



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

Künstliche Intelligenz in der Polizeiarbeit

herausgegeben von Wilfried Honekamp

**Band
25**




Schriftenreihe
der Deutschen Hochschule der Polizei

ISBN 978-3-945856-27-7



9783945856277

Honekamp, Wilfried (Hrsg.), Künstliche Intelligenz in der Polizeiarbeit – Schriftenreihe der DHPol, Band 25

 Schriftenreihe
der Deutschen Hochschule der Polizei
neue Folge

Band 25



hrsg. vom Kuratorium der Deutschen
Hochschule der Polizei

Künstliche Intelligenz in der Polizeiarbeit

herausgegeben von Wilfried Honekamp

Münster, 2025

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:

Ltd. Polizeidirektor i. H. Günther Epple
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 978-3-945856-27-7
ISSN 1865-0430

Inhaltsverzeichnis	5
Vorwort (Uwe Marquardt und Antonio Vera)	9
Polizeiarbeit durch Künstliche Intelligenz unterstützen (Wilfried Honekamp)	11
Polizei 4.0: Herausforderungen bei der Einführung von Systemen der Künstlichen Intelligenz (Benjamin Coors)	19
KI-Kompetenzen für Polizeibeamtinnen und -beamte: Die Zukunft der Polizeiausbildung in Baden-Württemberg (Christian Just)	37
Einfluss von Virtual Reality und KI- gesteuerten Trainingsprogrammen auf die Entscheidungsfindung von Polizeikräften (Philipp Rauthe)	56
Einsatz von Künstlicher Intelligenz bei der Polizei und deren gesellschaftliche Akzeptanz (Carolina Döring)	74
Menschliche oder Künstliche Intelligenz? Eine Konzeption für einen experimentellen Aufbau zur Erforschung der Effizienz von KI im Zusammenhang mit Bilderkennung (David Preuß)	92
Einsatz von Künstlicher Intelligenz bei der polizeilichen Sachbearbeitung von Massendelikten der Alltagskriminalität (Thomas Coldewei)	110

Potenziale der Nutzung von Large Language Models bei der Bearbeitung von gleichgelagerten Straftaten – Eine Szenarioanalyse am Beispiel der EG Corona (Christian Eggert)	127	Der retrograde biometrische Abgleich mit allgemein öffentlich zugänglichen Daten aus dem Internet (Paul Haacker)	288
Die Implementierung eines multifunktionalen Large Language Models in der polizeilichen Sachbearbeitung – Eine anwenderbezogene Technikfolgenabschätzung (Philipp Kreutzer)	146	Gemeinsamkeiten und Unterschiede der Datenschutz-Folgenabschätzung (DSFA) gem. Art. 35 DSGVO und der Grundrechte-Folgenabschätzung (GFA) gem. Art. 27 KI-Verordnung (Simon Kraft)	306
Anwendungsmöglichkeiten von Large Language Models beim Kriminaldauerdienst der Polizei Baden-Württemberg (Frank Gaiser)	166	Verzeichnis der Autorinnen und Autoren	322
Einführung eines auf Künstlicher Intelligenz basierenden Chatbots in das polizeiinterne Soziale Netzwerk null1 5 der Polizei des Landes Niedersachsen – Eine Machbarkeitsuntersuchung (Lars Schröder)	186		
Potenzial von Chatbots für das Online-Anzeigeverfahren der Bayerischen Polizei (Volker Hemmert)	204		
Einsatz von Technologien zur Detektion von Messern im öffentlichen Raum (Koray Habel)	226		
Der Einsatz von Künstlicher Intelligenz im Geldwäsche-Transaktionsmonitoring (Manuel Lubos)	248		
Drohnengestützte Wide-Area Surveillance-Systeme als Zukunftstechnik für die deutsche Polizei – Eine SWOT-Analyse (Marvin Mayer)	267		

Vorwort

Uwe Marquardt und Antonio Vera

Die Deutsche Hochschule der Polizei (DHPol) ist die zentrale Bildungseinrichtung für den höheren Polizeidienst in Deutschland. Als universitäre Hochschule, getragen von den Innenministerien des Bundes und der Länder, vereint sie akademische Exzellenz mit der praxisnahen Ausbildung zukünftiger Führungskräfte der Polizei. Mit ihrem Masterstudiengang „Öffentliche Verwaltung – Polizeimanagement“ bietet sie Polizeibeamtinnen und -beamten eine fundierte, wissenschaftlich basierte und zugleich praxisorientierte Qualifikation für Führungsaufgaben. Zusätzlich ermöglicht der berufs begleitende Masterstudiengang „Public Governance and Democratic Resilience“ interdisziplinäre Weiterbildung für Fach- und Führungskräfte aus sicherheitsrelevanten Organisationen. Ergänzt wird das Angebot durch ein breites Fortbildungsprogramm, das jährlich zahlreiche Teilnehmende aus dem In- und Ausland anzieht. Neben Lehre und Fortbildung ist die Forschung ein zentrales Standbein der DHPol, um aktuelle und zukünftige Herausforderungen im Sicherheitsbereich wissenschaftlich zu beleuchten und praxisnahe Lösungen zu entwickeln.

Innovative Lehrmethoden sind ein entscheidender Bestandteil unseres Bildungsansatzes. Die Kombination aus modernen digitalen Formaten, interaktiven Lernmethoden und praxisorientierten Fallstudien ermöglicht es unseren Studierenden, sich gezielt auf die komplexen Herausforderungen der Polizeiarbeit vorzubereiten. Gerade in Zeiten des digitalen Wandels ist es essenziell, dass sich auch die Polizeiausbildung an diesen Entwicklungen orientiert und kontinuierlich weiterentwickelt. Ein herausragendes Beispiel für eine dieser Entwicklungen ist der zunehmende Einfluss der Künstlichen Intelligenz (KI) auf die Polizeiarbeit. Prof. Dr. Wilfried Honekamp widmet sich in seiner Forschung intensiv den Auswirkungen und Potenzialen von KI im polizeilichen Kontext. Seine Arbeiten analysieren unter anderem, wie KI-gestützte Systeme zur Datenanalyse, zur Verbrechensprävention oder zur Unterstützung polizeilicher Ermittlungen genutzt werden können. Dabei legt er besonderes

Augenmerk auf die rechtlichen und ethischen Implikationen dieser Technologien und die Notwendigkeit einer verantwortungsvollen Implementierung. Es ist unabdingbar, dass sich alle Führungskräfte der Polizei mit diesem Thema auseinandersetzen, um die Chancen der KI sinnvoll zu nutzen und mögliche Risiken frühzeitig zu erkennen und zu minimieren.

Die in diesem Buch versammelten wissenschaftlichen Arbeiten unserer Studierenden verdeutlichen, dass diese weit über die Erfüllung akademischer Anforderungen hinausgehen. Sie leisten damit einen wichtigen Beitrag zum Wissenstransfer zwischen Wissenschaft und Praxis. Die Ergebnisse dieser Arbeiten haben das Potenzial, innovative Ansätze für die Polizeiarbeit zu liefern und Impulse für zukünftige Forschung und Entwicklung zu setzen sowie zur – gerade in diesen Zeiten so wichtigen – staatlichen Resilienz beizutragen. Dies unterstreicht die zentrale Rolle der DHPol als Schnittstelle zwischen wissenschaftlicher Forschung und praktischer Polizeiarbeit. Wir danken allen Studierenden, die mit ihren Arbeiten einen wertvollen Beitrag zur Weiterentwicklung der Polizeiarbeit und -wissenschaften leisten und die Diskussion über die Rolle der KI in diesen zunehmend an Bedeutung gewinnenden Themenfeldern bereichern. Wir wünschen allen Leserinnen und Lesern eine inspirierende Lektüre und neue Denkanstöße für die Zukunft der polizeilichen Führung und Praxis.

Polizeiarbeit durch Künstliche Intelligenz unterstützen

Wilfried Honekamp

Künstliche Intelligenz (KI) ist kein Zukunftsszenario mehr, sondern hat sich zu einer omnipräsenten Schlüsseltechnologie entwickelt, die nahezu alle Lebensbereiche durchdringt. Ob in der Medizin, Mobilität oder Kommunikation – KI verändert grundlegend, wie wir arbeiten, leben und miteinander interagieren (Schreiber & Jensen, 2023; Initiative Intelligente Vernetzung, 2018). Gerade dort, wo komplexe Entscheidungsprozesse auf riesige Datenmengen treffen, bietet KI einzigartige Potenziale. Diese reichen von der Automatisierung routinemäßiger Aufgaben über intelligente Entscheidungsunterstützungssysteme bis hin zur Vorhersage zukünftiger Ereignisse und Entwicklungen. KI ermöglicht nicht nur schnellere und genauere Analysen, sondern trägt auch maßgeblich zur Innovation bei, indem sie Prozesse optimiert und bislang unerkannte Muster und Zusammenhänge sichtbar macht (Stryker & Kavlakoglu, 2024). Gleichzeitig wirft ihre zunehmende Verbreitung aber auch grundlegende ethische, rechtliche und gesellschaftliche Fragen auf, die eine verantwortungsvolle Gestaltung ihres Einsatzes erfordern (Deutscher Ethikrat, 2023).

Die Anforderungen an die Polizeibehörden wachsen stetig, während das zur Verfügung stehende Personal vielerorts stagniert (Anders, 2024). Polizeikräfte müssen heute nicht nur mit steigenden Fallzahlen und komplexeren Kriminalitätsformen umgehen, sondern auch gigantische Datenmengen bewältigen. Vor diesem Hintergrund wird Künstliche Intelligenz zu einem entscheidenden Faktor für eine effiziente und effektive Strafverfolgung (Povalej et al., 2021). Dies zeigt sich u. a. an den polizeilichen Netzwerken und Arbeitsgruppen, die sich ausschließlich mit der Thematik KI befassen. Im Netzwerk der Single Points of Contact treffen sich regelmäßig die Ansprechpartner:innen zur KI der Polizeien der Bundesländer und des Bundes sowie der Deutschen Hochschule der Polizei (DHPol) und tauschen sich zu den aktuellen Entwicklungen der KI mit Relevanz zur Polizeiarbeit aus. Die Informationen werden dann als Multiplikatoren an die Länder, den Bund und die DHPol weitergegeben. Die Arbeitsgemeinschaft der Leiter der Landeskriminalämter mit

dem Bundeskriminalamt befasste sich im März 2024 mit der EU-KI-Verordnung und richtete eine Bund-Länder-Arbeitsgruppe zur Evaluation der Auswirkungen auf die Polizeiarbeit ein. Diese erhob die KI-Systeme der Polizeien des Bundes und der Länder und kategorisierte sie gemäß den Risikostufen der KI-Verordnung.

Auch der wissenschaftliche Diskurs verdeutlicht die Bedeutung der KI für die Strafverfolgungsbehörden. Kemme und Honekamp (2024) untersuchen in einem Projekt die Auswirkungen der KI auf die zukünftige Polizeiarbeit. Ein Teil dieses Projekts war die Bestandsaufnahme im Rahmen eines wissenschaftlichen Side Events auf dem Europäischen Polizeikongress in Berlin im April 2024. Dabei wurden technische, rechtliche und gesellschaftliche Aspekte der KI umfassend diskutiert. Von der KI-gestützten Auswertung von Kriminalitätsereignissen (Hamborg, Hall & Kahr, 2024) und polizeilichen Sachbearbeitung (Waldtmann, 2024) über Predictive Policing und KI-gestützte Wahrheitsfindung im Strafverfahren (Preuß, 2024) bis zu ethischen Herausforderungen zeigte die Veranstaltung die Relevanz der Thematik.

Auch die Fachtagung Polizei-Informatik im März 2024 in Mittweida setzte sich intensiv mit verschiedenen Anwendungsszenarien auseinander, beispielsweise mit der Nutzung generativer KI zur Analyse von Malware (Ernst & Fähndrich, 2024), den Potenzialen und Gefahren von Large Language Models (Brunnbauer, 2024) oder den Auswirkungen der EU-KI-Verordnung auf die smarte Gesichtserkennung (Pfeffer, 2024). Ergänzt wurden diese Diskurse durch die 2. Konferenz der Cyberkriminalologie, die im Juli 2024 an der Hochschule der Polizei des Landes Brandenburg in Oranienburg insbesondere die Auswirkungen der KI auf die Entstehung von Kriminalität sowie die Chancen und Herausforderungen für die Kriminalwissenschaften thematisierte (Rüdiger & Ehlert, 2024). Ebenfalls widmete sich das vom LKA Bayern (2024) im November 2024 veranstaltete 11. Internationale Symposium „Keue Technologien“ mit dem Leitthema „Künstliche Intelligenz – Polizeiarbeit und Gesellschaft der Zukunft – Chancen und Herausforderungen“ den aktuellen Entwicklungen wie KI-gestützten Befragungstechniken, digitalen Spürmethoden und der automatischen Detektion von Gewaltdarstellungen.

Die Europäische Union hat die regulatorischen Herausforderungen erkannt und mit der EU-KI-Verordnung einen umfassenden rechtlichen Rahmen geschaffen. Besonders relevant für die Polizeiarbeit sind dabei die Vorgaben zu Hochrisiko-KI-Systemen, die sicherstellen sollen, dass automatisierte Entscheidungsprozesse transparent, nachvollziehbar und diskriminierungsfrei erfolgen. Für die Polizeibehörden bedeutet dies eine klare Verpflichtung: Der Einsatz von KI muss ethischen Grundsätzen folgen, Algorithmen müssen audittierbar sein und die finale Entscheidungskompetenz darf nicht an Maschinen abgegeben werden. Dies erfordert nicht nur technische und rechtliche Anpassungen, sondern auch eine fundierte Ausbildung der Polizeikräfte, um die Chancen und Risiken der KI-Technologien richtig bewerten zu können. Seit dem Sommer 2024 wird an der DHPol Künstliche Intelligenz als fester Bestandteil der Polizeiausbildung gelehrt. In speziell entwickelten Modulen werden die Grundlagen, Möglichkeiten und Grenzen der Technologie vermittelt, wobei sowohl technologische als auch kriminologische, rechtliche und ethische Aspekte berücksichtigt werden. Die in diesem Band versammelten Arbeiten sind im Rahmen dieser Lehrveranstaltungen entstanden und zeigen die Vielfalt der KI-Anwendungen in der Polizeiarbeit. Sie decken ein breites Themenspektrum ab, das von praxisnahen Fallstudien über technische Innovationen bis hin zu rechtswissenschaftlichen Analysen reicht.

Benjamin Coors befasst sich in seinem Beitrag „Polizei 4.0: Herausforderungen bei der Einführung von Systemen der Künstlichen Intelligenz“ mit den rechtlichen, ethischen und organisatorischen Herausforderungen, vor denen Polizeibehörden bei der Implementierung von KI-Systemen stehen. Dabei hebt er insbesondere die Notwendigkeit einer klaren gesetzlichen Grundlage sowie umfassender Schulungen für die Mitarbeitenden hervor. Im Artikel „KI-Kompetenzen für Polizeibeamtinnen und -beamte: Die Zukunft der Polizeiausbildung in Baden-Württemberg“ diskutiert Christian Just die Bedeutung spezifischer KI-Kompetenzen in der Polizeiausbildung, um die wachsenden technologischen Anforderungen im Polizeialltag bewältigen zu können. Dabei betont er, dass neben technischen Fähigkeiten insbesondere ethische und kritische Bewertungsfähigkeiten im Umgang mit KI vermittelt werden müssen. Philipp Rauthe

beschäftigt sich in seinem Beitrag „Einfluss von Virtual Reality und KI-gesteuerten Trainingsprogrammen auf die Entscheidungsfindung von Polizeikräften“ mit den Potenzialen und Grenzen von VR- und KI-Technologien im polizeilichen Verhaltenstraining. Echtzeit-Analysen emotionaler Zustände und Stressniveaus während virtueller Trainings stehen dabei im Mittelpunkt. Der Artikel „Einsatz von Künstlicher Intelligenz bei der Polizei und deren gesellschaftliche Akzeptanz“ von Carolina Döring analysiert gesellschaftliche und ethische Herausforderungen beim Einsatz von KI in der Polizei. Sie beleuchtet systematisch Faktoren, die die öffentliche Akzeptanz beeinflussen, und diskutiert mögliche Spannungsfelder zwischen Sicherheit, Selbstbestimmung und Datenschutz.

David Preuß präsentiert in seinem Beitrag „Menschliche oder Künstliche Intelligenz? Eine Konzeption für einen experimentellen Aufbau zur Erforschung der Effizienz von KI im Zusammenhang mit Bilderkennung“ ein Konzept für einen experimentellen Ansatz zur Bewertung der Effektivität von KI im Vergleich zur menschlichen Bilderkennung. Dabei liegt der Schwerpunkt auf strafrechtlich relevanten Inhalten und deren effizienter, präziser Bearbeitung durch KI-Systeme. Im Beitrag „Einsatz von Künstlicher Intelligenz bei der polizeilichen Sachbearbeitung von Massendelikten der Alltagskriminalität“ thematisiert Thomas Coldewei gezielt die Möglichkeiten und Herausforderungen des Einsatzes von KI bei der Bearbeitung einfacher Straftaten mit geringer Schwere, jedoch hohem Aufkommen. Er analysiert, wie durch den gezielten Einsatz von KI-Systemen, insbesondere von Large Language Models, repetitive und wenig anspruchsvolle Aufgaben automatisiert werden könnten. Coldewei unterstreicht dabei zugleich die Notwendigkeit einer kritischen Begleitung dieses Transformationsprozesses, um mögliche Risiken wie Datenschutzverletzungen, Fehlentscheidungen und Akzeptanzprobleme innerhalb und außerhalb der Polizei zu minimieren.

Christian Eggert untersucht in seinem Beitrag „Potenziale der Nutzung von Large Language Models bei der Bearbeitung von gleichgelagerten Straftaten“ anhand der Ermittlungsgruppe Corona, wie KI die Qualität und Geschwindigkeit der polizeilichen Berichterstattung erheblich verbessern könnte. „Die Implementierung eines multi-

funktionalen Large Language Models in der polizeilichen Sachbearbeitung“ von Philipp Kreutzer betrachtet die Folgen des KI-Einsatzes für polizeiliche Anwender und beleuchtet technische, rechtliche sowie organisatorische Herausforderungen. Frank Gaiser analysiert in seinem Beitrag „Anwendungsmöglichkeiten von Large Language Models beim Kriminaldauerdienst der Polizei Baden-Württemberg“ das Potenzial von KI im Bereich der täglichen kriminalpolizeilichen Arbeit sowie die damit verbundenen praktischen Herausforderungen. Lars Schröder untersucht die Machbarkeit und Vorteile eines KI-basierten Wissensmanagements für interne Prozesse und Wissensverwaltung im Artikel „Einführung eines auf Künstlicher Intelligenz basierten Chatbots in das Polizeiliche Soziale Netzwerk null1|5 der Polizei des Landes Niedersachsen“. Die Chancen und Risiken des Einsatzes von Chatbots für das Online-Anzeigeverfahren der Bayerischen Polizei beleuchtet Volker Hemmert in seinem Beitrag und zeigt Möglichkeiten zur Steigerung von Anzeigenqualität und Bearbeitungseffizienz auf.

Im Kapitel „Einsatz von Technologien zur Detektion von Messern im öffentlichen Raum“ thematisiert Koray Habel innovative KI-Technologien zur präventiven und mobilen Erkennung von Waffen sowie die Herausforderungen beim praktischen Einsatz. Manuel Lubos analysiert im Beitrag „Der Einsatz von Künstlicher Intelligenz im Geldwäsche-Transaktionsmonitoring“ Möglichkeiten, mittels KI Geldwäschemuster frühzeitig zu erkennen und gleichzeitig Fehlalarme zu reduzieren. Im Kapitel „Drohngestützte Wide-Area Surveillance Systeme als Zukunftstechnik für die deutsche Polizei“ diskutiert Marvin Mayer Stärken, Schwächen, Chancen und Risiken der KI-gestützten Drohnenüberwachung. Paul Haacker setzt sich mit den technischen Möglichkeiten und rechtlichen Herausforderungen auseinander, die mit dem retrograden biometrischen Abgleich öffentlich zugänglicher Online-Daten verbunden sind. Die vergleichende Analyse „Gemeinsamkeiten und Unterschiede der Datenschutz-Folgenabschätzung (DSFA) gem. Art. 35 DSGVO und der Grundrechte-Folgenabschätzung (GFA) gem. Art. 27 KI-Verordnung“ von Simon Kraft liefert abschließend Einblicke in die Anforderungen hinsichtlich Datenschutz und Grundrechtsschutz.

Aus diesen Arbeiten lässt sich schlussfolgern, dass es unabdingbar ist, die zukünftigen Führungskräfte der Polizeien des Bundes und der Länder frühzeitig und umfassend mit KI vertraut zu machen, um diese Technologie sicher, effektiv und verantwortungsvoll in der Polizeiarbeit zu nutzen. Nur wer die Möglichkeiten ebenso wie die Grenzen und Risiken der KI genau kennt, kann fundierte und verantwortungsvolle Entscheidungen treffen. Die Integration von KI in die polizeiliche Ausbildung an der DHPol ist daher ein entscheidender Schritt, um diesen Herausforderungen adäquat begegnen zu können und die Polizeiarbeit auch zukünftig auf höchstem Niveau sicherzustellen.

Abschließend sei angemerkt, dass für die Erstellung der meisten Arbeiten, inklusive dieses Leitartikels, Large Language Models als Unterstützungswerkzeuge eingesetzt wurden. Diese Modelle haben das Potenzial, die Qualität wissenschaftlicher Arbeiten deutlich zu verbessern. Aufgrund ihrer systemimmanenten Neigung zum sogenannten „Halluzinieren“ müssen sie jedoch kritisch reflektiert und verantwortungsvoll eingesetzt werden. Auch diese wichtige Erkenntnis nehmen die Studierenden in ihren zukünftigen Berufsalltag mit.

Literaturverzeichnis

Anders, S. (2024) Gute Ausbildung ist nicht verhandelbar! DP – Deutsche Polizei Nordrhein-Westfalen. Düsseldorf. gdp.de/Nordrhein-Westfalen/DP/2024/DP09_2024.pdf (11.03.2025)

Brunnbauer, M. (2024) Potentiale und Gefahren von Large Language Models aus der polizeilichen Sicht. In: Honekamp, W. & Labudde, D. (Hrsg.) Polizei-Informatik 2024. Rediroma Verlag Remscheid. S. 234-239

Deutscher Ethikrat (2023) Mensch und Maschine – Herausforderungen durch Künstliche Intelligenz. Stellungnahme. Berlin. ethikrat.org/fileadmin/Publikationen/Stellungnahmen/deutsch/stellungnahme-mensch-und-maschine.pdf (11.03.2025)

Ernst, F. & Fähndrich, J. (2024) Einfach gelagerte Malware-Analysen im Zeitalter generativer KI-Sprachmodelle. In: Honekamp, W. & Labudde, D. (Hrsg.) Polizei-Informatik 2024. Rediroma Verlag Remscheid. S. 46-54

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

Initiative Intelligente Vernetzung (2018) Künstliche Intelligenz – Impulse zu einem Megatrend. Roland Berger GmbH. Berlin. bmwk.de/Redaktion/DE/Publikationen/Technologie/kuenstliche-intelligenz-impulse-zu-einem-megatrend.pdf (11.03.2025)

Kemme, S. & Honekamp, W. (2024) Impact of AI on the Future Work of Law Enforcement Agencies. AI Research EXPO. CeNoS and Inter-KI, Universität Münster

LKA Bayern (2024) 11. Internationales Symposium „Neue Technologien“ am 06. und 07. November 2024 in Fürstfeldbruck. Pressemitteilung. Bayerisches Landeskriminalamt. polizei.bayern.de/aktuelles/pressemitteilungen/075763 (11.03.2025)

Pfeffer, K. (2024) Die EU-Regulierung des Einsatzes künstlicher Intelligenz: Auswirkungen der KI-VO auf die Sicherheitsbehörden insbesondere bei der „smarten Gesichtserkennung“. In: Honekamp, W. & Labudde, D. (Hrsg.) Polizei-Informatik 2024. Rediroma Verlag Remscheid. S. 55-66

Povalej, R., Rittelmeier, H., Fähndrich, J., Berner, S., Honekamp, W. & Labudde D. (2021) Die Enkel von Locard. Informatik Spektrum 44, S. 355-363. doi.org/10.1007/s00287-021-01393-5

Preuß, T. (2024) Chancen und Risiken KI-basierter Wahrheitsfindung im Strafverfahren. In: Honekamp, W. & Labudde, D. (Hrsg.) Polizei-Informatik 2024. Rediroma Verlag Remscheid. S. 247-258

Rüdiger, T.-G. & Ehlert, C. (2024) Programm der 2. Konferenz der Cyberkriminologie. Hochschule der Polizei des Landes Brandenburg, Oranienburg. hpolbb.de/article/save-date-2-konferenz-der-cyberkriminologie-11-juli-2024 (11.03.2025)

Schreiber, P. & Jensen, J.-C. (2023) KI und Digitale Transformation: Was kommt auf Unternehmen und die Gesellschaft zu? Bundesverband Digitale Wirtschaft e.V. bvdw.org/news-und-publikationen/ki-und-digitale-transformation-was-kommt-auf-unternehmen-und-die-gesellschaft-zu (11.03.2025)

Stryker, C. & Kavlakoglu, E. (2024) Was ist künstliche Intelligenz (KI)? IBM Deutschland GmbH. Böblingen. ibm.com/de-de/think/topics/artificial-intelligence (11.03.2025)

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

Polizei 4.0: Herausforderungen bei der Einführung von Systemen der Künstlichen Intelligenz

Benjamin Coors

Künstliche Intelligenz (KI) hat in den letzten Jahren in vielen Bereichen des gesellschaftlichen Lebens an Bedeutung gewonnen. Die ihr zugrunde liegende Fähigkeit, erhebliche Datenmengen zu verarbeiten, darin Muster zu erkennen und in der Folge Entscheidungsprozesse zu unterstützen, macht sie auch zu einem für die Polizeiarbeit relevanten Instrument (Europol Innovation Lab 2024, S. 10-11). Das Bundeskriminalamt veranstaltet seit 1954 jährlich (mit Ausnahme des Corona-Jahrs 2020) die BKA-Herbsttagung, in deren Rahmen aktuell vordringliche Themen der Polizeiarbeit bzw. der Kriminalitätsbekämpfung diskutiert werden. Das Thema des Jahres 2024 lautete „Auf der Spur mit KI – wie KI die polizeiliche Welt revolutioniert“. Nicht zuletzt diese prominente und öffentlichkeitswirksame Platzierung verdeutlicht den aktuellen und weiter zunehmenden Stellenwert der Thematik rund um Künstliche Intelligenz in Polizeibehörden. Auch in der breiten Öffentlichkeit wird der vielfältige polizeiliche Nutzen von Systemen der Künstlichen Intelligenz regelmäßig diskutiert, beispielsweise bei der polizeilichen Textauswertung (Brauns 2022), der Gesichtserkennung (tagesschau.de 2024) oder auch durch die Nutzung von Sprachmodellen oder dem „Predictive Policing“ (Schwarzbeck 2024).

Dem polizeilichen Einsatz dieser vielversprechenden Technologien geht jedoch eine umfangreiche Befassung mit den begleitenden spezifischen Rahmenbedingungen dieser Systeme voraus, die Polizeibehörden vor diverse Herausforderungen stellt. Diese ergeben sich nicht zuletzt aus der besonderen gesetzlichen Stellung der Polizei und der Notwendigkeit, mit hochsensiblen, oft personenbezogenen Daten umzugehen. Darüber hinaus unterscheiden sich Systeme der Künstlichen Intelligenz in unterschiedlicher Ausprägung von klassischen informationstechnischen Systemen. Die Integration von Künstlicher Intelligenz in die Polizeiarbeit erfordert daher eine sorgfältige Betrachtung aller in diesem Kontext stehenden Rahmenbedingungen.

Ziel dieses Beitrags ist es, die bei der Einführung von Systemen der Künstlichen Intelligenz vorhandenen Herausforderungen von Polizeiorganisationen zu identifizieren, zu kategorisieren und damit einen Überblick über die wesentlichen Handlungsfelder zu geben. Hierfür wurde zunächst eine Literaturrecherche durchgeführt, um den bestehenden Forschungsstand zu sichten. Die in diesem Rahmen gewonnenen Erkenntnisse wurden kategorisiert und die Ergebnisse im Kapitel „Hintergrund“ zusammengefasst. In einem Folgeschritt wurden die zuvor gebildeten Kategorien mithilfe von offenen Interviewfragen an Experten aus zwei Polizeibehörden überprüft, um die Literaturrecherche um polizeipraktische Aspekte zu ergänzen und Schwerpunkte abzuleiten. Auf dieser Grundlage werden im Hintergrund zunächst die Erkenntnisse aus der Literaturrecherche dargestellt. Anschließend wird die soeben grob veranschaulichte Vorgehensweise im Detail erläutert. Dann werden die Ergebnisse der Experteninterviews dargestellt und darauffolgend in Verknüpfung mit den Befunden der Literaturrecherche diskutiert. Der vorliegende Beitrag endet mit den Schlussfolgerungen, die sich aus den insgesamt gewonnenen Ableitungen zusammensetzen.

Hintergrund

Im Folgenden werden die Themenfelder vorgestellt, die von der Literatur als zentrale Herausforderungen bei der Implementierung von KI-Systemen im Allgemeinen und in Polizeibehörden im Speziellen benannt und betrachtet werden. Die Ergebnisse der Literaturrecherche wurden in sieben Kategorien gegliedert. Für jede dieser Kategorien wurden die in dem jeweiligen Zusammenhang vorrangig diskutierten Themenfelder priorisiert.

Rechtliche Rahmenbedingungen

Die Polizei als Exekutivorgan des Staates ist in besonderem Maße an Recht und Gesetz gebunden. Dieser Umstand ergibt sich insbesondere aus dem sensiblen, umfangreichen und oftmals personenbezogenen Datenbestand, der von den Polizeibehörden des Bundes und der Länder erhoben und verwaltet wird. In der Folge ist bei der

Verwendung von personenbezogenen Daten durch ein System der Künstlichen Intelligenz beispielsweise das Recht auf informationelle Selbstbestimmung regelmäßig tangiert (Bitkom e.V. 2023, S. 12).

Vor diesem Hintergrund ist für das einzuführende System der Künstlichen Intelligenz u. a. zunächst spezifisch zu prüfen, für welche (grund-)rechtliche Reichweite dieses vorgesehen ist, welchen Datenbestand dieses verarbeiten soll sowie ob ein bzw. welcher Rechtsrahmen für den konkreten Einsatz einschlägig ist (Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit 2024, S. 4).

Auf europäischer Ebene ist mit Wirkung vom 01.08.2024 die EU-KI-Verordnung in Kraft getreten, die den Rechtsrahmen innerhalb der Europäischen Union harmonisieren soll und unter anderem Regelungen für Systeme der Künstlichen Intelligenz geordnet nach Risikoklassen enthält (Die Bundesregierung 2024). Auf nationaler Ebene enthalten je nach Einsatzzweck Landespolizeigesetze teilweise Regelungen für den Einsatz von Künstlicher Intelligenz. Darüber hinaus können die Datenschutz-Grundverordnung (DSGVO) sowie das Bundesdatenschutzgesetz (BDSG) bzw. analog die Landesdatenschutzgesetze betroffen sein (Bundesministerium des Innern und für Heimat 2024, S. 18).

Ethische Rahmenbedingungen

In der Literatur wird im Hinblick auf ethische Überlegungen überwiegend das Leitbild beschrieben, dass der Einsatz Künstlicher Intelligenz die menschlichen Fähigkeiten unterstützen, erweitern und verbessern sowie grundsätzlich wertorientiert arbeiten soll (Bitkom e.V. 2023, S. 12). Darüber hinaus müssen KI-Anwendungen insbesondere bei der Polizei frei von Diskriminierung von Herkunft, Geschlecht oder Sexualität sein (Bitkom e.V. 2023, S. 13). Grundsätzlich lässt sich jedoch feststellen, dass Computersysteme nicht zwingend vorurteilsfrei arbeiten und frei von Verzerrungen sind (Dechesne et al. 2019, S. 16). In diesem Zusammenhang häufig genannt wird die Problematik des Auftretens voreingenommener Ergebnisse, der sog. KI-Bias (IBM und Holdsworth 2023). Dieser KI-Bias kann in unterschiedlichen Ausprägungen vorkommen, zum Beispiel durch die bei der Entwick-

lung in das KI-System übertragene Einstellung und subjektive Empfindung der Entwicklerinnen und Entwickler (sog. Algorithmic Bias) oder auch durch die bereits vorurteilsbehaftete Datengrundlage des KI-Systems (sog. Big Data Bias) (European Crime Prevention Network 2022, S. 11). In der Literatur werden darüber hinaus noch etliche weitere ethische Fragestellungen diskutiert, zum Beispiel die bewusste oder unbewusste Abgabe der Entscheidungshoheit an KI-Systeme oder auch positive Feedback-Schleifen, durch die bereits verzerrte Ergebnisse sich selbst und damit die zugrunde liegende Verzerrung bestätigen (European Crime Prevention Network 2022).

Polizeibehörden stehen damit bei der Einführung entsprechender Systeme vor der Herausforderung, sowohl eine grundsätzliche ethische Haltung im Hinblick auf den Einsatz von KI zu entwickeln als auch für das jeweils konkret betrachtete System eine ethische Betrachtung über die Funktionsweise und den Einsatz zu erstellen (Deutscher Ethikrat 2023, S. 330-332).

Technologische Rahmenbedingungen

Grundsätzlich bestehen bei der Einführung von Systemen der Künstlichen Intelligenz in Polizeibehörden auch die Herausforderungen, die bei der Einführung klassischer IT-Systeme festzustellen sind, beispielsweise bei der Integration in bestehende Umgebungen (Multishoring 2024) oder bei der Betrachtung der IT- und Datensicherheit, z. B. im Hinblick auf Schwachstellen und Hackingangriffe (Dechesne et al. 2019, S. 22). Im Hinblick auf Systeme der Künstlichen Intelligenz werden in der Literatur jedoch einige Themen benannt, die in diesem Kontext von hervorgehobener Bedeutung sind. So ist die Qualität der für das KI-System bereitgestellten Daten und die Trainingsphase die Grundlage für eine erfolgreiche Anwendung (Bitkom e.V. 2023, S. 14). Darüber hinaus ist insbesondere für Systeme der Künstlichen Intelligenz eine umfassende Dokumentation und Protokollierung vorzusehen, um die Wirkweise des Systems und den damit ggf. verbundenen staatlichen Eingriff im Nachhinein überprüfen zu können (Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit 2024, S. 14).

Datenschutz

Wie bereits einleitend beschrieben, werden durch Polizeibehörden sensible, oft personenbezogene Daten verarbeitet. Auch in diesem Themenfeld stehen Polizeibehörden vor der Herausforderung, zunächst den von dem KI-System zu verarbeitenden Datenumfang zu definieren, insbesondere im Hinblick auf den Personenbezug der Daten (Fricke 2020, S. 8). Gegebenenfalls ist es erforderlich, den/die jeweils zuständige/n Landes- bzw. Bundesdatenschutzbeauftragte/n bereits in der Planungsphase einzubinden (vgl. § 69 (1) BDSG für Bundesbehörden) und die Notwendigkeit des Verfassens einer Datenschutzfolgenabschätzung zu prüfen (Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit 2022, S. 19).

Mögliche Problemstellungen ergeben sich darüber hinaus aus dem Grundsatz der Zweckbindung von Daten, die in der Regel nicht unmittelbar für die Nutzung durch ein KI-System als Teil einer umfangreichen Datenmenge („Big Data“) erhoben wurden (Fricke 2020, S. 9). Auch der Grundsatz der Datenminimierung muss mit den Anforderungen von KI-Systemen, auf einen möglichst großen Datenbestand zugreifen zu können, vereinbart werden (Bitkom e.V. 2023, S. 10).

Organisatorische Rahmenbedingungen

Die Einführung von Systemen der Künstlichen Intelligenz geht mit einer Vielzahl von organisatorischen und die Verwaltung betreffenden Herausforderungen einher (PwC – strategy& 2023, S. 5). So stehen Veränderungen in Arbeitsabläufen und die Einführung von neuen Technologien oftmals Bedenken der Beschäftigten gegenüber (dbb beamtenbund und tarifunion 2020). Damit verbunden ist die Notwendigkeit, umfangreiche Schulungsmaßnahmen sowohl für die Entwicklungs- als auch für die Anwendungsbereiche einzuplanen (Dechesne et al. 2019, S. 10).

Im Bereich der Beschaffung bzw. Entwicklung und Implementierung stehen Polizeibehörden vor Fragestellungen, ob entsprechende Systeme eigenentwickelt oder kommerziell (Bitkom e.V. 2023, S. 15) beschafft werden und mit welchem finanziellen und personellen

Aufwand (Fricke 2020, S. 10) dies verbunden ist. Weitere Themen können die Nachhaltigkeit und die organisatorische und energetische Effizienz von KI-Systemen betreffen (Bundesministerium des Innern und für Heimat 2024, S. 19).

Transparenz und Verantwortlichkeit

Maßnahmen der Polizei werden regelmäßig gerichtlich überprüft, darüber hinaus sind der Ursprung der durch die Polizei ermittelten Erkenntnisse und Beweismittel sowie die Art und Weise der Erhebung oftmals Gegenstand einer richterlichen Würdigung. Die Notwendigkeit dieser Nachvollziehbarkeit bzw. Reproduzierbarkeit muss mit der oftmals enorm ausgeprägten Komplexität von KI-Systemen („Blackbox“) (Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit 2022, S. 11) und der Beteiligung von ggf. einer Vielzahl von Akteuren von der Entwicklung bis zur Anwendung („Many Hands Problem“) (European Crime Prevention Network 2022) in Einklang gebracht werden. Für den Themenbereich der Verantwortung ist festzuhalten, dass KI-Systeme keine eigene Rechtspersönlichkeit innehaben und damit schlussendlich die Frage nach der Verantwortlichkeit bzw. der Haftung vor der Anwendung beantwortet sein muss (Dechesne et al. 2019, S. 9).

Gesellschaftliche Rahmenbedingungen

Polizeibehörden und ihre Maßnahmen stehen unter ständiger Beobachtung durch die Öffentlichkeit und der Medien (Dechesne et al. 2019, S. 10). Es ist davon auszugehen, dass die in diesem Kapitel genannten Herausforderungen im Allgemeinen bekannt sind und der Umgang mit ihnen durch die Polizei von der interessierten Öffentlichkeit verfolgt wird. Diesem Umstand muss die Polizei als Organisation bei der Einführung und Anwendung von KI-Systemen berücksichtigen, um dem Anspruch der Öffentlichkeit an einen verantwortungsvollen Umgang mit dem Potenzial von Künstlicher Intelligenz gerecht zu werden (Bundesamt für Sicherheit in der Informationstechnik et al. 2024, S. 16).

Material und Methodik

In diesem Kapitel werden die methodischen Ansätze erläutert, die der Beantwortung der Forschungsfrage zugrunde liegen. Die Untersuchung beruht zum einen auf einer umfassenden Literaturrecherche sowie zum anderen auf der Durchführung von zwei Experteninterviews. Diese Kombination aus theoretischer Fundierung und empirischer Datenerhebung soll eine differenzierte Betrachtung des Forschungsgegenstands sowie einen Vergleich der aus den beiden Methoden jeweils gewonnenen Erkenntnisse ermöglichen.

Literaturrecherche

Die Grundlage dieser Arbeit bildet eine umfangreiche Literaturrecherche. Um ein möglichst breites Spektrum relevanter Quellen zu erfassen, wurden verschiedene Datenbanken und Suchplattformen genutzt. Die Recherche umfasste allgemeine Suchmaschinen für einen ersten Überblick, Google Scholar für wissenschaftliche Publikationen sowie universitäre Datenbanken insbesondere für Fachzeitschriften. Bei der Suche wurden Schlüsselbegriffe wie „Künstliche Intelligenz“ unter anderem in Verbindung mit „Polizei“, „Herausforderungen“, „Implementierung“ und „Voraussetzungen“ verwendet, sowohl einzeln als auch in Kombination. Die Auswahl der Quellen erfolgte zum einen im Hinblick auf die Relevanz für die Forschungsfrage, zum anderen und insbesondere in Bezug auf die Aktualität der Quelle (vorwiegend Publikationen der letzten maximal 3 bis 5 Jahre). Das letztgenannte Kriterium ist speziell im Themenfeld der Künstlichen Intelligenz als besonders wichtig hervorzuheben, da sich die Rahmenbedingungen in allen im Zusammenhang mit dieser Arbeit betrachteten Themenfeldern rasant entwickeln. Zusätzlich wurden die Literaturverzeichnisse besonders relevanter Publikationen im Hinblick auf zugrunde liegende Quellen durchsucht, um weitere Anknüpfungspunkte zu identifizieren. Diese mehrstufige Suchstrategie ermöglichte es, einen umfassenden Überblick über den aktuellen Forschungsstand zu gewinnen und eine solide theoretische Grundlage für die weitere Untersuchung zu schaffen. Im Anschluss an die Literaturrecherche wurden die Quellen im Hinblick auf dort beschriebene Herausforderungen bei der Einführung von

Systemen der Künstlichen Intelligenz untersucht und daraufhin Kategorien gebildet, denen die einzelnen diskutierten Aspekte zugeordnet werden konnten.

Experteninterviews

Das Experteninterview lässt sich primär in der qualitativen Forschung verorten (Bogner et al. 2014, S. 3). Das Forschungsinteresse der Erhebungsmethode liegt im fachlichen Wissen, in Handlungs- und Sichtweisen von ausgewählten Expertinnen und Experten (Bogner et al. 2014, S. 25). In ihrer Erhebung hat Schiek aufgezeigt, dass „Leitfadeninterviews schriftlich ohne die gleichzeitige Anwesenheit der Beteiligten methodologisch sinnvoll durchgeführt werden können“ (Schiek 2022).

Vor diesem Hintergrund und auf dieser Basis erfolgte die schriftliche Befragung (E-Mail-Austausch) von zwei Experten für den vorliegende Beitrag. Die Auswahl der Experten erfolgte aufgrund ihrer Vortragstätigkeiten im Rahmen der diesem Beitrag zugrunde liegenden Seminarveranstaltung „Wahlpflichtmodul 1“ und des für das Thema des Beitrags vorhandenen fundierten Expertise im Bereich der Künstlichen Intelligenz in Polizeiorganisationen. Um die Darstellung von unterschiedlichen Sichtweisen zu ermöglichen, erfolgte die Befragung von je einem im Bereich der Künstlichen Intelligenz tätigen Beamten des Polizeivollzugsdienstes und eines polizeilichen Beschäftigten mit wissenschaftlichem Hintergrund.

Für die Befragung wurden fünf Fragestellungen formuliert, die im Hinblick auf die Literaturrecherche eine methodische Überprüfung und ggf. Ergänzung der dort gewonnenen Erkenntnisse ermöglichen. Um einen möglichst großen inhaltlichen Raum für die Beantwortung herzustellen, wurde neben Themenfeldern, die für die Polizeiorganisationen als Herausforderung wahrgenommen werden, auch nach betroffenen Akteuren gefragt, aus denen sich ggf. Rückschlüsse auf weitere Themenfelder bilden lassen. Darüber hinaus wurde in einem perspektivischen Schritt nach bereits bestehenden Konzeptionen, die die identifizierten herausfordernden Themenfel-

der ggf. bereits adressieren, und ihrer Notwendigkeit bei Nicht-Vorliegen gefragt, um hieraus Ableitungen für weiterführende wissenschaftliche Betrachtungen zu ermöglichen.

Datenanalyse

Die erhobenen Daten wurden in einem nächsten Schritt einer strukturierenden Inhaltsanalyse mittels deduktiver Kategorienanwendung nach Mayring zugeführt. Zunächst wurden die wesentlichen Informationen aus der Literatur systematisch ausgewertet und im Anschluss die für die Beantwortung der Forschungsfrage relevanten Themen identifiziert und kategorisiert. Darauf aufbauend wurde ein Kodierleitfaden erstellt, um die Antworten der befragten Experten systematisch den Kategorien zuordnen zu können (vgl. Mayring und Fenzl 2019, S. 638-641). Der Kodierleitfaden sowie die Ergebnisse dieser Datenanalyse wurden in den Ergebnisteil integriert, wo sie sowohl die Erkenntnisse aus der Literatur als auch die Ansichten der Experten zusammenführen.

Ergebnisse

Im Rahmen der Auswertung der Experteninterviews konnten die zuvor mittels der Literaturrecherche gebildeten Themenkategorien bestätigt werden. Im Ergebnis werden diejenigen Themenfelder der Herausforderungen, die von der Literatur diskutiert werden, auch von den beiden befragten Experten geteilt und sind somit grundsätzlich auch auf (mindestens die beiden vertretenen) Polizeibehörden übertragbar. Im Folgenden werden die durch die Experten vordringlich vorgebrachten Aspekte in den jeweiligen Themenkategorien zusammengefasst.

Aus den Experteninterviews ist ein besonderer Fokus auf die (datenschutz-)rechtlichen Rahmenbedingungen erkennbar. Die Notwendigkeit einer klaren gesetzlichen Grundlage für den Einsatz von Künstlicher Intelligenz in der Polizeiarbeit wird durchgängig betont. Eine ggf. vorhandene rechtliche Unsicherheit hingegen erschwere eine normgerechte Einführung entsprechender Systeme. Dies be-

treffe zum Beispiel die erst vor Kurzem eingeführten EU-KI-Verordnung, die eine detaillierte Auslegung und die Bildung von konkreten Schlussfolgerungen für die Implementierung und Nutzung von Systemen der Künstlichen Intelligenz unabdingbar mache. Darüber hinaus könne die Verarbeitung von Daten bei unklarer Rechtslage zu einem Vertrauensverlust führen. Des Weiteren wurde die Notwendigkeit einer klaren Definitionslage technischer bzw. rechtlicher Begriffe für eine praxisingerechte Umsetzung herausgestellt.

Organisatorische Aspekte nehmen bei den Rückläufen der Experten einen zentralen Punkt ein, der konkrete praktische Implikationen hervorbringt. Vorrangig genannt wird der umfangreiche Schulungsbedarf insbesondere für die Anwenderinnen und Anwender von Systemen der Künstlichen Intelligenz. Dieser umfasse nicht nur die notwendigen technischen Fähigkeiten, sondern auch ein Verständnis der ethischen und rechtlichen Rahmenbedingungen. Dieser Schulungsbedarf könne leicht unterschätzt werden. Die Berücksichtigung von Change-Management-Prozessen und hierbei insbesondere eine „gründliche Projektion der möglichen Auswirkungen auf Arbeitsabläufe und Mitarbeiter“ wird in diesem Zusammenhang ebenfalls genannt.

Unter den Punkt „organisatorische Rahmenbedingungen“ lassen sich auch die Rückmeldungen im Hinblick auf ökonomische bzw. die Ressourcen betreffende Fragestellungen subsumieren. Die Einführung und die Entwicklung von Systemen der Künstlichen Intelligenz binde erhebliche Ressourcen in Personal, Technologie, Budget und Infrastruktur. Von beiden Experten wurde daher in diesem Zusammenhang die Notwendigkeit einer strategischen Planung sowie Budgetierung konstatiert. In einem der beiden Experteninterviews wird darüber hinaus die Notwendigkeit von Evaluierungs- und Monitoringprozessen hinsichtlich der Ergebnisqualität und Funktionsweise der KI-Systeme durchweg benannt. Diese seien notwendig, „um die Effektivität zu messen und etwaig notwendige Anpassungen (z. B. Nachtrainieren) zu erkennen“.

Im Hinblick auf die technologischen Rahmenbedingungen kann als vordringliche Herausforderung die Integration von Systemen der Künstlichen Intelligenz in bestehende (System-)Strukturen festgestellt werden. Dies sei insbesondere im Hinblick auf die aktuell nicht einheitliche IT-Landschaft innerhalb der Polizei herausfordernd. Eine länderübergreifende Integration eines Produktes sei vor diesem Hintergrund und aufgrund unterschiedlicher Prozesse aktuell nicht möglich. Dies könne eine langfristige Harmonisierung für eine effiziente Nutzung entsprechender Systeme notwendig machen, die jedoch ihrerseits umfangreiche Aufwände bedeuten würde. Weitere von beiden Experten genannte Punkte sind die notwendige Robustheit entsprechender Systeme sowie die Berücksichtigung von beispielsweise BSI- und ISO-Standards.

In einer der beiden Rückmeldungen wurde die Notwendigkeit herausgestellt, der in der Öffentlichkeit teilweise bestehenden Unklarheit hinsichtlich der rechtlichen Möglichkeiten und des tatsächlichen Einsatzes von Systemen der Künstlichen Intelligenz in Polizeibehörden mit hoher Transparenz und der Möglichkeit der Nachvollziehbarkeit zu begegnen. Es sei notwendig, dass stets ein menschlicher Entscheider in entsprechenden Prozessen involviert sei. In diesen Kontext fallen auch die vorauszusetzende Genauigkeit und Zuverlässigkeit von KI-Systemen.

Auch die ethischen Rahmenbedingungen werden von beiden Experten als wichtige Rahmenbedingung bestätigt. In einem Rücklauf wird konstatiert, dass die Thematik auch „einen erheblichen Einfluss auf die Akzeptanzbewertung externer Akteure wie Bürger, Medien und in der Konsequenz auch auf die Politik“ haben könne. In diesem Zusammenhang wurde erwähnt, dass hierzu allerdings noch keine konkreten Erfahrungen vorliegen. Ein Experteninterview verknüpft die Frage nach den ethischen Rahmenbedingungen explizit mit der notwendigen Verhinderung von Diskriminierung und Missbrauch entsprechender Systeme.

Die in der Literatur weithin besprochenen gesellschaftlichen Rahmenbedingungen finden sich auch in den Rückmeldungen der Experteninterviews wieder. Insbesondere das Vertrauen der Ge-

sellschaft in den rechtskonformen Einsatz von Systemen der Künstlichen Intelligenz gelte es zu stärken. Von beiden Seiten wurde die Berücksichtigung der politischen Entscheidungsträger im Prozess der Einführung von Systemen der Künstlichen Intelligenz als wichtiges Kriterium hervorgehoben.

Abschließend wurde von beiden Experten betont, dass eine ganzheitliche Betrachtung der Herausforderungen von Polizeibehörden bei der Einführung von Systemen der Künstlichen Intelligenz mit dem Ziel, ein die Behörden unterstützendes Werkzeug (z. B. Leitfaden) zu erstellen, hilfreich sei. Ein solches Dokument müsse sich jedoch an bestehenden Prozessen und Leitlinien orientieren und ergänzend die spezifischen Charakteristika von Systemen der Künstlichen Intelligenz aufnehmen.

Diskussion

Die Ergebnisse der vorliegenden Untersuchung zeigen, dass die Herausforderungen bei der Einführung von KI-Systemen in Polizeibehörden komplex und vielschichtig sind. Es lässt sich ableiten, dass die von der Literatur im Allgemeinen behandelten Themenbereiche auch innerhalb der Polizeibehörden identifiziert wurden und umfassend behandelt werden. Insbesondere die Befassung mit den (datenschutz-)rechtlichen Rahmenbedingungen ist vor dem Hintergrund der verfassungsrechtlichen Stellung von Polizeibehörden, der dort vorliegenden und verarbeiteten Daten sowie der Möglichkeit von Grundrechtseingriffen nachvollziehbar.

Aus der Betrachtung ist abzulesen, dass das Thema Künstliche Intelligenz im Allgemeinen und insbesondere in Polizeibehörden derzeit noch einer erheblichen Veränderungsdynamik unterworfen ist. Dies gilt beispielsweise für den Bereich der rechtlichen Rahmenbedingungen und hier vorrangig mit Blick auf das Inkrafttreten der EU-KI-Verordnung und deren Umsetzung, wobei die damit verbundene Abschätzung der Auswirkungen auf den Einsatz von Systemen der Künstlichen Intelligenz in Polizeibehörden derzeit noch andauert. Diese u. U. vorhandene rechtliche Unsicherheit gilt im Übrigen

auch grundsätzlich zum Beispiel für die Einordnung von anzuwendenden Systemen in den rechtlichen Rahmen. Hier erscheint insgesamt eine konsolidierte Auslegung der rechtlichen Rahmenbedingungen notwendig.

Darüber hinaus ist erkennbar, dass Polizeibehörden als Organisationen bei der Einführung von Systemen der Künstlichen Intelligenz umfassende Herausforderungen im verwaltungstechnischen Sinne vor sich haben, beispielsweise mit Blick auf eine Priorisierung entsprechender Vorhaben durch die Bereitstellung von Budget, Personal, dem Umgang mit Schulungsaufwänden und der Schaffung von Akzeptanz entsprechender Systeme von den Mitarbeiterinnen und Mitarbeitern. Die Abhängigkeit von Polizeibehörden von politischen, folglich gesetzgebenden Entscheidungen in diesem Bereich wurde sowohl durch die Literaturrecherche als auch durch die Auswertung der Experteninterviews deutlich.

Ziel der Arbeit war es, einen Überblick über die Schlüsselthemen bei der Einführung von Systemen der Künstlichen Intelligenz zu erhalten, diese kategorisiert darzustellen und mit der Expertise von Experten aus der Polizeiorganisation abzugleichen. Die durch die Literaturrecherche identifizierten Kategorien konnten mit den Ergebnissen der Experteninterviews inhaltlich angereichert werden. Auf dieser Basis ist mit diesem Beitrag ein erster Blick auf die derzeit vorrangig vorhandenen Herausforderungen konkret von Polizeibehörden im Bereich der Künstlichen Intelligenz ermöglicht worden.

Einschränkend ist festzustellen, dass der Detailgrad einer überblicksartigen Betrachtung im Rahmen eines solchen Beitrags limitiert ist und die Reichweite der Untersuchung, die sich auf zwei Experteninterviews stützt, begrenzt ist und daher keine umfassende Generalisierung zulässt. Für eine tiefergehende Auseinandersetzung mit den Herausforderungen und insbesondere der Betrachtung von Folgefragen, z. B. im Hinblick auf die Ausarbeitung von Handlungsempfehlungen oder die Erarbeitung einer Orientierungshilfe im Charakter einer Leitlinie, ist die Bearbeitung in einem anderen wissenschaftlichen Rahmen erforderlich. Dieser könnte auch eine umfangreichere Erhebung bei und mit Polizeibehörden umfassen.

Schlussfolgerungen

Der vorliegende Beitrag ermöglicht einen überblicksartigen und zusammenfassenden Einstieg konkret in die Herausforderungen von Polizeibehörden bei der Einführung von Systemen der Künstlichen Intelligenz. Im Ergebnis hat dieser gezeigt, dass die Einführung von Systemen der Künstlichen Intelligenz in Polizeiorganisationen ein komplexes Unterfangen ist, das eine Vielzahl von Herausforderungen mit sich bringt. Die identifizierten Themenkategorien – von rechtlichen und ethischen Rahmenbedingungen über technologische und organisatorische Aspekte bis hin zu Fragen der Transparenz und gesellschaftlichen Auswirkungen – verdeutlichen die Notwendigkeit eines ganzheitlichen Ansatzes bei der Implementierung von KI in der Polizeiarbeit. Besonders hervorzuheben ist die Bedeutung einer klaren rechtlichen Grundlage, insbesondere im Hinblick auf die neue EU-KI-Verordnung, sowie die Notwendigkeit umfassender Schulungs- und Qualifizierungsmaßnahmen.

Für Polizeiorganisationen ergibt sich daraus die Empfehlung, bei der Einführung von KI-Systemen einen ganzheitlichen Ansatz zu verfolgen, der alle relevanten Akteure einbezieht und die identifizierten Herausforderungen systematisch adressiert. Die Entwicklung eines umfassenden Leitfadens, der sowohl theoretische Grundlagen als auch praktische Erfahrungen berücksichtigt, könnte ein wertvolles Instrument für Polizeiorganisationen darstellen. Zukünftige Forschung sollte sich auf die Entwicklung konkreter Implementierungsstrategien und die Evaluation bereits eingeführter KI-Systeme in der Polizeiarbeit konzentrieren, um Best Practices zu identifizieren und weiterzuentwickeln. In einer weiterführenden Arbeit könnte auf dieser Basis eine tiefere Analyse der Themenbereiche erfolgen. Darauf aufbauend wäre es möglich, die Grundlage für konkrete Handlungsempfehlungen zu schaffen bzw. eine Handlungshilfe für die Einführung entsprechender Systeme in Polizeibehörden zu erstellen. In diesem Rahmen könnten auch die Zusammenhänge mit den diesbezüglichen Bemühungen des Programms 2020 berücksichtigt werden.

Literaturverzeichnis

Bitkom e.V. (2023): KI in der Polizei – Einsatzpotentiale und Lösungsansätze zur Implementierung. Online verfügbar unter [bitkom.org/sites/main/files/2023-10/bitkom-positions-papier-ki-polizei-einsatz-implementierung.pdf](https://www.bitkom.org/sites/main/files/2023-10/bitkom-positions-papier-ki-polizei-einsatz-implementierung.pdf), zuletzt geprüft am 22.12.2024.

Bogner, Alexander; Littig, Beate; Menz, Wolfgang (2014): Interviews mit Experten. Eine praxisorientierte Einführung. Wiesbaden: Springer Fachmedien Wiesbaden (Springer eBook Collection). Online verfügbar unter link.springer.com/book/10.1007/978-3-531-19416-5, zuletzt geprüft am 22.12.2024.

Brauns, Michael (2022): Vertrauenswürdige KI für die polizeiliche Textauswertung. Hg. v. Universität der Bundeswehr München. Online verfügbar unter [idw-online.de/de/news791001](https://www.idw-online.de/de/news791001).

Bundesamt für Sicherheit in der Informationstechnik; Müller, Oliver; Lazar, Veronika (2024): Transparenz von KI-Systemen. Whitepaper. Bonn. Online verfügbar unter [bsi.bund.de/SharedDocs/Downloads/DE/BSI/KI/Whitepaper-Transparenz-KI-Systeme.pdf?__blob=publicationFile&v=3](https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/KI/Whitepaper-Transparenz-KI-Systeme.pdf?__blob=publicationFile&v=3), zuletzt geprüft am 22.12.2024.

Bundesministerium des Innern und für Heimat (2024): KI-Leitbild für das Ressort BMI. Berlin. Online verfügbar unter [bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/it-digitalpolitik/BMI24014.pdf?__blob=publicationFile&v=3](https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/it-digitalpolitik/BMI24014.pdf?__blob=publicationFile&v=3), zuletzt geprüft am 22.12.2024.

dbb beamtenbund und tarifunion (2020): Expertenrat künstliche Intelligenz: Auswirkungen auf den öffentlichen Dienst. Schleswig-Holstein. Online verfügbar unter [dbb.de/artikel/expertenrat-kuenstliche-intelligenz-auswirkungen-auf-den-oeffentlichen-dienst.html](https://www.dbb.de/artikel/expertenrat-kuenstliche-intelligenz-auswirkungen-auf-den-oeffentlichen-dienst.html), zuletzt geprüft am 22.12.2024.

Dechesne, Francien; Dignum, Virginia; Zardiashvili, Lexo; Bieger, Jordi (2019): AI & Ethics at the Police. Towards Responsible Use of Artificial Intelligence in the Dutch Police. Leiden/Delft. Online

verfügbar unter universiteit.leiden.nl/binaries/content/assets/rechtsgeleerdheid/instituut-voor-metajuridica/artificiele-intelligentie-en-ethiek-bij-de-politie/ai-and-ethics-at-the-police-towards-responsible-use-of-artificial-intelligence-at-the-dutch-police-2019.pdf, zuletzt geprüft am 22.12.2024.

Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (2022): Bericht über das öffentliche Konsultationsverfahren des BfDI. Einsatz von Künstlicher Intelligenz im Bereich der Strafverfolgung und der Gefahrenabwehr. Online verfügbar unter bfdi.bund.de/SharedDocs/Downloads/DE/Konsultationsverfahren/2_KI-Strafverfolgung/Konsultationsbericht.pdf?__blob=publicationFile&v=5, zuletzt geprüft am 22.12.2024.

Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (2024): Datenschutzrechtliche Grundlagen beim Einsatz von Künstlicher Intelligenz (KI) im Bereich der Sicherheitsbehörde des Bundes. Handreichung des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit. Online verfügbar unter bfdi.bund.de/SharedDocs/Downloads/DE/DokumenteBfDI/Dokumente-allg/2024/Handreichung-BfDI-KI-Sicherheitsbeh%C3%B6rden.pdf?__blob=publicationFile&v=3, zuletzt geprüft am 22.12.2024.

Deutscher Ethikrat (2023): Mensch und Maschine – Herausforderungen durch Künstliche Intelligenz. Stellungnahme. Online verfügbar unter ethikrat.org/fileadmin/Publikationen/Stellungnahmen/deutsch/stellungnahme-mensch-und-maschine.pdf, zuletzt geprüft am 22.12.2024.

Die Bundesregierung (2024): Einheitliche Regeln für Künstliche Intelligenz in der EU. Online verfügbar unter breg.de/aktuelles/ai-act-2285944#:~:text=AI%20Act%20verabschiedet%20Einheitliche%20Regeln,nun%20in%20nationales%20Recht%20umsetzen, zuletzt geprüft am 22.12.2024.

European Crime Prevention Network (2022): Artificial intelligence and predictive policing: risks and challenges. Recommendation Paper. Brüssel. Online verfügbar unter eucpn.org/sites/default/files/document/files/PP%20%282%29.pdf, zuletzt geprüft am 22.12.2024.

Europol Innovation Lab (2024): AI and policing. The benefits and challenges of artificial intelligence for law enforcement. Luxemburg. Online verfügbar unter europol.europa.eu/cms/sites/default/files/documents/AI-and-policing.pdf, zuletzt geprüft am 22.12.2024.

Fricke, Julia (2020): Big Data und künstliche Intelligenz – Chancen und Risiken für die Polizeiarbeit der Zukunft. KSV Polizeipraxis – Der Blog der Polizei Info Report 2020. Online verfügbar unter ksv-polizeipraxis.mwssupport.de/wp-content/uploads/2020/05/Fricke-Big-Data.pdf, zuletzt geprüft am 22.12.2024.

IBM; Holdsworth, James (2023): Was ist KI-Bias? Online verfügbar unter ibm.com/de-de/topics/ai-bias, zuletzt geprüft am 22.12.2024.

Mayring, Philipp; Fenzl, Thomas (2019): Qualitative Inhaltsanalyse. In: Nina Baur und Jörg Blasius (Hg.): Handbuch Methoden der empirischen Sozialforschung. Wiesbaden: Springer Fachmedien Wiesbaden, S. 633-648.

Multishoring (2024): The 7 Most Common Integration Issues – Why Do System Integration Failures Happen? Online verfügbar unter multishoring.com/blog/the-7-most-common-integration-issues-aka-why-system-integration-projects-fail/, zuletzt geprüft am 22.12.2024.

PwC – strategy& (2023): KI in deutschen Sicherheitsbehörden – Zwischen Ambition und Wirklichkeit. Ergebnisse einer Umfrage unter Experten deutscher Sicherheitsbehörden. Online verfügbar unter strategyand.pwc.com/de/de/branchen/oeffentlicher-sektor/ki-in-deutschen-sicherheitsbehoerden.html, zuletzt geprüft am 22.12.2024.

Schiek, Daniela (2022): Schriftliche Online-Interviews in der qualitativen Sozialforschung. Zur methodologischen Begründung einer neuen Forschungspraxis. Hg. v. Forum Qualitative Sozialforschung. Online verfügbar unter qualitative-research.net/index.php/fqs/article/download/3754/4803/16989, zuletzt geprüft am 22.12.2024.

Schwarzbeck, Martin (2024): Vom Iris-Scan bis zum automatischen Aufstandsmelder. Polizei und KI. Hg. v. netzpolitik.org e.V. Berlin. Online verfügbar unter netzpolitik.org/2024/polizei-und-ki-vom-iris-scan-bis-zum-automatischen-aufstandsmelder/#netzpolitik-pw, zuletzt geprüft am 22.12.2024.

tagesschau.de (2024): Mit Gesichtserkennung Terroristen aufspüren. Mehr Befugnisse für Polizei. Online verfügbar unter [tagesschau.de/inland/gesichtserkennungs-software-100.html](https://www.tagesschau.de/inland/gesichtserkennungs-software-100.html), zuletzt geprüft am 22.12.2024.

KI-Kompetenzen für Polizeibeamtinnen und -beamte: Die Zukunft der Polizeiausbildung in Baden-Württemberg

Christian Just

Die rasante Entwicklung Künstlicher Intelligenz (KI) hat in den letzten Jahren nahezu alle Lebensbereiche und Branchen tiefgreifend verändert. Unternehmen und öffentliche Institutionen stehen zunehmend vor der Herausforderung, KI-basierte Technologien in ihre Arbeitsprozesse zu integrieren, um effizienter und zukunftsfähiger zu werden (Bundesministerium für Bildung und Forschung 2023). Auch in sicherheitsrelevanten Bereichen wie der Kriminalitätsbekämpfung und der öffentlichen Sicherheit eröffnet KI neue Möglichkeiten, sei es durch automatisierte Datenanalyse, Mustererkennung oder vorausschauende Polizeistrategien (Polizeiliche Kriminalprävention 2023). Während sich viele Unternehmen und Behörden bereits intensiv mit der Implementierung solcher Technologien befassen, stehen die Polizeien des Bundes und der Länder vor besonderen ethischen und rechtlichen Herausforderungen, die einen verantwortungsvollen Umgang mit KI erfordern (Deutscher Ethikrat 2023, S. 301).

Für die Polizei in Baden-Württemberg bedeutet dies, sich den wachsenden Herausforderungen einer zunehmend digitalisierten Kriminalitätslandschaft zu stellen. Damit Polizeibeamtinnen und -beamte diese Technologien in Zukunft effektiv und zu gleich verantwortungsbewusst anwenden können, wird es immer wichtiger, entsprechende Kompetenzen frühzeitig zu vermitteln. Dies wirft die Frage auf, ob die bisherige Polizeiausbildung ausreichend darauf vorbereitet ist und ob zusätzliche KI-Kompetenzen notwendig sind, um den technologischen Anforderungen gerecht zu werden.

Im Rahmen dieses Beitrags soll untersucht werden, ob Polizeistudierende in Baden-Württemberg verstärkt und in tieferem Maße Kompetenzen im Bereich KI benötigen, um den wachsenden technologischen Anforderungen im Polizeialltag gerecht werden zu können. Angesichts der zunehmenden Bedeutung von KI in der Kriminalitätsprävention, Ermittlungsarbeit und Analyse großer Datenmengen

stellt sich die Frage, ob die derzeitige Ausbildung den zukünftigen beruflichen Anforderungen gerecht wird. Besonders relevant ist dabei, welche konkreten Fähigkeiten und Kenntnisse im Umgang mit KI-Technologien vermittelt werden sollten. Die Forschungsfrage zielt darauf ab, mögliche Lücken im aktuellen Curriculum zu identifizieren und mittels Experteninterviews zu klären, inwiefern eine Erweiterung des Ausbildungsangebots notwendig ist.

Hintergrund

Das folgende Kapitel vermittelt die grundlegenden Informationen zur Polizei Baden-Württemberg, zur Hochschule für Polizei sowie zum dreigeteilten Studium. Zudem werden die Begriffe der KI wie auch der im Rahmen dieses Beitrags relevanten KI-Kompetenzen definiert. Darüber hinaus werden aktuelle und potenzielle zukünftige Einsatzfelder der KI innerhalb der polizeilichen Arbeit untersucht, für deren Bewältigung die Polizeibeamtinnen und -beamten im Rahmen ihrer Ausbildung qualifiziert werden müssen.

Die Polizei Baden-Württemberg

Gem. § 115 PolG gliedert sich die Polizei Baden-Württemberg in 13 regionale Polizeipräsidien, das Polizeipräsidium Einsatz sowie das Landeskriminalamt. Für den Polizeivollzugsdienst unterhält das Land zudem das Präsidium Technik, Logistik, Service der Polizei sowie die Hochschule für Polizei Baden-Württemberg (HfPol BW). Die HfPol BW mit Hauptsitz in Villingen-Schwenningen ist dabei die zentrale Bildungseinrichtung für die Aus- und Fortbildung von Polizeikräften des Landes (Polizei Baden-Württemberg 2024). Neben der theoretischen Ausbildung legt die Hochschule großen Wert auf praxisorientierte Inhalte, die für die Bewältigung dieser Herausforderungen im polizeilichen Alltag erforderlich sind (Hochschule für Polizei Baden-Württemberg 2024b, S. 55).

Studium zum gehobenen Polizeivollzugsdienst

Das Studium für den gehobenen Polizeivollzugsdienst gliedert sich in drei thematische Schwerpunkte, zwischen denen die Studierenden zu verschiedenen Zeitpunkten eine Wahl treffen müssen. Neben den etablierten Schwerpunktbereichen „Schutz-“ und „Kriminalpolizei“ wurde in den letzten Jahren der Bereich „Kriminalpolizei IT-Ermittlungen/IT-Auswertungen (K-IT)“ eingeführt. Dieser Schwerpunkt vermittelt in einem Umfang von etwa sieben bis acht Wochenstunden grundlegende technische Kenntnisse im Bereich digitaler Spuren sowie deren Analyse und Auswertung. Für jeden neuen Studienjahrgang und Schwerpunkt erstellt die HfPol BW ein Modulhandbuch, das zugleich als Curriculum dient und die wesentlichen Studienziele sowie -inhalte darlegt (Hochschule für Polizei Baden-Württemberg 2024a).

Grundlagen und Definitionen

Um das Thema KI-Kompetenzen in der Polizeiausbildung einheitlich und fundiert zu betrachten, ist ein gemeinsames Verständnis zentraler Begriffe unerlässlich. Die folgenden Definitionen schaffen eine klare Grundlage und tragen dazu bei, Missverständnisse zu vermeiden. Sie bilden somit die Basis für die weitere inhaltliche Auseinandersetzung in diesem Beitrag.

Grundlagen Künstliche Intelligenz

KI beschreibt Technologien, die darauf abzielen, menschenähnliche Intelligenzleistungen nachzuahmen oder zu unterstützen. Dazu zählen Fähigkeiten wie das Erkennen von Mustern, das Verstehen und Verarbeiten von Sprache, das Lösen von komplexen Problemen oder das Treffen datenbasierter Entscheidungen (Bendel 2024, S. 138 f.). Grundlegend unterscheidet man zwischen regelbasierten KI-Systemen, die nach festgelegten Algorithmen arbeiten, und solchen, die auf maschinellem Lernen beruhen. Systeme des maschinellen Lernens können ihre Leistung durch die Analyse großer Datenmengen eigenständig verbessern, ohne dass sie explizit programmiert werden müssen (Bundesnetzagentur 2021, S. 7).

KI gilt heute als eine Schlüsseltechnologie, die in zahlreichen Lebensbereichen Anwendung findet, von der Medizin über die Wirtschaft bis hin zur öffentlichen Sicherheit. Im Kontext der Polizeiarbeit bietet sie vielfältige Möglichkeiten, etwa bei der Analyse großer Datenmengen oder der Unterstützung bei Ermittlungen, was ihre Relevanz für diesen Bereich besonders unterstreicht (Bundesministerium für Bildung und Forschung 2023).

Begriffsdefinitionen

Es gibt keine einheitliche und abschließend festgelegte Definition von KI, da der Begriff je nach Kontext und wissenschaftlicher Perspektive unterschiedlich interpretiert wird. Um jedoch im Rahmen dieses Beitrags eine klare Grundlage zu schaffen, wird die Definition der Bundesregierung herangezogen:

„Künstliche Intelligenz beschreibt die Fähigkeit von Maschinen, basierend auf Algorithmen Aufgaben autonom auszuführen und dabei die Problemlösungs- und Entscheidungsfähigkeiten des menschlichen Verstandes nachzuahmen“ (Die Bundesregierung 2024).

Um den begrenzten Umfang des Beitrags einhalten zu können, wird an dieser Stelle bewusst auf eine tiefgreifende Herleitung und Diskussion verschiedener Definitionen verzichtet. Stattdessen liegt der Fokus darauf, eine praktikable und konsensfähige Grundlage für die weitere Analyse zu schaffen.

In der wissenschaftlichen Diskussion wird KI häufig auf Grundlage ihrer Funktionalität und ihres Aufbaus in schwache und starke KI kategorisiert, wobei Letztere gegenwärtig vor allem ein theoretisches Konzept darstellt und bislang nicht praktisch umgesetzt wurde (Rachner 2023).

Schwache KI bezeichnet dabei spezialisierte Systeme, die für die Lösung klar definierter Aufgaben konzipiert sind. Die Systeme basieren auf Algorithmen, die spezifisch für ihre jeweilige Aufgabe optimiert

sind und kein allgemeines Verständnis oder Bewusstsein besitzen. Beispiele hierfür sind Spracherkennung, Bildverarbeitung oder Schachprogramme (BSI 2022).

Starke KI hingegen zielt darauf ab, menschenähnliche kognitive Fähigkeiten zu entwickeln, die über spezifische Aufgaben hinausgehen. Sie soll ein allgemeines Verständnis und die Fähigkeit besitzen, Wissen auf neue Situationen anzuwenden, eigenständig zu lernen und zu denken (Schümann 2024, S. 18).

Die Definition von „KI-Kompetenzen“ ist nicht einheitlich und umfasst eine Vielzahl von Themenbereichen, darunter technische, analytische, ethische, gesellschaftliche und anwendungsbezogene Aspekte. Art. 3 Nr. 56 der KI-Verordnung definiert KI-Kompetenzen als die Fähigkeiten, Kenntnisse und das Verständnis, die es Anbietern, Betreibern und betroffenen Personen ermöglichen, KI-Systeme sachkundig einzusetzen. Dies schließt die bewusste Auseinandersetzung mit den Chancen, Risiken und möglichen Schäden ein, die durch KI entstehen können. Diese Definition hat jedoch einen stark technischen Fokus und richtet sich vor allem an Personen, die KI-Systeme entwickeln oder betreiben (Europäische Kommission 2021).

Im Kontext dieses Beitrags wird der Begriff „KI-Kompetenzen“ auf die spezifischen Anforderungen an Polizeibeamtinnen und -beamten eingegrenzt. Hierbei liegt der Schwerpunkt weniger auf tiefgreifenden technischen Kenntnissen als vielmehr auf anwendungsbezogenen Fähigkeiten. Dies erscheint praktikabler und zielführender, da die umfassende Vermittlung technischer Expertise für die breite Masse der Polizeikräfte weder umsetzbar noch erforderlich ist.

Eine alternative Definition, wie sie von StepStone publiziert wird, betont ebenfalls die praktische Dimension von KI-Kompetenzen:

„KI-Skills umfassen die Fähigkeiten und Kompetenzen, die erforderlich sind, um künstliche Intelligenz zu verstehen, zu nutzen und in Unternehmen zu integrieren.“ (Oberrauter-Zabransky 2024)

Diese Perspektive deckt sich mit dem Ansatz dieses Beitrags, der darauf abzielt, Polizeibeamtinnen und -beamten die effektive Nutzung von KI-Technologien im Arbeitsalltag zu ermöglichen.

Im vorliegenden Kontext werden KI-Kompetenzen daher als eine Kombination von Fähigkeiten, Kenntnissen und Verständnis definiert, die es Polizeibeamtinnen und -beamten ermöglichen, KI-Technologien sachkundig, effektiv und verantwortungsvoll einzusetzen. Aufbauend auf der Definition der KI-Verordnung, die den sachgerechten Umgang mit KI sowie die Berücksichtigung ihrer Chancen, Risiken und möglichen Schäden hervorhebt (Art. 3 Nr. 56 KI-Verordnung), und der praxisnahen Beschreibung von StepStone, die den Fokus auf die Nutzung und Integration von KI legt (Oberrauter-Zabransky 2024), umfassen KI-Kompetenzen hierbei insbesondere:

- das Verständnis für die Möglichkeiten und Grenzen von KI in der Polizeiarbeit,
- die Fähigkeit, KI-Technologien gezielt in bestehende Prozesse zu integrieren, um deren Effizienz und Nutzen zu steigern,
- die Kompetenz, geeignete KI-Modelle oder Anwendungen für spezifische Einsatzszenarien auszuwählen,
- die kritische Bewertung der mit KI verbundenen Risiken, insbesondere im Hinblick auf ethische und rechtliche Implikationen, und
- die Fähigkeit, Ergebnisse von KI-Systemen verantwortungsvoll zu interpretieren und in die Entscheidungsfindung einzubinden.

Die Synopse hebt hervor, dass KI-Kompetenzen weit über technische Expertise hinausgehen und zusätzlich anwendungsbezogene, analytische sowie ethische Fähigkeiten erfordern. Dadurch werden Polizeibeamtinnen und -beamte befähigt, den Mehrwert von KI-Technologien zu erkennen und deren Einsatz im polizeilichen Kontext nachhaltig, effizient und gesellschaftlich verantwortungsvoll zu gestalten.

Aktueller Forschungsstand

Eine umfassende Internetrecherche ergab keine spezifische Literatur, die sich explizit mit der Integration von KI-Kompetenzen in die Polizeiausbildung in Baden-Württemberg befasst. Auch die Kontaktaufnahme mit der Studienkommission der HfPol BW bestätigte, dass hierzu bislang keine gezielten Studien oder Veröffentlichungen vorliegen. Diese Ergebnisse legen nahe, dass das Thema bisher nicht ausreichend wissenschaftlich aufgearbeitet wurde und somit eine Forschungslücke besteht.

Methodisches Vorgehen

Zur systematischen Untersuchung der Forschungsfrage werden im Folgenden die methodischen Grundlagen der Sozialforschung herangezogen. Nach einer Einführung in die Grundlagen wird der Ansatz der qualitativen Sozialforschung skizziert mit Fokus auf das leitfadengestützte Interview als Erhebungsinstrument. Schließlich werden die Kriterien für die Auswahl der Experten erläutert.

Theoretische Grundlagen der Sozialforschung

Untersuchungen, die einen bestimmten Ausschnitt der sozialen Welt beobachten, werden klassisch als empirische Sozialforschungen bezeichnet. Sie dienen der Weiterentwicklung bestehender oder neuer Theorien, indem sie, angeleitet durch Theorien, die soziale Realität beobachten und daraus theoretische Erkenntnisse gewinnen (Gläser/Laudel 2010, S. 24). Die empirische Sozialforschung lässt sich folglich in zwei grundlegende Forschungsstrategien aufteilen, die den Aspekten der jeweiligen quantitativen und qualitativen Strategie unterschiedliche Gewichtung beimessen (Gläser/Laudel 2010, S. 26). Quantitative und qualitative Forschungsmethoden unterscheiden sich dabei in ihrem Ansatz zur Datenerhebung und -analyse. Quantitative Methoden basieren auf messbaren, numerischen Daten und zielen darauf ab, Phänomene durch Statistiken, Umfragen oder Experimente objektiv zu analysieren. Sie suchen nach Mustern und Korrelationen, die verallgemeinerbare Aussagen ermögli-

chen. Im Gegensatz dazu konzentrieren sich qualitative Methoden auf das Verstehen von subjektiven Erfahrungen, Meinungen oder Verhaltensweisen. Durch Interviews, Beobachtungen oder Textanalysen werden tiefere Einblicke in komplexe soziale oder kulturelle Zusammenhänge gewonnen (Flick 2014, S. 39 f.).

Qualitative Forschung

Die Frage „Wie beurteilen ein wissenschaftlicher und ein polizeilicher Mitarbeiter der HfPol BW die Relevanz von KI-Kompetenzen sowie deren Integration in die Polizeiausbildung, einschließlich der entsprechenden Ansätze und Methoden zur Vermittlung dieser Kompetenzen?“ formuliert dabei die diesem Beitrag zugrunde liegende Untersuchungsfrage und verdeutlicht das entsprechende Erkenntnisinteresse. Die Untersuchungsfrage erfüllt dabei eine doppelte Funktion: Zum einen dient sie zur Entwicklung der strategischen Überlegungen, die wiederum in das Konzept der empirischen Erhebung fließen (Gläser/Laudel 2010, S. 62 f.). Denn „Alles, was die Untersuchungsfrage beantworten hilft, muss erhoben werden, und nur, was die Untersuchungsfrage beantworten hilft, soll erhoben werden“ (Gläser/Laudel 2010, S. 63). Zum anderen richtet die Untersuchungsfrage den Blick des Untersuchenden auf zentrale Fragestellungen der Forschung. Der Fokus der Untersuchung liegt demnach weniger auf numerischen Daten als vielmehr auf den individuellen Einschätzungen, Meinungen und Einstellungen der Befragten.

Leitfadengestütztes Experteninterview

Für die Erhebung der notwendigen Daten wurden daher leitfadengestützte Experteninterviews durchgeführt. Diese stellen eine qualitative Forschungsmethode dar, bei der ein vorstrukturierter Leitfaden Verwendung findet. Durch diesen können gezielt Informationen von Experten zu einem spezifischen Bereich gesammelt werden. Der Leitfaden gibt dabei eine vorab definierte Struktur vor, welche jedoch auch Raum für flexible und tiefgehende Antworten ermöglicht. Die Formulierung präziser, jedoch auch möglichst offener Fragen ermöglicht dabei den Experten, ihre Expertise bestmöglich ausschöpfen und mitteilen zu können (Gläser/Laudel 2010, S. 115).

In der Literatur werden drei Typen von Interviews unterschieden: explorative Interviews zur Orientierung in einem neuen Untersuchungsfeld, systematisierende Interviews zur Gewinnung von Kontextinformationen sowie das theoriegenerierende Interview (Flick 2014, S. 216). Letzteres zielt darauf ab, durch gezielte Befragungen von Experten und auf Grundlage derer Antworten neue theoretische Konzepte zu entwickeln. Dies ist insbesondere in Gebieten hilfreich, in denen innovative Perspektiven förderlich sind, weswegen diese Methodik auch verwendet wurde (Bogner/Littig/Menz 2014, S. 25 f.).

Auswahl der Interviewpartner

Der Begriff der Expertin oder des Experten, der der Durchführung der in diesem Beitrag vorgenommenen Interviews zugrunde liegt, beschreibt eine Person, die über umfangreiche Fachkenntnisse und spezifische Erfahrungen in einem bestimmten Tätigkeits- oder Forschungsbereich verfügt. Dabei „handelt der Experte mit sicherem, eindeutigen Wissen, das ihm jederzeit kommunikativ und reflexiv verfügbar ist“ (Bogner/Littig/Menz 2005, S. 41). Die Befragten werden dabei nicht nur als Einzelfall, sondern vielmehr als Repräsentant einer Gruppe betrachtet (Flick 2014, S. 214). Zur Berücksichtigung wissenschaftlicher und polizeilicher Perspektiven wurde je ein Vertreter aus beiden Bereichen mit fundierter Lehrerfahrung ausgewählt.

Qualitative Inhaltsanalyse

Die qualitative Inhaltsanalyse nach Mayring ist eine systematische Methode zur Auswertung von Texten, die sowohl deduktive als auch induktive Kategorisierungsverfahren nutzen kann. Ziel ist es, relevante Inhalte aus dem Material herauszuarbeiten, indem diese inhaltlich strukturiert und anhand klar definierter Kategorien interpretiert werden. In diesem Beitrag wurden die Fragen des Interviews bereits vorab kategorisiert, um eine gezielte und strukturierte Auswertung der Expertenaussagen zu ermöglichen. Aufgrund des begrenzten Umfangs wurde jedoch von Mayrings festem Schema abgewichen und die Analyse flexibel auf die spezifische Forschungsfrage angepasst (Mayring/Fenzl 2019).

Ergebnisse

Nachfolgend werden die Ergebnisse der Experteninterviews dargestellt. Die Fragen sind dabei in insgesamt fünf Kategorien eingeteilt. Die Hauptaussagen der Experten werden im Folgenden zusammenfassend dargestellt.

Allgemeine Bedeutung

Wie bewerten Sie allgemein die Bedeutung von KI-Kompetenzen für Polizeibeamtinnen und -beamte in der heutigen Zeit?

Beide Experten messen der Bedeutung von KI-Kompetenzen einen hohen Stellenwert bei. Sie betrachten grundlegende Fähigkeiten und ein fundiertes Basiswissen im Bereich der KI als essenzielle Voraussetzungen, insbesondere für die spätere Fall- und Sachbearbeitung von Straftaten, bei denen KI zum Einsatz kommt. Experte 1 hebt hervor, dass in diesen Kompetenzen ein erhebliches Optimierungspotenzial für die polizeiliche Arbeit liegt. Experte 2 betont mit der Aussage: „Im Rahmen des Studiengangs K-IT wird in diesem Kontext die Vorlesung ‚Auswertungsunterstützung durch KI‘ angeboten, was die Bedeutung dieses Themas innerhalb der Polizeiausbildung unterstreicht“, dass die Polizei Baden-Württemberg die Relevanz der Thematik erkannt hat und diese durch die Integration der Vorlesung in den neu geschaffenen und verwendungsorientierten Studiengang K-IT gezielt stärkt.

Notwendigkeit von KI-Kompetenzen

Welche spezifischen Kompetenzen werden als besonders wichtig für Polizeibeamtinnen und -beamte erachtet?

Experte 2 betont die Bedeutung eines grundlegenden Verständnisses von KI-Technologien und deren Funktionsweisen. Besonders wichtig sei dabei die Vermittlung der Fähigkeit, KI-generierte Ergebnisse kritisch zu hinterfragen und zu bewerten. Experte 1 legt den Fokus auf die praktische Anwendung und hebt hervor, dass der Schwerpunkt auf der Bedienung von Auswertewerkzeugen liegt, die

teilweise mit KI ausgestattet sind. Dies verdeutlicht er mit der Aussage: „Sie fahren Autos und bauen sie nicht“. Damit spielt er auf die praxisorientierte Nutzung an, die kein tiefgehendes technisches Wissen voraussetzt. Beide Experten betonen somit unterschiedliche, sich ergänzende Aspekte der Nutzung von KI: einerseits das kritische Verständnis und andererseits die praktische Bedienung.

Integration von KI in die Polizeiausbildung

Welche Herausforderungen sehen Sie bei der Integration von KI-Kompetenzen in die Polizeiausbildung?

Die Experten identifizieren mehrere Herausforderungen bei der Integration von KI-Kompetenzen in die Polizeiausbildung. Ein zentraler Aspekt ist die schnelle Entwicklung der Technologie, die eine kontinuierliche Anpassung der Lerninhalte erfordert, um mit den fortschreitenden Innovationen Schritt halten zu können. Zudem muss eine Balance zwischen technischem Wissen und praktischer Anwendung gefunden werden, um die Studierenden optimal vorzubereiten, ohne sie im Unterricht zu überfordern oder zu verlieren. Weitere Herausforderungen ergeben sich aus den unterschiedlichen IT-Vorkenntnissen der Teilnehmenden. Es stellt eine Herausforderung dar, alle Beteiligten auf ein einheitliches Kompetenzniveau zu bringen, ohne dabei eine Über- oder Unterforderung zu riskieren.

Experte 1 geht einen Schritt weiter und definiert KI-Kompetenzen umfassender, indem er sie mit tiefgehendem Wissen in den Bereichen Statistik, Informatik, Mathematik und Algorithmik assoziiert. Diese Anforderungen erscheinen jedoch im Rahmen einer traditionellen Polizeiausbildung schwer umsetzbar, da sie ein vertieftes theoretisches Verständnis erfordern, das über die praktischen Ausbildungsziele hinausgeht.

