jörg Blasius (Hrsg.): *Handbuch Methoden der empirischen Sozialforschung*, 3. Aufl. Wiesbaden: Springer VS, S. 533–548.

Frank, Alexander (2024). Die EU-Verordnung über Künstliche Intelligenz – ein Bericht aus Brüssel. In: Sven Eisenberger (Hrsg.): *FORSI-Jahresband 2023. Der Schutz Kritischer Infrastrukturen. Neuregelungen zum Einsatz Künstlicher Intelligenz und Drohnen*, S. 107–112, Stuttgart, München, Hannover, Berlin, Weimar, Dresden: Richard Boorberg Verlag, S. 113–120.

Franken, Rolf/Swetlana Franken (2023). *Wissen, Lernen und Innovation im digitalen Unternehmen. Mit Fallstudien und Praxisbeispielen*, 3. Aufl. Köln, Bielefeld: Springer Gabler.

Google/Ipsos (2025). Our life with AI: From innovation to application. static.googleusercontent.com/media/publicpolicy.google/en//resources/ipsos_google_our-life-with-ai_2024_25.pdf (07.12.2025).

Hawking, Stephen (2017). Stephen Hawking at Web Summit 2017. youtube.com/watch?v=H41Zk1GrdRg&t=139s (09.12.2025).

Helfferich, Cornelia (2022). Leitfaden- und Experteninterviews. in: Nina Baur/Jörg Blasius (Hrsg.): *Handbuch Methoden der empirischen Sozialforschung*, 3. Aufl., Wiesbaden: Springer VS, S. 875–892.

Just, Christian (2025). KI-Kompetenzen für Polizeibeamtinnen und -beamte: Die Zukunft der Polizeiausbildung in Baden-Württemberg. In: Wilfried Honekamp (Hrsg.): *Künstliche Intelligenz in der Polizeiarbeit*. *Schriftenreihe der Deutschen Hochschule der Polizei*, Bd. 25, Münster, S. 37–55.

Leffer, Lena (2025). *Automated Suspicion Algorithms. Strafverfolgung durch Künstliche Intelligenz am Beispiel der Geldwäsche. Schriftenreihe zum deutschen, europäischen und internationalen Wirtschaftsstrafrecht*, Bd. 60, Halle-Wittenberg: Nomos Verlagsgesellschaft mbH & Co. KG. doi:10.5771/9783748952831.

Lerch, Sebastian (2019). Interdisziplinäre Kompetenzbildung. Fächerübergreifendes Denken und Handeln in der Lehre fördern, begleiten und feststellen. In: *Nexus Impulse für die Praxis*, Ausgabe 18, S. 2–15.

Magill, Frank Northen (1998). *Psychology Basics*, California, New Jersey: Salem Press, Inc.

Mayring, Philipp (2023). *Einführung in die qualitative Sozialforschung*, Weinheim, Basel: Beltz Pädagogik.

Mayring, Philipp/Fenzl, Thomas (o. J.). Ablaufmodell deduktive Kategorienanwendung. In: QCAmap. qcamap.org/ui/assets/tutorials/de/Ablauf_Regeln_Deduktiv.pdf (03.12.2025).

Mayring, Philipp/Thomas Fenzl (2019). Qualitative Inhaltsanalyse. In: Nina Baur/Jörg Blasius (Hrsg.): *Handbuch Methoden der empirischen Sozialforschung*, 2. Aufl., Wiesbaden: Springer VS, S. 633–648.

Meuser, Michael/Ulrike Nagel (1991). ExpertInneninterviews − vielfach erprobt, wenig bedacht: ein Beitrag zur qualitativen Methodendiskussion. In: Detlef Garz/Klaus Kraimer (Hrsg.): *Qualitativ-empirische Sozialforschung. Konzepte, Methoden, Analysen*, 1. Aufl., Opladen: Springer Fachmedien Wiesbaden, S. 441–471.

Piaget, Jean (1923). *The Origin of Intelligence in the Child*, London: Roudledge & Kegan Paul Ltd.

Pohl, Nils (2024). Das Europäische Gesetz über Künstliche Intelligenz – was kommt auf die Polizei und die Sicherheitswirtschaft zu? In: Sven Eisenberger (Hrsg.): *FORSI-Jahresband 2023. Der Schutz Kritischer Infrastrukturen. Neuregelungen zum Einsatz Künstlicher Intelligenz und Drohnen*, Stuttgart, München, Hannover, Berlin, Weimar, Dresden: Richard Boorberg Verlag, S. 121–146.

Przyborski, Aglaja/Monika Wohlrab-Sahr (2022). Forschungsdesign für die qualitative Sozialforschung. In: Nina Baur/Jörg Blasius (Hrsg.): *Handbuch Methoden der empirischen Sozialforschung*, 3. Aufl., Wiesbaden: Springer VS, S. 123–162.

Rubehn, Nils (2025). Künstliche Intelligenz in der polizeilichen Fortbildung in Baden-Württemberg. In: *MEPA-Fachjournal. KI im Rahmen polizeilicher Aus- und Fortbildung – Möglichkeiten und Grenzen*, Bd. 2, S. 18–25.

Disselkamp, Marcus/Frank Schmiedchen (2026). Strategischer KI-Einsatz in Unternehmen. In: Frank Schmiedchen/Alexander von Gernler/Martina Hafner/Klaus Peter Kratzer (Hrsg.): Künstliche Intelligenz und Wir. Stand, Nutzung und Herausforderungen der KI, Berlin, Kirchheim, Ulm: Springer Vieweg. doi:10.1007/978-3-662-71567-3 (10.12.2025).

Simon, Béla (2025). Künstliche Intelligenz in der polizeilichen Aus- und Fortbildung in Ungarn – die Möglichkeiten und Hindernisse der Nutzung von KI. In: *MEPA-Fachjournal. KI im Rahmen polizeilicher Aus- und Fortbildung – Möglichkeiten und Grenzen*, Bd. 2, S. 12–17.

Watson, John B. (1913). Psychology as the Behaviorist Views It. In: *Psychological Review*, Bd. 20 (2), S. 158–177.

Westle, Bettina (2018). *Methoden der Politikwissenschaft*, 2. Aufl., Baden-Baden: Nomos Verlagsgesellschaft.

Wolfangel, Eva (2022). Fehler haben Konsequenzen für das Leben echter Menschen. In: Manon Bischoff (Hrsg.): Künstliche Intelligenz. Vom Schachspieler zur Superintelligenz?, Berlin, Heidelberg: Springer-Verlag GmbH. doi:10.1007/978-3-662-62492-0 (09.12.2025).

