Hausarbeit

Künstliche Intelligenz zur Bekämpfung von Kriminalität

Sommersemester 2022

Studiengang:	Computer Science and Media
Modul:	Aktuelle Themen: Künstliche Intelligenz – Aktueller Stand und ihre Auswirkungen auf die Zukunft
Dozent:	Prof. Dr. Andreas Koch
Datum:	16. Juli 2022
Verfasser:	Regina Dietrich

Inhaltsverzeichnis

1 Einleitung

Enorme Fortschritte im Bereich der künstlichen Intelligenz (KI) machen es möglich, verschiedenste Anwendungsgebiete zu unterstützen. Werden KI-basierte Programme darauf ausgerichtet, spezifische Aufgaben zu erledigen, können damit Ergebnisse erzielt werden, die menschlichen Fähigkeiten gleichen oder sie sogar übersteigen. Beispiele im Bereich der Sprachverarbeitung sind etwa Siri von Apple oder Alexa vom Amazon – Sprachassistenten, die in der Lage sind, Fragen zu verstehen, zu beantworten und eine ganze Reihe von Aufgaben selbständig zu erledigen. Ein weiteres großes Anwendungsgebiet ist das autonome Fahren – aber auch im Bereich von Spielen können Machine-Learning-basierte Programme mit der Leistungen von Menschen mithalten. So ist es DeepMind mit ihrem Programm *AlphaGo* bereits im März 2016 gelungen, den Gewinner 18 internationaler Titel im Spiel *Go* zu schlagen. [1, 2, 3]

Häufig werden die Begriffe *künstliche Intelligenz, Machine Learning* und *Deep Learning* synonym verwendet. Um diesbezüglich ein besseres Verständnis zu schaffen, ist in Abbildung 1 der Zusammenhang zwischen den drei Gebieten veranschaulicht: So ist *künstliche Intelligenz* ein Überbegriff über Algorithmen, die Eigenschaften von Menschen nachahmen, um Probleme auf eine Weise zu lösen,

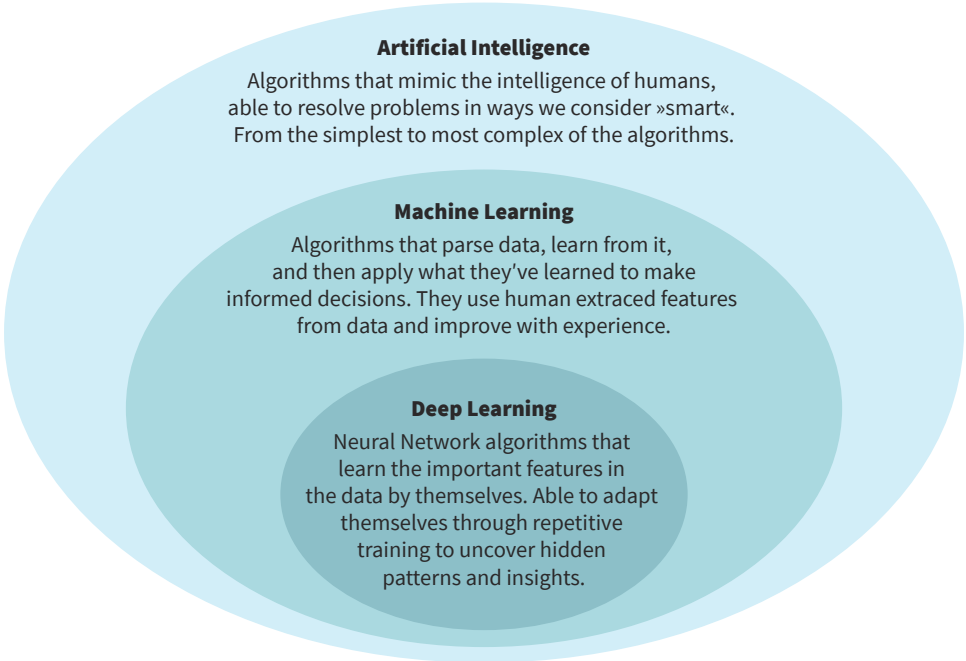

Abbildung 1: Zusammenhang zwischen künstlicher Intelligenz (Artificial Intelligence), Machine Learning und Deep Learning. Eigene Darstellung in Anlehnung an [4].

die als »intelligent« bezeichnet wird. Als *Machine Learning (ML)* wiederum wird ein Teilbereich von KI bezeichnet, bei dem Algorithmen aus Daten Muster lernen und darauf basierend Entscheidungen treffen. *Deep Learning* hingegen ist ein Teilgebiet von ML, bei welchem tiefe neuronale Netze zum Einsatz kommen. [4, 5]