Welche Ansätze und Methoden halten Sie für am effektivsten, um KI-Kompetenzen in der Ausbildung zu vermitteln?

Bei der Frage, welche Ansätze und Methoden für am effektivsten gehalten werden, verfolgen die Experten unterschiedliche Ansätze. Experte 1 legt den Fokus auf anwenderorientierte praktische Übungen mit KI-Werkzeugen, da eine theoretische Abhandlung oder technische Betrachtung der Methoden als unrealistisch für die Zielgruppe angesehen wird. Selbst die Bewertung von KI-generierten Ergebnissen stellt seiner Ansicht nach bereits eine Herausforderung dar, die für viele Studierende zu tiefgehend ist. Im Gegensatz dazu spricht sich Experte 2 für eine Kombination aus theoretischen und praktischen Inhalten aus. Dieser Ansatz ermögliche es den Studierenden, grundlegendes Wissen zu KI-Technologien zu erwerben und gleichzeitig deren praktische Anwendung zu erlernen. Während Experte 1 die Praxisnähe als zentralen Aspekt betont, sieht Experte 2 die Verknüpfung von Theorie und Praxis als wesentlich für eine umfassende Kompetenzvermittlung an.

Zukunftsperspektiven und Weiterentwicklung

Wie sehen Sie die Zukunft der Polizeiausbildung im Hinblick auf KI-Kompetenzen in den nächsten fünf bis zehn Jahren?

Die Experten zeichnen unterschiedliche Perspektiven zur zukünftigen Entwicklung der Polizeiausbildung im Hinblick auf KI-Kompetenzen. Experte 1 sieht die Integration technischer Kompetenzen als wünschenswert, jedoch durch derzeit fehlende Grundlagen bei den Polizeibeamtinnen und -beamten begrenzt. Er betont, dass KI-Methoden erst dann breiter einsetzbar sein werden, wenn ihre Anwendungen dahingehend so weit vereinfacht sind, dass sie auch von Laien genutzt werden können. Zudem sieht er insbesondere in forensischen Werkzeugen Potenzial. Experte 2 hingegen erwartet eine deutliche Ausweitung von Anwendungsfeldern für KI in der Polizeiarbeit, beispielsweise in der automatisierten Bildkategorisierung und der Analyse von Kommunikationsdaten.

Schlussbemerkungen

Möchten Sie noch etwas hinzufügen oder gibt es weitere Punkte, die Sie in Bezug auf die KI-Kompetenzen und Polizeiausbildung für besonders wichtig halten?

Abschließend wird die Integration von KI-Kompetenzen als „essenziell für die zukünftige Polizeiarbeit“ hervorgehoben, so Experte 2. Die zentralen Herausforderungen liegen insbesondere in der schnellen technologischen Entwicklung und der Gestaltung praxisrelevanter Ausbildungsinhalte. Eine Kombination aus theoretischen Grundlagen und praktischer Anwendung wird dabei als effektivster Ansatz zur Vermittlung von KI-Kompetenzen angesehen.

Diskussion

Wie in der Einleitung dargelegt, untersucht dieser Beitrag, ob Polizeistudierende in Baden-Württemberg verstärkt und in größerem Umfang Kompetenzen im Bereich KI benötigen, um den steigenden technologischen Anforderungen im Polizeialltag gerecht werden zu können. Die Ergebnisse der durchgeführten Experteninterviews bestätigen diese Notwendigkeit. Dabei deckt sich diese Einschätzung auch mit der grundsätzlichen Position des Ministeriums für Kultus, Jugend und Sport Baden-Württemberg, das die Vermittlung solcher Kompetenzen für alle Schülerinnen und Schüler als wesentlich erachtet (Ministerium für Kultus, Jugend und Sport Baden-Württemberg 2024). Eine ähnliche Perspektive vertritt der Branchenverband der deutschen Informations- und Telekommunikationsbranche bitkom. In einer aktuellen Befragung von über 500 Lehrkräften der Sekundarstufen I und II gaben mehr als 80 Prozent an, dass der Umgang mit KI grundlegender Bestandteil der schulischen Ausbildung sein sollte (bitkom 2024). Diese Ergebnisse verdeutlichen den breiten gesellschaftlichen Konsens über die Relevanz von KI-Kompetenzen, der auch in die Ausbildung von Polizeistudierenden integriert werden sollte.

Die Interviews zeigen, dass der Begriff „KI-Kompetenzen“ unterschiedlich interpretiert wird: Während Experte 1 den Schwerpunkt auf technische Aspekte wie Entwicklung und Funktionsweise legt, betont Experte 2 die theoretische und praktische Anwendung im Polizeialltag. Um eine konsistente und praxisorientierte Ausbildung zu gewährleisten, sollte im Studium eine klare, einheitliche Definition von KI-Kompetenzen festgelegt werden. Diese könnte sowohl technische Grundlagen als auch anwendungsbezogene Fähigkeiten berücksichtigen, um den vielfältigen Anforderungen gerecht zu werden.

Beide Experten bestätigen dabei insbesondere zwei zentrale Herausforderungen für die Integration von KI in die Polizeiausbildung. Zum einen erfordert die rasante technologische Entwicklung mit immer kürzeren Innovationszyklen eine kontinuierliche Aktualisierung der Lehrinhalte, was einen erheblichen Aufwand für die regelmäßige Überarbeitung und Anpassung von Vorlesungen bedeutet. Zum anderen variieren die Vorkenntnisse der Studierenden, insbesondere im Bereich IT und KI, teils stark, wodurch die Gefahr besteht, sowohl Über- als auch Unterforderungen zu erzeugen. Um diesen Herausforderungen zu begegnen, könnten modulare Lehrkonzepte entwickelt werden, die unterschiedliche Vorkenntnisniveaus berücksichtigen. Dies würde auch sicherstellen, dass alle Studierenden unabhängig von ihren Vorkenntnissen optimal auf die Anforderungen des Polizeialltags vorbereitet werden.

Die Stichprobengröße von lediglich zwei befragten Experten, bedingt durch den vorgegebenen begrenzten Umfang des Beitrags, stellt eine methodische Einschränkung dar, die die Übertragbarkeit der Ergebnisse auf eine größere Population limitieren könnte. Mögliche Verzerrungen könnten zudem durch die spezifischen Perspektiven und Erfahrungen der ausgewählten Experten entstehen, was die Generalisierbarkeit der Erkenntnisse beeinflussen kann. Dennoch bieten die gewonnenen Einblicke wertvolle erste Anhaltspunkte, die als Grundlage für weiterführende Untersuchungen mit einer breiteren Datenbasis dienen können.

Zudem bleibt die Frage offen, welche konkreten Kompetenzen die Zielgruppen selbst als relevant erachten. Eine umfassende Befragung von Studierenden und Absolventinnen und Absolventen nach ihrem ersten Dienstjahr könnte wertvolle Hinweise darauf liefern, welche Inhalte tatsächlich praxisrelevant sind. Diese Erkenntnisse sollten in die Konzeption neuer Lehrpläne einfließen, um die Ausbildung noch stärker an den realen Anforderungen des Polizeialltags auszurichten.

Schlussfolgerungen

Die vorliegende Diskussion verdeutlicht, dass die Vermittlung von KI-Kompetenzen für Polizeibeamtinnen und -beamte zunehmend an Bedeutung gewinnt und eine dringende Notwendigkeit darstellt. Der technologische Wandel, insbesondere die rasante Entwicklung und Anwendung von KI, eröffnet der Polizeiarbeit neue Möglichkeiten – von der Prävention über die Ermittlungsarbeit bis hin zur strategischen Entscheidungsfindung.

Ein erster wichtiger Schritt in Baden-Württemberg war die Einführung des K-IT-Studiengangs, der auf die Verbindung von Informatik und polizeilichen Anforderungen abzielt. Allerdings betrifft dieser jährlich nur eine begrenzte Zahl von Studierenden und deckt daher lediglich einen Bruchteil des tatsächlichen Bedarfs ab. Damit verbleibt die große Mehrheit der Studierenden ohne spezifische KI-Kompetenzen, was langfristig die Technologieakzeptanz und -anwendung im Polizeialltag hemmen könnte.

Die Bedeutung von Technologieoffenheit und die gezielte Förderung von Kompetenzen im Umgang mit KI sollten daher als zentrale Elemente in das Polizeistudium integriert werden. Dies erfordert jedoch eine systematische Weiterentwicklung der bestehenden Lehrpläne. Besonders wichtig ist dabei, nicht nur auf die technischen Grundlagen einzugehen, sondern auch ethische, rechtliche und operationale Fragestellungen zu behandeln. Ein solcher Lehrplan sollte praxisnah gestaltet werden, um den Polizeibeamtinnen und -beamten das Rüstzeug zu geben, KI-Technologien sowohl kritisch zu hinterfragen als auch effektiv zu nutzen.

Zusammenfassend lässt sich festhalten, dass die Integration von KI-Kompetenzen in die Polizeiausbildung nicht nur die Qualität der Polizeiarbeit steigern, sondern auch die Wettbewerbsfähigkeit der Polizei Baden-Württemberg im digitalen Zeitalter sichern kann. Dies erfordert jedoch eine strategische und langfristige Herangehensweise, die sowohl technische als auch organisatorische Aspekte berücksichtigt. Nur so kann sichergestellt werden, dass die Polizei auch in Zukunft effektiv, innovativ und verantwortungsvoll agieren kann.

Aus den vorangegangenen Analysen lassen sich damit folgende, nicht abschließende Handlungsempfehlungen ableiten:

- Durchführung von Befragungen unter Studierenden und Absolventinnen und Absolventen, um die im beruflichen Alltag tatsächlich relevanten KI-Kompetenzen zu identifizieren.
- Entwicklung einer einheitlichen und verbindlichen Definition des Begriffs „KI-Kompetenzen“ als Grundlage für die Ausbildung.
- Konzeption eines umfassenden Lehrplans, der KI-relevante Inhalte für alle Studierenden integriert und praxisorientiert vermittelt.
- Etablierung eines kontinuierlichen Evaluationsprozesses, um die Aktualität und Relevanz der Lehrinhalte überprüfen und diese fortlaufend an technologische sowie gesellschaftliche Entwicklungen anpassen zu können.

Literaturverzeichnis

Bendel, Oliver (2024): 300 Keywords Generative KI: Ökonomische, technische und ethische Grundlagen. Wiesbaden: Springer Fachmedien

bitkom (2024): Bereits jede zweite Lehrkraft hat KI für die Schule genutzt [online]: bitkom.org/Presse/Presseinformation/jede-zweite-Lehrkraft-KI-Schule-genutzt#_ (abgerufen am 22.11.2024)

Bogner, Alexander/Littig, Beate & Menz, Wolfgang (Hrsg.) (2005): Das Experteninterview: Theorie, Methode, Anwendung. 2. Auflage. Wiesbaden: VS Verlag für Sozialwissenschaften | GWV Fachverlage GmbH

Bogner, Alexander/Littig, Beate & Menz, Wolfgang (2014): Interviews mit Experten: eine praxisorientierte Einführung. Wiesbaden: Springer Fachmedien

BSI (Bundesamt für Sicherheit in der Informationstechnik) (2022): Künstliche Intelligenz – wir bringen Ihnen die Technologie näher [online]: [bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Technologien_sicher_gestalten/Kuenstliche-Intelligenz/kuenstliche-intelligenz_node.html](https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Technologien_sicher_gestalten/Kuenstliche-Intelligenz/kuenstliche-intelligenz_node.html) (abgerufen am: 22.11.2024)

Bundesministerium für Bildung und Forschung (2023): Künstliche Intelligenz [online]: [bmbf.de/bmbf/de/forschung/digitale-wirtschaft-und-gesellschaft/kuenstliche-intelligenz/kuenstliche-intelligenz_node.html](https://www.bmbf.de/bmbf/de/forschung/digitale-wirtschaft-und-gesellschaft/kuenstliche-intelligenz/kuenstliche-intelligenz_node.html) (abgerufen am: 22.11.2024)

Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen (2021): Weiterführende Informationen zum Themenbereich künstlicher Intelligenz [online]: [bundesnetzagentur.de/SharedDocs/Downloads/DE/Sachgebiete/Digitales/KI/Hintergrundpapier.pdf?__blob=publicationFile&v=1](https://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/Sachgebiete/Digitales/KI/Hintergrundpapier.pdf?__blob=publicationFile&v=1) (abgerufen am: 22.11.2024)

Deutscher Ethikrat (2023): Mensch und Maschine – Herausforderungen durch Künstliche Intelligenz – Stellungnahme [online]: ethikrat.org/fileadmin/Publikationen/Stellungnahmen/deutsch/stellungnahme-mensch-und-maschine.pdf (abgerufen am: 25.10.2024)

Die Bundesregierung (2024): Einheitliche Regeln für Künstliche Intelligenz in der EU [online]: bundesregierung.de/breg-de/aktuelles/ai-act-2285944 (abgerufen am 22.11.2024)

Europäische Kommission (2021): Verordnung über künstliche Intelligenz (KI-Verordnung), COM(2021) 206 final [online]: ai-act-law.eu/de/artikel/3/ (abgerufen am: 22.11.2024)

Flick, Uwe (2014): Qualitative Sozialforschung: Eine Einführung. 6. Auflage. Hamburg: Rowohlt Taschenbuch Verlag

Gläser, Jochen & Laudel, Grit (2010): Experteninterviews und qualitative Inhaltsanalyse: Als Instrumente rekonstruierende Untersuchungen. 4. Auflage. Wiesbaden: VS Verlag für Sozialwissenschaften | Springer Fachmedien Wiesbaden GmbH

Hochschule für Polizei Baden-Württemberg (2024a): Bachelor-Studiengänge [online]: hfpol-bw.de/studiengaenge/ (abgerufen am: 22.11.2024)

Hochschule für Polizei Baden-Württemberg (2024b): Jahresbericht 2023 [online]: hfpol-bw.de/wp-content/uploads/2024/09/Jahresbericht_2023-mittel.pdf (abgerufen am 24.11.2024)

Mayring, Philipp & Fenzl, Thomas (2019): Qualitative Inhaltsanalyse. In: Baur, Nina & Blasius, Jörg (Hrsg.): Handbuch Methoden der empirischen Sozialforschung. Wiesbaden: Springer VS, S. 633-648

Ministerium für Kultus, Jugend und Sport Baden-Württemberg (2024): KI im Unterricht – Informationsangebote für Lehrkräfte [online]: km.baden-wuerttemberg.de/de/schule/digitalisierung/kuenstliche-intelligenz-im-unterricht (abgerufen am 23.11.2024)

Oberrauter-Zabransky, Barbara (2024): KI-Skills: Welche Kompetenzen in Zeiten von ChatGPT und Co. wirklich zählen [online]: stepstone.at/e-recruiting/blog/ki-skills/#h-was-sind-ki-skills (abgerufen am 22.11.2024)

Polizei Baden-Württemberg (2024): Über uns [online]: polizei-bw.de/ueber-uns-2/ (abgerufen am: 25.11.2024)

Polizeiliche Kriminalprävention (2023): Künstliche Intelligenz im Alltag und in der Kriminalitätsbekämpfung [online]: polizei-beratung.de/aktuelles/detailansicht/kuenstliche-intelligenz-im-alltag-und-in-der-kriminalitaetsbekaempfung/ (abgerufen am: 24.10.2024)

Rachner, Lucas (2023): Starke vs. Schwache KI – Eigenschaften & Anwendungen [online]: visusadvisory.com/post/starke-vs-schwache-ki (abgerufen am 22.11.2024)

Schümann, Nicolai (2024): Gamechanger Künstliche Intelligenz: Wie künstliche Intelligenz inspiriert und kreatives Potenzial entfesselt. Freiburg: Haufe-Lexware GmbH & Co. KG

Einfluss von Virtual Reality und KI-gesteuerten Trainingsprogrammen auf die Entscheidungsfindung von Polizeikräften

Philipp Rauthe

Der Einsatz Künstlicher Intelligenz (KI) hat in den letzten Jahren nahezu in allen Bereichen des öffentlichen und privaten Lebens zugenommen (Deutscher Ethikrat, 2023, S. 5). Auch die Polizei versucht sich die Vorzüge der KI zunutze zu machen. Somit können Arbeitsprozesse zukünftig verändert, optimiert und vereinfacht werden. KI wird bereits in der polizeilichen Praxis bei der Bewältigung von Massendaten (Laude et al., 2022, S. 1509 ff.) sowie im Bereich des polizeilichen Verhaltenstrainings (Bock, 2023) eingesetzt. Ein weiteres Einsatzgebiet wird aktuell in der polizeilichen Aus- und Fortbildung mithilfe von KI erschlossen. Hierbei sollen Polizeikräfte anhand von Virtual Reality (VR) und KI auf reale Einsatzsituationen vorbereitet werden. Darüber hinaus soll mit dieser Technologie versucht werden, mittels Erkennung von Stressmomenten Polizeibeamtinnen und -beamte schon in der Aus- und Fortbildung psychisch zu unterstützen (Bioni, Achtziger und Gentsch, 2010, S. 4). Mithilfe dieser Simulationen und Trainingsmethoden bieten sich nicht nur innovative Ansätze für das Training, sondern auch Potenzial zur signifikanten Verbesserung der Entscheidungsfindung von Polizeikräften in realen kritischen Einsatzsituationen (Marler et al., 2020, S. 2). Diese Entwicklung wirft jedoch auch Fragen hinsichtlich der Effektivität, ethischen Implikationen (Anonym, 2021, S. 5) und der potenziellen Risiken auf, dass eine übermäßige Abhängigkeit von KI-Systemen zu einer Vernachlässigung des menschlichen Urteilsvermögens und kritischen Denkens führen könnte (Funke, 2024).

Ziel ist es eine Konzeption zu entwickeln, die untersucht, inwieweit VR-Trainingsprogramme mit KI-gesteuerten Simulationen die Entscheidungsfindung von Polizeikräften beeinflussen und zugleich den Aspekt der Affektivität von emotionalen menschlichen Zuständen in realen Einsatzsituationen bestimmen können. Dabei werden sowohl die potenziellen Vorteile als auch die Herausforderungen und Risiken

beleuchtet, die mit der Integration dieser Technologien in die polizeiliche Ausbildung einhergehen. Ziel ist es, eine Konzeption zu entwickeln, welche in der polizeilichen Praxis implementiert werden kann.

Hintergrund

Polizeibeamte stehen oft unter immensem Druck, in Sekundenbruchteilen lebenswichtige Entscheidungen zu treffen. Diese Situationen sind geprägt von Unsicherheiten, Stress und einer hohen emotionalen Belastung (Bioni, Achtziger und Gentsch, 2010, S. 3). Studien haben gezeigt, dass diese Faktoren sowohl die kognitive Leistung als auch die Entscheidungsfindung beeinflussen können (Seibold and Horn, 2021, S. 147). Somit stellt der Umgang mit Stress nicht nur eine emotionale Herausforderung dar, sondern auch einen Schlüsselfaktor, der das Verhalten und die Reaktionen von Beamten in Einsatzsituationen beeinflusst (Seibold and Horn, 2021, S. 87). Zudem spielt das Training eine entscheidende Rolle, um Beamte auf diese stressbeladenen Situationen vorzubereiten (Heil and Bechold, 2022, S. 379). Traditionelle Trainingsmethoden können die Komplexität und Unvorhersehbarkeit realer Situationen häufig nicht simulieren. Daher wird verstärkt nach innovativen Ansätzen gesucht, um solche Situationen realitätsnah zu trainieren. An dieser Stelle kommt die Kombination aus VR und KI ins Spiel. VR bietet die Möglichkeit, immersive und realistische Szenarien zu simulieren, die es Beamten ermöglichen, in sicheren Umgebungen ihre Reaktionen zu üben und zu verbessern (Caserman et al., 2019, S. 2). Gleichzeitig kann KI zur Echtzeitanalyse von Verhaltensmustern und emotionalen Zuständen genutzt werden, um ein präzises Feedback zu geben und so das Training effektiver zu gestalten (Caserman et al., 2023, S. 183).

Aktueller Forschungsstand

Verschiedene Forschungsarbeiten haben sich mit der Verbesserung von Entscheidungsprozessen unter Stress mithilfe von VR- und KI-Technologien auseinandergesetzt. Caserman et al. (2019) haben beispielsweise ein VR-Trainingssystem für die Polizei entwickelt, das gefährliche Bereiche mithilfe von KI in Echtzeit erkennt und da-

raufhin das Deckungsverhalten der Trainees analysiert. Diese Studie sollte Polizeibeamten die Möglichkeit geben, ihre Reaktionen in einer virtuellen Umgebung zu testen und dabei sofortiges Feedback zu erhalten. Die Autoren konzentrierten sich auf die Integration von VR in die Ausbildung und die Simulation von realen Einsatzsituationen. Jekauc et al. (2024) untersuchten, wie Künstliche Intelligenz zur Erkennung emotionaler Zustände von Athleten verwendet werden kann. Sie nutzten Convolutional Neural Networks (CNNs), um emotionale Reaktionen in realen Spielsituationen zu erkennen. Bei CNNs handelt es sich um eine Netzwerkarchitektur für Deep Learning. Sie sind besonders nützlich, um Muster in Bildern zu finden und Objekte zu erkennen (Mathworks, 2024). Hier konnte gezeigt werden, wie maschinelles Lernen eingesetzt werden kann, um affektive Zustände in Echtzeit zu analysieren. Das Ergebnis bietet eine Grundlage für die Idee, KI auch in anderen Bereichen zur Emotionserkennung, wie der Polizeiausbildung, anzuwenden. Eine weitere Untersuchung von Marler et al. (2020) befasste sich mit spielbasierten VR-Trainingsmethoden, die speziell auf die Entscheidungsfindung unter Stress abzielen. In dieser Studie wurde festgestellt, dass durch VR realitätsnahe Szenarien geschaffen werden können, die traditionelle Trainingsmethoden übertreffen. Die Umgebungen können dynamisch angepasst werden und bieten so die Möglichkeit, das Stresslevel des Trainees einzustellen, um die Entscheidungsfindung unter Druck zu trainieren.

Die methodischen Ansätze in diesen Studien zeigen, wie VR- und KI-Technologien genutzt werden können, um Trainingsszenarien für stressbelastete Berufe zu verbessern. In der Studie von Caserman et al. wurde ein VR-System entwickelt, das von KI unterstützt wird und in Echtzeit Feedback gibt, wenn Beamte in riskanten Bereichen ungeschützt agieren. Dies ermöglichte eine sofortige Korrektur von taktischen Fehlern. Jekauc et al. gingen methodisch mit maschinellen Lernalgorithmen vor, um emotionale Zustände anhand von Gesichtsausdrücken und Körperhaltungen zu analysieren. Die Forscher trainierten ihre CNN-Modelle mit realen Daten aus Wettkampfsituationen. Ihre Forschung lieferte wertvolle Erkenntnisse darüber, wie KI-basierte Emotionserkennung in stressigen und wettbewerbsorientierten Umgebungen funktioniert und wie sie zu präzisen Ergebnissen führt.

Methodik

Die Methodik in diesem Beitrag zielt darauf ab, ein umfassendes und fundiertes Konzept zur Integration von VR und KI in Trainings- und Entscheidungsfindungssystemen zu entwickeln. Dieses Konzept soll auf bestehenden wissenschaftlichen Erkenntnissen aufbauen, zugleich aber auch neue Anwendungsbereiche aufzeigen.

Vorgehensweise bei der Erstellung des Beitrags

Der erste Schritt bestand in der systematischen und gründlichen Analyse der existenten Literatur. Hierbei wurde gezielt nach dem aktuellen Stand der Forschung zu VR- und KI-Anwendungen in der Aus- und Fortbildung sowie zur Emotionserkennung gesucht. Anhand einer systematischen Literaturrecherche (Schwegmann, 2023) wurde mit unterschiedlichen Schlüsselwörtern wie „Virtual Reality Training“, „Virtual Reality“, „Artificial Intelligence AND Decision-Making“, „Machine Learning“, „Convolutional Neural Networks“, „KI-gestützte Simulationen AND Trainingsprogramme“, „Police Training“ und „Sports Psychology“ in wissenschaftlichen Datenbanken wie Google Scholar, PubMed und SpringerLink gesucht. Es wurden hauptsächlich aktuelle Arbeiten erfasst. Bei wenigen bis keinen Treffern auf ausgewählte Suchbegriffe wurde auch nach älteren Arbeiten recherchiert. Die Auswahl der Literatur basierte auf der Relevanz für das Thema und der Aktualität der Veröffentlichungen. Die systematische Analyse der Literatur wurde durch eine vergleichende Inhaltsanalyse ergänzt. Dabei wurden die identifizierten Theorien, Modelle und empirischen Ergebnisse auf Gemeinsamkeiten, Unterschiede und Lücken untersucht. Ziel dieser vergleichenden Analyse war es, eine kohärente theoretische Basis zu schaffen, auf der die spätere Konzeption aufbauen kann. Mittlerweile finden sich zu den o. g. Themen viele wissenschaftliche Arbeiten. Eine Kombination aus VR und KI im Einsatztraining ist jedoch noch recht einzigartig. Im Ergebnis der Literaturrecherche wurden mehrere Bücher, Fachartikel, Zeitschriften sowie Studien analysiert. Diese kamen aus unterschiedlichen untersuchten Themenbereichen der Arbeitswelt wie z. B. aus dem Bereich des Militärs, der Polizei sowie anderer Sicherheitsbehörden (Ahir et al., 2019; Pallavicini et al., 2016; Pallavicini et al., 2015). Die meis-

ten dieser Arbeiten widmeten sich der Analyse und dem Mehrwert von VR-Trainings im Bereich der Aus- und Fortbildung. Im Ergebnis wurde beispielhaft für den Bereich des VR-Trainings eine Arbeit ausgewählt, welche sich mit dem spielbasierten VR-Trainingssystem beschäftigt (Marler et al., 2020). Zudem wurden zwei weitere Arbeiten extrahiert, welche sich zum einen mit dem neuen Konzept der Emotionserkennung durch KI beim Menschen in Sportsituationen beschäftigt (Jekauc et al., 2024) und zum Zweiten eine Studie, in welcher ein VR-Simulator vorgestellt wird, der eine KI nutzt, um das Deckungsverhalten eines Trainees in Echtzeit zu erkennen und zu beurteilen (Caserman et al., 2023). Basierend auf den Ergebnissen der Literaturrecherche wurde eine Konzeption entwickelt, welche die relevantesten Theorien und empirischen Befunde zu einem kohärenten Rahmen zusammenfasst. Insbesondere wird auf Theorien des situativen Lernens, des adaptiven Lernens und der maschinellen Mustererkennung zurückgegriffen (Privenau, 2012, S. 17).

Evaluation

Die Überprüfung der entwickelten Konzeption soll durch Evaluationsstrategien erfolgen. Durch diese methodische Herangehensweise wird garantiert, dass die entwickelte Konzeption wissenschaftlich fundiert, praktisch relevant und methodisch solide ist.

Entwicklung einer Konzeption

Die Anforderungen an Polizeibeamte in realen Einsatzsituationen sind hoch. Stress und emotionale Belastungen spielen dabei eine zentrale Rolle, die sowohl die Entscheidungsfähigkeit als auch die Handlungssicherheit beeinträchtigen können (Heinrich et al., 2011, S. 2). Die Konzeption zielt darauf ab, ein theoretisches Modell zu entwickeln, das VR und KI für diese Situationen miteinander kombiniert, um ein Echtzeitfeedback zu generieren und den emotionalen Zustand sowie das Stresslevel zu analysieren.

VR als Trainingsplattform

VR bietet eine immersive Umgebung, die es Polizeibeamten ermöglicht, realitätsnahe Einsatzszenarien zu erleben, ohne sich in tatsächlicher Gefahr zu befinden (Marler et al., 2020, S. 183). Das Modell verwendet dabei die Theorie des situativen Lernens, die besagt, dass Lernen am effektivsten ist, wenn es einer realen Anwendungssituation ähnlich ist (Hartmann und Bannert, 2022). Die Integration von VR ermöglicht es zudem, die Resilienz und Handlungsfähigkeit der Beamten zu fördern.

Umsetzung im Modell

Die Entwicklung der VR-Plattform ist der erste und zugleich bedeutendste Schritt in der Erstellung der Konzeption. Diese generiert den Rahmen, um eine realitätsnahe und anpassungsfähige Szenarienerstellung im Training zu ermöglichen. Hierbei muss darauf geachtet werden, dass ein möglichst großer Facettenreichtum an Einsätzen simuliert werden kann. Beispiele hierfür wären z. B. Geiselnahmen oder Personen- und Verkehrskontrollen. Die Szenarien sollen dynamisch an die Trainingsbedürfnisse der Trainees angepasst werden können. Eine Über- oder Unterforderung soll vermieden werden. Für die Realisierung dieser Szenarienerstellung ist es von Bedeutung, dass interaktive Elemente in die Plattform integriert werden. Hierbei sollen Virtuelle Charaktere (NPCs) (Ionos, 2023), die durch KI gesteuert werden, mit den Trainees interagieren, indem sie auf deren Aktionen reagieren und die Szenarien entsprechend individuell gestalten. Die Situationen sollen so gestaltet werden, dass Stress bei Polizeibeamten ausgelöst wird. Diese können dabei vom sogenannten First-Person-Shooter-Szenario bis hin zum First-Person-Talker-Szenario (Marler et al., 2020, S. 3) variieren. Zusätzlich muss dem System eine Vielzahl von Daten zur Verfügung gestellt werden, welche die gewünschte Verhaltensweise bzw. -reaktion der Trainee zeigen. Diese Daten können sowohl durch tradierte Trainingsmethoden als auch über die realen Einsatzsituationen gesammelt werden, welche in beiden Varianten durch den Einsatz der Bodycam zugeliefert werden. Aufgrund der In-

dividualität jedes Beamten (Alter, Leistungsspektrum) ist es wichtig, dass während des Trainings eine individuelle Anpassung der Schwierigkeitsgrade vorgenommen werden kann.

KI-gestütztes Erkennen von Gefahrenbereichen und Echtzeit-feedback

KI, insbesondere maschinelles Lernen, ermöglicht nach dem umfangreichen Anlernen über eine Vielzahl von Daten und den daraus resultierenden Mustern eine Echtzeitanalyse und kann sofortiges Feedback geben (Bekker, 2018). Mit der Theorie des adaptiven Lernens wird gezeigt, wie wertvoll sofortiges Feedback ist und wie es das Lernen effektiver macht (Berger und Moser, 2020, S. 43).

Umsetzung im Modell

Die Studie von Caserman et al. analysiert mithilfe von KI das Deckungsverhalten der Trainees. Hierbei wird ein potenziell schlechtes Deckungsverhalten erkannt und folglich gefährliche Situationen erzeugt, um den Trainees aufzuzeigen, wo Schwächen im Deckungsverhalten vorhanden waren (Caserman et al., 2023, S. 184). Während der Trainingsdurchführung werden Daten wie Reaktionszeiten, gewählte Taktiken und der Umgang mit unerwarteten Ereignissen erfasst, gespeichert und ausgewertet. Dieses Feedback kann visuell (z. B. in einem VR-Display), auditiv oder durch Unterbrechung des Einsatztrainers erfolgen. Zur Verbesserung der Genauigkeit der KI sowie zur Vermeidung von Bias ist es wichtig, die Trainingsdaten sorgfältig zu kuratieren und sicherzustellen, dass sie repräsentativ für reale Einsätze sind. Neben den vorgestellten Punkten soll das System darüber hinaus bewerten können, ob sich der Trainee in einer für ihn emotional stressigen Situation befindet.

Analyse des emotionalen Zustands und des Stresslevels

Emotionen und Stress haben einen signifikanten Einfluss auf die Entscheidungsfindung (Heinrich et al., 2011, S. 2). Theorien zur emotionalen Intelligenz und Stressbewältigung legen nahe, dass das Erkennen emotionaler Zustände sowie das Stresslevel dazu beitragen

können, die Handlungsfähigkeit in kritischen Situationen zu verbessern (Eppel, 2007, S. 120 ff.). Diese Art der Stressbewältigung wird als verhaltens- und kognitiv bezogene Stressbewältigung bezeichnet (Grottko, 2021, S. 19).

Umsetzung im Modell

Mit dem vorliegenden Beitrag sollen die vorgestellten Forschungsmodelle um eine Verhaltensanalyse der Trainees ergänzt werden. Hierzu muss das System mit Daten aus Mimik und Gestik sowie mit Vitalfunktionen ergänzt werden, wie Polizeibeamte in realen Einsatzsituationen und Übungsszenarien reagierten. Diese Daten sind wichtig, um das System mit Vergleichs- und Übungsdaten anzulernen. Hierbei stellte sich die Frage, woher diese große Menge an Daten genommen werden kann, sodass sie auch einen repräsentativen Charakter aufweisen und das System ordnungsgemäß angelernt werden kann. Hierfür drängt sich ein dualmodaler Ansatz auf. Dieser kombiniert die dynamischen und komplexen Prozesse, welche sich in Übungsszenarien ergeben, mit Videosequenzen und -bildern, welche analysiert werden können. Ergänzend kommt hier die fortschrittliche CNN-Architektur zur Anwendung, welche speziell für die Aufgabe der Affekterkennung konzipiert wurde (Jekauc et al., 2024, S. 5). Um an die Daten aus realen Einsatzsituationen zu gelangen, ist die Nutzung der Bodycam-Aufnahmen die wohl geeignetste Variante. Zudem existiert im Internet eine Vielzahl an Einsatzsituationen, welche gefilmt wurden. Hierbei kann man auf eine erheblich größere Bandbreite an Daten zugreifen, da die Videosequenzen nicht nur aus Deutschland stammen, sondern auch aus anderen Ländern. Somit kann ein größerer repräsentativer Datensatz erstellt werden. Solche Daten können aber auch über Trainingsszenarien generiert werden. Hierfür ist eine spezielle technische Ausstattung unabdingbar. Diese muss bspw. aus Sensoren bestehen, welche Gesichtsausdrücke, Körperhaltung und andere physiologische Marker (z. B. Herzfrequenz, Schweißproduktion, Körperwärme) erkennen, registrieren und speichern. Durch eine KI-basierte Analyse werden diese Daten in Echtzeit ausgewertet, um Rückschlüsse auf den emotionalen Zustand und das Stresslevel des Trainees zu ziehen. Dies umfasst die Erkennung von Anzeichen für hohen Stress, Angst oder Unsi-

cherheit. Daraufhin kann eine individuelle Anpassung durch Erhöhung oder Reduzierung des Schwierigkeitsgrades erfolgen. Ebenso sind auch gezielte Entspannungsübungen innerhalb des Szenarios möglich, um eine Überforderung der Trainees zu vermeiden. Durch diese Analyse können ebenfalls Rückschlüsse gezogen werden, wie die Resilienz der Trainees ist. Im Ergebnis dessen kann eine optimale Auswahl für spezielle Einsatzbereiche der Polizei, wie z. B. das Spezialeinsatzkommando (SEK), erfolgen. Zudem hat die Analyse des emotionalen Zustands den Vorteil, dass Personen psychisch nicht überfordert werden. Dementsprechend kann mithilfe des Systems ein erheblicher Mehrwert in Sachen Gesundheitsprävention erfolgen, indem Beamte nicht in Verwendungen oder Auslandseinsätze gelangen, für die sie nicht die erforderliche Resilienz besitzen. Damit kann Gesundheitsproblemen wie Depressionen oder Burnout und den damit verbundenen Ausfallszeiten vorgebeugt werden (Ohmann und Heuse, 2021, S. 29).

Praktische Umsetzung

Um die beschriebene Theorie in die Praxis umzusetzen, muss eine schrittweise Implementierung des Modells stattfinden. In den meisten Fällen steht zu Beginn einer solchen Umsetzung eine Pilotphase. In dieser werden die theoretischen Grundlagen in einer Prototypenentwicklung umzusetzen versucht. Hierzu müsste ein Prototyp der VR- und KI-Plattform entwickelt werden, der grundlegende Szenarien und einfache Feedbackmechanismen integriert. Wie ein solcher erster Schritt in die Praxis umgesetzt werden kann, wird in der Studie „Virtual Reality Simulator for Police Training with AI-Supported Cover Detection“ (Caserman et al., 2023) beschrieben. Der Versuchsaufbau soll anschließend mit einer Kombination aus einem Pose- und einem Bildnetzwerk ergänzt werden. Beide basieren auf vortrainierten CNN-Modellen. Das Ergebnis der beiden Modelle wurde in einer gemeinsamen Merkmalsvektorkombination verarbeitet, um den affektiven Zustand zu klassifizieren (Jekauc et al., 2024). Ergänzend werden durch Sensoren die Gesichtsausdrücke, Körperhaltung und andere physiologische Marker erkannt, registriert und gespeichert, um Rückschlüsse auf den mentalen Zustand des Trainees zu zulassen. Nachdem der Prototyp entwickelt wurde, muss dieser von

einer kleinen Gruppe von Polizeibeamten getestet werden, um erste Daten über die Effektivität, Zuverlässigkeit und Benutzerfreundlichkeit des Systems zu sammeln. Sofern der erste Eindruck der Pilotstudie positiv ist und sich ein Mehrwert abzeichnet, kann im Folgenden eine Erweiterung der Einsatzszenarien entwickelt und integriert werden. Des Weiteren lernt die KI und kann mit fortgeschrittenen KI-Algorithmen weiterentwickelt werden, um präzisere Analysen des Verhaltens und emotionalen Zustands der Trainees durchzuführen. Dazu werden fortschrittliche CNNs und Algorithmen des Deep Learning verwendet. Um das System fortlaufend zu verbessern, muss eine kontinuierliche Anpassung und Optimierung erfolgen. Hierzu werden die gesammelten Daten und das Feedback der Nutzer verwendet, um den Nutzen für die Polizeiausbildung, Rekrutierung sowie die Gesundheitsvorsorge zu maximieren.

Technische Anforderungen für die Erstellung des Modells

Die Implementierung eines solchen Modells in die Aus- und Fortbildung erfordert neben der Akzeptanz der Nutzer auch technische Anforderungen und Voraussetzungen. Diese lassen sich in Komponenten der Hard- und Software differenzieren. Im Bereich der Hardware werden hochauflösende VR-Headsets, Motion-Capture-Anzüge, Sensoren zur Erfassung physiologischer Daten (z. B. Herzfrequenzmesser, Körpertemperaturmesser), Gesichtserkennungskameras und Sensoren sowie leistungsstarke Computer und Server benötigt. Die Software muss sowohl die Erstellung und Anpassung der VR-Umgebung als auch die Implementierung der KI-Modelle und der Emotionserkennung unterstützen. Ein Datenmanagement- und Analysetool ist unerlässlich, um die Vielzahl an gesammelten Daten effizient zu verarbeiten und zu analysieren. Die kontinuierliche Wartung und Aktualisierung der Hardware- und Software-Komponenten ist unabdingbar, um die langfristige Funktionsfähigkeit des Systems zu gewährleisten.

Evaluierung der Konzeption

Die Evaluierung erfolgt durch qualitative und quantitative Methoden. Qualitativ werden Polizeibeamte zur Praktikabilität des Systems befragt, wobei Feedbacks von Trainern und Verhaltenspsychologen zur

pädagogischen Wirksamkeit ebenfalls Berücksichtigung finden sollen. Quantitativ werden Leistungsmetriken wie Reaktionszeiten und Entscheidungsgenauigkeit des Systems analysiert. Die Genauigkeit der KI bei der Erkennung von Stress und emotionalen Zuständen wird durch Metriken wie Präzision und Recall gemessen und soll stets validiert werden, um die Zuverlässigkeit des Systems sicherzustellen.

Diskussion

Die in der Konzeption entwickelte Integration von VR und KI bietet ein neues theoretisches Modell zur Verbesserung der Entscheidungsfindung von Polizeibeamten, das Echtzeitfeedback liefert und gleichzeitig den emotionalen Zustand und das Stresslevel der Trainees analysiert. Im Vergleich zu den drei vorgestellten Arbeiten liefert diese Konzeption einige signifikante Verbesserungen und innovative Ansätze. Diese werden im Folgenden diskutiert. Eine Neuerung, die aus diesem Beitrag resultiert, ist eine umfassendere Integration von Echtzeitfeedback und Emotionserkennung. In den Arbeiten wurde bereits die Bedeutung von VR und KI für Trainings-szenarien hervorgehoben, insbesondere bei der Polizeiausbildung (Caserman et al., 2023). Allerdings integrierten diese Studien die Erkennung und Analyse des emotionalen Zustands der Trainees nicht vollständig in das Training. Die durch den Autor dieses Beitrags entwickelte Konzeption geht hier einen Schritt weiter, indem sie den emotionalen Zustand der Polizeibeamten durch Mimik- und Gestikanalyse sowie durch Aufzeichnung der Vitalfunktionen überwacht. Dadurch können sowohl die kognitiven als auch die emotionalen Reaktionen der Trainees erfasst und in das Feedback einbezogen werden. Dies ist besonders relevant, da Stress und Emotionen nachweislich einen starken Einfluss auf die Entscheidungsfindung haben. Ein weiterer Unterscheidungspunkt ist die personalisierbare Anpassung der Trainingsszenarien, welche auf den emotionalen und stressbezogenen Daten der Trainees basiert. Während Caserman et al. bereits Echtzeitfeedback in Trainingssystemen verwendet haben, wird hier das Training an die individuelle emotionale Belastbarkeit und Stressverarbeitung des Trainees angepasst. Dadurch wird das Training flexibler und effektiver, da es nicht nur auf rein kognitive

Leistungen ausgerichtet ist. Im Vergleich zur Arbeit von Jekauc et al. (2024), die sich auf die Erkennung von emotionalen Zuständen im Sport beschränkt, wird diese Konzeption um die detailliertere KI-Analyse emotionaler Punkte sowie den Anwendungsbereich der Polizeiausbildung und anderer stressintensiver Berufe ergänzt. Die KI-gestützte Analyse von Mimik, Gestik und physiologischen Daten bietet eine tiefere Einsicht in die emotionalen Zustände der Trainees. Dies ermöglicht eine detailliertere und differenziertere Analyse der individuellen Leistungsfähigkeit unter Stress, was bei den bisherigen Arbeiten nur rudimentär untersucht wurde.

Im Vergleich zu den bisherigen Erkenntnissen zeigt der vorliegende Beitrag einen ganzheitlichen Ansatz zur Verbesserung der Entscheidungsfindung und Stressbewältigung, der sowohl kognitive als auch emotionale Faktoren berücksichtigt. Dieser Ansatz führt zu einer umfassenden Betrachtung der Trainee-Performance, da nicht nur das Verhalten und die Leistung in stressigen Situationen analysiert wird, sondern auch der emotionale Zustand.

Ein weiterer Vorteil der Konzeption ist die höhere Flexibilität und individuelle Anpassung der Szenarien. Während Caserman et al. und Jekauc et al. hauptsächlich statische Szenarien oder einfache Feedback-Mechanismen verwenden, ermöglicht die vorliegende Konzeption eine dynamische Anpassung des Trainings an die individuellen Bedürfnisse der Trainees. Dies fördert ein maßgeschneidertes Training, was in den tradierten Trainingsmethoden bislang nur limitiert möglich war.

Neben einigen neuen Erkenntnissen und Fortschritten gibt es aber auch Einschränkungen der Konzeption. Zwei wesentliche Beschränkungen sind die technologische Komplexität und die hohen Kosten. Die Implementierung einer VR-Plattform, die sowohl hochauflösende Sensoren für Mimik und Gestik als auch fortschrittliche KI-Algorithmen zur Analyse von emotionalen Zuständen verwendet, ist technologisch anspruchsvoll. Die Integration von Motion-Capture-Suits und Gesichtserkennungstechnologien erfordert erhebliche finanzielle Investitionen, was die Verbreitung und Nutzung des Sys-

tems in der Praxis einschränken könnte. Zwei weitere sehr entscheidende Nachteile sind die Akzeptanz und ethische Fragen sowie die Zuverlässigkeit der emotionalen Analyse.

Die Erfassung von Emotionen und Stress durch Gesichtserkennung und andere biometrische Daten könnte Bedenken hinsichtlich der Privatsphäre und des Datenschutzes aufwerfen. Polizeibeamte könnten sich durch die kontinuierliche Überwachung und Analyse ihrer emotionalen Zustände unwohl fühlen, was die Akzeptanz des Systems beeinträchtigen könnte. Um diese Bedenken zu adressieren, sind strenge Datenschutzrichtlinien erforderlich, die sicherstellen, dass die Daten anonymisiert und nur für Trainingszwecke verwendet werden. Dies könnte aber dazu führen, dass die Trainingssätze der Trainees nicht zugeordnet werden können und somit auch keine stetige Verbesserung stattfinden kann.

KI-Modelle zur Erkennung von Emotionen und Stressleveln sind in der Theorie vielversprechend, jedoch gibt es Einschränkungen hinsichtlich der Genauigkeit dieser Analysen in realen Szenarien. Emotionale Reaktionen können von Person zu Person stark variieren, wodurch schnell Fehler passieren können. Eine präzise und zuverlässige Analyse erfordert fortlaufende Modellanpassungen und umfangreiche Trainingsdaten, um die Genauigkeit der KI zu gewährleisten.

Schlussfolgerungen

Die vorliegende Konzeption zur Integration von VR und KI in Trainingssysteme für Polizeibeamte zeigt ein hohes Potenzial, die Qualität und Effektivität der Ausbildung signifikant zu verbessern. Durch die Kombination von VR-Simulationen mit KI-gesteuertem Echtzeitfeedback und der Analyse emotionaler Zustände wird ein Ansatz vorgestellt, der nicht nur die technische Leistungsfähigkeit von Trainingsmethoden erweitert, sondern auch die psychologische Dimension tiefgreifend berücksichtigt. Die Konzeption nutzt die Stärken beider Technologien, um ein dynamisches und adaptives Trainingsumfeld zu schaffen, wodurch Polizeibeamte ihre Fähigkeiten unter kontrollierten Bedingungen verbessern können. Die Einbindung

von KI in das System erlaubt eine detaillierte Analyse der Traineeleistungen, indem physiologische und emotionale Reaktionen in Echtzeit erfasst und ausgewertet werden. Dies führt zu einem maßgeschneiderten Feedback, das direkt in das Training einfließen und die Lernkurve beschleunigen kann.

Trotz der vielversprechenden Ansätze gibt es jedoch auch Herausforderungen, die im weiteren Entwicklungsprozess berücksichtigt werden müssen. Die technische Komplexität der vorgeschlagenen Lösung stellt eine erhebliche Hürde dar. Die Implementierung erfordert nicht nur fortschrittliche Hardware-Komponenten, sondern auch eine leistungsfähige Software-Infrastruktur, die in der Lage ist, die große Menge an Daten in Echtzeit zu verarbeiten. Insbesondere die Echtzeitanalyse der physiologischen und emotionalen Daten erfordert hochentwickelte Algorithmen und eine robuste Software-Architektur, um Verzögerungen zu vermeiden.

Ein weiterer kritischer Punkt ist die Abhängigkeit von einer umfangreichen und qualitativ hochwertigen Datenbasis. Die Effektivität der KI-basierten Analysen hängt stark von der Verfügbarkeit und Diversität der zugrunde liegenden Daten ab. Des Weiteren muss erforscht werden, ob die derzeit verfügbaren Datenquellen, wie Bodycam-Aufnahmen, Videosequenzen aus dem OpenWeb und traditionelle Trainingsmethoden, ausreichen, um robuste und generalisierbare KI-Modelle entwickeln zu können.

Zusammenfassend lässt sich sagen, dass die Konzeption ein innovatives und vielversprechendes Modell für die Polizeiausbildung darstellt, das VR und KI effektiv kombiniert. Es bietet das Potenzial, die Qualität und Effizienz des Trainings signifikant zu verbessern, erfordert jedoch eine sorgfältige Planung und Umsetzung, um die technischen Herausforderungen zu meistern und sicherzustellen. Die erfolgreiche Implementierung dieses Modells könnte einen wichtigen Schritt in der Modernisierung der Polizeiausbildung darstellen und einen positiven Beitrag zur Vorbereitung der Beamten auf reale Einsatzsituationen leisten.

Literaturverzeichnis

Ahir, K., Govani, K., Gajera, R. et al. (2020): Zurückgezogener Artikel: Application on Virtual Reality for Enhanced Education Learning, Military Training and Sports. *Augment Hum Res* 5, 7. doi.org/10.1007/s41133-019-0025-2.

Anonym (2021): Künstliche Intelligenz. Ethische Herausforderungen durch die Digitalisierung. GRIN Verlag.

Bekker, A. (2018) Umfassender Leitfaden für Big Data Analytics in Echtzeit. scnsoft.de/blog/ein-leitfaden-zu-big-data-analysen-in-echtzeit (Zugriff: 12. September 2024).

Berger, S. und Moser, U. (2020): Adaptives Lernen und Testen, *Journal für LehrerInnenbildung* jlb 01-2020 Digitalisierung, 42-52. doi.org/10.35468/jlb-01-2020_03.

Bioni, D., Achtziger, A. und Gentsch, G. (2010): Psychologisch basiertes Training in der Polizeiarbeit. *Polizei und Wissenschaft*, 4, 16–29

Bock, A. (2023) Deeskalative Kommunikation lernen: Polizei-Verhaltenstraining mittels künstlicher Intelligenz. k3vr.de/wp-content/uploads/2023/05/Pressemitteilung-Verbund.pdf (Zugriff: 28. August 2024) S. 1-6.

Caserman, P., Zhang, H., Zinnäcker, J. und Göbel, S. (2019): Development of a Directed Teleport Function for Immersive Training in Virtual Reality, 11th International Conference on Virtual Worlds and Games for Serious Applications (VS-Games). Wien: IEEE, S. 1-8. doi.org/10.1109/VS-Games.2019.8864599.

Caserman, P., Müller, N. P., Göbel, T., Tonecker, P., Yildirim, S., Kecke, A., Purdach, D. und Göbel, S. (2023) Virtual Reality Simulator for Police Training with AI-Supported Cover Detection. In: Haahr, M., Rojas-Salazar, A., Göbel, S. (Hg.) *Serious Games. JCSG 2023. Lecture Notes in Computer Science*, vol 14309. Springer, Cham. doi.org/10.1007/978-3-031-44751-8_13

Deutscher Ethikrat (2023) Mensch und Maschine – Herausforderungen durch Künstliche Intelligenz. Available at: ethikrat.org/fileadmin/Publikationen/Stellungnahmen/deutsch/stellungnahme-mensch-und-maschine-kurzfassung.pdf (Zugriff: 13. August 2024).

Eppel, H. (2007): Stress als Risiko und Chance: Grundlagen von Belastung, Bewältigung und Ressourcen. Kohlhammer Verlag.

Funke, J. (2024) Mit KI bessere Entscheidungen treffen: Wie Künstliche Intelligenz die Entscheidungsfindung optimiert. it-p.de/blog/entscheidungen-ki-optimierung (Zugriff: 9. September 2024).

Grottko, J. (2021): Der Zusammenhang zwischen Stress, Coping und Empathie. Bachelorthesis an der University of Applied Sciences Europe – Berlin, Hamburg.

Hartmann, C. und Bannert, M. (2022): Lernen in virtuellen Räumen: Konzeptuelle Grundlagen und Implikationen für künftige Forschung, *Medien Pädagogik: Zeitschrift für Theorie und Praxis der Medienbildung*, Nr. 47, 373-391. doi.org/10.21240/mpaed/47/2022.04.18.X.

Heil, V. und Bechold, M. (2022) Mentale Stärke von Polizeibeamten*innen im Einsatz und im Polizeitraining. In: Staller, Mario, Koerner, Swen (Hg.) *Handbuch polizeiliches Einsatztraining*. Springer Gabler, 379-388.

Heinrich, C. et al. (2011) Wege aus dem Wirrwarr der Möglichkeiten, *Die Zeit*, 11 Oktober 2011. Available at: zeit.de/zeit-wissen/2011/06/Entscheidungen/seite-2 (Zugriff: 2. September 2024).

Ionos (2023) NPC: Was genau ist ein Non-Player-Character? ionos.de/digitalguide/online-marketing/social-media/npc (Zugriff: 2. September 2024).

Jekauc, D., Burkart, D., Fritsch, J., Hesenius, M., Meyer, O., Sarfraz, S. und Stiefelhagen, R. (2024): Recognizing affective states from the expressive behavior of tennis players using convolutional neural networks, Knowledge-Based Systems, Vol. 295. doi.org/10.1016/j.knsys.2024.111856.

Laude, T., Reinhardt, C. und Bomert, C. (2022): Einsatz von künstlicher Intelligenz, Data Science und Big Data: Anwendungsbeispiele zur Bewältigung von Massendaten in der niedersächsischen Polizei, in Wehe, D., Siller, H. (Hrsg.) Handbuch Polizeimanagement: Polizeipolitik – Polizeiwissenschaft – Polizeipraxis. Wiesbaden: Springer Fachmedien, S. 1509-1530.

Marler, T. et al. (2020): Effective Game-Based Training for Police Officer Decision-Making: Linking Missions, Skills, and Virtual Content; RAND Corporation; Santa Monica, CA, University of Southern California Institute for Creative Technologies; Playa Vista, CA, Spaces Inc.; Irvine, CA.

Mathworks (2024) Was ist ein Convolutional Neural Network? Available at: de.mathworks.com/discovery/convolutional-neural-network.html (Zugriff: 29. Oktober 2024)

Pallavicini, F., Toniuzzi, N., Argenton, L., Aceti, L. und Mantovani, F. (2015): Developing effective Virtual Reality training for military forces and emergency operators: From technology to human factors. 14th International Conference on Modeling and Applied Simulation, MAS 2015 (S. 206-210). Dime University of Genoa.

Pallavicini, F., Argenton L, Toniuzzi, N., Aceti, L. und Mantovani, F. (2016): Virtual reality applications for stress management training in the military. *Aerosp Med Hum Perform.* 87(12): 1021-1030.

Privenau, R. (2012): Neokognitron und Hopfield Netz als künstliche neuronale Netze zur Mustererkennung: Theorie, computergestützte Simulation und Anwendungen. Diplomica Verlag.

Schwegmann, C. (2023) Methoden | Literaturarbeit / Systematische Literaturanalyse, Schreibmentoren. schreibmentoren.de/allgemein/systematische-literaturanalyse/ (Zugriff: 2. September 2024).

Seibold, S. und Horn, A. (2021) Emotion und Fehlentscheidung: Wie Menschen auch unter Stress klug entscheiden. Springer Berlin/Heidelberg.

Einsatz von Künstlicher Intelligenz bei der Polizei und deren gesellschaftliche Akzeptanz

Carolina Döring

Künstliche Intelligenz (KI) hat sich in den vergangenen Jahren enorm entwickelt und beeinflusst zunehmend verschiedene Bereiche unserer Gesellschaft. Diese Digitalisierungs-Technologie hat das Potenzial, viele Aspekte unseres Lebens zu verändern und mitzugestalten (Stürz et al., 2020, S. 8). Vor allem seit den 2010er-Jahren ist ein stetiger Aufschwung der KI-Forschung zu verzeichnen, der mit einer weiten Verbreitung dieser Technologie in diverse gesellschaftliche Bereiche einhergeht. Diese Entwicklung führte bisher nicht nur zu technischen Neuerungen, sondern auch zu lebhaften Diskussionen über die sozialen Auswirkungen und die Akzeptanz von KI-Systemen. Die Geschichte der KI ist geprägt von Zyklen des Aufschwungs und der Ernüchterung (Hirsch-Kreinsen und Krokowski, 2023, S. 1). Trotz dieser wechselhaften Vergangenheit hat die jüngste Entwicklung, insbesondere die Einführung von großen Sprachmodellen, wie ChatGPT, zu einer bis zu diesem Zeitpunkt nie dagewesenen öffentlichen Aufmerksamkeit und Diskussion geführt. ChatGPT stellt hier einen Wendepunkt in der KI-unterstützten Anwendung dar (Block, 2024). Die Fähigkeit, menschenähnliche Texte zu erstellen und auf entsprechende Anfragen zu reagieren, ist ein Fortschritt technologischer Anwendungen. Zudem führt es zu einer grundlegenden Veränderung, wie Menschen mit Maschinen agieren. Die Einführung von ChatGPT hat jedoch auch zu einer erhöhten Skepsis gegenüber KI geführt. Gleichzeitig erhofft man sich für den Berufsalltag eine große Entlastung durch KI-Systeme. Diese ambivalente Haltung spiegelt die komplexe Natur der gesellschaftlichen Akzeptanz von KI wider (Christen, 2024). Dies zeigt, dass die gesellschaftliche Akzeptanz stark kontextabhängig ist und von Faktoren wie der Tragweite der Entscheidungen und dem Grad der menschlichen Kontrolle abhängt. Die Herausforderungen und Grenzen der KI-Entwicklung dürfen dabei nicht außer Acht gelassen werden. Trotz beeindruckender Fortschritte bleiben grundlegende Probleme, wie fehlendes Kontextverständnis, mangelnde Transparenz und Erklärbarkeit sowie Datenkomplexität, bestehen. Diese Aspekte beeinflussen nicht

nur die technische Entwicklung, sondern auch die gesellschaftliche Wahrnehmung und Akzeptanz von KI-Systemen (Hirsch-Kreinsen und Krokowski, 2023, S. 478). Dies hat weitreichende Auswirkungen auf unterschiedliche Bereiche unserer Gesellschaft.

Hierzu gehört auch der Bereich der Polizeiarbeit. Der Einsatz von KI-Systemen ermöglicht die Steigerung von Effizienz und Effektivität innerhalb der Polizeibehörden. Daneben müssen jedoch auch Fragestellungen zu den Themen Datenschutz, Rechtsstaatlichkeit und Grundrechte beachtet werden. Hierbei ist die gesellschaftliche Akzeptanz dieser Technologien in der Strafverfolgung und Gefahrenabwehr für ihre erfolgreiche Implementierung und nachhaltige Nutzung entscheidend. Dieser Beitrag untersucht die Einflussfaktoren auf die öffentliche Wahrnehmung von Künstlicher Intelligenz in der Polizeiarbeit. Er identifiziert und strukturiert ethisch relevante Zusammenhänge und beleuchtet mögliche Spannungsfelder. Darüber hinaus werden Strategien zur Steigerung der Akzeptanz erörtert und die Herausforderungen im Spannungsfeld zwischen KI-basierter Entwicklung und dem Schutz der informationellen Selbstbestimmung analysiert. Ziel ist es, einen Überblick über die Chancen und Risiken von KI-Systemen bei der Polizei zu geben und ihre Auswirkungen auf die Gesellschaft zu bewerten.

Hintergrund

Der Einsatz von KI in der Polizeiarbeit stellt ein komplexes Thema dar. Dieses bringt Chancen und Risiken mit sich. Ziel soll sein, KI effektiv zur Strafverfolgung und Präventionsarbeit einzusetzen, ohne dabei Grundrechte und ethische Aspekte zu verletzen. Hierbei bedarf es einer sorgfältigen Abwägung zwischen Sicherheitsinteressen und dem Schutz der Privatsphäre. Klare gesetzliche Regelungen sowie Transparenz, stetige Überprüfung und ein öffentlicher Dialog sind entscheidend, um die gesellschaftliche Akzeptanz zu gewährleisten und zu fördern sowie mögliche negative Auswirkungen zu minimieren. Der Einsatz von KI bei der Polizei soll ein unterstützendes Werkzeug sein, das die menschliche Expertise ergänzt, aber nicht ersetzt (Rüdiger und Bayerl, 2023). Länder wie Großbritannien

und die USA nutzen KI bei der Polizei mittlerweile standardmäßig. In Deutschland hingegen wird sie bisher nur teilweise in den Bereichen der Strafverfolgung und der Gefahrenabwehr eingesetzt (Ursuleac, 2023). Der Einsatz von KI hat gesellschaftliche Auswirkungen – „auf das Selbstverständnis des Menschen (Herrschaft über Maschinen, Autonomie), die soziale Struktur (soziales Handeln und Rollen), den Wert und die Gestaltung der Arbeit (strukturell und systematisch) sowie auf die politische Willens- und Meinungsbildung“ (Samsami, 2023). Die Einigung hinsichtlich grundlegender ethischer Standards ist ein Diskussionsaspekt, der nun bereits seit Jahrzehnten geführt wird (Samsami, 2023).

Die zentrale ethische Herausforderung liegt darin, KI-basierte Systeme zu entwickeln, die zeitgleich wertorientiert sind und mit dem menschlichen Leben im Einklang stehen. Hierdurch können eine Verbesserung des menschlichen Lebens, die Wahrung von Grundrechten sowie die Erweiterung von Handlungsoptionen gewährleistet werden (Samsami, 2023).

Material und Methode

Zur Erörterung der Forschungsfrage hinsichtlich der gesellschaftlichen Akzeptanz zum Einsatz von KI bei der Polizei wird in diesem Beitrag die wissenschaftliche Arbeitsmethodik „MEESTAR“ (Modell zur ethischen Evaluation sozio-technischer Arrangements) verwendet. Es handelt sich hierbei um eine methodische Anwendung, die bisher u. a. bei der ethischen Bewertung von technologischen Innovationen, insbesondere im Bereich der Pflege und Gesundheitsversorgung, verwendet wurde bzw. wird. Diese Methode dient dazu, ethische Implikationen technologischer Entwicklungen systematisch zu analysieren und zu bewerten. Bei dieser Methodik werden grundsätzlich insgesamt sieben ethische Dimensionen (Fürsorge, Selbstbestimmung, Sicherheit, Gerechtigkeit, Privatheit, Teilhabe und Selbstverständnis) betrachtet und jeweils auf vier Ebenen (individuelle, organisationale, gesellschaftliche und rechtliche Ebene) analysiert. Die abschließende ethische Bewertung erfolgt in vier Stufen (völlig unbedenklich, leicht bedenklich, bedenklich und sehr bedenklich) (Manzeschke et al., 2015, S. 14 ff.). Aufgrund des

begrenzten Umfangs dieses Beitrags ist es nicht möglich, alle genannten ethischen Dimensionen zu der Thematik zu erörtern und darzustellen. Stattdessen wird sich der vorliegende Beitrag auf die Elemente „Sicherheit“ und „Selbstbestimmung“ konzentrieren.

Sicherheit

Der Aspekt „Sicherheit“ beim Einsatz von KI soll insbesondere den Bereich der Privatsphäre schützen und Diskriminierung vermeiden. Im Zuge einer Abstimmung des Europäischen Parlaments aus dem Jahr 2021 wurde seitens der Abgeordneten im Kontext des Einsatzes von KI in der Strafverfolgung auf das Risiko algorithmischer Voreingenommenheit hingewiesen. Hier bedarf es aus Sicht des Parlaments weiterhin der Notwendigkeit menschlicher Aufsicht und rechtlicher Kontrollen, um diskriminierende Handlungen durch den Einsatz von KI, insbesondere im Bereich der Strafverfolgung, zu verhindern (Ojamo et al., 2021).

Individuelle Ebene

Der Einsatz von KI-Technologien wirft etliche Fragen auf, insbesondere hinsichtlich der Genauigkeit und der potenziellen Fehlerhaftigkeit von Vorhersagen, die durch KI-Systeme generiert werden. Diese sind eng verbunden mit der Überlegung, ob solche Vorhersagen für verschiedene Personengruppen gleich zuverlässig sind. Es besteht die ernsthafte Gefahr, dass Menschen aufgrund ihrer Herkunft, ihres Wohnorts oder ihrer persönlichen Vorgeschichte diskriminiert werden. Ob tatsächlich eine ungerechtfertigte Ungleichbehandlung vorliegt, hängt entscheidend von den genutzten Parametern ab, die im Rahmen der Prognoseentscheidung gewichtet werden, sowie von den zur Verfügung gestellten Daten und ihren spezifischen Charakteristika (Deutscher Ethikrat, 2023, S. 323).

Organisationale Ebene/Gesellschaftliche Ebene

Seitens des Europäischen Parlaments wird darauf verwiesen, dass durch Algorithmen gesteuerte Identifizierungstechnologien unverhältnismäßig viele falsche Identifizierungsprozesse durchführen.

Dies führt dazu, dass Personen nicht richtig identifiziert werden und mutmaßlich aufgrund von Rassismus (beispielsweise Angehörige bestimmter ethnischer Gemeinschaften) benachteiligt werden. Dies ist insbesondere bedenklich, da KI-Technologien im Rahmen der Strafverfolgung eingesetzt werden (Ojamo et al., 2021). Diese falschen Identifizierungsprozesse treten im Output von KI-Systemen auf und werden als „Technical Bias“ oder „Algorithmic Bias“ bezeichnet. Ein besonders viel diskutiertes Beispiel für solche Verzerrungen ist die Software COMPAS, die in den USA verwendet wird, um Risikoprofile für ehemalige straffällige Personen zu erstellen. Hierbei konnte nachgewiesen werden, dass die Prognosen, die durch diese Software erstellt wurden, diskriminierende Tendenzen aufwiesen. Insbesondere erhielten dunkelhäutige Menschen deutlich häufiger eine fälschlicherweise negativere Prognose, während hellhäutige Menschen im Gegensatz dazu oft fälschlicherweise positivere Prognosen erhielten. Diese Ungleichheit in den Vorhersagen wirft ernsthafte Fragen zur Fairness und Gerechtigkeit der verwendeten Algorithmen auf. Häufig ursächlich für solche diskriminierenden Systeme sind Verzerrungen in den Trainingsdaten, die zur Entwicklung der Algorithmen verwendet werden (Deutscher Ethikrat, 2023, S. 303).

Rechtliche Ebene

Die Nutzung von KI im polizeilichen Kontext wirft hinsichtlich des Diskriminierungsverbots wichtige rechtliche Fragen auf. Hier in Deutschland ist das Diskriminierungsverbot im Art. 3 Abs. 3 Grundgesetz (GG) geregelt. Eine entsprechende Konkretisierung hierzu findet man im Allgemeinen Gleichbehandlungsgesetz (AGG). Daneben gibt es weitere datenschutzrechtliche und polizeikonforme – sowohl auf länder-, bundes-, und europaweiter Ebene – Vorschriften und Regelungen, die im Kontext des Diskriminierungsverbots zu beachten sind. Der Einsatz von KI bei der Polizei bedarf daher einer sorgfältigen Prüfung im jeweiligen Einzelfall. Dies ist notwendig, um die Einhaltung der Grundrechte zu gewährleisten und Diskriminierung zu verhindern. Es ist eine stetige und kontinuierliche Herausforderung, technologische Möglichkeiten mit rechtlichen und ethischen Anforderungen zu vereinen.

Bewertung der Dimension „Sicherheit“

Obwohl Fehler auch bei menschlichen Urteilsentscheidungen unvermeidlich sind, birgt die Unterstützung von Entscheidungen durch Software ein mutmaßlich noch höheres Risiko. Hier können Fehler und Verzerrungen systembedingt eine besonders weitreichende Wirkung entfalten. Dies ist besonders kritisch, wenn es um polizeiliche Maßnahmen geht. In solchen Fällen können beide Arten von Fehlern schwerwiegende Folgen haben – sowohl, wenn fälschlicherweise polizeiliche Maßnahmen gegen unschuldige Personen ergriffen werden, als auch, wenn ein notwendiger polizeilicher Zugriff nicht erfolgt. Aus gesellschaftlicher Sicht muss somit entschieden werden, in welchem Umfang solche Risiken akzeptabel sind oder auch nicht. Es ist auch zu klären, ob ein Unterschied vorliegt, ob der Fehler auf technologische KI-basierte Mängel zurückzuführen ist oder auf menschliches Versagen (Deutscher Ethikrat, 2023, S. 323 ff.). Daher wird auf Grundlage der zuvor genannten Aspekte die Dimension „Sicherheit“ aus ethischer Sicht mit der Stufe III bewertet. Diese Stufe wird mit der Begrifflichkeit „bedenklich“ klassifiziert und besagt, dass die Anwendung äußerst sensibel – unter stetiger Aufmerksamkeit – erfolgen kann (Weber, 2019, S. 4).

Selbstbestimmung

Der Begriff „Selbstbestimmung“ bedeutet, dass jeder Mensch das Recht hat, selbst zu entscheiden, wie er sein Leben gestalten möchte. Diese Freiheit, die eigene Lebensweise zu wählen und zu bestimmen, ist ein fundamentales Menschenrecht. Dieses wird nicht nur von der Gesellschaft anerkannt, sondern ist auch durch unsere Verfassung umfassend geschützt (Schneider und Toyka-Seid, 2024). Hierzu gibt es bereits seit einigen Jahren mehrere repräsentative Bevölkerungsumfragen, die sich mit der Thematik des Einsatzes von KI und deren gesellschaftlicher Akzeptanz befassen. Im Gesamtergebnis zeigen hier sämtliche Studienerkenntnisse gleichartige Erkenntnisse auf. Diese Umfragen wurden u. a. durch die Bertelsmann Stiftung (Overdiek und Petersen, 2022, S. 1), das Bayerische Forschungsinstitut für Digitale Transformation (Stürz et al., 2020, S. 1) sowie die PricewaterhouseCoopers International (PwC) durchgeführt, analysiert und

ausgewertet (Zink et al., 2022, S. 1). Insbesondere PwC hat hier im Zuge zweier Studien die Akzeptanz der Gesellschaft auf den Einsatz KI-basierter Technologien seitens der Polizei erhoben (Zink et al., 2023, S. 2). Hierzu wurden neben einer im Jahr 2022 veröffentlichten Bevölkerungsstudie „Vertrauen, Präsenz und digitale Kompetenz – Wie sieht die Öffentlichkeit ihre Polizei?“ (Zink et al., 2022, S. 1) in einer weiteren Studie auch Sicherheitsexpertinnen und Sicherheitsexperten hierzu befragt (Zink et al., 2023, S. 2).

Individuelle Ebene

Auf der individuellen Ebene geht es grundsätzlich darum, ein selbstbestimmtes und unabhängiges Leben zu führen, frei von Einschränkungen (Weber, 2019, S. 8). Im Rahmen der oben genannten, durch PwC im Jahr 2022 durchgeführten Studie wurde untersucht, in welchem Maße die Gesellschaft das Gefühl hat, dass ihr Freiheitsgefühl durch den Einsatz von Technologie seitens der Polizei beeinträchtigt wird (Zink et al., 2022, S. 27).



Abbildung 1: Einfluss von Technologien auf die Freiheit der Gesellschaft aus Sicht der Bürgerinnen und Bürger (Zink et al., 2022, S. 27)

Demnach – wie in Abbildung 1 dargestellt – unterstützen 71 % der Befragten die Einführung von elektronischen Fußfesseln für besonders gefährliche entlassene Straftäterinnen und Straftäter. Zudem

befürworten sie die Verwendung von Bodycams, die an Polizeiuniformen angebracht werden. 70 % der Befragten sind für die Entwicklung einer Katastrophen-Warn-App, die im Katastrophenfall schnelle Informationen bereitstellt. 60 % sprechen sich für den Einsatz von Wärmebildkameras aus, während 53 % die Erfassung biometrischer Daten unterstützen. Im Gegensatz dazu zeigt sich bei anderen zur Abstimmung gestellten Instrumenten für die Polizeiarbeit eine Minderheit. So befürworten lediglich 30 % der befragten Personen Online-Durchsuchungen. Nur 24 % stimmen der Vorratsdatenspeicherung ohne konkrete Verdachtsmomente zu (Zink et al., 2022, S. 27).

Organisationale Ebene/Gesellschaftliche Ebene

Selbstbestimmung auf organisationaler bzw. gesellschaftlicher Ebene bedeutet, dass personale Unterstützung durch den Einsatz moderner Technik erheblich reduziert oder sogar vollständig ersetzt werden kann (Weber, 2019, S. 8). Wie bereits dargestellt, wurde eine eigenständige Studie seitens PwC durchgeführt, die den Einfluss von KI-Technologien auf die Freiheit der Gesellschaft aus Sicht von Sicherheitsmitarbeiterinnen und Sicherheitsmitarbeitern beleuchtet (Zink et al., 2023, S. 32).

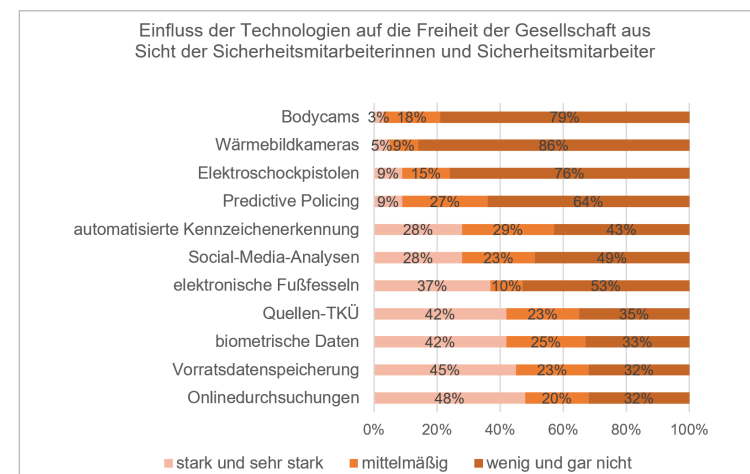


Abbildung 2: Einfluss von Technologien auf die Freiheit der Gesellschaft aus Sicht der Sicherheitsmitarbeiterinnen und Sicherheitsmitarbeiter (Zink et al., 2023, S. 32)

Im Zuge der Auswertung und des damit verbundenen Vergleichs der Abbildungen 1 und 2 ist erkennbar, dass es bei der Thematik „Freiheitsbeschränkung durch KI“ eine Übereinstimmung zwischen der individuellen und der organisationalen/gesellschaftlichen Ebene gibt. Im Wesentlichen sind sich beide Gruppen einig, dass die größten Freiheitsbeschränkungen für die Gesellschaft durch Technologien verursacht werden, die personenbezogene Daten sammeln und gebrauchen (Zink et al., 2023, S. 32). Im Zusammenhang mit dem Einsatz elektronischer Fußfesseln sind – wie in Abbildung 2 dargestellt – 37 % der Expertinnen und Experten der Meinung, dass dies eine starke oder sogar sehr starke Beeinträchtigung der individuellen Freiheit darstellt. Im Gegensatz dazu empfinden nur 22 % der Bürgerinnen und Bürger – dargestellt in Abbildung 1 – diese Einschränkung als so gravierend (Zink et al., 2023, S. 32).

Rechtliche Ebene

Das Recht auf Selbstbestimmung ist ein elementares verfassungsrechtlich geschütztes Menschenrecht. Es ergibt sich aus dem allgemeinen Persönlichkeitsrecht gemäß Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG und umfasst die Aspekte „Informationelle Selbstbestimmung“, „Recht auf Privatsphäre“ und „Schutz personenbezogener Daten“. Im Zuge des Einsatzes von KI im polizeilichen Kontext können hinsichtlich des Rechts auf Selbstbestimmung Konflikte mit der Datensammlung und -verarbeitung, dem automatisierten Datenabgleich sowie der Überwachung und Vorhersage auftreten. Der Einsatz von KI muss stets verhältnismäßig sein und darf nicht über das zur Gefahrenabwehr notwendige Maß hinausgehen. Daher bedarf es einer im jeweiligen Einzelfall erforderlichen sorgfältigen Abwägung zwischen dem Recht auf Selbstbestimmung und den Interessen der öffentlichen Sicherheit.

Bewertung der Dimension „Selbstbestimmung“

Bei Betrachtung der beiden durch PwC durchgeführten Studien ist erkennbar, dass die Akzeptanz hinsichtlich des Einsatzes von KI bei der Polizei seitens der Sicherheitsmitarbeiterinnen und Sicherheitsmitarbeiter grundsätzlich größer ist als die der Bürgerinnen und Bürger.

Es ist erkennbar, dass im Zuge anlassunabhängiger Verwendung von KI – beispielsweise im Kontext abstrakter Präventionstätigkeit – die Gesellschaft äußerst sensibel und mit kaum vorhandener Akzeptanz reagiert (Zink et al., 2023, S. 18). Aus hiesiger Sicht und unter Berücksichtigung der genannten Aspekte wird die Dimension „Selbstbestimmung“ aus ethischer Sicht ebenfalls mit der Stufe III bewertet. Eine entsprechende Anwendung bedarf aufgrund der Klassifizierungskategorie „bedenklich“ einer sensiblen Anwendung unter stetiger Aufmerksamkeit (Weber, 2019, S. 4). Diese Technologien, die oft in unserem Alltag integriert sind, können das individuelle Verhalten und die Entscheidungsfreiheit stark beeinflussen. Die Sorge besteht mutmaßlich insbesondere darin, dass durch die missbräuchliche Verwendung dieser Daten die Privatsphäre der Menschen gefährdet wird, was zu einer Einschränkung der persönlichen Freiheit führen kann.

Ergebnisse

Das Verständnis für KI-Technologien und deren vielfältige Anwendungen spielt eine entscheidende Rolle für die gesellschaftliche Akzeptanz. Viele Befragten zeigen Unsicherheiten, die sowohl gesellschaftliche als auch technische Aspekte von KI betreffen. Diese Unsicherheiten können die Bereitschaft zur Nutzung und Integration von KI im Alltag beeinflussen und zu Skepsis und Misstrauen gegenüber dem Einsatz von KI in der Polizeiarbeit führen (Stürz et al., 2020, S. 8). Um Vertrauen und somit eine entsprechende Akzeptanz in diese Technologien zu erhöhen, ist es wichtig, das öffentliche Verständnis für KI-Technologien zu fördern und aufzuklären, wie sie effektiv und verantwortungsvoll eingesetzt werden können. Derzeit wird der Einsatz von KI-Technologien und deren Akzeptanz in der Gesellschaft als kontrovers wahrgenommen. Ziel ist es, dass KI als Chance gesehen wird. Hierzu bedarf es intensiver gesellschaftlicher Dialoge, Gestaltungsmöglichkeiten und partizipativer Verfahren. Neben kultureller, rechtlicher und institutioneller Aspekte ist es entscheidend, KI auch in ethischer Hinsicht in die Gesellschaft zu integrieren (Die Bundesregierung, 2018, S. 45). Im Zuge von forschungsbasierten Erkenntnissen, hier u. a. durch das Bayerische Forschungsinstitut für Digitale Transformation, die Bertelsmann Stiftung und PwC, wur-

de festgestellt, dass ein Großteil der deutschen Bevölkerung wenig Kenntnisse über den KI-basierten Einsatz hat. Hierzu wurden in digitaler Form deutschlandweit kurze repräsentative Befragungen von Internetnutzerinnen und Internetnutzern durchgeführt. Im Gesamtergebnis wurde identifiziert, dass mehr Befragte die Verwendung von KI als Chance sehen – und nicht als Gefahr. Die Ergebnisse zeigen insbesondere, dass es wichtig ist, eine Strategie zu Wissensvermittlung und entsprechenden Weiterbildungsmaßnahmen hinsichtlich des Einsatzes von KI zu haben. Demnach ist es Aufgabe der Politik, hier einen Schwerpunkt zu setzen. Um die Akzeptanz des Einsatzes von KI zu steigern und die Gesellschaft hinsichtlich des Umgangs mit KI zu sensibilisieren, ist es notwendig, nicht nur Entscheidungsträgerinnen und Entscheidungsträger aus den Bereichen Wissenschaft und Wirtschaft anzusprechen, sondern vielmehr die Gesamtheit der Bevölkerung. Diese erreicht man beispielsweise durch bereitgestellte Online-Kurse, die durch ihre zielgruppenspezifische Ausrichtung eine Möglichkeit darstellen, Aufklärung hinsichtlich des Einsatzes von KI zu betreiben und somit die diesbezügliche Akzeptanz der Gesellschaft zu fördern. Dieses Format wird bereits in Finnland seit mehreren Jahren praktiziert und stellt einen vielversprechenden und zielführenden Ansatz der Wissensvermittlung und Transparenz dar.

Ziel soll es sein, dass Politik und Wirtschaft gemeinsam solche oder vergleichbare Kurse anbieten und die Gesellschaft zur Teilnahme motivieren (Stürz et al., 2020, S. 6 ff.). Im Rahmen der Strafverfolgung und der Gefahrenabwehr kann der Einsatz von KI-Technologien die Arbeit der Sicherheitsbehörden unterstützen und fördern. Der Einsatz von KI und die damit verbundenen Anwendungsmöglichkeiten bieten Risiken und Chancen für die staatliche Sicherheitsvorsorge. Aufgabe und Ziel des Staates ist insbesondere, die Chancen hinsichtlich der Anwendungsmöglichkeiten von KI-Systemen zu erörtern und diese für die Gesellschaft und den Staat rechtskonform anwendbar zu machen. Der Einsatz von KI-basierten Systemen ist ein wichtiger Bestandteil digitaler Souveränität innerhalb des deutschlandweiten Sicherheitsbereichs und trägt zum Erhalt der Sicherheit der Gesellschaft bei. Hierzu ergänzend kann der Einsatz von KI-Technologien eine enorme Effizienzsteigerung gegenüber herkömmlichen Auswertungsmethoden darstellen. KI wird bereits eingesetzt, um rele-

vante Informationen und Erkenntnisse zu gewinnen, die ohne den Einsatz von KI in keinem adäquaten Zeitraum erreicht werden können. Dies umfasst beispielsweise die Wiedererkennung von Personen im Kontext der Auswertung großer Datenmengen. Aber auch in anderen Bereichen der Strafverfolgung und Gefahrenabwehr kann KI zum Schutz der Gesellschaft oder aber auch zur Steuerung des Einsatzes von Polizeibeamtinnen und -beamten genutzt werden. Anwendungsbeispiele sind u. a. Predictive Policing und der Schutz von Kindern und Jugendlichen vor sexualisierter Gewalt im Internet sowie die Bekämpfung von Missbrauchsdarstellungen oder Social Media Forensics zur Bildung von Personenprofilen (Die Bundesregierung, 2018, S. 32 ff.). Zukünftig wird KI-Technologie nicht nur zur Analyse und Mustererkennung eingesetzt, sondern zunehmend zur Entscheidungsfindung unterstützend verwendet werden. Das hat auch Auswirkungen auf ethische Aspekte und die damit verbundene Akzeptanz der Gesellschaft. Hier ist es Ziel der Bundesregierung, zu gewährleisten, dass der Einsatz von KI die Grundwerte der freiheitlich-demokratischen Grundordnung und den verfassungsrechtlichen Schutz der Grundrechte, wie das Recht auf allgemeine Handlungsfreiheit, auf den Schutz der Privatsphäre und auf informationelle Selbstbestimmung, schützt und wahrt (Die Bundesregierung, 2018, S. 38). Die Erarbeitung von Standards hinsichtlich ethischer Aspekte ist unerlässlich. Dies muss sowohl auf Bundes- als auf europäischer Ebene erfolgen. Hierzu steht die Bundesregierung sowohl mit nationalen als auch mit internationalen Akteuren (beispielsweise mit der Datenethikkommission) im stetigen Austausch.

Ziel ist, dass beim Einsatz von KI ein Schutz vor Diskriminierung, Manipulation oder sonstiger missbräuchlicher Nutzung besteht. Das Vertrauen sowie die Akzeptanz der Gesellschaft können nur durch einen transparenten Umgang mit KI-Technologie gewährleistet und gesteigert werden (Die Bundesregierung, 2018, S. 39). Neben der KI-Strategie der Bundesregierung beinhaltet auch das Weißbuch zur KI der Europäischen Kommission u. a. wichtige ethische Ansätze, die jedoch der weiteren Konkretisierung und Umsetzung bedürfen. Um das Vertrauen der Gesellschaft zu stärken, ist eine weitere europaweite Zusammenarbeit unerlässlich (Stürz et al., 2020, S. 7).

Diskussion

Der Einsatz von KI bei der Polizei hat eine große Wirkung auf die Bereiche der Strafverfolgung und der Gefahrenabwehr. KI-Technologie bietet enormes Potenzial zur Verbesserung der Effizienz und Effektivität polizeilicher Tätigkeiten. Diese Technologien können beispielsweise bei der Analyse von Daten, der Vorhersage von Straftaten und der Optimierung von Ressourcen eingesetzt werden. In Deutschland setzen Polizeibehörden bereits eine Vielzahl von unterschiedlichen KI-Technologiesystemen ein, um die Ermittlungstätigkeit zu unterstützen und die Strafverfolgung zu optimieren. Diese Technologien unterstützen dabei, Musterstrukturen in großen datenbasierten Mengen festzustellen und potenzielle Brennpunkte vorherzusagen. Diese digitale Entwicklung verspricht neben einer effizienteren Strafverfolgung auch verbesserte Präventionsmaßnahmen. Diese dienen vor allem dazu, Straftaten im Vorfeld zu verhindern. Gleichzeitig ist der Einsatz von KI jedoch in gesellschaftlicher Hinsicht – insbesondere in Bezug auf Datenschutz, ethische Überlegungen und die potenzielle Verzerrung von Entscheidungen, die durch algorithmische Systeme beeinflusst werden könnten – als äußerst sensibel anzusehen. Diese Bedenken sind nicht unbegründet, da der Einsatz von KI auch möglicherweise zu ungewollten Verzerrungen führen kann. Auch in anderen Bereichen unserer Gesellschaft – wie beispielsweise im militärischen Kontext – findet KI zunehmend Anwendung, wobei auch hier die ethischen Implikationen dieser Entwicklung kritisch diskutiert werden müssen. Die Notwendigkeit, die Arbeit der Bundeswehr angesichts zukünftiger Bedrohungsszenarien effizient und effektiv zu technisieren, steht außer Frage. Neben KI-gestützten Systemen zur Lagebilderstellung werden auch neue Waffensysteme mit KI-Technologie erörtert und geprüft.

Es ist von entscheidender Bedeutung, dass der Einsatz von KI auch hier regelmäßigen Überprüfungen unterzogen wird, um potenzielle Risiken zu minimieren und die Einhaltung ethischer Standards zu gewährleisten. Für die gesellschaftliche Akzeptanz ist es – analog zum Einsatz von KI bei der Polizei – von zentraler Bedeutung, den durch KI generierten Mehrwert zu verdeutlichen, um somit das Verständnis und die Unterstützung der Bevölkerung zu fördern. Um einen

anwendungsorientierten und ausgewogenen Einsatz von KI im militärischen Bereich sicherzustellen, ist auch hier eine umfassende Berücksichtigung ethischer Aspekte unabdingbar. Dies erfordert einen interdisziplinären Ansatz, der technologische Expertise mit ethischen und gesellschaftlichen Überlegungen in Einklang bringt (Stelzner-Dogan, 2023). Um diese Herausforderungen entsprechend zu bewältigen, sind klare rechtliche Rahmenbedingungen, ethische Leitlinien und eine offene gesellschaftliche Debatte erforderlich. Es ist wichtig, dass die Gesellschaft versteht, wie ihre Daten verwendet werden, um die Akzeptanz zu stärken. Zwar herrscht bereits ein mutmaßlich hohes gesellschaftliches Vertrauen in den Einsatz von KI, jedoch werden rechtliche Rahmenbedingungen und ethische Leitlinien benötigt, die den Einsatz solcher Technologien regeln. Der erfolgreiche Einsatz von KI-Systemen bei der Polizei erfordert eine ausgewogene Balance zwischen den Sicherheitsinteressen der Gesellschaft und den geltenden Bürgerrechten. Hierbei sind regelmäßige Schulungen von Polizeibeamtinnen und Polizeibeamten unerlässlich, um zu gewährleisten, dass diese die Technologie verantwortungsvoll nutzen. Zudem erscheint aus hiesiger Sicht eine transparente Kommunikation gegenüber der Gesellschaft von großer Bedeutung, um Bedenken auszuräumen und das Verständnis für den Einsatz von KI bei der Polizei zu fördern. Diese Maßnahmen sind für eine verantwortungsvolle Nutzung der KI-Technologie unabdingbar und erforderlich, um das Vertrauen der Bevölkerung in die Polizei zu stärken.