Wörner, Liane (2024). Weg von den Hürden, hin zu den Möglichkeiten: KI in Polizei und Straftatverfolgung. In: *Zeitschrift für die gesamte Strafrechtswissenschaft*, Bd. 136 (3), S. 616–641.

Nutzung von generativer Künstlicher Intelligenz als Large Language Model im Rahmen der polizeilichen Cold-Case-Sachbearbeitung

Alexander Herdt

Die polizeiliche Ermittlungsarbeit befindet sich angesichts derzeitiger Megatrends wie der Globalisierung und Internationalisierung, der fortschreitenden Digitalisierung oder auch neuer technologischer Entwicklungen (Statista, 2025) vor vielfältigen Herausforderungen und muss sich fortlaufend anpassen. Insbesondere der Bereich der technologischen Entwicklungen ist aufgrund der hohen Dynamik hierbei besonders hervorzuheben. Künstliche Intelligenz (KI) gilt als Fortentwicklung der Digitalisierung und Schlüsseltechnologie des 21. Jahrhunderts, welche insbesondere in Form der generativen KI eine bedeutende Rolle im Alltag und Berufsleben der Menschen sowie auch bei Sicherheitsbehörden eingenommen hat (Rupprecht 2023, S. 44). Die Bundesregierung (2020, S. 24) beschreibt in ihrer „Strategie Künstliche Intelligenz der Bundesregierung", dass KI im polizeilichen Kontext dazu beitragen kann, die Leistungsfähigkeit zu steigern, Arbeitsprozesse effizienter und effektiver zu gestalten sowie Mitarbeitende zu entlasten. Die Art und Weise der Strafverfolgung, insbesondere die Möglichkeiten der Analyse komplexer Datensätze sowie der Forensik, wird sich angesichts dieses technologischen Fortschritts stetig weiterentwickeln (Europol 2024, S. 10).

Vor diesem Hintergrund erscheint es von wissenschaftlicher als auch praktischer Relevanz zu sein, wie KI-gestützte Anwendungen in klassischen Ermittlungstätigkeiten, wie beispielsweise der Cold-Case-Sachbearbeitung, unterstützend eingesetzt werden können. Cold Cases sind für die Polizei besonders herausfordernd und stehen gleichzeitig in einem besonderen öffentlichen Fokus. Trotz des Einsatzes von erheblichen personellen und technischen Ressourcen bleibt ein gewisser Teil von Tötungsdelikten ungeklärt (Eberz 2022). In Deutschland existieren rund 3300 Fälle, die als Cold Cases kategorisiert werden (Ziegler 2023). Auch wenn keine offizielle bundesweite Statistik vorliegt, dürfte die Zahl der Fälle in NRW mit über 1100 wohl am höchsten liegen, gefolgt von Baden-Württemberg mit 550 sowie Niedersachen mit 375 Fällen (Spiegel 2021). Die Zahlen verdeutlichen die bundesweite Relevanz des Themas und lassen die kriminalistischen, psychologischen und organisatorischen Herausforderungen erahnen.

Es stellt sich daher die Frage, ob und wie die traditionelle Ermittlungsarbeit durch KI unterstützt werden kann, um den eingeschränkten Personal- und Zeitressourcen effektiv entgegenzutreten. Infolge dieses Spannungsfeldes widmet sich dieser Beitrag der Forschungsfrage:

Welche Stärken und Schwächen besitzt generative KI in Form eines Large Language Models (LLM) im Rahmen der polizeilichen Cold-Case-Sachbearbeitung und welche Chancen und Risiken lassen sich hieran ableiten?

Hintergrund

Der Begriff des polizeilichen Cold Cases ist nicht einheitlich definiert. Gemeint sind schwere Verbrechen, die trotz langjähriger Ermittlungen ungeklärt geblieben sind. Auch wenn sie nicht mehr aktiv bearbeitet werden, bleiben sie strafprozessual anhängig (Pomberger 2017, S. 6). Cold Cases betreffen insbesondere (versuchte) Tötungsdelikte oder Vermisstenfälle, bei denen ein Kapitaldelikt nicht ausgeschlossen werden kann und auch nach Ausschöpfung aller Ermittlungsansätze keine Tatverdächtigen ermittelt oder keine rechtskräftigen Verurteilungen erreicht worden sind (Marquardt 2022). Die Bearbeitung von Cold Cases ist in mehrfacher Hinsicht anspruchsvoll. Zur Veranschaulichung sollen die nachfolgenden persönlichen Erfahrungen als Dienststellenleiter einer Zentralen Kriminalinspektion in Rheinland-Pfalz mit Fachkommissariat für Kapitaldelikte dienen.

In der Regel bearbeiten die Mitarbeitenden jeweils einen Cold Case neben aktuellen Ermittlungsverfahren. Diese Fälle liegen häufig Jahrzehnte zurück und sind durch den Verlust von Zeugen, Beweismitteln und Erfahrungswissen geprägt. Der Aufbau der Ermittlungsakten ist mit heutigen nicht zu vergleichen und sehr heterogen hinsichtlich Qualität, Vollständigkeit und Aufbau. Häufig umfassen sie über 15 Leitzordner mit Vermerken, Spurensicherungs- und Untersuchungsberichten, Zeugenaussagen, Lichtbildmappen und Beschlüssen. Zu Beginn der Bearbeitung werden die Inhalte digitalisiert, als maschinenlesbare Dokumente eingescannt und dem Vorgangsbearbeitungssystem hinzugefügt. Während sich die Originalakten bei den jeweiligen Staatsanwaltschaften befinden, verfügen die Polizeidienststellen über die polizeilichen Zweitschriften. Unterschiedliche Gliederung und Vollständigkeit zwischen Original- und Zweitakte erfordern einen zusätzlichen, zeitaufwändigen Abgleich. Zur Sichtung und dem Aktenstudium werden Programme verwendet, die klassischen PDF-Readern ähneln und lediglich die Suche mittels Suchbegriffs ermöglichen, wobei Treffer farblich markiert werden.

Die Phase des Aktenstudiums stellt die zentrale Herausforderung dar. Sie ist besonders arbeitsintensiv, fehleranfällig und kognitiv belastend. Das wiederholte Lesen, Vergleichen und Schlussfolgern über hunderte Seiten hinweg erschwert es, den Überblick über komplexe Zusammenhänge zu erhalten. Darüber hinaus kommt es durch neu auftretende Kapitaldelikte regelmäßig zu Unterbrechungen. Die Cold-Case-Bearbeitung ist daher nicht nur kriminalistisch, sondern auch organisatorisch und psychisch herausfordernd. Vor diesem Hintergrund stellt sich die Frage, inwieweit generative KI in Form von LLMs diese Phase gezielt unterstützen kann.