Neben den oben genannten Beispielen werden KI-basierte Techniken auch in vielen anderen Bereichen eingesetzt. Eine davon ist die Bekämpfung von Kriminalität. Auf diesem Gebiet gibt es zahlreiche Herausforderungen. Dazu gehört beispielsweise das Verhindern von Straftaten, die Analyse großer Mengen Beweismaterial, die Komplexität der Ermittlungsarbeit oder auch die Notwendigkeit schneller Fortschritte. Durch ihre Fähigkeit, Muster und Zusammenhänge zu erkennen und Daten in sehr großem Umfang zu analysieren, können Methoden der künstlichen Intelligenz dort unterstützen, wo herkömmliche Techniken an ihre Grenzen stoßen. [2, 3, 6]

Im Rahmen dieser Hausarbeit soll am Beispiel verschiedener Anwendungsfälle im Bereich der Prävention und der Unterstützung aktiver Ermittlungen aufgezeigt werden, wie künstliche Intelligenz eingesetzt werden kann, um Polizeiarbeit zu unterstützen und Kriminalität zu bekämpfen – aber auch, welche Herausforderungen und Schwierigkeiten dies mit sich bringt.

2 Prävention

Ein Einsatzbereich von KI im Bereich der Bekämpfung von Kriminalität ist die Prävention. So versprechen KI-basierte Systeme, Straftaten vorherzusagen, noch ehe sie passieren. Mithilfe großer Datenmengen über vergangene Delikte werden ML-Algorithmen trainiert, um Muster zu erkennen, mit deren Hilfe Vorhersagen bezüglich zukünftiger Straftaten getroffen werden sollen. Das Ziel dieses Ansatzes ist es, die Polizeiarbeit zu unterstützen und es zu ermöglichen, basierend auf diesen Vorhersagen zu handeln und die entsprechenden Ressourcen zur rechten Zeit an der richtigen Stelle bereitzustellen. [6]

Was zunächst etwas futuristisch klingen mag, wird bereits an vielen Stellen eingesetzt. Hierfür bieten diverse Firmen Software an, die einen solchen Ansatz verfolgen. Beispiele dafür sind das in England entwickelte System HART (kurz für *Harm Assessment Risk Tool*), das Unternehmen sowie die gleichnamige Software PredPol oder die Produkte von VoyagerLabs. [2, 6, 7]

HART entstand aus der Zusammenarbeit der Polizei in Durham und Fachleuten im Bereich Computer Science. Das System, das 2017 erstmals zum Einsatz kam, soll vorhersagen, wie hoch das Risiko ist, dass ein Täter innerhalb der nächsten zwei Jahre rückfällig wird und weitere Straftaten begeht. [8]

PredPol hingegen, kurz für *Predictive Policing,* hat eine allgemeinere Ausrichtung. Das Programm nutzt ML-Algorithmen, um Vorhersagen bezüglich Art, Ort, Datum und Uhrzeit von Verbrechen zu machen. Darüber hinaus soll das System es ermöglichen, die Polizeipräsenz gezielt an risikoträchtigen Gegenden zu verstärken. [7]

Ähnliches verspricht auch die Software VoyagerCheck von VoyagerLabs. Das als Bionic 8 Analytics Ltd. registrierte Unternehmen gibt an, mithilfe seiner KI-basierten Plattformen VoyagerInsights, VoyagerAnalytics, VoyagerCheck und VoyagerVision tiefgreifende Ermittlungserkenntnisse über Unternehmen, Personen, Gruppen und Themen gewinnen zu können. Auf diese Weise soll etwa organisiertes Verbrechen, Terrorismus und Schwarzhandel bekämpft werden können. [9]

Neben all den Vorteilen, die die aufgezählten Systeme zu haben scheinen, gibt es jedoch auch Schattenseiten. Experten kritisieren, dass Unternehmen wie VoyagerLabs häufig Buzzwords wie »künstliche Intelligenz« und »Algorithmen« verwenden, wenn es darum geht, ihre Vorgehensweise zu erklären, anstatt die Funktionsweise ihrer Technologien konkreter zu erläutern. [10]

Dokumente, die auf Anfrage einer Non-Profit-Organisation erlangt wurden, legen nahe, dass VoyagerLabs sich zum Teil einer ganzen Reihe ethisch fragwürdiger Strategien zur Erreichung seiner Ziele bedient – und es besteht sogar der Verdacht auf Verletzung von Grundrechten. Die Strategie des Un-

ternehmens beinhaltet das Sammeln immenser Mengen an Daten aus allen Arten von Social-Media-Auftritten – das beinhaltet u. a. Posts, Bilder, Status-Updates, Geotags und vieles mehr. Dieselben Informationen werden auch über Personen aus Freundeslisten und wiederum deren Kontakte gesammelt. Auch Inhalte, die nach einer Weile verändert oder gelöscht werden, bleiben bei VoyagerLabs archiviert. Darüber hinaus werden Fake-Profile eingesetzt, um etwa Zugang zu Gruppen oder privaten Social-Media-Profilen zu bekommen. [10]