Schlussfolgerungen

Die Akzeptanz von KI im Bereich der Polizei hängt maßgeblich von Faktoren wie Bildung, persönlichen Erfahrungen, Altersstrukturen und demografischen Aspekten ab. Menschen, die gut informiert sind, zeigen oft mehr Vertrauen in neue Technologien. Um das Vertrauen der Öffentlichkeit zu gewinnen, sind Transparenz, partizipative Ansätze und kontinuierliche Evaluierung entscheidend. Nur durch einen verantwortungsvollen und ausgewogenen Einsatz kann das vollständige Potenzial dieser Technologie ausgeschöpft werden, ohne dabei grundlegende Rechte und Freiheiten zu gefährden. Die

fortlaufende Zusammenarbeit zwischen Polizei, Wissenschaft und Gesellschaft ist entscheidend, um KI in der Strafverfolgung und Gefahrenabwehr erfolgreich und ethisch vertretbar zu implementieren.

Literaturverzeichnis

Block, S. (2024): ChatGPT – Künstliche Intelligenz & KI Technologien in der Praxis. rock-the-prototype.com/kuenstliche-intelligenz-ki/chatgpt/ (15.10.2024)

Christen, M. (2024): ChatGPT erhöht die Skepsis gegenüber KI. news.uzh.ch/de/articles/news/2024/dsi-insight-christen.html (28.03.2025)

Deutscher Ethikrat (2023): Mensch und Maschine – Herausforderungen durch Künstliche Intelligenz. ethikrat.org/publikationen/stellungnahmen/mensch-und-maschine/ (28.03.2025)

Die Bundesregierung (2018): Strategie Künstliche Intelligenz der Bundesregierung. bundesregierung.de/resource/blob/997532/1550276/3f7d3c41c6e05695741273e78b8039f2/2018-11-15-ki-strategie-data.pdf (28.03.2025)

Hirsch-Kreinsen, H., Krokowski, T. (2023): Technologieversprechen Künstliche Intelligenz. Vergangene und gegenwärtige Konjunkturen in der Bundesrepublik. Berlin J Soziol 33, S. 453-484 (2023). doi.org/10.1007/s11609-023-00504-1

Manzeschke, A., Weber, K., Rother, E., Fangerau, H. (2015): Ethical questions in the area of age appropriate assisting systems, VDI/VDE Innovation +Technik. researchgate.net/publication/304743219_Ethical_questions_in_the_area_of_age_appropriate_assisting_systems#fullTextFileContent (28.03.2025)

Ojamo, J., Wisdorf, A., Hercegfalvi, J. (2021): Einsatz von KI durch die Polizei: Abgeordnete lehnen Massenüberwachung ab. europa.eu/news/de/press-room/20210930IPR13925/einsatz-von-ki-durch-die-polizei-abgeordnete-lehnen-massenuberwachung-ab (28.03.2025)

Overdiek, M., Petersen, T. (2022): Was Deutschland über Algorithmen und Künstliche Intelligenz weiß und denkt. Bertelsmann Stiftung. [bertelsmann-stiftung.de/fileadmin/files/BSt/Publikationen/GrauePublikationen/DG_Was_Deutschland_ueber_Algorithmen_KI.pdf](https://www.bertelsmann-stiftung.de/fileadmin/files/BSt/Publikationen/GrauePublikationen/DG_Was_Deutschland_ueber_Algorithmen_KI.pdf) (28.03.2025)

Rüdiger, T.-G., Bayerl, P. (Hrsg.) (2023): Handbuch Cyberkriminalologie 1, Springer VS Wiesbaden

Samsami, N. (2023): Kann ausgerechnet KI die Verwaltung menschlicher machen? [cgi.com/de/de/blog/oeffentliche-verwaltung/kann-ki-die-verwaltung-menschlicher-machen](https://www.cgi.com/de/de/blog/oeffentliche-verwaltung/kann-ki-die-verwaltung-menschlicher-machen) (27.08.2024)

Schneider, G., Toyka-Seid, C. (2024): Selbstbestimmung. Das junge Politik-Lexikon. [bpb.de/kurz-knapp/lexika/das-junge-politik-lexikon/321117/selbstbestimmung/](https://www.bpb.de/kurz-knapp/lexika/das-junge-politik-lexikon/321117/selbstbestimmung/) (28.03.2025)

Stelzner-Doğan, A. (2023): Vom Gestern ins Heute nach Morgen: Die Innere Führung als eine geistesgeschichtliche Errungenschaft? In: Lammert, N., Koch, W. (Hrsg.): Bundeswehr der Zukunft – Verantwortung und KI. [kas.de/documents/252038/16166715/Bundeswehr+der+Zukunft+-+Verantwortung+und+K%C3%BCnstliche+Intelligenz+%28Sammelband%29.pdf/0a6be7cc-2965-5e30-0cec-334333a0854f?version=1.1&t=1673642730568](https://www.kas.de/documents/252038/16166715/Bundeswehr+der+Zukunft+-+Verantwortung+und+K%C3%BCnstliche+Intelligenz+%28Sammelband%29.pdf/0a6be7cc-2965-5e30-0cec-334333a0854f?version=1.1&t=1673642730568) (30.05.2025)

Stürz, R., Stumpf, C., Mendel, U. (2020): Künstliche Intelligenz verstehen und gestalten. bidt – Bayerisches Forschungsinstitut für Digitale Transformation, [bidt.digital/wp-content/uploads/sites/2/2022/08/bidt_KI-Studie_Juni-2020.pdf](https://www.bidt.digital/wp-content/uploads/sites/2/2022/08/bidt_KI-Studie_Juni-2020.pdf) (28.03.2025)

Ursuleac, S. (2023): KI in der Polizei: zahllose Möglichkeiten – begrenzter Einsatzrahmen. Crisis Prevention, 2, S. 64-66

Weber, K. (2019): Methoden der ethischen Evaluation von IT. In: Draude, C., Lange, M., Sick, B. (Hrsg.): INFORMATIK 2019: 50 Jahre Gesellschaft für Informatik. Informatik für Gesellschaft (Workshop-Beiträge), Gesellschaft für Informatik eV, Bonn, 2019, S. 431-444.

Zink, W., Heinzelmann, P., Ridderbusch, M., Schulte, N. (2022): Vertrauen, Präsenz und digitale Kompetenz. PricewaterhouseCoopers. [pages.pwc.de/studie-vertrauen-in-die-polizei](https://www.pwc.de/studie-vertrauen-in-die-polizei) (28.03.2025)

Zink, W., Heinzelmann, P., Zimmermann, K., Schulte, N. (2023): Der Einsatz digitaler Instrumente durch die Polizei. PricewaterhouseCoopers. [pwc.de/de/branchen-und-markte/oeffentlicher-sektor/pwc-studie-einsatz-digitaler-instrumente-durch-die-polizei.pdf](https://www.pwc.de/de/branchen-und-markte/oeffentlicher-sektor/pwc-studie-einsatz-digitaler-instrumente-durch-die-polizei.pdf) (28.03.2025)

Menschliche oder Künstliche Intelligenz? Eine Konzeption für einen experimentellen Aufbau zur Erforschung der Effizienz von KI im Zusammenhang mit Bilderkennung

David Preuß

Künstliche Intelligenz ein geflügeltes Wort, welches sich derzeit in allen Medien, Arbeitsbereichen und dem Alltag wiederfindet. Wenn man den Nachrichten Glauben schenken kann, ist dies unser aller Gamechanger. Aber ist das wirklich so? Viele kennen KI schon seit einigen Jahrzehnten aus Film und Fernsehen. Werden wir wie in Matrix (1999) erleben, dass die Maschinen unseren Planeten übernehmen und die gesamte Menschheit versklaven, oder handelt es sich bei KI um ein Hilfsmittel für den Menschen, wie J.A.R.V.I.S. für Tony Stark aus Iron Man (2008) im Marvel-Universum, welcher seinem Erfinder lästige Programmierungsaufgaben abnahm? Aus dem Bereich Wettkampf Mensch gegen Maschine gibt es viele Ereignisse aus der Vergangenheit, nehmen wir beispielsweise DeepBlue, AlphaGo oder Watson, welche alle in ihren jeweiligen Spielen meisterlich agieren. Doch die Wettkämpfe waren immer klar abgegrenzte Aufgaben und folgten definierten Regeln; Glück oder Zufall spielten dabei keine Rolle. (Lenzen 2023, S. 111-113) Dr. Leon R. Tsvasman, KI-Experte und freiberuflicher Dozent, äußerte in einem Interview, es sei nicht notwendig, Künstliche Intelligenz gegen Menschen antreten zu lassen. Das wäre vergleichbar damit, einen Menschen gegen ein Auto in einem Wettlauf zu testen oder mit der Faust, statt mit dem Hammer, einen Nagel in die Wand zu schlagen. Der Mensch bleibt der Entscheider, wann er welches Hilfsmittel einsetzt, aber befreit sich damit von Routine und gegenseitiger Instrumentalisierung. (Intelligente Welt 2022) Diesem Gedanken folgend, soll die Konzeption nicht dem Zweck dienen, den experimentellen Aufbau so darzustellen, dass KI besser als der Mensch ist, sondern ein so verlässliches Hilfsmittel, dass wir sehr stupide und langwierige Aufgaben bis zu einem gewissen Maß delegieren können. Die Systeme müssen dabei stets auf eine Weise entwickelt werden und funktionieren, welche weit über das Lösen technischer Probleme hinaus geht und Mensch sowie Umwelt einbezieht. (IEEE 2019) Eine der zentralen Fragestellungen wird sich dabei um die Feh-

lerquote drehen und welcher Wert dabei gegebenenfalls verkraftbar oder gar menschlich ist. Meine Hypothesen für den experimentellen Aufbau sollen sich damit beschäftigen, dass Systeme mit künstlichen neuronalen Netzen Bilder schneller und präziser sortieren als der Mensch. Der Mensch wiederum erkennt wahrscheinlich aber kontextuelle und subtile Details besser als eine KI.

Hintergrund

Dieser Beitrag beschäftigt sich mit drei großen Kernbegriffen für eine spezifische Bilderkennung. Es dreht sich dabei um Künstliche Intelligenz, menschliche Fähigkeiten und Kinder- bzw. Jugendpornografie (KiPo/JuPo). Die ersten Schritte der Künstlichen Intelligenz liegen schon einige Zeit zurück. Im Jahr 1950 fragte sich der bekannte Informatiker und Mathematiker Alan Mathison Turing, ob eine Maschine denken kann. Daraufhin entwickelte er den heute immer noch bekannten Turing-Test. Dieser beinhaltet, dass ein Mensch mittels Computer mit zwei verschiedenen Individuen ein Gespräch führt, die er beide nicht sehen kann. Es ist bekannt, dass einer der beiden Gesprächspartner eine Maschine ist, und der Proband muss nun mittels Fragestellungen herausfinden, welches die Maschine bzw. der Mensch ist. Sollte im Ergebnis die Maschine nicht ermittelt werden, würde dies bedeuten, dass diese ein zumindest ähnliches Denkmuster wie der Mensch aufweist. (Turing 1950, S. 432, 433, 441) Es dauerte bis ins Jahr 2014, ehe ein russisches Computerprogramm namens Eugene Goostman es schaffte, diesen Test zu bestehen, und ein Komitee davon überzeugte, ein 13-jähriger Junge aus der Ukraine zu sein. (Lenzen 2020, S. 12-15) Dies war eine Sensation in der Informatik. Doch zuvor müssen wir bis ins Jahr 1956 zurück, um die Geburt des Begriffes Künstliche Intelligenz nachzuvollziehen. John McCarthy verwendete diesen erstmals bei einer von ihm organisierten Konferenz im College von Dartmouth. Er beschrieb dabei die Intelligenz als Teil der Fähigkeiten, um Ziele zu erreichen. Ein weiterer bekannter Experte auf dem Feld der Künstlichen Intelligenz, Marvin Minsky, fügte hinzu, dass KI, um als solche bezeichnet zu werden, etwas leisten müsste, wozu Menschen Intelligenz benötigen. (Lenzen 2020, S. 18-25) Da es derzeit keine Legaldefinition zu diesem Begriff gibt, orientiert sich dieses

Konzept am Europäischen Parlament, welches KI im Jahr 2023 wie folgt erklärte: „Künstliche Intelligenz ist die Fähigkeit einer Maschine, menschliche Fähigkeiten wie logisches Denken, Lernen, Planen und Kreativität zu imitieren“. (Europäisches Parlament 2023, S. 1) Dabei handelt es sich wahrscheinlich um die Beschreibung einer starken KI, welche eine dem Menschen ebenwürdige Intelligenz und eine Art Bewusstsein impliziert. Derzeit gibt es noch kein bekanntes Programm, welches diese Anforderungen erfüllen kann. Dieser Beitrag soll sich allerdings mit der Vorstufe – und zwar der schwachen KI – beschäftigen. Dabei beschränken sich die Fähigkeiten der Computerprogramme auf klar definierte Tätigkeiten, für welche sie extra geschaffen wurden. Es wird nur ein kleines Spektrum menschlich intelligenten Verhaltens abgebildet, welches nach Erteilung eines Befehls mit zuvor erlernten Algorithmen abgearbeitet wird. (Wagner 2020, S. 61) Es handelt sich um eine Anleitung, die beschreibt, wie man Schritt für Schritt das Ziel erreicht und so Problemlösungsprozesse automatisiert. Oft tritt, sobald man KI auf diesen Aufgabenbereich beschränkt, ein paradoxes Phänomen auf: Wenn der Algorithmus bekannt ist und die Funktion nachvollziehbar, dann wirkt es nicht mehr intelligent. Die Diskussion dreht sich aber immer wieder im Kreis. Es geht um die Fragen, was Intelligenz ist und ob Künstliche Intelligenz über diese Erklärung abgeleitet werden kann.

Neben der Definitionsfrage geht es bei der Entwicklung von Künstlicher Intelligenz auch um technische Voraussetzungen und Funktionsweisen. Eine wichtige Rolle spielt dabei die Veröffentlichung des Perzeptrons von Frank Rosenblatt 1957. Vereinfacht reden wir von einem einzelnen Neuron, wie in unserem Gehirn, welches die Zustände „feuert“ oder „feuert nicht“ als Ausgabewerte einnehmen kann und dafür verschiedene Eingangswerte mit Gewichtungen zur Erreichung des Schwellenwertes für den jeweiligen Zustand vergleicht und dementsprechend reagiert. Im Binärsystem kann somit nur der Zustand 1 oder 0 angenommen werden. Der Startschuss für neuronale Netze, könnte man denken, doch es dauerte Jahrzehnte der technischen Entwicklung und das Voranschreiten der Digitalisierung, um Rechenleistungen zu entwickeln, welche ein Programm wie ChatGPT mit hunderten von Schichten und Millionen von Neuronen zu programmieren, sowie eine immense Anzahl an Trainingsdaten.

Man kann diese Aufgabenbewältigung mit der Baum-Suche erklären. Es beginnt mit der Ausgangsfrage, sozusagen der Wurzel. Im Anschluss wird über verschiedene Schichten die Suche mehr und mehr eingegrenzt. Dies stellt eine Art Verästelung dar. In die nächsttiefere Schicht gelangt man, wenn man der Lösung näherkommt. In eine benachbarte Schicht springt das Programm, wenn diese Variante ausgeschlossen wird. So endet man schließlich bei einer möglichen Lösung, welche als Blatt beschrieben werden könnte. (Lenzen 2020, S. 22, 29-50) Anders erklärt, handelt es sich bei dem neuronalen Netz um eine Struktur, bei der die zu bewertende Datei von den Input-Neuronen über die Hidden-Neuronen zu den Output-Neuronen geleitet werden. Dies kann Texte, Bilder, Signale oder jede andere Art von Muster umfassen. Die einzelnen Knoten modifizieren dann die Daten vor der Weitergabe und geben diesen eine Gewichtung. (Gabers & Brodthage 2021, S. 133) Das Trainieren von künstlichen neuronalen Netzen mit Trainingsdaten wird als Deep Learning bezeichnet – übersetzt so viel wie mehrschichtiges bzw. tiefgehendes Lernen. Auf diese Weise kann das System durch Überwachung von Trainingsdaten und einen anschließenden Vergleich mit den Ausgabepaaren durch den Menschen seine Gewichtung und somit auch das Ergebnis immer weiter verbessern. (Wagner 2020, S. 63) Nehmen wir beispielsweise an, ein neuronales Netz soll lernen, ein Auto von einem Flugzeug zu unterscheiden. Dem Programm werden dafür tausende von Bildern dieser beiden Transportmittel zur Verfügung gestellt. Ist die Abschätzung einer Datei nicht korrekt, werden die Gewichte angepasst und alle Bilder erneut geprüft. Bei jedem Durchgang verbessert sich das Ergebnis, bis schlussendlich das neuronale Netz selbstständig eine Differenzierung für weitere Bilder vornehmen kann. Dabei sind CNNs, Convolutional Neural Networks, welche aus mehreren Schichten bestehen und gemeinsame Merkmale aus Bildern extrahieren, klassifizieren sowie komplexe Muster bzw. Objekte erkennen, speziell für die Verarbeitung von Bildmaterial konzipiert. Ein lernender Algorithmus benötigt pro Kategorie zwischen 1000 und 1 Millionen Trainingsdaten. (Lenzen 2020, S. 15-18, 50-54) Das KI-gestützte Pokerprogramm Libratus beispielsweise benötigte 15 Millionen Prozessstunden, was ca. 1712 Jahren entspricht. (Lenzen 2023, S. 111-113) Diese zum Teil unvorstellbaren Größen sind mittlerweile längst zum Standard der KI-Entwicklung geworden und müssen heute eher anhand der Da-

tenqualität, Fehleranfälligkeit sowie Manipulationsresistenz den Anforderungen Rechnung tragen. Dennoch erreichen die Volumina der weltweit jährlich generierten digitalen Datenmengen unvorstellbare Sphären. Lag der gemessene Bestand 2022 noch bei 103 Zettabyte, wird dieser laut Prognose für 2027 auf 284 Zettabyte geschätzt. Dies entspräche 2,84 mal 1.000.000.000.000 Gigabyte – eine unvorstellbare Masse an Daten. (Tenzer 2024)

Neben der Künstlichen Intelligenz sind für diesen experimentellen Aufbau die menschlichen Fähigkeiten im Bereich der Kognition, insbesondere die Verarbeitung und Interpretation visueller Informationen im Gehirn, zu betrachten. Die menschliche visuelle Wahrnehmung ist ein komplexer Prozess, der die Interpretation von Lichtreizen durch das Auge und das Gehirn umfasst. Dieser Prozess beinhaltet das Erkennen von Formen, Farben, Bewegungen und Tiefen. Parameter wie Erfahrung, Intuition und Kontextwissen befähigen den Menschen, Bilder schnell und oft präzise zu kategorisieren. Allerdings bilden Ermüdung, subjektive Wahrnehmung und inkonsistente Leistungen eine nicht zu vernachlässigende Fehleranfälligkeit. (Krauss 2023, S. 1-12) Verantwortlich für die Aufnahme, Verarbeitung und Weiterleitung von Informationen im gesamten Körper ist das neuronale Netzwerk. Dieses besteht aus ca. 86 Milliarden Nervenzellen, die sogenannten Neuronen, welche über Synapsen miteinander verbunden sind. Die Gesamtzahl der Verbindungen im Gehirn wird auf grob eine Billion geschätzt. Die Verbindungen sollten auf einem durchschnittlichen Aktivitätsniveau gehalten werden. Aus informationstheoretischer Sicht sind Neuronen, welche nie feuern, nämlich genauso dysfunktional wie Neuronen, die dauerhaft feuern. (Krauss 2023, S. 17-30) Für eine genauere Betrachtung wird auf das Mehrkomponentenmodell des Arbeitsgedächtnisses von Alan Baddeley und Graham Hitch aus dem Jahr 1974 Bezug genommen. Dieses beinhaltet die Komponente „zentrale Exekutive“, welche die Aufmerksamkeit und Koordinierung der Informationsverarbeitung steuert – sozusagen die Zentrale, welche alles überwacht und bündelt. Die phonologische Schleife, welche über das Gehör die Geräusche interpretiert, speichert verbale Informationen. Der episodische Puffer integriert Reize aus verschiedenen Bereichen, wie dem Sehen. Zudem gibt es noch das visuell-räumliche Notizbuch, welches die temporäre Speicherung und Manipulation

verbildlichter Vorstellungen ermöglicht. Das Gedächtnis ist somit für die menschliche Kognition ein unerlässlicher Faktor, welcher zur Informationskodierung, -manipulation, -speicherung und -abrufbarkeit entscheidend ist. (Krauss 2023, S. 63-71)

Abschließend sind in der Vorbetrachtung noch die Begriffe Pornografie, Jugend- und Kinderpornografie zu erläutern. Im Zusammenhang mit der Strafverfolgung solcher Delikte ist insbesondere das National Center for Missing and Exploited Children (NCMEC) zu nennen, welches strafrechtlich relevante Inhalte im Internet feststellt und an die zuständigen Behörden weiterleitet. Im Jahr 2023 gingen dadurch rund 180.300 Hinweise im BKA ein. (BKA 2024) Laut BGH handelt es sich um eine pornografische Darstellung, wenn „unter Ausklammerung aller sonstigen menschlichen Bezüge sexuelle Vorgänge in grob aufdringlicher, anreißerischer Weise in den Vordergrund rücken und ihre Gesamttendenz überwiegend auf das lüsterne Interesse des Betrachters an sexuellen Dingen abzielt.“ (BGHSt 23, 44; 37, 55) Jugendpornografie gemäß § 184c StGB wiederum umfasst pornografische Inhalte, welche sexuelle Handlungen von, an oder vor Personen zum Gegenstand haben, die 14, aber noch nicht 18 Jahre alt sind, oder eine Abbildung einer ganz oder teilweise unbedeckten Person dieser Altersklasse in unnatürlicher geschlechtsbetonter Haltung zeigen. Der Unterschied zur Kinderpornografie beschränkt sich dabei auf das Alter und umfasst sämtliche Darstellungen von Kindern unter 14 Jahren. Das Tatbestandsmerkmal „Person unter vierzehn“ gemäß § 184b StGB ist aber auch erfüllt, wenn die gezeigte Person tatsächlich ein Kind ist, auch wenn es älter aussieht, sofern diese von einem objektiven Beobachter als Kind eingestuft wird. (Laubenthal 2012, S. 333)

Methode

Dieser Beitrag soll eine Konzeption eines experimentellen Aufbaus zur Erforschung der Effizienz von Künstlicher Intelligenz im Zusammenhang mit Bilderkennung aufzeigen. Dabei wird eine Anwendung betrachtet, welche mit Unterstützung von neuronalen Netzen arbeitet und Teilaufgaben von Sachbearbeitern übernehmen kann. Vorrangig sollen dabei die Geschwindigkeit und Genauigkeit im

Vergleich zum Menschen erforscht werden. Bei einer Konzeption handelt es sich um eine detaillierte Planung. In dieser werden Ziele, Zeitrahmen, Ressourcen und Methode beschrieben, um den erfolgreichen Ausgang sicherzustellen. Bei einem Experiment handelt es sich um einen Untersuchungsaufbau, welcher entweder neue Erkenntnisse generiert oder bereits bekannte Hypothesen bestätigt bzw. widerlegt. Eine experimentelle Versuchsanordnung beschäftigt sich im Kern also mit der Überprüfung von Kausalzusammenhängen. Der Einfluss von unabhängigen zu abhängigen Variablen wird zu betrachten versucht, um gemessene Veränderungen einzelnen Faktoren zuordnen zu können. (Meindl 2011, S. 33-54) Bei der Durchführung von Experimenten lässt sich grundsätzlich zwischen drei Phasen unterscheiden. Zuerst kommt die Planungsphase, welche Beobachtung, Forschungsfrage, Ziele und Hypothesenbildung beinhaltet. Bei der Erarbeitung der Hypothesen ist auf Präzision und Widerspruchsfreiheit sowie Operationalisierbarkeit der zu betrachtenden Variablen zu achten. Zudem sind Störvariablen, Stichproben und die Versuchssituation vorzudenken und zu benennen. Die zweite ist die Durchführungsphase. Hier geht es um organisatorische Erfordernisse, wie die Auswahl der Versuchspersonen, Rahmenbedingungen, Räumlichkeiten, Datensätze und Technik. Die Festlegungen sind in einem Versuchsplan darzustellen und mittels Protokoll sind Umgebungsveränderungen zu dokumentieren. Es geht in erster Linie um Datensammlung für die letzte Phase Auswertung. In diesem dritten Schritt finden Datenanalyse, Interpretation der Daten, Schlussfolgerungen und Ergebnisdarstellung statt. Insbesondere die Fehleranalyse des Versuchsaufbaus, Mittel- und Grenzwertbestimmungen sowie das Vermeiden von Übergeneralisierung der Ergebnisse sind zu beachten. Bei der Auswahl der Gütekriterien sollen nachfolgend drei besonders hervorgehoben werden: die Validität, welche sicherstellt, dass tatsächlich das gemessen wurde, was auch erforscht werden sollte; die Reliabilität, die aufzeigt, ob die Messmethode zuverlässig ist und sich bei einer erneuten Messung vergleichbare Ergebnisse feststellen lassen; abschließend die Objektivität, welche beschreibt, inwiefern die Ergebnisse unabhängig von der Person des Versuchsleiters so zustande kämen. (Meindl 2011, S. 55-66) In erster Linie soll es bei diesem experimentellen Aufbau darum gehen, eine Software-Anwendung, welche mithilfe von neuronalen

Netzen Massendaten im Bereich der Kinder- und Jugendpornografie sichtet, kategorisiert und filtert, in den Fähigkeiten Geschwindigkeit und Genauigkeit mit dem Menschen zu vergleichen. Dabei sollen belastbare Zahlen zu Fehlerquoten erforscht werden, um eine an Fakten orientierte Entscheidung zur verlässlichen Nutzung KI-basierter Systeme in diesem Bereich treffen zu können. Zudem könnte der generierte Datensatz auch für andere KI-Programme zur Wiederholung dieses experimentellen Aufbaus genutzt werden.

Ergebnisse

Dieser Abschnitt soll sich mit der Planung des Versuchsaufbaus beschäftigen. Hauptaugenmerk liegt beim Phänomenbereich Bekämpfung von Kinder- und Jugendpornografie im Zusammenhang mit Massendaten auf der Fähigkeit der Bilderkennung von Menschen und einer Software, welche neuronale Netze nutzt. Die Parameter, welche gemessen werden sollen, sind Geschwindigkeit und Fehlerquote. Ziel dabei ist es, eine faktenbasierte Einschätzung zur Nutzung von KI-basierter Software für die polizeiliche Bekämpfung von Kinder- und Jugendpornografie zu erlangen und auch Grenzen einzelner Anwendungen zu erforschen. Im Ergebnis sollen Handlungssicherheit, Arbeitsentlastung, Effizienzsteigerung und Schwerpunktverlagerung stehen.

Ein wichtiger Punkt für das Experiment ist die Auswahl des Testdatensatzes. Nach Gesprächen mit Sachbearbeitern und Kommisariatsleitern, Durchforsten von Fachliteratur und Überprüfen von Rechtsgrundlagen zur Nutzung von Datensätzen für Lehre und Wissenschaft ist es für mich entscheidend, Daten aus einem abgeschlossenen Echtfall zu verwenden. Dies hat mehrere Vorteile. Zum einen ist in § 80 Abs. 6 SächsPVDG geregelt, dass der Polizei mit Zustimmung der Staatsanwaltschaft Befugnisse zur Datenweiterverarbeitung zu Zwecken der Aus- und Fortbildung gewährt werden können. Zum anderen handelt es sich um reale Daten, welche einen besseren Bezug zur Praxis und eine authentische Zusammenstellung der Bilder bieten. Hinzu kommt, dass eine Repräsentativität über die Grundgesamtheit bei einem Echtfall mit höherer Wahrscheinlichkeit

gegeben ist. (Meindl 2011, S. 131-146) Aufgrund des Versuchsaufbaus muss die Gesamtheit der Bilder auf ein beherrschbares Maß für die Probanden reduziert und qualitativ ausgewählt werden. Das Konzept sieht eine Anzahl von insgesamt 1.000 Bildern für den Testdatensatz vor. Den überwiegenden Teil davon werden Alltagsdaten ohne Bezug zu Pornografie darstellen. Es wird sich dabei um Bilder aus dem Verfahren handeln, welche Menschen, Fahrzeuge, Häuser, Tiere und sonstige Gegenstände zeigen, in wechselnden Darstellungen und Mengen. Zudem sollen Außen- und Innenaufnahmen sowie unterschiedliche Ausleuchtungen und Bildqualität vorhanden sein. Die Anzahl pornografischer Materials ohne KiPo/JuPo-Bezug soll bei 10 % der Gesamtheit liegen, das entspräche 100 Bildern. Zudem würden 5 % KiPo/JuPo kommen, was 50 Bildern entspräche. Diese sollten Kinder unterschiedlichen Alters, Geschlechts, ethnischer Herkunft sowie wechselnder Anzahl und Pose abbilden. Zusätzlich sollte sich auch die Zusammensetzung der Datenformate an relevanten und typischen Alltagsdatensätzen ausrichten und beispielsweise jpeg, jpg, mp4, heic, png, mov oder ktx enthalten. Vorgesehen ist, dass ein Kommissariat der Polizei aus dem Bereich der IT-Forensik den Testdatensatz anhand der oben beschriebenen Parameter erzeugt und den technischen Support gewährleistet. Nach Abschluss der Zusammenstellung und vor der Durchführung wird ein Pretest – ein Test zur Benutzerfreundlichkeit und Machbarkeit – mit ausgewählten Personen durchgeführt, welche nicht am Experiment teilnehmen. Dies ermöglicht erste Einblicke in Fehlerquellen und auftretende Probleme, welche vor der Durchführung noch behoben werden können. (Vogel 2021, S. 5-21)

Ein weiterer wichtiger Schritt für den experimentellen Aufbau ist die Wahl der Software, welche getestet werden soll. Für Aufbereitung und Auswertung von Handydaten im Ermittlungsbereich Kinder- und Jugendpornografie nutzt die Polizei des Freistaates Sachsen den Physical Analyzer der Cellebrite GmbH aus Israel. Der Physical Analyzer bietet die Möglichkeit Medienklassifikationen mittels neuronaler Netze auf Grundlage vordefinierter Kategorien durchzuführen. Relevant für das dargestellte Experiment sind dabei Verdacht auf Kindesmissbrauch (CSA) und Nacktheit. Beim Importieren der Dateien ordnet die Software die Bilder sowie Videos mittels Medien-

analyse den vordefinierten Kategorien zu. Gleichzeitig wird ein Score für jede Datei erzeugt. Der sogenannte Confidence Score, welcher die Wahrscheinlichkeit beschreibt, dass es sich bei einem Bild oder Video um entsprechende Inhalte handelt, bewegt sich zwischen 50 und 90 Prozent. Cellebrite nutzte Trainingsmaterial, welches die Polizei in Harris County (Texas, USA) zur Verfügung stellte. Durch die Software werden folglich Bilder als „Verdacht auf Kinderpornografie“ kategorisiert, wenn das geschätzte Alter der abgebildeten Person zwischen null und zwanzig Jahren liegt. Allgemeine Pornografie wird oberhalb dieser Grenze als Nacktheit klassifiziert. (Möller 2022, S. 34-35) Bei der Software handelt es sich um eine Blackbox, die nur eine Betrachtung des äußeren Verhaltens zulässt, wobei der Weg zur Entscheidung sowie die zugrunde liegenden Annahmen der KI nicht nachvollzogen werden können. (Gethmann et al. 2021, S. 13-42)

Eine weitere wichtige Überlegung beschäftigt sich mit der Auswahl der menschlichen Probanden. Bei einer Stichprobenkennwertverteilung spielt der zentrale Grenzwert eine entscheidende Rolle. Dieser beschreibt die mathematische Gesetzmäßigkeit, dass sich, wenn man theoretisch unendlich viele Stichproben einer Population zieht, sich der Gesamtwert der Normalverteilung von 30 immer weiter annähert. Somit ist eine Stichprobengröße von mindestens 30 zu wählen, um ein repräsentatives Ergebnis zu erreichen. (Meindl 2011, S. 131-146) Mit steigender Anzahl wird die Schätzung der Populationsparameter immer genauer. Dies erklärt sich anhand der empirischen Gesetzmäßigkeit der großen Zahlen. Allerdings schreckt der Zeit- und Kostenaspekt dabei viele aufgrund der erheblichen Stichprobengrößen von einer detaillierten Stichprobenberechnung ab. (Vogel 2021, S. 35-38) Für das Experiment sieht das Konzept mindestens 30 Ermittlerinnen und Ermittler aus allen Kriminalpolizeiinspektionen sowie deren Kriminalaußenstellen, welche für die Bearbeitung von KiPo/JuPo zuständig sind, vor. Dies erhöht sowohl den repräsentativen Charakter im Bereich der Anzahl, zudem berücksichtigt es die regionalen Unterschiede. Voraussetzungen sind zudem eine dienstliche Mindestverweildauer in diesem Ermittlungsbereich von zwei Jahren und Erfahrungen in der Anwendung des Physical Analyzer von Cellebrite.

Die Rahmenbedingungen der Durchführung sollen sich, soweit möglich, an der Realität ausrichten. Aus diesem Grund wird der Testdatensatz zunächst von der Software geprüft und anhand der relevanten Kategorien sortiert. Die Probanden werden den Test an ihrem üblichen Arbeitsplatz durchführen, um reale Bedingungen des Alltags nicht künstlich zu beeinflussen. Über den UFED-Reader von Celebrite oder ggf. ein anderes Medium werden zunächst die Bilder des Testdatensatzes in Miniaturbildansicht aufbereitet und zur Verfügung gestellt. Die Ermittlerinnen und Ermittler haben die Aufgabe, den Testdatensatz auf KiPo/JuPo zu durchsuchen und zu markieren. Nach Abschluss soll das Ergebnis in Form eines Berichts weitergeleitet werden. Die jeweils benötigte Zeit ist anhand der Abgabezeit zu dokumentieren. Anschließend werden mittels Fragebogen zunächst die soziodemografischen Angaben durch die Probanden erfasst und mögliche Probleme bei der Bearbeitung dargestellt.

Die darauffolgende Auswertung soll die Bewertungskriterien der Konfusionsmatrix von Karl Pearson 1904 nutzen. Diese stellt die Ergebnisse der Klassifikationsaufgabe verständlich dar. Die Einzelergebnisse können nur einen der Werte richtig-positiv (TP), richtig-negativ (TN), falsch-positiv (FP) oder falsch-negativ (FN) annehmen. (Wilmott 2020, S. 44-47) Eine Interpretation dieser Werte kann durch eine Relation zueinander erfolgen und auch den Zeitfaktor mit einfließen lassen. Nachfolgende Qualitätsmaße für die Trefferleistung werden zum Gegenstand der Auswertung gemacht. Die Genauigkeitsrate stellt die Anzahl der richtig klassifizierten Bilder ins Verhältnis zur Gesamtheit mit der Formel $(TP+TN)/(TP+TN+FP+FN)$. Das Gegenstück dieses Qualitätsmaßes ist die Fehlerrate, welche alle Klassifizierungsfehler darstellt und mit der Formel $(FP+FN)/(TP+TN+FP+FN)$ berechnet wird. Einen weiteren Parameter soll die Präzision darstellen. Diese beschäftigt sich mit den positiven Werten, welche tatsächlich positiv waren, und wird mit der Formel $TP/(TP+FP)$ ermittelt. Einer der wichtigsten Qualitätswerte dieses Experiments ist die Sensitivität. Dabei wird angegeben, welcher Anteil aller positiven Bilder korrekt als positiv vorhergesagt wurden, sozusagen die Entdeckungswahrscheinlichkeit mit der Formel $TP/(TP+FN)$. Dessen Gegenstück ist die Spezifität, welcher Anteil aller negativen Proben korrekt negativ sortiert wurde, mit der Berechnung $TN/$

$(TN+FP)$. Abschließend wird der F1-Score berechnet. Dieser kombiniert Präzision sowie Sensitivität und bildet einen Mittelwert dieser beiden wichtigen Parameter mit der Formel $2TP/(2TP+FP+FN)$. (Wilmott 2020, S. 44-47) Zusätzlich wird der Faktor Zeit in Relation zur Genauigkeit geprüft.

Ein gutes Beispiel für die Anwendung dieser Auswertungsmethode stellt der Computertomograf des Fraunhofer-Instituts für bildgestützte Medizin in Bremen dar, welcher in der Radiologie zur Verdachtsuntersuchung von Lungenkrebs eingesetzt wird. Das mit neuronalen Netzen gestützte Programm prüft ca. 900 Schichten bzw. Aufnahmen auf Veränderungen im Gewebe. Die Software sieht schneller und präziser als ein Arzt, ob ein relevantes Bild dabei ist, da es Pixel für Pixel überprüft und so schon frühe Stadien von Tumoren erkennt. Der Arzt kann sich anschließend auf die ermittelten Bilder für die weitere Betrachtung konzentrieren. Markus Wenzel, Informatiker des Fraunhofer-Instituts äußerte dazu, wenn ein Computer weniger Fehler macht als der Mensch, sollte dieser auch eingesetzt werden. Insbesondere nimmt er auch auf die zeitaufwendige und ermüdende Routinetätigkeit Bezug. (Lenzen 2023, S. 152-164)

Diskussion

Die Entwicklung von Systemen mit Künstlicher Intelligenz ist längst in einem globalen Markt von weltweit agierenden IT-Unternehmen angekommen. Vorteile bieten sich insbesondere durch die konstante Leistung, hohe Geschwindigkeit, Skalierbarkeit und Objektivität. Für das Entwickeln von KI-Tools reichen die eigenen Ressourcen innerhalb der Polizei oft nicht aus. Investitionen sind notwendig, um Knowhow von Drittanbietern zur Verfügung gestellt zu bekommen. Daraus ergibt sich aufgrund von Lizenzen aber oft eine bedingte Abhängigkeit, welche in der Folge die Flexibilität von Weiterentwicklungen lähmt. (Lenzen 2020, S. 50-57) Durch zu geringe oder schlechte Vergleichsdaten können sich Fehleinschätzungen in KI-Systeme einschleichen. So könnten aufgrund einer eingeschränkten Datenbasis bestimmte Phänomene oder ganze Gruppen ausgeschlossen oder diskriminiert werden. (Lenzen 2020, S. 50-80) Ein anderes Risiko ist die Manipulation der Daten. Über Bilddateien könnte beispielsweise

ein weißes Rauschen gelegt oder einzelne Pixel könnten verändert werden. Dies stellt für das menschliche Auge zwar keinen Unterschied dar, lässt aber Prüfprogramme gegebenenfalls bei der Klassifizierung zu einem anderen Schluss kommen. Dabei können Fehler entstehen, welche für den gesunden Menschenverstand ausgeschlossen wären. Ein weiteres Problem von Künstlicher Intelligenz ist die Nachvollziehbarkeit. Die Systeme bearbeiten Befehle und generieren Ergebnisse, doch die Methode oder die Ansätze sind wie eine Art Blackbox. Es gibt zwar bereits Forschungen im Bereich der explainable AI – erklärbare KI –, doch diese können nur punktuell auf die vorhandene Vielzahl von Programmen reagieren. Dies kommt insbesondere zum Tragen, wenn man die europäische Datenschutz-Grundverordnung betrachtet, welche aussagt, dass alle Menschen das Recht haben, Gründe für algorithmenbasierte Entscheidungen, von denen sie betroffen sind, nachvollziehbar zu erfahren. (Lenzen 2020, S. 50-80) Somit muss der Weg vom Auftrag über die Verarbeitung bis zum Ergebnis plausibel und schlüssig sein. Ob sämtliche KI-gestützten Systeme dies leisten können, wird eine der Zukunftsfragen sein.

Menschen haben andere Fähigkeiten beim Sortieren von Bildern als die KI. Das Kontextverständnis ist dabei ein wichtiger Punkt, welcher das Erkennen von subtilen Details und Interpretation zur korrekten Kategorisierung ermöglicht. Zudem ist ein Mensch anpassungsfähig sowie flexibel und kann bei Bedarf neue Strategien entwickeln. Auch der Bereich Intuition und Erfahrung ist in diesem Kontext nicht zu unterschätzen. Klar ist aber auch, dass sowohl Ermüdung, langsame Verarbeitung als auch Subjektivität die Prozesse immens beeinflussen können und das Ergebnis dadurch verschlechtern. (Krauss 2023, S. 63-71) Für dieses konkrete Experiment ist der Datenschutz der Probanden zu beachten und die erlangten Ergebnisse sind zu anonymisieren. Dies könnte die freiwillige Teilnahme hemmen und erfordert detaillierte Vorbereitungsgespräche mit den in Betracht kommenden Dienststellen, was eine zwingende Voraussetzung für das Gelingen des Versuchsaufbaus darstellt. Auch Bedenken im Bereich der zukünftigen Nutzung von KI-Systemen müssen ausgeräumt werden, da es weiterhin erforderlich ist, akribisch die Daten auszu-

werten, um keine Missbrauchsfälle zu übersehen. Die menschliche Komponente bleibt schon aufgrund der Qualitätssicherung eine bindende Größe für die Interpretation der Daten.

Die Auswertung der Ergebnisse des Versuchsaufbaus soll zunächst einzeln stattfinden. Im Anschluss können anhand der oben beschriebenen statistischen Methoden Mittelwert und Spitzenwerte der Probanden ermittelt werden. Weiterführend erfolgt der Vergleich dieser Klassifizierungsleistungen mit dem Ergebnis des Physical Analyzer von Cellebrite. Die erlangten Erkenntnisse werden abschließend interpretiert und in einem Resümee zusammengefasst. Hauptaugenmerk anhand der Hypothesen nehmen die Werte Zeit und Genauigkeit ein. Nicht auszuschließen ist, dass technische Probleme, Fehlbedienung oder Ablenkung die Resultate der Probanden beeinflussen. Dies ist bei der Betrachtung, neben weiteren möglicherweise auftretenden Negativfaktoren, während der experimentellen Durchführung zu beachten und im Eintrittsfall im Pretest bereits zu korrigieren.

KI-Forschung ist ein sehr weites und uneinheitlich bestelltes Feld, ähnlich wie wir es schon im gesamten technischen Bereich der Polizeien des Bundes und der Länder kennen. Die meisten Anwendungen aus einem Bereich lösen ähnliche Aufgaben, sind aber nur sehr selten kompatibel. In der Wirtschaft beschleunigen Wettbewerbe wie beispielsweise der RoboCup oder die Grand Challenge der DARPA Entwicklungen, indem sie Preisgelder in Aussicht stellen und dadurch Ressourcen gebündelt, Aufträge fokussiert und Leistungen vergleichbar werden. (Lenzen 2023, S. 111-113) Eine solche Bündelung könnte P20 bringen, aber dafür sind die Erfolge derzeit noch nicht ersichtlich. Es stellt sich nicht die Frage, ob KI besser ist als der Mensch, sondern ob ein Mensch bessere Entscheidungen mithilfe von KI trifft.

Schlussfolgerungen

Die Diskussion über Vor- und Nachteile von KI-gestützten Systemen und menschlicher Bildsortierung zeigen, dass beide Ansätze ihre spezifischen Stärken und Schwächen haben. KI ist besonders effizient bei der schnellen und konstanten Verarbeitung großer Datenmen-

gen, während Menschen komplexe Szenarien, die kontextuelles Verständnis erfordern, erfolgreicher analysieren. Eine optimale Lösung wird aus meiner Sicht weiterhin in der Kombination beider Ansätze liegen, wobei KI für die Vorverarbeitung und schnelle Klassifikation verwendet werden sollte und Sachbearbeiter ihre Expertise für die endgültige Validierung und Kontextualisierung der Bilder einsetzen. Dafür müssen die Anwendungen funktionieren, erklärbar, robust und prüfbar sein. Es geht im Kern darum, dass es sich nur um Unterstützungsleistungen handelt. Die Entscheidungen sollten weiter durch Menschen getroffen werden. Für eine kontinuierliche Implementierung in der Polizei braucht es konkrete Ansprechdienststellen, welche KI-Leuchtturmprojekte gemeinsam mit IT-Unternehmen entwickeln und integrieren. (Bitkom e.V. 2023, S. 1-16) KI kann uns nur helfen, selbst bessere Entscheidungen zu treffen, und wir müssen bedenken, auch Menschen machen Fehler. Personen sind Stimmungen und Vorurteilen unterworfen, neigen dazu auszublenden, was nicht zu ihren Erwartungen passt, und haben eine beschränkte intellektuelle Kapazität. (Lenzen 2020, S. 80-98) Die Fragen der Zukunft beschäftigen sich gar nicht damit, ob in der Polizei Künstliche Intelligenz eingesetzt werden sollte, sondern welche Befugnisse mit welchen Rechtsgrundlagen die Polizei zur Erfüllung ihrer Aufgaben im Zusammenhang mit KI erhält und wo sich die ethischen roten Linien befinden, welche nicht überschritten werden dürfen. Diese Themen sollten in anderen Abhandlungen genauer betrachtet werden und sind nicht Teil dieser Konzeption.

Das menschliche Gedächtnis ist ein komplexes und vielschichtiges System, welches noch niemand vollständig entschlüsselt hat. Aus diesem Grund stellt es für Entwickler von KI-Systemen auch eine so große Herausforderung dar. Unabhängig davon, wie „intelligent“ neuronale Netze auch werden, sie sind nicht wie Menschen. (Krauss 2023, S. 63-71) Ungeachtet der konkreten Ergebnisse, welche das dargelegte Experiment erzielen wird, ist der Einsatz von neuronalen Netzen, insbesondere für den Phänomenbereich Bekämpfung der Kinder- und Jugendpornografie, als Gamechanger anzusehen. Ressourcen können entlastet, Prozesse beschleunigt und dadurch auch Missbrauchsfälle schneller aufgeklärt werden. Einen möglichen Schritt hin zu einer Synergie zwischen KI und Mensch könnten Aus-

werter einnehmen, welche die Anwendungen wie beschrieben für die schnelle Kategorisierung nutzen und aufgrund ihrer Erfahrung mit den Programmen Fehler sowie Lücken erkennen und so Sachbearbeiter entlasten. Ein weiterer Vorteil wäre, dass eine viel geringere Anzahl von Beamten bei einer Systemumstellung oder einem Software-Austausch intensiv geschult werden müsste. Das Experiment soll eine erste Datengrundlage im Bereich Bilderkennung von KiPo/JuPo bei der Polizei zum Vergleich zwischen neuronalem Netz und Mensch darstellen. Der entstandene Testdatensatz könnte mit einer zeitlichen Befristung anschließend auch für andere geeignete KI-Anwendungen genutzt werden. Dies soll auch ein Anstoß sein, die Zusammenarbeit der Polizeien des Bundes und der Länder weiter zu fördern.

Literaturverzeichnis

Bitkom e.V. (2023): KI in der Polizei – Einsatzpotentiale und Lösungsansätze zur Implementierung, bitkom.org/sites/main/files/2023-10/bitkom-positions-papier-ki-polizei-einsatz-implementierung.pdf [Zuletzt geprüft am 21.09.2024]

BKA (2024): Bundeslagebild Sexualdelikte zum Nachteil von Kindern und Jugendlichen 2023 vom 08.07.2024 bka.de/DE/Aktuelle-Informationen/Statistiken-Lagebilder/Lagebilder/Sexualdelikte-zu-Nv-Kindern-und-Jugendlichen/2023/BLB-Sexualdelikte_2023_node.html [Zuletzt geprüft am 11.09.2024]

Europäisches Parlament (2023): Was ist künstliche Intelligenz und wie wird sie genutzt? vom 20.06.2023 europarl.europa.eu/topics/de/article/20200827STO85804/was-ist-kunstliche-intelligenz-und-wie-wird-sie-genutzt [Zuletzt geprüft am 09.10.2024]

Gabers, N. & Brodthage, M. (2021): Einsatz künstlicher Intelligenz im Polizeialltag, Frankfurt: Verlag für Polizeiwissenschaften

Gethmann, C., Buxmann, P., Distelrath, J., Humm, B., Lingner, S., Nitsch, V., Schmidt, J. & Spiecker, I. (2021): Künstliche Intelligenz in der Forschung: Neue Möglichkeiten und Herausforderungen für die Wissenschaft, Heidelberg: Springer Berlin

IEEE (2019): Leitfaden Ethically Aligned Design automatisierter Systeme, vom 25. März 2019 algorithmwatch.org/de/ieee-ethically-aligned-design-first-draft-german/ [Zuletzt geprüft am 11.09.2024]

Intelligente Welt (2022): Interview KI und die Selbstverständlichkeit des Menschen mit Leon R. Tsvasman, vom 18. Mai 2022 digitalewelt-magazin.de/interviews/ki-und-die-selbstverstaendlichkeit-des-menschen/ [Zuletzt geprüft am 06.09.2024]

Krauss, P. (2023): Künstliche Intelligenz und Hirnforschung – Neuronale Netze, Deep Learning und die Zukunft der Kognition, Springer-Verlag

Laubenthal, K. (2012): Handbuch Sexualstraftaten – Die Delikte gegen die sexuelle Selbstbestimmung, Heidelberg: Springer Berlin

Lenzen, M. (2020): Künstliche Intelligenz – Fakten Chancen, Risiken, Sonderausgabe der Zentralen für politische Bildung, Verlag C.H. Beck

Lenzen, M. (2023): Künstliche Intelligenz – Was sie kann & was uns erwartet, Verlag C.H. Beck

Meindl, C. (2011): Methodik für Linguisten – Eine Einführung in Statistik und Versuchsplanung, Narr Francke Attempto Verlag

Möller, D. (2022): Künstliche Intelligenz im Phänomenbereich Kinderpornografie – Eine vergleichende Betrachtung der bei den Polizeien verwendeten Technologien, DHPol Münster, Masterarbeit

Tenzer, F. (2024): Volumen der jährlich generierten/replizierten digitalen Datenmenge weltweit von 2010 bis 2022 und Prognose bis 2027, de.statista.com/statistik/daten/studie/267974/umfrage/prognose-zum-weltweit-generierten-datenvolumen/ [Zuletzt geprüft am 13.02.2024]

Turing, A. M. (1950): Computing Machinery and Intelligence, Edited by B. Jack Copeland, Clarendon Press Oxford (2004) edwardfrenkel.com/turing-intelligence.pdf [Zuletzt geprüft am 21.09.2024]

Vogel, P. (2021): Laborstatistik für technische Assistenten und Studierende, Springer Spektrum – Nature 2021

Wagner, J. (2020): Legal Tech und Legal Robots, 2. Auflage, Wiesbaden: Springer Fachmedien

Wilmott, P. (2020): Grundkurs Machine Learning, Bonn: Rheinwerk Verlag

Einsatz von Künstlicher Intelligenz bei der polizeilichen Sachbearbeitung von Massendelikten der Alltagskriminalität

Thomas Coldewei

Die öffentliche Einführung von ChatGPT im November 2022 (vgl. Kero et al., 2023) markiert einen entscheidenden Punkt in der öffentlichen Wahrnehmung von Künstlicher Intelligenz (KI). Diese technologische Entwicklung, die bereits seit vielen Jahren in stetigem Fortschritt begriffen ist, ist nun in den Fokus der Öffentlichkeit gerückt. Die Leistungsfähigkeit dieser Technologie hat mittlerweile ein Niveau erreicht, das einen professionellen Einsatz in einer Vielzahl von Arbeits- und Lebensbereichen ermöglicht. Die Automatisierung von Prozessen gewinnt in einer Vielzahl von Wirtschaftsbereichen zunehmend an Bedeutung. Dabei wird die KI als unterstützende Technologie eingesetzt (vgl. Initiative Intelligente Vernetzung, 2019). Auch im Bereich der Polizei findet diese Technologie zunehmend Anwendung. In der Praxis wird bereits heute potenziell kinderpornografisches Material durch den Einsatz von KI vorselektiert, wodurch eine Reduktion der Datenmenge für die Auswertenden ermöglicht wird (vgl. LKA Niedersachsen, 2024). Eine der wiederkehrenden Zielsetzungen beim Einsatz von KI ist die Reduktion repetitiver Aufgaben für die Mitarbeitenden, um die Beschleunigung der Aufgabenbewältigung und somit eine Effizienzsteigerung zu erwirken. Folglich sind in der Betrachtung solche Aufgaben von Relevanz, die sich durch repetitive Muster und eine hohe Frequenz auszeichnen. Die Begrenzung personeller Ressourcen, die Verwaltung zunehmend größerer Datenmengen sowie der Wunsch nach einem Abbau der Bürokratie sind weitere Gründe für den Einsatz von KI (vgl. Parycek, Siegel, 2024).

In diesem Beitrag sollen speziell die Möglichkeiten des Einsatzes solcher Technologien bei der kriminalpolizeilichen Sachbearbeitung von Massendelikten der Alltagskriminalität betrachtet werden. Der Beitrag befasst sich mit der Frage, in welcher Form der Einsatz von KI die Sachbearbeitung von Ermittlungsvorgängen beschleunigen oder vereinfachen kann und welche Personalressourcen hierdurch freigesetzt werden könnten. Dies ist insbesondere vor dem Hinter-

grund der ansteigenden Aufgabenvielfalt im Zusammenhang mit den stetig sinkenden Einstellungszahlen relevant. Zudem werden die mit dem Einsatz von KI im Rahmen der Polizeiarbeit verbundenen Risiken beleuchtet. Die Sachbearbeitung von Massendelikten stellt ein besonders breites Anwendungsgebiet dar, da sie die gesamte kriminalpolizeiliche Praxis betrifft. Aus diesem Grund ist es von Bedeutung, diese Prozesse hinsichtlich einer Effizienzsteigerung durch den Einsatz von KI zu betrachten. Sollten dort personelle Ressourcen freigesetzt werden können, würden beispielsweise größere Ermittlungstiefen in anderen Vorgängen ermöglicht.

Hintergrund

Zunächst wird dargestellt, was die Sachbearbeitung der sogenannten Alltagskriminalität ausmacht und wie sich diese definiert. Der Begriff der Alltagskriminalität ist nicht eindeutig definiert, umfasst allerdings allgemein Delikte wie z. B. leichte Gewalttaten, sexuelle Übergriffe und Handlungen mit materiellen Folgen, wie z. B. Sachbeschädigung (vgl. Dammeyer, Falcone, 1999). Aber auch einfache Diebstahls- und Betrugsdelikte sind darunter zu fassen. Grundsätzlich sollen jene Delikte umfasst sein, welche von geringer Deliktschwere sind und verhältnismäßig häufig begangen werden (Massendelikte) (vgl. Lüdemann, 2002).

Eine Analyse der Polizeilichen Kriminalstatistik ergibt, dass ein signifikanter Anteil von etwa 53 % der registrierten Straftaten der sogenannten Alltagskriminalität zuzuordnen ist (7 % einfache Körperverletzung, 1,1 % Nötigung, 3,1 % Bedrohung, 19,7 % einfacher Diebstahl, 12,7 % Betrug und 9,4 % Sachbeschädigung) (vgl. Bundeskriminalamt, 2024). Darüber hinaus ist festzustellen, dass die polizeiliche Aufklärungsquote nur einen geringen Prozentsatz ausmacht (vgl. Bundeskriminalamt, 2024) und nur ein geringer Teil dieser Taten überhaupt zur Anklage kommt, da es sich in der Regel um Straftaten von geringer Schwere handelt oder der hinreichende Tatverdacht nicht konkret genug ist (Tab. 1).

	Taten nach PKS	Taten nach Verurteiltenstatistik	Quote der Verurteilten
Diebstahl	1.043.887	65.244	6,2 %
Betrug	801.412	65.129	8,1 %
Körperverletzung	399.699	29.278	7,3 %

Tabelle 1: Vergleich zwischen PKS (Bund) und Verurteiltenstatistik (vgl. Bundeskriminalamt, 2023; vgl. Statistisches Bundesamt, 2023)

In der Gesamtschau wird ersichtlich, dass es sich um eine hohe Anzahl von Arbeitsvorgängen handelt, die in der Masse einen hohen personellen Arbeitsaufwand erfordern und in einer Vielzahl von Fällen keine juristischen Konsequenzen nach sich ziehen (vgl. Brüggemann et al., 2016). Um die Betrachtung des Technologieeinsatzes in der kriminalpolizeilichen Sachbearbeitung nachvollziehen zu können, ist es zunächst erforderlich, die Arbeitsprozesse bei der Bearbeitung von einfachen Ermittlungsverfahren zu analysieren. Hierbei beziehen sich die nachfolgenden Ausführungen auf die Abläufe im Land Niedersachsen. In Anbetracht der Tatsache, dass die Grundlage der Ermittlungen auf Bundesgesetzen (StPO und StGB) beruht, lässt sich annehmen, dass die beschriebenen Abläufe mit denen in anderen Bundesländern vergleichbar sind. Der erste Schritt im Rahmen der strafrechtlichen Verfolgung einer Straftat stellt die Bekanntmachung der Straftat im Rahmen der Anzeigenaufnahme dar. Die Anzeige kann bei der Staatsanwaltschaft, der Onlinewache oder der Polizei erstattet werden. Im Rahmen der Anzeigenaufnahme erfolgen zunächst die Erhebung erster Informationen zum Sachverhalt, eine ggf. erforderliche Spurensicherung sowie die Befragung von Personen vor Ort (vgl. Niedersächsisches Landesjustizportal, 2024).

Die Prozesse, welche für die vorliegende Ausarbeitung von Relevanz sind, betreffen die weiteren Ermittlungen bzw. die weitere Sachbearbeitung. Die einfachen Ermittlungsvorgänge lassen sich dem Spektrum der bereits beschriebenen Alltagskriminalität zuordnen. Kennzeichnend ist, dass sie ohne nennenswerte Täterhinweise und Spuren aufgenommen werden. Diese Vorgänge stellen, wie bereits dargelegt, den quantitativ größten Anteil aller Ermittlungsvorgänge dar. Bei solchen Vorgängen sind durch die Sachbearbeitung insbesondere noch die folgenden Prozessschritte durchzuführen:

1. Sichten des im Rahmen der Anzeigenerstattung aufgenommenen Vorgangs nach Täterhinweisen oder Spuren.
2. Herstellung und Sicherung einer Datenqualität entsprechend den polizeilichen Richtlinien zum Zwecke der Übermittlung und Auswertung.
3. Ggf. gilt es insbesondere im Bereich der Betrugsdelikte, standardisierte Anfragen bei Internet Providern oder Diensteanbietern zu stellen, um Bestandsdaten zu täterseits verwendeten E-Mail-Adressen, Accounts oder IP-Adressen zu erhalten, welche weitere Ermittlungsschritte ermöglichen.
4. Rücksprache mit den Geschädigten und ggf. Einholen eines Strafantrages.
5. Zusammenfassung des Ermittlungsstandes im Rahmen eines kurzen Schlussvermerks
6. Abgabe des Vorgangs an die zuständige Staatsanwaltschaft

Nach bisherigem Stand erfolgen diese Schritte wenig automatisiert und ohne Einsatz nennenswerter technischer Unterstützung. Die Erfassung erfolgt in der Regel manuell durch die Sachbearbeitenden. Dazu werden vordefinierte Felder im Vorgangsbearbeitungssystem ausgefüllt, vorgefertigte Dokumente mit Auswahlfeldern generiert oder Texte (Abgabevermerk) verfasst (vgl. ZPD des Landes Niedersachsen, 2009).

Möglichkeiten von Künstlicher Intelligenz

KI wird in der Forschung und Praxis je nach Kontext und Perspektive unterschiedlich definiert. Wird der Begriff der KI sehr eng ausgelegt, liegt nach der Definition eine KI nur vor, wenn sie sich kaum oder gar nicht von einem Menschen unterscheidet (vgl. Turing, 1950). Dies wird auch „starke“ KI genannt. Bisher hat noch keine KI die von Turing entworfenen Voraussetzungen (Turing-Test) erfüllen können. Somit muss auf ein weniger enges Verständnis von KI zurückgegriffen werden.

Die Europäische Union hat sich erst kürzlich mit der Reglementierung von KI-Systemen befasst und definiert diese wie folgt: „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“ (Europäische Union, 2025). Diese bereits weiter gefasste Definition von KI fordert von KI nicht das Vermögen, menschlich zu denken, sondern lediglich aus Vorgegebenem Schlüsse ziehen zu können. Hiermit sind somit auch Systeme umfasst, die nur menschenähnliches Verhalten imitieren oder Vorgänge unterstützen. Hier schließt auch das sogenannte maschinelle Lernen, als Teilbereich der KI, an. Dabei wird KI als System definiert, das durch maschinelles Lernen aus Daten Muster erkennen und selbstständig lernen kann. KI wird dabei in erster Linie als Fähigkeit beschrieben, auf Basis von Erfahrung (Daten) zu lernen und sich anzupassen (vgl. SAP, 2024).

Noch weiter auszulegen ist bspw. die Definition von Russell und Norvig. In ihrem Buch „Artificial Intelligence: A Modern Approach“ definieren Russell und Norvig KI als das Entwickeln von „rationalen Agenten“ – Systemen, die autonom handeln, Wahrnehmungen verarbeiten und Aktionen durchführen, um ein bestimmtes Ziel zu erreichen (vgl. Russell, Norvig, 2021). In Anbetracht einer derart weit gefassten Definition können bereits Automatisierungssysteme von Prozessen als KI bezeichnet werden. Im Rahmen dieses Beitrags wird ein sehr weit gefasster Begriff von KI verwendet, da bereits einfache Automatisierungsfunktionen in der Vorgangserstellung einen Fortschritt gegenüber der bisherigen Erfassung und Bearbeitung darstellen.

Als besonders zu betrachtende Teildisziplin von KI sind für diesen Beitrag Large Language Models (LLMs) von Relevanz. Diese Sprachmodelle sind in der Lage, menschliche Sprache bzw. Texte zu generieren, zu analysieren und sprachbezogene Aufgaben ausführen. Die Erstellung der Ausgaben durch Large Language Models erfolgt auf Basis von Wahrscheinlichkeiten für den jeweils nächsten Token, wobei der Wahrheitsgehalt keine Berücksichtigung findet. Dies kann in Einzelfällen zu sogenannten Halluzinationen führen, d. h. Ausgaben, die nicht der Wahrheit entsprechen. Diese Problematik kann

durch die Bereitstellung eines Kontextes für das Sprachmodell bei der Antwortfindung vermindert werden. Als Kontext kann beispielsweise eine Menge an vorgegebenen Textdokumenten dienen, wie beispielsweise bei der Vorgangserstellung üblicher Berichte oder Formulare (vgl. Adams, 2024).

Unter anderem durch das Fraunhofer-Institut (vgl. Etscheid et al., 2020) ist bereits explizit der Sektor der öffentlichen Verwaltung hinsichtlich eines Einsatzes von KI betrachtet worden. In Bezug auf die (interne) Vorgangsbearbeitung werden hier Potenziale zur Effizienzsteigerung durch Automatisierung von wiederkehrenden Prozessen, der Erstellung von Protokollen oder auch das Konsolidieren von Daten aus unterschiedlichen Quellen genannt. Insgesamt kann festgehalten werden, dass KI in der Lage sein kann, Prozesse zu automatisieren, aus vorhandenen Daten eigene Schlüsse oder Analysen zu ziehen und dies durch Nutzung von LLMs in Schriftform wiederzugeben.

Methodik

Um der eingangs aufgestellten Fragestellung, inwiefern der Einsatz von KI die polizeiliche Sachbearbeitung von Massendelikten unterstützen kann, näherzukommen, wurde die wissenschaftliche Methodik der Expertenbefragung durchgeführt. Die Expertenbefragung ist eine qualitative Forschungsmethode, die eingesetzt wird, um detaillierte und fachkundige Einblicke in ein spezifisches Themengebiet zu gewinnen. Dies stellt auch die Anforderungen an die als Experten ausgewählten Personen dar. Um eine strukturierte und vergleichbare Erhebung zu gewährleisten, erfolgt die Befragung mithilfe eines kurzen, vorab entwickelten Fragebogens. Der Fragebogen umfasst acht Fragestellungen zu fünf Themenschwerpunkten. Die Fragen sind offen gestellt und umfassen inhaltlich die polizeiliche Sachbearbeitung von (einfachsten) Ermittlungsvorgängen und den Einsatz von KI. Dem Fragebogen ist eine Definition von KI und der Massendelikte der Alltagskriminalität vorangestellt. Dies ist für einheitliches Verständnis im Sinne der im Beitrag zugrunde gelegten Definition der beiden maßgeblichen Aspekte notwendig.

Die Auswahl der Experten erfolgt im Sinne des purposive sampling. Bei der Expertenbefragung wird purposive sampling genutzt, um gezielt Personen auszuwählen, die über spezialisiertes Wissen oder besondere Erfahrungen zu einem bestimmten Thema verfügen. Diese Methode stellt sicher, dass die Befragten relevante Einblicke liefern können. Einer der Experten verfügt über fundiertes Wissen und Erfahrung im Bereich der Polizeiarbeit, im Speziellen der Sachbearbeitung von Massendelikten der Alltagskriminalität. Hierbei handelt es sich um den Leiter einer Zentralen Ermittlungsgruppe (ZEG) im Kriminaldienst von Hannover. Die Ermittlungsgruppe bearbeitet u. a. den Telefonbetrug durch Callcenter. Neben umfänglichen Ermittlungsverfahren kommt es insbesondere zu einer sehr hohen Anzahl von Versuchstaten, bei denen Personen von Tätern angerufen werden, aber selbst die betrügerische Absicht des Anrufs erkannt haben. Die dominierenden Phänomene stellen hierbei die „falschen Polizisten“ und der „Enkeltrick“ dar. Im Jahr 2023 wurden in dieser ZEG knapp 5.000 Taten bearbeitet. Weiterhin wirkt der Experte in der Arbeitsgruppe (AG) Kripo, Teilprojekt „Automatisierte Bearbeitung von einfach(st) gelagerten Delikten ohne erfolgsversprechende Ermittlungsansätze“ mit.

Der weitere ausgewählte Experte ist Sachgebietsleiter im LKA Niedersachsen. In dem von ihm verantworteten Sachgebiet werden technische Lösungen unter Einsatz von KI für das Land Niedersachsen entworfen. Hier ist u. a. Software wie der „KiPo-Analyzer“ und dem „Tracebook KiPo“ zur KI-unterstützten Auswertung und Selektion von (kinder-)pornografischem Material entwickelt worden (vgl. LKA Niedersachsen, 2023).

Die Auswertung der Fragebögen erfolgte im Rahmen einer induktiven qualitativen Inhaltsanalyse (vgl. Mayring, 2022). Hierbei haben sich die auszuwertenden Kategorien direkt aus den vorstrukturierten Fragebögen ergeben und es wurden keine weiteren Theoriekonzepte zur Auswertung einbezogen. Der Fragebogen bildet folgende Kategorien ab:

- Möglichkeiten des Einsatzes von KI
- Herausforderungen
- Zukunftsperspektive

Zielsetzung bei der Kategorienbildung über den Fragebogen ist es, sowohl einen aktuellen als auch einen prognostischen Stand hinsichtlich der Untersuchungsfrage zu erlangen. Diese Methodik ermöglicht es, sowohl spezifische Fachkenntnisse als auch individuelle Meinungen zu sammeln, was zu einer fundierten und differenzierten Bewertung des KI-Einsatzes in der polizeilichen Sachbearbeitung von Massendelikten führt. Als Einschränkung ist der im Rahmen des Beitrags kleine Kreis von nur zwei befragten Experten zu nennen. Diese stellen zwei fundierte Einzelmeinungen dar, welche keine Generalisierung erlauben.

Ergebnisse

Zunächst sind beide Experten nach der Besonderheit bei der Bearbeitung von Massendelikten befragt worden. Der Experte des LKA hebt allgemein die Herausforderungen durch die hohe Fallmenge und den Mangel an Ressourcen hervor, ohne dabei spezifische Details zu nennen, da die Bearbeitung von Massendelikten nicht in seinen Zuständigkeitsbereich fällt. Der Leiter der ZEG beschreibt konkrete Probleme aus der Praxis: Die monotone Arbeit kann die Motivation des Personals senken, die Datenqualität muss trotz hoher Fallzahlen aufrechterhalten werden und zusätzliche Arbeit entsteht durch die Erfassung der Delikte über die Onlinewachen und der Protokolle aus dem Lagezentrum.

In der folgenden Fragestellung wurde sich mit Entlastungspotenzial durch den Einsatz von KI befasst. Der Sachgebietsleiter des LKA sieht den Nutzen von KI bei der Bearbeitung von Massendelikten vor allem in der Automatisierung wiederkehrender Arbeitsschritte, etwa durch Robotic Process Automation (RPA). Auch generative KI könne Texte wie Berichte und Abverfügungen vorformulieren, sodass Mitarbeitende nur noch die Qualität prüfen müssten. Aus der operativen Praxis heraus betont der andere Experte den Einsatz von Automatisierung speziell für einfach gelagerte Delikte ohne Ermittlungsansätze, etwa bei Diebstahl oder Sachbeschädigung. Seiner Einschätzung nach könnten bis zu 50 % aller Straftaten teilweise oder vollständig automatisiert bearbeitet werden. Hinsichtlich des

Entlastungspotenzials durch den Einsatz von KI befragt, gibt der Experte des LKA an, die Frage nicht valide beantworten zu können. Der andere Befragte schätzt, dass die Automatisierung von mindestens einem Drittel der Vorgänge die Kriminal- und Ermittlungsdienste erheblich entlasten könnte. Auch wenn eine Endkontrolle durch Sachaufsichten weiterhin nötig wäre, könnten so Kapazitäten der Sachbearbeitenden freigesetzt werden, wodurch die Belastung durch einfach gelagerte Delikte deutlich reduziert würde.

Der Experte des LKA sieht verschiedene Herausforderungen beim KI-Einsatz in der Bearbeitung von Massendelikten, darunter rechtliche Anforderungen (z. B. Datenschutzgesetze und EU-KI-Verordnung), technische und organisatorische Voraussetzungen sowie mögliche gesellschaftliche und interne Vorbehalte. Weitere Herausforderungen umfassen die Reproduzierbarkeit von Ermittlungsergebnissen und die Akzeptanz von KI-basierten Ergebnissen vor Gericht. Der ZEG-Leiter betont hinsichtlich der Herausforderungen die praktischen Bedenken: eine potenziell sinkende Aufklärungsquote, unzufriedene Bürger bei automatisierten Entscheidungen und mögliche Widerstände unter Kollegen, die sich durch KI überflüssig fühlen könnten. Er sieht auch die Gefahr, dass Fälle vorschnell zur automatisierten Bearbeitung weitergeleitet werden, um die eigene Arbeitslast zu verringern.

Als Ansätze zur Begegnung mit diesen Herausforderungen benennt der Experte des LKA, dass KI-Systeme so gestaltet sein sollten, dass sie allen rechtlichen und organisatorischen Anforderungen entsprechen. Herausforderungen könnte man durch gezielte Öffentlichkeitsarbeit und internes Change-Management angehen. Auch sollte die Erklärbarkeit der KI bei der Entwicklung und Beschaffung berücksichtigt werden. Der Leiter der ZEG schlägt diesbezüglich vor, ein leichtes Absinken der Aufklärungsquote zu akzeptieren, solange es im tolerierbaren Bereich bleibt. Offen bleibt hierbei, wie sich ein solch tolerierbarer Bereich definiert. Transparente Kommunikation mit Bürger:innen und eine klare interne Einbindung der Mitarbeitenden wären wichtig, damit diese sich auf ihre Kernaufgaben konzentrieren können und sich wertgeschätzt fühlen. Eine einheitliche

und nachvollziehbare Fachaufsicht bei der Zuteilung und Beurteilung der Vorgänge würde ebenfalls helfen, Akzeptanz für den KI-Einsatz zu schaffen.

Beide Experten wagen zudem einen prognostischen Blick in die Zukunft. Seitens des Experten des LKA wird in den kommenden fünf bis zehn Jahren eine zunehmende Nutzung technischer Assistenzsysteme, sowohl mit als auch ohne KI, zur Unterstützung der polizeilichen Sachbearbeitung gesehen. Diese Systeme sollen die Effizienz steigern und die Arbeitslast verringern. Der Leiter der ZEG hingegen geht aufgrund des demografischen Wandels, des Fachkräftemangels und steigender Fallzahlen (besonders durch Internetkriminalität) davon aus, dass der Druck auf die Polizei zur Effizienzsteigerung stark zunehmen wird. Er sieht drei mögliche Szenarien:

1. Minimaler Wandel: Nur geringe Verbesserungen werden umgesetzt, was jedoch zu einer Überlastung der Mitarbeitenden führen könnte.
2. Einsatz von KI und Automatisierung: Durch KI-gestützte Prozesse wird die Effizienz erhöht, sodass auch ein kleineres Personalaufkommen die Aufgaben bewältigen kann.
3. Nichtbearbeitung bestimmter Delikte: Geringfügige Delikte könnten künftig möglicherweise gar nicht mehr bearbeitet werden. Dies könnte jedoch die Akzeptanz der Polizei in der Bevölkerung negativ beeinflussen.

Abschließend benennt er dringenden Optimierungsbedarf bei ineffizienten Arbeitsabläufen in der Polizei. Er nennt als Beispiele die wenig intuitive Gestaltung der Systeme (PIAV, VBS), unnötige Papierprozesse und das Festhalten an überflüssiger Dokumentation. Er plädiert für Investitionen in die Automatisierung und eine Straffung der Abläufe, was die Effizienz steigern und die Ressourcen der Justiz und Polizei schonen könnte. Zudem kritisiert er die Entwicklung von IT-Lösungen in Form von kostengünstigen Inselprojekten, die später an anderer

Stelle höhere Kosten verursachen. Projekte, die langfristig entlasten könnten, wie der „Cyberguide“, würden oft nicht weiter gepflegt oder eingestellt, wodurch potenziell sinnvolle Lösungen verloren gingen.

Diskussion

Die beiden Experten sind sich einig, dass die Implementierung umfassender Automatisierungsfunktionen, ergänzt durch den Einsatz von LLMs, das Potenzial birgt, die Sachbearbeitung in der kriminalpolizeilichen Ermittlungsarbeit signifikant zu entlasten. Diese Einschätzung findet sich auch in anderen Befassungen zum KI-Einsatz in der öffentlichen Verwaltung wieder (vgl. Etscheid et al., 2020; Eichholz, 2020; Parycek, Siegel, 2024). Hervorzuheben ist die Betrachtung von Waldtmann (2024), welcher sich unmittelbar mit dem Einsatz von KI und der Automatisierung von Prozessen bei der Bearbeitung von Massendelikten auseinandersetzt und ebenfalls das Entlastungspotenzial durch den Einsatz von KI benennt. Der Leiter der ZEG schätzt die Möglichkeit der Arbeitserleichterung als sehr hoch ein. Diese Einschätzung findet ihre Bestätigung in der oben dargestellten quantitativen Verteilung der einfachen Kriminalität am Gesamtkriminalitätsgeschehen.

Es wird ersichtlich, dass ein vollständiger Verzicht auf eine menschliche Kontrollinstanz nicht möglich ist. Diesbezüglich ist zunächst die nicht gänzlich verlässliche Technologie zu nennen, wobei insbesondere das Phänomen der Halluzinationen zu berücksichtigen ist. Die Relevanz der Vermeidung von Halluzinationen der Systeme wird auch von Waldtmann (2024) betont, der ebenfalls auf den geringen Beweiswert vor Gericht für die automatisiert erledigten Aufgaben verweist. Darüber hinaus ist auch aus rechtlicher Perspektive die Präsenz einer Kontrollinstanz erforderlich.

Bei Betrachtung der oben dargestellten Prozesse lässt sich insbesondere bei den Aspekten der „Herstellung und Sicherung einer Datenqualität“, der „standardisierten Abfragen“, der „Zusammenfassung des Ermittlungsstandes“ und der „Abverfügung“ ein Einsatz von Automatisierung und LLMs als besonders zielführend identifizieren.

Der Einsatz von LLM ist in Bezug auf die Polizeiarbeit von Adams für den amerikanischen Raum untersucht worden. Er bestätigt die Auffassung der Experten und benennt unter anderem auch eine Effizienzsteigerung und qualitativ bessere Polizeiberichte durch den Einsatz von LLMs (vgl. Adams, 2024).

In Konsequenz dessen wäre die Fachaufsicht bzw. Sachbearbeitung lediglich mit einer Ein- und Ausgangskontrolle sowie der Bewertung des Vorgangs betraut. Dies hätte neben einer Steigerung der Effizienz der Vorgangsbearbeitung auch eine Entlastung von wenig attraktiver, repetitiver Arbeit zur Folge, was zu einer Steigerung der Arbeitszufriedenheit und möglicherweise auch zu einer Steigerung der Attraktivität des Berufsfeldes führen dürfte und Ressourcen für priorisierte Ermittlungsverfahren freisetzen könnte. Unter Berücksichtigung der Überlastung von Ermittlungsdienststellen sowie des zukünftig zu prognostizierenden Verlustes an Personal erscheint eine Automatisierung der Prozesse zunächst als eine durchaus erstrebenswerte Maßnahme. Andererseits wurde aufgezeigt, dass auch einfachste Vorgänge einen beträchtlichen quantitativen Umfang aufweisen. In der Konsequenz lässt sich ableiten, dass eine derart signifikante Reduktion von Aufgaben für diese Art von Vorgängen auch organisatorische Anpassungen und personelle Veränderungen in einzelnen Arbeitsbereichen nach sich ziehen würde. Die genannten organisatorischen Konsequenzen eröffnen Möglichkeiten zur Konzentration auf polizeiliche Kernaufgaben sowie zur Stärkung oder auch nur Kompensation eines Personalrückgangs in anderen Dienstzweigen. Es ist jedoch klar erkennbar, dass die gesamte Organisation durch den Einsatz solcher Technologien in einen umfassenden Veränderungsprozess involviert würde. Diese Einschätzung wird auch von Experten geteilt, die davon überzeugt sind, dass solche Veränderungen notwendig sind, um den Herausforderungen der Zukunft gerecht zu werden. Dieser Change-Prozess wird auch in der Literatur für unabdingbar erachtet und geht mit Qualifikation der Mitarbeitenden und einer Betrachtung der dann automatisierten Arbeitsabläufe vor dem Hintergrund einer weiteren Arbeitsverdichtung einher (vgl. Waldtmann, 2024).

In der bisherigen Diskussion wurden die konkreten rechtlichen, IT-infrastrukturellen und organisatorischen Abhängigkeiten und Folgen, die die flächendeckende Implementierung solcher Technologie für die Kriminalpolizei bedeuten würde, jedoch nur rudimentär betrachtet. Diesbezüglich wäre eine gesonderte und weitaus ausführlichere Auseinandersetzung erforderlich, die im Rahmen dieses Beitrags jedoch nicht geleistet werden kann.

Schlussfolgerungen

Aus diesen Ergebnissen lässt sich schlussfolgern, dass sich die öffentliche Verwaltung, in diesem Kontext auch die Polizei, nicht die Möglichkeit erlauben kann, die knappe und in der Regel hoch qualifizierte Ressource Mensch mit repetitiven Aufgaben zu belasten, welche bereits in der Praxis durch KI-Systeme in vergleichbarer Qualität bei deutlich geringerem Zeiteinsatz ausgeführt werden könnten. Fachkräftemangel und die Ansprüche der Mitarbeitenden erfordern einen überlegten, effizienten und sinnstiftenden Einsatz der Menschen. Gerade das Berufsfeld der Kriminalpolizei bietet solche sinnstiftenden Aufgaben, wenn KI-Systeme es ermöglichen, dass aus den Sachbearbeitenden wieder vornehmlich Ermittler werden.

In weiteren Schritten ist der Wandel insbesondere rechtssicher zu gestalten. Zudem müssen die Organisation sowie insbesondere die Mitarbeitenden von der Notwendigkeit und den Vorteilen überzeugt werden. Ängste sind ernst zu nehmen und Ressourcen und Kompetenzen sind dort einzusetzen, wo sie für die Bewältigung der polizeilichen Kernaufgaben erforderlich sind. Auch ist eine IT-Infrastruktur erforderlich, welche den Einsatz von KI in sämtlichen Arbeitsbereichen der Polizei überhaupt ermöglicht und eine flexible Anpassung an individuelle Prozesse erlaubt.

Es ist erkennbar, dass eine Organisation, welche sich bislang vornehmlich mit der Digitalisierung der zum Teil nach wie vor analogen Prozesse beschäftigt hat, nun auch mit der breiten Implementierung von KI in beinahe alle Verwaltungsprozesse konfrontiert wird. Eine flächendeckende Implementierung dieser Thematik ist jedoch

zukunftsweisend und aufgrund der hohen Anforderungen an die Polizeiarbeit in Korrelation mit den sinkenden Personalressourcen zwingend erforderlich.

Literaturverzeichnis

Adams, I. T. (2024). Large Language Models and Artificial Intelligence for Police Report Writing. CrimRxiv. DOI: 10.21428/cb6ab371.779603ee.

Brüggemann, K.-H.; Südbeck, B.; Maßmann, M. (2016). Rahmenvereinbarung über die Gewährleistung von Qualitätsstandards und Verfahrensvereinfachungen in der polizeilichen Bearbeitung von Fällen der leichten bis mittleren Kriminalität (Insbesondere sog. Massenkriminalität) Sowie in der Bearbeitung von Verkehrsstraftaten. Polizeiinspektion Emsland/Grafschaft Bentheim, Polizeiinspektion Osnabrück und Staatsanwaltschaft Osnabrück.

Bundeskriminalamt (2023). PKS 2022 Tabelle 01. bka.de/DE/AktuelleInformationen/StatistikenLagebilder/PolizeilicheKriminalstatistik/PKS2022/PKSTabellen/BundFalltabellen/bundfalltabellen.html?nn=211742 [abgefragt am: 05.11.2024].

Bundeskriminalamt (2024). PKS 2023 Tabelle 01. bka.de/DE/AktuelleInformationen/StatistikenLagebilder/PolizeilicheKriminalstatistik/PKS2023/PKSTabellen/pksTabellen_node.html [abgefragt am: 05.11.2024].

Dammeyer, M.; Falcone, V. (1999). (COM-4/015) Stellungnahme des Ausschusses der Regionen vom 18. November 1999 zum Thema 'Kriminalität und Sicherheit in den Städten'. edz.bib.uni-mannheim.de/www-edz/doku/adr/1999/cdr294-1999_fin_ac_de.pdf [abgefragt am: 26.05.2025].

Eichholz, C. (2020). Einsatz von Verfahren der Künstlichen Intelligenz in der öffentlichen Verwaltung. Veränderung der Anforderungen an die Bediensteten und Auswirkungen auf die Prozesse. Meißen: Hochschule Meißen (FH) und Fortbildungszentrum.

Etscheid, J.; von Lucke, J.; Stroh, F. (2020). Künstliche Intelligenz in der öffentlichen Verwaltung | Anwendungsfelder und Szenarien. In: Bauer, W. (Hg.). Fraunhofer-Institut für Arbeitswirtschaft und Organisation IAO. publica.fraunhofer.de/bitstreams/d3d9f520-1fd4-4516-98d6-a3370c134155/download [abgefragt am: 26.05.2025].

Europäische Union (2025). (2024/1689) Verordnung (EU) 2024/1689 des Europäischen Parlaments und des Rates vom 13. Juni 2024 zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz und zur Änderung der Verordnungen (EG) Nr. 300/2008, (EU) Nr. 167/2013, (EU) Nr. 168/2013, (EU) 2018/858, (EU) 2018/1139 und (EU) 2019/2144 sowie der Richtlinien 2014/90/EU, (EU) 2016/797 und (EU) 2020/1828 (Verordnung über künstliche Intelligenz).

Initiative Intelligente Vernetzung (Hg.) (2019). Künstliche Intelligenz Impulse zu einem Megatrend. bmwk.de/Redaktion/DE/Publikationen/Technologie/kuenstliche-intelligenz-impulse-zu-einem-megatrend.pdf?__blob=publicationFile&v=1 [abgefragt am: 26.05.2025].

Kero, S.; Akyürek, S. Y.; Golo Flaßhoff, F. (2023). Bekanntheit und Akzeptanz von ChatGPT in Deutschland. (Nr. 10) MeMo KI (Meinungsmonitor Künstliche Intelligenz). cais-research.de/wp-content/uploads/Factsheet-10-ChatGPT.pdf [abgefragt am: 26.05.2025].

LKA Niedersachsen (2024). Lagebild Cybercrime und Kinderpornografie in Niedersachsen 2023. Dezernat 62 Zentralstelle Cybercrime/Kinderpornografie. Hannover: LKA Niedersachsen.

Lüdemann, C. (2002). Massendelikte, Moral und Sanktionswahrscheinlichkeit: eine Analyse mit den Daten des ALLBUS 2000. Soziale Probleme. Zeitschrift für soziale Probleme und soziale Kontrolle, 13. Jahrgang (Heft 2), S. 128-155.

Mayring, P. (2022). Qualitative Inhaltsanalyse: Grundlagen und Techniken. (13., überarbeitete Auflage). Weinheim, Basel: Beltz.

Niedersächsisches Landesjustizportal. (2024). Die Einleitung und der Ablauf des Ermittlungsverfahrens. justizportal.niedersachsen.de/startseite/gerichte_und_staatsanwaltschaften/staatsanwaltschaften/ablauf_des_ermittlungsverfahrens/die-einleitung-und-der-ablauf-des-ermittlungsverfahrens-155739.html [abgefragt am: 05.11.2024].

Parycek, P.; Siegel, T. (2024). Von der Digitalisierung zur Automatisierung des Verwaltungsverfahrens. (Stand: 25.01.2024). Kompetenzzentrum Öffentliche IT, Fraunhofer-Institut für Offene Kommunikationssysteme FOKUS: Berlin. oeffentliche-it.de/documents/10181/14412/Von+der+Digitalisierung+zur+Automatisierung+des+Verwaltungsverfahrens [abgefragt am: 05.11.2024].

Russell, S. J.; Norvig, P. (2021). Artificial Intelligence: A Modern Approach. (Fourth Edition). Hoboken, NJ: Pearson.

SAP (2024). Was ist Machine Learning? sap.com/germany/products/artificial-intelligence/what-is-machine-learning.html [abgefragt am: 12.11.2024].

Statistisches Bundesamt (2023). Strafverfolgungsstatistik Deutschland, Verurteilte nach Anzahl. destatis.de/DE/Themen/Staat/Justiz-Rechtspflege/_inhalt.html#234460 [abgefragt am: 05.11.2024].

Turing, A. M. (1950). I.—Computing Machinery and Intelligence. *Mind*, LIX(236), S. 433-460. DOI: 10.1093/mind/LIX.236.433.

Waldtmann, C. (2024). Einsatz KI-basierter Technologien zur Bewältigung des polizeilichen Vorgangsaufkommens bei Massendelikten. In: Honekamp, W.; Labudde, D. (Hg.). *Polizei-Informatik 2024*. Remscheid: Rediroma-Verlag, S. 259-263.