Generative KI bildet einen spezialisierten Bereich der KI-Forschung (Illgen et al. 2025, S. 4). Sie umfasst Systeme, die aus Eingaben eigenständig neue Inhalte generieren können, etwa Text-, Audio-, Videodateien, Programmcodes oder 3D-Modelle (Bendel 2023). Ein Großteil aktueller Anwendungen, wie der Chatbot ChatGPT von OpenAI, basiert auf LLMs, die in mehreren Phasen mit umfangreichen Datensätzen trainiert werden (Albrecht 2023, S. 9–10). Diese Sprachmodelle erkennen Zusammenhänge, Gewichtungen und Gruppenzugehörigkeiten und leiten daraus eigenständig Regeln ab, die auf neue Daten angewendet werden (Thüne 2022, S. 17). Vereinfacht dargestellt, handelt es sich bei LLMs um mathematische Modelle, die sequenziell, mit einem wahrscheinlichkeitsbasierten Ansatz, Ausgaben im Kontext der Eingabe erzeugen. Einen vertiefenden Überblick zur Entwicklung und Funktionsweise bietet Blüthgen (2025).

Bereits heute wird generative KI in unterschiedlicher Weise in der polizeilichen Ermittlungsarbeit eingesetzt oder erprobt, z. B. bei der Schuhspurrekonstruktion, Transkriptionen oder der Aufbereitung von Bild- und Videodateien (Weiss 2025). Diese Anwendungen knüpfen jedoch an einem späteren Zeitpunkt des Bearbeitungsprozesses an und setzen eine vorherige umfassende Einarbeitung in die Aktenlage voraus. Trotz vereinzelter Erprobungen von LLMs zur Auswertung großer Datenmengen (Vaughan 2024) besteht weiterhin eine Forschungslücke in diesem Bereich, insbesondere in Deutschland und den dortigen Rahmenbedingungen. Bisherige Untersuchungen befassten sich mit der Nutzung im Kriminaldauerdienst (Gaiser 2025), bei Massendelikten der Alltagskriminalität (Coldewei 2025) oder bei gleichgelagerten Straftaten am Beispiel der EG Corona (Eggert 2025). Eine spezifische Betrachtung des Einsatzes von LLMs in der polizeilichen Cold-Case-Ermittlung erfolgte bislang nicht.

Methodik

Ziel des vorliegenden Beitrags ist es, den Nutzen von generativer KI in Form eines LLM in der polizeilichen Cold-Case-Sachbearbeitung systematisch zu analysieren. Die strategische Einführung von neuen Technologien erfordert in der kriminalpolizeilichen Praxis eine Betrachtung, die über den Aspekt der Effizienz hinausgeht und bspw. auch die Rechtmäßigkeit, Akzeptanz und möglichen Anwendungsrisiken berücksichtigt. Als methodisches Instrument wird hierfür die SWOT-Analyse in bewusster Abweichung von ihrem klassischen Einsatz in den Wirtschaftswissenschaften verwendet (Wollny & Paul 2015, S. 189). Bei dem Begriff handelt es sich um ein Akronym für **S**trenghts, **W**eaknesses, **O**pportunities und **T**hreats (Kaufmann 2021, S. 290).

Die SWOT-Analyse ermöglicht die Darstellung von Chancen und Risiken anhand ermittelter Stärken und Schwächen im Rahmen eines strategischen Entscheidungsprozesses (Dehmel et al. 2017, S. 88–89) und bietet somit ein geeignetes Rahmenmodell, in dem unterschiedliche Perspektiven strukturiert und gleichzeitig flexibel betrachtet sowie kontextbasiert bewertet werden können. Die Analyse erfolgt vorliegend auf Basis einer theoretischen und praxisorientierten Grundlage. Sowohl wissenschaftliche Veröffentlichungen als auch die zuvor geschilderten praxisnahen Erfahrungen werden hierbei berücksichtigt. Die modifizierte SWOT-Analyse erfolgt in mehreren Schritten. Zunächst werden relevante Einflussfaktoren gesammelt und dann den vier SWOT-Kategorien zugeordnet. Die Ergebnisse werden anschließend in einer Vier-Feld-Matrix dargestellt und dienen der anschließenden Diskussion und Bewertung (Kaufmann 2021, S. 291 ff.). Hierbei werden auch die Erkenntnisse von Coldewei, Eggert und Gaiser berücksichtigt.

Ergebnisse

Im Folgenden werden die Ergebnisse der durchgeführten SWOT-Analyse in Bezug auf die Nutzung eines LLM in der Cold-Case-Sachbearbeitung strukturiert nach ihren Kategorien als Matrix dargestellt und anschließend erläutert.

Stärken	**Schwächen**
• Breites Anwendungsspektrum in Analyse, Textgenerierung und Kommunikation • Keine Programmierkenntnisse erforderlich; intuitive Bedienung • Schnelle Verarbeitung großer, unstrukturierter und mehrsprachiger Daten • Fähigkeit zur Extraktion von Entitäten und semantischen Zusammenhängen • Multimodale Verarbeitung verschiedener Dateiformate • Flexible Generierung von Texten; fortlaufende Anpassung durch Dialog • Anpassungs-/Integrationsfähigkeit	• Ergebnisqualität abhängig von Prompts und Trainingsdaten (Bias möglich) • Technische Limitierung • Eingeschränkte Nachvollziehbarkeit und fehlende Erklärbarkeit (Blackbox) • Halluzinationen • Eingeschränkte Reproduzierbarkeit von Ergebnissen
Chancen	**Risiken**
• Automatisierung und Beschleunigung von Analyse-, Dokumentations- und Rechercheprozessen • Entlastung durch Reduktion repetitiver Tätigkeiten • Verbesserung der Informationsgewinnung und Wissenserschließung • Unterstützung bei Hypothesenbildung und Entwicklung neuer Ermittlungsansätze • Verbesserung des Behördenimages	• Fehlendes Vertrauen und mangelnde Fachkompetenz im Umgang mit KI • Bias, insb. Automation Bias • Verstärkung von Vorurteilen und Diskriminierungen • Gerichtliche Verwertbarkeit • Spezifische Datenschutz-, Sicherheits- und Compliance-Risiken • Regulatorische Anforderungen • Missbräuchliche Verwendung und unzureichende Kontrollmechanismen • Kosten

Abbildung 1: Grafische Gegenüberstellung der Ergebnisse der durchgeführten SWOT-Analyse (eigene Darstellung)

Stärken

LLMs zeigen ein breites Anwendungsspektrum. Sie können Aufgaben aus kurzen Texteingaben eigenständig ableiten und in natürlicher Sprache beantworten (Leible et al. 2024, S. 248 ff.). Dabei fungieren sie als Frage-Antwort-Systeme oder Chatbots und erfordern keine Programmierkenntnisse (Albrecht 2023, S. 28). Durch gezieltes Prompt-Engineering lässt sich die Ergebnisqualität optimieren, wenn die Aspekte Rolle, Kontext, Format, Aufgabe und Präzision systematisch berücksichtigt werden (Illgen et al. 2025, S. 4).