ZPD des Landes Niedersachsen (2009). Richtlinie zur Standardisierung der Bearbeitungsprozesse im VBS NIVADIS. NIVADIS Richtlinie. Abteilung 4, Zentrale Polizeidirektion Niedersachsen. Hannover.

Potenziale der Nutzung von Large Language Models bei der Bearbeitung von gleichgelagerten Straftaten – Eine Szenarioanalyse am Beispiel der EG Corona

Christian Eggert

Die deutschen Polizeibehörden stehen angesichts von Krisen, demografischem Wandel und wachsenden Datenmengen vor der Herausforderung, mit sinkenden Personalressourcen ein steigendes Arbeitspensum zu bewältigen, insbesondere im Bereich der Auswertung und Bearbeitung von Straftaten. Technische Lösungen zur Effizienzsteigerung der kriminalpolizeilichen Sachbearbeitung können hierbei wesentliche Unterstützung leisten (Klotter, 2017). Besonders Potenzial zur Entlastung wird der Technologie der Large Language Models (LLMs) zugeschrieben. Es wird vermutet, dass der Einsatz von LLMs die Polizeiarbeit, insbesondere die Berichterstellung, erheblich verbessern könnte. Da nicht alle Beamten über ausgeprägte Schreibfähigkeiten verfügen, sollen LLMs präzisere und vollständigere Berichte generieren, was Ermittlungen und Gerichtsprozesse erleichtert. Zudem wird hierdurch eine Effizienzsteigerung erwartet, da Berichte schneller erstellt werden können, was Ressourcen spart und mehr Zeit für Kernaufgaben schafft (Adams, 2024, S. 2-4).

Besondere Herausforderungen ergeben sich, wenn krisenbedingte Kriminalitätsphänomene in großer Zahl auftreten und auf eine nicht dafür ausgelegte Sicherheitsarchitektur treffen. Ein Beispiel hierfür sind die Betrugs- und Subventionsbetrugsfälle, die das Landeskriminalamt der Polizei Berlin während der Corona-Pandemie bewältigen musste. Zur Zeit der Gründung der hierfür zuständigen Ermittlungsgruppe EG Corona standen LLMs als Technologie noch nicht zur Verfügung. Das Ziel dieses Beitrages ist es, mittels einer Szenarioanalyse zu untersuchen, inwiefern der Einsatz von LLMs die Bearbeitungszeit sowie die Qualität der Verfahren zu Betrugs- und Subventionsbetrugsfällen in Berlin beeinflusst hätte. Die EG Corona, eine Dienststelle, die bereits stark auf Effizienz ausgerichtet ist und standardisierte sowie teilweise automatisierte Bearbeitungsschritte nutzt, bietet eine besonders interessante Grundlage für diese Analyse. Die Ergebnisse dieser Untersuchung sollen die Potenziale und

Grenzen von LLMs für die kriminalpolizeiliche Bearbeitung gleichgelagerter Strafverfahren aufzeigen und eine fundierte Einschätzung ermöglichen, inwieweit diese Technologie zur weiteren Effizienzsteigerung der kriminalpolizeilichen Sachbearbeitung beitragen kann.

Hintergrund

Um die Besonderheiten der Bearbeitung in der EG Corona nachvollziehen zu können, werden diese zunächst detailliert beschrieben. Anschließend erfolgt eine Darstellung der zentralen Erkenntnisse zu LLMs.

Bearbeitung in der EG Corona

Der erste Lockdown in Deutschland während der Corona-Pandemie stellte eine bis dahin beispiellose Maßnahme des Staates dar. Um die wirtschaftlichen Folgen abzumildern, beschlossen die Bundes- und Landesregierungen verschiedene Hilfsprogramme, darunter die Hilfen der Soforthilfe II. In Berlin wurde ein unbürokratisches, voll-elektronisches Antragsverfahren eingeführt, was jedoch zahlreiche Betrugsfälle nach sich zog. Diese Entwicklung stellte das Landeskriminalamt Berlin vor die Herausforderung, die hohe Zahl von rund 11.000 Verfahren der Soforthilfe II innerhalb der fünfjährigen Verjährungsfrist zu bearbeiten – allesamt Fälle mit erheblichem Schaden und entsprechendem Ermittlungsaufwand.

Um innerhalb der Verjährungsfrist die Verfahren bearbeiten zu können, wurde eine standardisierte Bearbeitung entwickelt. Hierfür wurden sämtliche relevanten Antragsdaten in einer Verwaltungsdatenbank strukturiert erfasst. Dies war durch das bereits erwähnte vollelektronische Antragsverfahren einfach umzusetzen. Die Grundermittlungen und Abfragen der polizeilichen Informationssysteme wurden nach einem festen Schema durchgeführt und dokumentiert. Hierdurch lagen die verfahrensrelevanten Daten in einer strukturierten und immer gleichen Form vor. Die Strafanzeigen konnten so automatisiert erstellt werden. Der Anzeigentext ergab sich üblicherweise aus der vorgangsbegründenden Geldwäscheverdachtsmeldung.

Die sachbearbeitenden Ermittlerinnen und Ermittler mussten aus den in tabellarischer Form vorliegenden Ermittlungsergebnissen einen Abgabebereich für die Staatsanwaltschaft entwickeln. Hierfür gab es zwar in der Ermittlungsgruppe entwickelte Musterberichte, die aber je nach Fall und persönlichem Stil der bearbeitenden Dienstkraft angepasst wurden. Die EG Corona zeigt exemplarisch, wie groß der Aufwand bei der Erstellung von Berichten sein kann, selbst wenn standardisierte Verfahren und strukturierte Daten vorliegen (eigene Erhebung, 2024). An dieser Stelle könnten LLMs als innovative Technologie neue Wege eröffnen, um diesen Aufwand zu minimieren und die Berichterstellung zu optimieren.

Large Language Models

LLMs sind spezialisierte Systeme der Künstlichen Intelligenz (KI) im Bereich des Natural Language Processing (NLP), die aufgrund ihrer beeindruckenden Leistungsfähigkeit aktuell stark im Zentrum der Debatte um KI stehen. NLP ist ein Bereich der KI, der sich auf die maschinelle Analyse, die Verarbeitung und Erzeugung natürlicher Sprache konzentriert. LLMs beruhen auf künstlichen neuronalen Netzen (KNN). Generative Pre-Trained Transformer (GPT) gehören zu den prominentesten LLM-Systemen. Besonders die Firma OpenAI hat mit ihrem Chatbot ChatGPT und Modellen wie GPT-4 große Erfolge erzielt. Obwohl viele andere LLMs technisch ebenfalls zu den GPT-Systemen zählen, nutzt vor allem OpenAI den Begriff, um ihre eigenen Modelle zu kennzeichnen (Seemann, 2023, S. 11).

Die Einführung von vortrainierten Modellen wie Transformern ermöglichte die direkte Anpassung der Sprachmodelle, wodurch spezialisierte Architekturdiseins überflüssig wurden. Diese Entwicklung hat viele NLP-Aufgaben, z. B. Leseverständnis und Textlogik, erheblich verbessert. Ein zentrales Problem besteht jedoch darin, dass weiterhin umfangreiche, aufgabenspezifische Datensätze für das Feintuning nötig sind, was die Anwendbarkeit in der Praxis einschränkt. Ein Ansatz zur Überwindung dieser Herausforderung ist das Meta-Learning, bei dem Sprachmodelle wie GPT-3 die Fähigkeit entwickeln, kontextbezogen zu lernen. Dabei werden die LLMs anhand einer natürlichen Sprachanweisung oder weniger Korrekturen an Aufgaben

angepasst. GPT-3 beispielsweise zeigt hier hohe Kompetenzen, die oft mit oder sogar über denen feinabgestimmter Modelle liegen, etwa bei Frage-Antwort-Aufgaben (Brown et al., 2020, S. 3-6).

LLMs wie GPT-3 oder GPT-4 sind besonders fähig darin, kohärente und oft inhaltlich überzeugende Texte zu erstellen, wobei sie grundlegende sprachliche Kompetenzen wie Grammatik zuverlässig beherrschen. Sie verfügen über funktionale Fähigkeiten in begrenztem Maße. In Logik und Weltwissen treten jedoch immer wieder Fehler wie Halluzinationen oder fehlerhafte Berechnungen auf. Zudem fehlen ihnen ein Langzeitgedächtnis und aktuelles Wissen über ihre Trainingsdaten hinaus, was die Anwendbarkeit in der Praxis einschränkt. Der Umgang mit LLMs erfordert daher eine genaue Kenntnis ihrer Funktionsweise, um ihre Stärken zu nutzen und Fehlerquellen zu minimieren (Seemann, 2023, S. 27-30).

Methode

Zur Beantwortung der Forschungsfrage wurden eine Szenarioanalyse und mehrere Experteninterviews durchgeführt.

Instrumente der Szenarioanalyse

Die Szenarioanalyse ist eine strategische Methode, die dazu dient, mögliche Entwicklungen zu analysieren und ihre Auswirkungen auf Entscheidungen oder Strategien zu bewerten. Dabei wird nicht versucht, die Zukunft vorherzusagen, sondern ein Spektrum plausibler Entwicklungen zu entwerfen, um Unsicherheiten zu reduzieren und die Anpassungsfähigkeit zu erhöhen (Kosow, 2008, S. 10-16). Die Szenarioanalyse gliedert sich in mehrere aufeinander aufbauende Phasen, die systematisch durchgeführt werden, um plausible Entwicklungen zu erarbeiten.

Szenariofeldbestimmung

In der ersten Phase wird das Thema des Szenarios klar definiert. Es wird entschieden, welche Fragestellung behandelt und welche Grenzen gesetzt werden. Dabei wird das Betrachtungsfeld festgelegt. Im hiesigen Beitrag wird untersucht, welchen Einfluss der Einsatz von LLMs auf die Berichterstellung bei den Verfahren der Soforthilfe II in der EG Corona gehabt hätte. Hierbei liegt der Fokus auf dem potenziellen Nutzen und der konkreten Anwendbarkeit. Die rechtlichen und organisatorischen Rahmenbedingungen für die Nutzung von LLMs in der Polizei werden hier nur am Rande betrachtet.

Identifikation der Schlüsselfaktoren

Im nächsten Schritt werden zentrale Variablen, sogenannte Schlüsselfaktoren, identifiziert, die das Szenariofeld beschreiben oder beeinflussen. Die Auswahl dieser Faktoren ist entscheidend für die Tiefe und Relevanz des späteren Szenarios. Untersucht wird die Geeignetheit von LLMs für die Berichterstellung in der EG Corona. Zudem soll untersucht werden, ob ein Einsatz von LLMs tatsächlich effizienter, insbesondere schneller gewesen wäre und welchen Einfluss dies auf die Qualität der Berichte gehabt hätte.

Analyse der Schlüsselfaktoren

In dieser Phase werden mögliche zukünftige Ausprägungen der Schlüsselfaktoren analysiert. Diese Analyse findet sich im Kapitel „Ergebnisse“.

Szenariogenerierung

Die ermittelten Faktoren werden zu konsistenten Szenarien kombiniert. Dabei können narrative oder mathematische Methoden angewendet werden. Aufgrund der begrenzten kognitiven Verarbeitbarkeit wird die Anzahl der Szenarien meist begrenzt, um verschiedene Perspektiven und mögliche Entwicklungen abzubilden. In dem vorliegenden Beitrag wird sich auf das eine beschriebene Szenario beschränkt.

Szenariotransfer

Abschließend können die erstellten Szenarien weiterverwendet werden, z. B. für Wirkungs- oder Strategiebewertungen. Diese Phase wird jedoch nicht in allen Ansätzen als Teil des Szenarioprozesses betrachtet (Kosow, 2008, S. 20-24).

Experteninterview EG Corona

Die für die Szenarioanalyse notwendigen Erkenntnisse zu LLMs ergeben sich aus der einschlägigen Literatur. Für die Daten die EG Corona betreffend wurden Experteninterviews durchgeführt, da es hierzu nicht genügend öffentlich zugängliche Informationen gibt.

Das Experteninterview ist ein qualitatives methodisches Instrument, um gezielt Wissen und Erfahrungen von Personen zu erheben, die über spezielles Fachwissen oder spezifische Erfahrungen in einem bestimmten Bereich verfügen. Es wird insbesondere dann gewählt, wenn die Forschung ein tiefgehendes Verständnis komplexer Zusammenhänge erfordert, die durch standardisierte Methoden wie Umfragen nicht adäquat abgebildet werden können (Bogner et al., 2014).

Zum einen wurden der Kommissariatsleiter der EG Corona und zum anderen vier sachbearbeitende Dienstkräfte mit unterschiedlicher Diensterfahrung und Verweildauer auf der Dienststelle befragt. Die Befragung erfolgte per E-Mail mittels eines qualitativen Fragebogens. In Abstimmung mit der Dienststelle wurde sich für diese Form des Interviews entschieden, da es neben dem reduzierten organisatorischen Aufwand die Möglichkeit bietet, die Fragen länger zu reflektieren und zielgenau zu beantworten. Das Interview zielt darauf ab, die Arbeitsprozesse und Herausforderungen der EG Corona sowohl auf strategischer als auch auf operativer Ebene zu analysieren. Dabei liegt der Fokus auf der Effizienzsteigerung, der Nutzung technischer Hilfsmittel und der Identifikation von Optimierungspotenzialen, insbesondere im Kontext der Bearbeitung von Verfahren der

Soforthilfe II. Die gesammelten Daten sollen als Grundlage dienen, um den hypothetischen Einsatz von LLMs bewerten zu können. Die Fragen sind in der untenstehenden Tabelle 1 aufgeführt.

Fragebogen	Nr.	Frage
Führungskraft	1	Bitte beschreiben Sie kurz das Delikt und dessen Phänomenologie, das zur Gründung der EG Corona führte. Gehen Sie bitte dezidiert auf die Verfahren der Soforthilfe II ein.
	2	Welche technischen Mittel zur Effizienzsteigerung werden in der EG Corona genutzt?
	3	Wie viele Verfahren der Soforthilfe II werden insgesamt in der EG Corona bearbeitet und wie viele Dienstkräfte sind über welchen Zeitraum damit beschäftigt?
	4	Wie sehen die Bearbeitungsschritte eines Verfahrens zur Soforthilfe II typischerweise aus und wie viel Zeit nimmt die Erstellung des Abgabeberichtes in der Regel in Anspruch? Sind Arbeitsschritte standardisiert worden?
Sachbearbeitung	1	Nutzen Sie Hilfsmittel (auch technische), um die Erstellung des Abgabeberichtes zu Verfahren der Soforthilfe II effizienter zu gestalten?
	2	Wie lange benötigen Sie üblicherweise für die Erstellung eines Abgabeberichtes? Versuchen Sie bitte die Frage möglichst konkret zu beantworten.
	3	Was sind die wesentlichen Herausforderungen bei der Erstellung eines Abgabeberichtes?

Tabelle 1: Fragen der Experteninterviews

Ergebnisse

Nachfolgend werden die Überlegungen und Ergebnisse der Szenarioanalyse dargestellt.

Anwendbarkeit von LLMs in der EG Corona

Im Hinblick auf die Geeignetheit und Anwendbarkeit von LLMs bei der Berichterstellung in der EG Corona gibt es zwei wesentliche Problemfelder zu betrachten. Zum einen ist die Frage zu klären, welche technischen Voraussetzungen gegeben sein müssten, um LLMs für

den beschriebenen Anwendungsfall zu nutzen. Zum anderen muss geklärt werden, ob LLMs für die beschriebene Aufgabe als Technologie überhaupt geeignet sind.

Viele marktverfügbare Anwendungen von LLMs sind cloud-basiert (Pröhl et al., 2023, S. 1100-1102), was an gewisse Voraussetzungen geknüpft ist. Fraglich ist, ob solche Lösungen für die Polizei infrage kommen. Hierfür müsste die Polizei über eine IT-Infrastruktur verfügen, die Cloud-Dienste und APIs (Schnittstellen) unterstützt, um eine reibungslose Integration der Anwendungen zu gewährleisten. Gleichzeitig ist es wichtig, dass die eingesetzten Modelle zuverlässig, präzise und für Echtzeitanwendungen geeignet sind. Die Nutzung externer IT-Infrastruktur verursacht fortwährend Kosten, bietet aber gleichzeitig den Vorteil, dass der Anbieter für das Funktionieren der Anwendung zu sorgen hat. Die Nutzung dieser Anwendungen bringt jedoch auch Herausforderungen mit sich. Datenschutz und Datensicherheit spielen eine zentrale Rolle, insbesondere bei sensiblen Informationen wie personenbezogenen Daten oder Dokumenten aus Strafverfahren, die einem besonderen Schutz unterliegen. Die Abhängigkeiten von spezifischen Anbietern bergen ein erhebliches Risiko für unvorhergesehene Kostensteigerungen und mangelnde Kontrolle durch die Polizei. Für eine erfolgreiche Einführung empfiehlt sich ein strukturiertes Vorgehen. Nach einer Analyse der Anforderungen sollten geeignete Anbieter recherchiert und bewertet werden. Ein Proof-of-Concept hilft, die tatsächliche Eignung der Lösungen zu testen. Die Implementierung sollte schrittweise erfolgen, begleitet von kontinuierlicher Überwachung und Anpassung. Mit dieser Strategie könnten Polizeibehörden die Potenziale cloud-basierter KI-Anwendungen effektiv nutzen und gleichzeitig Risiken minimieren (Pröhl et al., 2023, S. 1100-1105).

Es wäre aber auch möglich, vortrainierte Open-Source-LLMs auf polizeieigener Hardware zu betreiben. Open-Source-LLMs bieten eine Reihe von Vorteilen gegenüber kommerziellen Modellen, obwohl letztere derzeit in vielen Bereichen führend sind. Ein entscheidender Vorteil ist die Unabhängigkeit von externen Diensteanbietern, die Preise erhöhen, Dienste einstellen oder Modelle entfernen könnten. Zudem bleiben alle Daten innerhalb des eigenen Polizeinetzwerks,

wodurch der Schutz sensibler Informationen und Codes gewährleistet ist. Dies ermöglicht die sichere Verarbeitung auch vertraulicher Daten mit solchen Modellen. Kosten für Open-Source-LLMs entstehen nicht durch die Nutzung – etwa basierend auf der Anzahl der verarbeiteten Tokens oder durch Abonnements –, sondern durch die Betriebskosten der eigenen Infrastruktur, mögliche Anschaffungen sowie den Aufbau der erforderlichen Kompetenzen. Je nach Anwendungsfall kann dies eine kostengünstigere Lösung darstellen. Ein weiterer Vorteil liegt in der Transparenz: Viele Details zu Open-Source-Modellen sind bekannt, was das Vertrauen in ihre Anwendung erhöht. Darüber hinaus können diese Modelle feinjustiert werden, um spezifischen Anforderungen gerecht zu werden. Für besondere Einsatzgebiete, wie die Nutzung in der deutschen Sprache oder in der medizinischen Forschung, gibt es bereits spezialisierte, feinabgestimmte Open-Source-Modelle. Die aktive Community rund um Open-Source-LLMs trägt ebenfalls zu ihrem Mehrwert bei. Neben einer großen Auswahl an Modellen stehen zahlreiche hochwertige Bibliotheken und Tools zur Verfügung, die den Einsatz und die Anpassung dieser Modelle erleichtern (Honroth et al., 2024, S. 2).

Beide Ansätze, ließen sich für polizeiliche Anwendungen und damit auch für die Vorgangsbearbeitung in der EG Corona umsetzen. Darüber hinaus muss das verwendete LLM für die spezifische Aufgabe der Erstellung des Abgabeberichtes geeignet sein, beziehungsweise darauf angepasst werden. Das Trainieren eines Sprachmodells auf spezifische Aufgaben hin ist sehr rechen- und ressourcenintensiv und damit sehr teuer (Bharathi Mohan et al., 2024, S. 5054).

Wesentlich für die Berichterstellung ist das kohärente Sprachverständnis, was aktuelle Pre-Trained LLMs bereits beherrschen. Für die Anpassung auf die Abgabeberichte der EG Corona gäbe es die Ansätze des Fine-Tunings, der Content Injection und des Prompt-Engineerings.

Fine-Tuning ermöglicht es, ein Modell mit zusätzlichen spezifischen Datensätzen weiter zu trainieren. Das ist jedoch kostenintensiv und oft nur begrenzt effektiv, da neue Datenmengen meist deutlich kleiner als das ursprüngliche Pre-Training-Datenset sind. Content Injec-

tion hingegen integriert spezifisches Wissen direkt in die Abfrage, indem relevante Informationen dynamisch eingefügt werden, was flexibler, aber durch die maximale Eingabelänge begrenzt ist. Eine vorgeschaltete KI oder Vektordatenbank kann helfen, relevante Inhalte effizient auszuwählen und einzubinden. Dabei ist es entscheidend, den Aufwand und die Anwendungsfälle zu berücksichtigen. Fine-Tuning eignet sich für langlebige, tief integrierte Anpassungen, während Content Injection besser für dynamische, aufgabenspezifische Abfragen geeignet ist (Reinking & Becker, 2023, S. 2-14).

Prompt-Engineering ist eine Technik, um vortrainierte Sprachmodelle für spezifische Aufgaben zu nutzen, indem die Eingabe (Prompt) so gestaltet wird, dass sie die gewünschte Antwort hervorruft. Es beinhaltet die Umwandlung der Aufgabe in ein Format, das das Modell bereits durch sein Pre-Training kennt, wie beispielsweise das Erstellen von Lückentexten oder spezifischen Vorlagen. Diese Methode ermöglicht oft wenige oder keine zusätzlichen Trainingsdaten und eignet sich für Szenarien mit begrenzten Ressourcen oder Daten. Die Auswahl geeigneter Prompts ist entscheidend für die Modellleistung (Liu et al., 2021, S. 4-5). LLMs können hierbei durch In-Context-Learning (ICL) noch bessere Ergebnisse erzielen. Hierbei wird dem LLM beim Prompting ein Muster zur Verfügung gestellt, anhand dessen das Ergebnis kontextualisiert wird (Dong et al., 2022, S. 1).

In der EG Corona liegen die Daten mit den Ermittlungsergebnissen in strukturierter Form vor und es gibt Musterberichte. Beides kann für das Prompten genutzt werden. Grundsätzlich spielen LLMs ihre Stärken bei der Verarbeitung unstrukturierter Daten aus (Gill et al., 2024, S. 3-4). Die Nutzung von strukturierten Daten für das Prompten unter Einbeziehung der Musterberichte lassen in Anbetracht der Sprachleistung von LLMs konsistente und zuverlässige Ergebnisse erwarten. Dass sich polizeiliche Berichte mittels Prompt-Engineering ohne spezifisches Training durch ChatGPT 4 erfolgreich erstellen lassen, hat Adams (2024) bereits zeigen können.

Effizienz und Qualität der Berichterstellung

Um die Effizienz und Qualität des Einsatzes von LLMs im Vergleich bewerten zu können, wurde durch die Interviews der Stand in der EG Corona erhoben. Die Befragten nutzen unterschiedliche Hilfsmittel, um die Effizienz bei der Erstellung von Abgabeberichten zu Verfahren der Corona-Soforthilfe II zu steigern. Häufig kommen Bearbeitungsvorlagen mit vorformulierten Textbausteinen, Drop-Down-Feldern oder Formularen zum Einsatz. Einige setzen auf die Wiederverwendung bereits geschriebener Berichte, während andere die rollierende Bearbeitung mit Drag-and-Drop-Optionen bevorzugen. Die Zeit für die Erstellung eines Abgabeberichts variiert stark in Abhängigkeit von der Komplexität der Fälle. Bei einfachen Sachverhalten wird die Bearbeitungsdauer auf 20 Minuten bis eine Stunde geschätzt, während komplexere Fälle zwei bis acht Stunden in Anspruch nehmen können. Dabei spielen die Anzahl und Vielfalt der Anträge sowie vorliegende Unterlagen wie Kontoumsätze eine entscheidende Rolle. In der Regel wird von einem Zeitansatz von mindestens einer Stunde für die Erstellung der Abgabeberichte ausgegangen.

Fragen	Antwort SB 1	Antwort SB 2	Antwort SB 3	Antwort SB 4
Hilfsmittel	Bearbeitungsvorlage, Textbausteine, Drop-Down-Felder	Bearbeitungsvorlage mit Drop-Down-Optionen	Rollierende Bearbeitung, Drag'n'Drop-Formular	Vorlage bestehender Berichte, keine Technik
Bearbeitungszeit	Ø 1,5 Std., einfache Fälle: 20 Min., komplexe: mehrere Stunden	2 bis 8 Std., je nach Unterlagen und Komplexität	Einfache: 1 Std., komplexe: 2 bis 3 Std.	Einfache: 1 Std., komplexe: 2 bis 3 Std.
Herausforderungen	Nachweis und Formulierung der Täuschungsabsicht	Querverbindungen, Beweise bei Strohleuten	Entscheidung über Berechtigung von Anträgen	Strukturierte Zusammenfassung der Ergebnisse

Tabelle 2: Zusammenfassung der Beantwortung der Interviews der Sachbearbeitenden (SB)

Die Berichterstellung in der EG Corona zeigt sich trotz aller Optimierungen als zeitintensiver Prozess. LLMs könnten diesen Prozess erheblich beschleunigen. Durch die Fähigkeit, strukturierte Daten

direkt in kohärente und vollständige Berichte umzuwandeln, ließe sich die Bearbeitungszeit deutlich reduzieren. Die Abgabeberichte könnten nahezu in Echtzeit generiert werden (Sun et al., 2024). Dies würde den Sachbearbeitenden mehr Kapazitäten für die Analyse und Bewertung von Ermittlungsergebnissen schaffen.

Zur Illustration des Einsparpotenzials wird die nachfolgende hypothetische und stark vereinfachende Rechnung aufgestellt (siehe Abbildungen 1 und 2). Unter Annahme einer optimistisch geschätzten durchschnittlichen Zeit von anderthalb Stunden für die Erstellung der Abgabeberichte ergibt sich eine Gesamtzeit für diesen Arbeitsschritt bei den 10.887 Verfahren der Soforthilfe II von 16.331 h. Acht Sachbearbeitende sind demnach bei einem Arbeitstag von acht Stunden 255 Arbeitstage und damit ein Jahr nur mit diesem Arbeitsschritt beschäftigt. Nimmt man an, dass sich inklusive der Qualitätskontrolle die Zeit durch den Einsatz von LLMs auf eine halbe Stunde reduziert, würde sich diese Zeit auf etwa vier Monate reduzieren.

<p>T: Gesamtzeit für den Arbeitsschritt (in Stunden)</p> <p>N: Anzahl der Verfahren (10.887)</p> <p>t: Zeit pro Verfahren ohne LLM (1,5 Stunden)</p> <p>t_{LLM}: Zeit pro Verfahren mit LLM (0,5 Stunden)</p> <p>A: Anzahl der Sachbearbeiter:innen (8)</p> <p>h_{day}: Arbeitsstunden pro Tag (8)</p> <p>d_{year}: Arbeitstage pro Jahr (255)</p>	<p>Formeln zur Berechnung:</p> <p>1. Gesamtzeit ohne LLM:</p> $T = N \cdot t$ <p>2. Gesamtzeit mit LLM:</p> $\bar{T}_{LLM} = N \cdot t_{LLM}$ <p>3. Benötigte Arbeitstage ohne LLM:</p> $D = \frac{T}{A \cdot h_{day}}$ <p>4. Benötigte Arbeitstage mit LLM:</p> $D_{LLM} = \frac{\bar{T}_{LLM}}{A \cdot h_{day}}$ <p>5. Arbeitszeitersparnis (in Tagen):</p> $\Delta D = D - D_{LLM}$	<p>Einsetzen der Werte:</p> <p>1. Ohne LLM:</p> $T = 10.887 \cdot 1,5 = 16.330,5 \text{ h}$ $D = \frac{16.330,5}{8 \cdot 8} = 255 \text{ Arbeitstage}$ <p>2. Mit LLM:</p> $\bar{T}_{LLM} = 10.887 \cdot 0,5 = 5.443,5 \text{ h}$ $D_{LLM} = \frac{5.443,5}{8 \cdot 8} = 85 \text{ Arbeitstage}$ <p>Fazit:</p> <p>Die Arbeitszeitersparnis beträgt:</p> $\Delta D = 255 - 85 = 170 \text{ Arbeitstage.}$
-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Abbildung 1: Berechnung des Einsparpotenzials

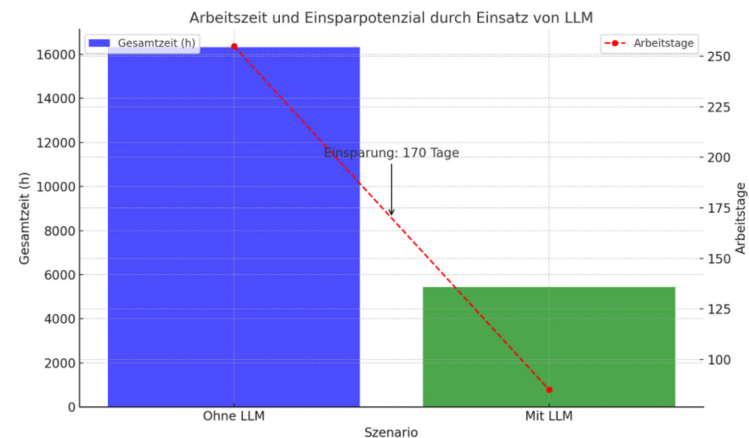


Abbildung 2: Visualisierung der Einsparung bei acht SB

Zu den größten Herausforderungen werden die Nachweisführung und die Formulierung der Betrugsabsicht, die Entscheidung über die Berechtigung eines Antrags sowie die übersichtliche Darstellung von Querverbindungen zwischen Anträgen durch die befragten Dienstkräfte angeführt. Auch die Strukturierung und Zusammenfassung aller Ergebnisse wird als anspruchsvoll beschrieben (siehe Tabelle 2). Die Bewältigung dürfte maßgeblich mit der kriminalistischen Erfahrung und Übung beim Schreiben von Berichten der Sachbearbeitenden zusammenhängen. Neben der Effizienzsteigerung bietet der Einsatz von LLMs auch Potenziale zur Verbesserung der Qualität der Berichte. LLMs erzeugen standardisierte und konsistente Berichte, die sowohl inhaltlich präzise als auch sprachlich korrekt sind. Durch den Human-in-the-Loop-Ansatz, die Rückmeldung von Menschen bei der Anwendung von LLMs, können die Ergebnisse weiter verbessert werden (Wu et al., 2022, S. 369-370).

Bei der Nutzung von LLMs zur Erstellung von Arztbriefen konnte bereits in einer Studie gezeigt werden, dass auf diese Weise erstellte Texte in 93,1 % der Fälle qualitativ hochwertig waren, sodass nur minimale Anpassungen notwendig waren (Heilmeyer et al., 2024, S. 5-6). Es scheint plausibel, dass bei der Wahl des richtigen LLM ähnliche Ergebnisse in der kriminalpolizeilichen Berichterstellung zu erwarten sind.

Diskussion

Das Ergebnis der Szenarioanalyse zeigt, dass die Nutzung von LLMs zur Berichterstellung geeignet gewesen wäre, um die Effizienz der Berichterstellung in der EG Corona zu steigern. Eine zentrale Erkenntnis der Analyse ist das mögliche Einsparungspotenzial an Zeit bei der Erstellung von Abgabeberichten. Die hypothetische Reduktion der Bearbeitungszeit um bis zu zwei Drittel illustriert den potenziellen praktischen Mehrwert dieser Technologie. Besonders in Fällen mit hohen Fallzahlen, wie in der EG Corona, könnte dies zu einer Entlastung der Sachbearbeitenden beitragen und zusätzliche Kapazitäten für andere Aufgaben schaffen.

Zeitgleich ist jedoch festzuhalten, dass die Annahmen dieser Analyse auf hypothetischen Szenarien und begrenzten Daten basieren. Die zugrunde gelegten Schätzungen zur Effizienzsteigerung durch LLMs beruhen auf der Voraussetzung, dass die Integration der Technologie nahtlos und ohne größere Hindernisse erfolgt. Untersuchungen von Adams et al. (2024) haben gezeigt, dass eine Effizienzsteigerung bei der polizeilichen Berichterstellung durch die Nutzung von LLMs nicht der Fall sein muss. In der Studie konnten keine signifikanten Zeitersparnisse durch den Einsatz von LLMs bei der polizeilichen Berichterstellung festgestellt werden. Wobei hier zu beachten ist, dass in dieser Studie Berichte anhand unstrukturierter Daten mit dem kommerziell verfügbaren cloud-basierten Produkt „Draft One“ der Firma Axon erstellt worden sind. Ein wesentlicher Zeitfaktor war hier die Eingabe in das Vorgangsbearbeitungssystem (Adams et al., 2024, S. 10-14). Diese Einschränkungen lägen bei den Abgabeberichten, wie sie in der EG Corona gefertigt werden, nicht vor. Das heißt, die hier ermittelten Zeitersparnisse und Einflüsse auf die Qualität sind fundiert, bedürfen aber einer praktischen Überprüfung.

Die hier durchgeführte Szenarioanalyse stützt sich überwiegend auf Literatur aus dem Bereich der Technologieentwicklung und auf Studien mit spezifischen Anwendungsfällen. Es gibt bisher kaum Untersuchungen im kriminalpolizeilichen Kontext. Aus diesem Grund wurde hier die Berichterstellung in der EG Corona mit anderen Kontexten, wie beispielsweise der Erstellung von Arztbriefen, vergli-

chen. Obwohl es Parallelen in der Notwendigkeit strukturierter und präziser Berichte gibt, handelt es sich um unterschiedliche Anwendungsbereiche mit spezifischen Anforderungen. Es muss kritisch betrachtet und überprüft werden, inwieweit Ergebnisse aus Studien wie die von Heilmeyer et al. (2024) im medizinischen Bereich auf die kriminalpolizeiliche Berichterstellung übertragen werden können.

Zudem sollte berücksichtigt werden, dass nicht alle Herausforderungen der Berichterstellung allein durch den Einsatz von LLMs bewältigt werden können. Insbesondere komplexe Aufgaben erfordern kriminalistische Expertise, die von LLMs nicht komplett ersetzt werden kann. Auch die Fähigkeit, Querverbindungen zwischen Fällen zu erkennen und zu analysieren, bleibt weitgehend eine Aufgabe der Ermittlerinnen und Ermittler. Der Human-in-the-Loop-Ansatz verspricht hier die besten Ergebnisse.

Schlussfolgerungen

Die Untersuchung lässt den Schluss zu, dass der Einsatz von LLMs selbst bei stark effizienzorientierten und standardisierten Dienststellen wie der EG Corona erhebliches Potenzial für eine Effizienz- und Qualitätssteigerung birgt. Um die hypothetischen Ergebnisse zu validieren, sollten zukünftig empirische Studien anhand der tatsächlichen Nutzung von LLMs zur kriminalpolizeilichen Berichterstellung durchgeführt werden. Hierfür bieten sich insbesondere Dienstbereiche an, die über strukturierte Daten zu den Ermittlungen und entsprechende Musterberichte verfügen. Die Auswahl von Open-Source-LLMs unter Nutzung von Prompt-Engineering und ICL können eine niedrigschwellige Möglichkeit sein, LLMs polizeilich nutzbar zu machen. Die testweise Nutzung in spezialisierten Dienstbereichen bietet die Chance, Erfahrungen zu sammeln und die Technologie schrittweise auf weitere Bereiche der kriminalpolizeilichen Sachbearbeitung auszuweiten.

Der Beitrag empfiehlt eine schrittweise Einführung von LLMs, begleitet von Tests in der Praxis und einer kontinuierlichen Evaluation. Gleichzeitig erfordern Datenschutz, technische Anforderungen und

die Integration kriminalistischer Expertise eine sorgfältige Planung. Die Entwicklungen im Bereich generativer KI und LLMs sind derzeit sehr dynamisch, sodass zu erwarten ist, dass die verfügbaren Modelle immer leistungsfähiger werden (Adams, 2024, S. 15).

Literaturverzeichnis

- Adams, I. T. (2024). Large Language Models and Artificial Intelligence for Police Report Writing. *CrimRxiv*. Vorab-Online-Publikation. doi.org/10.21428/cb6ab371.779603ee
- Adams, I. T., Barter, M., McLean, K., Boehme, H. & Geary, I. A. (2024). No Man's Hand: Artificial Intelligence Does Not Improve Police Report Writing Speed. *CrimRxiv*. Vorab-Online-Publikation. doi.org/10.21428/cb6ab371.4a6d42e9
- Bharathi Mohan, G., Prasanna Kumar, R., Vishal Krishh, P., Keerthinathan, A., Lavanya, G., Meghana, M. K. U., Sulthana, S. & Doss, S. (2024). An analysis of large language models: their impact and potential applications. *Knowledge and Information Systems*, 66(9), 5047-5070. doi.org/10.1007/s10115-024-02120-8
- Bogner, A., Littig, B. & Menz, W. (2014). *Interviews mit Experten*. Springer Fachmedien Wiesbaden. doi.org/10.1007/978-3-531-19416-5
- Brown, T. B., Mann, B. & Ryder, N. et al. (2020). Language Models are Few-Shot Learners. *arxiv.org/pdf/2005.14165v4*
- Dong, Q., Li, L., Dai, D., Zheng, C., Ma, J., Li, R., Xia, H., Xu, J., Wu, Z., Liu, T., Chang, B., Sun, X. & Sui, Z. (2022). A Survey on In-context Learning. *arxiv.org/pdf/2301.00234v6*
- Gill, J. K., Chetty, M., Lim, S. & Hallinan, J. (2024). Large language model based framework for automated extraction of genetic interactions from unstructured data. *PloS one*, 19(5), e0303231. doi.org/10.1371/journal.pone.0303231
- Heilmeyer, F., Böhringer, D., Reinhard, T., Arens, S., Lyssenko, L. & Haverkamp, C. (2024). Viability of Open Large Language Models for Clinical Documentation in German Health Care: Real-World Model Evaluation Study. *JMIR medical informatics*, 12, e59617. doi.org/10.2196/59617

Honroth, T., Siebert, J. & Kelbert, P. (19. Januar 2024). Open Source Large Language Models selbst betreiben. Fraunhofer IESE. [iese.fraunhofer.de/blog/open-source-large-language-models-selbst-betreiben/?utm_source=chatgpt.com](https://www.iese.fraunhofer.de/blog/open-source-large-language-models-selbst-betreiben/?utm_source=chatgpt.com)

Klotter, G. (2017). Polizei im Umbruch – Herausforderungen und Zukunftsstrategien: Polizei ist Ländersache – Polizeiarbeit im Spannungsfeld zwischen Ressourcenwirklichkeit und gesellschaftlichem Anspruch. Bundeskriminalamt. BKA Herbsttagung vom 15. – 16. November 2017. [polizei.de/SharedDocs/Downloads/DE/Publikationen/Herbsttagungen/2017/herbsttagung2017KlotterLangfassung.pdf?__blob=publicationFile&v=2](https://www.polizei.de/SharedDocs/Downloads/DE/Publikationen/Herbsttagungen/2017/herbsttagung2017KlotterLangfassung.pdf?__blob=publicationFile&v=2)

Kosow, H. (2008). Methods of future and scenario analysis: Overview, assessment, and selection criteria. *Studies*: Bd. 39.

Liu, P., Yuan, W., Fu, J., Jiang, Z., Hayashi, H. & Neubig, G. (2021). Pre-train, Prompt, and Predict: A Systematic Survey of Prompting Methods in Natural Language Processing. doi.org/10.48550/ARXIV.2107.13586

Pröhl, T., Baumgartner, S. & Zarnekow, R. (2023). Cloud-basierte KI-Anwendungen für Natural Language Processing: Marktüberblick und Vorstellung von typischen Anwendungsfällen für den Mittelstand. *HMD Praxis der Wirtschaftsinformatik*, 60(5), 1093-1107. doi.org/10.1365/s40702-023-00994-w

Reinking, E. & Becker, M. (2023). Einsatzmöglichkeiten von KI in Unternehmen – Zeitnah erreichbare Personalisierung von Large Language Models (wie ChatGPT) in Zeiten der Industrie 5.0. IUCF Working Paper (9/2023). hdl.handle.net/10419/275737

Seemann, M. (2023). Künstliche Intelligenz, Large Language Models, ChatGPT und die Arbeitswelt der Zukunft. Working Paper Forschungsförderung der Hans Böckler Stiftung. [boeckler.de/fpdf/HBS-008697/p_fofoe_WP_304_2023.pdf](https://www.boeckler.de/fpdf/HBS-008697/p_fofoe_WP_304_2023.pdf)

Sun, C., Zhang, H., Lin, Z., Zhang, J., Zhang, F., Wang, Z., Chen, B., Song, C., Zhang, D., Gai, K. & Xiong, D. (2024). Decoding at the Speed of Thought: Harnessing Parallel Decoding of Lexical Units for LLMs. arxiv.org/pdf/2405.15208v1

Wu, X., Xiao, L., Sun, Y., Zhang, J., Ma, T. & He, L. (2022). A survey of human-in-the-loop for machine learning. *Future Generation Computer Systems*, 135, 364-381. doi.org/10.1016/j.future.2022.05.014

Die Implementierung eines multifunktionalen Large Language Models in der polizeilichen Sachbearbeitung – Eine anwenderbezogene Technikfolgenabschätzung

Philipp Kreutzer

Die Auswertung und Erstellung polizeilicher Schriftstücke stellt einen obligatorischen, elementaren und zugleich zeitintensiven Arbeitsschritt im Alltag von Polizeibeamten dar. Einzelne quantitative Schätzungen in den Vereinigten Staaten gehen diesbezüglich von zwischen 40 (Axon, 2024) und 50 (Al Bataineh et al., 2023) Prozent der Dienstzeit zur Erstellung und Einreichung von Berichten aus.

Optimierungsmöglichkeiten könnten hier durch den integrierten Einsatz von KI, konkret in Form eines Large Language Models (LLM) bestehen, welches die Polizeibeamten bei der Anzeigensachbearbeitung, wie der Vertextung von Vernehmungen und Bodycam-Aufzeichnungen, Übersetzungen, der Zusammenfassung von Texten, der Erstellung von Schriftstücken sowie der Datenerfassung in Form eines multifunktionalen Software-Tools unterstützt.

Bislang wurden sukzessive diverse KI-Anwendungen etabliert, die sich auf die verschiedensten Bereiche polizeilicher Einzeltätigkeiten beziehen. Der Status quo ist hierbei, dass KI-Systeme gegenwärtig als separierte Einzelanwendungen die Sachbearbeiter unterstützen. Gängige Anwendungsfälle stellen exemplarisch die Verwendung von Transkriptions- und Übersetzungssoftware, Analysesoftware im Bereich Massendatenauswertung und Chat-Auswertung oder im administrativen Bereich der Verwaltung dar (Brunnbauer, 2024).

Für den Bereich der Strafverfolgungsbehörden ermöglicht der Einsatz maßgeschneiderter LLMs, die auf ihren eigenen, spezialisierten Daten trainiert wurden, eine gezieltere und spezifischere Nutzung dieser Technologie (Europol, 2023). Insofern erscheint es mittelfristig realistisch, dass jedenfalls als Quick-Win bereits auf dem kom-

merziellen Markt bestehende LLMs für polizeiliche Aufgabenbereiche modifiziert und angepasst werden oder langfristig gar eigene polizeiliche LLMs geschaffen werden.

Fraglich ist in diesem Kontext, welche anwenderspezifischen, organisationalen, technischen, rechtlichen sowie gesellschaftlichen Folgen die Implementierung einer derartigen KI-Technik bedingen würden. Diesbezüglich soll sich der gegenständliche Beitrag der Frage annehmen, welche Folgen die in Rede stehende Technik hierbei auf die Sachbearbeitung, konkret die unmittelbaren Anwenderinnen und Anwender der Technik, haben würde.

Hintergrund

Um die Anwendungsmöglichkeiten von LLMs zu skizzieren, soll zunächst ein Blick auf die grundlegenden technischen Hintergründe eines LLM erfolgen. Ferner wird auf den aktuellen Forschungsstand zum Einsatz von LLMs im Bereich der Polizei und den theoretischen Ansatz der Technikfolgenabschätzung (TA) eingegangen.

Technischer Hintergrund – LLMs im Allgemeinen

LLMs nutzen maschinelles Lernen und Deep Learning, um Muster in Trainingsdaten zu erkennen. Obwohl sie weder über Wissen noch Verständnis verfügen, erzeugen sie plausible und korrekte Texte, indem sie die wahrscheinlichsten Wortfolgen vorhersagen und auswählen (Mielke & Wolff, 2023). Durch die Herstellung von Beziehungen zwischen einzelnen Worteinheiten, den sogenannten Tokens, werden einzelne Wörter von einem LLM nicht separiert betrachtet, sondern in einer mathematischen Darstellung mit den umgebenden Wörtern oder Tokens verknüpft (Brunnbauer, 2024).

Zu ihren Kernkompetenzen gehören die Analyse und das vermeintliche Verständnis von Texten, die Erstellung zusammenhängender, kontextualisierter Texte sowie die Bewältigung verschiedener sprachlicher Aufgaben. Durch ihre Fähigkeit, Sprache zu interpre-

tieren und mit korrekter Grammatik und Rechtsschreibung zu produzieren, ermöglichen diese Modelle eine vielseitige Anwendung in sprachbezogenen Bereichen (Fraunhofer Institut, 2023).

Insofern stellen LLMs eine Form der KI im Sinne der Definition des Europäischen Parlaments dar, da das LLM als Maschine eine menschliche Fähigkeit imitiert (Europäisches Parlament, 2023).

Die Sprachmodelle weisen verschiedene Fehlertypen auf. Ein bemerkenswertes Phänomen ist das sog. Halluzinieren, bei dem die Modelle fiktive Fakten generieren, beispielsweise nicht existente wissenschaftliche Quellen. Zudem neigen sie dazu, Inhalte aus ihrem Trainingsmaterial oder sogar die Eingabeaufforderungen (sog. Prompts) nahezu wortgetreu zu reproduzieren. Dies verdeutlicht die Grenzen ihrer Fähigkeit zur eigenständigen Problemlösung und unterstreicht ihre Abhängigkeit von den während des Trainings verarbeiteten Informationen (Mielke & Wolff, 2023).

Fachlicher Hintergrund

Im Vergleich zu kommerziellen Anbietern wie OpenAI fehlen demokratisch legitimierten Strafverfolgungsbehörden momentan die Finanzmittel und Fähigkeiten, die den heutigen Software-Lösungen der Tech-Konzerne annähernd entsprechen (Stock, 2023). Dennoch legen der technische Fortschritt und die Vielzahl an aktuellen Entwicklungsprojekten den Schluss nahe, dass in Zukunft auch bei deutschen Polizeibehörden noch deutlich komplexere Aufgaben durch KI und LLMs übernommen werden können (Brunnbauer, 2024).

Theoretischer Hintergrund der TA

Die TA ist ein Instrument zur Bewertung technischer Innovationen im gesellschaftlichen Kontext, das Mitte des 19. Jahrhunderts zur Unterstützung demokratischer Entscheidungsfindung entstand und durch die aktive und interdisziplinäre Einbindung von Fachexpertise zunehmend an Bedeutung gewann (Grunwald & Saretzki, 2020).

TA bietet hierbei keine Lösungen für identifizierte Probleme, sondern liefert Orientierungshilfen und kumuliertes Wissen als Beratungsleistung. TA konzentriert sich auf Technologien mit kollektiver Tragweite und politischer Relevanz, wie Sicherheits- und Umweltstandards, Datenschutz und Forschungspolitik. TA weist nach Grunwald mit den Merkmalen der Folgenorientierung, der Wissenschaftlichkeit und dem Beratungsbezug drei Kernelemente auf. Der Schwerpunkt der TA liegt auf der Antizipation und Bewertung zukünftiger technologischer Entwicklungen und deren möglicher gesellschaftlicher Implikationen, nicht auf der Betrachtung bereits existierender Technologien. Herauszustellen ist hierbei, dass TA nicht die tatsächlichen Technikfolgen untersucht, sondern die Erwartungen und Prognosen möglicher Auswirkungen. Dies ermöglicht eine vorausschauende Analyse und Bewertung technologischer Entwicklungen (Grunwald et al., 2021).

Die Wahl des Zeitpunktes der Durchführung einer TA stellt eine besondere Herausforderung dar, da ein Dilemma hinsichtlich des Informationsdefizits bezüglich der neuen Technologie sowie akutem Handlungsbedarf besteht (Grunwald, 2022). In frühen Entwicklungsphasen fehlen Informationen über mögliche Folgen. Später, wenn die Auswirkungen erkennbar sind, ist die Technologie oft bereits so etabliert, dass Änderungen schwer, teuer und zeitaufwendig sind (Collingridge, 1982).

Methodik

Nachdem auch Europol die künftige Möglichkeit sieht, dass Strafverfolgungsbehörden maßgeschneiderte LLMs entwickeln könnten, die aufgrund ihrer eigenen, spezialisierten Daten trainiert wurden, besteht insofern Handlungsbedarf, die Technikfolgen für die Polizei abzuschätzen. So weist Europol konkret darauf hin, dass die Implementierung solcher Systeme eine sorgfältige Abwägung zwischen technologischem Fortschritt und der Einhaltung strenger ethischer und rechtlicher Standards erfordert, um einen Technologieeinsatz im Einklang mit demokratischen Werten und Grundrechten zu ge-

währleisten (Europol, 2023). Folglich kann für die Etablierung eines polizeilichen LLM aktueller Handlungsbedarf für eine TA unterstellt werden.

Wissenschaftlich haben sich mehrere Ansätze hinsichtlich der Herangehensweise an eine TA etabliert. Wenngleich diese im Detail voneinander abweichen, beinhalten sie maßgebliche Grundelemente (Grunwald, 2010). Dem folgend, sollen in Hinblick auf eine Abschätzung der Folgen der Implementierung eines LLM im Bereich der Sachbearbeitung die folgenden Handlungsfelder erörtert werden:

- Beschreibung der Technologie
- Beschreibung der Betroffenen
- Erkundung und Beschreibung von Wirkungen der Technologie
- Bewertungen der Folgen und Analyse (politischer) Handlungsoptionen
- Allgemeinverständliche Vermittlung der Resultate

Der gegenständliche Beitrag bezieht sich hierbei auf eine anwenderbezogene Betrachtung der Technikfolgen. Die gegenständliche TA zieht Fachliteratur aus den Bereichen Natur- und Rechtswissenschaften, Ethik und Kriminalwissenschaften heran. Grundlage für die Bewertung der Technikfolgen und die Erörterung von Handlungsoptionen stellt die Aufarbeitung wissenschaftlicher Fachliteratur dar.

Ergebnisse

Nachfolgend sollen die im Rahmen der TA gewonnenen Ergebnisse anhand der Beschreibung der Technologie sowie der Betroffenen, der Erkundung und Beschreibung von Wirkungen der Technologie und die Bewertungen ihrer Folgen und eine Analyse (politischer) Handlungsoptionen dargestellt werden.

Beschreibung der Technologie – ein polizeiliches LLM in der Sachbearbeitung

Im Rahmen der Vorgangssachbearbeitung erfordert die Auswertung der im Rahmen des Ermittlungsvorgangs erhobenen Daten und Akten einen erheblichen Zeitaufwand. Die Daten müssen letztlich mindestens in einem strukturierten Bericht zu einem Ermittlungsergebnis zusammengeführt und zumindest einer vorläufigen, rechtlichen Würdigung unterzogen werden. Oftmals ist darüber hinaus die Erstellung weiterer Schriftstücke an Verfahrensbeteiligte, Behörden etc. erforderlich.

Ferner sind zeitintensive Meldeverpflichtungen und statistische Erhebungen im Rahmen der Vorgangsbearbeitung vonnöten. Technisch sind das Aufgabenteile, die grundsätzlich auch durch ein LLM übernommen werden könnten. Perspektivisch ist im Rahmen der digitalen Transformation denkbar, dass die geschilderten Prozesse verschmolzen werden und durch KI automatisiert durchgeführt werden. Hierzu könnte ein LLM dienen, das durch spezifische Anpassung auf die Bedürfnisse der Polizei beziehungsweise Training mit Daten respektive Schriftstücken aus dem polizeilichen Kontext entsprechend befähigt wird. Dem Sachbearbeiter obläge einerseits die Anforderung der konkreten Maßnahme mittels Prompts. Diese Rolle wäre durch den Sachbearbeiter mehr (komplexe Ermittlungsverfahren) oder weniger bis gar nicht (Massendelikte) ausgeprägt.

Zudem wäre der Sachbearbeiter als „Human-in-the-loop“ letztlich für die Kontrolle der Resultate des LLM zuständig. Dies käme einer Rollenverschiebung und Arbeitsentlastung gleich, vom momentanen hierarchischen Binnenverhältnis Mitarbeiter–Vorgesetzter hin zur Kontrolle der KI durch den Mitarbeiter.

Erkundung und Beschreibung von Wirkungen der Technologie

Durch die Implementierung eines polizeilichen LLM ergäbe sich eine Verschiebung von der Nutzung von KI als Expertenwerkzeug hin zur breiten Verwendung als Basisinstrument. Die Auswirkungen wären insbesondere aus arbeitsökonomischer Sicht hervorzuheben, exem-

plarisch sind sog. Massendelikte anzuführen, bei denen der administrative Aufwand zur Berichterstellung sowie der Vorgangsverwaltung im Vergleich zur eigentlichen Ermittlungszeit derzeit in einem unangemessenen Verhältnis steht. Durch die erhoffte Reduzierung des Verwaltungsaufwands, die Unterstützung der Sachbearbeitung – und dies bei fehlerfreier Anwendung deutscher Rechtsschreibung – können polizeiliche Ressourcen anderweitig priorisiert werden. Eine entscheidende Voraussetzung ist, dass der Zeitaufwand für die Überprüfung der Ergebnisse des LLM durch den Sachbearbeiter so gering gehalten werden kann, dass die gewonnene Zeit nicht wieder relativiert wird (Waldtmann, 2024).

Insbesondere geistige Routineaufgaben mit wiederholendem und zeitintensivem Charakter werden durch das LLM automatisiert. Dies steigert die Verwaltungseffizienz und -effektivität und kann Beamte sowie Angestellte entlasten (FieldFisher, 2023). In einfach gelagerten Fällen (z. B. Ordnungswidrigkeiten) kann das LLM eigenständig Berichte aus den strukturierten Daten der Vorgangsverwaltung erstellen. Es erleichtert die Erschließung von Daten sowie das Erkennen von Zusammenhängen und den schnellen Dokumentenabgleich, was insbesondere im Falle eines Sachbearbeiterwechsels, eines Zuständigkeitswechsels oder des Akteneingangs von anderweitigen Behörden einen zeitlichen Mehrwert bietet. Zudem verbessert es die Barrierefreiheit durch Übersetzungen und Texte in leichter Sprache (Mielke & Wolff, 2023).

Die Implementierung eines polizeilichen LLM birgt somit das Potenzial, die Anzeigensachbearbeitung in ihren Grundzügen zu verändern und von Beginn der Anzeigenaufnahme, etwa durch einen auf dem LLM basierenden Chatbot, über den Prozess der Sachbearbeitung (Zusammenfassung von Akteninhalten) hin zum Abschluss der Ermittlungen (Abschlussbericht, Qualitätssicherung) maßgebliche Unterstützung zu leisten sowie als übergeordnete Wissensdatenbank zu fungieren.

Beschreibung der technikbetroffenen Anwender

Wie bereits dargestellt, soll sich der Blick in der gegenständlichen Untersuchung ausschließlich auf die Technikfolgen hinsichtlich der internen Fachanwender konzentrieren:

- (Kriminal-)Polizeiliche Sachbearbeitung im klassischen Sinne
- Schreibkräfte, welche die Sachbearbeitung unterstützen (Zuständigkeit für Verschriftung von Diktaten, Vernehmungen sowie Datenerfassungen)
- Dienstvorgesetzte, vor allem im Hinblick auf deren veränderte Rolle im Rahmen der Qualitätssicherung

Die Folgen der Technikimplementierung wirken sich auf die vorgeannten Betroffenen in unterschiedlicher Ausprägung aus. Insofern muss diesbezüglich bei der Bewertung der Technikfolgen differenziert werden.

Bewertungen der anwenderbezogenen Technikfolgen und Erörterung von Handlungsoptionen

Grundsätzlich kann die Etablierung von LLMs Berufsfelder auf drei verschiedenen Arten tangieren. So kann zwischen dem Verschwinden beziehungsweise der existenziellen Bedrohung (Disruption), der Implementierung in Teilbereichen (Integration) sowie der Veränderung (Transformation) unterschieden werden (Seemann, 2023). Zwar stellt Seemann (2023) fest, dass gegenwärtig Studien über Arbeitsplatzverlust und Produktivitätsgewinne durch LLMs oft an methodischen Mängeln leiden und sich in einer Frühphase befinden, dennoch kann festgehalten werden, dass die zunehmende Einführung von KI-Technologien sich auch auf die Arbeitsbedingungen von Beamten und Angestellten im öffentlichen Dienst bedeutend auswirkt (FieldFisher, 2023).

Nachfolgend werden die erwarteten Folgen der Technikimplementierung näher bewertet und untersucht. Zudem werden basierend auf dieser Folgebewertung etwaige Handlungsoptionen beleuchtet und dargestellt.

Verschiebung des Tätigkeitsschwerpunkts

Hinsichtlich der Folgen für die Verschiebung des Tätigkeitsschwerpunkts gilt es zwischen Sachbearbeitern und Schreibkräften zu differenzieren:

Folgen für Sachbearbeiter

Die Verwendung eines LLM zur Berichterstattung kann die Effizienz der Polizeiarbeit steigern, indem sie den Prozess der Datenerhebung und -verarbeitung (teil-)automatisiert. Anstatt Zeit mit administrativen Tätigkeiten, Dateneingabe und Berichterstellung zu verbringen, können sich die Beamten vermehrt ihren Kernaufgaben widmen (Al Bataineh et al., 2023).

Wenngleich selbstredend nicht davon auszugehen ist, dass der Zeitanteil der Berichterstellung in Gänze zur anderweitigen Nutzung freigesetzt wird – schließlich sind die Ergebnisse der KI zu kontrollieren und ggf. eigenständig weitere Dokumente zu erstellen –, würden durch den Einsatz eines LLM innerhalb der Sachbearbeitung bedeutende Kapazitäten freigesetzt, welche anderweitig genutzt werden können.

Diese Steigerung der Effizienz wird ebenso in einer Qualitätssteigerung münden, da komplexere und erfolgsversprechende Ermittlungsmaßnahmen dadurch priorisiert werden können (Waldtmann, 2024). Die Möglichkeiten der Nutzung der Effizienzgewinne sind mannigfaltig und reichen neben kurzfristigen, motivationssteigernden Folgen wie einem erhöhten Zeitanteil für erfolgsversprechende Ermittlungsverfahren (Steigerung der Aufklärungsquote) oder Streifenfälligkeit und öffentlicher Präsenz, Überstundenabbau, Gesundheitsprävention hin zu langfristigen, dann organisationalen Folgen (Stellenreduzierung, -verschiebungen). Diese Faktoren wirken sich zumindest mittelbar auch auf Kenngrößen der PKS wie Aufklärungsquote und Häufigkeitsziffer aus.

Zusammenfassend ist festzuhalten, dass sich die Sachbearbeiter mit einer neuen zusätzlichen Rolle in Form des officer-in-the-loop konfrontiert sehen. In welchem Ausmaß dahingehend Maßnahmen zu ergreifen sind, wird von individuellen persönlichen Faktoren (z. B. Alter, Interesse, Qualifikation) abhängen und bedingt hierdurch auch eine neue und anspruchsvolle Führungsaufgabe.

Hervorzuheben ist in diesem Kontext, was ein LLM ausdrücklich nicht bezwecken soll: eine automatisierte Entscheidungsfindung durch das LLM. Das LLM soll lediglich Entscheidungen und Arbeitsergebnisse der Sachbearbeitung vorbereiten und unterstützen (Bitkom, 2023).

Folgen für Schreibkräfte

Eine Vielzahl der Beschäftigten des Schreibdienstes führt mit einfach gelagerten Routinetätigkeiten, wie der Verschriftung von Tonbandaufnahmen, Tätigkeiten aus, welche gerade großen Stärken der LLMs darstellen. Derartige Tätigkeiten werden im öffentlichen Sektor perspektivisch durch den Einsatz von KI automatisiert (Field-Fisher, 2023), was eine disruptive Veränderung des Tätigkeitsbereichs mit sich bringt.

Über die Folgen dieses nicht nur polizeispezifischen Umstandes, sondern der gesellschaftlichen Herausforderung digitaler Transformation gilt es die Betroffenen durch die Dienstvorgesehenen transparent und zeitgerecht aufzuklären.

Sofern möglich, ist die Tätigkeit der Angestellten neu auszurichten, da neben dem Wegfall einfach gelagerter Tätigkeiten auch neuartige Tätigkeiten entstehen werden (FieldFisher, 2023). Qualifizierungsmaßnahmen stellen bei unbefristeten Beschäftigungsverhältnissen geeignete Mittel dar.

Dennoch werden nicht alle Schreibkräfte umgeschult werden können, daher ist der Wegfall diverser Tarifstellen absehbar. Gegenwärtige Stellenausschreibungen müssen im Lichte deren Zukunftsfä-

higkeit sowie einer etwaigen KI-Kompatibilität kritisch hinterfragt werden und könnten im Einzelfall lediglich befristet erfolgen. Die Verlängerung derartiger befristeter Tarifstellen ist zu hinterfragen.

Akzeptanz und Vertrauen bei den Anwendern

Im Zuge der Einführung einer neuen Software-Anwendung gilt es auch die Akzeptanz der neuen Anwendung im Kreise der Anwender zu berücksichtigen.

Angehörige von Polizeibehörden, die den Nutzen von KI in ihrer Arbeit erkennen, nehmen eine kritische, aber verständnisvolle Haltung gegenüber maschinellen Lernmodellen ein. Für die Akzeptanz bei Mitarbeitern waren die Kriterien der Nützlichkeit und Benutzerfreundlichkeit entscheidend (Herrewijnen et al., 2024). Laut einer Studie von PwC steht eine Mehrheit von 83 Prozent der befragten Behördenmitarbeiter dem Einsatz von KI in Sicherheitsbehörden positiv gegenüber und über 80 Prozent sehen darin großes Potenzial für die Verbesserung der inneren Sicherheit (PwC, 2023).

So überrascht es nicht, dass bis zur Etablierung eines LLM von Organisationsseite, die Technik auch auf irreguläre Weise Einzug in den Arbeitsalltag der Beschäftigten finden wird. Konkret ist anzunehmen, dass einzelne Mitarbeiter im Zuge ihres täglichen Dienstes aus Eigeninteresse auf LLMs zurückgreifen und dies heimlich durch die Nutzung frei verfügbarer Software tun (Seemann, 2023).

Wesentlich für die Akzeptanz eines LLM ist das Vertrauen der Anwender in das System. Während Fehler in zwischenmenschlichen Interaktionen oft nachsichtig behandelt werden, werden an KI-Systeme höchste Maßstäbe angelegt. Die derzeit verfügbaren KI-Modelle erfüllen diese hohen Anforderungen nicht und es ist unwahrscheinlich, dass ein Unternehmen dies in absehbarer Zeit garantieren kann. Zudem spielt die polizeispezifische Fachsprache eine wichtige Rolle, die von derzeitigen KI-Systemen noch nicht vollständig erfasst wird (Haas, 2023).

Ziel innerbetrieblicher Maßnahmen und Auftrag der Dienstvorgesetzten muss sein, durch interne Öffentlichkeitsarbeit sowie Fort- und Weiterbildung eine breite und nachhaltige Akzeptanz für den Einsatz des LLM herzustellen. Es wird als zweckmäßig erachtet, die vorteilhaften Effekte des Einsatzes von KI auf administrative Prozesse durch gut durchdachte und detailliert ausgearbeitete Fallbeispiele zu veranschaulichen. Diese Herangehensweise ermöglicht es, die praktischen Vorteile von KI-Anwendungen in der Verwaltung anhand greifbarer und realistischer Szenarien aufzuzeigen (DBB, 2020). Nachdem der Einsatz eines polizeieigenen LLM mittelfristig unwahrscheinlich ist, sind entsprechende Regelungslagen zu schaffen, wie hinsichtlich des unmandatierten Einsatzes verfügbarer Software in datenschutzrechtlicher und dienstrechtlicher Hinsicht zu verfahren ist. Hier besteht schon heute Handlungsbedarf.

Um Halluzinationen der KI zu vermeiden, sind technische Maßnahmen erforderlich. Die KI sollte so programmiert sein, dass sie Fakten nur aus vorgangsimmanenten Daten nutzt und keine ungewollten Ergänzungen vornimmt. Denkbar wären hierzu Retrieval-Augmented-Generation und der Einsatz von Vektordatenbanken (Waldtmann, 2024).

Gleichzeitig kann, wie oben dargestellt, allein technisch ein Halluzinieren nicht gänzlich ausgeschlossen werden. Dieses Bewusstsein muss eine zentrale Kernkompetenz der Sachbearbeiter werden, sodass diese sich der Fehlbarkeit des Systems sowie der Funktion des human-in-the-loop vollumfänglich bewusst sind.

Veränderungen von Prozessen in der Sachbearbeitung

Mit Etablierung eines umfassenden LLMs sind des Weiteren psychologische Effekte auf Ebene der Sachbearbeitung zu berücksichtigen, konkret der sogenannte Automation Bias. Dieser beschreibt die Tendenz von Menschen, automatisierten Entscheidungen mehr zu vertrauen als menschlichen. Dies kann zu einer unbewussten Verantwortungsübertragung an diese Systeme führen. Selbst wenn KI-Systeme offiziell nur zur Entscheidungsunterstützung dienen sollen,

kann der Automation Bias dazu führen, dass sie de facto zu Entscheidungsträgern werden, wodurch menschliche Autorität und Verantwortung untergraben werden (Deutscher Ethikrat, 2023).

Um diesem Risiko entgegenzuwirken, sind angemessene technische und organisatorische Maßnahmen erforderlich. Diese sollten es Anwender erschweren, KI-Empfehlungen unreflektiert zu übernehmen, selbst wenn sie die letzte Entscheidungsinstanz bleiben (Deutscher Ethikrat, 2023). Daher ist es alternativlos, dass die Anwender eine vollumfängliche Schulung zu dem eingesetzten LLM erhalten, um hinsichtlich des Automation Bias sensibilisiert zu werden und Möglichkeiten aufgezeigt zu bekommen, diese zu verhindern (Egbert, 2024). So sind die Sachbearbeiter als human-in-the-loop entsprechend gefordert, die Resultate des LLM kritisch zu prüfen. Weitere Ansätze bieten das Vier-Augen-Prinzip oder die sequenzielle Freigabe von einzelnen Textabschnitten, sodass Gesamttexte nicht lediglich überflogen werden können.

Unabdingbarkeit der Verschriftungskompetenz

Der polizeiliche Alltag erfordert die Erstellung von Schriftstücken in Fällen, in denen aus ethischen oder rechtlichen Gründen eine Übernahme durch das LLM nicht angezeigt ist. Exemplarisch sind die Erstellung von zeugenschaftlichen Berichten zu nennen, die von jedem Beamten selbst gefertigt werden, wenn diese selbst Zeuge respektive Opfer einer Straftat wurden. Persönliche Wahrnehmungen und Einschätzungen spielen hierbei für Beweis Zwecke eine wichtige Bedeutung, insbesondere wenn hierauf folgenschwere Maßnahmen gestützt werden (z. B. Schusswaffengebrauch). Bei einer Darstellung persönlicher Einschätzungen und Beweggründe kann der Einsatz eines LLM keinen Mehrwert bieten, da es hier gerade nicht um die bloße faktische neutrale Darstellung von Ereignissen handelt.

Insofern wird die Fähigkeit zur Verschriftung von Ereignissen nicht gänzlich obsolet werden. Polizeibeamte müssen diesbezüglich weiterhin befähigt bleiben und insbesondere die Wichtigkeit und der Stellenwert eigener Berichte verdeutlicht werden. So stellen die Beobachtungen von Polizeibeamten oftmals die einzige Informations-

quelle von Staatsanwaltschaft und Gericht dar, wovon wiederum der justizielle Verfahrensausgang maßgeblich beeinflusst wird. Durch die persönliche Erstellung der Berichte wird den Anforderungen an die Gründlichkeit der Dokumentation und der Ermessensabwägung sowie einer adäquaten Erinnerungsfähigkeit und Aussageverhalten vor Gericht Rechnung getragen.

Auswirkungen in der Leistungsbeurteilung

Beamte des Freistaats Bayerns sind gemäß Art. 56 ff. LlbG (Leistungslaufbahngesetz) alle drei Jahre dienstlich zu beurteilen, wobei auch die schriftliche Ausdrucksfähigkeit ein Kriterium ist. Da Sachbearbeiter viele Schriftstücke erstellen, war dieses Kriterium bisher gut beurteilbar. Mit dem zunehmenden Einsatz von LLMs stellt sich jedoch die Frage, ob dieses Beurteilungsmerkmal zukünftig noch objektiv angewendet werden kann, da die bisherige Praxis überholt sein könnte.

Allgemeinverständliche Vermittlung der Resultate

Die Einführung eines LLM als Unterstützung der Sachbearbeitung würde sich mit Blick auf die Anwender durch Verschiebung des Tätigkeitsschwerpunktes, die Frage nach Akzeptanz und Vertrauen in die neue Technologie, die Veränderung von Prozessen, eine fort-dauernde Unabdingbarkeit der Verschriftungskompetenz sowie Änderungen in der Leistungsbeurteilung auswirken. Eine veränderte Rolle als LLM-Prompter und officer-in-the-loop bringt neue Anforderungsprofile und folglich einen erheblichen Schulungsbedarf mit sich. Dem gegenüber stehen eine deutliche Effizienzsteigerung, die zu veränderten Arbeitsbedingungen und Motivationssteigerung führt. Im Bereich des Vollzugsdienstes sowie bei Schreibkräften werden erhebliche Qualifizierungsmaßnahmen vonnöten sein. Routine-tätigkeiten werden wegfallen und vom LLM übernommen werden. Der Wegfall niedrig eingruppierter Stellen ist die Folge.

Diskussion

Die Ergebnisse der Untersuchung zeigen, dass die Einflüsse von KI und fortschreitender Digitalisierung auf die Anwender im polizeilichen Bereich ähnlich denen der freien Wirtschaft sind. Insofern sind auch die festgestellten Technikfolgen wie der Wegfall einfach gelagerter Routinetätigkeiten und ein hoher Qualifizierungsbedarf nicht ausschließlich polizeispezifisch.

Für Vollzugsbeamte ergeben sich neue Herausforderungen, da diese insbesondere im Rahmen des Human-in-the-loop-Konzepts weitere Rollen übernehmen müssen und hierfür entsprechende Qualifizierungen benötigen. Obwohl noch kein ganzheitliches polizeieigenes LLM existiert, sind beispielsweise mit der KI-Toolbox bereits Einzelwerkzeuge im Einsatz, die teilweise die hier beschriebenen Folgen mit sich bringen. Daher besteht bereits jetzt Handlungsbedarf, um sich auf die kommenden Veränderungen vorzubereiten und diese aktiv zu gestalten. Insofern erscheint die gegenständliche TA zeitgerecht.

Dies stellt auch eine große Führungsaufgabe dar, da es gilt, die Mitarbeiter durch diesen Transformationsprozess zu leiten und zu unterstützen. Dies birgt erhebliche Herausforderungen im innerbetrieblichen Kontext, um Promotoren und Opponenten der Technologie gleichermaßen ernst zu nehmen. Konkret wird dies dadurch deutlich, dass KI – womöglich sogar illegal – genutzt wird, sofern diese nicht von den zuständigen Institutionen selbst eingeführt wird. Vorgesetzte, die ebenfalls Anwender sind, bleibt einerseits die Schlüsselaufgabe, den Prozess des Change-Managements zu moderieren. Gleichzeitig können auch diese von einer Verlagerung ihrer zeitintensiven Tätigkeit als Instanz der Qualitätssicherung hin zu den Anwendern profitieren und haben jenseits dieser Sachaufgaben mehr Kapazitäten für Führungsaufgaben.

Die Auswirkungen dieser technologischen Entwicklungen reichen bis in die Dimensionen des Beamtenrechts hinein. So wird das Beurteilungswesen ebenfalls von diesen Veränderungen tangiert, was weitere Herausforderungen für die Personalführung im öffentlichen Dienst aufwirft. Zu betonen bleibt gleichzeitig, dass ein LLM den Sach-

bearbeiter nicht ersetzen wird. Die finale Entscheidungsgewalt obliegt weiterhin der Sachbearbeitung. Folglich bleibt das LLM ein Mittel zum Zweck, die letztlich jede andere Technik auch (Grunwald, 2019).

Schlussfolgerungen

Besonders im tariflichen Bereich wird die Art und Weise, wie Einstellungen und Beschäftigungsverhältnisse gestaltet werden, maßgeblich von den genannten Veränderungen betroffen sein. Schon heute besteht hier dringender Handlungsbedarf, um bei der Stellenbewirtschaftung zukunftsfähige Lösungen zu schaffen.

Die zentrale Aufgabe wird die Qualifizierung der künftigen Anwender sein. Im Hinblick auf das digitale Anforderungsprofil des „Polizeibeamten der Zukunft“ sind umfangreiche und grundlegende Anpassungen im Bereich Aus-/Fortbildung erforderlich. Perspektivisch wird jeder Vollzugsbeamte über grundlegende IT-Kenntnisse verfügen müssen, darüber hinaus gewinnen Fähigkeiten in den Bereichen Programmierung, Diskriminierungsfreiheit und KI-Technologien an Bedeutung. Nachdem bereits gegenwärtig immer mehr KI-Anwendungen in den Arbeitsalltag integriert werden, gilt es die Qualifizierung hier zügig, ganzheitlich und nachhaltig zu forcieren.

Der entstehende gesetzgeberische Bedarf im Bereich des Beurteilungswesens stellt neben einer anwenderbezogenen zudem eine organisationale Folgeerscheinung dar, welche es aufgrund des langwierigen zeitlichen Horizontes zeitnah anzugehen gilt.

Weitere organisationale Technikfolgen bleiben genauso wie weitere Dimensionen der TA offen und damit zu beantworten, inwiefern die Etablierung eines polizeilichen LLM Folgen auf technischer, sozialgesellschaftlicher sowie rechtlicher Ebene mit sich bringen könnte.

Literaturverzeichnis

- Al Bataineh, A., Sickler, R., Morris, W. T. & Pedersen, K. (2023) The Impact of AI-generated reports for law enforcement: A call for responsible integration and interpretability [Online]. Verfügbar unter information-professionals.org/the-impact-of-ai-generated-reports-for-law-enforcement-a-call-for-responsible-integration-and-interpretability-2/ (Abgerufen am 19. September 2024).
- Axon (2024) FAQs about DraftOne [Online]. Verfügbar unter axon.com/products/draft-one (Abgerufen am 19. September 2024).
- Bitkom (2023) KI in der Polizei – Einsatzpotentiale und Lösungsansätze zur Implementierung [Online], Bitkom. Verfügbar unter bitkom.org/Bitkom/Publikationen/KI-in-der-Polizei-Einsatzpotentiale-und-Loesungsansaeetze-zur-Implementierung (Abgerufen am 19. September 2024).
- Brunnbauer, M. (2024) Potentiale und Gefahren von Large Language Models aus der polizeilichen Sicht, in: Honekamp, W. & Labudde, D. (Hg.) Polizei-Informatik 2024, Remscheid, Rediroma-Verlag, S. 235-240.
- Collingridge, D. (1982) The social control of technology, London, Pinter.
- dbb (2020) Expertenrat künstliche Intelligenz: Auswirkungen auf den öffentlichen Dienst [Online]. Verfügbar unter dbb.de/artikel/expertenrat-kuenstliche-intelligenz-auswirkungen-auf-den-oeffentlichen-dienst.html (Abgerufen am 19. September 2024).
- Deutscher Ethikrat (2023) Mensch und Maschine – Herausforderungen durch Künstliche Intelligenz [Online]. Verfügbar unter ethikrat.org/publikationen/stellungnahmen/mensch-und-maschine/ (Abgerufen am 19. September 2024).
- Egbert, S. (2024) Diverse Daten, nicht-diskriminierende Algorithmen: Die Relevanz von Diversität im Rahmen der Datafizierung der Polizei, in: Staller, M. S. & Koerner, S. (Hg.) Diversität und Polizei, Wiesbaden, Springer Fachmedien, S. 281-303.
- Europäisches Parlament (2023) Was ist künstliche Intelligenz und wie wird sie genutzt? [Online]. Verfügbar unter europarl.europa.eu/topics/de/article/20200827STO85804/was-ist-kunstliche-intelligenz-und-wie-wird-sie-genutzt (Abgerufen am 19. September 2024).
- Europol (2023) Tech Watch Flash – ChatGPT – The Impact of Large Language Models on Law Enforcement [Online]. Verfügbar unter europol.europa.eu/publications-events/publications/chatgpt-impact-of-large-language-models-law-enforcement (Abgerufen am 19. September 2024).
- FieldFisher (2023) Künstliche Intelligenz im öffentlichen Sektor: Die Zukunft der Beamten und Angestellten in Deutschland [Online]. Verfügbar unter fieldfisher.com/de-de/insights/kuenstliche-intelligenz-im-oeffentlichen-sektor-die-zukunft-der-beamten (Abgerufen am 19. September 2024).
- Fraunhofer Institut (2023) Was sind Large Language Models? Und was ist bei der Nutzung von KI-Sprachmodellen zu beachten? [Online]. Verfügbar unter iese.fraunhofer.de/blog/large-language-models-ki-sprachmodelle/ (Abgerufen am 19. September 2024).
- Grunwald A. (2010) Technikfolgenabschätzung – eine Einführung: Zweite, grundlegend überarbeitete und wesentlich erweiterte Auflage, Baden-Baden, Nomos Verlagsgesellschaft mbH & Co. KG.
- Grunwald A. (2022) Technikfolgenabschätzung: Einführung, 3. Aufl., Baden-Baden, Nomos.
- Grunwald A. & Saretzki T. (2020) Demokratie und Technikfolgenabschätzung, TATuP – Zeitschrift für Technikfolgenabschätzung in Theorie und Praxis, Vol. 29, No. 3, S. 11-17.

Grunwald A, Bösch S, Krings B-J & Rösch C (Hg.) (2021) Technikfolgenabschätzung: Handbuch für Wissenschaft und Praxis [Online], Baden-Baden, Nomos Verlagsgesellschaft mbH & Co. KG. Verfügbar unter nbn-resolving.org/urn:nbn:de:bsz:31-epflicht-1861819.

Haas S. (2023) Von Skepsis zu Chancen: Generative KI und die Polizei [Online]. Verfügbar unter de.linkedin.com/pulse/von-skepsis-zu-chancen-generative-ki-und-die-polizei-steve-haas-vg1re?trk=public_post_feed-article-content (Abgerufen am 19. September 2024).

Herrewijnen, E., Loerakker, M. B., Vredenburg, M. & Woźniak, P. W. (2024) Requirements and Attitudes towards Explainable AI in Law Enforcement. Designing Interactive Systems Conference. IT University of Copenhagen Denmark. New York, NY, USA, ACM, S. 995-1009.

Mielke, B. & Wolff, C. (2023) Künstliche Intelligenz und Large Language Models in der Rechtsprechung, LRZ [Online]. Verfügbar unter [lrz.legal.de/lrz/kuenstliche-intelligenz-und-large-language-models-in-der-rechtsprechung](https://legal.de/lrz/kuenstliche-intelligenz-und-large-language-models-in-der-rechtsprechung) (Abgerufen am 19. September 2024).

PwC (2023) Künstliche Intelligenz in deutschen Sicherheitsbehörden: Zwischen Ambition und Wirklichkeit [Online]. Verfügbar unter strategyand.pwc.com/de/de/branchen/oeffentlicher-sektor/ki-in-deutschen-sicherheitsbehoerden.html (Abgerufen am 19. September 2024).

Seemann, M. (2023) Künstliche Intelligenz, Large Language Models, ChatGPT und die Arbeitswelt der Zukunft. Working Paper Forschungsförderung, No. 304 [Online]. Verfügbar unter boeckler.de/de/faust-detail.htm?sync_id=HBS-008697 (Abgerufen am 19. September 2024).

Stock, O. (2023) Datafizierung, Cloudifizierung, Virtualisierung und KI: das polizeiliche Auftragsverständnis zur Verteidigung der Freiheit im digitalen Zeitalter, in: Wehe, D. & Siller, H. (Hg.) Handbuch Polizeimanagement, Wiesbaden, Springer Fachmedien Wiesbaden, S. 1445-1470.

Waldtmann, C. (2024) Einsatz KI-basierter Technologien zur Bewältigung des polizeilichen Vorgangsaufkommens bei Massendelikten, in: Honekamp, W. & Labudde, D. (Hg.) Polizei-Informatik 2024, Remscheid, Rediroma-Verlag, S. 260-264.

Anwendungsmöglichkeiten von Large Language Models beim Kriminaldauerdienst der Polizei Baden-Württemberg

Frank Gaiser

Die rasante Entwicklung Künstlicher Intelligenz (KI) in den letzten Jahren eröffnet der modernen Gesellschaft zahlreiche neue Möglichkeiten und bringt umfassende Änderungen mit sich, die sich bereits jetzt schon in verschiedensten Bereichen manifestieren. Von der Navigation im Straßenverkehr über Smart Homes (Verbraucherzentrale 2024) bis hin zur Unterrichtsgestaltung im Bildungswesen (Unterberg 2023) – überall hält die neue Technologie rapide Einzug in den Alltag der Menschen. Doch bringt die fortschreitende Entwicklung der KI nicht nur Positives mit sich – längst haben Kriminelle das Potenzial solcher Software-Programme erkannt. Die Anwendungsbereiche sind hier gleichsam vielfältig wie schädlich: Täter verwenden KI-gestützte Methoden für Cyberangriffe, Falschmeldungen, Propagandatexte und Hassnachrichten oder, noch perfider – für Social Engineering. Letzgenannte Methode nutzt den „Faktor Mensch“ als Sicherheitslücke, indem typische Eigenschaften wie Angst, Vertrauen oder Respekt vor Autorität in Phishing-Mails gezielt manipuliert werden. Als besonders effizient haben sich dabei Large Language Models (LLMs) erwiesen, die automatisch in verschiedenen Sprachen und mit hoher Qualität beliebige Texte erzeugen können (Bundesamt für Sicherheit in der Informationstechnik 2024, S. 11). Um Cyberkriminelle, welche KI im negativen Sinne nutzen, strafrechtlich beweissicher zu verfolgen und das Potenzial von KI selbst nutzen zu können, haben mehrere Polizeien der Länder sowie das Bundeskriminalamt (BKA) begonnen, KI-basierte Systeme in verschiedensten Anwendungsbereichen zu erproben (Bundeskriminalamt 2024). Doch wie sieht es abseits dieser Pilot- und Forschungsprojekte auf Makroebene mit dem Nutzen der neuen Technologie im operativen Bereich aus?

Ziel dieses Beitrags ist es, einen greifbaren Mehrwert für die Praxis aufzuzeigen und den Fokus dieses abstrakten und komplexen Themas auf einen konkreten Anwendungsbereich, den Kriminaldauerdienst (KDD) der Polizei Baden-Württemberg, sowie eine konkrete

Form der KI, nämlich die LLMs, zu legen. Daraus abgeleitet ergibt sich die Forschungsfrage, welche Anwendungsmöglichkeiten sich für LLMs im Aufgabenbereich des KDD der Polizei Baden-Württemberg ergeben und welche Herausforderungen es bei der Implementierung ebensolcher Anwendungen zu beachten gilt.

Hintergrund

Um die Basis für die folgende Analyse und Diskussion zu legen, muss zunächst festgehalten werden, was unter „Künstlicher Intelligenz“ zu verstehen ist. Das Europäische Parlament (2020) sieht KI als „die Fähigkeit einer Maschine, menschliche Fähigkeiten wie logisches Denken, Lernen, Planen und Kreativität zu imitieren“. Gerade das „Lernen“ kann hierbei als zentrale Eigenschaft hervorgehoben werden: Alle KI-Anwendungen zeichnet demnach aus, dass sie in ihrer Verarbeitungsfähigkeit trainiert werden und dadurch lernen. In der Folge können derartige Systeme in einer Art Transferleistung in hoher Qualität mit Sachverhalten umgehen, die nicht Teil des Trainingsdatensatzes waren (Bitkom e.V. 2023, S. 6). Zur weiteren Präzisierung hat sich die Einteilung in starke und schwache KI etabliert. Schwache KI-Systeme existieren bereits und beherrschen mathematische sowie informationstechnische Lösungen von konkreten Anwendungsproblemen und sind darüber hinaus zur Selbstoptimierung fähig (Die Bundesregierung 2018, S. 4). Eine starke KI, die menschlichem Intellekt nachempfunden ist und menschlicher Intelligenz gleichsteht oder diese übertrifft, ist aus heutiger Sicht „Science-Fiction“ und in absehbarer Zeit nicht realisierbar (Kirn, Müller-Hengstenberg 2014, S. 226).

LLMs sind, trotz ihres enormen Potenzials, der schwachen KI zuzuordnen. Dennoch handelt es sich bei LLMs um leistungsstarke KI-Anwendungen, die menschliche Sprache verarbeiten und generieren, indem sie Texte analysieren, kohärente Antworten erzeugen sowie sprachbezogene Aufgaben ausführen (Kelbert, Siebert, Jöckel 2023). Dies funktioniert in vier Schritten: Das LLM zerlegt einen Text zunächst in kleinere Teile, sogenannte Token. In der Folge werden die Token dergestalt eingebettet, dass ihre semantische Information

und ihre Position im Satz berücksichtigt werden. In einem dritten Schritt erfolgt die Berechnung der Wahrscheinlichkeit des nächsten Tokens. Schließlich nutzt das LLM eine Dekodierungsstrategie, um die Token-Sequenzen zu einem Ausgabertext zusammenzufügen (Siebert, Kelbert 2024). Zum aktuellen Forschungsstand lässt sich festhalten, dass die Entwicklung sehr dynamischen Prozessen unterliegt und durch viele Anbieter vorangetrieben wird. Während die Version ChatGPT 3.5 von OpenAI Ende 2022 veröffentlicht wurde und qualitativ hochwertige Antworten als Text in unterschiedlichen Sprachen zu verschiedensten Problemstellungen geben konnte, aber oftmals mit der Analyse umfangreicher kontextabhängiger Schriften Schwierigkeiten hatte, weist die Version GPT-4o aus dem Mai 2024 umfangreichere Weiterentwicklungen auf. So ist diese deutlich performanter bei vergleichbaren Aufgaben, hat einen erheblich größeren Funktionsumfang und kann sogar Bilder generieren, umfassende Codes und Skripte erstellen sowie mannigfaltige Inputs wie Bilder, PDF-Dateien etc. verarbeiten und transkribieren (Brunnbauer 2024, S. 234).

Als weiteres wesentliches Element dieses Beitrags wird nachstehend der KDD der Polizei Baden-Württemberg genauer vorgestellt. Bei der operativen Organisationseinheit handelt es sich um die kriminalpolizeiliche Vertretung, die, abgesehen von der Leitung und den Schreibkräften im Tagesdienst, 24/7 im Schichtdienst arbeitet und sich zum Großteil aus jungen Kriminalbeamten zusammensetzt. Aufgrund durchgängiger Verfügbarkeit und Expertise im Bereich der Kriminalpolizei wird der KDD im Rahmen der Zuständigkeit regelmäßig als „Service-Einheit“ für andere polizeiliche Organisationseinheiten tätig (Küster 2019, S. 1 ff.). Die Deliktsbreite reicht von Einbruchsdiebstählen, über Sexualdelikte und Raubstrafaten bis hin zu ungeklärten Todesfällen sowie Tötungsdelikten. Der KDD übernimmt die Ermittlungen im Erstaufschlag, sichert vergängliche Spuren und fixiert Aussagen der Beteiligten in Festlegervernehmungen (Innenministerium Baden-Württemberg – Landespolizeipräsidium 2024). Die Erkenntnisse werden für Folgeermittlungen und Endsachbearbeitung an Fachinspektionen oder Kriminalkommissariate übergeben (Küster 2019, S. 2).

Für die Schnittmenge zwischen IT, LLM und Polizeiarbeit ist es wesentlich, das Projekt P20 kurz zu erläutern. Das betreffende Projekt entstand infolge der Saarbrücker Agenda, in der sich die Innenminister der Länder und des Bundes im Jahr 2016 auf eine Modernisierung der IT der Polizeien in Deutschland verständigten. Seither arbeitet P20 primär an der Grundlage einer digitalen Vernetzung der Polizei, die kontinuierlich dem jeweiligen Stand der Technik angepasst wird und die polizeiliche IT-Architektur harmonisiert und modernisiert (Bundesministerium des Innern und für Heimat 2024). Die Lösungen sollen dabei anwenderfreundlich sein und den Grundsatz verfolgen, dass polizeiliche IT-Angebote nur einmal entwickelt und allen Bedarfsträgern in den Ländern und im Bund zur Verfügung gestellt werden sollen. Eine Umsetzung der Vorgaben ist für das Jahr 2030 vorgesehen (Klan 2024, S. 192).

Rechtliche Anforderungen an KI-Software und somit an LLMs wurden erstmals in dem im Mai verabschiedeten und ab Dezember 2024 stufenweise in Kraft tretenden EU AI Act (KI-VO) formalgesetzlich fixiert. Die KI-VO teilt KI-Systeme nach verschiedenen Anwendungsbereichen sowie Fähigkeiten ein und sieht je nach Einstufung unterschiedliche Restriktionen vor. Wesentliche Klassifizierungen von KI ergeben sich aus Art. 5 Abs. 1 und Art. 6 mit Anhang III der KI-VO. Während die erstgenannte Rechtsnorm, mit Ausnahmen für Gefahrenabwehr und Strafverfolgung, acht grundsätzlich unzulässige KI-Praktiken formuliert, beschreibt die zweitgenannte Regelung Einstufungen als Hochrisiko-KI. Für diese gelten verpflichtende Grundrechtsfolgenabschätzungen sowie Melde- und Berichtspflichten. Auch müssen Einsatz und Überwachung nach strikten Maßstäben dokumentiert werden (Pfeffer 2024, S. 57 ff.). Schließlich sind nur solche Anwendungen als verboten anzusehen, die offensichtlich nicht mit den Werten der EU, wie der Achtung der Menschenwürde, der Grundrechte sowie der Demokratie und der Rechtsstaatlichkeit, in Einklang stehen (Krönke 2024, S. 531).

Neben dem Rechtlichen sind vor allem organisationsstrategische Faktoren von Belang. Ein zentraler Begriff in diesem Sinne ist das Change-Management. Dieser „hat sich in den letzten Jahren für die gezielte Durchführung von Veränderungen etabliert. [...] Die

wesentliche Aufgabe von Change Management [ist es], gezielt und aktiv, strategisch wohlüberlegt und wirkungsvoll in die Anpassungsprozesse einzugreifen.“ (Brendt, Amberg 2018, S. 5 f.) Hierbei ist es enorm wichtig, personalorientierte Aspekte zu berücksichtigen. All dies wird im 8-Stufen-Modell nach Kotter (2011) dargelegt: Anfänglich sollte die Dringlichkeit zu Veränderung in der Organisation aufgezeigt werden, um in der Folge eine unterstützende Führungskoalition aufzubauen. Anschließend sollte eine Vision und Strategie entwickelt werden, die dann in der Organisation kommuniziert werden muss. Bestehende Hindernisse sollten in einem nächsten Schritt aus dem Weg geräumt werden, um sodann kurzfristige Erfolge anstreben zu können. Abschließend sollten nötige Veränderungen in der Organisation weiter angestoßen und schließlich in der Organisationskultur verankert werden.

Als Analyse-Werkzeug wird in diesem Beitrag die SWOT-Analyse verwendet. Der Begriff SWOT ist ein Akronym und steht für die englischen Worte Strengths (Stärken), Weaknesses (Schwächen), Opportunities (Chancen) und Threats (Risiken), die den Kern der Analysemethode bilden. Vorab erhobene Informationen zur Ausgangssituation werden den vier Themenfeldern zugeordnet und die kritischen Punkte in einer 4-Felder-Matrix präsentiert (Stephan 2010). Während die ersten drei Kategorien selbsterklärend sind, wird die Kategorie Risiko, aufgrund unterschiedlicher Auslegungsmöglichkeiten, für diesen Beitrag mit der Definition Eintrittswahrscheinlichkeit multipliziert mit der Schadenshöhe festgelegt.

Methodik

Nach einer kurzen Einführung zum Thema und der Darlegung des relevanten Hintergrunds werden in diesem Kapitel die verwendete Methode und ihre Eignung zur Beantwortung der Forschungsfrage genauer beschrieben. Die Forschungsfrage verfolgt das Ziel darzustellen, welche Anwendungsmöglichkeiten es für LLMs im KDD der Polizei Baden-Württemberg gibt und welche Herausforderungen bei einer Einführung zu beachten sind. Da in der betreffenden operativen Einheit der Kriminalpolizei zum momentanen Zeitpunkt keine

derartige KI-Anwendung in Gebrauch ist, beschreibt dieser Beitrag die Einführung von etwas Neuem in einer Organisation, das Änderungen an bisherigen Ablaufprozessen bewirkt und in einer Welt zunehmender Digitalisierung perspektivisch an Bedeutung gewinnen wird. Es betrifft somit die strategische Ausrichtung des KDD.

Als geeignetes Analyse-Werkzeug in diesem Bereich hat sich die SWOT-Analyse etabliert – „eine gängige und beliebte Methode für Strategiearbeit [...]. Ihre Anwendung kommt zum Einsatz, wenn eine Ausgangssituation möglichst umfassend und differenziert darzustellen ist“ (Trippner 2021, S. 150). Das Instrument dient dabei der Erfassung, Strukturierung und Aufdeckung von Stärken und Schwächen sowie Chancen und Risiken einer Organisationseinheit und kann bei paarweiser Kreuzung der vier Elemente dazu dienen, Handlungsempfehlungen abzuleiten und Potenziale aufzuzeigen. So sollten Stärken genutzt werden, um Chancen zu ergreifen. Schwächen sollten ausgebessert werden, um Chancen nutzen zu können. Stärken sollten wiederum genutzt werden, um Risiken zu neutralisieren, und Schwächen sollten reduziert werden, um Risiken zu entgehen (Bundesministerium des Innern und für Heimat 2023).

Konkret wird in der nachstehenden SWOT-Analyse der Hintergrund des Beitrags dergestalt angewendet, dass darin enthaltene Stärken und Schwächen sowie Chancen und Risiken der Einführung von LLMs beim KDD aufgezeigt werden, die Ausgangssituation somit differenziert dargestellt und die Herausforderungen einer Implementierung beleuchtet werden. Im folgenden Abschnitt werden die Ergebnisse der SWOT-Analyse vorgestellt, um diese anschließend diskutieren und interpretieren zu können. Insgesamt werden dabei in der Analyse und Diskussion aus Gründen der Übersichtlichkeit nur ausgewählte, besonders herausragende Aspekte dargestellt. Final wird dieser Beitrag mit einer zusammenfassenden Schlussfolgerung und Handlungsempfehlung für die Implementierung von LLMs im KDD abgerundet.

Ergebnisse

Bei Anwendung der SWOT-Analyse lässt sich beginnend mit den Stärken festhalten, dass LLMs jederzeit in der Lage sind, enorme Informations- und Datenmengen in diversen Eingabeformaten sofort zu erfassen, aufzubereiten und dem Anwender auf entsprechende Anfragen in hoher Qualität auszugeben. Außerdem können sie eine Vielzahl an Sprachen simultan übersetzen und mittels Transkriptionsfunktion Diktate automatisch verschriften (Brunnbauer 2024, S. 234). Ebenso positiv zu werten ist, dass der überwiegende Teil polizeilicher Tätigkeit sich in standardisierten Arbeitsprozessen abbilden lässt (Pekar-Milicevic 2016, S. 91). Das spiegelt sich im Bereich der Sachbearbeitung durch eine Vielzahl an vorgefertigten Formularen im digitalen Vorgangsbearbeitungssystem wider.

Darüber hinaus verfügt die Polizei Baden-Württemberg über eine umfassende und zeitgemäße IT-Ausstattung, zu der unter anderem Smartphones mit entsprechenden App-Anwendungen gehören (Ministerium des Inneren, für Digitalisierung und Kommunen Baden-Württemberg 2019). Erste Kooperationen im Bereich KI und LLMs wurden in der zweiten Jahreshälfte 2024 mit dem deutschen Unternehmen Aleph Alpha angestoßen (SWR Aktuell 2024). Im Sinne einer Modernisierung und Harmonisierung der deutschlandweiten polizeilichen IT-Infrastruktur bietet das Projekt P20 zusätzlich eine passende Ausgangsbasis für die Implementierung von LLMs (Bundesministerium des Innern und für Heimat 2024).

Aufgrund umfassender bürokratischer Vorgaben werden polizeiliche Vorgänge regelmäßig und detailliert in digitalen Systemen dokumentiert und bilden so große Datensätze (Gebhardt 2024). Diese können anonymisiert neben frei verfügbaren Gesetzestexten als Trainingsdatenbasis für LLMs dienen. Im Bereich der Schwächen ist die fehlende oder zumindest unzureichende KI-Kompetenz der Mitarbeitenden im KDD hinsichtlich Anwendung und Umgang mit entsprechenden Programmen zu nennen. Derartige Fähigkeiten konnten bislang noch nicht erlangt werden, da erste Kooperationen der Polizei zu KI und LLMs, wie zuvor beschrieben, erst in der zweiten Jahreshälfte 2024 gestartet wurden.

Auch besteht aufgrund zurückliegender Fehleranfälligkeit, weitreichender Auswirkungen auf die Sachbearbeitung und der fehlenden Erfahrung im Umgang mit KI eine gewisse Skepsis innerhalb der Organisation. Diese schmälert die Akzeptanz für LLMs in der Polizei und behindert deren Einführung (Haas 2024, S. 81). Ebenfalls negativ ist die Tatsache, dass die Polizei Baden-Württemberg keine haus-eigen entwickelten LLMs verwendet, sondern, wie oben genannt, mit einer externen Firma kooperiert. Auch fanden LLMs bisher im geschützten operativ-polizeilichen Bereich keine Anwendung und konnten nicht mit entsprechenden Daten angereichert werden. Das Training sowie die Anpassung bestehender Programme wird einige Zeit in Anspruch nehmen und macht die Technik für die Einsatzkräfte nicht sofort nutzbar (Brunnbauer 2024, S. 236 f.).

Schließlich ist als weitere Schwäche zu nennen, dass Einführung und Betrieb von LLMs sowie nötige Anpassungen an der IT-Infrastruktur extrem kostenintensiv sind. Dem steht ein begrenztes Budget der Polizei, das im Jahr 2020 in Baden-Württemberg für den Bereich KI mit lediglich 7,5 Millionen Euro ausgewiesen war, gegenüber (Landtag von Baden-Württemberg 2020, S. 6).

Die Anwendung von LLMs im KDD bietet etliche Chancen. Die Systeme können als ständig verfügbare Wissensdatenbank alle Vorschriften, Gesetze, polizeilichen Themen und Prozesse auf Anfrage aufbereitet wiedergeben (Bitkom e.V. 2023, S. 9). Aufgrund ihrer Fähigkeiten eignen sich LLMs darüber hinaus zur Optimierung der polizeilichen Kommunikation. So können Mailsteuerung oder Einbindung, Informationsweitergabe und Berichterstattung mit den zuständigen Organisationseinheiten automatisiert werden (Waldtmann 2024, S. 261).

Mittels Informationsanalyse können LLMs wertvolle Ermittlungsunterstützung leisten. Dies geschieht, indem sie Massendaten, wie Chatprotokolle im Rauschgiftbereich, aufbereiten, Bildaufnahmen bei der Tatortarbeit auswerten, Vernehmungsinhalte unmittelbar aufbereiten oder kriminelle Muster bei Tatserien erkennen (Bitkom e.V. 2023, S. 9). Darüber hinaus besteht bei Übernahme von standardisierten Dokumentations-, Verschriftungs- und Analyseprozessen durch LLMs

die Chance personeller Entlastung der Ermittlungskräfte und – mit der Eigenschaft als Übersetzungs- und Transkriptionssoftware – die Möglichkeit erheblicher finanzieller Einsparung (Münch 2024, S. 3).

Der Einsatz von LLMs entspricht moderner Kriminalitätsbekämpfung, lässt die Polizei aktuellen Kriminalitätsphänomenen auf Augenhöhe begegnen und schafft bei konsequenter Weiterentwicklung die Möglichkeit, diesen sogar einen Schritt voraus zu sein. Auch können mit fortschreitender Entwicklung immer anspruchsvollere Aufgaben automatisiert werden (Brunnbauer 2024, S. 236 ff.). Der wachsende Markt für LLMs generiert vielzählige Anbieter, welche entsprechende Software zur Verfügung stellen. Dies ermöglicht es Kunden, sich ihren Anbieter aussuchen zu können (Metzmacher 2024).

Bei Darlegung der Risiken sind zunächst die vielzähligen unbestimmte Rechtsbegriffe der KI-VO zum Betrieb von KI zu erwähnen, welche im Rahmen der Rechtsprechung erst noch zu definieren sind (Krönke 2024, S. 532). Auch müssen gesetzliche Anpassungen auf Bundes- und Landesebene im Bereich Datenschutz und Eingriffsrecht vorgenommen werden, um den Anwendungsrahmen entsprechender Software abstecken zu können (Pfeffer 2024, S. 65). Ein besonderes Sicherheitsrisiko ergibt sich aus der Bündelung sämtlicher polizeilicher Prozessabläufe und sensibler Informationen für die Datengrundlage entsprechender LLMs. Dies und der Umstand, dass die Systeme im Anwendungsfall mit personenbezogenen Daten und Informationen zu höchstpersönlichen Lebensumständen arbeiten, macht polizeiliche LLMs besonders attraktiv für kriminelle Hacker (Haas 2024, S. 85 f.).

Da seitens der Polizei kein hausinternes LLM zum Einsatz kommt, wird, wie bereits erwähnt, die Software-Lösung von einem externen Anbieter bezogen. Dadurch besteht das Risiko einer technologischen Abhängigkeit eines hart umkämpften und unstetigen Bereichs der Privatwirtschaft (Trichtl 2023). Ebenso kann es bei der Anwendung von LLMs zu systemseitigen Fehlern oder ungewünschten Ergebnissen kommen, die nicht immer offensichtlich sind. Dies reicht von unausgewogenen oder nicht korrekten Trainingsdaten, die zu Verzerrungen (Bias) in der Ausgabe führen, bis hin zu erfundenen

Informationen in den Antworttexten, die nicht Teil von Eingabe oder Trainingsdatensatz waren (Halluzinieren) (Bundesamt für Sicherheit in der Informationstechnik 2024, S. 9).

Stärken	Schwächen
<ul style="list-style-type: none"> ▪ Schnelle Verarbeitung großer Datenmengen ▪ Übersetzung und Transkription ▪ Standardisierte Prozesse ▪ IT-Grundlage ▪ Große Datenbasis für Trainingsdaten 	<ul style="list-style-type: none"> ▪ Fehlende KI-Kompetenz ▪ Fehlendes Vertrauen ▪ Keine interne Entwicklung von LLMs ▪ Zeitverzug bis zur Anwendung ▪ Limitierte Finanzmittel/Kosten für IT-Infrastruktur
Chancen	Risiken
<ul style="list-style-type: none"> ▪ Ständig verfügbares Fachwissen ▪ Interne Kommunikationsoptimierung ▪ Informationsanalyse ▪ Kostensenkung, Personalentlastung und -einsparung ▪ Moderne Kriminalitätsbekämpfung ▪ Anbietervielfalt 	<ul style="list-style-type: none"> ▪ Rechtliche Unsicherheiten ▪ Sicherheitsrisiken ▪ Technologische Abhängigkeit ▪ Fehler durch LLMs

Abbildung 1: SWOT-Analyse Anwendungsmöglichkeiten von für LLMs im KDD Baden-Württemberg

Diskussion

Die vorausgegangene SWOT-Analyse mit den vier Themenfeldern dient bei paarweiser Betrachtung der Ergebnisse im Folgenden als Grundlage für die weitere Diskussion. Zusätzlich lässt dies erstmals eine Interpretation von Anwendungsmöglichkeiten und Herausforderungen von LLMs im KDD der Polizei Baden-Württemberg zu. Bei Nutzung der beschriebenen Stärken lässt sich eine Vielzahl an Chancen bei der Anwendung von LLMs im KDD ergreifen. So wird es möglich sein, Vernehmungen vor Ort in der Einsatzlage per dienstlichem Smartphone zu realisieren, selbst wenn das Gegenüber der deutschen Sprache nicht mächtig ist – zeitaufwendiges Warten auf teure Dolmetscher entfällt. Auch das zeitverzögerte Verschriften des Diktats durch Schreibkräfte wird dadurch hinfällig. Die durch Wegfall von Schreibkräften und externen Dolmetschern eingesparten Finanzmittel dürften dabei nicht unerheblich sein (Münch 2024, S. 3).

Ein weiterer Aspekt ist, dass die mobile Sachbearbeitung durch LLMs grundsätzlich wesentlich verbessert werden kann. Erhobene Vernehmungen und Bildaufnahmen können vor Ort in das System eingespeist werden. In der Folge können Einsatzberichte, Anzeigenaufnahmen, Asservatenlisten, Lichtbildmappen und relevante Formulare automatisiert erstellt und nach Prüfung durch den Sachbearbeiter für die zuständige Fachdienststelle freigegeben werden. Dies sorgt für erhebliche personelle Entlastungen und verhindert, dass zur händischen Anfertigung von Berichten Überstunden auf der Dienststelle erbracht werden müssen (Bataineh et al. 2023 und Haas 2024, S. 82). Auch können LLMs die Vernehmungsqualität an sich erhöhen. Durch direkte Aufbereitung der Sachverhalts- und Vernehmungsinformationen werden widersprüchliche Angaben sofort erkannt und dem Vernehmenden mitgeteilt, welcher sie als Vorhalt aufgreifen kann – ähnlich dem, wie es Volkmann, Schildein und Po-valej (2024, S. 41) beschreiben.

Neben dieser beschriebenen Effizienzsteigerung kann durch LLMs ebenso die Effektivität polizeilichen Einschreitens optimiert werden. Dies ist möglich, wenn riesige Datenmengen zu bestehenden Tatsachen durch die Systeme analysiert und Vorhersagen zu Folgetaten getroffen oder LLMs dafür genutzt werden, öffentliche Bereiche des Internets automatisiert zu durchsuchen, um Gefahren, Radikalisierungen oder Straftaten frühzeitig zu erkennen und Profile zu Personen mit entsprechenden Verhaltensmustern zu erstellen (Bitkom e.V. 2023, S. 9). Neben einer objektiven Leistungssteigerung kann aber auch im subjektiven Bereich das Sicherheitsempfinden der Bevölkerung und das Vertrauen in eine fortschrittliche und leistungsfähige Polizei erhöht werden. Gleichsam dürfte die moderne Technologie und fortschrittliche IT-Ausstattung attraktiv für technikaffine Nachwuchskräfte aus der Generation der „Digital Natives“ sein und sich positiv auf die Nachwuchswerbung auswirken.

Da es sich beim KDD um eine personell junge Organisationseinheit handelt und erfahrene Kollegen diese oftmals aufgrund der gesundheitlichen Nachteile des Schichtdienstes zeitig verlassen, ist die Gewährleistung eines adäquaten Wissenstransfers meist sehr eingeschränkt. LLMs kompensieren diese Lücke, indem sie mit ihrem

antrainierten Wissen jungen und unerfahrenen Kollegen dauerhaft zur Verfügung stehen (Haas 2024, S. 81). Bei konsequenter Nutzung der Stärken können mehrere Risiken minimiert werden. So können die standardisierten Prozesse im KDD das Risiko von rechtlichen Unsicherheiten erheblich verringern, da die LLMs zunächst primär zur Automatisierung bereits bewährter Prozesse vorgesehen sind und lediglich menschliche Tätigkeiten ersetzen. Erst ein in Folgeschritten denkbarer Einsatz über diesen Bereich hinaus bedürfte einer rechtlichen Abklärung und wird je nach Anwendungsfall, wie Preuß (2024, S. 253) für den Bereich der KI-gestützten Polygraphen darstellt, kritisch gesehen. Es erscheint daher sinnvoll, neue Anwendungswege erst dann zu beschreiten, wenn die Vorgaben der KI-VO auch in deutschen bzw. baden-württembergischen Gesetzesvorgaben ausgestaltet sind. Die Vielzahl an standardisierten Prozessen und die umfassende Datenbasis ermöglichen ein optimales KI-Training. Hierdurch können Fehler durch LLMs deutlich verringert werden.

Die bestehenden IT-Grundlagen und Kompetenzen des P20 bieten bereits eine solide Basis für die Implementierung von LLMs. Auf dieser Grundlage können Sicherheitsfragen frühzeitig geklärt, eine robuste IT-Infrastruktur aufgebaut und Redundanzen implementiert werden, wodurch eine vollständige Abhängigkeit vermieden wird. Denn käme es zur illegalen Penetration des Systems, wäre der Schaden hinsichtlich der erlangten Informationen und der Ausfall eines dann zentralen Elements der Sachbearbeitung desaströs (Haas 2024, S. 86). Um möglichen Risiken zu entgehen, sollte im Umgang mit den internen Schwächen die bislang fehlende KI-Kompetenz der Mitarbeitenden im KDD eine adäquate Berücksichtigung finden. Dadurch lässt sich vermeiden, dass Fehler seitens der LLMs unerkannt bleiben, und stattdessen wird ein professioneller Umgang gewährleistet. Dies sieht auch die KI-VO in Art. 4 vor: Sicherheitsbehörden, die KI-Systeme einsetzen, müssen zuvor sicherstellen, dass ihre Mitarbeitenden über ausreichend KI-Kompetenz verfügen (Pfeffer 2024, S. 64).

Da keine polizeiinterne Entwicklung von LLMs erfolgt, ist es entscheidend, den daraus resultierenden rechtlichen Unsicherheiten und Sicherheitsrisiken, wie sie auch Haas (2024, S. 82) und Pfeffer (2024, S. 57) erwähnen, gebührend Rechnung zu tragen. Auf diese

Weise wird sichergestellt, dass die Vorgaben der KI-VO Berücksichtigung finden und keine sensiblen Daten über ausländische Firmenserver aufgrund dortiger Gesetzesvorgaben abfließen. Auch sind verbindliche vertragliche Regelungen mit externen LLM-Anbietern, die Support-, Update- und Sicherheitsgarantien umfassen, von besonderer Bedeutung, um eine einwandfreie Funktionsfähigkeit der Software sowie eine kontinuierliche Anpassung an den aktuellen Entwicklungsstand zu gewährleisten. Dadurch wird die bestehende technologische Abhängigkeit bestmöglich ausgestaltet.

Um die Chancen von LLMs nutzen zu können, muss im Bereich der Schwächen das Vertrauen in die Technik, wie auch Waldtmann (2024, S. 263) beschreibt, durch angemessenes Change-Management im KDD aufgebaut werden. Durch schnelle und spürbare Personalentlastung und Effizienzsteigerung bei den Ermittlungen wird der Wandel konsolidiert. Die proaktive Aufbereitung vorhandener Trainingsdaten und standardisierter Prozesse innerhalb der Polizei ermöglicht es, den Zeitverzug bis zur Anwendung von LLMs so gering wie möglich zu halten, die Chancen der Technik schnellstmöglich zu nutzen und technologisch nicht gegenüber kriminellen Akteuren ins Hintertreffen zu geraten. Dadurch können externe Anbieter ihre LLMs ohne Verzögerung auf die beabsichtigten polizeilichen Bedürfnisse anpassen. Dieser Aspekt wird insbesondere vor dem Hintergrund einer großen Anbietervielfalt mit einhergehender Option zum regelmäßigen Wechsel des Anbieters aus Preisvergleichs- oder Skalierungsgründen verstärkt (Klan 2024, S. 197).

Fraglich ist, ob die hohen Kosten für die Implementierung und Anpassung einer entsprechenden IT-Infrastruktur durch eine bundesweite Bündelung auf Basis von P20 effizienter kanalisiert werden könnten. Die erzielten Ergebnisse stünden hierbei im Sinne einer Einmalentwicklung und Mehrfachnutzung anderen Bundesländern zur Verfügung. Ein solch gebündeltes Vorgehen würde darüber hinaus eine stärkere Verhandlungsbasis im hart umkämpften und teuren Markt der LLM-Anbieter ergeben und gleichzeitig die angestrebte Harmonisierung auf bundesweiter Ebene fördern. Zumindest die Struktur von P20, das mit agilen Management-Methoden arbeitet, würde eine derartige Bündelung grundsätzlich zulassen (Wiemann 2023).

Schlussfolgerung

„Künstliche Intelligenz (KI) hat das Potenzial, unser Leben ganz grundsätzlich zu verändern“, betonte der baden-württembergische Innenminister Thomas Strobl (2024) zur Eröffnung des sechsten CyberSicherheitsForums. Tatsächlich lässt sich in der Gesamtschau festhalten, dass die Anwendungsmöglichkeiten von LLMs im Aufgabenbereich des KDD der Polizei Baden-Württemberg enormes Potenzial freisetzen. Speziell die in den vorhergehenden Abschnitten beschriebenen Stärken und Chancen zeigen, dass die Polizei optimale Grundvoraussetzungen für eine Implementierung aufweist und bei einer Einführung von LLMs erhebliche Effizienz- und Effektivitätssteigerungen erfährt. Trotz der positiven Aspekte ist es ebenso wichtig, die Herausforderungen bei einer Implementierung von LLMs angemessen zu berücksichtigen. Hier zeigt die Analyse im Bereich der Schwächen und Risiken, dass besonders die Aspekte KI-Kompetenz der Mitarbeitenden, rechtliche Unsicherheiten, Kosten und Sicherheit erfolgskritisch sind.

Die im Rahmen einer abschließenden Gesamtbetrachtung ableitbaren Handlungsempfehlungen sehen somit bei aller Automatisierung der polizeilichen Tätigkeit im KDD den Menschen als fachkompetente, finale und vor allem unabdingbare Kontrollinstanz vor. Damit er die grundlegenden Änderungen, welche LLMs im Arbeitsalltag bewirken, akzeptiert, ist ein gelungenes Change-Management von zentraler Bedeutung. Zudem bedarf es entsprechender Fortbildungen und Anpassungen im Studium, damit die Anwendenden über entsprechende KI-Kompetenz verfügen, alle Möglichkeiten und insbesondere die Grenzen der Systeme kennen und die Polizei den Vorgaben der KI-VO entspricht. Um den bestehenden Rechtsunsicherheiten bei der Implementierung von LLMs im polizeilichen Kontext entgegenzuwirken, ist darüber hinaus eine schrittweise Einführung essenziell, da sonst mögliche Klagen eine schnelle technische Weiterentwicklung der Polizei hemmen könnten. Darüber hinaus empfiehlt es sich, die durch die Einführung von LLMs freigesetzten Finanzmittel gezielt dafür einzusetzen, Kosten für notwendige Anpassungen in der IT-Infrastruktur zu tragen und gleichzeitig die Programmierung von LLM-basierten App-Anwendungen für dienstliche Smartphones

voranzutreiben, um die mobile Sachbearbeitung nachhaltig zu stärken. Abschließend sollte, bei Verzicht auf eine eigene Entwicklung von LLMs und zur Reduzierung von rechtlichen Unsicherheiten sowie Sicherheitsrisiken, stets auf deutsche oder europäische Anbieter als Vertragspartner zurückgegriffen werden.

Abseits dieses Beitrags gilt es zukünftig insbesondere noch zu untersuchen, inwieweit sich zu erlassende nationalrechtliche Anpassungen infolge der KI-VO oder Rechtsprechungen zu unbestimmten Begriffen konkret auf die Anwendung von LLMs im polizeilichen Kontext auswirken und welche Schwerpunkte Bildungsangebote zur Steigerung der KI-Kompetenz von Polizeibeamtinnen und Polizeibeamten setzen sollten.

Literaturverzeichnis

Bataineh A, Sickler R, Morris W, Pedersen K (2023) The Impact of AI-Generated Reports for Law Enforcement: a Call for Responsible Integration and Interpretability. IPA Information Professionals Association. information-professionals.org/the-impact-of-ai-generated-reports-for-law-enforcement-a-call-for-responsible-integration-and-interpretability-2/ (22.12.2024)

Bitkom e.V. (2023) KI in der Polizei – Einsatzpotentiale und Lösungsansätze zur Implementierung. bitkom.org/sites/main/files/2023-10/bitkom-positions-papier-ki-polizei-einsatz-implementierung.pdf (23.11.2024)

Brendt D, Amberg J (2018): Mitarbeiterführung erfolgreich und praxisorientiert; Changemanagement – Führungsinstrumente – Betriebliche Gesundheitsförderung. Praxiswissen Wirtschaft, Band 146. Expert-Verlag GmbH Fachverlag für Wirtschaft und Technik, Tübingen

Brunnbauer M (2024): Potentiale und Gefahren von Large Language Models aus der polizeilichen Sicht. In: Honekamp W, Labudde D (Hrsg.): Polizei-Informatik 2024. Rediroma-Verlag, Remscheid; 234-239

Bundesamt für Sicherheit in der Informationstechnik (2024) Generative KI-Modelle; Chancen und Risiken für Industrie und Behörden. bsi.bund.de/SharedDocs/Downloads/DE/BSI/KI/Generative_KI-Modelle.pdf?__blob=publicationFile&v=5 (25.11.2024)

Bundeskriminalamt (2024) Technologien. bka.de/DE/UnsereAufgaben/Ermittlungsunterstuetzung/Technologien/technologien_node.html (21.08.2024)

Bundesministerium des Innern und für Heimat (2023) SWOT Analyse. orghandbuch.de/Webs/OHB/DE/Organisationshandbuch-NEU/4_MethodenUndTechniken/Methoden_A_bis_Z/SWOT_Analyse/swot_analyse_node.html (24.11.2024)

Bundesministerium des Innern und für Heimat (2024) P20 Polizei 20/20. bmi.bund.de/DE/themen/sicherheit/programm-p20/programm-p20-node.html (23.11.2024)

Die Bundesregierung (2018) Strategie Künstliche Intelligenz der Bundesregierung. bundesregierung.de/resource/blob/997532/1550276/3f7d3c41c6e05695741273e78b8039f2/2018-11-15-ki-strategie-data.pdf (14.11.2024)

Europäisches Parlament (2020) 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 (14.11.2024)

Gebhardt K (2024) Das Kriminal-Lexikon, alles über Polizei und Strafrecht! Dokumentation von Ereignissen. kriminal-lexikon.de/cms/lexikon/38-lexikon-d/4812-dokumentation-von-ereignissen.html (12.12.2024)

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

Innenministerium Baden-Württemberg – Landespolizeipräsidium (2024) Die Vielfalt des Polizeiberufs. karriere-polizei-bw.de/berufsvielfalt/ (23.11.2024)

Kelbert P, Siebert J, Jöckel L (2023) Was sind Large Language Models? Und was ist bei der Nutzung von KI-Sprachmodellen zu beachten? Fraunhofer IESE. Blog des Fraunhofer-Institut für Experimentelles Software Engineering. iese.fraunhofer.de/blog/large-language-models-ki-sprachmodelle/ (14.11.2024)

Kirn S, Müller-Hengstenberg C (2014): Intelligente (Software-)Agenten: Von der Automatisierung zur Autonomie? Verselbstständigung technischer Systeme. MMR – MultiMedia und Recht 2014, Heft 4; 225-232

Klan D (2024): P20 – Polizeiliche Sachbearbeitung der Zukunft schon heute. In: Honekamp W, Labudde D (Hrsg.): Polizei-Informatik 2024. Rediroma-Verlag, Remscheid; 192-200

Kotter J (2011): Leading Change. Wie Sie Ihr Unternehmen in acht Schritten erfolgreich verändern. Verlag Franz Vahlen GmbH, München

Krönke Ch (2024): Das europäische KI-Gesetz: Eine Verordnung mit Licht und Schatten. NVwZ – Neue Zeitschrift für Verwaltungsrecht 2024, Heft 8; 529-533

Küster S (2019) Wann wird eigentlich die Mordkommission eingeschaltet? Alexandra Herbstrith weiß es. Sie erzählt von ihren Ermittlungen und unerträglichen Einsätzen. Südkurier. suedkurier.de/baden-wuerttemberg/Wann-wird-eigentlich-die-Mordkommission-ingeschaltet-Alexandra-Herbstrith-weiss-es-Sie-erzaehlt-von-ihren-Ermittlungen-und-unertraeglichen-Einsaetzen;art417930,10355107 (23.11.2024)

Landtag von Baden-Württemberg (2020) Drucksache 16/7855; Antrag der Abg. Dr. Ulrich Goll u. a. FDP/DVP und Stellungnahme des Ministeriums für Inneres, Digitalisierung und Migration; Digitalisierung der Polizeiarbeit in Baden-Württemberg. landtag-bw.de/files/live/sites/LTBW/files/dokumente/WP16/Drucksachen/7000/16_7855_D.pdf (30.11.2024)

Metzmacher D (2024) Wettrennen der Tech-Firmen. Welches KI-Sprachmodell ist das beste? zdfheute.zdf.de/nachrichten/wissen/kuenstliche-intelligenz-ki-sprachmodell-vergleich-100.html (30.11.2024)

Ministerium des Inneren, für Digitalisierung und Kommunen Baden-Württemberg (2019) Neue App für die Polizei. im.baden-wuerttemberg.de/de/service/presse-und-oeffentlichkeitsarbeit/pressemitteilung/pid/neue-app-fuer-die-polizei (25.11.2024)

Münch H (2024) Wie wir die Welle reiten – Chancen und Potenziale von KI für die polizeiliche Arbeit. BKA Herbsttagung. [bka.de/SharedDocs/Downloads/DE/Publikationen/Herbsttagungen/2024/herbsttagung2024PR_Muench.pdf?__blob=publicationFile&v=5](https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/Herbsttagungen/2024/herbsttagung2024PR_Muench.pdf?__blob=publicationFile&v=5) (14.12.2024)

Pekar-Milicevic M (2016): Polizeiliches Performance Management; Theorie, Implementierung und Wirkung. Springer VS. Wiesbaden

Pfeffer K (2024): Die EU-Regulierung des Einsatzes künstlicher Intelligenz: Auswirkungen der KI-VO auf die Sicherheitsbehörden insbesondere bei der „smarten Gesichtserkennung“. In: Honekamp W, Labudde D (Hrsg.): Polizei-Informatik 2024. Rediroma-Verlag, Remscheid; 55-66

Preuß T (2024): Chancen und Risiken KI-basierter Wahrheitsfindung im Strafverfahren. In: Honekamp W, Labudde D (Hrsg.): Polizei-Informatik 2024. Rediroma-Verlag, Remscheid; 247-258

Siebert J, Kelbert P (2024) Wie funktionieren LLMs? Ein Blick ins Innere großer Sprachmodelle. Fraunhofer IESE. Blog des Fraunhofer-Institut für Experimentelles Software Engineering. [iese.fraunhofer.de/blog/wie-funktionieren-llms/](https://www.iese.fraunhofer.de/blog/wie-funktionieren-llms/) (26.11.2024)

Stephan M (2010): SWOT-Analyse: Controllinginstrument zur Identifikation strategischer Handlungsoptionen. In: Klein A (Hrsg.): Strategische Controlling-Instrumente: Die wichtigsten Konzepte und Methoden; der Ablauf der strategischen Planung; kommunikatives Handwerkszeug für den Controller. Haufe-Mediengruppe, Freiburg; 81-100

Strobl T (2024) 6. CyberSicherheitsForum. Ministerium des Inneren, für Digitalisierung und Kommunen Baden-Württemberg. [baden-wuerttemberg.de/de/service/presse/pressemitteilung/pid/sechstes-cybersicherheitsforum](https://www.baden-wuerttemberg.de/de/service/presse/pressemitteilung/pid/sechstes-cybersicherheitsforum) (03.12.2024)

SWR Aktuell (2024) Aleph Alpha: Land setzt ab September auf Künstliche Intelligenz in Behörden. [swr.de/swraktuell/baden-wuerttemberg/aleph-alpha-ki-landesregierung-entlastung-behoerden-100.html](https://www.swr.de/swraktuell/baden-wuerttemberg/aleph-alpha-ki-landesregierung-entlastung-behoerden-100.html) (25.11.2024)

Trichtl U (2023) Big Tech: Der Kampf um die KI-Vorherrschaft. Capital. [capital.de/geld-versicherungen/big-tech--der-kampf-um-die-ki-vorherrschaft-33868804.html](https://www.capital.de/geld-versicherungen/big-tech--der-kampf-um-die-ki-vorherrschaft-33868804.html) (13.12.2024)

Trippner D (2021): Das 1x1 der Strategie; Know-how und Methoden für Menschen, die etwas bewegen wollen. Haufe Group, Freiburg München Stuttgart

Unterberg S (2023) So nutzen Lehrkräfte ChatGPT im Unterricht. Spiegel. [spiegel.de/panorama/bildung/chatgpt-im-unterricht-so-nutzen-lehrkraefte-die-ki-a-10669546-a1a0-49d1-915b-27beae9962fc](https://www.spiegel.de/panorama/bildung/chatgpt-im-unterricht-so-nutzen-lehrkraefte-die-ki-a-10669546-a1a0-49d1-915b-27beae9962fc) (25.11.2024)

Verbraucherzentrale (2024) Künstliche Intelligenz: Funktionsweise, Anwendungsgebiete und Risiken. [verbraucherzentrale.de/wissen/digitale-welt/apps-und-software/kuenstliche-intelligenz-funktionsweise-anwendungsgebiete-und-risiken-89112](https://www.verbraucherzentrale.de/wissen/digitale-welt/apps-und-software/kuenstliche-intelligenz-funktionsweise-anwendungsgebiete-und-risiken-89112) (21.08.2024)

Volkman D, Schildein S, Povalej R (2024): Digitaler Zwilling – Potenziale für die Polizei. In: Honekamp W, Labudde D (Hrsg.): Polizei-Informatik 2024. Rediroma-Verlag, Remscheid; 30-45

Waldtmann C (2024): Einsatz KI-basierter Technologien zur Bewältigung des polizeilichen Vorgangsaufkommens bei Massendelikten. In: Honekamp W, Labudde D (Hrsg.): Polizei-Informatik 2024. Rediroma-Verlag, Remscheid; 259-263

Wiemann T (2023): Von der Konzeption in die Umsetzung; P20 nimmt weiter Gestalt an. DP – das MitgliederMagazin der Gewerkschaft der Polizei. [dp-digital.gdp.de/collection/de.gdp.dp.issue022023_165/article/de.gdp.dp.issue202302.bund61229](https://www.dp-digital.gdp.de/collection/de.gdp.dp.issue022023_165/article/de.gdp.dp.issue202302.bund61229) (15.12.2024).

Einführung eines auf Künstlicher Intelligenz basierenden Chatbots in das polizeiinterne Soziale Netzwerk null1|5 der Polizei des Landes Niedersachsen – Eine Machbarkeitsuntersuchung

Lars Schröder

Die fortschreitende Digitalisierung stellt Organisationen vor große Herausforderungen, wie etwa die Anpassung an neue Technologien, die Gewährleistung einer schnellen und sicheren Informationsverarbeitung sowie die Integration digitaler Lösungen in bestehende Strukturen. Dies gilt auch für Polizeibehörden, die aufgrund ihrer komplexen Strukturen und Aufgabenfelder auf eine effektive Informationsverarbeitung angewiesen sind. Neben der Bewältigung neuer Deliktsfelder und der Einführung neuer Fachanwendungen sind sie gefordert, umfangreiche Informationen effizient zu verwalten und Mitarbeitenden zeit- und ortsunabhängig bereitzustellen. Wissensmanagementsysteme gewinnen in diesem Kontext zunehmend an Bedeutung, da sie den Zugriff auf aktuelle Informationen erleichtern, die Zusammenarbeit fördern und die Effizienz interner Prozesse steigern können (vgl. Offergelt et.al, 2024, S. 8).

Vor diesem Hintergrund führte die Polizei des Landes Niedersachsen 2021 das polizeiinterne soziale Netzwerk „null1|5“ (PSN) ein. Diese Plattform kombiniert Kommunikations- und Kollaborationsfunktionen mit einem Wissensmanagementsystem, dessen zentraler Bestandteil eine durchsuchbare Wissensdatenbank ist. Mit mittlerweile über 700 Fachbeiträgen zu polizeirelevanten Themen leidet die Datenbank jedoch unter unkontrolliertem Wachstum und mangelnder systematischer Kontrolle. Dies führt zu Unübersichtlichkeit und veralteten Inhalten, wodurch die Informationssuche erschwert wird. Studien zeigen, dass ineffiziente Wissensbereitstellung in Kombination mit hohen Suchzeiten Frustration, psychische Belastung und eine sinkende Arbeitszufriedenheit der Nutzenden begünstigen kann (vgl. Piecha & Hacker, 2021, S. 3). Eine vielversprechende Lösung, dieser Herausforderung zu begegnen, könnte der Einsatz von Künstlicher Intelligenz (KI) in Verbindung mit der Chatbot-Technologie sein. Die Implementierung eines KI-basierten Chatbots in das

PSN der Polizei des Landes Niedersachsen könnte zukünftig die Effizienz der Informationssuche steigern, die Übersichtlichkeit der Wissensdatenbank verbessern und somit die Akzeptanz der Plattform nachhaltig steigern.

Dieser Beitrag analysiert vor diesem Hintergrund den potenziellen Nutzen, die technischen Anforderungen und die organisatorischen Rahmenbedingungen, die für eine erfolgreiche Implementierung eines solchen Chatbots notwendig wären. Zudem werden Herausforderungen und Risiken bei der Einführung betrachtet. Zur Untersuchung wurde eine qualitative Machbarkeitsstudie durchgeführt, die auf Experteninterviews mit dem technischen Projektleiter der Plattform und einer Führungskraft der IT-Abteilung der Polizei Niedersachsen basiert. Ziel war es, sowohl die strategischen als auch die technologischen Voraussetzungen für die Implementierung eines KI-basierten Chatbots zu beleuchten.

Zunächst werden die technologischen Grundlagen von KI-basierten Chatbots erläutert und die Wissensdatenbank des PSN vorgestellt, um ein grundlegendes Verständnis für den Kontext des Beitrags zu schaffen. Anschließend folgen eine ausführliche Beschreibung der Methodik der Untersuchung sowie eine detaillierte Darstellung des methodischen Vorgehens. Darauf aufbauend werden die Ergebnisse der Experteninterviews präsentiert und analysiert, die als Grundlage für die anschließende Diskussion dienen. In dieser wird die Umsetzbarkeit eines KI-basierten Chatbots im Kontext des PSN kritisch bewertet. Abschließend werden die zentralen Erkenntnisse zusammengefasst und ein Ausblick auf die Chancen und Herausforderungen einer möglichen Implementierung gegeben.

Hintergrund

In diesem Kapitel soll zunächst die Wissensdatenbank des PSN vorgestellt werden. Anschließend erfolgt eine theoretische Einführung in die technologischen Grundlagen und Funktionsweisen von Chatbots unter der Berücksichtigung von KI.

Polizeiinternes Soziales Netzwerk null1|5

Das PSN dient als zentrale Plattform zur Unterstützung der internen Kommunikation, Kollaboration und Wissensverwaltung innerhalb der niedersächsischen Polizei. Es bietet verschiedene Module, wie strukturierte Organisationsübersichten, Diskussions- und Informationsbereiche, sowie Werkzeuge für den Zugriff auf Fachanwendungen. Personalisierte Funktionen wie ein Newsfeed und integrierte Suchfunktion mit Filtern auf Tags und Schlagwörter sollen die Navigation erleichtern und einen schnellen Zugriff auf relevante Informationen ermöglichen (vgl. Niedersächsisches Ministerium für Inneres und Sport, 2021, S. 4-5).

Die Wissensdatenbank ist das Kernstück von PSN und dient als zentrale, durchsuchbare Ablage für dienstliches Fach- und Strukturwissen. Sie gliedert sich grundsätzlich in „Wikis“ (allgemeine Wikis und Fachwikis) und eine „Dokumentenablage“, welche Erlasse, Geschäftsverteilungspläne, Checklisten und Mustervorlagen enthält. Die allgemeinen Wikis können von allen Nutzenden frei bearbeitet und ergänzt werden, wodurch die kollaborative Wissensgenerierung ermöglicht werden soll. Die Fachwikis hingegen werden von autorisierten Redaktionen betreut und bieten spezialisiertes Wissen zu verschiedenen Themengebieten, beispielsweise zum Umgang mit dem Vorgangsbearbeitungssystem der Polizei des Landes Niedersachsen (Niedersächsisches Ministerium für Inneres und Sport, 2021, S. 5). Insgesamt sind in der Wissensdatenbank inzwischen mehr als 700 Wikis zu finden, welche nur teilweise von Redaktionen aktuell gehalten werden können. Die zunehmende Informationsfülle trägt maßgeblich zur Unübersichtlichkeit der Plattform bei und erschwert es den Nutzenden trotz der vorhandenen Suchfunktion, relevante Inhalte effizient zu finden.

Chatbots

Chatbots sind komplexe, IT-gestützte Dialogsysteme, die flexibel auf verschiedene Datenquellen zugreifen und sich in unterschiedlichste Plattformen integrieren lassen. Mithilfe von Technologien der KI können sie auch komplexe Anfragen präzise beantworten (vgl. Koh-

ne et al., 2020, S. 1). Es ist jedoch wichtig zu betonen, dass nicht alle Chatbot-Systeme auf KI basieren. Es wird zwischen KI-basierten Dialogsystemen und regelbasierten Chatbot-Anwendungen unterschieden (vgl. Böhm et al., 2021, S. 6). Regelbasierte Systeme arbeiten mit vordefinierten Frage-Antwort-Vorlagen und reagieren auf vorab programmierte Schlüsselwörter, wodurch ihre Funktionalität begrenzt ist (vgl. Gärtner, 2020, S. 70). In diesem Beitrag wird der Fokus jedoch ausschließlich auf Chatbots gelegt, die auf KI-Technologien basieren – eine Betrachtung von regelbasierten Chatbots erfolgt nicht. KI wird in diesem Zusammenhang als Sammelbegriff für Technologien verstanden, die Maschinen mit der Fähigkeit ausstatten, eigenständig Probleme zu lösen, und die entweder das Niveau menschlicher Intelligenz erreichen oder übertreffen sollen (vgl. Petry & Jäger, 2021, S. 45-46). Grundsätzlich unterscheidet die Wissenschaft dabei in drei Kategorien von KI (schwache KI, starke KI und Superintelligenz), wobei in diesem Beitrag lediglich die bereits erforschte und sowohl theoretisch als auch praktisch einsetzbare schwache KI beim Einsatz von Chatbots Anwendung findet. Schwache KI ist auf spezifische Anwendungsbereiche wie Spracherkennung, Navigation oder Übersetzungsdienste beschränkt. Sie imitiert sprachliche und logisch-mathematische Intelligenz und wird zunehmend in Chatbots eingesetzt, um Benutzeranfragen zu verstehen und relevante Informationen bereitzustellen (vgl. Etscheid et al., 2020, S. 8).

Technologische Grundlagen

Ein zentraler Aspekt von Chatbots ist ihre Fähigkeit, menschenähnliche Dialoge über Audio- oder Textschnittstellen zu führen (Haristiani, 2019, S. 1-2). Diese Systeme basieren auf Spracherkennung und simulieren Konversationen durch ein Frage-Antwort-Protokoll, das selbstständig agiert (Ali & Amin, 2019, S. 1-2). Ein wesentlicher technologischer Bestandteil ist das Natural Language Processing (NLP), das alle Prozesse umfasst, die es einem System ermöglichen, natürlichsprachliche Eingaben zu verarbeiten. NLP dient als Überbegriff für Technologien, die menschliche Sprache analysieren, verstehen und darauf reagieren können (vgl. Wilke & Bendel, 2022, S. 651-653). Es beinhaltet Teilbereiche wie die Segmentierung von Texten in kleinere Einheiten, die Identifikation von Schlüsselbegrif-

fen und die grammatikalische Analyse, die notwendig sind, um die Struktur und Bedeutung von Eingaben zu erkennen und korrekt zu verarbeiten. Ein bedeutender Fortschritt im Bereich NLP sind Large Language Models (LLMs). Diese KI-basierten Modelle sind darauf spezialisiert, Sprache zu verstehen und zu generieren. Sie werden auf umfangreichen Textdatensätzen trainiert, was ihnen ermöglicht, den Kontext von Anfragen präzise zu analysieren und relevante Antworten zu generieren (vgl. Brown et al., 2020, S. 2). Innerhalb von NLP spielen ebenfalls Natural Language Understanding (NLU) und Natural Language Generation (NLG) eine zentrale Rolle. NLU fokussiert sich darauf, die Bedeutung hinter der Eingabe zu interpretieren und Benutzerabsichten zu erkennen, während NLG passende und kontextgerechte Antworten generiert (vgl. Wilke & Bendel, 2022, S. 653; Gärtner, 2020, S. 42). Diese Technologien sind entscheidend, um die Fähigkeit von Chatbots zu gewährleisten, komplexe Benutzeranfragen präzise zu bearbeiten und so ihre Einsatzmöglichkeiten im Wissensmanagement effektiv zu ermöglichen. Sie bilden die Basis für die Funktionsweise von Chatbots, die im nächsten Abschnitt genauer erläutert wird.

Funktionsweise von Chatbots

Die Funktionsweise von Chatbots lässt sich in vier Phasen gliedern. In der ersten Phase wird die Anfrage des Nutzers über eine Schnittstelle entgegengenommen, beispielsweise über ein Chat-Fenster, eine App, soziale Netzwerke oder Spracheingabe. In der zweiten Phase erfolgt die Verarbeitung der Anfrage. Der Text wird direkt oder mithilfe von „Speech-to-Text“-Technologien in eine maschinenlesbare Form umgewandelt, der Sinn und Kontext der Anfrage werden erfasst und anschließend durch entsprechende Technologien analysiert (vgl. Kohne et al., 2020, S. 2). In der dritten Phase wird eine passende Antwort generiert, indem der Chatbot auf Informationsquellen wie Wissensdatenbanken, externe Schnittstellen oder Expertensysteme zugreift. Dabei kommt NLG zum Einsatz, das mithilfe von Regeln oder trainierten Modellen personalisierte und kontextgerechte Antworten erstellt (vgl. Kohne et al., 2020, S. 3; Gärtner, 2020, S. 42). Abschließend wird in der vierten Phase die generierte Antwort entweder textuell oder über Sprachsynthese („Text-to-Speech“) an

den Nutzenden zurückgegeben. Neben diesen vier Phasen spielt maschinelles Lernen (ML) eine zentrale Rolle in der Chatbot-Technologie. ML ermöglicht die präzise Verarbeitung natürlicher Sprache, das Lernen aus Interaktionen und die kontinuierliche Optimierung von Antworten (vgl. Kreuzer & Sirrenberg, 2019, S. 5). Anders als statische Systeme können Chatbots durch Rückmeldungen ihre Fähigkeiten zur Mustererkennung stetig verbessern (vgl. Wittpahl, 2019, S. 24-26). Dadurch sind sie in der Lage, Benutzerabsichten besser zu deuten und Konversationen über mehrere Schritte hinweg sinnvoll anzupassen (vgl. Wagener, 2019, S. 25-26).

Moderne Chatbots sind somit in der Lage, auch komplexe Anfragen zu beantworten, verschiedene Datenquellen zu kombinieren und den Kontext vorheriger Interaktionen zu berücksichtigen. Diese Eigenschaften machen sie zu einer Schlüsseltechnologie für effiziente Informationssysteme im Wissensmanagement. Um zu prüfen, inwiefern ein solcher Chatbot in diesem spezifischen Kontext realisierbar ist, wird im nächsten Kapitel die Methodik der durchgeführten Untersuchung beschrieben.

Methodik der Machbarkeitsuntersuchung

Im Rahmen der Machbarkeitsuntersuchung wird ein qualitativer Ansatz verfolgt, um systematisch die Voraussetzungen und Herausforderungen der Einführung eines KI-Chatbots im Intranet der Polizei Niedersachsen zu analysieren. Es wurden Experteninterviews mit einer langjährigen Führungskraft der IT-Abteilung des Landes Niedersachsen sowie dem technischen Verantwortlichen und Projektleiter von PSN durchgeführt. Diese Expertenperspektiven ermöglichen eine fundierte Analyse, da sie sowohl strategische als auch technische Aspekte der möglichen Einführung eines KI-basierenden Chatbots abdecken.

Die erhobenen Daten werden mithilfe der qualitativen Inhaltsanalyse nach Mayring ausgewertet. Diese Methode ist dadurch besonders geeignet, dass sie strukturiert und systematisch zentrale Aussagen aus den Interviews extrahiert und einordnet. Durch die Kombination

von deduktivem und induktivem Vorgehen wird sichergestellt, dass sowohl vorhandene theoretische Konzepte geprüft als auch neue, aus den Antworten der Experten entwickelte Aspekte berücksichtigt werden. Der deduktive Ansatz wird genutzt, indem die Kategorien des Fragebogens aus bestehender Literatur abgeleitet werden. Gleichzeitig erlaubt der induktive Ansatz die Generierung neuer Subkategorien aus den Interviews, um praxisnahe und bislang unbeachtete Themen in die Analyse einzubeziehen. (vgl. Mayring & Fenzl, 2019, S. 633-638).

Der Fokus der Untersuchung liegt dabei auf folgenden Themengebieten: potenzieller Nutzen, Herausforderungen und Risiken, technische Machbarkeit sowie organisatorische Faktoren (untergliedert in Ressourcenbedarfe, Zeitaufwand und die Übernahme bestehender Lösungen). Eine datenschutzrechtliche Betrachtung wird aufgrund der Komplexität in diesem Beitrag nicht durchgeführt. Die Ergebnisse der Analyse werden im Anschluss im Rahmen der Diskussion mit wissenschaftlichen Erkenntnissen verglichen und umfassend bewertet. Die qualitative Inhaltsanalyse nach Mayring stellt somit eine ideale Methode dar, um die Machbarkeit eines KI-Chatbots in einem komplexen und spezifischen Kontext wie dem der Polizei Niedersachsen fundiert und nachvollziehbar zu untersuchen.

Ergebnisse

Im Folgenden werden die Ergebnisse der Experteninterviews kategorisch dargestellt.

Potenzieller Nutzen, Herausforderungen und Risiken

Ein KI-gestützter Chatbot im Intranet der Polizei Niedersachsen könnte laut den Experten die Nutzerakzeptanz und Nutzung des Netzwerks erheblich steigern. Derzeit nutzen nur etwa 5.000 bis 6.000 von 26.000 Mitarbeitenden das Netzwerk aktiv. Ein Chatbot könnte Gelegenheitsnutzende durch vereinfachte Such- und Recherchemöglichkeiten unterstützen und die Vernetzung sowie Wissensnutzung innerhalb der Organisation fördern. Die Interaktion in

natürlicher Sprache würde komplexe, kontextbezogene Antworten ermöglichen und die Effizienz der Informationsbeschaffung steigern, wodurch er über klassische Suchfunktionen hinaus einen dynamischen Mehrwert schafft.

Die Einführung eines Chatbots birgt laut dem technischen Verantwortlichen Herausforderungen, da er bei komplexen Anfragen oft nur begrenzte Antworten liefern könne, was Frustration bei den Nutzenden verursachen könnte. Die Führungskraft ergänzt, dass die „vermenschlichte“ Form der Interaktion für manche Mitarbeitenden ungewohnt sei und anfängliche Skepsis auslösen könnte. Beide Experten sehen diese Herausforderungen jedoch als überwindbar, etwa durch gezielte Öffentlichkeitsarbeit und die Bereitstellung alternativer Suchmöglichkeiten für skeptische Nutzende.

Die Experten betonen unterschiedliche, sich ergänzende Aufgaben für den Chatbot. Der technische Verantwortliche sieht den Hauptnutzen in der Optimierung von Recherchefunktionen und der Bereitstellung von Wissen. Die Führungskraft erweitert dies um kontextuelle Erklärungen, die Einarbeitung neuer Mitarbeitender und die Digitalisierung operativer Prozesse wie Checklisten und standardisierte Abläufe. Beide Experten erkennen das Potenzial des Chatbots, die Nutzung und Effizienz des Netzwerks zu steigern. Herausforderungen wie die Begrenztheit bei komplexen Anfragen und anfängliche Akzeptanzprobleme sind real, jedoch mit gezielten Maßnahmen überwindbar. Einig sind sie sich darin, dass der Chatbot nicht nur als Informationswerkzeug, sondern als vielseitiges Unterstützungstool konzipiert werden sollte, um organisatorische Abläufe zu erleichtern und die Wissensnutzung zu verbessern.

Technische Machbarkeit

Die technische Machbarkeit eines Chatbots im Intranet der Polizei Niedersachsen hängt von Integrationsmöglichkeiten, Technologien und Infrastruktur ab. Der technische Verantwortliche betont die Notwendigkeit einer flexiblen API, um eine nahtlose Integration in bestehende Webanwendungen zu ermöglichen. API steht für Application Programming Interface und bezeichnet eine Schnittstelle, die es

Software-Anwendungen ermöglicht, miteinander zu kommunizieren und Daten oder Funktionen auszutauschen. Eine Implementierung könnte über ein separates Chatsystem erfolgen, das Schlüsselbegriffe erkennt und Antworten direkt bereitstellt, wobei der Entwicklungsaufwand durch den Einsatz nichtproprietärer Technologien reduziert werden könnte. Ein robustes Verständnis natürlicher Sprache (NLP) ist essenziell, damit der Chatbot den Sinn von Anfragen erfassen kann, insbesondere da viele Nutzende wenig technisches Verständnis haben. Die Führungskraft schlägt ein polizeispezifisches LLM vor, das sich durch Analyse von Inhalten selbstständig weiterentwickeln und so manuelle Anpassungen minimieren könnte. Beide Experten sind sich einig, dass die Interaktion in natürlicher Sprache den Mehrwert des Chatbots entscheidend steigert.

Hinsichtlich der IT-Infrastruktur bestehen Herausforderungen. Die fehlende Cloud-Unterstützung erfordert lokale Rechenressourcen, die derzeit unzureichend sind. Hochleistungs-Chips für ML wären notwendig, deren Verfügbarkeit jedoch eingeschränkt ist. Die technischen Anpassungen hängen maßgeblich von strategischen Zielen und der Häufigkeit ab, mit der der Chatbot neue Daten lernen soll. Zusammenfassend ist die technische Machbarkeit grundsätzlich gegeben, jedoch nur mit sorgfältiger Planung und Investitionen umsetzbar, um die hohen Anforderungen zu erfüllen. Ein leistungsfähiger Chatbot mit modernen Technologien wie NLP und LLMs könnte erhebliche Vorteile bieten, wenn diese Hürden bewältigt werden.

Organisatorische Faktoren

Die Betrachtung der organisatorischen Faktoren gliedert sich in personelle und finanzielle Ressourcenbedarfe, den Zeitaufwand und das organisatorische Vorgehen.

Ressourcenbedarfe

Die Einführung eines Chatbots für PSN erfordert aus Sicht des technischen Verantwortlichen erhebliche finanzielle und personelle Ressourcen, abhängig von der Implementierungsstrategie. Dabei kommen Eigenentwicklungen, Erwerb eines bestehenden Pro-

dukts oder Übernahme einer externen Lösung infrage. Erfahrungen zeigen, dass die Entwicklungskosten – bei einer Eigenentwicklung – zwischen 100.000 und 200.000 Euro liegen könnten, wobei die genaue Höhe von Funktionalitäten und Integration abhängt. Aufgrund fehlender interner Expertise im Bereich ML ist externe Unterstützung erforderlich, was weitere Kosten verursachen würde und als absolut elementar für die Umsetzung angesehen wird. Alternativ könnte der Plattformanbieter den Chatbot direkt integrieren, was langfristig Wartungsaufwand und Ressourcen sparen könnte.

Zeitaufwand

Die Implementierung könnte bis zu zwei Jahre dauern, einschließlich eines Jahres für die gesetzlich vorgeschriebene Ausschreibung sowie weitere Abstimmungsphasen zwischen Entwicklern und der Polizei. Die Priorisierung des Projekts innerhalb der Behörde ist entscheidend, da es mit anderen Projekten um Ressourcen konkurriert. Eine Machbarkeitsstudie wird von den Experten empfohlen, um organisatorische Hürden frühzeitig zu identifizieren und den Aufwand realistisch einzuschätzen.

Übernahme bestehender Lösungen

Die Übernahme bestehender Chatbot-Lösungen erscheint realistisch. Ein vielversprechendes Beispiel ist ein Chatbot, der in Kooperation mit der TU Berlin für die Onlinewache der Polizei Niedersachsen entwickelt wurde und nun angepasst werden könnte. Da die Polizei die Rechte am Programmcode besitzt, wäre eine kostenfreie Anpassung möglich. Weitere potenzielle Ansätze bieten Chatbots aus anderen Bundesländern, wie Hamburg und Baden-Württemberg, die während der Coronapandemie eingesetzt wurden. Diese könnten an die Anforderungen des PSN angepasst werden und Inspiration oder Grundlage für die Einführung darstellen.

Diskussion

Die Einführung eines KI-basierten Chatbots in das PSN bietet nach Ansicht der polizeilichen Experten nicht nur erhebliche Potenziale zur Verbesserung der Suchfunktionen in der Wissensdatenbank, sondern auch die Möglichkeit, die allgemeine Akzeptanz der Nutzenden für das System zu erhöhen. Weitere Einsatzmöglichkeiten erscheinen ebenfalls als realistisch und ausbaubar. Diese Einschätzung wird durch die Expertise von Schmidt (2024, S. 4) gestützt, der Chatbots in der Lage sieht, die richtigen Informationen im Bereich des Wissensmanagements direkt und schnell bereitzustellen. Zudem sieht Schmidt, genauso wie die polizeiliche Expertise, als einen vieler positiver Nebeneffekte, dass die Einarbeitung neuer Mitarbeitender in den jeweiligen Fachbereichen effektiver gestaltet werden kann. Durch den Zugriff auf aufbereitetes und hinterlegtes Wissen entfallen die Abhängigkeit von Kolleginnen und Kollegen sowie die mühsame Erarbeitung von Hintergrundinformationen (vgl. Schmidt, 2024, S. 4). Damit decken sich die Aussagen der Experten in der Einschätzung, dass der Einsatz eines KI-basierten Chatbots sowohl die Effizienz der Informationsbeschaffung als auch die Arbeitsprozesse insgesamt nachhaltig optimieren kann.

Eine der größten Herausforderungen bei der Einführung des Chatbots wird sowohl seitens der polizeilichen als auch wissenschaftlichen Expertise darin gesehen, dass der Chatbot von Nutzenden akzeptiert und angenommen werden muss, um den größtmöglichen Nutzen zu entfalten (vgl. Kohne et al., 2020, S. 113). Um dieser Herausforderung zu begegnen, wird aus polizeilicher Sicht eine frühzeitige interne Öffentlichkeitsarbeit sowie eine klare Kommunikation der Chatbot-Funktionen angestrebt. Aus wissenschaftlicher Perspektive liegt der Fokus besonders auf dem Entwicklungs- und Einführungsprozess, bei dem ein agiles Vorgehen und somit eine größtmögliche Beteiligung der Nutzenden angestrebt werden sollte (vgl. Kohne et al., 2020, S. 114-115). Ein sorgfältig geplanter Einführungsprozess ist entscheidend, um die Vorteile des Chatbots nachhaltig nutzen zu können und mögliche Widerstände frühzeitig zu minimieren. Dabei ist die kontinuierliche, nutzerzentrierte Weiterentwicklung des Chatbots ein entscheidender Faktor, um den Mehrwert, insbeson-

dere in Hinblick auf die Antwortqualität und die Erweiterung der Inhalte, zu maximieren und die spätere Akzeptanz des Produkts zu steigern (vgl. Kohne et al., 2020, S. 114-115). Der wichtigste Faktor zur regelmäßigen Nutzung von Chatbots wird allerdings darin gesehen, dass das Produkt einen Mehrwert für den Nutzenden generiert. Dieser Mehrwert zeigt sich insbesondere dann, wenn der Chatbot so konzipiert ist, dass er Informationen effizient und präzise bereitstellt und damit das Problem der umfangreichen Datenmengen nachhaltig adressiert (vgl. Kohne et al., 2020, S. 135). Folglich sind bereits in der Frühphase der Implementierung hohe Ansprüche an die Qualität des Chatbots zu stellen sowie längerfristige Ausfallzeiten zu vermeiden (vgl. Lewandowski et al., 2022, S. 12).

Die Implementierung eines Chatbots in die Infrastruktur der Polizei des Landes Niedersachsen wird grundsätzlich als möglich angesehen. Jedoch stellen die hohen Anforderungen an die Rechenkapazitäten, insbesondere durch die essenziellen Technologien wie NLP, LLMs und die intelligente Suche, eine wesentliche Herausforderung dar. Da die vorhandenen Kapazitäten derzeit seitens der polizeilichen Expertise als unzureichend bewertet werden, könnte dies die Performance der Anwendung erheblich beeinträchtigen. Auch aus wissenschaftlicher Sicht gelten Technologien wie NLP und LLMs als unerlässlich für die effektive Nutzung eines Chatbots und gehen zugleich mit erheblichen Anforderungen an die Rechenkapazitäten einher (vgl. Kohne et al., 2020, S. 60). Bei zu hoher Auslastung können Performanceprobleme entstehen, was zu einer verminderten Qualität sowie Verzögerung der Antworten und folglich zu Akzeptanzproblemen bei den Nutzenden führt. Dieser Problematik kann ausschließlich durch die Erweiterung der Serverkapazitäten und sonstiger Infrastruktur begegnet werden, welche teuer angemietet oder beschafft werden müsste (vgl. Schwarz, Ertel, 2023, S. 42). Die Anforderungen an die Rechenkapazitäten und die infrastrukturellen Anpassungen verdeutlichen, dass die technische Umsetzbarkeit eines Chatbots eng mit den verfügbaren Ressourcen verknüpft ist.

Beim Ressourcenbedarf ist zwischen der Entwicklung einer individuellen Lösung und dem Erwerb einer kommerziellen Software zu unterscheiden. Gemäß § 7 der Landeshaushaltsordnung müssen bei

finanzwirksamen Maßnahmen – und somit auch in dieser Betrachtung – die Kriterien der Wirtschaftlichkeit und Sparsamkeit entscheidungsleitend sein. Die Wahl zwischen den beiden Varianten richtet sich nach dem Ergebnis der Wirtschaftlichkeitsuntersuchung, wobei die wirtschaftlichere Option zu bevorzugen ist. Aus polizeilicher Sicht stellen beide Ansätze grundsätzlich realisierbare Möglichkeiten für die Implementierung des Chatbots dar. Bei der Entwicklung einer individuellen Lösung sind sowohl die initialen Entwicklungskosten als auch die laufenden Kosten für Pflege und Wartung zu berücksichtigen (vgl. Kohne et al., 2020, S. 113). Beim Erwerb einer kommerziellen Lösung als Plattform setzen sich die Kosten hingegen aus Lizenzgebühren und Wartungskosten zusammen (vgl. Kohne et al., 2020, S. 113).

Für eine Eigenentwicklung ist die erforderliche fachliche Expertise unverzichtbar, die aus polizeilicher Sicht insbesondere im Bereich des ML extern eingekauft werden müsste. Aus wissenschaftlicher Sicht wird darüber hinaus für die Entwicklung einer Konversation mit Chatbots ein disziplinär übergreifendes Projektteam benötigt, welches Wissen aus den Disziplinen Linguistik, Konversationsdesign, Inhaltsmanagement, IT und Psychologie vereint (vgl. Kohne et al., 2020, S. 113). Diese Expertisen sind im polizeilichen Umfeld nicht vorhanden, weswegen von einer Eigenentwicklung abgesehen werden sollte. Als zielführend könnte eher die kommerzielle Entwicklung des Chatbots über den Plattformanbieter sein, der das Produkt selbstständig weiterentwickelt und an die Bedarfe der Polizei anpasst. Die entstehenden Kosten würden über Lizenzkosten umgelegt und in den laufenden Haushalt der Polizei des Landes Niedersachsen überführt werden.

Als sinnvollste und wirtschaftlichste Alternative dürfte sich allerdings die Übernahme einer bereits bestehenden Lösung herauskristallisieren. Bereits in anderen Behörden stehen verschiedene Chatbots zur Verfügung, die kostenneutral übernommen werden könnten, sofern sie die erforderliche Funktionalität bieten und in die bestehende Infrastruktur integriert werden können. Aus polizeilicher Sicht wird dies grundsätzlich als umsetzbar eingeschätzt. Eine gezielte Marktanalyse sowie die Beobachtung aktueller Entwicklungen in anderen

Bundesländern könnten dazu beitragen, eine passende Lösung zu identifizieren und zum geeigneten Zeitpunkt zu übernehmen. In der Gesamtbetrachtung dürfte dies die praktikabelste und wirtschaftlichste Variante darstellen.

Schlussfolgerungen

Der vorliegende Beitrag hat gezeigt, dass die Implementierung eines KI-gestützten Chatbots im PSN der Polizei Niedersachsen ein großes Potenzial zur Optimierung der Wissensmanagementprozesse bietet. Angesichts der stetig wachsenden Informationsmengen und der damit einhergehenden Unübersichtlichkeit stellt ein Chatbot eine vielversprechende Lösung dar, um die Effizienz der Informationssuche zu erhöhen, die Arbeitszufriedenheit der Mitarbeitenden zu fördern und die Nutzung der Plattform insgesamt zu verbessern.

Die Analyse hat deutlich gemacht, dass ein Chatbot durch den Einsatz moderner Technologien wie NLP und ML in der Lage ist, komplexe Anfragen präzise zu bearbeiten, relevante Informationen bereitzustellen und den Kontext vorheriger Interaktionen zu berücksichtigen. Damit kann er nicht nur die bestehenden Herausforderungen in der Nutzung der Wissensdatenbank adressieren, sondern auch einen Mehrwert schaffen, indem er die Interaktion für die Nutzenden intuitiver und effizienter gestaltet.

Trotz dieser Potenziale birgt die Implementierung eines solchen Systems auch Herausforderungen. Insbesondere die technischen Anforderungen, wie der Bedarf an Rechenkapazitäten und die Integration in die bestehende Infrastruktur, wurden als wesentliche Hürden sowohl aus polizeilicher als auch aus wissenschaftlicher Sicht identifiziert. Darüber hinaus zeigt sich, dass die Akzeptanz der Nutzenden ein zentraler Erfolgsfaktor ist. Hier sind gezielte Öffentlichkeitsarbeit, klare Kommunikation der Vorteile und eine nutzerzentrierte Entwicklung entscheidend, um mögliche Widerstände frühzeitig zu überwinden.

Die Wahl der Implementierungsstrategie – sei es die Entwicklung einer individuellen Lösung, der Erwerb einer kommerziellen Lösung oder die Übernahme bestehender Systeme – sollte sich an einer fundierten Wirtschaftlichkeitsuntersuchung orientieren. Eine Übernahme bereits bestehender Lösungen könnte dabei die praktikabelste und wirtschaftlichste Variante darstellen, sofern diese an die spezifischen Anforderungen von PSN angepasst werden können.

Zusammenfassend lässt sich feststellen, dass die Einführung eines KI-Chatbots unter den richtigen Rahmenbedingungen eine signifikante Verbesserung der Wissensmanagementprozesse und der organisatorischen Effizienz bewirken kann. Die Umsetzung erfordert jedoch eine sorgfältige Planung, klare Zieldefinitionen und eine enge Abstimmung zwischen den technischen und organisatorischen Akteuren. Mit einer strategischen Herangehensweise bietet die Integration eines Chatbots die Möglichkeit, die Nutzung des PSN nachhaltig zu optimieren und die Polizei Niedersachsen auf ihrem Weg zur digitalen Transformation weiter voranzubringen.

Literaturverzeichnis

Ali, A. & Amin, M. Z. (2019, November). Conversational AI Chatbot Based on Encoder-Decoder Architectures with Attention Mechanism. Paper präsentiert bei der Pakistan's National AI Conference, Karachi, Pakistan. doi.org/10.13140/RG.2.2.12710.27204

Böhm, S. H., Linnyk, O., Jäger, W., & Teetz, I. (2021). KI im Recruiting: Anwendungsfelder, Entwicklungsstand und Anwendungsbeispiele aus der Praxis. In T. Barton & C. Müller (Hrsg.), Künstliche Intelligenz in der Anwendung: Angewandte Wirtschaftsinformatik (S. 195-218). Springer Vieweg.

Brown, T., Mann, B., & Ryder, N. et al. (2020). Language Models are Few-Shot Learners. *Advances in Neural Information Processing Systems*, 33, 1877-1901.

Cornelius, A. (2019). Künstliche Intelligenz: Entwicklungen, Erfolgsfaktoren und Einsatzmöglichkeiten. Haufe.

Etscheid, J., von Lucke, J., & Stroh, F. (2020). Künstliche Intelligenz in der öffentlichen Verwaltung. Fraunhofer IAO. doi.org/10.24406/publica-fhg-300105.

Gärtner, C. (2020). Smart HRM: Digitale Tools für die Personalarbeit. Wiesbaden: Springer Gabler.

Haristiani, N. (2019). Artificial Intelligence (AI) Chatbots as Language Learning Medium: An Inquiry. *Journal of Physics: Conference Series*, 1387(1), 1-6. doi.org/10.1088/1742-6596/1387/1/012020.

Kohne, A., Kleinmanns, P., Rolf, C., & Beck, M. (2020). Chatbots: Aufbau und Anwendungsmöglichkeiten von autonomen Sprachassistenten. Wiesbaden: Springer Vieweg.

Kreutzer, R. T., & Sirrenberg, M. (2019). Künstliche Intelligenz verstehen: Grundlagen – Use-Cases – unternehmenseigene KI-Journey. Heidelberg: Springer-Verlag.

Lewandowski, T., Heuer, M., Vogel, P., & Böhm, T. (2022). Design Knowledge for the Lifecycle Management of Conversational Agents. *Wirtschaftsinformatik 2022 Proceedings*, 3(1), 1-18. aisel.ais-net.org/wi2022/ai/ai/3.

Mayring, P., & Fenzl, T. (2019). Qualitative Inhaltsanalyse. In N. Baur & J. Blasius (Hrsg.), *Handbuch Methoden der empirischen Sozialforschung* (S. 633-648). Wiesbaden: Springer VS.

Niedersächsisches Ministerium für Inneres und Sport (2021): Erlass MI 21 – 02830/4 „Einführung eines Polizeiinternen Sozialen Netzwerks (PSN) mit dem Namen null1|5 für die Polizei Niedersachsen vom 07.01.2021“.

Offergelt, F., Hofreiter, S., & Steiner, T. (2024). *Wissensmanagement in modernen Organisationen: Impulse aus der Forschung und Erkenntnisse aus der Praxis*. Berlin, Heidelberg: Springer Gabler.

Petry, T., & Jäger, W. (2021). Digital HR – Gesamtkomplex im Überblick. In T. Petry & W. Jäger (Hrsg.), *Digital HR: Smarte und agile Systeme, Prozesse und Strukturen im Personalmanagement* (2. Aufl., S. 27-113). Freiburg: Haufe.

Piecha, A., & Hacker, W. (2021). Informationsflut am Arbeitsplatz – Umgang mit großen Informationsmengen vermittelt durch elektronische Medien. *baua: Bericht kompakt*. Dortmund: Bundesanstalt für Arbeitsschutz und Arbeitsmedizin. baua.de/DE/Angebote/Publicationen/Berichte/F2373 (30.05.2025).

Schmidt, M. (2024). Einsatz von künstlicher Intelligenz für sachbearbeitende Tätigkeiten im öffentlichen Dienst. *Wirtschaftsinformatik & Management*. doi.org/10.1365/s35764-024-00516-3.

Schwarz, M., & Ertel, C. (2023). Planung und Steuerung von Business Ecosystems: Erkenntnisse und Erfahrungen für einen Controlling-Ansatz. *Controlling*, Nr.5/2023, 39-42.

Wagener, A. (2019). *Künstliche Intelligenz im Marketing – ein Crashkurs: Data Driven Marketing, Predictive Analytics, Deep Learning*. Freiburg: Haufe-Lexware.

Wilke, G., & Bendel, O. (2022). KI-gestütztes Recruiting – technische Grundlagen, wirtschaftliche Chancen und Risiken sowie ethische und soziale Herausforderungen. *HMD Praxis der Wirtschaftsinformatik*, 59(2), 647-666.

Wittpahl, V. (2019). *Künstliche Intelligenz: Technologie, Anwendung, Gesellschaft*. Heidelberg: Springer.

Potenzial von Chatbots für das Online-Anzeigeverfahren der Bayerischen Polizei

Volker Hemmert

Die Digitalisierung stellt sowohl Unternehmen als auch öffentliche Institutionen vor die Herausforderung, Prozesse effizienter und benutzerfreundlicher zu gestalten. Während Unternehmen wie die Lufthansa bereits Chatbots nutzen, um Flugumbuchungen vorzunehmen (Lufthansa 2024), bleibt die Polizei oft hinter diesen technologischen Möglichkeiten zurück. Eine Umfrage des Bitkom e. V. kommt zu dem Ergebnis, dass im Jahr 2022 40 % der befragten Unternehmen Chatbots zur Kundenkommunikation im Einsatz haben oder deren Einsatz planen (Bitkom e. V. 2023, S. 6). Im Gegensatz dazu erfolgt die Bearbeitung von Online-Anzeigen bei der Bayerischen Polizei weiterhin formularbasiert. Unvollständige Anzeigen erfordern regelmäßig aufwendige Nachermittlungen (Piazza und Honekamp 2021, S. 79). Diese Diskrepanz verdeutlicht das ungenutzte Potenzial, das Chatbots bei der Polizei für Effizienz und Modernisierung bieten könnten.

Der Einsatz von Chatbots könnte das Online-Anzeigeverfahren der Bayerischen Polizei grundlegend transformieren, die Benutzerfreundlichkeit verbessern, die Anzeigenqualität erhöhen und die Arbeitsbelastung senken. Zugleich könnten Herausforderungen wie Datenschutz, Akzeptanz und technische Komplexität bestehen. Die zentrale Fragestellung lautet daher: Welches Potenzial bietet der Einsatz von Chatbots im Online-Anzeigeverfahren der Bayerischen Polizei?

Das Ziel dieses Beitrags ist es, systematisch Stärken, Schwächen, Chancen und Risiken zu ermitteln. Aus der Gegenüberstellung der gewonnenen Ergebnisse sollen dann das Potenzial analysiert und Handlungsempfehlungen abgeleitet werden. Die Ergebnisse sollen einen Beitrag zur Diskussion leisten, wie die Polizei von modernen Technologien profitieren kann.

Hintergrund

In diesem Abschnitt wird das Online-Anzeigeverfahren der Bayerischen Polizei, gestützt auf Presseberichte und eigene Beobachtungen, dargestellt. Auf Grundlage einer Literaturanalyse wird der Begriff „Chatbot“ erläutert sowie der Forschungsstand anhand des konkreten Einsatzszenarios dargestellt.

Das Online-Anzeigeverfahren der Bayerischen Polizei

Seit dem 23.02.2018 bietet das Bayerische Innenministerium die Möglichkeit, Online-Anzeigen für Kleinkriminalität zu erstatten (Bayerisches Staatsministerium des Innern, für Sport und Integration 2018). Das Verfahren wurde mit fiktiven Daten bis kurz vor der Datenübermittlung an die Polizei getestet. Die dabei gemachten Erfahrungen entsprechen der Berichterstattung der Stiftung Warentest (Stiftung Warentest 2019). Nutzende wählen anhand starrer Eingabefelder das Delikt und den Ort aus, beantworten W-Fragen, beschreiben den Sachverhalt, laden Dateien hoch und geben personenbezogene Daten an. Je nach Delikt variieren die Formulare. Pflichtfelder prüfen lediglich die Eingabe und nicht deren Plausibilität, da auch Platzhalter wie „xyz“ akzeptiert wurden. Dabei steht die Online-Anzeige nur in deutscher Sprache zur Verfügung. Nach der Übermittlung wird die Anzeige durch einen Menschen vorbewertet und an das zuständige Fachkommissariat weitergeleitet. Im Jahr 2019 gingen ca. 1100 Anzeigen pro Monat ein (München TV 2019). Aktuell dürften dies weitaus mehr sein.

Chatbot

Der Begriff Chatbot setzt sich aus den englischen Worten Chat (dt. plaudern) und Bot (dt. Roboter) zusammen (Kohne et al. 2020, S. 1). Ein Chatbot ist somit ein System, das fähig ist, mit einem menschlichen Benutzenden in einen Dialog zu treten (Chat) und gewisse Aufgaben autonom auszuführen (Bot) (Stucki et al. 2019, S. 3). In der Literatur wird zwischen regelbasierten Chatbots, die auf statischen Regeln basieren, und datenbasierten Chatbots unterschieden. Letztere verwenden Künstliche Intelligenz (KI), um nicht vorprogram-

mierte Dialoge zu verarbeiten (IBM 2024). Datenbasierte Chatbots nutzen oft Large Language Models (LLMs) wie der Generative Pretrained Transformer (GPT) ChatGPT (Stöhr et al. 2024, S. 1). Damit dies gelingt, müssen diese die Eingaben des Nutzenden mithilfe von Natural Language Processing (NLP) „verstehen“ (Kusber 2017, S. 233). NLP umfasst die Verarbeitung und Generierung natürlicher Sprache (Kohne et al. 2020, S. 43). Zusätzliche Funktionen wie Übersetzung, Dokumentenanalyse, Bilderkennung und Emotionsanalyse erweitern die Einsatzmöglichkeiten (ebd., S. 52-56, 60).

Chatbots finden vielseitige Anwendungen, von der einfachen Informationsweitergabe durch Informationsbots über die Interaktion im Bürgerservice (Kohne et al. 2020, S. 26-27, 35-36) bis hin zum Abschluss rechtsverbindlicher Geschäfte (Kusber 2017, S. 238). Der Beitrag orientiert sich bei der weiteren Betrachtung am aktuellen Stand der Technik, also datenbasierten Chatbots auf Basis eines LLM (ChatGPT Deutsch 2024).

Chatbots im Online-Anzeigeverfahren

Der aktuelle Forschungsstand zeigt, dass der Einsatz von Chatbots im Online-Anzeigeverfahren bislang nicht untersucht wurde. Großes Potenzial von Chatbots im Allgemeinen ist durch Untersuchungen bereits für die Polizei, Verwaltung und Wirtschaft belegt. Dies soll im Folgenden anhand konkreter Einsatzüberlegungen kurz dargestellt werden. Piazza und Honekamp (2021, S. 66-84) belegen, dass sie durch die Interaktion mit einem Polizeibeschäftigten bei der Erstattung einer Anzeige an einem Bürgerinformationssystem die Anzeigenqualität verbessern und die Bearbeitungszeit verkürzen können. Diese Effekte könnten auch durch einen Chatbot erzielt werden. Der Chatbot könnte von einem einfachen Informationsbot zur Unterstützung bei Fragen bis hin zur vollständigen Annahme von Anzeigen eingesetzt werden. Dabei müsste er Nutzereingaben entgegennehmen, interpretieren und entsprechend reagieren. Obwohl die Forschung bereits das Entgegennehmen und Interpretieren von Nutzereingaben als größte Herausforderung für Chatbots identifiziert hat (Kohne et al. 2020, S. 4; Kusber 2017, S. 233; Stucki et al. 2019, S. 35), lassen aktuelle Forschungsergebnisse und der rasante technische Fortschritt

einen optimistischen Blick zu. Brunnbauer (Brunnbauer 2024, S. 237) zeigt, dass Chatbots relevante Inhalte erkennen, aufbereiten, Kriminalitätsphänomene automatisiert zuordnen (Hamborg et al. 2024, S. 240; Siegel 2024) und bei der Berichtserstellung sowie komplexer Ermittlungsarbeit unterstützen können (Haas 2024, S. 81). Die aktuelle Forschung zeigt auch, dass Aspekte wie Akzeptanz (Haas 2024, S. 80; Makasi et al. 2022, S. 5; van Noordt und Misuraca 2020, S. 14), der richtige Einsatzkontext (Wangler und Botthof 2018, S. 122-123; Makasi et al. 2022, S. 1; Schmidt 2024, S. 1) sowie Transparenz (Preuß 2024, S. 253; Aoki 2021, S. 6; Initiative D21 e. V. und Technische Universität München 2024) und das Recht (Apt und Priesack 2018, S. 233; Madiega 2024, S. 3) eine bedeutende Rolle spielen.

Das Potenzial zum Einsatz von KI und Chatbots in Unternehmen wird in einer aktuellen Umfrage erhoben. Diese führt die Möglichkeiten zur Steigerung der Effizienz, Automatisierung und Mitarbeitermotivation an und adressiert dabei die Herausforderungen Datenschutz, Sicherheit, technische Limitation, fehlende Ressourcen und Kompetenzen (Statista 2024b, S. 7-8).

Methodik

Der Urheber des Begriffs „SWOT“ ist unbekannt. Auch wird die Entwicklung der Methodik unterschiedlichen Personen zugeschrieben (Helms und Nixon 2010, S. 216). Dieser Beitrag verwendet die SWOT-Analyse nach der Beschreibung des Bundesministeriums des Innern und für Heimat (2024) und analysiert hierfür wissenschaftliche Publikationen, Berichte, Studien und Umfragen. Zur Klärung der Forschungsfrage muss das Potenzial von Chatbots im Online-Anzeigeverfahren der Bayerischen Polizei erhoben werden. Das Potenzial ergibt sich aus der Gegenüberstellung der Stärken und Chancen mit den Schwächen und Risiken (Wollny und Paul 2015, S. 191). Daraus folgt das Ziel, die allgemeinen Stärken und Schwächen eines Chatbots zu erheben und die Chancen und Risiken, die sich dadurch auf den Ablaufprozess der Online-Anzeige ergeben, zu identifizieren. Zudem sollen Handlungsempfehlungen abgeleitet werden.