Die zentrale Stärke liegt in der Verarbeitung, Analyse und Generierung von Texten (Albrecht 2023, S. 35 ff.). Umfangreiche, unstrukturierte und mehrsprachige Dokumente können mit hoher Geschwindigkeit klassifiziert und inhaltlich erschlossen werden. LLMs erfassen semantische Zusammenhänge, extrahieren Entitäten wie Personen, Orte oder Zeitpunkte und ermöglichen eine strukturierte Darstellung komplexer Inhalte (Bundesamt für Sicherheit in der Informationstechnik (BSI) 2024, S. 7). Neuere multimodale Modelle verarbeiten zusätzlich verschiedene Dateiformate, z. B. Text- und Bilddateien (Leible et al. 2024, S. 249). Darüber hinaus können Große Sprachmodelle Texte in unterschiedlichen Formaten generieren, z. B. als Fließtext oder Stichpunkte bis hin zu Tabellen und Protokollen (Illgen et al. 2025, S.

9–10). Die Ergebnisse lassen sich in dialogischer Form fortlaufend anpassen (Leible et al. 2024, S. 356–357). Auch Zusammenfassungen und Übersetzungen umfangreicher Dokumente sind in variabler Länge möglich (Albrecht 2023, S. 20, 35–36).

Neben der intuitiven Bedienbarkeit und Geschwindigkeit ist vor allem die Anpassungs- und Integrationsfähigkeit hervorzuheben. LLMs können als selbstlernende Systeme auf Nutzerfeedback reagieren und über Programmierschnittstellen (API) in bestehende IT-Infrastrukturen eingebunden werden. Dadurch wird ein Zugriff auf organisationsinterne Datensätze ermöglicht, ohne bestehende Systeme vollständig zu ersetzen (ebd., S. 26, 32–33).

Schwächen

Die Qualität der Ergebnisse hängt wesentlich von den Eingaben (Prompts) und den zugrunde liegenden Trainingsdaten ab (BSI 2024, S. 10–15; Albrecht 2023, S. 11). Zudem besteht eine spezifische technische Limitierung der Eingabelänge, weshalb zu umfangreiche Texte nicht verarbeitet werden können (Leible et al. 2024, S. 359). Aufgrund ihres komplexen Aufbaus weisen LLMs eine Blackbox-Eigenschaft auf (Fähndrich & Labudde 2023, S. 154), welche die Erklärbarkeit, Nachvollziehbarkeit und Quellenzuordnung einschränkt (Albrecht 2023, S. 43, 68, 81; Wildhirt et al. 2025, S. 120–121; Kreyßing 2025, S. 81–82). Dies bedeutet, dass es schwer nachzuvollziehen ist, auf welche Art und Weise eine Ausgabe des LLM generiert worden ist und auf welche Daten dabei zurückgegriffen wurde.

Da Inhalte dabei auf Basis statistischer Wahrscheinlichkeiten erzeugt werden (BSI 2024, S. 10), können formal plausible, aber faktisch unzutreffende Ergebnisse entstehen, sog. Halluzinationen (Farwick & Pohlmann 2023, S. 63). Zudem sind Ergebnisse oft nicht reproduzierbar, da wiederholte, identische Eingaben zu unterschiedlichen Ergebnissen führen können (Albrecht 2023, S. 68; BSI 2024, S. 10). Verzerrungen in den Trainingsdaten, etwa in Bezug auf Geschlecht, Nationalität oder Alter, können zudem Bias-Effekte hervorrufen und zu diskriminierenden Inhalten führen (BSI 2024, S. 13; Kreyßing 2025, S. 75–80).

Chancen

Der Einsatz von LLMs als digitaler Assistent bietet vielfältige Potenziale (Illgen et al. 2025, S. 9–10; Leible et al. 2024, 354–357). Besonders in Textverarbeitung, Entscheidungsunterstützung und Dokumentation können Prozesse automatisiert und beschleunigt werden (BSI 2024, S. 7; Breiter et al. 2025, S. 1215). Dies könnte die Effektivität sowie Effizienz steigern und gleichzeitig die Ermittlerinnen und Ermittler entlasten (Kreyßing 2025, 65–68). Durch die Automatisierung wiederkehrender Tätigkeiten könnten Kapazitäten für andere kriminalistische Aufgaben entstehen (Albrecht 2023, S. 80; Leible et al. 2024, S. 346, 366).

Auch in der Informationsgewinnung und dem Wissensmanagement zeigen sich deutliche Vorteile. Große, teils unstrukturierte Datenmengen lassen sich kontextbezogen und dialogisch erschließen, ohne auf eine klassische Stichwortsuche angewiesen zu sein (Farwick & Pohlmann 2023, S. 65; Breiter et al. 2025, S. 1215; Europol 2024, S. 18–20, 30). Darüber hinaus können Hypothesen überprüft, neue Ermittlungsansätze generiert und alternative Szenari-

en entwickelt werden (Leible et al. 2024, S. 355; Kunze 2019, S. 26–29). Schließlich kann der sichtbare Einsatz moderner KI-Systeme zu einem innovationsorientierten Behördenimage und einer positiven öffentlichen Wahrnehmung beitragen (Kreyßing 2025, S. 61, 112–113).

Risiken

Der erfolgreiche Einsatz von LLMs setzt Vertrauen und entsprechende Fachkompetenz voraus (Wildhirt et al. 2025, S. 120–121). Unpräzise Prompts können falsche oder irreführende Ergebnisse erzeugen (Leible et al. 2024, S. 363). Besonders kritisch ist die unreflektierte Übernahme solcher Ergebnisse (sog. Automation Bias) (Farwick & Pohlmann 2023, S. 64; BSI 2024, S. 10). Dadurch können bestehende Vorurteile und Diskriminierungen verstärkt (Albrecht 2023, S. 68) und gleichzeitig gegen Art. 3 GG und das Allgemeinen Gleichbehandlungsgesetz verstoßen werden (Kreyßing 2025, S. 165–168). Werden Ergebnisse ohne menschliche Kontrolle übernommen, gefährdet dies insgesamt die Vertrauenswürdigkeit in solche KI-Systeme (Wildhirt et al. 2025, S. 120). Daneben stellen halluzinierte oder diskriminierende Ergebnisse ebenfalls ein grundsätzliches Risiko für die Vertrauenswürdigkeit Großer Sprachmodelle dar (Albrecht 2023, S. 39–41, 68). Zudem mindert die eingeschränkte Reproduzierbarkeit von Ergebnissen (BSI 2024, S. 11; Kreyßing 2025, S. 81–82) die gerichtliche Verwertbarkeit (Leible et al. 2024, S. 358).

Auch datenschutzrechtlich bestehen erhebliche Risiken (Wildhirt et al. 2025, S. 121), da eine automatisierte Verarbeitung personenbezogener Daten in jeder Verarbeitungsphase einen Grundrechtseingriff darstellt (BVerfG 2023, 1 BvR 1547/19; 1 BvR 2634/20). Entsprechende präventive Ermächtigungsgrundlagen liegen bislang nur teilweise in einzelnen Polizeigesetzen vor. Es bleibt unklar, ob sich die Datenverarbeitung auch auf die bisherigen Ermächtigungsnormen der StPO zu Zwecken der Strafverfolgung stützen lassen (Bundesrechtsanwaltskammer (BRAK) 2024, S. 22). Die KI-Verordnung klassifiziert KI-Systeme zur Strafverfolgung jedenfalls als Hochrisiko-Anwendungen (Artikel 6 Absatz 2 i. V. m. mit Anhang III KI-VO) und stellt dementsprechend hohe regulatorische Anforderungen.

Darüber hinaus ergeben sich ethische Fragen hinsichtlich der Verantwortlichkeit und zum Vertrauen in algorithmisch gestützte Entscheidungen (Deutscher Ethikrat 2023, S. 170–176). Ebenso bestehen Compliance- und Sicherheitsrisiken, etwa durch die Möglichkeit unautorisierter Zugriffe von außen, Datenabflüsse sowie die fehlende Datenhoheit bei externen, cloudbasierten Lösungen (Albrecht 2023, S. 41, 83; BSI 2024, S. 11, 16 ff.; Kreyßing 2025, S. 182, 412, 438–439). Nicht zuletzt besteht zudem die Gefahr einer missbräuchlichen Benutzung des LLMs, was verbindliche Anwendungsrichtlinien erforderlich werden lässt (Breiter et al. 2025, S. 1215–1218; Wildhirt et al. 2025, S. 120–122). Nicht zuletzt besteht auch das Risiko hoher Entwicklungs- und Wartungskosten, insbesondere bei Eigenentwicklungen oder häufigen Softwareupdates, was eine zusätzliche organisatorische Herausforderung darstellen kann (Albrecht 2023, S. 29–30, 53; Breiter et al. 2025, S. 1217; Wildhirt et al. 2025, S. 121).

Diskussion

Das nachfolgende Kapitel bewertet die Ergebnisse, ordnet sie in den Kontext vergleichbarer Studien von Eggert (2025), Gaiser (2025) sowie Coldewei (2025) ein und betrachtet Limitationen. Die Ergebnisse zeigen, dass LLMs ein erhebliches Potenzial zur Effizienzsteigerung in der Cold-Case-Sachbearbeitung besitzen, zugleich aber mit signifikanten Risiken verbunden sind. Besonders in der Phase des repetitiven und oftmals unterbrochenen Aktenstudiums könnten Große Sprachmodelle durch die schnelle Verarbeitung unstrukturierter Textdaten und die Erzeugung kontextbezogener Ausgaben deutliche Arbeitsentlastungen bewirken.

Im Dialog könnten sich Ermittlerinnen und Ermittler bspw. einen Überblick über Akteninhalte verschaffen sowie Auflistungen aller Vernehmungen und gesicherter Spuren oder Asservate erstellen lassen. Einzelne Vernehmungen könnten zusammengefasst und mit anderen in Bezug auf Übereinstimmungen oder Widersprüche abgeglichen werden. Die Spuren- und Asservatenlisten könnten nützliche Informationen bereithalten, wie z. B. den letztmaligen Zeitpunkt einer kriminaltechnischen Untersuchung. Auf Grundlage dieser Informationen könnten dann weitere Entscheidungen getroffen werden, etwa welche Personen nochmals vernommen werden sollten bzw. noch nicht umfassend vernommen wurden oder welche Spuren mit den neuesten kriminaltechnischen Möglichkeiten erneut untersucht werden könnten. Über diesen Dialog und die daraus gewonnenen Erkenntnisse könnte dann ein Ermittlungsvermerk oder Auswertebericht durch das Sprachmodell erstellt und der Ermittlungsakte als letztmaliger Bearbeitungsstand hinzugefügt werden. Sofern der Cold Case erst wieder in einigen Jahren durch eine andere Person überprüft werden sollte, kann auf diesen Bearbeitungsvermerk zurückgegriffen werden. Die hier geschilderten Arbeitsschritte könnten durch den Einsatz eines Sprachmodells in kürzester Zeit durchführbar sein und einen signifikanten Zeitgewinn darstellen. Auch bei einer Unterbrechung der Ermittlungsarbeit könnte auf den Dialog mit dem Sprachmodell zurückgegriffen werden, sodass die weiteren Ermittlungen zügig fortgeführt werden könnten. Eine manuelle Erledigung dieser Arbeitsschritte und erneute Einarbeitung in die Ermittlungsakten ist in der Praxis derzeit noch mit einem erheblichen Mehraufwand und einer potenziellen Fehleranfälligkeit verbunden.

Einige der hier dargestellten Befunde korrespondieren mit Gaiser (2025), der im Kriminaldauerdienst ähnliche Strukturierungs- und Automatisierungseffekte beschreibt. Während Gaiser jedoch den Fokus auf den Echtzeitbetrieb legt, zeigt der vorliegende Beitrag, dass die Vorteile von LLMs auch in retrospektiven, dokumentenbasierten Prozessen zu sehen sind. Hier dominieren die Informationskomplexität, Aktenheterogenität und der Verlust ursprünglichen Wissens. Der Einsatz eines LLM in einer kontrollierten, rechtlich abgesicherten Umgebung kann Fehlinterpretationen reduzieren, ohne Effizienzvorteile einzubüßen, und dabei die Akzeptanz sowie die gerichtliche Verwertbarkeit positiv beeinträchtigen.