Die SWOT-Analyse ermöglicht eine Erfassung der aktuellen Unternehmenssituation durch die Gegenüberstellung interner Faktoren – Stärken und Schwächen – und externer Faktoren – Chancen und Risiken (Wollny und Paul 2015, S. 198). Somit ist die Methode in der Lage, das Potenzial zu erheben. Im behördlichen Kontext hilft die SWOT-Analyse, die Situation einer Organisation zu erfassen und als Grundlage für die Strategieentwicklung zu nutzen. Sie unterstützt bei der Ableitung von Zielen und Handlungsempfehlungen zur Erreichung eines Soll-Zustands und findet Anwendung in der Produkt- und Prozessentwicklung, Evaluation und bei der Lösung spezifischer Fragestellungen (Bundesministerium des Innern und für Heimat 2024). Die Methode kann somit Veränderungen im Ablaufprozess der Online-Anzeige analysieren und Handlungsempfehlungen ableiten.

Erkenntnisse zu dem Einsatz von Chatbots im Online-Anzeigeverfahren fehlen, jedoch ist die SWOT-Analyse geeignet, neue und komplexe Sachverhalte zu bewerten (Wollny und Paul 2015, S. 211). Die Methode fundiert auf subjektiven Einschätzungen, die willkürlich oder unvollständig ausfallen können (ebd., S. 190). Dieser Schwäche wird begegnet, indem festgelegt wird, dass die Methode dann erfolgreich angewandt wurde, wenn alle im Abschnitt „Chatbots im Online-Anzeigeverfahren“ genannten Aspekte berücksichtigt werden. Da die SWOT-Analyse eine ganzheitliche Betrachtung des neuen Sachverhalts durch die Untersuchung von internen und externen Faktoren zulässt, ist diese im Vergleich zu anderen Methoden die am besten geeignete Methode, um die Forschungsfrage zu beantworten.

Ergebnisse

Die Stärken, Schwächen, Chancen und Risiken werden in diesem Abschnitt erhoben. Im Abschnitt „Diskussion“ werden diese zusammengeführt und diskutiert.

Stärken

Chatbots bieten eine 24/7-Verfügbarkeit und schnelle Reaktionszeiten, sodass Nutzende jederzeit darauf zugreifen können (Kusber 2017, S. 242) und eine Antwort auf ihre Anfragen erhalten (Calvaresi et al. 2023, S. 2). Die Eingaben können schriftlich, in natürlicher Sprache (Nirala et al. 2021, S. 24) und in allen vom Chatbot unterstützten Sprachen erfolgen (Kusber 2017, S. 233). Chatbots kommunizieren über Schnittstellen mit den Nutzenden und lassen sich flexibel in Messaging-Plattformen integrieren (ebd., S. 232). Sie können aus den Eingaben relevante Inhalte erkennen und aufbereiten (Brunnbauer 2024, S. 237). Chatbots speichern vergangene Interaktionen, reagieren bei erneutem Kontakt personalisiert und senken durch ihre Personifizierung die Hemmschwelle zur Kontaktaufnahme (Kohne et al. 2020, S. 3). Den größten Nutzen bieten Chatbots bei wiederkehrenden Aufgaben (Kusber 2017, S. 232). Sie übernehmen Routineaufgaben, unterstützen Mitarbeitende bei komplexeren Anfragen und ermöglichen damit besseren Service bei geringeren Kosten. Selbst bei hoher Auslastung werden Chatbots weder müde noch gereizt (Kohne et al. 2020, S. 4). Zudem dokumentieren Chatbots Anfragen einheitlich, was dazu beiträgt, wiederkehrende Probleme schneller zu identifizieren und den Wissenstransfer durch gute Lösungsbeschreibungen zu sichern (ebd., S. 25).

Schwächen

Die Implementierung und das Training eines Chatbots erfordern einen erheblichen Zeit- und Fachaufwand (Nirala et al. 2021, S. 3). Neben dem Training mit Fragen und Antworten erfordert ihre Qualitätssicherung eine kontinuierliche Überwachung und Anpassung, da unbeaufsichtigtes KI-Lernen zu ungewollten Veränderungen führen kann (Kohne et al. 2020, S. 4-5, 135-136). Es müssen sowohl die Infrastrukturen für den Einsatz von Chatbots geschaffen werden (Wangler und Botthof 2018, S. 122) als auch die Kompetenzen der Mitarbeitenden (Stucki et al. 2019, S. 36). Bei komplexen Fragen sind sie oft nicht in der Lage, präzise Antworten zu geben (Kohne et al. 2020, S. 4). Chatbots haben Schwierigkeiten, Emotionen, Ironie (Kohne et al. 2020, S. 4) oder Intentionen (Kusber 2017, S. 233) zu

erfassen, was ihre Fähigkeit zur Imitation menschlicher Gesprächspartner einschränkt (Stucki et al. 2019, S. 35). Diese Limitationen werden durch überhöhte Nutzererwartungen weiter verstärkt (Kohne et al. 2020, S. 136). Chatbots erheben im Rahmen der Interaktion personenbezogene und vertrauliche Daten (Sağlam und Nurse 2020, S. 2), daher ist die Datenschutz-Grundverordnung (DSGVO) einschlägig (Apt und Priesack 2018, S. 233). Die DSGVO fordert die Einhaltung strikter Regeln für die Verarbeitung und Speicherung personenbezogener Daten sowie Informationspflichten gegenüber den Nutzenden (Kohne et al. 2020, S. 124-126). Ferner sind die Vorgaben des Artificial Intelligence Act zu beachten (Madiaga 2024, S. 3). Die Verarbeitung sensibler Daten durch Maschinen verursacht in westlichen Ländern ethische Bedenken, Akzeptanzprobleme und Ängste vor der Technologie und den Unternehmen (Kohne et al. 2020, S. 133, 136-137).

Chancen

Piazza und Honekamp (2021) zeigen, dass Interaktionen mit Polizeibeschäftigten während der Online-Anzeigenerstellung die Qualität dieser Anzeigen verbessern können (ebd., S. 77-81). Zusätzliche Hinweise oder Erläuterungen zum Verfahren und zu präventiven Maßnahmen steigern die Servicequalität (ebd., S. 67-74). Auch die Bearbeitungszeit wird dadurch verkürzt (ebd., S. 84). Ähnliche Effekte könnten mit Chatbots erreicht werden, da sie gezielt fehlende Angaben identifizieren und beim Anzeigenerstattenden einholen. Aufwendige Nachermittlungen würden entfallen.

Die Überlastung in Sicherheitsbehörden nimmt zu (Bernnat und Mette 2024, S. 2). Länder wie Dänemark und Estland zeigen, dass durch Digitalisierungsstrategien Effizienz- und Entlastungspotenziale genutzt werden können (Wangler und Botthof 2018, S. 122-123). Viele Routineaufgaben, die durch Digitalisierung und Automatisierung effizienter gestaltet werden könnten, binden Ressourcen (ebd.) und beeinträchtigen die Effizienz der Servicebereitstellung (Makasi et al. 2022, S. 1). Im öffentlichen Dienst entfallen etwa 25 % der Sachbearbeitungsarbeiten auf Routinetätigkeiten, die aufgrund geringer kognitiver und Interaktionsanforderungen durch KI und Automatisierung übernommen werden können, z. B. das formular-

basierte Erfassen von Anzeigen. In komplexeren Fällen kann KI als unterstützende Technologie eingesetzt werden. Der Mensch bleibt in der Verantwortung (sog. Human-in-the-Loop) (Schmidt 2024, S. 1), z. B. bei der Berichtserstellung (Haas 2024, S. 81). Dadurch werden Ressourcen für andere Aufgaben und Bereiche frei (Chen et al. 2021, S. 1), was die Zufriedenheit der Mitarbeitenden fördert (Kohne et al. 2020, S. 26). Bereits einfache Informationsbots können die Anzahl der Anfragen reduzieren, während komplexere Chatbots Servicefälle bearbeiten, die Servicequalität steigern und den Arbeitsaufwand minimieren (ebd., S. 38). Vassilakopoulou et al. (2023, S. 6) zeigen am Beispiel des Chatbots der norwegischen Arbeits- und Wohlfahrtsbehörde, dass 2021 nur eine von fünf Anfragen an einen Servicemitarbeitenden weitergeleitet wurde, während der Chatbot den Rest bearbeitete. Ähnliche Ergebnisse liefert ein Projekt des LKA NRW zur automatisierten Zuordnung von Kriminalitätsphänomenen (Hamborg et al. 2024, S. 245).

Der Einsatz von Chatbots treibt den Digitalisierungsprozess voran (Wangler und Botthof 2018, S. 122-123). Laut einer repräsentativen Bitkom-Studie zur digitalen Verwaltung (2024, S. 7) wünschen sich 61 % der Befragten Kunden mehr Chatbots in der Verwaltung. Chatbots benötigen zum Training eine umfangreiche Datengrundlage. Vorhandene Daten müssen von hoher Qualität sein, kategorisiert und aufbereitet werden (Maragno et al. 2023, S. 16). Dies kann entweder von spezialisierten Teams oder durch die Mitarbeit aller Angestellten erfolgen (ebd., S. 24). Dadurch entsteht eine umfassende, strukturierte Wissensdatenbank (Kohne et al. 2020, S. 2, 57, 104), die durch die standardisierte Dokumentation von Anfragen und Lösungen kontinuierlich wächst und als Quelle für den Wissenstransfer innerhalb der Organisation genutzt werden kann (Maragno et al. 2023, S. 20). Die Dokumentation von Wissen und Prozessen in der öffentlichen Verwaltung hilft, ineffiziente Abläufe zu erkennen und zu optimieren. Dies spart Arbeitszeit, ermöglicht Stellenzusammenlegungen und wirkt dem Fachkräftemangel entgegen (Schmidt 2024, S. 8).

Der effektive Einsatz von Chatbots erhöht die Akzeptanz digitaler Kommunikationskanäle und hebt das Kundenerlebnis auf ein neues Niveau (Kohne et al. 2020, S. 29). Unternehmen wirken durch den

Einsatz von Chatbots moderner und bürgernäher, was sich positiv auf die Kundenzufriedenheit auswirkt (ebd., S. 24-25). Fortschritte im NLP lassen Chatbots immer menschähnlicher agieren (Stucki et al. 2019, S. 3). Durch die Personifizierung des Chatbots, z. B. durch einen Avatar, senken Unternehmen ebenfalls die Kommunikationsschwelle für den Nutzenden (Kohne et al. 2020, S. 3). Chatbots können relevante Informationen aus Dokumenten herausfiltern (Brunnbauer 2024, S. 237). So könnten dem Chatbot betrügerische Mails übergeben werden, welcher die relevanten Informationen extrahiert. Im Kontext der örtlichen Flexibilität und der Vermeidung von Wartezeiten gaben in der repräsentativen Bitkom-Studie zur digitalen Verwaltung (2024, S. 7) 41 % der Befragten an, lieber mit einem Chatbot als mit einem Menschen zu kommunizieren.

Die Studie „SKiD – Sicherheit und Kriminalität in Deutschland“ (Birkel et al. 2022, S. 90–92) zeigt, dass viele Personen aufgrund des hohen Aufwands von einer Anzeigenerstattung absehen. Da Chatbots ohne zeitliche und örtliche Einschränkungen (Nirala et al. 2021, S. 24) sowie plattform-übergreifend betrieben werden können (Kusber 2017, S. 232), könnte dies zu einer Erhöhung der Mitteilungen an die Polizei führen. Dies würde in der Folge zu einem besseren Bild der Kriminalitätslage in Deutschland führen (Birkel et al. 2022, S. 1). Viele gleichartige Anfragen zu einem bestimmten Thema weisen auf eine Störung hin (Kohne et al. 2020, S. 25), was die Polizei in die Lage versetzen könnte, neue Phänomene schneller zu erkennen und darauf zu reagieren. Zudem könnte die Schutzpolizei entlastet werden, da diese weniger Anzeigen aufnehmen müsste (Piazza und Honekamp 2021, S. 79).

Bannister und Connolly (2011, S. 144-145) zeigen, dass Transparenz und verbesserte Dienstleistungen das Vertrauen in die Regierung stärken können. Chen et al. (2021) folgern, dass Chatbots in der Verwaltung durch barrierefreie, transparente und effiziente Dienstleistungen und durch die Reduzierung menschlicher Fehler sowie durch zeitnahe und personalisierte Informationen die Bedürfnisse der Bürgerinnen und Bürger gezielter erfüllen, sie stärker einbinden und somit das Vertrauen weiter stärken können (ebd., S. 2). Können alle

Verzerrungen (Bias), wie Vorurteile aufgrund schlechter Trainingsdaten, im KI-Training behoben werden, kann ein Chatbot nach dem Diskriminierungsverbot agieren (Schmidt 2024, S. 8).

Risiken

Es besteht Skepsis gegenüber Automatisierungen ohne menschliche Beteiligung. (Aoki 2021, S. 6). Die Bitkom-Umfrage zur digitalen Verwaltung (2024, S. 6) zeigt, dass viele Befragte bei der Anzeigenerstattung den persönlichen Kontakt bevorzugen. Der eGovernment Monitor (Initiative D21 e. V. und Technische Universität München 2024, S. 45) hebt als Hauptbedenken der Bürgerinnen und Bürger beim Einsatz von KI in der Verwaltung fehlende Verantwortlichkeit, mögliche Fehler, Datenschutzsorgen, den Verlust menschlicher Ansprechpartner und schwer nachvollziehbare Entscheidungen hervor. Verzerrungen (Bias) können zu diesem Blackbox-Effekt hinzukommen, wenn die Trainingsdatensätze die Realität nicht repräsentieren oder systematische Fehler enthalten (Preuß 2024, S. 254). Diese Bedenken können in tatsächliche Ängste vor Überwachung und exzessivem Datensammeln münden (Kohne et al. 2020, S. 137).

Sowohl Polizeiangestellte, aus Angst vor Arbeitsplatzverlust (van Noordt und Misuraca 2020, S. 14) und Mehraufwand (PwC Strategy& 2024, S. 9), als auch Bürgerinnen und Bürger könnten dem Einsatz von Chatbots kritisch gegenüberstehen, was die Akzeptanz und Nutzung des Systems behindern könnte. Nach Makasi et al. (2022, S. 5) sind für interaktive Serviceleistungen, wie die Aufnahme und Bewertung von Lebenssachverhalten im Rahmen der Anzeigenerstattung, komplexe Chatbots erforderlich. Diese erfordern anfangs einen hohen Kostenaufwand für das Training und im Betrieb weiterhin für die Überwachung und Anpassung (Kohne et al. 2020, S. 5, 113-114). Einfache und kostengünstige Chatbots sind nicht in der Lage, komplexe Sachverhalte zu bewerten (Makasi et al. 2022, S. 4). Die mangelhafte Qualität der Interaktion mit solchen Chatbots führt zu einer fehlenden Akzeptanz der Nutzenden und einem Rückgriff auf traditionelle Kommunikationskanäle, was Androutsopoulou et al. (2019, S. 8) als das E-Government-Paradoxon bezeichnet. Ohne Nutzerakzeptanz steigen die Supportkosten, wodurch der Mehrwert

des Chatbots verloren geht (Kohne et al. 2020, S. 113). Nach Statista (2024a, S. 8) sieht knapp die Hälfte aller Unternehmen die größte Herausforderung für den Einsatz von Chatbots in der mangelhaften Qualität der Chatbot-Antworten.

Individuelle Chatbot-Lösungen benötigen umfassendes Fachwissen. Die Qualität des Chatbots wird durch die Komplexität des integrierten Fachwissens bestimmt, was sich wiederum im erforderlichen Aufwand (Kosten und Zeit) für die Implementierung widerspiegelt (Kohne et al. 2020, S. 113-114). Ressourcenmangel kann die Chatbot-Qualität beeinträchtigen, während Standardlösungen Abhängigkeiten von externen Dienstleistern schaffen (ebd., S. 14). Dem Dienstleister fehlt dabei das oft als Verschlussache eingestufte Fachwissen, weshalb aufwendige Sicherheitsmaßnahmen zum Schutz der sensiblen Daten erforderlich sind (Haas 2024, S. 85).

Trotz des Hinweises „Keine Notrufannahme! Im Notfall rufen Sie die 110 an!“ (Bayerisches Staatsministerium für Digitales 2024), der dem Online-Anzeigeportal vorgeschaltet ist, könnten Nutzende Fälle mit akutem Handlungsbedarf an den Chatbot übermitteln. Ferner kann ein Chatbot anfällig für Spam oder missbräuchliche Anfragen sein (Kohne et al. 2020, S. 4). Gleichzeitig könnte er dabei Social Intents, also den Wunsch nach menschlicher Kommunikation, übersehen (Stucki et al. 2019, S. 27), was die Effektivität und Glaubwürdigkeit beeinträchtigen könnten. Die zunehmende Zahl an Anzeigen könnte die Kriminalpolizei zusätzlich belasten (Piazza und Honekamp 2021, S. 79).

Chatbots treffen rein datenbasierte Entscheidungen, was in kritischen Situationen problematisch sein kann, da Emotionen und moralische Werte nicht berücksichtigt werden. Dies erfordert klare gesetzliche Regelungen zur Haftung und Abgrenzung von Zuständigkeiten (Kohne et al. 2020, S. 148-149). Der Einsatz von Chatbots im öffentlichen Sektor birgt die Gefahr, die Kontrolle über vertrauliche Daten zu verlieren (Boston Consulting Group 2021, S. 10). Informationspflichten und Einwilligungen bergen datenschutzrechtliche Risiken, insbesondere durch die Speicherung personenbezogener Daten außerhalb der eigenen Organisation (Stucki et al. 2019, S. 21).

Unklare Regelungen in Auftragsvertragsverträgen und unzureichende technische und organisatorische Maßnahmen können die Datensicherheit gefährden und rechtliche Konsequenzen nach sich ziehen. Die DSGVO enthält strikte Vorschriften zur Verarbeitung und Speicherung personenbezogener Daten sowie Informationspflichten gegenüber dem Nutzenden (Kohne et al. 2020, S. 124-128).

Diskussion

Für die Diskussion wurden die Ergebnisse der SWOT-Analyse thematisch geclustert und in der Abbildung 1 visualisiert.

Stärken	Schwächen
<ul style="list-style-type: none"> Verfügbarkeit und Zugänglichkeit Effizienz und Produktivität Sprachliche und kommunikative Vielseitigkeit Nutzerorientierung Wissensmanagement 	<ul style="list-style-type: none"> Technischer und organisatorischer Aufwand Recht und Datensicherheit Akzeptanzprobleme Limitierungen der KI-Funktionalität
Chancen	Risiken
<ul style="list-style-type: none"> Effizienzsteigerung und Ressourcenoptimierung Verbesserung der Servicequalität Wissensmanagement und Datenqualität Prozessoptimierung Technologische und gesellschaftliche Integration Mitarbeiterorientierung und Arbeitszufriedenheit 	<ul style="list-style-type: none"> Datenschutz und Datensicherheit Soziale und psychologische Auswirkungen Technologische Limitierungen Organisatorische und wirtschaftliche Herausforderungen Rechtliche Unsicherheiten und Verantwortung Vertrauensverlust und gesellschaftliche Skepsis

Abbildung 1: Geclusterte Ergebnisse der SWOT-Analyse

Die SWOT-Analyse liefert eine umfassende Betrachtung der Aspekte des Kapitels „Chatbots im Online-Anzeigeverfahren“. Durch die Integration aktueller Literatur, Studien und Umfragen ergibt sich eine ausgewogene Bewertung von Stärken und Chancen im Verhältnis zu Schwächen und Risiken. Die Ergebnisse verbinden technische, wirtschaftliche, rechtliche und gesellschaftliche Perspektiven und heben sowohl Chancen als auch Risiken klar hervor. Sie bieten eine strukturierte Entscheidungsgrundlage, die besonders für die Polizei von Bedeutung ist. Allerdings basiert die Analyse überwiegend auf

Sekundärliteratur und berücksichtigt praktische Erfahrungen sowie die Nutzerperspektive nur begrenzt, was die Realitätsnähe der Bewertung einschränkt. Ergänzende praxisorientierte Daten wären erforderlich, um die Analyse weiter zu fundieren.

Die Analyse der Stärken und Chancen zeigt, dass Chatbots die Effizienz und Qualität in Prozessen und Dienstleistungen positiv beeinflussen. Durch die Automatisierung werden Arbeitsprozesse optimiert und die Servicequalität sowie die Zufriedenheit von Nutzenden und Mitarbeitenden gesteigert. Die Arbeitsbelastung könnte, insbesondere bei der Schutzpolizei, sinken. Auch könnte der Einsatz von Chatbots eine strukturierte Wissensverwaltung mit sich bringen, wodurch Transparenz und eine effiziente Nutzung von Informationen gewährleistet werden. Eine geringere Zugangsschwelle fördert die Barrierefreiheit und könnte zur Zunahme der Anzeigen und einem besseren Bild der Kriminalitätsslage beitragen.

Trotz dieser Möglichkeiten ergeben sich Schwächen und Risiken, die technologische und organisatorische Grenzen aufzeigen. Technologische Limitierungen, wie fehlerhafte Antworten oder schwer nachvollziehbare Entscheidungen, sowie hohe Implementierungskosten und der Bedarf an Fachwissen erschweren die effiziente Nutzung und Integration der Technologie in bestehende Strukturen. Zudem stellen der Umgang mit sensiblen Daten, rechtliche Unsicherheiten und fehlende Akzeptanz – insbesondere der Wunsch, Anzeigen persönlich zu erstatten – Herausforderungen dar, die das Vertrauen in die Technologie und deren Implementierung beeinträchtigen können. Die Arbeitsbelastung bei der Kriminalpolizei könnte steigen.

Werden Stärken und Chancen den Schwächen und Risiken gegenübergestellt, wird deutlich, dass komplexe Chatbots grundsätzlich in der Lage sind, das Online-Anzeigeverfahren zu unterstützen. Jedoch wird auch deutlich, dass ein falscher Umgang mit den Herausforderungen das Potenzial für die Integration von Chatbots in das Online-Anzeigeverfahren gefährdet. Voraussetzung für die Entfaltung des Potenzials ist eine strategische Implementierung, welche die identifizierten Herausforderungen adressiert. Um Effekte wie dem eGovernment-Paradoxon zu begegnen, müssen die technischen

Möglichkeiten des Chatbots mit den Anforderungen an das Online-Anzeigeverfahren abgeglichen werden. Eine zentrale Bereitstellung und Überwachung des Chatbots sowie eine dezentral angereicherte Wissensdatenbank würden dabei die meisten Synergien erzielen. Die Zunahme der Online-Anzeigen könnten zu einer höheren Arbeitsbelastung führen. Gleichzeitig wird erwartet, dass die Qualität der Anzeigen steigt und aufwendige Nachermittlungen entfallen, wodurch der Arbeitsaufwand sinken dürfte (Piazza und Honekamp 2021, S. 84-85). Wird den Herausforderungen durch adäquate Maßnahmen begegnet, besteht großes Potenzial von Chatbots für das Online-Anzeigeverfahren der Bayerischen Polizei. Das identifizierte Potenzial deckt sich mit der oben beschriebenen aktuellen Studie von Statista zum Einsatz von KI und Chatbots in Unternehmen.

Der in der Forschung beschriebene Wunsch nach mehr Chatbots in der Verwaltung sowie der Priorisierung eines Chatbots vor der menschlichen Kommunikation im Kundenservice kann mit den vorliegenden Ergebnissen nicht eindeutig nachgewiesen werden. So wird in der Bitkom-Studie zur digitalen Verwaltung explizit der persönliche Kontakt bei der Erstattung von Anzeigen gefordert. Zieht man weitere Umfragen aus der freien Wirtschaft zur Kundenkommunikation hinzu, identifizieren diese ebenfalls eine hohe Zufriedenheit der Kunden bei dem Einsatz von Chatbots (Capgemini 2023, S. 13). Die Bitkom-Studie zur digitalen Verwaltung führte keine qualitativen Erhebungen durch. Es bleibt daher offen, ob die Ursache an einer fehlenden Technikakzeptanz oder an anderen Merkmalen festzumachen ist.

Schlussfolgerungen

Die SWOT-Analyse zeigt, dass die Integration von Chatbots im Online-Anzeigeverfahren der Bayerischen Polizei bei richtiger Umsetzung ein Potenzial zur Steigerung der Effizienz und Servicequalität bietet sowie zur Entlastung der Mitarbeitenden beiträgt. Begleitend werden die Digitalisierung vorangetrieben, Prozesse optimiert, Ressourcen besser genutzt und eine Wissensdatenbank geschaffen. Die

Umsetzung erfordert jedoch Maßnahmen gegen Herausforderungen wie hohe Implementierungskosten, Datenschutzrisiken sowie interne und externe Akzeptanzprobleme.

Das Potenzial von Chatbots sollte für das Online-Anzeigeverfahren der Bayerischen Polizei eingesetzt werden. Maßnahmen, die den Datenschutz und das Akzeptanzmanagement adressieren, sollten vor der Implementierung zentral umgesetzt werden. Von hier aus sollte auch ein regelmäßiger Abgleich mit den fortschreitenden technischen Möglichkeiten erfolgen. Um Akzeptanzproblemen vorzubeugen, kann der Chatbot schrittweise integriert werden. Beginnend als Informationsbot zur Unterstützung bei Fragen, bis hin zur vollständigen Entgegennahme der Anzeige. Da der Informationsbot zunächst nur unterstützt, bleibt die Kontrolle beim Anzeigenerstatenden. Da die Voraussetzungen für die Integration der Verfahren ähnlich sind, können bereits in diesem Stadium wertvolle Lerneffekte erzielt werden.

Führungskräfte könnten dezentral geeignete Vorgänge mit ihren Mitarbeitenden identifizieren und zum Aufbau einer Wissensdatenbank beitragen. Bevor die identifizierten Akzeptanzprobleme bei der Nutzung von Chatbots genauer analysiert werden, sollte die generelle Akzeptanz von Online-Anzeigen erforscht werden. Weiterer Forschungsbedarf ergibt sich ferner zu den betriebswirtschaftlichen Aspekten, insbesondere einer Kosten-Leistungs-Rechnung, welche aufgrund der Komplexität nicht im Rahmen des Beitrags untersucht werden konnte.

Literaturverzeichnis

Androutsopoulou, Aggeliki; Karacapilidis, Nikos; Loukis, Euripidis; Charalabidis, Yannis (2019): Transforming the communication between citizens and government through AI-guided chatbots. *Government Information Quarterly* 36 (2), S. 358-367. DOI: 10.1016/j.giq.2018.10.001.

Aoki, Naomi (2021): The importance of the assurance that „humans are still in the decision loop“ for public trust in artificial intelligence: Evidence from an online experiment. *Computers in Human Behavior* 114, S. 106572. DOI: 10.1016/j.chb.2020.106572.

Apt, Wenke; Priesack, Kai (2018): KI und Arbeit – Chance und Risiko zugleich. In: Volker Wittpahl (Hg.): *Künstliche Intelligenz. Technologien | Anwendung | Gesellschaft*. 2019. Berlin, Heidelberg: Springer, S. 221-238.

Bannister, Frank; Connolly, Regina (2011): Trust and transformational government: A proposed framework for research. *Government Information Quarterly* 28 (2), S. 137-147. DOI: 10.1016/j.giq.2010.06.010.

Bayerisches Staatsministerium des Innern, für Sport und Integration (2018): Herrmann startet ‚Anzeigenerstattung online‘. Hg. v. Bayerisches Staatsministerium des Innern, für Sport und Integration. [stmi.bayern.de/med/pressemitteilungen/pressearchiv/2018/52b/index.php](https://www.stmi.bayern.de/med/pressemitteilungen/pressearchiv/2018/52b/index.php), zuletzt geprüft am 02.12.2024.

Bayerisches Staatsministerium für Digitales (Hg.) (2024): Anzeigenerstattung bei der Bayerischen Polizei online – BayernPortal. [bayernportal.de/dokumente/onlineverfahren/305652977295](https://www.bayernportal.de/dokumente/onlineverfahren/305652977295), zuletzt geprüft am 10.12.2024.

Bernnat, Rainer; Mette, Philipp (2024): Arbeitsbelastung in deutschen Sicherheitsbehörden. Hg. v. PwC Strategy&. [strategyand.pwc.com/de/de/industrie-teams/oeffentlicher-sektor/arbeitsbe](https://www.strategyand.pwc.com/de/de/industrie-teams/oeffentlicher-sektor/arbeitsbe)

lastung-in-deutschen-sicherheitsbehoerden/strategyand-arbeitsbelastung-in-deutschen-sicherheitsbehoerden.pdf, zuletzt geprüft am 02.12.2024.

Birkel, Christoph; Church, Daniel; Erdmann, Anke; Hager, Alisa; Leitgöb-Guzy, Nathalie (2022): Sicherheit und Kriminalität in Deutschland – SKiD 2020. Bundesweite Kernbefunde des Viktimisierungssurvey des Bundeskriminalamts und der Polizeien der Länder (V1.4). Hg. v. Bundeskriminalamt Wiesbaden. bka.de/SharedDocs/Downloads/DE/Publikationen/Publikationsreihen/Forschungsergebnisse/SKiD2020_Ergebnisse_V1.4.html, zuletzt geprüft am 02.12.2024.

Bitkom e. V. (Hg.) (2023): Kundenkommunikation der Zukunft: Vom Status quo zur Vision. Unter Mitarbeit von Christian Gericke, Khaled Daftari, Klaus Ganter, Marc Drögsler, Matthias Fertig, Melanie Ringhut et al. bitkom.org/sites/main/files/2023-01/230124Kundenkommunikation-derZukunft.pdf, zuletzt geprüft am 02.12.2024.

Bitkom e. V. (2024): Digitalisierung von Verwaltung und öffentlicher Hand. Hg. v. Bitkom e. V. bitkom.org/sites/main/files/2023-11/Bitkom-Praesentation-Digitalisierung-von-Verwaltung-und-oeffentlicher-Hand-2023.pdf, zuletzt geprüft am 02.12.2024.

Boston Consulting Group (2021): Konzept für die Entwicklung und den Einsatz von Chatbots in Rechtsantragstellen erstellt im Auftrag des Bundesministeriums der Justiz und für Verbraucherschutz. Hg. v. Bundesministerium der Justiz und für Verbraucherschutz. bmj.de/SharedDocs/Downloads/DE/Fachpublikationen/Chatbot_Rechtsantragstelle_Abschlussbericht.pdf?__blob=publicationFile&v=5, zuletzt geprüft am 02.12.2024.

Brunnbauer, Matthias (2024): Potentiale und Gefahren von Large Language Models aus polizeilicher Sicht. In: Wilfried Honekamp und Dirk Labudde (Hg.): Polizei-Informatik 2024. Remscheid: Rediroma-Verlag, S. 234-239.

Bundesministerium des Innern und für Heimat (2024): SWOT-Analyse. orghandbuch.de/Webs/OHB/DE/Organisationshandbuch-NEU/4_MethodenUndTechniken/Methoden_A_bis_Z/SWOT_Analyse/swot_analyse_node.html, am 08.02.2024, zuletzt geprüft am 07.11.2024.

Calvaresi, Davide; Eggenschwiler, Stefan; Mualla, Yazan; Schumacher, Michael; Calbimonte, Jean-Paul (2023): Exploring agent-based chatbots: a systematic literature review. *Journal of Ambient Intelligence and Humanized Computing* 14 (8), S. 11207-11226. DOI: 10.1007/s12652-023-04626-5.

Capgemini (2023): Why Consumers love Generative AI. prod.ucwe.capgemini.com/wp-content/uploads/2023/06/GENERATIVE-AI_Final_WEB_060723.pdf, zuletzt geprüft am 16.12.2024.

ChatGPT Deutsch (2024): ChatGPT Deutsch. chatopenai.de, zuletzt geprüft am 18.12.2024.

Chen, Tao; Guo, Wenshan; Gao, Xian; Liang, Zhehao (2021): AI-based self-service technology in public service delivery: User experience and influencing factors. *Government Information Quarterly* 38 (4), S. 101520. DOI: 10.1016/j.giq.2020.101520.

Haas, Steve (2024): Von der Theorie zur Praxis: Generative KI in der modernen Polizeiarbeit. In: Wilfried Honekamp und Dirk Labudde (Hg.): Polizei-Informatik 2024. Remscheid: Rediroma-Verlag, S. 80-86.

Hamborg, Felix; Hall, Florian; Kahr, Robert (2024): Auswertung von Kriminalitätsereignissen mithilfe von KI. In: Wilfried Honekamp und Dirk Labudde (Hg.): Polizei-Informatik 2024. Remscheid: Rediroma-Verlag, S. 240-246.

Helms, Marilyn M.; Nixon, Judy (2010): Exploring SWOT analysis – where are we now? *Journal of Strategy and Management* 3 (3), S. 215-251. DOI: 10.1108/17554251011064837.

IBM (2024): Was ist ein Chatbot? Generative KI-gestützte Chatbots. IBM. [ibm.com/de-de/topics/chatbots](https://www.ibm.com/de-de/topics/chatbots), zuletzt geprüft am 02.12.2024.

Initiative D21 e. V.; Technische Universität München (2024): eGovernment MONITOR 2024. Nutzung und Akzeptanz digitaler Verwaltungsleistungen aus Sicht der Bürger*innen. Die deutschen Bundesländer, Deutschland, Österreich und die Schweiz im Vergleich. Hg. v. Initiative D21 e. V. und Technische Universität München. initiatives21.de/uploads/03_Studien-Publikationen/eGovernment-MONITOR/2024/egovernment_monitor_24.pdf, zuletzt geprüft am 02.12.2024.

Kohne, Andreas; Kleinmanns, Philipp; Rolf, Christian; Beck, Moritz (2020): Chatbots. Aufbau und Anwendungsmöglichkeiten von autonomen Sprachassistenten. Wiesbaden: Springer Vieweg.

Kusber, Robert (2017): Chatbots – Conversational UX Platforms. In: Remigiusz Smolinski (Hg.): Innovationen und Innovationsmanagement in der Finanzbranche: Springer Fachmedien Wiesbaden, S. 231-244.

Lufthansa (2024): Lufthansa Chat Assistant. Hg. v. Lufthansa. [lufthansa.com/digitalassistant/support/webchat.html](https://www.lufthansa.com/digitalassistant/support/webchat.html), zuletzt geprüft am 16.12.2024.

Madiega, Tambiama (2024): Artificial intelligence act. Hg. v. Europäisches Parlament. [europarl.europa.eu/RegData/etudes/BRIE/2021/698792/EPRS_BRI\(2021\)698792_EN.pdf](https://europarl.europa.eu/RegData/etudes/BRIE/2021/698792/EPRS_BRI(2021)698792_EN.pdf), zuletzt geprüft am 02.12.2024.

Makasi, Tendai; Nili, Alireza; Desouza, Kevin C.; Tate, Mary (2022): A Typology of Chatbots in Public Service Delivery. *IEEE Software* 39 (3), S. 58-66. DOI: 10.1109/MS.2021.3073674.

Maragno, Giulia; Tangi, Luca; Gastaldi, Luca; Benedetti, Michele (2023): AI as an organizational agent to nurture: effectively introducing chatbots in public entities. *Public Management Review* 25 (11), S. 2135-2165. DOI: 10.1080/14719037.2022.2063935.

München TV (2019): Rund 12.000 Online-Anzeigen in Bayern. München Live TV Fernsehen GmbH & Co. KG, 06.03.2019. [muenchen.tv/rund-12-000-online-anzeigen-in-bayern-306073/](https://www.muenchen.tv/rund-12-000-online-anzeigen-in-bayern-306073/), zuletzt geprüft am 17.12.2024.

Nirala, Krishna Kumar; Singh, Nikhil Kumar; Purani, Vinay Shivshanker (2021): A survey on providing customer and public administration based services using AI: chatbot. *Multimedia tools and applications* 81 (16), S. 22215-22246. DOI: 10.1007/s11042-021-11458-y.

Piazza, Martin; Honekamp, Wilfried (2021): Anzeigenunterstützung mithilfe eines Bürgerinformationssystems an der Polizeidienststelle. In: Wilfried Honekamp, Roman Povalej, Heiko Rittelmeier, Silvio Berner, Johannes Fähndrich und Dirk Labudde (Hg.): *Polizei-Informatik 2021*. Remscheid: Rediroma-Verlag, S. 65-86.

Preuß, Tamina (2024): Chancen und Risiken KI-basierter Wahrheitsfindung im Strafverfahren. In: Wilfried Honekamp und Dirk Labudde (Hg.): *Polizei-Informatik 2024*. Remscheid: Rediroma-Verlag, S. 247-258.

PwC Strategy& (Germany) GmbH (2024): Arbeitsbelastung in deutschen Sicherheitsbehörden. Hg. v. PwC Strategy& (Germany) GmbH. strategyand.pwc.com/de/de/industrie-teams/oeffentlichersektor/arbeitsbelastung-in-deutschen-sicherheitsbehoerden/strategyand-arbeitsbelastung-in-deutschen-sicherheitsbehoerden.pdf, zuletzt geprüft am 02.12.2024.

Sağlam, Rahime Belen; Nurse, Jason R. C. (2020): Is your chatbot GDPR compliant? In: María Inés Torres, Stephan Schlögl, Leigh Clark und Martin Porcheron (Hg.): *Proceedings of the 2nd Conference on*

Conversational User Interfaces. CUI ,20: 2nd Conference on Conversational User Interfaces. Bilbao, Spain, 22.07.2020 – 24.07.2020. New York, NY, USA: ACM, S. 1-3.

Schmidt, Marcus (2024): Einsatz von künstlicher Intelligenz für sachbearbeitende Tätigkeiten im öffentlichen Dienst. In: *Wirtschaftsinformatik & Management* 16 (2), S. 123-132. DOI: 10.1365/s35764-024-00516-3.

Siegel, M. (2024): Projekt BoTox. Hochschule Darmstadt; Hochschule Fresenius; Gemeinnützige Trägergesellschaft MBH. ikum.medien-campus.h-da.de/projekt/projekt-botox, zuletzt geprüft am 12.12.2024.

Statista (2024a): KI in deutschen Unternehmen. Einsatz von Künstlicher Intelligenz in deutschen Unternehmen in Hinblick auf Potenziale, Herausforderungen und Voraussetzungen. Hg. v. Statista. de-statista-com.eu1.proxy.openathens.net/statistik/studie/id/173446/dokument/ki-in-deutschen-unternehmen/, zuletzt geprüft am 02.12.2024.

Statista (2024b): KI in deutschen Unternehmen – Statista Spotlight-Report. Einsatz von Künstlicher Intelligenz in deutschen Unternehmen in Hinblick auf Potenziale, Herausforderungen und Voraussetzungen. Hg. v. Statista. de-statista-com.eu1.proxy.openathens.net/statistik/studie/id/173446/dokument/ki-in-deutschen-unternehmen/, zuletzt geprüft am 16.12.2024.

Stiftung Warentest (2019): Strafanzeige: So erstatten Sie eine Online-Anzeige. Stiftung Warentest, 13.08.2019. test.de/Strafanzeige-So-erstatten-Sie-eine-Online-Anzeige-5003664-0/, zuletzt geprüft am 02.12.2024.

Stöhr, Christian; Ou, Amy Wanyu; Malmström, Hans (2024): Perceptions and usage of AI chatbots among students in higher education across genders, academic levels and fields of study. *Computers and Education: Artificial Intelligence* 7, S. 100259. DOI: 10.1016/j.caeai.2024.100259.

Stucki, Toni; D'Onofrio, Sara; Portmann, Edy (2019): Chatbots gestalten mit Praxisbeispielen der Schweizerischen Post: HMD Best Paper Award 2018. Wiesbaden, Germany: Springer Vieweg. ebook-central.proquest.com/lib/dhpol/detail.action?docID=5978978.

van Noordt, Colin; Misuraca, Gianluca (2020): Evaluating the impact of artificial intelligence technologies in public services. In: Yannis Charalabidis, Maria Alexandra Cunha und Demetrios Sarantis (Hg.): *Proceedings of the 13th International Conference on Theory and Practice of Electronic Governance. ICEGOV 2020: 13th International Conference on Theory and Practice of Electronic Governance*. Athens, Greece, 23.09.2020 – 25.09.2020. New York, NY, USA: ACM, S. 8-16.

Vassilakopoulou, Polyxeni; Haug, Arve; Salvesen, Leif Martin; Pappas, Ilias O. (2023): Developing human/AI interactions for chat-based customer services: lessons learned from the Norwegian government. *European Journal of Information Systems* 32 (1), S. 10-22. DOI: 10.1080/0960085X.2022.2096490.

Wangler, Leo; Botthof, Alfons (2018): E-Governance: Digitalisierung und KI in der öffentlichen Verwaltung. In: Volker Wittpahl (Hg.): *Künstliche Intelligenz. Technologien | Anwendung | Gesellschaft*. 2019. Berlin, Heidelberg: Springer, S. 122-141.

Wollny, Volrad; Paul, Herbert (2015): Die SWOT-Analyse: Herausforderungen der Nutzung in den Sozialwissenschaften. In: Marlen Niederberger und Sandra Wassermann (Hg.): *Methoden der Experten- und Stakeholdereinbindung in der sozialwissenschaftlichen Forschung*. Wiesbaden: Springer Fachmedien (SpringerLink Bücher), S. 189-213.

Einsatz von Technologien zur Detektion von Messern im öffentlichen Raum

Koray Habel

Tödliche Messerangriffe stehen durch die intensive mediale Berichterstattung häufig im Fokus der Öffentlichkeit. So titelte die Bild-Zeitung Anfang September 2024 vom „Angst-Sommer“ und dokumentierte eine Reihe von Taten, die sich im Zeitraum vom 19. August bis zum 6. September ereigneten (Hildebrand 2024). Der Vorfall von Solingen am 23. August 2024, bei dem der mutmaßliche 26-jährige syrische Täter drei Menschen mit einem Messer während eines Stadtfestes tötete und acht weitere zum Teil schwer verletzte, erhielt besondere mediale Aufmerksamkeit und führte zu weiteren öffentlichen Diskussionen in Bezug auf die Messerkriminalität. Allein in NRW kam es innerhalb einer Woche zu mehreren folgenschweren Messerangriffen (ebd.). Als Folge wurden u. a. die Sicherheitsvorkehrungen beim Oktoberfest in München verschärft, indem die Stadt München erstmals stichprobenartig und verdachtsabhängig mittels händischer Metalldetektoren im Hinblick auf gefährliche Waffen kontrollierte (Tagesspiegel 2024).

Im Juni 2024 fasste der Bundesrat in einen Beschluss zusammen, dass die Kriminalität mit dem Tatmittel „Messer“ ansteigt und weitere Maßnahmen notwendig sind, um Messertaten zu verhindern (Bundesrat 2024). Explizit wird dabei der Schutz für Orte, an denen Menschenmengen im öffentlichen Raum entstehen, benannt (ebd.: S. 1). Neben Verschärfungen des Waffenrechts sollen insbesondere Verbote in Bezug auf den Umgang mit Messern ausgeweitet werden. Fraglich ist, wie die Polizei in der Praxis bereits bestehende gesetzliche Messerverbote und die beabsichtigten Neuerungen wirksam kontrollieren kann.

Das Ziel dieses Beitrages ist, technische Optionen darzustellen, die die Erkennung von Messern mithilfe von Künstlicher Intelligenz (KI) im öffentlichen Raum ermöglichen. Die Forschungsfrage lautet: Welche Technologien können die Detektion von Messern durch die Polizei in der Öffentlichkeit unterstützen?

Die Abgrenzung der Technologien findet insbesondere durch die Art der Durchführung statt. Dies impliziert, dass beispielsweise Sicherheitstechniken der Zugangs- bzw. Zutrittskontrollen, wie sie am Flughafen stattfinden, nicht betrachtet werden, da der Schwerpunkt dieses Beitrages auf der verdachtsunabhängigen mobilen Kontrolle im öffentlichen Raum liegt.

Hintergrund

In diesem Kapitel werden wesentliche Entwicklungen in Bezug auf die Kriminalität mit dem Tatmittel Messer und ein kurzer Überblick über die mit Messern einschlägigen waffenrechtlichen Bestimmungen sowie polizeiliche Maßnahmen zur Kontrolle dargestellt.

Entwicklung der Messerkriminalität

Mit Beschluss der Innenministerkonferenz im Jahr 2018 wurde festgelegt, dass Messerangriffe bundeseinheitlich erfasst werden sollen (Bundesministerium des Innern und für Heimat 2023: S. 15). Demnach werden Messerangriffe nach der Polizeilichen Kriminalstatistik (PKS) definiert als „solche Tathandlungen, bei denen der Angriff mit einem Messer unmittelbar gegen eine Person angedroht oder ausgeführt wird. Das bloße Mitführen eines Messers reicht hingegen für eine Erfassung als Messerangriff nicht aus.“ (ebd.)

Nach der aktuellen PKS-Bund 2023 sind die Fallzahlen im Jahr 2023 im Vergleich zum Vorjahr bei den Delikten gefährliche und schwere Körperverletzung um 9,7 % von 8160 auf 8951 Fälle und bei Raubüberfällen um 16,7 % von 4195 auf 4893 Fälle gestiegen (ebd.). Für NRW existiert eine detaillierte statistische Auswertung in Form eines Lagebildes „Gewalt im öffentlichen Raum – Tatmittel Messer in Nordrhein-Westfalen 2019 bis 2023“ (Landeskriminalamt NRW 2024). Aus dieser ist zu entnehmen, dass ein Anstieg um 3,4 % von 3420 Fällen im Jahr 2019 im Vergleich zum Jahr 2023 mit 3536 Fällen vorliegt (ebd.: S. 7).

Eine Analyse einer eingerichteten Waffenverbotszone von November 2018 bis August 2020 in Leipzig zeigt, dass die am häufigsten sichergestellten Gegenstände verschiedene Arten von Messern (279) waren (Mühler et al. 2022: S. 11). Laut einem Bericht des Ministeriums des Innern des Landes Nordrhein-Westfalen (2024: S. 12) wurden bei durchgeführten Aktionstagen zur Bekämpfung von Messergewalt in NRW im Jahr 2023 im Rahmen von 40.000 Personenkontrollen 237 verbotene Gegenstände, davon 130 Messer, sichergestellt. Bisher gilt als der zentrale Risikofaktor für den Einsatz von Messern schlicht der Umstand des Mitführens eines Messers (Baier & Bergmann 2018; Emmert et al. 2018).

Messer im Kontext Waffenrecht und polizeilicher Maßnahmen

Das Waffengesetz (WaffG) untersagt grundsätzlich den Besitz von verbotenen Messern wie z. B. Butterflymessern (§ 1 Abs. 2 WaffG i. V. m. Anlage 2). Darüber hinaus dürfen jegliche Arten von Messern nicht bei Veranstaltungen geführt werden (§ 42 Abs. 1 WaffG). Das bestehende Führungsverbot von Waffen bei Veranstaltungen soll zukünftig auf Fahrzeuge und baulich umschlossene Einrichtungen des ÖPV erweitert werden (Bundesrat 2024: S. 4). Neben der Untersagung des Besitzes und Erwerbs von bestimmten Waffen (§ 41 WaffG) kann die Polizei NRW ein individuelles Waffentrageverbot auf Grundlage der Generalklausel (§ 8 PolG NRW) verhängen. Seit der Änderung des Waffengesetzes im Jahr 2020 (Bundesgesetzblatt 2020) können zudem Waffenverbotszonen unter bestimmten Voraussetzungen eingerichtet werden (§ 42 Abs. 5 und Abs. 6 WaffG), so wie in NRW bereits in Köln und Düsseldorf geschehen (Staatskanzlei des Landes Nordrhein-Westfalen 2021).

Das Konzeptpapier „Bekämpfung der Messergewalt im öffentlichen Raum“ sieht in seinem 10-Punkte-Plan neben Präventionskonzepten vor allem Maßnahmen wie Aktionstage, Verhängung von Waffentrageverboten, Einrichtung von Waffenverbotszonen, Nutzung der strategischen Fahndung und den verstärkten Einsatz mobiler Videoüberwachung vor (Ministeriums des Innern des Landes Nordrhein-Westfalen 2024). Die letztgenannten Maßnahmen sorgen dafür, dass Personen hinsichtlich des Mitführens von Messern überprüft werden.

Bislang kontrolliert die Polizei NRW Messer auf konventionelle Weise: Entweder bemerken die Beamten vor Ort, dass eine Person ein Messer unerlaubt bei sich trägt oder benutzt, oder es besteht ein begründeter Verdacht, dass jemand ein Messer rechtswidrig mitführt, was dann zu einer Durchsuchung führt. In Ausnahmefällen kann eine anlasslose Durchsuchung in Fällen der strategischen Fahndung (§ 12a PolG NRW) und an „gefährlichen“ oder „gefährdeten“ Orten (§ 12 Abs. 1 Nr. 2a und Abs. 3 PolG NRW) rechtlich zulässig sein.

Methodik

Um das Ziel, eine Orientierung und einen Überblick über die technischen Möglichkeiten zur Detektion von Messern und deren aktuellen Forschungsstand zu gewinnen, wird sich der literaturbasierten Methodik des Scoping Reviews mit Einschränkungen bedient (von Elm et al. 2019). Auf die Fertigung eines Protokolls und die unabhängige Durchführung der Studienauswahl durch einen zweiten Reviewer wurde aufgrund des beschränkten Umfangs und mangels eines zweiten Reviewers in diesem Beitrag verzichtet. Die Ergebnisse sind thematisch in Fließtextform zusammengefasst, ohne zusätzliche tabellarische Datenextraktion.

Das wesentliche Einschlusskriterium ist die mobile und ohne Anhalten einer Person einsetzbare technische Detektion von Messern im öffentlichen Raum.

Als Ausschlusskriterien für Forschungsberichte wurden stationäre Techniken wie Röntgengeräte zur Überprüfung von mitgeführten Gegenständen und 3D-Scanner, wie sie beispielsweise am Flughafen eingesetzt werden, bestehende Techniken wie Metalldetektoren, die nur unmittelbar am Körper angewendet werden können, häufige Suchtreffer wie die industrielle Fertigung und Messgenauigkeit bei Messern und anderen Gegenständen sowie militärische Luft- und Geländeüberwachung gewählt. Als Informationsquellen sind veröffentlichte wissenschaftliche Forschungsartikel, aber auch Websites, einbezogen worden.

Sofern Forschungsartikel ähnliche Themen behandeln, z. B. die Genauigkeit von einzelnen Deep-Learning-Methoden im Bereich der Objekterkennung von Messern bei Videostreams, wurde aufgrund der Vielzahl und des beschränkten Umfangs dieses Beitrags lediglich der aktuelle Forschungsbericht gewählt. Für die Literaturrecherche diente die auf wissenschaftliche Literatur spezialisierte Suchmaschine Google Scholar sowie im Einzelfall Google, um z. B. zu ergründen, ob Polizeien abseits wissenschaftlicher Quellen bereits technische Detektion einsetzen und ob es (kommerzielle) Anbieter gibt, die solche Produkte anbieten bzw. damit werben.

Die Eingabe der Suchbegriffe erfolgte sowohl in deutscher als auch übersetzt in englischer Sprache. Der überwiegende Teil der als relevant erachteten Treffer ist den englischen Begriffen zuzurechnen. Die Suchergebnisse wurden gefiltert nach Relevanz, Erscheinungsdatum der letzten fünf Jahre (Filter ab 2020), um möglichst aktuelle Forschung zum Themengebiet zu erhalten. Viele der Suchergebnissen lieferten mehr als 17.000 Einträge. Hierbei erfolgte eine Beschränkung auf die ersten fünf Ergebnisseiten. Die letzte Recherche wurde am 10. Oktober 2024 durchgeführt.

Ergebnisse

Zunächst erfolgt die Darstellung der Erkennungsmethoden in Bezug auf die Videoüberwachung. Anschließend werden Techniken dargestellt, die versteckt getragene Messer detektieren können.

Messerdetektion durch Videoüberwachungstechnik

Nachfolgend wird die intelligente, also mittels Künstlicher Intelligenz automatisierte Videoüberwachungstechnik (Janitzki 2024: S. 50) zur Detektion von Messern vorgestellt. Diese lassen sich in Verhaltensüberwachung und Objekterkennung von Messern unterscheiden. Die Erkennung von Verhalten und Emotionen in der Videoüberwachung hat nicht die direkte Messerererkennung zum Ziel,

kann aber sich anbahnende eskalierende Situationen erkennen und damit auch die Nutzung von Waffen bzw. Messern verhindern (Golda et al. 2022: S. 1489).

Mithilfe von neuronalen Netzwerken sollen bestehende oder zukünftige Videoüberwachungsanlagen so ertüchtigt werden, dass sie zur automatisierten Objekt- bzw. Waffendetektion eingesetzt werden können (Hnoohom et al. 2022: S. 3). Die neuronalen Netze You Only Look Once (YOLO) und das Region-based Convolutional Neural Network (R-CNN) gelten als die derzeit leistungsfähigsten und am häufigsten verwendeten Deep-Learning-Erkennungsmodelle zur Detektion von Messern (Santos, Oliveira & Cunha 2024: S. 8).

Während der Trainingsphase lernen diese Algorithmen die Merkmale im laufenden Betrieb. Daher benötigen diese Algorithmen eine große Menge an Daten, um trainiert zu werden (Yadav et al. 2023: S. 6). Ein generelles Problem im Zusammenhang mit Deep Learning und der Messerdetektion ist der Umstand, dass zwar Trainingsdatensätze existieren, aber kaum reale Daten (Debnath & Bhowmik 2021: S. 16). Die Erkennung von Messern basiert bisher hauptsächlich auf Trainingsdaten aus öffentlichen Datenbanken (Yadav et al. 2023: S. 3). Ein Ansatz, mehr Trainingsdaten zu erhalten, sind Ergänzungstechniken wie Drehung, Spiegelung, Vergrößern und Verkleinern der Originalbilder (Liu & Hu 2023: S. 176).

Zur Verfügung stehende Trainingsdaten wurden im Rahmen unterschiedlicher Studien individuell angepasst, was eine Vergleichbarkeit der Studien erschwert (Santos et al. 2024: S. 8). Es wird ferner als erforderlich angesehen, mehr reelle Trainingsdaten zu erhalten, wie sie im echten Einsatz von Überwachungskameras vorzufinden sind, um die Erkennung zu verbessern (ebd.). Zudem sind die meisten Deep-Learning-Methoden dazu konzipiert worden, größere Objekte zu erkennen. Kleine Objekte wie Messer haben jedoch andere Anforderungen (u. a. weniger Pixel), sodass hier Forschungsbedarf gesehen wird (Debnath & Bhowmik 2021: S. 16).

Generelle Schwierigkeiten bei der Erkennung von Waffen und Messern sind Fehlklassifizierungen, ein dynamischer Hintergrund, Verdeckung und unterschiedliche Lichtverhältnisse (Yadav et al. 2023: S. 10). Santos et al. (2024: S. 8) formulieren als aktuelle wesentliche Herausforderung zusätzlich die geringe Auflösung. Letztlich fordern sie die Erprobung im Realbetrieb unter echten Bedingungen, um zu ermitteln, wie gut die Systeme tatsächlich funktionieren (ebd.: S. 9).

Das Forschungsprojekt i-Police aus Sri Lanka entwickelte ein intelligentes Überwachungssystem für die öffentliche Sicherheit, wozu u. a. auch die Erkennung von Messern und anderen Waffen bei der Videoüberwachung gehörte. Die Autoren kamen zu dem Schluss, dass die Genauigkeit gut genug ist, um es in der Praxis einzusetzen (Jayakody et al. 2021: S. 152). Jedoch war die Reaktionszeit des Systems mit ca. 30 Sekunden so hoch, dass es mit Stand 2021 als zu langsam für den Einsatz in Echtzeit galt und daher Forschungsbedarf gesehen wurde (ebd.: S. 154).

In einer im Jahr 2022 vorgestellten Studie wurde ein Trainingsdatensatz mit elf abweichenden menschlichen Handlungen, darunter Belästigung, Kampf und Bedrohung mit Messern, erstellt und mit einem neuronalen Netzwerk getestet (Vrskova et al. 2022). Im Ergebnis wurde eine hohe Klassifizierungsgenauigkeit von über 90 % erreicht, wobei diese anhand mit Laiendarstellern generierten Videoaufnahmen unter „Laborbedingungen“ stattfand (ebd.: S. 14).

Das Fraunhofer-Institut für Optronik, Systemtechnik und Bildauswertung (IOSB) testet seit dem Jahr 2018 und bis voraussichtlich zum Jahr 2026 (Beer 2024) gemeinsam mit dem Land Baden-Württemberg und dem Polizeipräsidium Mannheim eine intelligente Videoüberwachung, die es ermöglichen soll, den Fokus auf die automatisierte Erkennung von aggressivem Verhalten und damit polizeilich relevanten Situationen in Echtzeit zu legen (Golda et al. 2022). Dabei wird anhand von ca. 70 Full-HD-Kameras an Kriminalitätsschwerpunkten in der Innenstadt Mannheims das Videosignal analysiert und bei Erkennen eines zuvor klassifizierten Verhaltens dieses einem Entscheider gemeldet (ebd.: S. 1488). Die Erkennung funktioniert technisch durch ein neuronales Netz, welches mit Trainingsdaten gespeist wird

und in einem ersten Schritt Personen zunächst in eine Strichfigur bzw. Skelett umwandelt. Es erfolgt eine Filterung nach Auffälligkeit und im letzten Schritt die Klassifikation der Aktivität. Als Trainingsdaten dienen sowohl öffentliche als auch selbst erstellte Daten (ebd.: S. 1490 f.). Perspektivisch ist denkbar, dass im Rahmen dieses Projektes NEST (Network Enabled Surveillance and Tracking) auch Objekte wie Waffen detektiert werden (ebd.: S. 1493).

Detektion von verdeckt getragenen Messern

Neben der Detektion mittels optischer Videoüberwachungstechnik existieren weitere bildgebende Verfahren, um verdeckt getragene bzw. versteckte Gegenstände wie Messer zu erkennen. Dazu zählen die Wärmebild- bzw. Infrarottechnik, Millimeterwellen und Terahertzwellen (MMW/THz) sowie Röntgentechnologie (Jayachitra et al. 2023: S. 2710; Gosain et al. 2021: S. 1374). Zudem gibt es Bildfusionsverfahren zur Fusion von zwei oder mehreren Bildquellen, um die Erkennung weiter zu verbessern (Gosain et al. 2021: S. 1374; Ünal 2023: S. 5). Die Röntgentechnologie wird aufgrund von Gesundheitsrisiken nicht bei der Objekterkennung am Menschen eingesetzt (Khor et al. 2024: S. 2).

Infrarot- bzw. Wärmebildtechnik

Die Infrarot-/Wärmebildtechnik basiert auf der Infrarot- bzw. Wärmestrahlung, die von allen Objekten ausgeht. Die Wärmesignatur einer Waffe bzw. eines Messers weicht von der des menschlichen Körpers ab, sodass eine Waffe im Wärmebild identifiziert werden kann (Gosain et al. 2021: S. 1375). Zunächst überträgt die Haut Wärme auf ein verdeckt getragenes Objekt, wodurch sich dieses erwärmt. Anschließend gibt das verdeckte Objekt Wärme an die Kleidung ab. Gleichzeitig erwärmt die Haut auch den umgebenden Stoff in einem anderen, von dem Objekt getrennten Bereich. Der Temperaturunterschied, der auf dem Stoff festgestellt wird, wird zum Indikator für das verborgene Objekt unter dem Stoff (Ünal 2023: S. 3).

Vorteile des Wärmebildverfahrens sind, dass es für den menschlichen Körper im Gegensatz zur bspw. Röntgenstrahlung unschädlich ist, kompakt und bei jedem Wetter eingesetzt werden kann (Hou et al. 2022: S. 2) und im Hinblick auf Persönlichkeitsrechte bzw. Datenschutz Personen bzw. Gesichtszüge nicht erkannt werden können (Khor et al. 2024: S. 2). Infrarottechnik kann in höherer Entfernung als die MMW/THz-Technik genutzt werden, hat eine höhere Auflösung und kann mehrere Personen und Objekte gleichzeitig erfassen (Hou et al. 2022: S. 3). Da aber mehrere Kleidungsschichten die Detektion mittels Infrarottechnik signifikant verschlechtern, wurde vermehrt die MMW/THz-Technik für die Detektion erforscht und entwickelt (ebd.: S. 3). Aufgrund des geringen Bildkontrastes und der geringen Bildauflösung bedarf die Infrarot-Wärmebildtechnik zusätzlich einiger Optimierungsprozesse, um Objekte zuverlässig detektieren zu können (ebd.: S. 2).

In einer Studie wurden mittels des neuronalen Netzwerks Google-Net Infrarotbilder von unterschiedlich großen Messern nach „vorhanden“ und „nicht vorhanden“ mit einer Genauigkeit von ca. 97 % klassifiziert (Yuenyong et al. 2018). Eine Studie aus dem Jahr 2024 untersucht die Erkennung verdeckter Objekte mittels Infrarot-Wärmebildtechnik und verwendet dabei verschiedene Methoden des maschinellen Lernens zur Optimierung des Bildes sowie ein neuronales Netzwerk zur Klassifizierung, ob ein verdeckt getragenes Objekt vorhanden ist oder nicht (Khor et al. 2024). Dabei liefert ein kleiner trainierter Datensatz (n = 900 Bilder) und ein größerer Datensatz (n = 3082 Bilder) einen AUC-Wert von 0,869 bzw. 0,922, was eine hohe Genauigkeit der Klassifizierung impliziert (ebd.: S. 10).

Millimeterwellen- und Terahertzwellentechnik

Passive MMW/THz-Bildgebungssysteme beruhen, ähnlich wie Infrarotsysteme, auf selbst emittierter Strahlung, die auch der Mensch ausstrahlt. Diese Eigenschaft macht externe Quellen wie Sonnenlicht oder zusätzliche Beleuchtung überflüssig. Außerdem sind Materialien wie Stoff in den MMW/THz-Bändern transparent (Ünal 2023: S. 1), nicht jedoch metallische Gegenstände (Kasjoo et al. 2020: S. 1). Dies ermöglicht die Erkennung von anderen Materialien unter der Kleidung. Die

Herausforderung bei passiven MMW/THz-Bildern ist es aufgrund eines geringen dynamischen Bereiches, den Unterschied zwischen verschiedenen Materialien auf dem Körper darzustellen. Da dies manuell sehr schwer ist und bisherige Methoden des maschinellen Lernens insbesondere bei komplexeren Bildhintergründen an ihre Grenzen gelangen, kommen Deep-Learning-Methoden zum Einsatz, um die Erkennung zu verbessern (Cheng et al. 2022: S. 2, 4). Versteckte Waffen können dann durch einen Kontrastunterschied in den erzeugten Bildern erkannt werden (Ünal 2023: S. 2). Auch eine visuelle schlechte Sichtbarkeit durch z. B. Nebel kann damit umgangen werden, allerdings muss eine gewisse Nähe (unter zehn Meter) vorhanden sein, um Objekte an einer Person erkennen zu können (Khor et al. 2024: S. 2).

Eine Studie aus dem Jahr 2022 versucht mittels MMW/THz die bestehenden Probleme der Objekterkennung, eine zu geringe Genauigkeit sowie Geschwindigkeit, mit verschiedenen Anpassungen zu lösen (Cheng et al. 2022: S. 2). Im Ergebnis wurden mittels eines speziell angepassten neuronalen Netzwerks (ResNet-50) und dem Single Shot MultiBox Detector (SSD)-Algorithmus eine Genauigkeit von 99,9 % und eine Erkennungsgeschwindigkeit von 17 FPS erreicht (ebd.: S. 13). Die Autoren gehen davon aus, dass ihre Studie damit den Echtzeitanforderungen genügt (ebd.). Analog zu anderen Studien wurde auch hier der Bedarf gesehen, dass mehr Trainingsdatensätze erforderlich sind (ebd.: S. 10).

Im Rahmen eines Projektes an der Universität Oxford wurde ein tragbarer, kostengünstiger und stromsparender MMW-Scanner zur Erkennung von versteckten Waffen entwickelt, der mit den drei Gegenständen Telefon, Messer und Schraubendreher getestet wurde (Khachaturov 2022: S. 7). Genutzt wurden ein MMW-Sensor zusammen mit einem Android-Smartphone zur Positionsbestimmung sowie ein Notebook, welches zur Klassifizierung mittels eines neuronalen Netzwerks eingesetzt wurde (ebd.: S. 62). Perspektivisch soll das Notebook gänzlich durch das Smartphone ersetzt werden können (ebd.: S. 63). Insgesamt konnte unter Laborbedingungen eine Genauigkeit von mehr als 85 % erreicht werden (ebd.).

Einen weiteren Ansatz, versteckte Waffen zu erkennen, liefern japanische Forscher, indem sie eine Art Durchgangskontrollsystem auf Basis von MMW-Technik entwickelten (Khan et al. 2023). Dabei kommen zwei parallele MMW-Sensoren zum Einsatz, die ein 3D-Bild erstellen, welches durch ein neuronales Netzwerk klassifiziert wird (ebd.: S. 674 f.). Bei einer Genauigkeit von ca. 89 % und einer Bearbeitungsdauer von unter 50 ms stellen die Autoren fest, dass sich das System für den Echtzeiteinsatz in der Praxis eignet (ebd.: S. 678-680). Einschränkend ist zu erwähnen, dass in den Versuchen lediglich die Erkennung von Pistolen getestet wurde.

Ein Forscherteam der Universität Glasgow entwickelte „mmSense“, ein mobiles auf MMW-Technik basierendes System, welches bis zu einer Reichweite von drei Metern versteckte Waffen in Echtzeit und mit gängiger Hardware wie Notebooks erkennen soll (Mitchell et al. 2024). Dabei wird der Soli-Sensor von Google auf Basis der MMW-Technik verwendet, der bereits zum Einsatz bei der Erkennung von Gesten und Bewegungen kommt, sowie ein selbst entwickeltes neuronales Netzwerk „TransDope“ zur Klassifizierung (ebd.: S. 2 f.). Die Entwickler stellen ihr System „mmSense“ zudem „open source“ zur Verfügung, um weitere Forschung zu ermöglichen (ebd.: S. 2). Es wurden verschiedene Szenarien erstellt, darunter ein Szenario mit fünf Personen, die verschiedene Alltagsgegenstände wie Telefone, Schlüssel und Gürtel bei sich trugen. Eine der Personen trug ein Messer. In dieser Szene wurde die Detektion des Messers mit einer Genauigkeit von bis zu 87 % erreicht (ebd.: S. 4). Die Genauigkeit des Systems nahm jedoch auf bis zu 74 % ab, wenn die Szene in geschlossenen Räumen stattfand, was auf die Reflexionen der Signale zurückzuführen war (ebd.).

Die Firma Thruvision bietet seit einigen Jahren kommerzielle THz-basierte Waffendetektoren mit der Bezeichnung „TS4-SC“ an, die im Abstand von drei bis acht Metern eingesetzt werden können und mit 24 kg bedingt mobil einsetzbar sind (Kasjoo et al. 2020: S. 3). Das System soll in Echtzeit verschiedene Arten von Material bzw. Waffen detektieren und mehr als 2.000 Personen pro Stunde kontrollieren können (Thruvision 2019).

Auch die Firma CEIA bietet ein mobiles Produkt zur Erkennung von Waffen namens „Opengate“ an (Heckmann 2021: S. 94). Dies besteht aus zwei portablen Säulen, die auf Basis elektromagnetischer Technik eine Durchgangskontrolle mit einer Breite von 68 cm bis 100 cm ermöglichen sollen (ebd.). Das System soll dabei autark bis zu 14 Stunden betrieben werden können und meldet sowohl akustisch als auch über eine visuelle Lichtanzeige einen Treffer. Explizit nennt der Hersteller nicht die Messerdetektion, sondern formuliert als Ziel die Detektion von Schusswaffen sowie metallhaltigen Sprengvorrichtungen (CEIA 2024).

Die britische Polizei testet verschiedene Systeme zur Detektion von Messern (Hymas 2024a, 2024b; Coyle 2024; NTU 2019). Bereits im Jahr 2019 erhielten die Nottingham Trent University (NTU 2019) und die Loughborough University den Auftrag des britischen Innenministeriums, innovative Techniken zur Messerdetektion zu erforschen. Dabei sollen elektromagnetische Infrarotwellen, optische Videokameras und Smartphones in Verbindung mit Computeralgorithmen zum Einsatz kommen. Ersten Tests zufolge soll das System aus einer Entfernung mit bis zu sechs Metern versteckte Messer erkennen (ebd.). Ein Vertreter des Innenministeriums äußerte in einem Zeitungsbericht, dass das System voraussichtlich im Jahr 2025 bei der Polizei eingesetzt werden soll (Hymas 2024a). Ein weiteres mobiles System basierend auf THz-Technik der Firma Lassen Peak sei nach Aussage des britischen Innenministeriums ebenfalls in Erprobung (Hymas 2024b). Hierbei könnte es sich um das System „Airfrisk“ der Firma handeln (Lassen Peak 2024a). In dem Artikel wird aber auch darauf hingewiesen, dass das System noch nicht ausgereift sei (Hymas 2024b). Zudem erweckt der Hersteller in einem Präsentationsvideo den Eindruck, dass es nur bei Personen eingesetzt werden kann, die vor der kontrollierenden Person still stehen (Lassen Peak 2024b). In West Yorkshire sollen zukünftig fünf mobile Säulensysteme der Firma Metrasens mit der Bezeichnung „Ultra“ zur Messerdetektion eingesetzt werden (Coyle 2024). Praktische Erfahrungen oder Forschungsartikel, die die Leistungsfähigkeit bzw. Genauigkeit der Systeme belegen, konnten öffentlich zugänglich weder für die Systeme von Thruvision, Lassen Peak, Opengate noch das Metrasens ermittelt werden.

Diskussion

Der vorliegende Beitrag untersucht die technischen Möglichkeiten zur Detektion von Messern, auch unter Einsatz von KI, im öffentlichen Raum. Die intelligente Videoüberwachungstechnik kann mit der Erkennung von aggressivem Verhalten und der Objekterkennung von Messern eine Unterstützung für Polizeibeamte darstellen, die bisher Überwachungsmonitore auf konventionelle Art betrachten. Systeme, wie in Mannheim eingesetzt, schützen die Polizei vor Racial-Profilings-Vorwürfen, indem die KI lediglich anhand von gefilterten Bewegungsmerkmalen ein potenziell bedrohliches Verhalten erkennt und meldet. Der Vorteil der intelligenten Videoüberwachung ist, dass sie bereits auf vorhandene Systeme zurückgreifen und durch KI-Einsatz ergänzt werden kann.

Die aktuellen Herausforderungen der Messerdetektion in der Videoüberwachung mittels KI liegen neben Fehlklassifizierungen bei dynamischem Hintergrund, unterschiedlichen Lichtverhältnissen, geringer Auflösung, Mangel an realen Trainingsdaten und geringer Erprobung im Realbetrieb. Eine vertretbare Menge an Fehlklassifizierungen wären dabei durch den Umstand, dass immer noch Polizeibeamte das Ergebnis bzw. die Meldung kontrollieren bzw. über Folgemaßnahmen entscheiden, hinnehmbar. Ein Problem, welches die Messerererkennung in der Videoüberwachung nicht verhindern kann, ist die Reaktionszeit, wenn ein Messer erkannt wird und die Person bereits dieses gegen andere Menschen einsetzt. Hier können Methoden zur verdeckten bzw. versteckten Messerdetektion im Vordergrund eingesetzt werden.

Die MMW-/THz-Technik stellt derzeit den Schwerpunkt der Erforschung der verdeckten Messerdetektion dar und beinhaltet einige vielversprechende Ansätze. Deep-Learning-Methoden werden hier eingesetzt und könnten zukünftig der Entwicklung endanwenderfreundlicher Systeme dienen, die jeder Polizeibeamte ohne gesonderte technische Ausbildung oder spezielle Fortbildung bedienen kann. Dennoch sind die meisten Ansätze zur Messerdetektion noch nicht in der Praxiserprobung. Einschränkungen bei der technischen Detektion von Messern mittels KI stellen aber auch ein Risiko dar,

wie an einer Schule in den USA im Jahr 2023 berichtet wurde, als Messer von einem System nicht erkannt wurden (Clayton 2023). Allerdings sind auch Polizeibeamte bei der Durchsichtung nicht unfehlbar. Zudem könnte eine Vielzahl von Messerdetektionen perspektivisch erst durch eine Trefferanzeige der Systeme ermöglicht werden. Damit hat die technische Messerdetektion auch den Vorteil, dass Personen nur angehalten, kontrolliert und ggf. durchsucht werden, wenn das System einen Treffer meldet bzw. anzeigt. Dies ist grundrechtsschonender und beugt ebenfalls Racial Profiling vor. Einschränkend könnte möglicherweise der restriktive Datenschutz in Deutschland und auch der europäische AI Act wirken, der risikoorientiert den Einsatz bestimmter KI-Modelle durch hohe Auflagen einschränkt oder verbietet. Letztlich wurden weder eine detaillierte Vergleichsanalyse der Detektionsverfahren bzw. vorgestellten Systeme noch eigene Tests durchgeführt, sodass eindeutige Empfehlungen für den polizeilichen Einsatz nicht formuliert werden können.

Schlussfolgerungen

Das Potenzial moderner Techniken zur Messerdetektion in Verbindung mit dem Einsatz von KI bzw. Deep-Learning-Methoden bietet vielversprechende Ansätze, die noch weiter erforscht und unter Realbedingungen erprobt werden müssen. Praktisch betrachtet, könnten die vorgestellten Technologien in Zukunft einen wertvollen Beitrag zur öffentlichen Sicherheit leisten, insbesondere in Bereichen mit hohen Menschenansammlungen wie Stadtfesten oder in öffentlichen Verkehrsmitteln. Auch könnten Polizeibehörden im Allgemeinen ihre Effizienz bei Waffenkontrollen erhöhen.

Innovative Technik wie die dargestellte Messerdetektion ist geeignet, das Sicherheitsgefühl der Bevölkerung zu stärken und das Bild der Polizei als moderne Institution zu verbessern. Ebenso kann ein wertvoller Beitrag in Bezug auf die Eigensicherung der Polizeibeamtinnen und Polizeibeamten geleistet werden, da sie eine Möglichkeit erhalten, bereits vor dem Durchsuchen nach gefährlichen Gegenständen diese schon mit einem Sicherheitsabstand zu detektieren. Weiterentwicklungen könnten zukünftig auch für die Detektion von

anderen versteckten Gegenständen, die potenziell gefährlich sind, verbotenen Stoffen wie Drogen oder z. B. für Diebesgut ausgeweitet und damit sinnvoll eingesetzt werden.

Literaturverzeichnis

Baier, D. & Bergmann, M.C. (2018). Messer im Jugendalltag. Befunde aus niedersachsenweit repräsentativen Schülerbefragungen. Kriminalistik. Ausgabe 5/2018. Heft 72. S. 275-281.

Beer, K. (2024). Videoüberwachung mit KI: Mannheimer Projekt bis 2026 verlängert. heise online. [heise.de/news/Evaluation-von-intelligenter-Videoueberwachung-in-Mannheim-erst-2027-9580827.html](https://www.heise.de/news/Evaluation-von-intelligenter-Videoueberwachung-in-Mannheim-erst-2027-9580827.html) [Zuletzt geprüft am 16.10.2024].

Bundesgesetzblatt (2020). Drittes Gesetz zur Änderung des Waffengesetzes und weiterer Vorschriften (Drittes Waffenrechtsänderungsgesetz – 3. WaffRÄndG). 17. Februar 2020. [bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBI&start=//%5b@attr_id=%27bgbl120s0166.pdf%27%5d#__bgbl__%2F%2F*%5B%40attr_id%3D%27bgbl120s0166.pdf%27%5D__1728471632276](https://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBI&start=//%5b@attr_id=%27bgbl120s0166.pdf%27%5d#__bgbl__%2F%2F*%5B%40attr_id%3D%27bgbl120s0166.pdf%27%5D__1728471632276) [Zuletzt geprüft am 07.10.2024].

Bundesministerium des Innern und für Heimat (2023). Polizeiliche Kriminalstatistik 2023. Ausgewählte Zahlen im Überblick. Stand März 2024 V1.0. Berlin.

Bundesrat (2024). Entschließung des Bundesrates „Messerkriminalität wirksam bekämpfen und Novelle des Waffenrechts zügig voranbringen“. Drucksache 263/24 (Beschluss) vom 14.06.2024.

CEIA GmbH (2024). OPENGATE. Automatisches & mobiles Waffendetektionssystem für Events und kritische Infrastrukturen, ceia.net/security/product.aspx?a=OPENGATE [Zuletzt geprüft am 10.10.2024].

Cheng, L., Ji, Y., Li, C., Liu, X. & Fang, G. (2022). Improved SSD network for fast concealed object detection and recognition in passive terahertz security images. Scientific Reports. 2022. 12. S. 1-12. doi.org/10.1038/s41598-022-16208-0 [Zuletzt geprüft am 10.10.2024].

- Clayton, J. (2023). AI scanner used in hundreds of US schools misses knives. BBC Online Artikel vom 23.05.2023. [bbc.com/news/technology-65342798](https://www.bbc.com/news/technology-65342798) [Zuletzt geprüft am 10.10.2024].
- Coyle, H. (2024). High-tech detectors launched to tackle knife crime. BBC Online Artikel vom 12.08.2024. [bbc.com/news/articles/cgl2y-087w5ko](https://www.bbc.com/news/articles/cgl2y-087w5ko) [Zuletzt geprüft am 10.10.2024].
- Debnath, R., Bhowmik, M.K. (2021). A comprehensive survey on computer vision based concepts, methodologies, analysis and applications for automatic gun/knife detection. *Journal of Visual Communication and Image Representation*. 78. S. 1-19. doi.org/10.1016/j.jvcir.2021.103165 [Zuletzt geprüft am 10.10.2024].
- Emmert, A.D., Hall, G.P. & Lizotte, A.J. (2018). Do weapons facilitate adolescent delinquency? An examination of weapon carrying and delinquency among adolescents. *Crime & Delinquency*. 64. S. 342-362. doi.org/10.1177/0011128717714466
- Golda, T., Cormier, M. & Beyerer, J. (2022). Intelligente Bild- und Videoauswertung für die Sicherheit. In: Wehe, D., Siller, H. (Hrsg.). *Handbuch Polizeimanagement. Polizeipolitik – Polizeiwissenschaft – Polizeipraxis*. 2. Auflage. Springer Gabler. Wiesbaden.
- Gosain, S., Sonare, A. & Wakodkar S. (2021). Concealed Weapon Detection using Image Processing and Machine Learning. *International Journal for Research in Applied Science and Engineering Technology*. 2021. Volume 9. No. 12. S. 1374-1384. doi.org/10.22214/ijraset.2021.39506 [Zuletzt geprüft am 10.10.2024].
- Heckmann, L. (2021). Revolutionäre Detektion von Waffen bei der Kontrolle von Personen mit Gepäck, Rucksäcken und Taschen. *Crisis Prevention. Das Fachmagazin für Gefahrenabwehr, Innere Sicherheit und Katastrophenhilfe*. 3/2021. S. 94-95.
- Hildebrand, K. (2024). Macheten! Messer! Terror! Der Angst-Sommer. Bild dokumentiert die schrecklichen Taten der vergangenen Wochen. *Bild.de*. [bild.de/news/inland/messer-angriffe-schuesse-tote-chronologie-der-angst-in-deutschland-66dac6f09a47a66118e1d736#fromWall](https://www.bild.de/news/inland/messer-angriffe-schuesse-tote-chronologie-der-angst-in-deutschland-66dac6f09a47a66118e1d736#fromWall) [Zuletzt geprüft am 07.10.2024].
- Hnoohom, N., Chotivatunyu, P. & Jitpattanakul, A. (2022). ACF: An Armed CCTV Footage Dataset for Enhancing Weapon Detection. *Sensors*. 2022. 22. 7158. S. 1-30. doi.org/10.3390/s22197158 [Zuletzt geprüft am 10.10.2024].
- Hou, F., Zhang, Y., Zhou, Y., Zhang, M., Lv, B. & Wu, J. (2022). Review on Infrared Imaging Technology. *Sustainability*. 2022. Volume 14. S. 1-26. doi.org/10.3390/su141811161 [Zuletzt geprüft am 10.10.2024].
- Hymas, C. (2024a). Police to use handheld 'X-ray cameras' to detect hidden knives under clothes. *The Telegraph Online Artikel* vom 25.01.2024. [telegraph.co.uk/news/2024/01/25/police-x-ray-cameras-detect-hidden-knives-chris-philp/](https://www.telegraph.co.uk/news/2024/01/25/police-x-ray-cameras-detect-hidden-knives-chris-philp/) [Zuletzt geprüft am 10.10.2024].
- Hymas, C. (2024b). Portable knife scanners to keep our streets safe. *The Telegraph Online Artikel* vom 04.06.2024. [telegraph.co.uk/news/2024/06/04/portable-knife-scanners-detect-weapons-distance-trials/](https://www.telegraph.co.uk/news/2024/06/04/portable-knife-scanners-detect-weapons-distance-trials/) [Zuletzt geprüft am 10.10.2024].
- Janitzki, D. (2024). Intelligente Videoüberwachung. Funktionsweise und Möglichkeiten der Nutzung durch die Polizei. *Kriminalistik* 2024. S. 49-53.
- Jayachitra, J., Devi, K.S., Manisekaran, S.V. & Satti, S.K. (2023). An optimal deep learning model for recognition of hidden hazardous weapons in terahertz and millimeter wave images. *Earth Science Informatics*. 2023. Volume 16. S. 2709-2726. doi.org/10.1007/s12145-023-01056-x [Zuletzt geprüft am 10.10.2024].

Jayakody, A., Lokuliyana, S., Dasanayaka, K., Iddamalgoda, A. Ganepola, I. & Dissanayake, A. (2021). i-Police – An Intelligent Policing System Through Public Area Surveillance. 2021 IEEE 12th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON). 2021. S. 148-154.

Kasjoo, S.R., Mokhar, M.B.M., Zakaria, N.F., Juhari, N.J. (2020). A brief overview of detectors used for terahertz imaging systems, AIP Conf. Proc. 8 January 2020. The 2nd International Conference on applied photonics and electronics 2019 (InCAPE 2019). Volume 2203. Issue 1. Malaysia. S. 1-8. doi.org/10.1063/1.5142112 [Zuletzt geprüft am 10.10.2024].

Khachaturov, D.G. (2022). Portable, Low-Cost, and Low-Power mmWave Radar Imaging for Concealed Weapon Detection. Dissertation. University of Oxford. davidobot.net/resources/msc_oxford_dissertation.pdf [Zuletzt geprüft am 10.10.2024].

Khan, N.S., Ogura, K., Cosatto, E. & Ariyoshi, M. (2023). Real-Time Concealed Weapon Detection on 3D Radar Images for Walk-Through Screening System. Proceedings of the IEEE/CVF Winter Conference on Applications of Computer Vision. 2023. Waikoloa. Hawaii. S. 673-681. openaccess.thecvf.com/content/WACV2023/papers/Khan_Real-Time_Concealed_Weapon_Detection_on_3D_Radar_Images_for_Walk-Through_WACV_2023_paper.pdf [Zuletzt geprüft am 10.10.2024]

Khor, W., Chen, Y.K., Roberts, M. & Ciampa, F. (2024). Infrared thermography as a non-invasive scanner for concealed weapon detection. Cranfield Online Research Data (CORD). Cranfield University. S. 1-14. dspace.lib.cranfield.ac.uk/items/fe7d5456-a13d-4d54-aaff-ba8594c9d2e8 [Zuletzt geprüft am 10.10.2024].

Landeskriminalamt Nordrhein-Westfalen (2024). Gewalt im öffentlichen Raum – Tatmittel Messer in Nordrhein-Westfalen 2019 bis 2023. Stand 27. August 2024. Düsseldorf.

Lassen Peak (2024a). AIRFRISK. lassenpeak.com/airfrisk/ [Zuletzt geprüft am 31.10.2024].

Lassen Peak (2024b). 2-minute introductory video. Video des Herstellers mit Stand 31.10.2024. URL der Website: lassenpeak.com/public-safety/. URL des Videos: lassenpeak.com/wp-content/uploads/2024/02/24lsn3221_scanner_overview_d1-720p.mp4 [Zuletzt geprüft am 31.10.2024].

Liu, H., Hu, Z. (2023). An Edge Computing-based Handgun and Knife Detection Method in IoT Video Surveillance Systems. International Journal of Advanced Computer Science and Applications (IJACSA). 2023. Volume 14. No. 11. S. 175-185. dx.doi.org/10.14569/IJACSA.2023.0141117 [Zuletzt geprüft am 10.10.2024].

Ministerium des Innern des Landes Nordrhein-Westfalen (2024). Konzeptpapier „Bekämpfung der Messergewalt im öffentlichen Raum“. polizei.nrw/sites/default/files/2024-08/2024-08-28_konzept-bekämpfung-messergewalt.pdf [Zuletzt geprüft am 07.10.2024].

Mitchell, K., Kassem, K., Kaul, C., Kapitany, V., Binner, P. & Andrew, R. (2024). mmSense: Detecting Concealed Weapons with a Miniature Radar Sensor. 2023 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP 2023). Rhodes Island, Greece. S. 1-5. doi.org/10.1109/ICASSP49357.2023.10095884 [Zuletzt geprüft am 10.10.2024].

Mühler, K., Dittrich, F., Fleps, T., Grohmann, P., Heyden, A., Keßler P. & Radici, J. (2022). Die Leipziger Waffenverbotszone. Analysen zu Kriminalitätsverlauf, Akzeptanz und Sicherheitsgefühl. Rothenburger Beiträge zur Polizei- & Sicherheitsforschung – Band 109. Sächsisches Institut für Polizei- und Sicherheitsforschung.

NTU (Nottingham Trent University) (2019). Scanners to spot hidden knives and reduce unnecessary police searches. Online-Artikel vom 04.04.2019. ntu.ac.uk/about-us/news/news-articles/2019/04/scanners-to-spot-hidden-knives-and-reduce-unnecessary-police-searches [Zuletzt geprüft am 10.10.2024].

Polizeigesetz des Landes Nordrhein-Westfalen (PolG NRW) vom 25. Juli 2003, das zuletzt durch Gesetz vom 19. Dezember 2023 (GV. NRW. S. 1394) geändert worden ist, in Kraft getreten am 29. Dezember 2023.

Santos, T., Oliveira, H. & Cunha, A. (2024). Systematic review on weapon detection in surveillance footage through deep learning. *Computer Science Review*. 2024. Volume 51. S. 1-10. doi.org/10.1016/j.cosrev.2023.100612 [Zuletzt geprüft am 10.10.2024].

Staatskanzlei des Landes Nordrhein-Westfalen (2021). Köln und Düsseldorf: Innenministerium bringt Waffenverbotszonen auf den Weg. 7. Dezember 2021. land.nrw/pressemitteilung/koeln-und-duesseldorf-innenministerium-bringt-waffenverbotszonen-auf-den-weg [Zuletzt geprüft am 07.10.2024].

Tagesspiegel (2024). Metalldetektoren, Abtastungen und mehr Ordner: Schärfere Sicherheitsmaßnahmen auf dem Oktoberfest. 12.09.2024. tagesspiegel.de/gesellschaft/panorama/scharfersicherheitsmassnahmen-nach-anschlagen-metalldetektoren-abtastungen-und-mehr-ordner-auf-wiesn-12363395.html [Zuletzt geprüft am 07.10.2024].

Thruvision (2019). Thruvision TS4-SC. Data Sheet. 03/2019. V.1.4. thruvision.com/wp-content/uploads/2019/07/1903-TV-TS4-SC-Data-sheet-v1.4.pdf&ved=2ahUKEwiDh6WR77iJAxVz9LsIHZceLv0QF-noECBUQAQ&usq=AOvVaw05kMrhQNedQMm8uTGVjiXg [Zuletzt geprüft am 10.10.2024].

Ünal, A. (2023). Multi-band passive detection and imaging system for concealed weapon with dual assessment method. *Engineering Research Express*. 2023. Volume 5. No. 4. S. 1-16. doi.org/10.1088/2631-8695/ad0bda [Zuletzt geprüft am 10.10.2024].

von Elm, E., Schreiber, G. & Haupt C.C. (2019). Methodische Anleitung für Scoping Reviews (JBI-Methodologie). *Zeitschrift für Evidenz, Fortbildung und Qualität im Gesundheitswesen*. Volume 143. Juni 2019. S. 1-7. zefq-journal.com/article/S1865-9217(19)30066-2/fulltext [Zuletzt geprüft am 10.10.2024].

Vrskova, R., Hudec, R., Kamencay, P. & Sykora, P. (2022). A New Approach for Abnormal Human Activities Recognition Based on ConvLSTM Architecture. *Sensors*. 2022. 22 (8). 2946. S. 1-16. doi.org/10.3390/s22082946 [Zuletzt geprüft am 10.10.2024].

Waffengesetz (WaffG) vom 11. Oktober 2002 (BGBl. I S. 3970, 4592), 2003 I 1957), das zuletzt durch Artikel 228 der Verordnung vom 19. Juni 2020 (BGBl. I S. 1328) geändert worden ist.

Yadav, P., Gupta, N., Sharma, P.K. (2023). A comprehensive study towards high-level approaches for weapon detection using classical machine learning and deep learning methods. *Expert Systems with Applications*. 2023. 212. S. 1-20. doi.org/10.1016/j.eswa.2022.118698 [Zuletzt geprüft am 10.10.2024].

Yuenyong, S., Hnoohom, N. & Wongpatikaseree K. (2018). Automatic detection of knives in infrared images. 15th International Conference on Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology (ECTI-NCON2018). S. 65-68. doi.org/10.1109/ECTI-NCON.2018.8378283 [Zuletzt geprüft am 10.10.2024].

Der Einsatz von Künstlicher Intelligenz im Geldwäsche-Transaktionsmonitoring

Manuel Lubos

Die aktuelle Dimension der Geldwäsche in Deutschland zeigt sich in besorgniserregenden Zahlen. Die Financial Intelligence Unit (FIU) des deutschen Zolls verzeichnete im Jahr 2023 insgesamt 322.590 Verdachtsmeldungen, was die anhaltende Brisanz der Situation unterstreicht (Zoll 2024). Dies stellt zwar einen bemerkenswerten Wendepunkt dar, da es sich um den ersten Rückgang seit 2008 handelt – dem Jahr, in dem die FIU noch dem Bundeskriminalamt (BKA) unterstand. Im Vergleich zum Vorjahr 2022, in dem 337.186 Meldungen eingingen, zeigt sich eine Abnahme um 4,33 % (FIU 2024, S. 12). In der Gesamtbetrachtung muss jedoch konstatiert werden, dass die aktuellen Zahlen eine Steigerung der Verdachtsmeldungen von 1457,2 % (2013: 20.716) in den vergangenen zehn Jahren darstellen (FIU 2024, S. 12). Die Berichtsperiode verzeichnete darüber hinaus einen deutlichen Anstieg der übermittelten Analyseberichte: Etwa 82.000 wurden an Empfängerbehörden gesendet, was einer Steigerung von 116 % gegenüber dem Vorjahr (38.000) entspricht. Die polizeilich erfassten Geldwäschedelikte erreichten mit 32.600 Fällen einen neuen Höchststand (Zoll 2024). Eine Aufklärungsquote von 90,6 % (PKS 2024) mag ggf. auf den ersten Blick positiv wirken, erklärt sich jedoch durch die Struktur und Prozesse der Kenntniserlangung entsprechender Fälle.

Das Phänomen ist von einer zunehmenden Internationalisierung und Expansion geprägt. Aktuelle Schätzungen beziffern das globale Volumen der Geldwäsche auf eine Spanne von 500 Milliarden bis zu einer Billion US-Dollar (ca. 477 Milliarden Euro bis 953 Milliarden Euro). Die Konsequenzen dieser illegalen Finanzströme sind weitreichend und manifestieren sich in gravierenden Beeinträchtigungen sowohl der globalen Ökonomie als auch der gesellschaftlichen Strukturen (Council of Europe 2023, S. 10).

Diese Zahlen verdeutlichen, dass neue Ermittlungs- und Detektionsmethoden für die Entdeckung verdächtiger Muster im Sachzusammenhang angezeigt scheinen. Der vorliegende Beitrag betrachtet den Einsatz von Künstlicher Intelligenz (KI), insbesondere beim Finanztransaktionsmonitoring bei Kredit- und Finanzinstituten. Das Ziel dieses Beitrags ist es, die Potenziale und Herausforderungen des Einsatzes von KI im Geldwäsche-Transaktionsmonitoring zu untersuchen. Dabei soll insbesondere folgende Frage untersucht werden:

„Inwiefern kann der Einsatz von KI die Effektivität und Effizienz des Geldwäsche-Transaktionsmonitorings steigern und welche Herausforderungen gilt es dabei zu bewältigen?“

Die Beantwortung dieser Forschungsfrage ist von hoher Relevanz, da sie nicht nur für Finanzinstitute und Regulierungsbehörden von Interesse ist, sondern auch weitreichende Implikationen für die gesellschaftliche Sicherheit und die Stabilität des globalen Finanzsystems hat.

Hintergrund

Die Geldwäschebekämpfung unterscheidet sich von konventioneller Strafverfolgung durch ein präventives Meldesystem. „Verpflichtete“ aus dem Finanzsektor sind gesetzlich angehalten, verdächtige Transaktionen an Behörden zu melden. Dieses System ergänzt reaktive und proaktive Ermittlungsmethoden und ermöglicht eine frühzeitige Identifikation potenzieller Geldwäscheaktivitäten (Boberg 2017, S. 46).

Das erste deutsche Geldwäschegesetz (GWG) trat bereits 1991 in Kraft (Quedenfeld 2021, S. 16). Am 30. Mai 2023 verabschiedete der EU-Rat als jüngste Entscheidung zu diesem Komplex ein umfassendes Gesetzespaket zur Bekämpfung von Geldwäsche und Terrorismusfinanzierung. Die neue Verordnung harmonisiert EU-weite Vorschriften, präzisiert Sorgfaltspflichten und stärkt Aufsichtsbehörden. Finanzinstitute und bestimmte Berufsgruppen fungieren in diesem Rahmen als zentrale „Gatekeeper“ (Europäischer Rat 2024).

Zum Stand der Forschung soll an dieser Stelle ein Forschungsprojekt hervorgehoben werden: Das Projekt „MaLeFiz“ (Maschinelles Lernen zur Identifikation auffälliger Finanztransaktionen) zielt darauf ab, die Geldwäschebekämpfung mittels Künstlicher Intelligenz zu optimieren. Zu den Projektpartnern zählen die Deloitte GmbH, die Martin-Luther-Universität Halle-Wittenberg, die Universität Leipzig und das Zentrum Technik und Gesellschaft der TU Berlin. Unter der Leitung des Fraunhofer SIT entwickeln Forscherinnen und Forscher ein KI-basiertes System, das präziser illegale Geldflüsse erkennen und Fehlalarme reduzieren soll. Das Projekt umfasst auch die Erarbeitung von Mindestanforderungen für KI in der Finanzwirtschaft sowie die Gewährleistung der Nachvollziehbarkeit von KI-Entscheidungen. Ein Demonstrator wird unter realen Bedingungen getestet und die Ergebnisse sollen nach Projektabschluss 2025 veröffentlicht werden (Fraunhofer SIT 2023).

Grundlagen der Geldwäsche

Der Begriff der „Geldwäsche“ (engl. „money laundering“) lässt sich historisch auf die Zeit der Prohibition in den Vereinigten Staaten von Amerika zurückführen (1920-1933). Die bekannte Geschichtsgröße Al Capone soll zu dieser Zeit die Notwendigkeit erkannt haben, illegal erworbene Gelder zu „waschen“. Um den unrechtmäßigen Ursprung der hauptsächlich aus dem Betäubungsmittelhandel stammenden Gelder zu verschleiern, vermischte er diese mit legalen Einnahmen aus Münzwaschsalons (engl. „laundromats“) (Diergarten & Barreto Da Rosa 2021, S. 2). Formalrechtlich ist Geldwäsche im Strafgesetzbuch unter Strafe gestellt, hiernach gilt gem. § 261 Abs. 1 StGB:

„Wer einen Gegenstand, der aus einer rechtswidrigen Tat herrührt,

1. verbirgt,
2. in der Absicht, dessen Auffinden, dessen Einziehung oder die Ermittlung von dessen Herkunft zu vereiteln, umtauscht, überträgt oder verbringt,
3. sich oder einem Dritten verschafft oder

4. verwahrt oder für sich oder einen Dritten verwendet, wenn er dessen Herkunft zu dem Zeitpunkt gekannt hat, zu dem er ihn erlangt hat,

wird mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe bestraft (...).“

Über die Jahre wurde die Strafbarkeit des § 261 StGB immer weiter angepasst, sodass eine einfache Definition der Geldwäschebehandlung per se nicht möglich erscheint (Bülte 2017, S. 276-277).

Phasen der Geldwäsche

Personen, die durch illegale Aktivitäten Geld verdienen, stehen vor der Herausforderung, dieses „schmutzige“ Geld so erscheinen zu lassen, als wäre es auf legalem Wege erworben worden. Dieser Prozess wird oft als Drei-Phasen-Modell beschrieben und gliedert sich in eine Platzierungsphase (engl. „Placement“), eine Verschleierungsphase (engl. „Layering“) und eine Integrationsphase (engl. „Integration“) (BKA o. J.). Der erste Schritt der Geldwäsche, das „Placement“, beinhaltet die Umwandlung illegaler Bargeldbestände in Buchgeld oder Sachwerte. Dies geschieht durch Einzahlungen auf Bankkonten oder den Kauf von Vermögenswerten wie Immobilien oder Luxusgütern. Ziel ist es, die illegale Herkunft der Gelder zu verschleiern und sie in den legalen Wirtschaftskreislauf einzubringen (Quedenfeld 2021, S. 4). Die zweite Phase des „Layering“ dient der Verschleierung der Herkunft illegaler Gelder durch ein Netzwerk komplexer Finanztransaktionen, bspw. durch Überweisungen zwischen verschiedenen, unauffälligen Bankkonten oder Briefkastenfirmen. Ziel ist es, die Rückverfolgung der Geldflüsse zu erschweren oder unmöglich zu machen (Quedenfeld 2021, S. 4). Um eine Rückverfolgung zu erschweren, werden verschiedene Methoden eingesetzt, die darauf abzielen, die dokumentarische Spur des Geldes (engl. „Paper Trail“) zwischen den einzelnen Transaktionen zu verwischen (Diergarten & Barreto Da Rosa, 2021, S. 4-5). In der dritten und abschließenden Phase, der „Integration“, werden verschleierte Gelder in den legalen Wirtschaftskreislauf eingeführt. Dies geschieht u. a. durch Investitionen in legale Geschäfte, Immobilien, Luxusgüter sowie durch Geldanlagen und Unternehmensbeteiligungen (Quedenfeld 2021, S. 4). Diese Phase vollendet den Prozess der

Geldwäsche. Zusammenfassend zielen die skizzierten Vorgehensweisen darauf ab, den illegal erworbenen Geldern den Anschein vollständiger Legalität zu verleihen.

Geldwäsche-Transaktionsmonitoring

IT-gestützte Überwachungssysteme in Finanzinstituten nutzen automatisierte Abgleiche mit internationalen Sanktionslisten. Spezialisierte Datenanbieter unterstützen dabei, indem sie aktuelle Informationen sammeln, analysieren und in Datenbanken bereitstellen, um eine effektive Finanztransaktionskontrolle zu ermöglichen (Quendenfeld 2021, S. 147-148).

Das traditionelle Transaktionsüberwachungssystem (TMS) in Banken kategorisiert Fälle als „positiv“ (verdächtig) oder „negativ“ (unverdächtig) und leitet positive Fälle zur manuellen Überprüfung weiter. Trotz regelmäßiger Anpassungen weist dieses System oft mangelnde Flexibilität bei komplexen Geldwäschemustern und hohe Betriebskosten durch umfangreiche manuelle Überprüfungen auf (Andrae 2019, S. 24). TMS von Banken basieren oft auf generischen Risikotypologien und schwellenwertbasierten Regeln, was zu vielen falschen Alarmen führt. Obwohl Above-the-Line- (ATL-) und Below-the-Line- (BTL-) Tests zur Optimierung empfohlen werden, erfolgen diese häufig nicht umfassend, was die Anpassungsfähigkeit des Systems einschränkt (Hirtreiter et al. 2023, S. 4). ATL/BTL Testing ist eine Methode, die von Finanzinstituten verwendet wird, um die Effizienz ihrer TMS zu optimieren. ATL bedeutet die Erhöhung der Parameter über die Grundlinie, um die Schwelle zu identifizieren, an der falsch-positive Ergebnisse zunehmen könnten. BTL meint die Senkung der Parameter unter die Grundlinie, um den Punkt zu ermitteln, an dem das System möglicherweise verdächtige Aktivitäten übersieht (Luttrell 2023). Es dient zusammenfassend dazu, die optimalen Schwellenwerte für Transaktionsüberwachungsregeln zu finden, um ein Gleichgewicht zwischen der Erkennung verdächtigter Aktivitäten und der Minimierung falscher Alarme zu erreichen.

Die rechtliche Basis für das Transaktionsmonitoring zur Geldwäscheprävention in deutschen Finanzinstituten ist im Geldwäschegesetz (GwG) verankert. Gemäß § 51 Absatz 8 Satz 1 GwG konkretisiert die Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) diese Verpflichtung durch Auslegungs- und Anwendungshinweise (AuA) (BaFin 2024a). Die BaFin aktualisiert diese Hinweise regelmäßig, um den sich ändernden Anforderungen im Bereich der Geldwäschebekämpfung gerecht zu werden (BaFin 2024b).

Einführung in die Künstliche Intelligenz (KI)

Im Bereich der Künstlichen Intelligenz (KI) existiert eine große Vielfalt an Definitionen und Verständnisansätzen, die die Komplexität und den multidisziplinären Charakter dieses Forschungsfeldes widerspiegeln. Trotz unterschiedlicher KI-Definitionen besteht ein grundlegender Konsens: KI beschreibt die Entwicklung von Computerprogrammen oder Maschinen, die ein Verhalten zeigen, das bei Menschen als „intelligent“ eingestuft würde (Kaplan 2017, S. 15).

Grundlage des vorliegenden Beitrags ist die aktuelle Definition der Europäischen Union (EU), die im Rahmen des EU Artificial Intelligence (AI) Act (EU-KI-Verordnung) einen Rechtsrahmen eingeführt und somit fundamentale Prinzipien für die Regulierung Künstlicher Intelligenz innerhalb des EU-Gebiets etabliert hat. Das Europäische Parlament strebt hiermit eine technologieneutrale, universelle KI-Definition an, die auch auf künftige KI-Systeme anwendbar sein soll (Europäisches Parlament, 2023).

Gem. Artikel Abs. 1 EU AI Act, welcher am 02.02.2025 in Kraft treten soll, bezeichnet ein

„KI-System‘ ein maschinengestütztes System, das für einen Betrieb mit unterschiedlichem Grad an Autonomie ausgelegt ist und das nach der Einführung Anpassungsfähigkeit aufweisen kann und das für explizite oder implizite Ziele aus den erhaltenen Eingaben ableitet, wie Ausgaben wie Vorhersagen, Inhalte, Empfehlungen oder Entscheidungen zu generieren sind, die physische oder virtuelle Umgebungen beeinflussen können [...]“.

Methodik

Für den vorliegenden Beitrag wurde ein zweistufiger methodischer Ansatz gewählt. Zunächst erfolgte eine umfassende literaturbasierte Analyse, um den aktuellen Forschungsstand zu erfassen und relevante Erkenntnisse zu identifizieren. Im Anschluss daran wurde die SWOT-Analyse als strukturiertes Instrument eingesetzt, um die gewonnenen Erkenntnisse systematisch zu evaluieren.

In der methodischen Herangehensweise dieses Beitrags wurden neben traditionellen Forschungsmethoden auch moderne KI-gestützte Werkzeuge in Form von Software-Lösungen auf der Basis großer Sprachmodelle (u. a. Claude 3.5 Sonnet, GPT-4o) eingesetzt. Diese KI-Tools fungierten als kreative Impulsgeber und Ausgangspunkt für weiterführende Überlegungen in unterstützender Funktion. Die vollständige Verantwortung für den Inhalt, die Argumentation und die gezogenen Schlussfolgerungen liegt beim Autor. Der Einsatz dieser Technologien zielte darauf ab, den Forschungsprozess zu optimieren und neue Blickwinkel zu eröffnen, ohne dabei die wissenschaftliche Integrität und die eigenständige Leistung zu beeinträchtigen.

SWOT-Analyse

Das analytische Werkzeug der SWOT-Analyse ermöglicht eine strukturierte Erfassung und Bewertung wesentlicher Faktoren, die für den Erfolg einer Organisation von Bedeutung sind. Durch die gleichzeitige Betrachtung interner Stärken (Strengths) und Schwächen (Weaknesses) sowie externer Chancen (Opportunities) und Risiken (Threats) liefert die SWOT-Analyse ein ganzheitliches Bild der strategischen Position. Sie dient als Grundlage für fundierte Entscheidungen zur Marktpositionierung und identifiziert Bereiche, in denen Verbesserungspotenziale bestehen, um die Wettbewerbsfähigkeit nachhaltig zu stärken und zukünftige Herausforderungen effektiv zu bewältigen (Schawel & Billing 2018, S. 331; Wollny & Paul 2015, S. 189).

Modifizierte SWOT-Analyse

In diesem Beitrag wird die SWOT-Analyse zur Untersuchung des KIEinsatzes bei der Geldwäschebekämpfung verwendet. Dabei werden interne Stärken und Schwächen der KI-Technologien selbst sowie externe Chancen und Risiken analysiert. Diese Methodik soll ermöglichen, die strategische Position von KI im Kampf gegen Geldwäsche zu analysieren, Potenziale zu identifizieren und Empfehlungen für einen effektiven Einsatz abzuleiten.

Ergebnisse

Im Folgenden werden die zentralen Stärken, Schwächen, Chancen und Risiken dieser innovativen Technologie im Kontext der Finanzbranche beleuchtet. Aufgrund des begrenzten Umfangs dieses Beitrags konzentriert sich die Analyse auf ausgewählte Kernthemen, die aus Sicht des Autors besonders relevant für das aktuelle und zukünftige Potenzial von KI in der Geldwäscheprävention erscheinen.

Stärken (Strengths)

Künstliche Intelligenz besitzt u. a. das Potenzial, die Anomalieerkennung in der Geldwäschebekämpfung zu optimieren. Dies erfolgt durch ihre Fähigkeit, komplexe Muster und verdächtige Transaktionen effektiver zu identifizieren als herkömmliche regelbasierte Systeme (Andrae 2019, S. 24). KI-Algorithmen können enorme Datenmengen verarbeiten und subtile Abweichungen erkennen, die menschlichen Analysten oder starren Regelsystemen möglicherweise entgehen. Durch kontinuierliches Lernen passen sie sich an neue Geldwäskemethoden an und ermöglichen eine proaktive Erkennungsstrategie. Diese verbesserte Fähigkeit erhöht die Identifikationsrate von Geldwäscheaktivitäten, reduziert Fehlalarme und steigert die Effizienz in der Ressourcennutzung, was die Effektivität der Geldwäschebekämpfung insgesamt verbessert (Jurisch 2023). Anders als statische Schwellenwertmodelle, die bei Marktvolatilitäten – beispielsweise während eines Kryptowährungsbooms – zu einer Häufung von Fehlalarmen neigen könnten, passen sich KI-Sys-

teme autonom an veränderte Marktbedingungen an (Schmuck 2023, S. 56). Zusammenfassend ermöglicht Maschinelles Lernen in der Geldwäschebekämpfung eine kontextbasierte Analyse von Transaktionen. Dies führt einerseits zur Reduktion von Fehlalarmen, indem scheinbar auffällige Transaktionen (wie Überweisungen in Hochrisikoländer) im Kontext des Kundenverhaltens bewertet werden. Andererseits verbessert es die Anomalie-Erkennung, indem es geringste Abweichungen identifiziert, die statische Regeln möglicherweise nicht erfassen. So können Transaktionen, die oberflächlich unauffällig erscheinen, im Vergleich zu ähnlichen Kundentypen als abweichend erkannt werden (Schmuck 2023, S. 56). Das Wirtschaftsunternehmen Deloitte implementierte bspw. bei einer asiatischen Bank im Rahmen eines Pilotprojektes ein KI-gestütztes Transaktionsüberwachungssystem als Ergänzung zum bestehenden regelbasierten System. Das neue Modul fokussiert sich auf die Erkennung unbekannter verdächtiger Muster und die Priorisierung von Alarmen. Durch kontinuierliche Hintergrundüberwachung optimierte die KI-Software Regeln und Schwellenwerte, was zu einem Anstieg der „True Positive“-Meldungen um 5 %, einer Reduzierung der „False Positive“-Meldungen um 40 % sowie insgesamt einer Steigerung der operativen Effizienz um 40 % führte (Hirtreiter et al. 2023, S. 11).

Zusammenfassend zeigt sich, dass der Einsatz von KI in der Geldwäschebekämpfung einige Stärken aufweist. KI-gestützte Systeme verbessern die Anomalieerkennung, passen sich an Marktveränderungen an und analysieren Transaktionen kontextbasiert. Ein Pilotprojekt von Deloitte demonstrierte signifikante Verbesserungen: mehr „True Positive“-Meldungen, weniger Fehlalarme und höhere Effizienz. Dies ermöglicht Finanzinstituten potenziell, verdächtige Aktivitäten gezielter zu identifizieren, Ressourcen zu optimieren und die Qualität ihrer Geldwäschebekämpfungsmaßnahmen zu steigern.

Schwächen (Weaknesses)

Eine potenzielle Schwäche des KI-basierten Transaktionsmonitorings beschreibt die Diskussion über den Mangel an Transparenz von KI-Technologien (Financial Stability Board 2017, S. 26). Für die rechtliche Gültigkeit von KI-Analysen müssen IT-Systeme hinsichtlich

der Transparenz bestimmte Kriterien erfüllen. Die Ergebnisse der Algorithmen dürfen hierbei nicht als „Blackbox“ fungieren, sondern müssen klar dargelegt werden, insbesondere hinsichtlich der Frage, warum ein Fall als verdächtig eingestuft wurde. Hierzu reicht es gerade nicht aus, lediglich Verdachtslisten aufgrund der vorliegenden Datenlage zu erstellen. Vielmehr muss die KI detailliert aufzeigen, welche Kriterien und Überlegungen dazu geführt haben, einen bestimmten Fall als verdächtig einzustufen (IDW 2023).

Eine weitere Schwäche stellt die Datenerfassung und -weitergabe dar. Die globale Praxis der Weitergabe von Informationen über verdächtige Transaktionen im Bankensystem ist äußerst limitiert. Banken melden meist nur selbst als verdächtig eingestufte Transaktionen, was zu einem unausgewogenen Datensatz führt. Dies kann beim Training von ML-Modellen zu Überanpassung (engl. „Over-Fitting“) führen, wobei das Modell auf nicht repräsentative Transaktionsmerkmale reagiert. Die begrenzte Datenbasis erschwert die Erkennung echter Risikomuster, was dazu führen kann, dass das ML-Modell nichtexistierende Zusammenhänge „halluziniert“ (Hirtreiter et al. 2024, S. 9).

Chancen (Opportunities)

Wie bereits oben dargestellt, können KI-Systeme potenziell die Effizienz des Monitorings positiv beeinflussen, wodurch sich Möglichkeiten zur sinnvollen Nutzung frei gewordener Ressourcen ableiten lassen. Zur Erreichung dieser Optimierung streben Unternehmen einerseits die Reduktion von False-Positive-Meldungen an, welche betriebswirtschaftliche Ressourcen binden. Andererseits steht die Aufrechterhaltung einer konstanten False-Negative-Rate im Fokus, um potenzielle Verstöße gegen geldwäscherechtliche Vorschriften zu vermeiden (Hauler et al. 2023, S. 12). Dieser Ressourceneinsatz lässt sich insbesondere für Kreditinstitute und Finanzdienstleister in Bezug auf Personal- und Systemkosten präzise identifizieren und quantifizieren. Anhand dieser Gesamtkostenanalyse, welche als Grundlage für die Evaluation potenzieller Effizienzsteigerungen durch Automatisierung von Warnmeldung dient, lassen sich in der Folge valide Ableitungen treffen (Hirtreiter et al. 2023, S. 9). Darüber hinaus ist die Minimierung falsch gemeldeter Verdachtsfälle für

Finanzinstitute aus Gründen der Reputation von erheblicher Bedeutung. Eine initiierte strafrechtliche Verfolgung eines Kunden kann die Geschäftsbeziehung nachhaltig beeinträchtigen. Stellt sich heraus, dass die Ermittlungen bei falschem Verdacht auf systematische Mängel in den Verfahren der Institute zurückzuführen sind, können empfindliche finanzielle Sanktionen drohen (BaFin 2018, S. 89).

Risiken (Threats)

Die Implementierung von Künstlicher Intelligenz (KI) in der Geldwäschebekämpfung bietet zwar signifikante Vorteile und Chancen, ist jedoch auch mit diversen Risiken behaftet. Ein besonderer Fokus liegt hierbei auf den externen Risiken, insbesondere den juristischen und regulatorischen Herausforderungen. Diese Aspekte erfordern eine sorgfältige Betrachtung und Analyse, um die effektive und konforme Nutzung von KI-basierten Systemen in diesem sensiblen Bereich des Finanzsektors zu gewährleisten.

Auf europäischer Ebene könnte in Bezug auf den EU AI Act ein KI-System zum Transaktionsmonitoring als Hochrisikosystem eingestuft werden, wenn es in den Bereich der Strafverfolgung und Finanzdienstleistungen fällt. Dies würde strenge Anforderungen an Transparenz, Robustheit und menschliche Aufsicht mit sich bringen (European Commission 2024). Artikel 6 der EU-KI-Verordnung definiert die Kriterien für die Einstufung von KI-Systemen als Hochrisikosysteme. Gemäß Art. 6 Abs. 1 muss ein KI-System zwei kumulative Bedingungen erfüllen, um als Hochrisikosystem zu gelten: Erstens muss es entweder als Sicherheitskomponente eines Produkts verwendet werden oder selbst ein Produkt darstellen, das unter die in Anhang I aufgeführten Harmonisierungsrechtsvorschriften der Union fällt (lit. a). Zweitens muss für dieses Produkt eine Konformitätsbewertung durch Dritte vorgeschrieben sein (lit. b). Anhang I listet die relevanten EU-Rechtsvorschriften auf, mit denen die KI-Verordnung harmonisiert werden soll. Zusätzlich zu den in Art. 6 Abs. 1 definierten Systemen werden gemäß Art. 6 Abs. 2 auch die in Anhang III aufgeführten KI-Systeme als hochriskant eingestuft. Die EU-Geldwäscherichtlinien sind nicht in Anhang I aufgeführt, weshalb KI-Systeme zur Geldwäschedetektion regelmäßig nicht unter Art. 6 Abs. 1 fallen

dürften. Gemäß Anhang III Absatz (6) der EU-KI-Verordnung werden unterschiedliche Formen der Nutzung von KI-Systemen für die Strafverfolgung geregelt, was eine Prüfung dieser Norm nahelegt. Es ist anzumerken, dass eine detailliertere Prüfung der Einstufung von KI-Systemen zur Geldwäschedetektion nach Anhang III an dieser Stelle aufgrund des umfangreichen Regelwerks nicht möglich ist. Eine solche Analyse würde den Rahmen dieses Beitrags deutlich überschreiten und bedarf einer gesonderten, tiefergehenden Untersuchung.

Die unbeabsichtigte Diskriminierung durch algorithmische Systeme stellt eine weitere, nicht unerhebliche Herausforderung dar. Trotz expliziter Verbote bestimmter Differenzierungsmerkmale können sich KI-Modelle diesen indirekt durch die Analyse korrelierender Faktoren annähern. Um derartige unzulässige Differenzierungen zu verhindern, sind Unternehmen gefordert, umfassende Kontroll- und Transparenzmechanismen zu etablieren. Zudem müssen sie gewährleisten, dass ihre algorithmischen Systeme die rechtlichen Rahmenbedingungen vollumfänglich berücksichtigen und einhalten (BaFin 2018, S. 182). In Bezug auf den Einsatz von KI bei der Geldwäschedetektion könnten sich demnach ähnliche Herausforderungen ergeben. KI-Systeme könnten unbeabsichtigt bestimmte Gruppen oder Individuen aufgrund von Merkmalen wie ethnischer Herkunft, Nationalität oder Wohnort als risikoreicher einstufen. Dies könnte zu unfairen Behandlung oder verstärkter Überwachung bestimmter Kundengruppen führen. Die juristische Auseinandersetzung mit den Auswirkungen von Algorithmen auf Fragen der Gleichbehandlung und Fairness ist ein relativ junges Forschungsfeld (Peters 2023, S. 159), das zunehmend an Bedeutung gewinnt.

Diskussion

Ein zentrales Ergebnis der Analyse ist das erhebliche Potenzial von KI zur Optimierung der Anomalieerkennung in der Geldwäschebekämpfung. Die Fähigkeit von KI-Algorithmen, komplexe Muster zu erkennen und sich an neue Geldwäschemethoden anzupassen, stellt einen signifikanten Fortschritt gegenüber herkömmlichen regelbasierten Systemen dar. Trotz der vielversprechenden Potenziale

zeigen sich auch bedeutende Herausforderungen. Die mangelnde Transparenz von KI-Systemen, oft als „Blackbox“-Problem bezeichnet, stellt eine erhebliche Hürde für die rechtliche Gültigkeit von KI-Analysen dar (Financial Stability Board 2017, S. 26). Die Notwendigkeit, die Entscheidungsprozesse der KI nachvollziehbar zu machen, wie vom IDW (2023) betont, ist ein kritischer Aspekt, der bei der Implementierung solcher Systeme berücksichtigt werden muss.

Zudem wirft die begrenzte globale Praxis der Informationsweitergabe über verdächtige Transaktionen im Bankensystem Fragen zur Datenqualität auf. Die daraus resultierende Gefahr des „Over-Fitting“ bei ML-Modellen (Hirtreiter et al. 2024, S. 9) verdeutlicht die Notwendigkeit einer verbesserten internationalen Zusammenarbeit und Datenaustauschpraxis. Ziel des Beitrags war es auch, mit der Analyse einen umfassenderen Blick auf die Implementierung von KI in der Geldwäschebekämpfung zu erhalten. Während viele Untersuchungen sich auf technische Aspekte konzentrieren, berücksichtigt dieser Beitrag auch rechtliche und ethische Dimensionen, insbesondere im Kontext der EU-KI-Verordnung und der Problematik algorithmischer Diskriminierung.

Gleichwohl weist die Analyse mehrere bedeutende Einschränkungen auf. Ein zentrales Problem ist die begrenzte Verfügbarkeit empirischer Daten zur langfristigen Wirksamkeit von KI-Systemen in der Geldwäschebekämpfung. Obwohl das Pilotprojekt von Deloitte wertvolle Einblicke liefert, kann es nicht als repräsentativ für den gesamten Finanzsektor betrachtet werden. Zudem fehlt eine detaillierte juristische Analyse der Einstufung von KI-Systemen zur Geldwäschedetektion nach der EU-KI-Verordnung, was für ein umfassendes Verständnis der regulatorischen Implikationen notwendig wäre. Die Diskussion der algorithmischen Diskriminierung basiert hauptsächlich auf theoretischen Überlegungen, da konkrete Fallstudien in diesem Bereich kaum existieren. Aufgrund des umfang- und facettenreichen Themas der Künstlichen Intelligenz in der Geldwäschebekämpfung konnte die Analyse nur sehr ausgewählte Bereiche und einzelne Aspekte betrachten. Viele der diskutierten Potenziale und Risiken basieren auf theoretischen Modellen oder begrenzten Pilotprojekten, was die Notwendigkeit von Langzeitstudien zur Wirk-

samkeit und den Auswirkungen von KI-Systemen in der Praxis unterstreicht. Schließlich erfordert die sich ständig weiterentwickelnde Regulierungslandschaft, insbesondere im Kontext der EU-KI-Verordnung, eine kontinuierliche Neubewertung der rechtlichen Implikationen, was über den Rahmen dieses Beitrages hinausgeht.

Schlussfolgerungen

Die vorliegende Analyse des Einsatzes von Künstlicher Intelligenz (KI) in der Geldwäschebekämpfung offenbart ein vielschichtiges Bild mit weitreichenden Implikationen für die Finanzbranche. Die Untersuchung zeigt deutlich, dass KI-Systeme sowohl erhebliche Chancen als auch bedeutende Herausforderungen mit sich bringen, die sorgfältig gegeneinander abgewogen werden müssen. Die sich entwickelnde regulatorische Landschaft, insbesondere im Kontext der EU-KI-Verordnung, wird die Implementierung von KI-Systemen im Sachzusammenhang maßgeblich beeinflussen. Es ist von entscheidender Bedeutung, dass Finanzinstitute, Technologieentwickler und Regulatorsbehörden die rechtlichen Rahmenbedingungen genau beobachten und ihre Systeme entsprechend anpassen. Die mögliche Einstufung von KI-Systemen zur Geldwäschedetektion als Hochrisikosysteme gemäß der EU-KI-Verordnung könnte weitreichende Konsequenzen für deren Entwicklung und Einsatz haben.

Darüber hinaus sollte die Entwicklung von Methoden zur Erkennung und Vermeidung unbeabsichtigter Diskriminierung ein zentraler Fokus zukünftiger Forschung und Entwicklung sein. Daneben besteht ein dringender Bedarf an Methoden, die die Entscheidungsprozesse von KI-Systemen transparent und nachvollziehbar machen. Dies erscheint nicht nur aus regulatorischer Sicht wichtig, sondern auch, um das Vertrauen in diese Technologien zu stärken. Ferner könnten umfassende empirische Studien zur langfristigen Wirksamkeit und zu den Auswirkungen von KI-Systemen in der Praxis der Geldwäschebekämpfung erforderlich sein. Diese sollten sowohl die technische Leistungsfähigkeit als auch die organisatorischen und gesellschaftlichen Auswirkungen berücksichtigen. Ein weiterer sich

aufdrängender Forschungskomplex ist die Entwicklung von Methoden und Rahmenwerken für einen verbesserten internationalen Datenaustausch bei gleichzeitiger Wahrung des Datenschutzes.

Dieser Beitrag trägt zur aktuellen Diskussion bei, indem er einen interdisziplinären Überblick über verschiedene Aspekte des KI-Einsatzes in der Geldwäschebekämpfung bietet. Er legt eine Grundlage für weiterführende, tiefere Forschungen, die notwendig sind, um die komplexen Wechselwirkungen zwischen Technologie, Recht und Ethik in diesem Bereich vollständig zu erfassen und zu verstehen. Die Zukunft der Geldwäschebekämpfung wird voraussichtlich stark von KI-Technologien geprägt sein. Es liegt an Forschenden, Personen aus der Praxis und Regulierungsbehörden, gemeinsam daran zu arbeiten, das volle Potenzial dieser Technologien zu realisieren und gleichzeitig die damit verbundenen Risiken zu minimieren. Nur durch eine ausgewogene, verantwortungsvolle und vorausschauende Herangehensweise kann sichergestellt werden, dass KI zu einem effektiven und ethisch vertretbaren Werkzeug in der Bekämpfung von Finanzkriminalität wird.

Literaturverzeichnis

Andrae S (2019): Geldwäsche und Maschinelles Lernen – ein Strukturierungsrahmen. *bank und markt*, 02/2019; 73-77

BaFin (2018) Studie: Big Data trifft auf künstliche Intelligenz. [bafin.de/SharedDocs/Downloads/DE/dl_bdai_studie.html](https://www.bafin.de/SharedDocs/Downloads/DE/dl_bdai_studie.html) (19.12.2024)

BaFin (2024a) Geldwäschegesetz: BaFin aktualisiert Auslegungs- und Anwendungshinweise. [bafin.de/SharedDocs/Veroeffentlichungen/DE/Meldung/2024/meldung_24_11_29_GW_Aenderung_AuA.html](https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Meldung/2024/meldung_24_11_29_GW_Aenderung_AuA.html) (19.12.2024)

BaFin (2024b) Geldwäschegesetz: BaFin wird Auslegungs- und Anwendungshinweise aktualisieren. [bafin.de/SharedDocs/Veroeffentlichungen/DE/Meldung/2024/meldung_2024_07_09_Konsultation_06_2024.html](https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Meldung/2024/meldung_2024_07_09_Konsultation_06_2024.html) (19.12.2024)

Boberg M (2017): Geldwäsche und Organisierte Kriminalität – Eine kriminologische Untersuchung unter besonderer Berücksichtigung der polizeilichen Erledigungspraxis. Boorberg, Stuttgart München Hannover Berlin Weimar Dresden

Bülte J (2017): Zu den Gefahren der Geldwäschebekämpfung für Unternehmen, die Rechtstaatlichkeit und die Effektivität der Strafverfolgung. *NZWiSt* 2017. 276-288

BKA (Bundeskriminalamt) (o. J.) Geldwäsche. [bka.de/DE/UnserAufgaben/Deliktsbereiche/Geldwaesche/geldwaesche_node.html](https://www.bka.de/DE/UnserAufgaben/Deliktsbereiche/Geldwaesche/geldwaesche_node.html) (19.12.2024)

Council of Europe (2023) Committee of Experts on the Evaluation of Anti-money Laundering Measures and the Financing of Terrorism (MONEYVAL) – Annual Report 2022. rm.coe.int/moneyval-annual-report-2022-%0Aweb-a4/1680abe10a (19.12.2024)

Diergarten A, Barreto da Rosa S (2021): *Praxiswissen Geldwäsche Prävention*. 2. Auflage. De Gruyter, Berlin

Europäischer Rat (2024) Bekämpfung von Geldwäsche und Terrorismusfinanzierung in der EU. consilium.europa.eu/de/policies/against-terrorism/against-terrorist-financing/ (19.12.2024)

Europäisches Parlament (2023) KI-Gesetz: erste Regulierung der künstlichen Intelligenz. europarl.europa.eu/topics/de/article/20230601STO93804/ki-gesetz-erste-regulierung-der-kuenstlichen-intelligenz (19.12.2024)

European Commission (2024) AI Act. digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai (19.12.2024)

Financial Stability Board (2017) Artificial intelligence and machine learning in financial services – Market developments and financial stability implications. fsb.org/uploads/P011117.pdf (19.12.2024)

FIU (2023): Jahresbericht 2023. https://www.zoll.de/DE/FIU/Fachliche-Informationen/Jahresberichte/jahresberichte_node.html (19.12.2024)

Fraunhofer SIT (2023) KI gegen Geldwäsche. sit.fraunhofer.de/de/presse/details/news-article/show/ki-gegen-geldwaesche/ (19.12.2024)

Hauler T, Höffler K, Reisch K (2023): „Im Zweifel“, aber nicht „ins Blaue hinein“ Die strafrechtliche Dimension der geldwäscherechtlichen Verdachtspflicht. *wistra* 2023; 265-271

Hirtreiter M, Koller J, Uspelkat J (2023): Künstliche Intelligenz in der Geldwäschebekämpfung. deloitte.com/content/dam/assets-zone2/de/de/docs/services/financial-advisory/2024/Deloitte-K%C3%BCnstliche-Intelligenz-Geldwaeschebekaempfung.pdf (19.12.2024)

Hirtreiter M, Schmuck R, Uspelkat J, Bohm T, Rodin I (2024) Optimizing rule-based transaction monitoring systems. deloitte.com/content/dam/assets-zone2/de/de/docs/services/financial-advisory/2024/Deloitte-Optimizing-rule-based-transaction-monitoring-systems.pdf (19.12.2024)

Jurisch T (2023) Einen Schritt voraus: Wie KI im Kampf gegen Geldwäsche helfen kann. klardenker.kpmg.de/financialservices-hub/einen-schritt-voraus-wie-ki-im-kampf-gegen-geldwaesche-helfen-kann/ (19.12.2024)

Kaplan J (2017): Künstliche Intelligenz – Eine Einführung. mitp, Frechen

Luttrell T (2023) Optimizing your AML program with above-the-line/below-the-line testing. abrigo.com/blog/optimizing-your-aml-program-with-above-the-line-below-the-line-testing/ (19.12.2024)

IDW (Nachrichten Informationsdienst Wissenschaft) (2023) KI gegen Geldwäsche. nachrichten.idw-online.de/2023/05/08/ki-gegen-geldwaesche/ (19.12.2024)

Peters A (2023): Smarte Verdachtsgewinnung: Eine strafprozessuale und verfassungsrechtliche Untersuchung der Verdachtsgewinnung mittels künstlicher Intelligenz. Nomos Verlagsgesellschaft, Baden-Baden

PKS (Polizeiliche Kriminalstatistik) (2024): Bund – Falltabellen, T01 Grundtabelle – Fälle (V1.0). bka.de/DE/AktuelleInformationen/StatistikenLagebilder/PolizeilicheKriminalstatistik/PKS2023/PKS-Tabellen/BundFalltabellen/bundfalltabellen.html?nn=226082 (19.12.2024)

Quedenfeld R (2021): Handbuch Bekämpfung der Geldwäsche und Wirtschaftskriminalität, 5. Auflage. Erich Schmidt Verlag, Berlin

Schawel C, Billing F (2018): Top 100 Management Tools: Das wichtigste Buch eines Managers. Von ABC-Analyse bis Zielvereinbarung: Springer Fachmedien Wiesbaden GmbH.

Schmuck R (2023): Künstliche Intelligenz im Geldwäsche-Transaktionsmonitoring. ZRFC Risk, Fraud & Compliance, 2/23; 55-60

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

Zoll (2024) Die Financial Intelligence Unit veröffentlicht ihren Jahresbericht 2023. zoll.de/DE/FIU/Aktuelles-FIU-Meldungen/2024/fiu_jahresbericht_2023.html (19.12.2024)

Drohngestützte Wide-Area Surveillance-Systeme als Zukunftstechnik für die deutsche Polizei – Eine SWOT-Analyse

Marvin Mayer

In den letzten Jahren haben technologische Entwicklungen den Einsatz von Drohnen erheblich vorangetrieben. Früher wurden für die militärische Luftaufklärung vor allem Flugzeuge und Hubschrauber genutzt, heute ermöglichen drohngestützte Technologien einerseits die Durchführung zahlreicher militärischer Operationen, andererseits eröffnen sie aber auch neue Anwendungsbereiche im polizeilichen Kontext, wie beispielsweise unbemannte Überwachungsmissionen, Such- und Rettungseinsätze (Shahzad und Gupta 2020, S. 289), Verhaltensanalyse von Fußgängern (Irizarry et al. 2012, S. 194) sowie Untersuchung von Verkehrsunfällen (Ma et al. 2016, S. 1).

Eine vielversprechende Innovation stellen dabei drohngestützte Wide-Area Surveillance-Systeme (WAS-Systeme) dar. Diese ermöglichen Strafverfolgungsbehörden, großflächige Gebiete effizient in Echtzeit zu überwachen und kriminelle Aktivitäten frühzeitig zu erkennen (Marion 2017; Logos Technologies 2021). Die Bedeutung dieser Technologie zeigt sich nicht nur in ihrer Fähigkeit, umfangreiche Überwachungsaufgaben schnell und diskret zu erfüllen, sondern auch in ihrer Kosteneffizienz (Royo et al. 2022, S. 1).

In diesem Beitrag werden diese drohngestützten WAS-Systeme als potenzielle Zukunftstechnologie für die deutsche Polizei im Rahmen einer SWOT-Analyse (Stärken, Schwächen, Chancen und Risiken) untersucht und die gewonnenen Erkenntnisse diskutiert. Im Fokus steht die Frage, inwieweit diese Technologie die polizeiliche Effizienz und Aufgabenerfüllung verbessern kann, sowie die Analyse der damit einhergehenden Herausforderungen und Risiken. Dazu befasst sich der Beitrag zunächst mit dem thematischen Hintergrund, den grundlegenden Begriffen und einer Einführung in das Thema. Anschließend werden die SWOT-Analyse beschrieben, die Methodik

angewandt und die Ergebnisse präsentiert. Darauf aufbauend folgt eine Diskussion der Ergebnisse, bevor abschließend Schlussfolgerungen gezogen werden.

Hintergrund

Folgend wird zur fundierten Einführung in die Thematik der thematische Hintergrund sowie die grundlegenden Begriffe näher erläutert.

Drohnen

Der Begriff der Drohne ist nicht einheitlich definiert. Gebräuchlich sind Begriffe wie Unbemannte Luftfahrzeuge, englisch Unmanned Aerial Vehicle (UAV), oder Unmanned Aircraft (UA). Für nicht autonom fliegende Drohnen ist die Abkürzung RPA (Remotely Piloted Aircraft) gängig. Die internationale Zivilluftfahrt-Organisation (ICAO) und das deutsche Luftfahrt-Bundesamt sprechen von Unmanned Aircraft System, kurz UAS (International Civil Aviation Organization 2011, S. 9; Luftfahrt-Bundesamt 2023). Neben den Begrifflichkeiten wird zwischen den Erscheinungsformen unterschieden in Flächenflugzeuge, Helikopterdrohnen und Multikopterdrohnen (Christen et al. 2018b, S. 50). Vom Einsatzgebiet werden Drohnen international bei sog. ISR-Einsätzen (engl. Intelligence, Surveillance, Reconnaissance), bei bewaffneten Kampfeinsätzen, zur nichtmilitärischen Sicherheitsarbeit, aber auch für vielfältige andere zivile Zwecke eingesetzt (Malone et al. 2013, S. 1).

Wide-Area Surveillance

Der englische Begriff Wide-Area Surveillance (WAS) bedeutet großflächige Überwachung und ist ein Ansatz, bei dem spezielle Wide-Area Motion Imagery-Systeme (WAMI-Systeme) eingesetzt werden. Diese kombinieren leistungsfähige Kamertechnologie mit spezieller Analysesoftware. Sie zeichnen sich insbesondere durch ihre Reichweite aus, die es ermöglicht, Gebiete mit einem Durchmesser von mehreren Kilometern zu erfassen. Das erste WAMI-System, Constant Hawk, war 680 Kilogramm schwer, in Flugzeugen verbaut

und wurde 2006 im Irak-Krieg eingesetzt (Logos Technologies 2021). 2011 montierte die US-Armee das weiterentwickelte System Kestrel an Aerostaten, um durch eine großflächige und langfristige Überwachung vorgeschobene Operationsbasen in Afghanistan zu schützen (Marion 2017). Die aktuellen Systeme können an einer Vielzahl von Plattformen montiert werden, einschließlich unbemannter Drohnen (Logos Technologies 2021). Mithilfe eines drohnengestützten WAMI-Systems ist es möglich, hunderte von sich bewegenden Objekten zu detektieren und gleichzeitig zu verfolgen (Reilly et al. 2010, S. 186-199). Während einer laufenden Observation aus der Luft können die aufgezeichneten Bilder auch forensisch rückwärts ausgewertet werden, um Wege zurückzuverfolgen (Logos Technologies 2021). Dabei sind eine Schlüsselkomponente der Systeme die integrierten geografischen Informations- und Analysesysteme (GIS). Durch die Kombination verschiedener Geodatensätze können komplexe räumliche Analysen durchgeführt und Zusammenhänge zwischen Kriminalitätsphänomenen und Umgebungsfaktoren aufgedeckt werden (Hartwig, 2001, S. 435-439).

Das System WASP des israelischen Luft- und Raumfahrtkonzern IAI ist mit Tag- und Nacht-WAMI-Sensoren ausgestattet, misst 27x33x22 cm und wiegt sechs Kilogramm. Es verfügt über ein integriertes Navigationssystem, das jeden einzelnen Pixel georeferenziert, und kann an Drohnen wie dem UAV-Hebron oder UAV-BirdEye 650D installiert werden (Israel Aerospace Industries 2023). Die jüngsten Kriegserfahrungen in Europa zeigen, welche wichtige Rolle solche Aufklärungsergebnisse in Echtzeit spielen. Die Bundeswehr hat deswegen dreizehn Drohnensysteme LUNA bei der Fa. Rheinmetall in Auftrag gegeben (Hoffmann 2023; Rheinmetall AG 2023). In diese neuartigen Systeme sind zunehmend Technologien der Künstlichen Intelligenz (KI) integriert. Bei der verschmelzenden Anwendung von KI und der geografischen Datenverarbeitung spricht man von GeoAI (engl. Geospatial Artificial Intelligence). Dies ist entscheidend für die Analyse, Verbindung und Bewertung der räumlichen Daten, die bei einer großflächigen Überwachung erzeugt werden (Chauhan und Shekhar 2021, S. 355-370). Der stellvertretende NATO-Generalsekretär für Nachrichtendienste und Sicherheit betonte im Mai 2024, dass GeoAI die Aufklärung der NATO revolutionieren wird (Brandi 2024).

Polizeiliche Entwicklungen und Implikationen

Länder wie Israel, Japan und Südkorea setzten bereits 2010 UAVs für nichtmilitärische Zwecke ein (Haddal und Gertler 2010, S. 7). Ein Forschungsprojekt der EU-Grenzschutzagentur FRONTEX entwickelte Border Security Unmanned Aerial Vehicles (BSUAV) zur Kontrolle der Außengrenzen sowie zur Terrorismusbekämpfung (Hayes et al. 2014, S. 28). Das EU-Projekt INDECT erforschte, wie Personen mit auffälligem Verhalten autonom von Drohnen überwacht werden können (Marques 2014, S. 5-9, 22). In der US-amerikanischen Stadt Baltimore kommen seit 2015 WAS-Systeme zur großflächigen Überwachung und Unterstützung der polizeilichen Ermittlungsarbeit zum Einsatz (Gaissert 2017; Powers 2017). 2016 montierten brasilianische Sicherheitsbehörden ein WAMI-System an einen Aerostaten und setzten es anlässlich der Olympischen Sommerspiele in Rio de Janeiro ein. Es flog während der Spiele statisch in der Luft und überwachte die komplette Stadt (Griffin 2016). Eine spanische Studie demonstrierte die Effektivität von Drohnen bei der Überwachung großer Menschenmengen, wie bei Sportereignissen und Festivals (Royo et al. 2022, S. 1-2). 2022 beauftragte das Bundesministerium für Digitales und Verkehr ein Projekt, dessen Ziel es ist, UAS-Sensorik für automatisierte Monitoring-Ansätze zu ertüchtigen und bspw. bei Massenkarambolagen mit Verletzten oder der Überwachung kritischer Infrastrukturen einzusetzen (Bundesministerium für Digitales und Verkehr 2020). Die Europäische Kommission legte im gleichen Jahr ihre Drohnenstrategie 2.0 vor, um bis 2030 umfangreiche nichtmilitärische Drohnendienste im Inland zu implementieren (Europäische Kommission 2022, S. 1-4, 23-24). 2023 beschloss Frankreich als erstes Land in der EU ein Gesetz zum Einsatz KI-basierter Überwachungssysteme. Die französische Polizei setzte diese Systeme darauffolgend erstmals in Paris anlässlich der Olympischen Spiele 2024 ein (Blaschke 2024).

Methodik

In diesem Beitrag wird anhand der SWOT-Analyse der Einsatz drohnengestützter WAS-Systeme als Zukunftstechnik für die deutsche Polizei bewertet. SWOT ist ein Akronym für Strengths (Stärken), Wea-

knesses (Schwächen), Opportunities (Chancen) und Threats (Bedrohungen/Risiken) (Künzli 2012, S. 126) und ist eine bewährte Methode zur Ordnung und Zusammenfassung der wesentlichen Stärken, Schwächen, Chancen und Risiken. Sie wird als Grundlage zur Strategieentwicklung oder direkt zur Ableitung von Zielen und Handlungsempfehlungen verwendet, indem sie die intern und extern relevanten Faktoren analysiert (Schawel und Billing 2018, S. 331-333; Kaufmann 2021, S. 289-293). Als Quellen wurden Artikel über Google Scholar und aus Katalogen sowie Datenbanken von Hochschulbibliotheken abgerufen, Querverweise aus diesen Artikeln eingeholt und Recherchen in Open-Source-Quellen durchgeführt.

Ergebnisse

Nachfolgend werden die Stärken und Schwächen von drohnengestützten WAS-Systemen aufgezeigt und die Chancen und Risiken untersucht, um darauf aufbauend drohnengestützte WAS-Systeme als mögliche Zukunftstechnik für die deutsche Polizei zu diskutieren und zu bewerten sowie Handlungsempfehlungen ableiten zu können.

Stärken (Strengths)

Die spezifischen Vorteile von WAS-Systemen gegenüber herkömmlichen Überwachungsmethoden sind eine großflächige Abdeckung, die Effizienzsteigerung, die Echtzeitmöglichkeiten, die schnelle Reaktionszeit bei Vorfällen, der flexible Einsatz in verschiedenen Szenarien, die Fähigkeit zur Objektverfolgung und forensischen Rückverfolgung sowie die Kosteneffizienz.

Eine bedeutende Stärke ist die Möglichkeit, große Flächen effizient zu überwachen. Das WASP-System kann in einer Flughöhe von ca. 1800 m 2 km² und in ca. 6100 m Höhe 20 km² Fläche gleichzeitig und in Echtzeit überwachen (Israel Aerospace Industries 2023). Dies übersteigt die Möglichkeiten herkömmlicher bodengebundener Überwachungskameras um ein Vielfaches. Das an einem UAV befestigte WASP-System kann die überflogene Landschaft und jeden, der sich durch diese bewegt, in Echtzeit charakterisieren. Die Sensorik erkennt

spektrale Signaturen, der WAMI verfolgt die Bewegung und zoomt auf die Ziele (Logos Technologies 2021, S. 5). Ein einzelnes WAMI-Gerät ist in der Lage, gleichzeitig mehrere Nutzer am Boden zu unterstützen, sodass jeder einen anderen Video-Feed aus dem großen Sichtfeld des Sensors streamen kann (Marion 2017). Diese Flexibilität ermöglicht den Einsatz in einer Vielzahl von gleichzeitigen Szenarien. Bereits 2022 setzte FRONTEx unbemannte Flugzeuge ein, um Griechenland bei der Grenzkontrolle zu unterstützen (FRONTEx 2022). Darüber hinaus können die UAV zum Schutz von Polizeikräften, dem Schutz von polizeilichen Liegenschaften oder gefährdeter Infrastruktur, zur Routenaufklärung, Terrorismusbekämpfung und Veranstaltungssicherheit eingesetzt werden (Logos Technologies 2018, S. 1-6; Christen et al. 2018b, S. 14, 70, 208-210). Auch wäre der Einsatz zur Katastrophenhilfe, zur Analyse von Verkehrsmustern, zur Strafverfolgung (Persistent Surveillance Systems 2018), zur verdeckten Observation (Buckler 2019, S. 23) oder zum Erkennen von Schleuser- und illegalen Migrationsströmen denkbar (Marion 2017). Durch die Integration von Edge-Computing-Technik kann zudem eine hochautomatisierte und skalierbare Objekterkennung und -verfolgung in Echtzeit erfolgen (Alam und Gupta 2020, S. 289-290, 301-302). Edge Computing verlagert dabei die Datenverarbeitung vom eigentlichen Gerät oder zentralen Rechenzentren auf lokale Geräte am Rand des Netzwerks. Dadurch sinken Latenzzeiten, der Bandbreitenbedarf wird reduziert und Echtzeit-Entscheidungen werden möglich. Alam und Gupta haben in ihrem Experiment dazu einen zusätzlichen Raspberry Pi 3 in die Drohne integriert (Alam und Gupta 2020, S. 295). Verzahnt man diese Daten zusätzlich mit GIS und GeoAI, können die detektierten Objekte präzise verortet und mit räumlichen Daten in Bezug gesetzt werden (Chauhan und Shekhar 2021).

Eine weitere Stärke ist die Wirtschaftlichkeit, da solche Systeme günstiger in der Anschaffung und im Betrieb sind als herkömmliche Helikopter oder bemannte Flugzeuge (Tikanmäki und Tuohimaa 2011, S. 89 ff.; Malone et al. 2013; Bolkcom 2005, S. 3-4) und Einsätze dadurch kostengünstiger durchgeführt werden können (Magrassi 2016, S. 36 ff.). Das UAV Thunder-B, ein Starrflügler-Drohnen-System, das von der griechischen Polizei eingesetzt wird, kostet in der Anschaffung rund 200.000 €, wobei Kamera- und Software-Kosten

inkludiert sind. Die jährlichen Servicekosten werden auf 5000 € geschätzt. Die Kosten für zwei Stunden ständiger Überwachung betragen in einer Untersuchung 100,55 € je Flugstunde (Tsiamis et al. 2023, S. 6, 9). Das Bundesland Nordrhein-Westfalen (NRW) hat dagegen im Jahr 2017 für sechs Helikopter einen Anschaffungspreis von 65.000.000 € veranschlagt, das sind rund 10.830.000 € pro Stück (RP Online 2016). Das hessische Innenministerium hat des Weiteren veröffentlicht, dass ihre Polizeihelikopter vom Typ Eurocopter 145, 1.297,13 € je Flugstunde kosten (ohne Personalkosten) (Franco 2019). Die vergleichsweise geringen Kosten der UAV könnten dazu weiter gesenkt werden, wenn die umfangreichen Rechenleistungen an Bord des UAV begrenzt und in eine Cloud verlagert werden (Shahzad und Gupta 2020, S. 289).

Als weitere Stärke ist die längere Flugdauer anzubringen. Das UAV-System Predator B kann schweben und dadurch mehr als dreißig Stunden am Stück in der Luft operieren, ohne aufzutanken zu müssen (Bolkcom 2005, S. 3-4). Der in NRW eingesetzte Polizeihelikopter vom Typ Airbus H 145 fliegt dagegen nur maximal drei Stunden am Stück (Heeren 2016). Diese längere Flugzeit und die dadurch durchgängige Abdeckung des Zielgebiets stellt einen wichtigen operativen Vorteil gegenüber bemannten Flugzeugen oder Helikoptern dar (Bolkcom 2005, S. 3-4).

Schwächen (Weaknesses)

Der Einsatz von drohnengestützten WAS-Systemen unterliegt einigen Einschränkungen bzw. potenziellen Schwächen, beispielsweise durch technische Limitierungen. Schlechte Wetterbedingungen wie starker Wind, Regen oder extreme Temperaturen können den Einsatz von Drohnen einschränken und reduzieren die Flexibilität und Einsatzbereitschaft der Technologien (Haddal und Gertler 2010, S. 4). Dazu gab es in den letzten Jahren regelmäßig Beinahe-Kollisionen von Flugzeugen mit Drohnen (Christen et al. 2018b, S. 119), da Drohnen für andere Luftfahrzeuge visuell nur schwer erkennbar sind und nicht über ein „Detect and Avoid“-System verfügen (Haddal und Gertler 2010, S. 5). Weitere Faktoren sind mögliche Systemausfälle, Kommunikationsfehler oder menschliche Fehler, die zu

Abstürzen führen können (Christen et al. 2018b, S. 51 ff.). Derzeit gibt es jedoch keine valide Datengrundlage zur genauen Anzahl von Drohnenabstürzen. Nur im militärischen Bereich liegen Daten vor. Laut veröffentlichten Vergleichsdaten zu sogenannten Mishaps (Verlust von Flugzeugen oder Drohnen pro 100.000 Flugstunden) ist festzustellen, dass das Risiko zu verunglücken bei UAVs exorbitant höher liegt als bei bemannten Flugzeugen. Beispielsweise sind pro 100.000 Flugstunden 32 Predator-Drohnen, 334 Pioneer-Drohnen und 55 Hunter-Drohnen ausgefallen, dagegen aber nur drei F-16-Kampfflugzeuge, 0,1 Regionalflugzeuge und 0,01 Großraumflugzeuge (Christen et al. 2018b, S. 120-121).

Chancen (Opportunities)

Das System bietet die Chance, die öffentliche Sicherheit zu erhöhen (Li und Hsu 2022, S. 1). Eine Möglichkeit ist die Implementierung von Predictive-Policing-Algorithmen, um Probleme frühzeitig zu detektieren und zu bekämpfen (Bone-Winkel 2020, S. 73). In ländlichen und schwer zugänglichen Gebieten sind die Drohnen zudem schneller am Einsatzort (Laksham 2019, S. 343 ff.). Bei zivilen Großveranstaltungen tragen sie zu einer effizienteren Koordination und einem verbesserten Sicherheitsmanagement bei: Menschenmassen können aus der Luft beobachtet werden, auffällige Aktivitäten wie beispielsweise Anomalien in Besucherströmen detektiert und reaktive Maßnahmen eingeleitet werden (Choi und Savarese 2014, S. 71-91). Kritische Situationen können autonom aus der Luft erfasst, als sicherheitsrelevant eingestuft und zur Validierung automatisch mit verfügbaren Videodaten bodengebundener Überwachungskameras abgeglichen werden (Chiappino et al. 2014). Die Technologie bietet zudem Vorteile bei der Unterstützung von zivilen Such- und Rettungseinsätzen. Große Gebiete können schnell und effizient abgesucht werden. Verbaute Thermalkameras ermöglichen es, selbst bei schlechter Sicht, Personen aufzufinden (Ayamga et al. 2021, S. 2; Laksham 2019, S. 343, 344). Dies belegt auch eine Untersuchung von Eftychidis et al. (2018). Durch interdisziplinäre Kooperationen und Zusammenarbeit mit anderen Behörden kann die Polizei ihre Systeme des Weiteren zur Unterstützung bei Search and Rescue-Opera-

tionen auf offener See (Maritime Rescue Coordination Centre 2024) einsetzen und Personen oder Boote im Wasser lokalisieren (Laksham 2019, S. 344; SearchWing 2023).

Risiken (Threats)

Mögliche Sicherheitslücken in den technischen Systemen können von Angreifern ausgenutzt und gehackt werden, um das UAV als Waffe einzusetzen (Laksham 2019, S. 345) oder gezielt zum Ausspionieren von Menschen zu missbrauchen (Scott und Scott 2017, S. 2). Die aufgenommenen Daten können abgefangen, mitgelesen oder verändert werden (Weichert 2012, S. 3-4). Ein weiteres Risiko besteht in der Akzeptanz und somit im Vertrauen der Bevölkerung. Eine Befragung dazu zeigte, dass australische Bürgerinnen und Bürger Drohnentechnologie für nicht übermäßig unsicher, riskant, vorteilhaft oder bedrohlich hielten, jedoch Bedenken hinsichtlich der Privatsphäre und möglicher Missbrauchsfälle haben (Clothier et al. 2015, S. 3). Bei einer deutschen Befragung im Jahr 2018 äußerten 84 % der Befragten, bezüglich einer möglichen Verletzung ihrer Privatsphäre durch Drohnen besorgt zu sein, was für eine eher ablehnende Haltung in der eigenen Bevölkerung spricht (Deutsches Zentrum für Luft- und Raumfahrt, 2018). Zum polizeilichen Drohneneinsatz zeigt eine Studie, dass 60 % der Bevölkerung grundsätzlich den Einsatz und somit eine gewisse Form der Überwachung akzeptiert, jedoch bei persönlicher Betroffenheit die Akzeptanz auf 43 % sinkt. Dagegen geben 97 % der Befragten an, dem Drohneneinsatz im Rahmen des Katastrophenschutzes positiv gegenüberzustehen (Vogt 2017, S. 22).

Der Einsatz von drohnengestützten WAS-Systemen wirft zudem rechtliche Fragen im Zusammenhang mit der Nutzung des Luftraumes, dem Schutz der Grundrechte und der Wahrung der Privatsphäre auf (Buckler 2019, S. 1-10). Das Bundesverfassungsgericht hat 1983 im Rahmen des Volkszählungsurteils festgestellt, dass es angesichts der modernen Datenverarbeitung keine per se rechtlich belanglosen Daten gibt (BVerfG, Urteil vom 15.12.1983 – 1 BvR 209/83). Die umfangreiche Erfassung und Speicherung von Daten tangiert somit die Wahrung der Privatsphäre von unzähligen, sich im Überwachungsgebiet bewegendem Bürgerinnen und Bürgern (Christen et al. 2018a, S. 25;

Christen et al. 2018b, S. 158 ff.). Nach ersten rechtlichen Überlegungen scheinen deshalb für den polizeilichen Drohneneinsatz die gleichen Anforderungen einschlägig zu sein wie für den herkömmlichen Einsatz von polizeilichen Helikoptern (Buckler 2019, S. 6, 9).

Diskussion

Die SWOT-Analyse berücksichtigt technologische, taktische, rechtliche, monetäre sowie gesellschaftliche Aspekte. Ihre Ergebnisse zeigen, dass WAS-Systeme Stärken aufweisen, die ihre Attraktivität für den polizeilichen Einsatz begründen. Primär zeichnen sie sich durch ihre Fähigkeit zur großflächigen Überwachung aus, was eine erhebliche Erweiterung des Beobachtungsradius im Vergleich zu konventionellen Methoden darstellt (Israel Aerospace Industries 2023). Diese umfassende Gebietsabdeckung wird ergänzt durch die Möglichkeit zur Echtzeitüberwachung, die Fähigkeit zur Objektverfolgung und forensischen Analyse (Logos Technologies 2021, S. 5; Marion 2017; Alam und Gupta 2020, S. 289-290, 301-302). Zugleich haben UAV gegenüber konventionellen Luftfahrzeugen den entscheidenden Vorteil, dass sie nicht nur für offene Maßnahmen, sondern auch für verdeckte Maßnahmen eingesetzt werden können (Buckler 2019, S. 23). Dabei spielt die Integration von KI und maschinellem Lernen zur autonomen Objekterkennung und -verfolgung eine entscheidende Rolle. Die Verzahnung mit Aspekten der GeoAI verspricht zudem eine verbesserte räumliche Analyse und Interpretation der erfassten Daten (Chauhan und Shekhar 2021, S. 355-370; Reilly et al. 2010, S. 186-199; Logos Technologies 2021, S. 5; Blaschke 2024; Brandi 2024).

Eine weitere wesentliche Stärke liegt in der Kosteneffizienz der Drohnen. Im direkten Vergleich zu bemannten Systemen wie Polizeihelikoptern erweisen sich diese sowohl in der Anschaffung als auch im operativen Betrieb als deutlich kostengünstiger (Tikanmäki und Tuohimaa 2011, 89 ff.; Malone et al. 2013; Bolkcom 2005, S. 3-4; Magrassi 2016, 36 ff.; Tsiamis et al. 2023, S. 6, 9; RP Online 2016; Franco 2019) und verfügen über eine deutlich längere Flugdauer (Bolkcom 2005, S. 3-4; Heeren 2016). Dies eröffnet Potenziale für einen breiteren und häufigeren Einsatz, was wiederum die Effektivität polizeili-

cher Arbeit steigern wird. Ihre Flexibilität ermöglicht zudem einen Einsatz in den unterschiedlichsten Szenarien, vom Schutz der eigenen Kräfte, dem Schutz gefährdeter Infrastruktur, zur Aufklärung, Observation, bis hin zur Veranstaltungssicherheit (Logos Technologies 2018, S. 1-6; Christen et al. 2018b, S. 14, 70, 208-210).

Trotz dieser Stärken weist die Technologie Schwächen auf, die einer kritischen Betrachtung bedürfen. Zu den primären Limitierungen zählt die Anfälligkeit gegenüber widrigen Wetterbedingungen, die den Einsatz der Systeme beeinträchtigt (Haddal und Gertler 2010, S. 4). Darüber hinaus bestehen Sicherheitsrisiken, wie potenzielle Kollisionen mit anderen Luftfahrzeugen oder die Gefahr von Systemausfällen und Abstürzen, die nicht nur die Funktionalität beeinträchtigen, sondern auch abstrakt eine Gefährdung für die Öffentlichkeit darstellen (Christen et al. 2018b, S. 119). Ein Schlüsselement, um Drohnen zukünftig autonom im Luftraum einsetzen zu können, ist deshalb die Entwicklung eines zuverlässigen Systems zur Vermeidung von Zusammenstößen (Haddal und Gertler 2010, S. 5).

Die Chancen und die Effizienzsteigerung bei der Bewältigung von Einsatzszenarien, die sich durch den Einsatz von WAS-Systemen eröffnen, sind weitreichend. Hier sind insbesondere die Möglichkeit zur Verbesserung der öffentlichen Sicherheit durch präventive Maßnahmen, der Ausbau von interdisziplinären Kooperationen mit anderen Behörden und eine schnellere Reaktion auf Vorfälle zu nennen (Bone-Winkel 2020, S. 73; Ayamga et al. 2021, S. 2; Laksham 2019, S. 343, 344; Eftychidis et al. 2018).

Den Chancen stehen jedoch Risiken gegenüber, die einer sorgfältigen Abwägung bedürfen. Ein wichtiger Punkt sind die mit dem Einsatz von drohnengestützten WAS-Systemen verbundenen Datenschutzbedenken. Die umfassende und detaillierte Datenerfassung wirft rechtliche Fragen hinsichtlich der Wahrung der Privatsphäre und des Schutzes der Grundrechte auf (Buckler 2019, S. 1-10; Christen et al. 2018a, S. 25; Christen et al. 2018b, S. 158 ff.). Diese gewinnen insbesondere vor dem Hintergrund zunehmender gesellschaftlicher Sensibilität an Brisanz und könnten zu Akzeptanzproblemen in der Bevölkerung führen (Vogt 2017, S. 22).

Daneben müssen aber auch regulatorische Aspekte hinsichtlich der Nutzung des Luftraums vereinbart werden (Buckler 2019, S. 1-10). Die rechtlichen Rahmenbedingungen sind nicht eindeutig geklärt. Nach ersten rechtlichen Überlegungen scheinen deshalb für die Polizei die gleichen Anforderungen zu gelten wie für den herkömmlichen Einsatz von polizeilichen Helikoptern (Buckler 2019, S. 6, 9).

Ein weiteres Risiko liegt in potenziellen Sicherheitslücken der Systeme. Ein erfolgreicher Hackerangriff kann die Funktionalität der Systeme und die Integrität der Daten gefährden (Laksham 2019, S. 345; Scott und Scott 2017, S. 2; Weichert 2012, S. 3-4).

Schlussfolgerung

Es lässt sich konstatieren, dass die WAS-Technik neue Möglichkeiten zur Kriminalitätsbekämpfung und Gefahrenabwehr bietet und das Potenzial hat, die Polizeiarbeit grundlegend zu verändern. Der polizeiliche Einsatz von drohnengestützten WAS-Systemen wird den Mangel an stationären Überwachungsmöglichkeiten oder Streifenpolizisten auf den Straßen beseitigen und den wachsenden Bedarf an Überwachung ermöglichen, um die Sicherheit der Menschen in Deutschland zu gewährleisten. Ein einziges System ist in der Lage, zeitgleich eine ganze Stadt in Echtzeit zu monitoren und Objekte autonom zu klassifizieren. Auch wenn es Schwächen und Risiken beim Einsatz von drohnengestützten WAS-Systemen durch die deutsche Polizei gibt, können diese mit fortschreitender Entwicklung sowie einer normklaren und verhältnismäßigen rechtlichen Grundlage überwunden werden.

Die vorliegenden Ergebnisse liefern einen wichtigen Beitrag zur zukünftigen Diskussion. Durch die Betrachtung aktueller Aspekte wie beispielsweise der GeoAI und der autonomen Objekterkennung sowie aktueller technischer Systeme (WASP-System, LUNA-Drohnen, Thunder-B, Predator), wurden wichtige Entwicklungen in die Analyse miteinbezogen. Der ganzheitliche Ansatz, technologische, taktische, rechtliche, monetäre sowie gesellschaftliche Aspekte zu berücksichtigen, ermöglicht zudem eine differenziertere Beurteilung.

Doch trotz dieser Stärken bestehen auch Einschränkungen, die bei der Interpretation zu berücksichtigen sind. Eine zentrale Limitation liegt in der begrenzten Verfügbarkeit polizeispezifischer, offen zugänglicher, empirischer Daten. Untersuchungen, die eine Evaluation der Technologie in verschiedenen polizeilichen Einsatzszenarien ermöglichen würde, fehlen. Zudem erschwert die rechtliche Unsicherheit die Bewertung. Zukünftige Forschung sollte sich deswegen mit einem möglichen Rechtsrahmen für den Einsatz von WAS-Systemen durch die Polizei beschäftigen sowie auf die Generierung umfassender empirischer Daten konzentrieren, um eine spezifischere Bewertung der Möglichkeiten, Auswirkungen und Effizienz zu ermöglichen.

Abschließend kann festgestellt werden, dass zusätzliche technische Implikationen notwendig sind, um eine sichere Integration von Drohnen in den deutschen Luftraum zu gewährleisten. Zur erfolgreichen Umsetzung besteht außerdem auf polizeilicher Seite ein Erfordernis, sich aktiv an der Entwicklung, Rechtsetzung und dem Prozess der öffentlichen Meinungsbildung zu beteiligen.

Literaturverzeichnis

Alam, M. S.; Gupta, S. K. (2020): Cost-Effective Real-Time Aerial Surveillance System Using Edge Computing. In: Kamal Jain, Kourosh Khoshelham, Xuan Zhu und Anuj Tiwari (Hg.): Proceedings of UASG 2019. Unmanned Aerial System in Geomatics. International Conference on Unmanned Aerial System in Geomatics. Cham: Springer International Publishing, S. 289-299.

Association for Computing Machinery (Hg.) (2021): Thirteenth International Conference on Contemporary Computing (IC3). August 5 – 7, 2021. IC3 ,21: 2021 Thirteenth International Conference on Contemporary Computing. Noida India, 05.08.2021. New York (ICPS).

Ayamga, Matthew; Akaba, Selorm; Nyaaba, Albert Apotele (2021): Multifaceted applicability of drones: A review. *Technological Forecasting and Social Change* 167. DOI: 10.1016/j.techfore.2021.120677.

Blaschke, Ronny (2024): Aufrüstung im Zeichen der Ringe. Hg. v. Amnesty International Deutschland e.V. [amnesty.de/informieren/amnesty-journal/frankreich-ueberwachung-biometrisch-olympia-2024-aufruestung-im-zeichen-der-ringe](https://www.amnesty.de/informieren/amnesty-journal/frankreich-ueberwachung-biometrisch-olympia-2024-aufruestung-im-zeichen-der-ringe), zuletzt geprüft am 12.09.2024.

Bolkcom, Christopher (2005): Homeland Security: Unmanned Aerial Vehicles and Border Surveillance. Report for Congress. Congressional Research Service (CRS) (RS21698). [epic.org/wp-content/uploads/privacy/surveillance/spotlight/0805/rscb.pdf#page=3](https://www.epic.org/wp-content/uploads/privacy/surveillance/spotlight/0805/rscb.pdf#page=3), zuletzt geprüft am 11.09.2024.

Bone-Winkel, Eike (2020): Predictive Policing in der Risikogesellschaft. Auswirkungen auf die soziale Kontrolle und die Gesellschaft. Frankfurt am Main: Verlag für Polizeiwissenschaft (Schriftenreihe Polizei & Wissenschaft).

Brandi, Vincent (2024): AI will 'revolutionize' the way NATO looks at geospatial intelligence, leader says. *DefenseScoop*, 07.05.2024. [defensescoop.com/2024/05/07/nato-geoai-revolutionize-geoint-scott-bray](https://www.defensescoop.com/2024/05/07/nato-geoai-revolutionize-geoint-scott-bray), zuletzt geprüft am 10.09.2024.

Buckler, Julius (2019): (Verfassungs-)Rechtliche Rahmenbedingungen für den polizeilichen Einsatz sog. „Drohnen“. *Zeitschrift für das Gesamte Sicherheitsrecht (GSZ)* (1), S. 23-28.

Bundesministerium für Digitales und Verkehr (2020): Infrarot-Sensoren für Micro Rapid Mapping – IR4MRM. Hg. v. Bundesministerium für Digitales und Verkehr. [bmdv.bund.de/SharedDocs/DE/Artikel/DG/UAV-Projekte/infrarot-ensoren-micro-rapid-mapping.html](https://www.bmdv.bund.de/SharedDocs/DE/Artikel/DG/UAV-Projekte/infrarot-ensoren-micro-rapid-mapping.html), zuletzt geprüft am 12.09.2024.

Chauhan, Lokendra; Shekhar, Shashi (2021): GeoAI – Accelerating a Virtuous Cycle between AI and Geo. In: Association for Computing Machinery (Hg.): Thirteenth International Conference on Contemporary Computing (IC3). August 5 – 7, 2021. IC3 ,21: 2021 Thirteenth International Conference on Contemporary Computing. Noida India, 05.08.2021. New York (ICPS), S. 355-370. dl.acm.org/doi/fullHtml/10.1145/3474124.3474179, zuletzt geprüft am 10.09.2024.

Chiappino, Simone; Marcenaro, Lucio; Morerio, Pietro; Regazzoni, Carlo (2014): Event Based Switched Dynamic Bayesian Networks for Autonomous Cognitive Crowd Monitoring. In: Vijayan K. Asari (Hg.): Wide area surveillance. Real-time motion detection systems, Bd. 6. Heidelberg, New York, Dordrecht, London, Berlin: Springer (Augmented Vision and Reality, Vol. 6), S. 93-122.

Choi, Wongun; Savarese, Silvio (2014): Recognizing Complex Human Activities via Crowd Context. In: Vijayan K. Asari (Hg.): Wide area surveillance. Real-time motion detection systems, Bd. 6. Heidelberg, New York, Dordrecht, London, Berlin: Springer (Augmented Vision and Reality, Vol. 6), S. 71–91.

Christen, Markus; Guillaume, Michel; Jablonowski, Maximilian; Lenhart, Peter; Moll, Kurt (2018a): Drohnen als Partner im Luftraum. TATuP – Zeitschrift für Technikfolgenabschätzung in Theorie und Praxis 27 (3), S. 20-26. DOI: 10.14512/tatup.27.3.20.

Christen, Markus; Guillaume, Michel; Jablonowski, Maximilian; Lenhart, Peter; Moll, Kurt (2018b): Zivile Drohnen – Herausforderungen und Perspektiven. Zürich: vdf (TA-SWISS, 66). vdf.ch/zivile-drohnen-herausforderungen-und-perspektiven-e-book.html.

Clothier, Reece A.; Greer, Dominique A.; Greer, Duncan G.; Mehta, Amisha M. (2015): Risk Perception and the Public Acceptance of Drones. Risk Analysis 35 (6), S. 1-30. DOI: 10.1111/risa.12330.

Deutsches Zentrum für Luft- und Raumfahrt (2018): Umfrage zur Akzeptanz unbemannter Luftfahrzeuge. Hg. v. Statista Research Department. de-statista-com.eu1.proxy.openathens.net/statistik/daten/studie/596521/umfrage/umfrage-zu-moeglichen-problemen-durch-die-nutzung-ziviler-drohnen, zuletzt geprüft am 10.09.2024.

Eftychidis, George; Gkotsis, Ilias; Kolios, Panayiotis; Peleties, Costas (2018): UAVs and Their Use in Servicing the Community. In: Georgios Leventakis und M. R. Haberfeld (Hg.): Community-Oriented Policing and Technological Innovations. Cham: Springer International Publishing (SpringerBriefs in Criminology), S. 119-131.

Europäische Kommission (2022): A Drone Strategy 2.0 for a Smart and Sustainable Unmanned Aircraft Eco-System in Europe. transport.ec.europa.eu/document/download/1cb5fb4f-4252-4f97-abf4-c4a167b1c7d2_en?filename=COM_2022_652_drone_strategy_2.0.pdf, zuletzt geprüft am 07.09.2024.

Franco, Maria (2019): 41 Flüge: Landesregierung mit Polizei-Hubschraubern unterwegs. Osthessen News, 26.11.2019. osthessen-news.de/n11628173/41-fluege-landesregierung-mit-polizei-hubschraubern-unterwegs.html, zuletzt geprüft am 13.09.2024.

FRONTEX (2022): Frontex deploys unmanned aircraft to support Greece with border control. Hg. v. FRONTEX – European Border and Coast Guard Agency. frontex.europa.eu/media-centre/news/news-release/frontex-deploys-unmanned-aircraft-to-support-greece-with-border-control-McmYki, zuletzt geprüft am 12.09.2024.

Gaissert, Susan (2017): Why Wide Area Surveillance is a Big Deal. Hg. v. Defending Rights & Dissent. rightsanddissent.org/news/wide-area-surveillance-big-deal/, zuletzt geprüft am 10.09.2024.

Griffin, Matthew (2016): One camera to watch an entire city, meet WAMI. fanaticalfuturist.com/2016/07/one-camera-to-watch-an-entire-city-meet-wami, zuletzt geprüft am 11.09.2024.

Haddal, Chad C.; Gertler, Jeremiah (2010): Homeland Security: Unmanned Aerial Vehicles and Border Surveillance. trac.syr.edu/immigration/library/p4798.pdf.

Hartwig, M.-A. (2001): Geographische Informationssysteme (GIS). Kriminalistik (6), S. 435-439.

Hayes, Ben; Jones, Chris; Toepfer, Eric (2014): EURODRONES Inc. Hg. v. Statewatch. Transnational Institute (TNI). statewatch.org/media/documents/news/2014/feb/sw-tni-eurodrones-inc-feb-2014.pdf, zuletzt geprüft am 12.09.2024.

Heeren, U. (2016): H145T2 Neuer Polizeihubschrauber für NRW. web.archive.org/web/20160916013459/polizeifliegerstaffel.de/?Willkommen___Aktuelles___H145T2, zuletzt geprüft am 13.09.2024.

Hoffmann, Oliver (2023): Rheinmetall liefert HUSAR an die Bundeswehr | Rheinmetall. Hg. v. Rheinmetall AG. rheinmetall.com/de/media/news-watch/news/2023/09/2023-09-28-rheinmetall-liefert-husar-an-bundeswehr, zuletzt geprüft am 10.09.2024.

ICAO (International Civil Aviation Organization) (2011): Unmanned aircraft systems (UAS). Hg. v. International Civil Aviation Organization (ICAO). Montreal (ICAO cir, AN 190). [icao.int/Meetings/UAS/Documents/Circular%20328_en.pdf](https://www.icao.int/Meetings/UAS/Documents/Circular%20328_en.pdf), zuletzt geprüft am 12.09.2024.

Irizarry, J.; Gheisari, M.; Walker, B. N. (2012): Usability assessment of drone technology as safety inspection tools. *Journal of Information Technology in Construction* 17 (12), S. 194-212. sonify.psych.gatech.edu/~walkerb/publications/pdfs/2012itconstruction-irizarrygheisariwalker.pdf.

Israel Aerospace Industries (2023): IAI WASP WAMI – Wide Area Motion Imagery. Hg. v. Israel Aerospace Industries. iai.co.il/p/wasp, zuletzt geprüft am 10.09.2024.

Künzli, Benjamin (2012): SWOT-Analyse. Ein klassisches Instrument der Strategieentwicklung mit viel ungenutztem Potenzial. *Zeitschrift Führung+ Organisation* 81 (02), S. 126-129. clc-consulting.ch/fileadmin/content/swot_analyse_benjamin_kuenzli.pdf.

Laksham, Karthik Balajee (2019): Unmanned aerial vehicle (drones) in public health: A SWOT analysis. *Journal of family medicine and primary care* 8 (2), S. 342-346. DOI: 10.4103/jfmpc.jfmpc_413_18.

Li, Wenwen; Hsu, Chia-Yu (2022): GeoAI for Large-Scale Image Analysis and Machine Vision: Recent Progress of Artificial Intelligence in Geography. *IJGI* 11 (7), S. 385. DOI: 10.3390/ijgi11070385.

Logos Technologies (2018): Kestrel Block II. logotech.net/products/kestrel-block-ii, zuletzt geprüft am 11.09.2024.

Logos Technologies (2021): No Surprise Attacks: How Wide-Area Surveillance Enables „Deterrence by Detection“. Hg. v. Aviation Week Network. aviationweek.com/defense/no-surprise-attacks-how-wide-area-surveillance-enables-deterrence-detection, zuletzt geprüft am 10.09.2024.

Luftfahrt-Bundesamt (2023): Allgemeine Informationen. lba.de/DE/Drohnen/FAQ/01_FAQ_Allgemein/FAQ_node.html, zuletzt geprüft am 09.09.2024.

Ma, Yalong; Wu, Xinkai; Yu, Guizhen; Xu, Yongzheng; Wang, Yunpeng (2016): Pedestrian Detection and Tracking from Low-Resolution Unmanned Aerial Vehicle Thermal Imagery. *Sensors* 16 (4), S. 446. DOI: 10.3390/s16040446.

Magrassi, Federico (2016): The automation of air traffic: Legislative evolution and economic development 2016. *tesi.luiss.it/17012/1/106103_MAGRASSI_FEDERICO.pdf*, zuletzt geprüft am 10.09.2024.

Malone, P.; Apgar, H.; Stukes, S.; Sterk, S. (2013): Unmanned Aerial Vehicles unique cost estimating requirements. In: IEEE (Hg.): *Aerospace Conference. Big Sky, Montana, March 2-9, 2013*. Piscataway, N.J.: IEEE, S. 1-8. ieeexplore.ieee.org/document/6496852.

Marion, John (2017): *Wide-Area Motion Imagery Systems: Evolution, Capabilities and Mission Sets*. Royal United Services Institute. rusi.org/explore-our-research/publications/rusi-defence-systems/wide-area-motion-imagery-systems-evolution-capabilities-and-mission-sets, zuletzt geprüft am 09.09.2024.

Maritime Rescue Coordination Centre (2024): Rettungsleitstelle See. seenotretter.de/crews-stationen/rettungsleitstelle-see, zuletzt geprüft am 11.10.2024.

Marques, Hernani (2014): INDECT-Forschungsergebnisse der Europäischen Union. Chancen und Gefahren der Möglichkeiten zur zentralisierten und transnationalen Überwachung. Universität Zürich. Soziologisches Institut. vecirex.net/docs/soz_140515--marques.hernani-indect_web.pdf, zuletzt geprüft am 12.09.2024.

Persistent Surveillance Systems (2018): HawkEye II. Hg. v. Persistent Surveillance Systems (PSS). pss-1.com/hawkeye-ii, zuletzt geprüft am 11.09.2024.

Powers, Benjamin (2017): Eyes Over Baltimore: How Police Use Military Technology to Secretly Track You. Rolling Stone, 06.01.2017. [rollingstone.com/culture/culture-features/eyes-over-baltimore-how-police-use-military-technology-to-secretly-track-you-126885](https://www.rollingstone.com/culture/culture-features/eyes-over-baltimore-how-police-use-military-technology-to-secretly-track-you-126885), zuletzt geprüft am 10.09.2024.