Auch im Vergleich zu Eggert (2025), der LLMs bei massenhaften, gleichgelagerten Betrugsdelikten während der Corona-Pandemie untersuchte, unterscheidet sich die vorliegende Befassung. Statt strukturierter Daten und standardisierter Ermittlungsabläufe zeichnen sich Cold-Case-Ermittlungen durch heterogene, teils unvollständige Aktenbeständen aus. Hierbei tritt die Stärke generativer Textverarbeitung deutlicher hervor. Insbesondere die Fähigkeit, semantische Bezüge zwischen Akteninhalten herzustellen, könnte Ermittlerinnen und Ermittlern neue Hypothesen und Zusammenhänge aufzeigen. Coldewei (2025) fokussiert in

seiner Untersuchung auf Massendelikte und repetitive Prozesse, während der vorliegende Beitrag technologische Potenziale mit kriminalpsychologisch geprägten Ermittlungsprozessen verbindet. LLMs könnten dabei eine innovative Durchsicht von Akteninhalten ermöglichen, Hypothesen vorstrukturieren sowie Beziehungsgeflechte zwischen Spuren und Personen übersichtlich und schnell abbilden, was einen bislang kaum untersuchten Funktionsbereich darstellt.

Interpretation im Kontext bestehender Forschung

Dieser Beitrag erweitert den Forschungsstand, indem er LLMs erstmals systematisch auf Cold-Case-Ermittlungen anwendet, ein Feld mit hohen kognitiven Anforderungen, fragmentierten Informationslagen und psychologischer Belastung. Die Ergebnisse zeigen auf, dass Große Sprachmodelle nicht als autonome Systeme, sondern als Assistenzsysteme eine sinnvolle Ergänzung darstellen können. Die in der SWOT-Analyse herausgearbeiteten Stärken, etwa die schnelle Verarbeitung unstrukturierter Daten und die intuitive Bedienbarkeit, stehen im Spannungsfeld zu Schwächen und Risiken, wie mangelnder Nachvollziehbarkeit (Blackbox-Charakter), Bias und Halluzinationen. Das Risiko des Automation Bias dürfte diese Problematik verstärken. Somit erfordert der Einsatz ein ausgewogenes Verhältnis zwischen Automatisierung und menschlicher Kontrolle (sog. Human-in-the-Loop).

Die Chancenanalyse verdeutlicht, dass LLMs geeignet sind, kognitive wie organisatorische Engpässe zu überwinden. Eine Integration als interner Ermittlungsassistent im Einklang mit den Anforderungen an vertrauenswürdige KI könnte qualitative Fortschritte bringen, ohne menschliche Expertise zu verdrängen. Besonders innovativ ist der Fokus auf das Aktenstudium als neuralgischer Punkt in der polizeilichen Ermittlungsarbeit. Anders als bei Eggert und Geiser wird hierbei besonders die semantische Rekonstruktion alter Ermittlungsakten beleuchtet. Somit handelt es sich um ein Einsatzfeld, in dem generative KI die kognitiven Fähigkeiten der Ermittlerinnen und Ermittler entlasten und kriminalistische Schlussfolgerungen verbessern könnte.

Zentrale Risiken betreffen die Aspekte Datenschutz, Bias und rechtliche Rahmenbedingungen. Der Status als Hochrisiko-Technologie im Sinne der KI-VO impliziert besondere regulatorische Pflichten, die derzeit technisch wie organisatorisch nur eingeschränkt erfüllt werden können (Blackbox-Problematik). Zudem bestimmte das BVerfG hohe rechtliche Hürden für die automatisierte Datenanalyse in der Prävention, sodass für den Bereich der Repression wohl eine entsprechend hohe rechtliche Anforderung zu erwarten ist. Es dürfte fraglich sein, ob die bisherigen Regeln der StPO den jüngsten Anforderungen genügen. Für den internen Polizeieinsatz zeigt sich zudem ein Defizit an technischer Governance sowie auch in der gerichtlichen Verwertbarkeit. In Anbetracht der Blackbox-Problematik dürften technische Lösungen nicht nur wünschenswert, sondern vielmehr unumgänglich sein. Darüber hinaus könnten Große Sprachmodelle die Ermittlungsarbeit von einer linearen Informationsauswertung zu einem dialogischen Erkenntnisprozess mit dokumentierten Zwischenschritten verändern. Dies würde sich sowohl in moderne Ansätze kooperativer Mensch-Maschine-Systeme (Huchler et al. 2020, S. 5–6) als auch in das Paradigma der Augmented Intelligence (Kreipp 2021) einfügen.

Limitationen

Der vorliegende Beitrag kombiniert theoretische und praxisbezogene Elemente und überträgt sie erstmals auf den Cold-Case-Kontext. Dadurch konnten technische, rechtliche und forensische Dimensionen ganzheitlich betrachtet werden. Dabei muss aber beachtet werden, dass die Analyse auf theoretischen Grundlagen und einer Praxisreflexion beruht, jedoch nicht auf empirischen Feldtests. Notwendige praktische Erprobungen fehlen, ebenso wie eine quantitative Validierung. Die Ergebnisse spiegeln zudem den Stand der Technik zum Untersuchungszeitpunkt wider und sind daher nur bedingt übertragbar. Zudem unterliegt die Bewertung der rasanten technologischen Entwicklung. Modelle, die heute führend sind, können binnen kürzester Zeit überholt sein. Gleichermaßen könnten technische Durchbrüche zur Reduzierung der Blackbox-Problematik führen. Ferner bleibt unklar, inwieweit Erkenntnisse zu strukturierten Daten auf heterogene Aktenlandschaften übertragbar sind. Das hohe Potenzial der LLMs für Textanalysen im Cold-Case-Kontext ist plausibel, empirisch aber nur eingeschränkt gestützt. Zusätzlich hängt die tatsächliche Wirksamkeit stark vom Reifegrad der Organisationsstruktur, dem Digitalisierungsstand und den Kompetenzen der Mitarbeitenden ab.