Reilly, Vladimir; Idrees, Haroon; Shah, Mubarak (2010): Detection and Tracking of Large Number of Targets in Wide Area Surveillance. In: Daniilidis, K., Maragos, P., Paragios, N. (Hg.): Computer Vision – ECCV 2010, Bd. 6313. Berlin, Heidelberg: Springer Nature (Lecture Notes in Computer Science), S. 186-199.

Rheinmetall AG (2023): LUNA – Unbemannte luftgestützte Aufklärungssysteme. Rheinmetall AG. [rheinmetall.com/de/produkte/unbemannte-systeme/luna#anchor-luna-uas](https://www.rheinmetall.com/de/produkte/unbemannte-systeme/luna#anchor-luna-uas), zuletzt geprüft am 10.09.2024.

Royo, Pablo; Asenjo, Àlex; Trujillo, Juan; Çetin, Ender; Barrado, Cristina (2022): Enhancing Drones for Law Enforcement and Capacity Monitoring at Open Large Events. Drones 6 (11), S. 359. DOI: 10.3390/drones6110359.

RP Online (2016): Neue Hubschrauber-Flotte für die NRW-Polizei. RP ONLINE, 07.09.2016. [rp-online.de/nrw/staedte/duesseldorf/neue-hubschrauber-flotte-fuer-die-nrw-polizei_aid-18531733](https://www.rp-online.de/nrw/staedte/duesseldorf/neue-hubschrauber-flotte-fuer-die-nrw-polizei_aid-18531733), zuletzt geprüft am 13.09.2024.

Schawel, Christian; Billing, Fabian (2018): Top 100 Management Tools: Das wichtigste Buch eines Managers. Von ABC-Analyse bis Zielvereinbarung: Springer Fachmedien Wiesbaden GmbH ebook-central.proquest.com/lib/dhpol/detail.action?docID=5205509.

Scott, Judy; Scott, Carlton (Hg.) (2017): Drone Delivery Models for Healthcare. 50th Hawaii International Conference on System Sciences (Global Health IT Strategies Minitrack). scholarspace.manoa.hawaii.edu/handle/10125/41557, zuletzt geprüft am 07.09.2024.

SearchWing (2023): UAVs for SAR. [tha.de/searchwing/de/sar-drohne](https://www.tha.de/searchwing/de/sar-drohne), zuletzt geprüft am 11.10.2024.

Shahzad, Alam; Gupta, Sujit Kumar (2020): Cost-Effective Real-Time Aerial Surveillance System Using Edge Computing. In: Kamal Jain, Kourosh Khoshelham, Xuan Zhu und Anuj Tiwari (Hg.): Proceedings of UASG 2019. Unmanned Aerial System in Geomatics. International Conference on Unmanned Aerial System in Geomatics. Cham: Springer International Publishing, S. 289-299. Online verfügbar unter link.springer.com/chapter/10.1007/978-3-030-37393-1_25.

Walker, Scott W. (2010): Integrating Department of Defense Unmanned Aerial Systems into the National Airspace Structure. [irp.fas.org/program/collect/uas-airspace.pdf](https://www.irp.fas.org/program/collect/uas-airspace.pdf), zuletzt geprüft am 07.09.2024.

Weichert, Thilo (2012): Drohnen und Datenschutz. Bedrohungspotenzial und Gesetzgebungsbedarf bei der Beobachtung von oben. Zeitschrift für Datenschutz (11), S. 501-504. [beck-online.beck.de/Dokument?vpath=bibdata%2Fzeits%2Fzd%2F2012%2Fcont%2Fzd.2012.501.1.htm&anchor=Y-300-Z-ZD-B-2012-S-501-N-1](https://www.beck-online.beck.de/Dokument?vpath=bibdata%2Fzeits%2Fzd%2F2012%2Fcont%2Fzd.2012.501.1.htm&anchor=Y-300-Z-ZD-B-2012-S-501-N-1), zuletzt geprüft am 14.10.2024.

Wissenschaftliche Dienste – Deutscher Bundestag (2021): Einsatz von Drohnen durch die Bundespolizei, Artikel WD 3 - 3000 - 281/20. [bundestag.de/resource/blob/829742/87f3df4071fc9c1266ce1e0b450b2d98/WD-3-281-20-pdf-data.pdf](https://www.bundestag.de/resource/blob/829742/87f3df4071fc9c1266ce1e0b450b2d98/WD-3-281-20-pdf-data.pdf), zuletzt geprüft am 07.09.2024.

Der retrograde biometrische Abgleich mit allgemein öffentlich zugänglichen Daten aus dem Internet

Paul Haacker

Die rasante Entwicklung biometrischer Technologien bietet Polizeibehörden neue Möglichkeiten, unbekannte Personen zu identifizieren. Ein prominentes Beispiel für die Effizienz solcher Technologien lieferte der Fall Daniela Klette, einer mutmaßlichen ehemaligen RAF-Terroristin, die über Jahrzehnte als flüchtig galt. Im Jahr 2023 gelang es einem Journalisten, Frau Klette mithilfe des Gesichtserkennungsdienstes PimEyes auf einem öffentlich zugänglichen Bild im Internet zu identifizieren. Diese Information führte schließlich zu ihrer Festnahme durch die Polizei (Koopmann, 2024). Der Fall verdeutlicht das Potenzial biometrischer Gesichtserkennung im Rahmen der Strafverfolgung. Gleichzeitig werfen diese neuen Möglichkeiten auch Fragen im Hinblick auf gesellschaftliche und rechtliche Herausforderungen auf.

Im Jahr 2024 ereigneten sich in Deutschland mehrere Terroranschläge. Am 23. August tötete ein islamistischer Attentäter während eines Stadtfestes in Solingen drei Menschen und verletzte acht weitere (Krištofski et al., 2024). Am 20. Dezember fuhr ein Mann in eine Menschenmenge auf einem Weihnachtsmarkt in Magdeburg, wodurch fünf Menschen starben und zahlreiche verletzt wurden (MDR Sachsen-Anhalt, 2024). Dies führte in Deutschland zu kontroversen Debatten um das sogenannte „Sicherheitspaket“, das mit dem „Gesetz zur Verbesserung der Terrorismusbekämpfung“ u. a. eine stärkere Nutzung biometrischer Gesichtserkennung durch die Polizei bei der Bekämpfung von schweren Straftaten ermöglichen sollte (Zeit Online, 2024).

In diesem Beitrag wird untersucht, wie der nachträgliche biometrische Abgleich zur Identifizierung unbekannter Personen in Deutschland durch Polizeibehörden genutzt werden könnte. Dabei werden zunächst technische Grundlagen zur Gesichtserkennung und die politische Kontroverse um das „Sicherheitspaket“ dargestellt. Im Weiteren wird der aktuelle Stand zum Einsatz von Gesichtserkennungstechnologie betrachtet. Zudem werden rechtliche Problemfelder

erörtert. Abschließend werden Vorschläge erarbeitet, wie technische Innovationen und gesetzliche Regelungen für einen Einsatz biometrischer Verfahren in der Polizeiarbeit in Einklang gebracht werden könnten.

Hintergrund

Als Grundlage für die Auseinandersetzung mit dem Thema werden zunächst die technologischen Grundlagen der Gesichtserkennung sowie die politische Kontroverse um das „Sicherheitspaket“ beleuchtet.

Technologische Grundlagen

Die automatisierte Gesichtserkennung ermöglicht die Identifizierung oder Verifizierung von Personen anhand ihrer Gesichtsmarkmalen in digitalen Bildern oder Videos. Biometrische Fernidentifizierungssysteme lassen sich in Echtzeit- und retrograde Systeme unterscheiden. Echtzeit-Systeme erfassen Daten und führen Abgleiche sowie Identifizierungen unmittelbar oder mit minimaler Verzögerung durch, basierend auf „Live“- oder „Near-live“-Material wie Kameraaufnahmen. Retrograde Systeme arbeiten hingegen mit zuvor aufgezeichneten Daten und führen die Analyse mit deutlicher Verzögerung anhand von Bild- oder Videoaufnahmen durch (ERPS 2021, S. 30). Gegenstand dieser Untersuchung sind ausschließlich retrograde Systeme.

Gesichtserkennungssysteme durchlaufen in der Regel mehrere Schritte. Im ersten Schritt wird ein Gesicht innerhalb eines Bildes oder Videos lokalisiert, üblicherweise durch den Einsatz von Methoden der Computer Vision. Dabei werden nicht nur Frontalaufnahmen erfasst, sondern auch Gesichter in Profilansicht erkannt. Anschließend analysiert das System zur Gesichtserkennung die biometrischen Merkmale des identifizierten Gesichts. Die analysierten Gesichtsdaten werden von einem Algorithmus in eine digitale Signatur überführt, die als „Faceprint“ bezeichnet wird. Diese mathematische Repräsentation des Gesichts ist aufgrund der individuellen Gesichtszüge einer Person einzigartig und vergleichbar mit einem Fingerabdruck. Im letz-

ten Schritt vergleicht das Gesichtserkennungssystem den erstellten „Faceprint“ mit einer Datenbank bekannter Gesichter. Mithilfe fortschrittlicher Algorithmen können trotz variierender Lichtverhältnisse, unterschiedlicher Gesichtsausdrücke oder Aufnahmewinkel Übereinstimmungen erkannt und die Wahrscheinlichkeit einer Identitätseinstimmung bewertet werden (Ionos, 2024).

Die Gesichtserkennung hat in den letzten Jahren durch den Einsatz von Deep-Learning-Technologien enorme Fortschritte gemacht. Diese Entwicklungen haben die Genauigkeit und Leistungsfähigkeit der Systeme deutlich verbessert. Allerdings bestehen weiterhin Herausforderungen. Wie Buolamwini und Gebru (2018) zeigen, weisen viele Gesichtserkennungssysteme nach wie vor systematische Verzerrungen auf. Insbesondere schneiden sie bei der Erkennung von Frauen und Menschen mit dunkler Hautfarbe schlechter ab. Um solche Ungerechtigkeiten zu überwinden, arbeiten Forschende daran, Algorithmen fairer und transparenter zu gestalten, damit Diskriminierung in Zukunft vermieden werden kann (Buolamwini & Gebru 2018, S. 1-2).

Politische Kontroverse

Im Koalitionsvertrag der Ampel-Regierung aus dem Jahr 2021 fand der Schutz von Grundrechten besonderen Ausdruck. Die Regierungsparteien erklärten, dass der Einsatz von KI-gestützter biometrischer Überwachung im öffentlichen Raum auf europäischer Ebene ausgeschlossen werden solle. Weiter hieß es, dass sie den Einsatz biometrischer Erfassung zu Überwachungszwecken grundsätzlich ablehnen (SPD, Bündnis 90/Die Grünen & FDP, 2021). Als Folge aus dem Terroranschlag in Solingen legte die Bundesregierung dennoch das „Sicherheitspaket“ vor und ließ es am 18. Oktober 2024 von den Parteien der Ampel-Koalition im Bundestag verabschieden (Bundestag, 2024). Allerdings erfuhr das Gesetzespaket im Bundesrat nicht die volle Zustimmung. Nach Beratungen wurde das „Sicherheitspaket“ nur teilweise angenommen. Das „Gesetz zur Verbesserung der Terrorismusbekämpfung“ wurde abgelehnt (Bundesrat, 2024).

Nach dem vorübergehenden Aus für das neue Gesetz einigten sich die Länder und der Bund auf zentrale Maßnahmen zur Bekämpfung schwerer Straftaten auf der Innenministerkonferenz (IMK) vom 4. bis 6. Dezember 2024, darunter auch die biometrische Gesichtserkennung. Bundesinnenministerin Nancy Faeser erklärte, dass es notwendig sei, Terrorverdächtige, Mörder und Vergewaltiger mithilfe von KI-gestützter Gesichtserkennung und Stimmerkennung effektiv identifizieren zu können. Diese Technologien böten laut Faeser entscheidende Werkzeuge, um die Strafverfolgung effizienter und gezielter zu machen (IMK, 2024). Die politische Debatte zeigt, wie sehr sich der Fokus der Sicherheitsbehörden auf die Nutzung technologischer Innovationen verlagert hat. Nach dem Ende der Ampel-Koalition ist fraglich, ob die Einigung der IMK zeitnah in der Verabschiedung eines Gesetzes mündet. Nach dem Terroranschlag in Magdeburg ist das Thema jedoch weiterhin auf der politischen Agenda.

Methodik

Für die Untersuchung wird eine qualitative Inhaltsanalyse nach Philipp Mayring durchgeführt, um das Thema systematisch und fundiert zu analysieren. Als Grundlage dient eine zielgerichtete Auswahl von Quellen. Dazu zählen Primärquellen wie die Datenschutz-Grundverordnung der EU (DSGVO), die EU-Verordnung über Künstliche Intelligenz (KI-VO) und nationale Gesetzesentwürfe sowie Sekundärquellen wie wissenschaftliche Publikationen, Berichte und journalistische Artikel. Die Auswahl der Texte erfolgt nach ihrer Relevanz für die Fragestellung. Ein zentrales Element der Analyse ist die Entwicklung von Kategorien, die aus der Zielsetzung dieses Beitrags abgeleitet werden. Hierbei werden zunächst deduktiv Kategorien wie „Technologische Grundlagen“, „Politische Rahmenbedingungen“, „Rechtliche Rahmenbedingungen“, „Einsatz von Gesichtserkennung“ und „Diskussion“ definiert. Während der Analyse werden diese Kategorien induktiv ergänzt, um unerwartete Aspekte im Material aufgreifen zu können. Das Material wird systematisch ausgewertet, indem die Inhalte den Kategorien zugeordnet und kontextbezogen interpretiert werden. Der Fokus liegt dabei auf der Identifikation potenzieller Konfliktlinien, insbesondere im Hinblick auf die rechtlichen Rahmen-

bedingungen. In der Diskussion erfolgt eine kritische Reflexion der gewonnenen Erkenntnisse, unter Einbeziehung von verschiedenen Perspektiven. Auf Grundlage der gewonnenen Erkenntnisse werden in der Schlussfolgerung konkrete Vorschläge erarbeitet, die darauf abzielen, praktikable Ansätze für eine verstärkte Anwendung biometrischer Gesichtserkennung in Deutschland zu entwickeln.

Ergebnisse

Im Folgenden werden die Ergebnisse der Untersuchung dargestellt, wobei der Fokus zunächst auf den Einsatzmöglichkeiten von Gesichtserkennungstechnologien liegt, bevor ausgewählte rechtliche Problemfelder betrachtet werden.

Einsatz von Gesichtserkennung

In den USA wird Gesichtserkennungstechnologie bereits umfassend eingesetzt. In der nachstehenden Ausführung soll dies analysiert und im Anschluss der Stand von Gesichtserkennung in Deutschland dargestellt werden.

Clearview AI

Clearview AI ist ein US-amerikanisches Unternehmen, das sich auf Gesichtserkennungstechnologie spezialisiert hat. Das Unternehmen verfügt über eine Datenbank mit mehr als 30 Milliarden Bildern, die ohne Zustimmung der betroffenen Personen von sozialen Netzwerken wie Facebook gesammelt wurden. Das Unternehmen hat sich eine Datenbank mit 100 Milliarden Bildern als Ziel gesetzt (Kremppl, 2022). Diese Datenbank ermöglicht es der Polizei, unbekannte Personen anhand von Fotos mit der umfangreichen Bildsammlung abzugleichen und dadurch zu identifizieren. Bis März 2023 sollen laut Clearview AI etwa eine Million Suchanfragen von US-amerikanischen Polizeibehörden durchgeführt worden sein. Die Technologie soll insbesondere bei der Aufklärung schwerer Verbrechen, etwa Mordfällen, erfolgreich zum Einsatz gekommen sein. In einer BBC-Dokumentation aus dem Jahr 2023 erklärte jedoch ein leitender Po-

lizist aus Miami, dass Clearview AI auch bei Ladendiebstählen eingesetzt werden könne und keine Grenzen in der Anwendung dieser Technologie für Polizeibehörden in den USA bestehen (BBC News, 2023; Clayton & Derico, 2023).

Im Jahr 2020 wurde erstmals die Nutzung von Clearview AI in der EU bekannt. Schwedische Polizeibeamte nutzten den Dienst ohne offizielle Genehmigung zu Ermittlungszwecken. Infolgedessen verhängte die schwedische Datenschutzbehörde im Februar 2021 eine Geldstrafe von 2,5 Millionen SEK (rund 250.000 Euro) und verpflichtete die Polizei, betroffene Personen zu informieren sowie die übermittelten Daten zu löschen (EDPB, 2021). Im Jahr 2022 ging auch die italienische Datenschutzbehörde gegen Clearview AI vor. Sie stellte fest, dass das Unternehmen biometrische Daten italienischer Bürger ohne rechtliche Grundlage sammelte, insbesondere durch das sogenannte „Scraping“ von Bildern aus sozialen Netzwerken. Diese Praktiken verstießen gegen mehrere Vorschriften der DSGVO, insbesondere in Bezug auf Transparenz, Zweckbindung und Speicherbegrenzung. Die Behörde verhängte eine Geldstrafe von 20 Millionen Euro (EDPB, 2022). Einen vergleichbar begründeten Verstoß stellte auch die niederländische Datenschutzbehörde im September 2024 fest und verhängte eine Geldstrafe von 30,5 Millionen Euro. Die Behörde hob hervor, dass Gesichtserkennungstechnologien ohne rechtliche Grundlage eine erhebliche Verletzung der Privatsphäre darstellen (EDPB, 2024). Diese Erfahrungen von anderen EU-Mitgliedsstaaten mit Clearview AI verdeutlichen die Herausforderungen, die mit dem Einsatz von Gesichtserkennungstechnologien verbunden sind. Gleichzeitig unterstreichen die Maßnahmen gegen Clearview AI die Entschlossenheit der EU, die Rechte ihrer Bürgerinnen und Bürger gegenüber unrechtmäßigen Praktiken internationaler Unternehmen zu schützen.

Gesichtserkennung in Deutschland

In Deutschland sind bislang keine Fälle der Nutzung von Clearview AI öffentlich bekannt geworden. Allerdings ging das BKA im Jahr 2008 einen bedeutenden Schritt in der Anwendung biometrischer Technologien zur Identifikation unbekannter Personen mit der Einführung des Gesichtserkennungssystems (GES). Dabei erfolgt ein

automatisierter Abgleich mit der INPOL-Datenbank, die im Jahr 2024 über 7,3 Millionen Bilder von 5,1 Millionen Personen enthielt (BKA, 2024). Die Bedeutung des Systems zeigt sich in der Zunahme der Suchanfragen. Während 2021 insgesamt 90.425 Abfragen registriert wurden, stieg die Zahl 2023 auf 117.900 Suchanfragen an. Im gleichen Zeitraum verringerte sich die Zahl der identifizierten Personen durch das GES von 4.403 im Jahr 2021 auf knapp 3.800 im Jahr 2023 (Monroy, 2021; BKA, 2023).

Im Jahr 2024 führte das BKA ein verbessertes, KI-gestütztes Gesichtserkennungssystem ein, das laut Aussagen des BKA-Präsidenten Holger Münch nahezu fehlerfrei arbeitet. Trotz dieser technologischen Fortschritte bleibt eine menschliche Prüfung („human in the loop“) erforderlich, um Fehlentscheidungen zu vermeiden und die Integrität des Systems zu gewährleisten. Mit der Einführung des verbesserten Systems wurden zudem strukturelle Veränderungen vorgenommen. Bislang wurden auf der für das GES zuständigen Dienststelle im BKA 15 Stellen abgebaut und bis 2026 ist ein weiterer Stellenabbau auf insgesamt 50 Stellen geplant (Monroy, 2024).

Im Zusammenhang mit dem Einsatz von Gesichtserkennungstechnologie in Deutschland muss auch das Pilotprojekt am Berliner Südkreuz genannt werden. Im Rahmen des Projekts wurde von 2017 bis 2018 im Teilprojekt 1 die Leistungsfähigkeit moderner Gesichtserkennungssysteme untersucht, die eine hohe Präzision bei der Erkennung und eine niedrige Fehlerrate zeigten (Bundespolizei, 2018). Zudem wurde im Dezember 2024 eine Reform des Polizeirechts in Hessen angekündigt, die biometrische Identifizierungen bei erheblichen Gefahren und nach menschlicher Prüfung ermöglichen soll (Hessischer Landtag, 2024).

Rechtliche Rahmenbedingungen

Der Einsatz von Gesichtserkennungstechnologien und der Umgang mit Massendaten werfen eine Vielzahl rechtlicher Fragestellungen auf. Im Folgenden werden ausgewählte rechtliche Problemfelder der DSGVO, der KI-VO und des geplanten „Sicherheitspakets“ analysiert, um zentrale Herausforderungen und mögliche Konflikte aufzuzeigen.

Problemfelder in der DSGVO

Der rechtliche Rahmen für die Verarbeitung personenbezogener Daten in Europa wird maßgeblich durch die DSGVO definiert. In Artikel 5 werden wesentliche Grundsätze für den Umgang mit Daten in der EU geregelt. Die folgenden sind im Hinblick die Erhebung und Speicherung von biometrischen Daten in Datenbanken besonders problematisch. In Absatz 1 b) des Artikels 5 DSGVO ist der Grundsatz der Zweckbindung geregelt. Danach dürfen personenbezogene Daten nur für klar festgelegte, eindeutige und legitime Zwecke erhoben werden. Eine Weiterverarbeitung dieser Daten ist nur zulässig, wenn sie mit den ursprünglichen Zwecken vereinbar ist. Dieses Prinzip stellt sicher, dass die Erhebung und Nutzung von Daten nicht willkürlich erfolgt, sondern an vorher definierte Ziele gebunden ist. In Absatz 1 c) wird der Grundsatz der Datenminimierung geregelt. Hierbei wird gefordert, dass personenbezogene Daten dem Verarbeitungszweck angemessen, erheblich und auf das notwendige Maß beschränkt sein müssen. Dieser Grundsatz soll die Menge der erhobenen Daten minimieren, um das Risiko für die Betroffenen zu reduzieren und gleichzeitig die Effizienz und Sicherheit der Datenverarbeitung zu erhöhen. In Absatz 1 e) wird der Grundsatz der Speicherbegrenzung geregelt. Danach dürfen personenbezogene Daten nur so lange in einer identifizierbaren Form gespeichert werden, wie dies für die Zwecke der Verarbeitung erforderlich ist. Dies schützt die betroffenen Personen vor einem Missbrauch ihrer Daten durch übermäßig lange Speicherfristen und stellt sicher, dass die Daten nach Wegfall des Verarbeitungszwecks gelöscht oder anonymisiert werden.

Artikel 9 der DSGVO regelt den Umgang mit besonderen Kategorien personenbezogener Daten, darunter auch biometrischen Daten. Solche Daten sind grundsätzlich von der Verarbeitung ausgeschlossen. Ausnahmen sind jedoch erlaubt, etwa wenn die betroffene Person ihre Daten bewusst öffentlich zugänglich gemacht hat oder wenn die Verarbeitung aufgrund von Unionsrecht oder nationalem Recht im öffentlichen Interesse, etwa zur Sicherheit oder Forschung, erforderlich ist.

In Artikel 6 i.V.m. Artikel 23 der DSGVO sind mögliche Ausnahmen von der Zweckbindung geregelt. Artikel 6 regelt insbesondere die Verarbeitung für einen anderen Zweck als den ursprünglich vorgesehenen. Solche Zweckänderungen sind zulässig, wenn sie notwendig und verhältnismäßig zum Schutz spezifischer Ziele nach Artikel 23 Absatz 1 sind und mit dem ursprünglichen Verarbeitungszweck vereinbar bleiben. Artikel 23 erlaubt es den Mitgliedstaaten, Pflichten und Rechte der DSGVO einzuschränken, etwa zur Verhütung oder Verfolgung von Straftaten, sofern nationale oder europäische Rechtsvorschriften dies rechtfertigen.

Problemfelder in der KI-VO

Auch in der KI-VO werden rechtliche Rahmenbedingungen für den Einsatz von biometrischer Gesichtserkennung definiert. Die Verordnung zielt darauf ab, den sicheren Einsatz von KI-Systemen zu gewährleisten und gleichzeitig Innovationen in diesem Bereich zu fördern. Gemäß Artikel 5 der KI-VO sind bestimmte KI-Praktiken grundsätzlich verboten. Dazu gehört nach Artikel 5 Absatz 1 Buchstabe e insbesondere die Nutzung von KI-Systemen, die Datenbanken für die Gesichtserkennung durch ungezieltes Auslesen von Gesichtsbildern aus dem Internet („Scraping“) oder aus Videoüberwachungsaufnahmen erstellen oder erweitern.

In Artikel 6 der KI-VO sind die Einstufungsvorschriften für sogenannte Hochrisiko-KI-Systeme aufgeführt. Diese Einstufung betrifft KI-Systeme, die in sensiblen Bereichen eingesetzt werden und ein erhöhtes Risiko für die Rechte und Freiheiten der Menschen darstellen können. Im Anhang III der KI-VO werden spezifische Kategorien von Hochrisiko-KI-Systemen genannt, darunter biometrische Fernidentifizierungssysteme. Somit handelt es sich bei dem Einsatz von nachträglicher biometrischer Gesichtserkennung um ein Hochrisiko-KI-System, das die Einhaltung von strengen Anforderungen von den Herstellern und Betreibern verlangt. Dazu gehören die Gewährleistung der Genauigkeit und Robustheit der Systeme, die Minimierung von Verzerrungen sowie die Transparenz und Nachvollziehbarkeit

der Funktionsweise. Ferner müssen diese Systeme regelmäßigen Konformitätsbewertungen unterzogen werden, um sicherzustellen, dass sie den Anforderungen der Verordnung entsprechen.

Regelungen im „Sicherheitspaket“

Das im Rahmen des „Sicherheitspakets“ angestrebte „Gesetz zur Verbesserung der Terrorismusbekämpfung“ in Deutschland sollte u. a. die Befugnisse des BKA um den Einsatz biometrischer Technologien erweitern. Das Gesetz wurde bislang nicht erfolgreich verabschiedet. Nach dem neuen § 10b Bundeskriminalamtgesetz dürfte das BKA biometrische Daten wie Gesichtsprofile mit allgemein öffentlich zugänglichen personenbezogenen Daten aus dem Internet abgleichen. Gemäß Absatz 9 dürften die personenbezogenen Daten auch durch Dritte im Auftrag des BKA verarbeitet werden. Die beteiligten Firmen müssten ihren Sitz aber ausschließlich in der Europäischen Union oder in einem Schengen-assoziierten Staat haben. Die Übermittlung personenbezogener Daten wäre ebenfalls auf diese geografischen Regionen beschränkt. Gemäß Absatz 11 würde die Bundesregierung durch Rechtsverordnung die technischen und rechtlichen Rahmenbedingungen für den biometrischen Abgleich durch das BKA festlegen. Dabei müssten detaillierte Vorgaben für das Verfahren und Maßnahmen zur Sicherstellung des Datenschutzes gemacht werden. Zu diesen Regelungen gehören die Bestimmung von Eingabe- und Zugangsberechtigungen, Speicher- und Löschrufen, die Art der zu speichernden Daten, der von der Speicherung betroffene Personenkreis, die maximale Dauer der Speicherung sowie Vorgaben zur Protokollierung.

Durch den neuen § 16a Absatz 1 BKAG würde das BKA die Befugnis erhalten, personenbezogene Daten, die im polizeilichen Informationsverbund oder im Informationssystem gespeichert sind, mittels automatisierter Anwendungen zusammenzuführen und für analytische Zwecke weiterzuverarbeiten. Auch hier würde die konkrete Ausgestaltung der Umsetzung durch eine Rechtsverordnung der Bundesregierung geregelt werden.

In § 22 Absatz 3 BKAG würde dem BKA die Möglichkeit eingeräumt, personenbezogene Daten, die bereits bei der Behörde vorhanden sind, zu weiteren Zwecken zu verarbeiten. Dazu soll die Nutzung dieser Daten zur Entwicklung, Überprüfung, Änderung oder zum Trainieren von IT-Produkten gehören. Diese Befugnis würde auch die Übermittlung der Daten an Dritte umfassen, sofern dies für die genannten Zwecke erforderlich ist. Auch hier würde die konkrete Ausgestaltung der Umsetzung durch eine Rechtsverordnung der Bundesregierung geregelt werden. Der Gesetzesvorschlag bleibt insofern an vielen Stellen unbestimmt und bietet dadurch Räume für die spätere Ausgestaltung, aber auch für Kritik.

Diskussion

Clearview AI bietet ein wirkungsvolles System zur Gesichtserkennung, das bereits umfangreich von US-amerikanischen Polizeibehörden genutzt wird. Das Unternehmen betont, seinen Dienst ausschließlich für Sicherheitsbehörden zur Verfügung zu stellen und dass dieser nicht für die allgemeine Öffentlichkeit bestimmt sei. Es ist jedoch fraglich, inwiefern das Unternehmen ein Modell entwickeln könnte, dass mit dem „Scraping“-Verbot der KI-VO sowie den Grundsätzen der Zweckbindung, Datenminimierung und Speicherbegrenzung in der DSGVO vereinbar wäre. Gegner argumentieren, dass die Nutzung von Clearview AI dazu führen würde, dass jede Person potenziell als Verdächtige in einer dauerhaften polizeilichen Identifikationsprüfung steht. Insbesondere die Tatsache, dass die gespeicherten Bilder ohne Einwilligung der betroffenen Personen erfasst wurden, stößt auf große Bedenken hinsichtlich der Privatsphäre und des Datenschutzes (Clayton & Derico, 2023).

Clearview AI verarbeitet auch die Gesichter von Personen, die nur im Hintergrund eines Fotos unbeabsichtigt fotografiert wurden (Clearview AI, 2022, 00:42 min). Dies stellt eine besondere Herausforderung mit der Vereinbarkeit mit der DSGVO dar, da nicht alle Betroffenen ihre Fotos bewusst öffentlich gemacht haben. Zudem zeigen die seit 2020 regelmäßig von EU-Mitgliedsstaaten verhäng-

ten Strafen gegen Clearview AI, dass das Unternehmen bislang offensichtlich nicht an einer EU-rechtskonformen Lösung für den europäischen Markt gearbeitet hat.

In Deutschland steigen die Suchanfragen an das GES des BKA zwar deutlich an, allerdings sanken die Zahlen der erfolgreichen Identifizierungen im Vergleich der Jahre 2021 und 2023 leicht ab. Dies legt nahe, dass die INPOL-Referenzdatenbank bei der Identifizierung von unbekanntem Tatverdächtigen offensichtlich an Grenzen stößt und eine Erweiterung der Referenzdatenbank vermutlich mit einer deutlichen Steigerung der Identifizierungsquote verbunden wäre. Der Vorsitzende des BDK kritisiert im Rahmen der Debatte um das „Sicherheitspaket“ die geplanten Einschränkungen bei der biometrischen Gesichtserkennung, wie die Genehmigungspflicht durch den BKA-Präsidenten und die Begrenzung auf schwere Straftaten, als bürokratisch und ineffizient (Decker & Ottenberg, 2024).

Die Bundesbeauftragte für Datenschutz und Informationssicherheit wurde im Zuge des Gesetzgebungsverfahrens zum geplanten „Gesetz zur Verbesserung der Terrorismusbekämpfung“ angehört. Sie äußert erhebliche Bedenken hinsichtlich der Regelungen zur biometrischen Gesichtserkennung, insbesondere im Hinblick auf § 16a BKAG und dessen Vereinbarkeit mit der KI-VO. Sie warnt vor der Gefahr, dass durch die Umsetzung eine „Superdatenbank“ entstehen könnte, die biometrische Daten aus allen im Internet verfügbaren Bildern vereint. Eine solche Entwicklung sieht sie als schwerwiegende Bedrohung für die Grundrechte und den Datenschutz. Zudem bezweifelt sie, dass das BKA kurzfristig eine technisch einwandfreie und rechtlich zulässige Lösung entwickeln kann, und erwartet eine langwierige Lösungsfindung auf technischer Ebene. Zudem wurde insbesondere die Unbestimmtheit des neuen Gesetzes kritisiert, das an vielen Stellen auf spätere Regelungen durch eine Rechtsverordnung der Bundesregierung verweist (BfDI 2024, S. 7-8).

Schlussfolgerungen

Clearview AI kann in seiner jetzigen Form nicht von deutschen Polizeibehörden genutzt werden, da das massenhafte „Scraping“, die Verarbeitung biometrischer Daten ohne ausdrückliche Einwilligung der Betroffenen sowie die dauerhafte Speicherung der Bilder in einer Datenbank sowohl gegen die DSGVO als auch gegen die KI-VO verstößt. Möglicherweise wird das Unternehmen in Zukunft versuchen, neue Märkte zu erschließen, und an einer EU-rechtskonformen Lösung arbeiten. Dies ist jedoch bislang nicht erkennbar.

Ein Dienst wie der von Clearview AI könnte in der EU rechtskonform eingesetzt werden, wenn er die genannten Regelungen von DSGVO sowie KI-VO beachtet. Anstelle einer ungezielten Erfassung und dauerhaften Speicherung von öffentlich zugänglichen Bildern aus dem Internet, könnte eine regelmäßige, gezielte Recherche nach öffentlich zugänglichen Fotos erfolgen, wobei diese nur temporär gespeichert und verarbeitet werden. Zusätzliche KI-basierte Systeme könnten anstreben, nur die Personen im Vordergrund auf den Bildern zu verarbeiten und „unbeteiligte“ Personen im Hintergrund zu ignorieren. Dies würde Artikel 9 der DSGVO insofern gerecht werden, als dass nur bewusst veröffentlichte Bilder erhoben werden. Der dann folgende Abgleich würde mit einer vorab definierten Liste gesuchter Personen erfolgen. Nach Abschluss des Abgleichs müssten alle nicht relevanten Daten unverzüglich gelöscht werden, um eine dauerhafte Speicherung zu vermeiden und die datenschutzrechtlichen Vorgaben zu erfüllen. Dies würde auch die Grundsätze der Speicherbegrenzung und der Datenminimierung erfüllen. Zudem müssten die Anforderungen an Hochrisiko-KI-Systeme erfüllt sein.

Das GES wird in Deutschland bereits umfassend und erfolgreich durch das BKA als Serviceprovider und andere Polizeibehörden genutzt. Es nutzt zur Identifizierung von unbekannt Personen jedoch ausschließlich INPOL als Referenzdatenbank mit den dort einliegenden Bildern von ca. 5,1 Millionen Menschen. Um den rückläufigen Zahlen bei der Identifizierung von unbekannt Personen entgegenzuwirken, müsste die Referenzdatenbank für den Abgleich erweitert werden. Hierzu könnte der neue § 16a BKAG herangezogen werden.

Dieser erweitert die Befugnisse des BKA dahingehend, dass sowohl Daten aus „Informationssystemen“ als auch dem „polizeilichen Informationsverbund“ für den nachträglichen biometrischen Abgleich zusammengeführt werden dürfen. Dies kann als unbestimmt kritisiert werden. Durch die Unbestimmtheit können unter dem Begriff der „Informationssysteme“ aber auch das Einwohnermeldesystem und das Ausländerzentralregister gefasst werden. Da das Gesetz noch nicht verabschiedet wurde, gibt es hierzu keine Rechtsprechung. Letztlich würde – bei einer Verabschiedung des analysierten Gesetzes – die genaue Umsetzung ohnehin auf Basis einer Rechtsverordnung durch die Bundesregierung erfolgen.

In Deutschland leben ca. 83,5 Millionen Menschen (Statistisches Bundesamt, 2023a). Zu den überwiegend deutschen Staatsbürgern sind aufgrund der Ausweisdokumente Bilder im Einwohnermeldesystem gespeichert. Für die ca. 13,9 Millionen in Deutschland lebenden ausländischen Staatsangehörigen könnten die Daten aus dem Ausländerzentralregister herangezogen werden (Statistisches Bundesamt, 2023b). Auch hier sind Fotos zu den Personen gespeichert. In beiden Fällen wurden die Bilder zum Zweck der Ausstellung eines Dokuments erhoben. Durch ein nationales Gesetz könnte jedoch eine DSGVO-konforme Zweckänderung nach Art. 6 i.V.m. Art. 23 DSGVO erfolgen. Eine Integration dieser Systeme in das bestehende GES des BKA könnte die Identifizierungsquote erheblich steigern, da die Datenbasis umfassender wird und auch Personen einschließt, die bisher nicht in polizeilichen Datenbanken verzeichnet waren. Fraglich ist jedoch, ob dies – bei einer Verabschiedung des Gesetzes – von der künftigen Bundesregierung überhaupt beabsichtigt ist und das neue Gesetz vor dem Bundesverfassungsgericht Bestand haben wird. Es wäre jedoch eine Möglichkeit, die nur schwer umsetzbare Zusammenarbeit beim Umgang mit sensiblen Massendaten mit privaten Akteuren zu umgehen und die biometrische Gesichtserkennung in staatlicher Hand zu belassen.

Literaturverzeichnis

SPD, Bündnis 90/Die Grünen & FDP (2021). Mehr Fortschritt wagen: Koalitionsvertrag zwischen SPD, Bündnis 90/Die Grünen und FDP. cms.gruene.de/uploads/assets/Koalitionsvertrag-SPD-GRUENE-FDP-2021-2025.pdf [Zuletzt geprüft am 27. Dezember 2024].

BBC News (2023). US police forces using controversial facial recognition technology. YouTube. youtube.com/watch?v=uGeRTmDdqUI [Zuletzt geprüft am 27. Dezember 2024].

BfDI (2024). Stellungnahme zum Entwurf eines Gesetzes zur Verbesserung der Terrorismusbekämpfung. Die Bundesbeauftragte für Datenschutz und Informationsfreiheit. bfdi.bund.de/SharedDocs/Downloads/DE/DokumenteBfDI/Stellungnahmen/2024/StgN_Innere-Sicherheit-Asylsystem-Gesetz.pdf?__blob=publicationFile&v=3 [Zuletzt geprüft am 27. Dezember 2024].

Bundeskriminalamt (2023). Erkennungsdienst. bka.de/DE/UnserAufgaben/Ermittlungsunterstuetzung/Erkennungsdienst/erkennungsdienst_node.html [Zuletzt geprüft am 27. Dezember 2024].

Bundespolizei (2018). Teilprojekt 1: Biometrische Gesichtserkennung. Bundespolizeipräsidium Potsdam. bundespolizei.de/Web/DE/04Aktuelles/01Meldungen/2018/10/181011_abschlussbericht_gesichtserkennung_down.pdf;jsessionid=A43B634F7FC693A779DD4D6160073AD6.internet622?__blob=publicationFile&v=1 [Zuletzt geprüft am 27. Dezember 2024].

Bundesrat (2024). Beschluss des Bundesrates – Gesetz zur Verbesserung der Terrorismusbekämpfung. Bundesrat, Drucksache 512/24. [bundesrat.de/SharedDocs/drucksachen/2024/0501-0600/512-24\(B\).pdf?__blob=publicationFile&v=3](https://bundesrat.de/SharedDocs/drucksachen/2024/0501-0600/512-24(B).pdf?__blob=publicationFile&v=3) [Zuletzt geprüft am 27. Dezember 2024].

Bundestag (2024). Entwurf eines Gesetzes zur Verbesserung der Terrorismusbekämpfung. Bundestag, Drucksache 20/12806. dserver.bundestag.de/btd/20/128/2012806.pdf [Zuletzt geprüft am 27. Dezember 2024].

Buolamwini, J., & Gebru, T. (2018). Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification. MIT Media Lab. media.mit.edu/publications/gender-shades-intersectional-accuracy-disparities-in-commercial-gender-classification/ [Zuletzt geprüft am 27. Dezember 2024].

Clayton, J. & Derico, T. (2023). Clearview AI used nearly 1m times by US police, it tells the BBC. BBC. bbc.com/news/technology-65057011 [Zuletzt geprüft am 27. Dezember 2024].

Clearview AI (2022). Clearview AI Company Overview. YouTube. youtube.com/watch?v=PZLUujBPolk [Zuletzt geprüft am 27. Dezember 2024].

Decker, M. & Ottenberg, T. (2024). Kriminalbeamte: Das Sicherheitspaket muss kommen und verschärft werden. Redaktionsnetzwerk Deutschland. rnd.de/politik/sicherheitspaket-kriminalbeamten-baldige-verabschiedung-an-Q55HVPOBFRFVTKLQM4MB-4PX33Y.html [Zuletzt geprüft am 27. Dezember 2024].

EDPB (2021). Swedish DPA: Police unlawfully used facial recognition app. European Data Protection Board. edpb.europa.eu/news/national-news/2021/swedish-dpa-police-unlawfully-used-facial-recognition-app_en [Zuletzt geprüft am 27. Dezember 2024].

EDPB (2022). Facial Recognition: Italian SA fines Clearview AI EUR 20 million. European Data Protection Board. edpb.europa.eu/news/national-news/2022/facial-recognition-italian-sa-fines-clearview-ai-eur-20-million_en [Zuletzt geprüft am 27. Dezember 2024].

EDPB(2024). Dutch Supervisory Authority imposes a fine on Clearview because of illegal data collection for facial recognition. European Data Protection Board. edpb.europa.eu/news/national-news/2024/dutch-supervisory-authority-imposes-fine-clearview-because-illegal-data_en [Zuletzt geprüft am 27. Dezember 2024].

ERPS (2021). Regulierung der Gesichtserkennung in der EU. Wissenschaftlicher Dienst des Europäischen Parlaments. [europarl.europa.eu/RegData/etudes/IDAN/2021/698021/EPRS_IDA\(2021\)698021_DE.pdf](https://europarl.europa.eu/RegData/etudes/IDAN/2021/698021/EPRS_IDA(2021)698021_DE.pdf) [Zuletzt geprüft am 27. Dezember 2024].

Hessischer Landtag (2024). Gesetz zur Modernisierung des Polizeirechts beschlossen. Land Hessen. hessen.de/presse/gesetz-zur-modernisierung-des-polizeirechts-beschlossen [Zuletzt geprüft am 27. Dezember 2024].

IMK (2024). Herbst-IMK – 80 Beschlüsse zu innenpolitischen Themen. Land Brandenburg. imk2024.brandenburg.de/imk2024/de/presse/pressemittelungen/detail/~06-12-2024-herbst-imk-80-beschluesse-zu-innenpolitischen-themen# [Zuletzt geprüft am 27. Dezember 2024].

IONOS (2024). Gesichtserkennung – Was ist Facial Recognition? ionos.de/digitalguide/websites/web-entwicklung/gesichtserkennung/ [Zuletzt geprüft am 27. Dezember 2024].

Koopmann, C. (2024). RAF-Terroristin Klette: Raus aus dem Untergrund. Süddeutsche Zeitung. [sueddeutsche.de/politik/raf-daniela-klette-berlin-garweg-staub-1.6401707?reduced=true](https://www.sueddeutsche.de/politik/raf-daniela-klette-berlin-garweg-staub-1.6401707?reduced=true) [Zuletzt geprüft am 27. Dezember 2024].

Krempf, S. (2022). Überwachung: Clearview AI will Datenbank mit 100 Milliarden Gesichtsfotos füllen. heise online. [heise.de/news/Überwachung-Clearview-peilt-Datenbank-mit-100-Milliarden-Gesichtsfotos-an-6491056.html](https://www.heise.de/news/Überwachung-Clearview-peilt-Datenbank-mit-100-Milliarden-Gesichtsfotos-an-6491056.html) [Zuletzt geprüft am 27. Dezember 2024].

Kristofski, A., Boch, B., Böhnke, M. (2024). Täter ist auf der Flucht: Stadtjubiläum: Mindestens drei Tote bei Anschlag auf dem Fronhof. Solinger Tageblatt. [solinger-tageblatt.de/lokales/solingen/anschlag-in-solingen-mindestens-drei-tote-bei-messerangriff-auf-stadtfestival-INBGJVQ2DZCDNMZCAGF2NIZLI4.html](https://www.solinger-tageblatt.de/lokales/solingen/anschlag-in-solingen-mindestens-drei-tote-bei-messerangriff-auf-stadtfestival-INBGJVQ2DZCDNMZCAGF2NIZLI4.html) [Zuletzt geprüft am 27. Dezember 2024].

MDR Sachsen-Anhalt (2024). Anschlag in Magdeburg: Eine Stadt trauert. MDR. [mdr.de/nachrichten/sachsen-anhalt/magdeburg/magdeburg/liveticker-anschlag-weihnachtsmarkt-magdeburg-110.html](https://www.mdr.de/nachrichten/sachsen-anhalt/magdeburg/magdeburg/liveticker-anschlag-weihnachtsmarkt-magdeburg-110.html) [Zuletzt geprüft am 27. Dezember 2024].

Monroy, M. (2021). Gesichtserkennung: Polizei verdoppelt Zahl identifizierter Personen jährlich. Netzpolitik.org. [netzpolitik.org/2021/gesichtserkennung-polizei-verdoppelt-zahl-identifizierter-personen-jaehrlich/](https://www.netzpolitik.org/2021/gesichtserkennung-polizei-verdoppelt-zahl-identifizierter-personen-jaehrlich/) [Zuletzt geprüft am 27. Dezember 2024].

Monroy, M (2024). Neues BKA-System: Polizeiliche Gesichtserkennung geht steil. Netzpolitik.org. [netzpolitik.org/2024/neues-bka-system-polizeiliche-gesichtserkennung-geht-steil/?utm_source=chatgpt.com#netzpolitik-pw](https://www.netzpolitik.org/2024/neues-bka-system-polizeiliche-gesichtserkennung-geht-steil/?utm_source=chatgpt.com#netzpolitik-pw) [Zuletzt geprüft am 27. Dezember 2024].

Statistisches Bundesamt (2023a). Bevölkerung: Bevölkerungsstand. Destatis. [destatis.de/DE/Themen/Gesellschaft-Umwelt/Bevoelkerung/Bevoelkerungsstand/_inhalt.html](https://www.destatis.de/DE/Themen/Gesellschaft-Umwelt/Bevoelkerung/Bevoelkerungsstand/_inhalt.html) [Zuletzt geprüft am 27. Dezember 2024].

Statistisches Bundesamt (2023b). Bevölkerung: Migration und Integration. Destatis. [destatis.de/DE/Themen/Gesellschaft-Umwelt/Bevoelkerung/Migration-Integration/_inhalt.html](https://www.destatis.de/DE/Themen/Gesellschaft-Umwelt/Bevoelkerung/Migration-Integration/_inhalt.html) [Zuletzt geprüft am 27. Dezember 2024].

Zeit Online (2024). Kritik an entschärftem Sicherheitspaket der Ampel. Zeit Online. [zeit.de/politik/deutschland/2024-10/sicherheitspaket-migration-ampel-koalition-anpassungen-kritik](https://www.zeit.de/politik/deutschland/2024-10/sicherheitspaket-migration-ampel-koalition-anpassungen-kritik) [Zuletzt geprüft am 27. Dezember 2024].

Gemeinsamkeiten und Unterschiede der Datenschutz-Folgenabschätzung (DSFA) gem. Art. 35 DSGVO und der Grundrechte-Folgenabschätzung (GFA) gem. Art. 27 KI-Verordnung

Simon Kraft

Die rasante Entwicklung und der zunehmende Einsatz von Technologien im Bereich der Künstlichen Intelligenz (KI) haben sowohl große Chancen als auch erhebliche Risiken mit sich gebracht. Die Europäische Kommission erkannte die Notwendigkeit, ein Gleichgewicht zwischen der Förderung von Innovationen und dem Schutz der Bürger vor potenziellen negativen Auswirkungen von KI zu finden. Ohne klare Regelungen bestand die Gefahr, dass KI-Systeme in Bereichen eingesetzt werden, die das Risiko von Grundrechtsverletzungen, Diskriminierung und sozialer Ungleichheit erhöhen. Daher entwickelte die Europäische Kommission die sogenannte KI-Verordnung, die darauf abzielt, Transparenz, Sicherheit und Verantwortlichkeit im Umgang mit KI zu gewährleisten (Europäische Kommission, 2021, S. 1 ff.).

Am 21. Mai 2024 nahm der Europäische Rat die KI-VO offiziell an. Am 12. Juli 2024 wurde es im Gesetzesblatt der EU veröffentlicht und trat zum 01. August 2024 in Kraft (Future of Life Institute, 2024). Die KI-VO ist umfassend und deckt verschiedene Aspekte des Einsatzes von KI-Systemen ab. Das zentrale Merkmal der Verordnung ist die risikobasierte Klassifizierung von KI-Systemen (Rockenschaub 2023, S. 24). Diese Klassifizierung teilt KI-Anwendungen in vier Kategorien ein: verbotene KI, hochriskante KI, KI mit begrenzten Risiken und KI mit geringen Risiken (Dahm und Twesten, 2023, S. 16).

Besondere Aufmerksamkeit in der Verordnung wird der Kategorie der hochriskanten KI-Systeme gewidmet. Diese Systeme haben potenziell erhebliche Auswirkungen auf das Leben und die Rechte von Menschen. Hochrisiko-KI umfasst Anwendungen in unterschiedlichsten Bereichen. KI-Systeme in diesen Bereichen unterliegen strengen Anforderungen und müssen ein Konformitätsbewertungsverfahren durchlaufen. Anbieter solcher Systeme müssen nachweisen, dass ihre KI-Lösungen sicher sind, und dies auch über den Lebenszyklus

lus einer KI hinweg bewerten. Im Abschnitt II der KI-VO werden die umfassenden Reglementierungen zu Hochrisiko-KI aufgeführt. So müssen ein Risikomanagementsystem eingeführt werden, Risiken bewertet, Risikomanagementmaßnahmen definiert sowie eine Vielzahl an Dokumentationspflichten und technischen Beschreibungen erfüllt werden (Dahm und Twesten, 2023, S. 17 ff.)

Außerdem muss gemäß Art. 27 KI-VO auch eine Grundrechte-Folgenabschätzung (GFA) für Hochrisiko-KI-Systeme vorgenommen werden. Grundsätzlich bleiben die bestehenden Regelungen zum Datenschutz, also insbesondere auch die DSGVO, von der KI-VO unberührt (Art. 2 Abs. 7 KI-VO; Kugelmann, 2024, S. 497). Beide Rechtsvorschriften teilen das Ziel, den Schutz der Grundrechte der EU-Bürger zu gewährleisten (Art. 1 Abs. 1 KI-VO; Art. 1 Abs. 2 DSGVO). Neben der genannten Grundrechte-Folgenabschätzung gemäß Art. 27 KI-VO ist auch nach Artikel 35 DSGVO eine Folgenabschätzung durchzuführen. Dabei handelt es sich um die Datenschutz-Folgenabschätzung (DSFA).

Mit dem vorliegenden Beitrag soll untersucht werden, wie eine DSFA angepasst werden muss, damit eine GFA mit allen Vorgaben integriert werden kann. Durch die Analyse der Artikel 27 KI-VO und 35 DSGVO soll ein Grundstein dafür gelegt werden. Die inhaltlichen Vorgaben dieser Artikel sollen unter Hinzuziehung kontextueller Erkenntnisse analysiert, verglichen sowie Gemeinsamkeiten und Unterschiede herausgearbeitet werden.

Hintergrund

Bei der KI-VO handelt es sich um eine Verordnung der Europäischen Union (Europäische Kommission, 2021, S. 1). Dadurch entfaltet die KI-VO eine bedeutende rechtliche Bindungswirkung für die Mitgliedstaaten. Als Verordnung stellt sie eine verbindliche Rechtsnorm dar, die unmittelbar in allen Mitgliedstaaten gilt, ohne dass es einer weiteren Umsetzung in nationales Recht bedarf. Dies unterscheidet sie von Richtlinien, die von den Mitgliedstaaten erst in nationales Recht umgesetzt werden müssen (Art. 288 AEUV).

Die Verordnung verpflichtet die Mitgliedstaaten, die in ihr festgelegten Vorschriften unmittelbar anzuwenden. Dies bedeutet auch, dass die Mitgliedstaaten sicherstellen müssen, dass die Anforderungen der Verordnung eingehalten werden. Dazu sollen nationale Aufsichtsbehörden geschaffen werden, die die Einhaltung der Verordnung überwachen (Europäische Kommission, 2021, S. 17; Art. 70 KI-VO). Bei Verstößen gegen die Verordnung drohen erhebliche Sanktionen, die je nach Schwere des Verstoßes bis zu 7 % des weltweiten Jahresumsatzes eines Unternehmens betragen können (Art. 99 Abs. 3 KI-VO).

Überschneidungen zwischen DSGVO und KI-VO

Durch das Inkrafttreten der KI-VO bestehen Harmonisierungserfordernisse zu bereits bestehenden Rechtsvorschriften wie der DSGVO. Überschneidung sind denkbar, sobald KI-Systeme betrachtet werden, die personenbezogene Daten verarbeiten. Sowohl die KI-VO als auch die DSGVO legen strenge Anforderungen an die Verarbeitung dieser Daten fest. Während die DSGVO den rechtlichen Rahmen für die Verarbeitung personenbezogener Daten definiert und Prinzipien wie Zweckbindung, Datenminimierung und Transparenz vorschreibt (Art. 5 DSGVO), verweist auch die KI-VO in Artikel 10 auf Datenqualität sowie in Artikel 13 auf die Informationspflicht von betroffenen Personen.

Kugelmann (2024, S. 498 f.) führt aus, dass bei KI-Systemen, die personenbezogene Daten verarbeiten, die Vorschriften der DSGVO einzuhalten sind. So muss für jeden Datenverarbeitungsprozess des KI-Systems eine Rechtsgrundlage gem. Art. 6 DSGVO vorliegen. Die Vorgaben zu Fairness und Transparenz, also insbesondere ein Verbot von Diskriminierung und umfassende Dokumentationspflichten, sind einzuhalten. Weiterhin muss der Verantwortliche für das KI-System erklärbar machen, was mit personenbezogenen Daten innerhalb des Systems passiert, um seinen Rechenschaftspflichten gegenüber den Aufsichtsbehörden nachkommen zu können (ebd.).

Die KI-VO ist ein komplexes Rechtskonstrukt, das Anbieter, Betreiber oder Verantwortliche von KI-Systemen vor Herausforderungen stellt, den gesetzlichen Reglementierungen zu entsprechen. Da es zu

der DSGVO bereits umfangreiche Rechtsprechung und praktische Erfahrungen gibt, können diese als wichtige Anknüpfungspunkte dienen (Kugelmann, 2024, S. 501). Der Landesdatenschutzbeauftragte von Bayern (Bayerischer Landesdatenschutzbeauftragter, 2024) wie auch Keber et al. (2024, S. 522) erkennen ebenfalls zwischen der KI-VO und der DSGVO Überschneidungen und Synergieeffekte.

Überschneidungen zwischen DSFA und GFA

Die Grundrechte-Folgenabschätzung gemäß Artikel 27 der KI-VO ist ein zentrales Instrument, das von Anbietern hochriskanter KI-Systeme durchgeführt werden muss. Diese Folgenabschätzung zielt darauf ab, potenzielle Risiken für Grundrechte wie das Recht auf Privatsphäre, Nichtdiskriminierung, freie Meinungsäußerung und den Schutz personenbezogener Daten frühzeitig zu identifizieren und zu minimieren. Anbieter und Bereitsteller sind zur Risikominimierung verpflichtet (Art. 27 KI-VO; Erwägungsgründe 93, 96 zur KI-VO).

Die Datenschutz-Folgenabschätzung gemäß Art. 35 DSGVO ist dann durchzuführen, wenn ein hohes Risiko besteht, dass Rechte und Freiheiten von Personen durch die Verarbeitung ihrer Daten betroffen sein könnten. Auch die DSFA stellt spezifische Anforderungen an die Verarbeitungsprozesse von personenbezogenen Daten. Der Verantwortliche soll die Risiken für die betroffenen Personen abschätzen und Maßnahmen zur Risikominimierung identifizieren (Art. 35 DSGVO; Friedewald et al., 2016, S. 16). Aus der DSGVO ergeben allgemeine Anforderungen an eine DSFA. Hierbei werden keine Vorgaben zur tatsächlichen praktischen Umsetzung hinsichtlich der konkreten inhaltlichen und organisatorischen Ausgestaltung einer DSFA vorgegeben (Friedewald et al., 2016, S. 15; Aden und Fährmann, 2020, S. 26).

Wird nun ein neues KI-System, welches als Hochrisiko-KI eingestuft wird und bei dem personenbezogene Daten gemäß Art. 35 DSGVO verarbeitet werden, entwickelt und anschließend eingesetzt, bleiben die Vorgaben der DSGVO neben den neuen Vorgaben aus der KI-VO bestehen. Eine DSFA ist nach den Vorgaben des Art. 35 DSGVO durchzuführen. Aus Art. 27 Abs. 4 KI-VO geht hervor, dass bei der Verpflichtung zur Erstellung einer GFA diese lediglich eine bestehende

DSFA ergänzen muss. Mithilfe dieser Regelung versucht der Gesetzgeber offensichtlich, die KI-VO mit der DSGVO zu harmonisieren. Es ist abzusehen, dass es aufgrund konkreter praktischer Vorgaben zur Durchführung einer DSFA zu komplexen Synchronisationsüberlegungen kommen muss, um eine rechtskonforme Integration der GFA in eine DSFA zu gewährleisten. Gelingt eine Integration der GFA in die DSFA, ergeben sich Synergieeffekte.

Methodik

Die qualitative Inhaltsanalyse stellt eine systematische Methode zur Bearbeitung von Kommunikationsmaterial dar, die darauf abzielt, Forschungsfragen zu beantworten. Als Kommunikationsmaterial kann verschiedenstes Material wie Texte, Bilder, Musik oder Ähnliches herangezogen werden und einer regelgeleiteten und systematischen Analyse unterzogen werden (Mayring, 2022, S. 11 f.). Der Prozess der qualitativen Inhaltsanalyse umfasst mehrere grundlegende Schritte. Zunächst wird das zu analysierende Material ausgewählt und die Richtung der Analyse festgelegt. Anschließend wird die spezifische Form der Inhaltsanalyse bestimmt, gefolgt von der Interpretation der Ergebnisse (Mayring, 2022, S. 49 ff.).

Neben den Inhalten, die aus dem Untersuchungsmaterial zu entnehmen sind, sollen auch kontextuale Zusammenhänge einbezogen werden und dadurch latente Inhalte analysiert werden (Kuckartz und Rädiker, 2022, S. 38 f.). Ein zentrales Instrument der qualitativen Inhaltsanalyse stellt die Kategorienbildung dar. Die Kategorien können unterschiedlichste Ausprägungen aufweisen. So können Kategorien aus bestimmten Themenbereichen bestehen, denen bestimmte Aussagen, Argumente oder Regelungen zugeordnet werden können. Außerdem können Kategorien in ihrer Ausprägung bezogen auf Komplexität, Abstraktion oder Bedeutung erheblich variieren (Kuckartz und Rädiker, 2022, S. 53 ff.).

Es wird zwischen der Methode der deduktiven und der induktiven Kategorienbildung unterschieden. Bei der deduktiven Kategorienbildung werden die Kategorien unabhängig von dem zu analy-

sierenden Material entwickelt. Dazu werden verschiedene Quellen herangezogen, wie beispielsweise bereits bestehende Theorien, Forschungsstände oder Alltagswissen (Kuckartz und Rädiker, 2022, S. 70 ff.). Die induktive Kategorienbildung wird oft in der qualitativen Forschung angewandt und entwickelt sich aus dem Untersuchungsmaterial selbst. Um Kategorien aus dem Material selbst abzuleiten, sollte der vorliegende Text vollständig abgearbeitet werden. Daraus sollten je nach Forschungsfrage und Zielrichtung Kategoriearten wie beispielsweise thematische Kategorien identifiziert werden. Wurden erste Kategorien entwickelt sind, im Folgenden Textabschnitte mit diesen abzugleichen. Entweder diese können anhand bereits entwickelter Kategorien kodiert werden oder es müssen neue Kategorien abgeleitet werden. Ob Kategorien noch zusammengefasst oder weiter differenziert werden müssen, sind individuelle Überlegungen, die von vielen Kriterien wie beispielsweise der Forschungsfrage oder der zur Verfügung stehenden Zeit abhängig zu betrachten sind (Kuckartz und Rädiker, 2022, S. 82 ff.).

Um eine qualitative Inhaltsanalyse nachvollziehbar und auch für Außenstehende interpretierbar zu machen, bedarf es eines Kategorienhandbuchs und eines Kodierleitfadens. Dem Kategorienhandbuch sind die Kategorien selbst, aber vor allem auch deren Definitionen zu entnehmen. Durch die Definition von Kategorien wird zum einen verständlich gemacht, weshalb Zuordnungen zu diesen Kategorien erfolgten. Zum anderen wird dadurch demjenigen, der die Zuordnung oder das Kodieren durchführt, verdeutlicht, welche Kategorie für was genau steht. Mithilfe des Kodierleitfadens können weitere Regelungen für den Kodierprozess festgelegt werden, mit denen präzisiert wird, wann und warum bestimmte Textpassagen einer spezifischen Kategorie zugeordnet werden. (Kuckartz und Rädiker, 2022, S. 65 ff.). Hierbei können sich auch Zuordnungsregeln anbieten, um inhaltlich ähnliche Kategorien hinsichtlich ihrer Ausprägungen deutlicher voneinander unterscheidbar zu machen (Mayring, 2022, S. 60 ff.).

Ergebnisse

Im vorliegenden Beitrag wurden die Kategorien induktiv aus dem Artikel 27 KI-VO abgeleitet. Hierzu wurden zunächst insgesamt 17 relevante Textpassagen herausgearbeitet. Diese werden nachfolgend als Items bezeichnet. Die Items sind direkte Zitate oder kurze Zusammenfassungen eines Absatzes oder Satzes des Artikel 27 KI-VO, ohne an inhaltlicher Aussagekraft einzubüßen. Um diese Items zu ordnen, wurden fünf Kategorien entwickelt, denen diese 17 Items zugeordnet werden konnten. Anschließend wurde der Art. 35 DSGVO analysiert. Dabei konnten ebenfalls 17 relevante Items identifiziert und diese anschließend den bereits erstellten Kategorien zugeordnet werden. Dass aus beiden Artikeln jeweils 17 Items herausgearbeitet wurden, war Zufall. Die Entwicklung der Kategorien und deren Definitionen und die Erstellung des Kodierleitfadens mit der Formulierung von Kodierregeln und Zuordnungsregeln erfolgte in einem zirkulären Verfahren.

Im nächsten Schritt wurden die identifizierten Items innerhalb der Kategorien inhaltlich gegenübergestellt und analysiert. Die inhaltliche Interpretation der Items innerhalb der fünf Kategorien erfolgte unter Hinzuziehung weiterer Erkenntnisquellen und geht daher über eine rein wortgetreue Analyse der Items hinaus. Dazu wurden weitere Quellen, Erwägungsgründe zu den Gesetzestexten und ein Musterbeispiel einer Datenschutz-Folgenabschätzung genutzt. Jedes Item wurde katalogisiert. Bei Item A.1.1 handelt es sich beispielsweise um „KI-Systeme mit hohem Risiko“.

Bei der Kategorie A handelt es sich um die Anwendungsvoraussetzungen der beiden Artikel, unter welchen Voraussetzungen und zu welchem Zeitpunkt also eine GFA oder eine DSFA durchgeführt werden muss. Aus Art. 27 KI-VO wurden hierzu die beiden Items A.1.1 und A.1.2 extrahiert, aus Art. 35 DSGVO die Items A.2.1 bis A.2.4. Item A.1.1 benennt KI-Systeme mit hohem Risiko. Es sind gemäß Art. 6 Nr. 1 a, b KI-VO sowie gemäß Anhang III Nr. 2 KI-VO Hochrisiko-KI-Systeme denkbar, die keine personenbezogenen Daten (pbD) verarbeiten. Ein Großteil der in Anhang III KI-VO genannten Anwendungsfelder von KI-Systemen dürfte allerdings pbD verarbeiten. Hierunter fallen

Systeme, mit denen biometrische Daten verarbeitet werden oder die im Bereich der Bildung, Beschäftigung, Strafverfolgung, Migration oder Rechtspflege eingesetzt werden. Prüft ein KI-System beispielsweise Asylanträge, greift es dabei unweigerlich auf personenbezogenen Daten von natürlichen Personen zurück und verarbeitet diese.

In diesem Zusammenhang müssen Items A.2.1 bis A.2.4 abgeglichen werden. A.2.1 spricht von „hohem Risiko für Rechte und Freiheiten natürlicher Personen“, was unter Hinzuziehung der Ausführungen der Artikel-29-Datenschutzgruppe (Datenschutzgruppe nach Artikel 29, 2017, S. 10 ff.) den Erläuterungen zu A.1.1 entspricht, soweit pbD verarbeitet werden. A.2.2 bis A.2.4 nennen weitere Voraussetzungen, in welchen Fällen eine DSFA durchgeführt werden muss. Item A.2.2 entspricht teilweise den Ausführungen zu Systemen gem. Anhang III Nr. 7, 8 KI-VO. Item A.2.3 verweist auf besondere Kategorien pbD wie Daten zu Ethnie, politischer Meinung, Religion oder Gewerkschaftszugehörigkeit (Art. 9 DSGVO) oder Daten zu strafrechtlichen Verurteilungen (Art. 10 DSGVO). Item A.2.4 zielt auf die Überwachung öffentlicher Bereiche. Würden entsprechende pbD durch Hochrisiko-KI-Systeme verarbeitet oder Hochrisiko-KI-Systeme zur Überwachung öffentlicher Bereiche eingesetzt, müsste neben einer GFA auch eine DSFA durchgeführt werden.

Item A.1.2 fordert die Erstellung einer GFA vor dem ersten Einsatz eines Hochrisiko-KI-Systems. Eine explizite zeitliche Komponente wird in Art. 35 DSGVO nicht genannt. Allerdings kann man aus dem Wort „Abschätzung“ aus Datenschutz-Folgenabschätzung ableiten, dass eine solche ebenfalls vor der Anwendung eines Daten-Verarbeitungsprozesses durchgeführt werden muss. Ziel der DSFA ist die Risikoeinschätzung hinsichtlich des Daten-Verarbeitungsprozesses. Liegt eine DSFA nicht vor, könnten die Daten rechtswidrig verarbeitet werden (BfDI – Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, 2020, S. 13). Auch deshalb sollte eine DSFA unbedingt vor dem erstmaligen Verarbeitungsprozess durchgeführt werden.

Bei der Kategorie B wird der Frage nachgegangen, wer für die Durchführung einer GFA und DSFA verantwortlich ist. Während der „Anbieter“ (Item B.1.1) ein KI-System für allgemeine Zwecke entwickelt

oder entwickeln lässt und es dann unter eigenem Namen in Verkehr bringt oder in Betrieb nimmt, setzt ein „Bereitsteller“ (Item B.1.2) das KI-System unter seiner eigenen Aufsicht ein (Art. 3 Abs. 3, 4 KI-VO). Der Bereitsteller muss die GFA durchführen, kann aber auf bereits durchgeführte Folgenabschätzungen des Anbieters aufbauen (Art. 27 KI-VO). Bei ihm liegt aber eine besondere Verantwortung, da nur er den Einsatz der KI in einem konkreten Fall ausreichend beurteilen kann (Erwägungsgrund 93 zu Art. 27 KI-VO).

Der „Verantwortliche“ (Item B.2.1) ist derjenige, der laut Art. 4 Nr. 7 DSGVO „über die Zwecke und Mittel der Verarbeitung von pbD entscheidet“. Die Definitionen aus der KI-VO und der DSGVO deuten darauf hin, dass derjenige, der letztendlich ein entsprechendes KI-System tatsächlich nutzt, auch eine GFA bzw. eine DSFA durchführen beziehungsweise für den konkreten Anwendungsfall fortführen muss.

Die Kategorie C erweitert die Analyse um kontextuelle Bezüge. Was sind die Gründe für die Erstellung einer GFA oder DSFA, was sind die tatsächlichen Zweckrichtungen und wer soll durch die Erstellung geschützt werden? Item C.1.1 nimmt die Auswirkungen eines KI-Systems auf die Grundrechte in den Blick, während Item C.2.1 die Auswirkungen der Folgen eines Verarbeitungsprozesses für pbD fokussiert.

Laut Art. 1 KI-VO soll „ein hohes Schutzniveau in Bezug auf Gesundheit, Sicherheit und die in der Charta verankerten Grundrechte“ gewährleistet werden. Insbesondere dürften hier das Recht auf Privatsphäre (Art. 7 GRCh), Recht auf Datenschutz (Art. 8 GRCh), Recht auf Nicht-Diskriminierung (Art. 21 GRCh), Recht auf Meinungs- und Informationsfreiheit (Art. 11, GRCh), Recht auf effektiven Rechtsschutz (Art. 47 GRCh) und das Recht auf körperliche Unversehrtheit (Art. 3 GRCh) eine gewichtige Rolle spielen. Bei der Bewertung von Verarbeitungsprozessen von pbD muss bewertet werden, welche Gefahren für natürliche Personen bestehen, wenn Daten zu ihrer Person verloren gehen, unrechtmäßig abfließen oder öffentlich werden. Somit sind auch hier die genannten Grundrechte zu berücksichtigen. In der Muster-DSFA des BfDI (2020, S. 5) sind die betroffenen Rechte und Freiheiten auch zu benennen. Bei der GFA müssen die betroffenen Personen und Gruppen identifiziert werden (Item C.1.2),

während Item C.2.2 den Schutz von pbD fordert. Eine entsprechende Identifizierung ist auch im Rahmen der Erstellung einer DSFA notwendig, um den Schutz von pbD zu gewährleisten (BfDI, 2020, S. 3).

Kategorie D konnten mit jeweils acht Items die meisten Items zugeordnet werden. Hier sollen die spezifischen Anforderungen an eine GFA und eine DSFA verglichen werden. Items D.1.1 und Item D.2.1 fordern jeweils eine Verfahrensbeschreibung. Weiterhin wird eine Beschreibung der Zweckrichtung gefordert. Bei der Beschreibung des Zwecks eines Hochrisiko-KI-Systems, welches pbD verarbeitet, dürfte auch immer der Zweck der Verarbeitung der pbD einfließen.

Auch die Items D.1.3 und D.2.3, bei denen die Schadensrisiken für betroffene Personen und somit mögliche Auswirkungen auf deren Rechte und Freiheiten abgeschätzt werden sollen, überlagern sich GFA und DSFA. Werden Risiken festgestellt, verlangen GFA und DSFA die Entwicklung von technisch-organisatorischen Maßnahmen zur Eindämmung dieses Risikos (Item D.1.5 und Item D.2.4).

Hinsichtlich etwaiger Verweismöglichkeiten kann bei der Erstellung einer GFA auf eine bestehende GFA des Anbieters (Item D.1.8) und bei der DSFA auf eine gegebenenfalls bestehende allgemeine DSFA (Item D.2.7) aufgebaut werden. Vor Erstellung einer DSFA soll eine Vorprüfung erfolgen (Item D.2.8). Vor Erstellung einer GFA sollte insbesondere geprüft werden, ob Integrationsmöglichkeiten mit einer DSFA bestehen (Item D.1.7). Hier hat der Gesetzgeber ausdrücklich eine normierte Zusammenführung von DSFA und GFA ermöglicht.

In der Kategorie D werden aber auch Unterschiede im Bereich der inhaltlichen Anforderungen an eine GFA und eine DSFA sichtbar. So sollen in der GFA die Häufigkeit und der Zeitraum des Einsatzes des KI-Systems (Item D.1.2) prognostiziert und menschliche Überwachungskomponenten (Item D.1.4) sowie interne Steuerungs- und Beschwerdemechanismen (Item D.1.6) implementiert werden. Item D.1.2 könnte im weitesten Sinne die Prüfung des Umfangs der Datenverarbeitung gemäß der Muster-DSFA des BfDI (2020, S. 2) zugeordnet werden. Allerdings wird hier explizit keine zeitliche Angabe gefordert. Auch die DSFA enthält in Kategorie D Anforderungskriterien

en, die so nicht in der GFA abgebildet sind. Dabei handelt es sich um die Prüfung der Verhältnismäßigkeit und der Notwendigkeit (Item D.2.2), die Prüfung der Einhaltung der Verhaltensregeln gemäß Art. 40 DSGVO (Item D.2.5) und die Einholung des Standpunktes von Betroffenen (Item D.2.6).

Kategorie E umfasst letztlich die Regelungen zu GFA und DSFA hinsichtlich der Verpflichtungen und Reglementierungen nach Durchführung der Folgenabschätzung. Beide Folgenabschätzungen fordern eine fortlaufende Prüfung und Aktualisierung, wenn Änderungen auftreten (Item E.1.1 und Item E.2.2). Item E.1.2 und E.1.3 regeln die Verpflichtung zur Vorlage der GFA bei der Überwachungsbehörde beziehungsweise Ausnahmeregelungen dazu. Für KI-Systeme werden unterschiedliche Aufsichtsbehörden in Abhängigkeit von der Risikostufe des KI-Systems und deren Einsatzbereich zuständig sein (BfDI – Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, 2024). Die DSFA hingegen verlangt nur die Einbindung des Datenschutzbeauftragten (Item E.2.1). Gemäß Art. 36 DSGVO muss die Aufsichtsbehörde nur konsultiert werden, wenn ein hohes Risiko der Verarbeitung besteht und die geplanten Maßnahmen keinen ausreichenden Schutz ausstrahlen.

Diskussion

Der Vergleich zwischen dem bereits bestehenden Instrument der DSFA aus der DSGVO und der neu implementierten GFA der KI-VO anhand einer qualitativen Inhaltsanalyse hat deutliche Überschneidungen aufgezeigt. Insbesondere die Zweckrichtung, also der Schutz von Betroffenen und deren Grundrechten, ist bei beiden Instrumenten ähnlich, obwohl die DSFA dies immer in Beziehung mit der Verarbeitung von pD setzt.

Die wenigen Unterschiede zwischen GFA und DSFA lassen sich insbesondere bei den Anforderungen an die inhaltliche Ausgestaltung der beiden Folgenabschätzungen feststellen. Im Hinblick auf die Beantwortung der Forschungsfrage konnte durch die Analyse aber aufgezeigt werden, dass die DSFA in ihrer jetzigen Form und unter

Heranziehung der Muster-DSFA des BfDI lediglich um die folgenden drei inhaltlichen und einen organisatorischen Baustein erweitert werden muss:

- Abschätzung der Häufigkeit und des Zeitraums des Einsatzes des KI-Systems
- Planung einer menschlichen Überwachungskomponente für das KI-System
- Planung interner Steuerungsregel und Beschwerdemechanismen
- Vorlage bei der zuständigen Aufsichtsbehörde

Hinsichtlich der angewandten Methodik der qualitativen Inhaltsanalyse liegen deren Stärken in ihrer Flexibilität und Anpassungsfähigkeit an verschiedene Forschungsfragen sowie in der Möglichkeit, tiefere Einblicke in komplexe Phänomene zu gewinnen (Kuckartz und Rädiker, 2022, S. 261; Mayring, 2022, S. 125 f.). Allerdings weist die qualitative Inhaltsanalyse auch mehrere Schwächen auf. Auch wenn eine systematische Analyse durchgeführt wird, bleiben die Bildung von Kategorien und die Zuordnung der Textbausteine eine interpretative Vorgehensweise der Untersuchenden (Mayring, 2022, S. 126). Außerdem wird die qualitative Inhaltsanalyse in der Regel bei Vorliegen größerer Mengen eines Ausgangsmaterials angewandt (ebd.). Auch wird die qualitative Inhaltsanalyse eher im Bereich der Sozialwissenschaften genutzt (Mayring, 2022, S. 125).

Bei der vorliegenden Untersuchung wurde lediglich jeweils ein Artikel zweier Gesetze untersucht. Allerdings war die Methodik dennoch dafür geeignet, die beiden Artikel systematisch durchzuarbeiten und auf Gemeinsamkeiten und Unterschiede zu untersuchen. Durch die Anwendung der Methodik konnte sichergestellt werden, dass beide Artikel vollständig betrachtet wurden. Allerdings könnte die Interpretation unter Hinzuziehung der rechtswissenschaftlichen Methodenlehre noch umfassender durchgeführt werden. Hier wären seitens der Untersuchenden aber auch umfassende Rechtskenntnisse notwendig.

Zu beachten war auch, dass hinsichtlich der neu eingeführten KI-VO noch wenig wissenschaftliche Arbeiten vorlagen. Meist ließen sich nur einzelne Meinungen, Interpretationen und Analysen von ausgewiesenen Rechtsexperten finden. Dies mag auch daran liegen, dass die KI-VO in der vorliegenden Version noch durch nationales Recht in Deutschland ergänzt werden könnte. Dadurch könnten sich auch noch Erweiterungen und Ergänzungen in den Vorgaben ergeben, die Auswirkungen auf die Anwendung und Durchführung einer GFA haben könnten. Zum jetzigen Zeitpunkt und bei derzeitiger Gesetzeslage erscheinen die herausgearbeiteten Gemeinsamkeiten und Unterschiede zwischen GFA und DSFA aber eine Grundlage für zukünftige Betrachtungen darzustellen.

Schlussfolgerung

Eine DSFA muss immer erstellt werden, wenn pbD verarbeitet werden. Soll nun ein als hochriskant eingestuftes KI-System genutzt werden, mit welchem auch pbD verarbeitet werden, muss zwingend für dieses System vor dessen Verwendung eine DSFA durchgeführt werden. In diesen Konstellationen erscheint es effizient, die ebenfalls durchzuführende GFA in die DSFA zu integrieren und die DSFA um die oben bereits angeführten vier Bausteine zu erweitern.

Um die herausgearbeiteten Ableitungen des vorliegenden Beitrags zu verifizieren, sollte anhand eines Hochrisiko-KI-Systems, welches pbD verarbeitet, ein Praxistest anhand der Erstellung einer erweiterten DSFA durchgeführt werden. Weiterhin sollte eine erneute vergleichende Untersuchung der GFA und der DSFA durchgeführt werden, wenn die KI-VO in nationales Recht integriert wird. Hierbei wäre auch interessant, ob das nationale Recht über die bereits hinausgehenden Anforderungen des Artikels 27 KI-VO hinausgehen wird und eine Synchronisation mit der bestehenden DSFA dann noch sinnvoll ist. Zur Absicherung der Ergebnisse sollte themenbezogene rechtswissenschaftliche Expertise hinzugezogen werden.

Literaturverzeichnis

Aden, Hartmut; Fähmann, Jan (2020): Datenschutz-Folgenabschätzung und Transparenzdefizite der Techniknutzung: Eine Untersuchung am Beispiel der polizeilichen Datenverarbeitungstechnologie. Zeitschrift für Technikfolgenabschätzung in Theorie und Praxis – TATuP 29 (3), S. 24-29. DOI: 10.14512/tatup.29.3.24.

Bayrischer Landesdatenschutzbeauftragter (2024): KI-VO und DSGVO – Spannungsverhältnis oder Synergiepotentiale? [lda.bayern.de/de/ki.html](https://www.la-datenschutz.de/de/ki.html), zuletzt geprüft am 10.09.2024.

BfDI – Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (2024): Die KI-Verordnung der EU. Online verfügbar unter [bfdi.bund.de/DE/Fachthemen/Inhalte/Technik/KI-Verordnung.html](https://www.bfdi.bund.de/DE/Fachthemen/Inhalte/Technik/KI-Verordnung.html), zuletzt geprüft am 12.09.2024.

BfDI – Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (2020): Muster mit Hinweisen für die Durchführung einer Risiko- und Datenschutzfolgenabschätzung (DSFA nach § 67 BDSG. Online verfügbar unter [bfdi.bund.de/SharedDocs/Downloads/DE/Muster/Muster_Hinweise_DSFA.pdf?__blob=publicationFile&v=7](https://www.bfdi.bund.de/SharedDocs/Downloads/DE/Muster/Muster_Hinweise_DSFA.pdf?__blob=publicationFile&v=7), zuletzt geprüft am 12.09.2024.

Dahm, Markus H.; Twesten, Niklas (2023): Der Artificial Intelligence Act als neuer Maßstab für Künstliche Intelligenz: Das Spannungsfeld zwischen Regulatorik und Unternehmen. Wiesbaden: Springer Gabler.

Datenschutzgruppe nach Artikel 29 (2017): Leitlinien zur Datenschutz-Folgenabschätzung (DSFA) und Beantwortung der Frage, ob eine Verarbeitung im Sinne der Verordnung 2016/679 „wahrscheinlich ein hohes Risiko mit sich bringt“. Online verfügbar unter [datenschutzkonferenz-online.de/media/wp/20171004_wp248_rev01.pdf](https://www.datenschutzkonferenz-online.de/media/wp/20171004_wp248_rev01.pdf), zuletzt geprüft am 08.09.2024.

Europäische Kommission (2021): Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz (Gesetz über künstliche Intelligenz) und zur Änderung bestimmter Rechtsakte der Union. 2021/0106 (COD). Hg. v. Europäische Kommission.

Friedewald, Michael; Obersteller, Hannah; Nebel, Maxi; Bieker, Felix; Rost, Martin (2016): White Paper Datenschutz-Folgenabschätzung. Ein Werkzeug für einen besseren Datenschutz. Hg. v. Peter Zoche, Regina Ammicht Quinn, Michael Friedewald, Marit Hansen, Jessica Heesen, Thomas Hess, Jörn Lamla, Christian Matt, Alexander Roßnagel, Sabine Trepte, Michael Waidner. Fraunhofer-Institut / Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein, Universität Kassel. Karlsruhe (Forum Privatheit und selbstbestimmtes Leben in der digitalen Welt).

Future of Life Institute (2024): The EU Artificial Intelligence Act. Up-to-date developments and analyses of the EU AI Act. artificialintelligenceact.eu, zuletzt geprüft am 12.09.2024.

Keber, Tobias; Iuliano, Michela; Maslewski, Daniel; Steinbrück, Anne (2024): Zur Rolle der Datenschutzbehörden bei der künftigen KI-Aufsicht. *Datenschutz und Datensicherheit – DuD*, 48 (8), S. 521-525.

Kuckartz, Udo; Rädiker, Stefan (2022): *Qualitative Inhaltsanalyse. Methoden, Praxis, Computerunterstützung*. 5. Auflage. Weinheim Basel: Beltz Juventa.

Kugelman, Dieter (2024): Scharniere zwischen DS-GVO und KI. Zum datenschutzrechtlichen Rahmen für lernende Systeme. *Datenschutz und Datensicherheit – DuD*, 48 (8), S. 496-502.

Mayring, Philipp (2022): *Qualitative Inhaltsanalyse. Grundlagen und Techniken*. 13. Auflage. Weinheim: Beltz Verlag.

Rockenschaub, Florian (2023): *Der Artificial Intelligence Act der EU*. Diplomarbeit zur Erlangung des akademischen Grades Magister der Rechtswissenschaften im Diplomstudium Rechtswissenschaften. Linz: Johannes Kepler Universität Linz.

Verzeichnis der Autorinnen und Autoren

Thomas Coldewei ist Polizeivollzugsbeamter der niedersächsischen Polizei und Masterstudent im Studiengang Öffentliche Verwaltung – Polizeimanagement an der Deutschen Hochschule der Polizei in Münster-Hiltrup.

Benjamin Coors ist Polizeivollzugsbeamter beim Bundeskriminalamt und Masterstudent im Studiengang Öffentliche Verwaltung – Polizeimanagement an der Deutschen Hochschule der Polizei in Münster-Hiltrup.

Carolina Döring ist Polizeivollzugsbeamtin der Hessischen Polizei und Masterstudentin im Studiengang Öffentliche Verwaltung – Polizeimanagement an der Deutschen Hochschule der Polizei in Münster-Hiltrup.

Christian Eggert ist Polizeivollzugsbeamter der Polizei Berlin und Masterstudent im Studiengang Öffentliche Verwaltung – Polizeimanagement an der Deutschen Hochschule der Polizei in Münster-Hiltrup.

Frank Gaiser ist Polizeivollzugsbeamter aus Baden-Württemberg und Masterstudent im Studiengang Öffentliche Verwaltung – Polizeimanagement an der Deutschen Hochschule der Polizei in Münster-Hiltrup.

Paul Haacker ist Kriminalbeamter des Bundeskriminalamts und Masterstudent im Studiengang Öffentliche Verwaltung – Polizeimanagement an der Deutschen Hochschule der Polizei in Münster-Hiltrup.

Koray Habel ist Polizeivollzugsbeamter der nordrhein-westfälischen Polizei und Masterstudent im Studiengang Öffentliche Verwaltung – Polizeimanagement an der Deutschen Hochschule der Polizei in Münster-Hiltrup.

Volker Hemmert ist Polizeivollzugsbeamter der Bayerischen Polizei und Masterstudent im Studiengang Öffentliche Verwaltung – Polizeimanagement an der Deutschen Hochschule der Polizei in Münster-Hiltrup.

Univ.-Prof. Dr. Wilfried Honekamp ist Professor für Polizeitechnik mit Schwerpunkt Digitalisierung und Leiter des Polizeitechnischen Instituts an der Deutschen Hochschule der Polizei in Münster-Hiltrup.

Christian Just ist Polizeivollzugsbeamter der Baden-Württembergischen Polizei und Masterstudent im Studiengang Öffentliche Verwaltung – Polizeimanagement an der Deutschen Hochschule der Polizei in Münster-Hiltrup.

Simon Kraft ist Polizeivollzugsbeamter der Hessischen Polizei und Masterstudent im Studiengang Öffentliche Verwaltung – Polizeimanagement an der Deutschen Hochschule der Polizei in Münster-Hiltrup.

Philipp Kreutzer ist Polizeivollzugsbeamter der Bayerischen Polizei und Masterstudent im Studiengang Öffentliche Verwaltung – Polizeimanagement an der Deutschen Hochschule der Polizei in Münster-Hiltrup.

Manuel Lubos ist Polizeivollzugsbeamter der Hessischen Polizei und Masterstudent im Studiengang Öffentliche Verwaltung – Polizeimanagement an der Deutschen Hochschule der Polizei in Münster-Hiltrup.

Uwe Marquardt ist seit 2020 Vizepräsident und seit Juli 2024 bis zu einer dauerhaften Stellenneubesetzung amtierender Präsident der Deutschen Hochschule der Polizei in Münster-Hiltrup.

Marvin Mayer ist Polizeivollzugsbeamter der Polizei des Saarlandes und Masterstudent im Studiengang Öffentliche Verwaltung – Polizeimanagement an der Deutschen Hochschule der Polizei in Münster-Hiltrup.

David Preuß ist Polizeivollzugsbeamter der sächsischen Polizei und Masterstudent im Studiengang Öffentliche Verwaltung – Polizeimanagement an der Deutschen Hochschule der Polizei in Münster-Hiltrup.

Philipp Rauthe ist Polizeivollzugsbeamter der sächsischen Polizei und Masterstudent im Studiengang Öffentliche Verwaltung – Polizeimanagement an der Deutschen Hochschule der Polizei in Münster-Hiltrup.

Lars Schröder ist Polizeivollzugsbeamter der niedersächsischen Polizei und Masterstudent im Studiengang Öffentliche Verwaltung – Polizeimanagement an der Deutschen Hochschule der Polizei in Münster-Hiltrup.

Univ.-Prof. Dr. Dr. Antonio Vera ist Professor für Organisation und Personalmanagement an sowie Dekan der Deutschen Hochschule der Polizei in Münster-Hiltrup.