Schlussfolgerungen

Die Ergebnisse legen nahe, dass der gezielte Einsatz von LLMs in der Cold-Case-Sachbearbeitung deutliche Effizienz- und Qualitätsgewinne ermöglichen kann, insbesondere in der Phase der Informationserschließung, Hypothesengenerierung und Dokumentation. Große Sprachmodelle können ein wirksames Instrument zur Bewältigung begrenzter Ressourcen darstellen, sofern sie in ein rechtlich abgesichertes und organisatorisch reflektiertes Gesamtkonzept eingebettet sind. Eine bloße technische oder institutionelle Implementierung genügt jedoch nicht. Erforderlich sind flankierende Kontrollmechanismen und die Gewährleistung, dass Entscheidungen stets durch Menschen getroffen werden. Die Einbindung von LLMs würde tiefgreifende organisatorische Veränderungen bewirken, vergleichbar mit den von Coldewei (2025, S. 121–122) beschriebenen Transformationsprozessen bei Massendelikten.

Für die polizeiliche Praxis ergibt sich daher die Notwendigkeit, Pilotprojekte unter kontrollierten Bedingungen zu initiieren, um Wirksamkeit, Fehleranfälligkeit und rechtliche Zulässigkeit empirisch zu prüfen. Datenschutzbeauftragte, IT-Sicherheitsstellen und juristische Fachbereiche sollten hierbei frühzeitig und kontinuierlich eingebunden werden. Für die Forschung eröffnet sich die Perspektive, qualitative Analysen durch empirische Untersuchungen zu ergänzen. Fragen der Bias-Kontrolle, Ergebnisvalidierung und Systemintegration bieten Ansatzpunkte für interdisziplinäre Folgearbeiten (Fähndrich & Labudde 2023). Auch ethische Fragestellungen, wie etwa zur Verantwortungszuschreibung bei fehlerhaften KI-Ergebnissen, bleiben weiterhin zentral. In Anbetracht der neu erlassenen Eingriffsermächtigungen für den Einsatz von KI im Bereich der Gefahrenabwehr wäre eine entsprechende Anpassung der repressiven Eingriffsermächtigungen zu prüfen und gegebenenfalls auf eine gesetzgeberische Anpassung hinzuarbeiten.

Im Ergebnis stellen LLMs kein Allheilmittel für ungelöste Fälle dar, besitzen jedoch das Potenzial, die Effizienz, Erkenntnistiefe und Qualität der polizeilichen Sachbearbeitung zu steigern. Der Erfolg hängt von klaren Rahmenbedingungen, Transparenzmechanismen und mensch-

licher Kontrolle ab. Erst das Zusammenspiel von technologischem Fortschritt, organisatorischer Anpassung und rechtlicher Regulierung ermöglicht eine verantwortbare Integration in die polizeiliche Praxis. Die Chancen dürften überwiegen, sofern der Mensch als interpretierende Instanz im Zentrum verbleibt und der technische Stand den rechtlichen Anforderungen entspricht. Der Ansatz, generative KI als Unterstützungssystem für kognitive und dokumentarische Prozesse zu verstehen, eröffnet neue Perspektiven für eine lernende, moderne Polizeiarbeit im digitalen Zeitalter. Dabei sollte KI nicht als Ersatz, sondern als Werkzeug polizeilicher Erkenntnisarbeit im Sinne einer Augmented Intelligence verstanden werden.

Literaturverzeichnis

Albrecht, S. (2023). ChatGPT und andere Computermodelle zur Sprachverarbeitung. Grundlagen, Anwendungspoteniale und mögliche Auswirkungen. Berlin, Deutschland. Von publikationen.bibliothek.kit.edu/1000158070/150614893 (22.12.2025).

Bendel, O. (2023). *Generative KI*. Von Wirtschaftslexikon Gabler: wirtschaftslexikon.gabler.de/definition/generative-ki-124952/version-388556 (22.12.2025).

Blüthgen, C. (2025). Technische Grundlagen großer Sprachmodelle. *Die Radiologie*, S. 227−234.

Breiter, K., Lohmann, T., Stahl, B., Zilmans, C., Reischl-Lenz, B., & Gimpler, H. (2025). Generative KI in der Finanzbranche: Strategische, technologische und organisationale Implementierung am Beispiel der DZ BANK AG. *HMD Praxis der Wirtschaftsinformatik*, S. 1212−1230.

Bundesamt für Sicherheit in der Informationstechnik (BSI) (2024). *Große KI-Sprachmodelle. Chancen und Risiken für Industrie und Behörden.* Von BSI-Bund: bsi.bund.de/DE/Service-Navi/Presse/Alle-Meldungen-News/Meldungen/LLM-Chancen-Risiken_240502.html (12.12.2025).

Bundesrechtsanwaltskammer (BRAK) (2024). *Stellungnahme Nr. 1, Januar 2024. Reformvorschläge für das Strafrecht und den Strafprozess angesichts der Digitalisiserung*. Von BRAK: brak.de/fileadmin/05_zur_rechtspolitik/stellungnahmen-pdf/stellungnahmen-deutschland/2024/stellungnahme-der-brak-2024-01.pdf (01.12.2025).

Bundesregierung (2020). *Strategie Künstliche Intelligenz der Bundesregierung.* Von Das Publikationsportal − Die Bundesregierung: https://www.publikationen-bundesregierung.de/pp-de/publikationssuche/strategie-kuenstliche-intelligenz-der-bundesregierung-2415392 (10.08.2025).

Coldewei, T. (2025). Einsatz von Künstlicher Intelligenz bei der polizeilichen Sachbearbeitung von Massendelikten der Alltagskriminalität. In: W. Hohnekamp: *Künstliche Intelligenz in der Polizeiarbeit. Schriftenreihe der Deutschen Hochschule der Polizei. Band 25* (S. 110−126). Münster: Deutsche Hochschule der Polizei − Hochschulverlag.

Dehmel, K., Götz, J., & Otten, H. (2017). Analyse ausgewählter QM-Instrumente und aufgabengerechte Anpassung für den Einsatz bei strategischen Entscheidungen. In: H. Otten, J. Götz, & S. Pollak: *Heutige und zukünftige Herausforderungen an die Qualitätswissenschaft in Forschung und Praxis* (S. 85−109). Erlangen: FAU University Press.

Deutscher Ethikrat (2023). *Mensch und Maschine − Herausforderungen durch Künstliche Intelligenz.* Von Deutscher Ethikrat: ethikrat.org/presse/mitteilungen/ethikrat-kuenstliche-intelligenz-darf-menschliche-entfaltung-nicht-vermindern/ (15.11.2025).

Eberz, D. (2022). *Mord verjährt nie: Ein Chefermittler erklärt, wie Cold Cases nach Jahrzehnten wieder aufgerollt werden*. Von Rhein-Zeitung: rhein-zeitung.de/mord-verjaehrt-nie-ein-chefermittler-erklaert-wie-cold-cases-nach-jahrzehnten-wieder-aufgerollt-we_arid-2479436.html (15.10.2025).

Eggert, C. (2025). Potenziale der Nutzung von Lage Language Models bei der Bearbeitung von gleichgelagerten Straftaten − Eine Szenarioanalyse am Beispiel der EG Corona. In: W. Hohnekamp: *Künstliche Intelligenz in der Polizeiarbeit. Schriftenreihe der Deutschen Hochschule der Polizei. Band 25* (S. 127−145). München: Deutsche Hochschule der Polizei − Hochschulverlag.

Europol (2024). *AI and policing. The benefits and challenges of artificial intelligence for law enforcement.* Von Europol: europol.europa.eu/publications-events/publications?q=Ai%20and%20policing (01.12.2025).

Fähndrich, J., & Labudde, D. (2023). Vertrauen ist schlecht, Kontrolle ist besser. In: W. Hohnekamp & J. Fähndrich: *Polizei-Informatik 2023* (S. 154−171). Remscheid: Re Di Roma-Verlag.

Farwick, P., & Pohlmann, N. (2023). Vom angemessenen Umgang mit künstlicher Sprachintelligenz. Chancen und Risiken von ChatGPT. *IT-Sicherheit*, S. 62−65.

Gaiser, F. (2025). Anwendungsmöglichkeiten von Large Language Models beim Kriminaldauerdienst der Polizei Baden-Württemberg. In: W. Hohnekamp: *Künstliche Intelligenz in der Polizeiarbeit. Schriftenreihe der Deutschen Hochschule der Polizei. Band 25* (S. 166−185). Münster: Deutsche Hochschule der Polizei − Hochschulverlag.

Huchler, N., Adolph, L., André, E., Bauer, W., Bender, N., Neuburger, R., Suchy, O. (2020). Kriterien für die Mensch-Maschine-Interaktion bei KI. Ansätze für die menschengerechte Gestaltung in der Arbeitswelt. München, Bayern, Deutschland. Von plattform-lernende-systeme.de/files/Downloads/Publikationen/AG2_Whitepaper2_220620.pdf (20.12.2025).

Illgen, K.-M., Hein, L., & Thomas, O. (2025). Generative Künstliche Intelligenz als digitales Werkzeug für Kreativität: Status quo und Implikationen für Forschung und Praxis. *HMD Praxis der Wirtschaftsinformatik*. doi.org/10.1365/s40702-025-01179-3.

Kaufmann, T. (2021). *Strategiewerkzeuge aus der Praxis. Analyse und Beurteilungen der strategischen Ausgangslage.* Bregenz: Springer.

Kreipp, A.-S. (2021). *Assisted, Augmented und Autonomous Intelligence. Die Evolution von Künstlicher Intelligenz*. Von Magazin des Fraunhofer Instituts für Kognitive Systeme IKS: safe-intelligence.fraunhofer.de/artikel/die-evolution-von-kuenstlicher-intelligenz (10.12.2025).

Kreyßing, R. (2025). *Verwaltungsentscheidungen durch Künstliche Intelligenz.* Oldenburg: Springer.

Kunze, D. (2019). Künstliche Intelligenz im kriminalpolizeilichen Kontext. *Der Kriminalist* (7), S. 26−29.

Leible, S., Gücük, G.-L., Simic, D., von Brackel-Schmidt, C., & Lewandowski, T. (2024). Zwischen Forschung und Praxis: Fähigkeiten und Limitationen generativer KI sowie ihre wachsende Bedeutung in der Zukunft. S. 344−370.

Marquardt, A. (2022). *Cold Case-Erfahrungen aus Sicht der Staatsanwaltschaft*. Von KSV Polizeipraxis: ksv-polizeipraxis.de/cold-case-erfahrungen-aus-sicht-der-staatsanwaltschaft/ (10.10.2025).

Pomberger, G. T. (2017). Strafrechtliche und kriminalwissenschaftliche Aspekte bei der Bearbeitung von „Cold Cases“ in Österreich. Graz, Steiermark, Österreich.

Rupprecht, R. (2023). Künstliche Intelligenz unterstützt den Sicherheitsdienstleister. (B. B. Sicherheitswirtschaft, Hrsg.) *Der Sicherheitsdienst*, S. 44−48.

Spiegel (2021). *Mehr als 3000 Tötungsdelikte in Deutschland sind ungeklärt*. Von Spiegel: spiegel.de/panorama/justiz/mehr-als-3000-toetungsdelikte-in-deutschland-sind-laut-einem-medienbericht-ungeklaert-a-58b3f4b2-6897-45b0-b66e-46e045f1e376 (01.11.2025).

Statista (2025). *Megatrends: Globale Entwicklungen der Zukunft*. Von Statista: de.statista.com/themen/3274/megatrends/#topicOverview (20.12.2025).

Thüne, M. (2022). Anwendungsfelder und Potenziale algorithmenbasierter Polizeiarbeit. In: K. Pfeffer: *Algorithmic Policing − Chancen und regulative Herausforderungen* (S. 15−25). Göttingen: Cuvillier Verlag.

Vaughan, H. (2024). *AI tool that can do ‚81 years of detective work in 30 hours‘ trialled by police*. Von Sky News: news.sky.com/story/ai-tool-that-can-do-81-years-of-detective-work-in-30-hours-trialled-by-police-13220891 (15.11.2025).

Weiss, S. (2025). *Spurensuche mit KI-Einsatz. Ist das die Revolution in der Verbrechensbekämpfung? Wie KI dabei hilft, Cold Cases zu lösen*. Von Web: web.de/magazine/panorama/revolution-verbrechensbekaempfung-ki-hilft-cold-cases-loesen-41150332 (15.11.2025).

Wildhirt, K., Bub, U., & Vogel, M. (2025). Generative KI erfolgreich in Unternehmen implementieren. *Wirtschaftsinformatik & Management*. doi.org/10.1365/s35764-025-00558-1.

Wollny, V., & Paul, H. (2015). Die SWOT-Analyse: Herausforderungen der Nutzung in den Sozialwissenschaften. In: M. Niederberger & S. Wassermann: *Methoden der Experten- und Stakeholdereinbindung in der sozialwissenschaftlichen Forschung* (S. 189−213). Wiesbaden: Springer.

Ziegler, J.-O. (2023). *Diese Spezialeinheiten sollen alte Verbrechen aufklären – aber funktioniert das überhaupt?* Von Spiegel: spiegel.de/panorama/warum-cold-case-einheiten-nicht-jeden-fall-loesen-und-dennoch-wichtig-sind-a-6a7ca177-4633-49c1-99e9-c07af5a8588e (12.11.2025).