Ein weiterer Punkt ist, dass präventive Systeme häufig im Verdacht stehen, Probleme mit Voreingenommenheit zu haben bzw. diese zu reproduzieren. Der Grund dafür ist, dass Menschen dunkler Hautfarbe häufiger für ein Verbrechen angezeigt werden als weiße. Wenn also ML-basierte Algorithmen mit Daten aus vergangenen Delikten trainiert werden, um darin Muster zu erkennen und diese auf neue Fälle zu übertragen, dann kann sich diese Ungleichheit in mit Stigmatisierung behafteten Vorhersagen niederschlagen. So ergab sich aus Untersuchungen der Non-Profit-Organisation Propublica, dass ein in den USA eingesetztes Tool – welchem bei der Entscheidung über ein Urteil durchaus Bedeutung zugemessen wird – dunkelhäutige Menschen fast doppelt so oft irrtümlicherweise als rückfällig einstuft wie weiße. [11]

Viele Polizeidienststellen, die sich solcher Software bedienen – wie etwa das Los Angeles Police Department (LAPD) – sind aus den oben genannten Gründen auch öffentlicher Kritik ausgesetzt. Dennoch ist die Bereitschaft häufig gering, auf den Einsatz solcher Systeme zu verzichten – auch wenn es bislang nur wenig Beweise dafür gibt, dass sie tatsächlich zur Verringerung der Kriminalität beitragen. [10]

3 Unterstützung aktiver Ermittlungen

Neben den präventiven Ansätzen gibt es auch zahlreiche Möglichkeiten, künstliche Intelligenz auf andere Weise zur Unterstützung von Ermittlungen einzusetzen. Im Folgenden werden drei Anwendungsbereiche vorgestellt.

3.1 Bild- und Videoerkennung

Ein weiterer großer Punkt, an dem ML-basierte Techniken ansetzen, ist die Bild- und Videoerkennung. Mit bildverarbeitenden Methoden ist es etwa möglich, Gesichter zu identifizieren und mit polizeilichen Datenbanken abzugleichen – das vereinfacht und beschleunigt die Analyse großer Mengen Bild-Videomaterial enorm. [2]

Das Polizeipräsidium Mannheim beispielsweise setzt seit Ende 2018 eine sogenannte algorithmenbasierte Videoerkennung ein. Die Software entstand aus der Zusammenarbeit der Stadt, des Landes Baden-Württemberg und des Fraunhofer Instituts für Optronik, Systemtechnik und Bildauswertung (IOSB). Mit der polizeilichen Nutzung dieser Technik ist Baden-Württemberg europaweit Vorreiter. Besonders an diesem System ist, dass nicht auf Basis von Gesichtserkennung gearbeitet, sondern das Videomaterial automatisch hinsichtlich verschiedener Bewegungs- und Verhaltensmuster analysiert wird, die auf Straftaten hindeuten – wie etwa Treten oder Schlagen. Damit sollen gefährliche Situation frühzeitig erkannt und ein schnelles Einschreiten ermöglicht werden. [12]

Ein Unternehmen, das jedoch durchaus mit Gesichtserkennung arbeitet, ist Clearview AI. Mittels einer Datenbank bestehend aus 10 Milliarden Aufnahmen von Gesichtern soll Strafverfolgungsbehörden auf der ganzen Welt die Identifizierung von Personen erleichtert werden. Ähnlich wie auch VoyagerLabs bedient sich Clearview AI hierbei im Internet verfügbarer Daten und bekommt seine Bilder von Facebook, YouTube oder LinkedIn. Mittels Machine Learning wird für jedes auf den Bildern erkannte Gesicht ein biometrisches Profil erstellt. Beliebige Bilder können dann mit der Clearview-Datenbank abgeglichen werden, um in dieser Bilder mit demselben Gesicht zu finden. Außerdem wird ausgegeben, woher die Bilder stammen – das ermöglicht zum Beispiel, den Namen und weitere Informationen über die Person leichter zu finden. Laut eigener Informationen hat Clearview AI eine Treffgenauigkeit von über 99 %. [13, 14]

Dass zahllose Strafverfolgungsbehörden mit der Software arbeiten, scheint demnach wenig verwunderlich. Die Gesichtserkennungstechnologie ist zweifellos nützlich. Im Krieg zwischen Russland und der Ukraine wird sie etwa eingesetzt, um Gefallene zu identifizieren. Doch wie auch bei Unternehmen wie VoyagerLabs kommen hier einige fragwürdige Methoden zum Einsatz, die immer wieder Debatten über die Auswirkungen des Systems auf den Datenschutz und die Rechtmäßigkeit der zur Erstellung der Datenbank verwendeten Web-Scraping-Techniken auslösen. [14, 15]

3.2 Analyse von Beweismaterial

Im Zuge von Ermittlungen fallen regelmäßig enorme Mengen an Beweismaterial an. Bei der West Australia Police Force (WAPF) nehmen Fälle mit digitalen Beweismitteln jeweils mindestens 2,8 Terabyte ein – darunter E-Mails, Textnachrichten, Bilder, Social-Media-Posts und Aufnahmen von Überwachungskameras. [14, 16]

Das manuelle Sichten dieser Daten auf der Suche nach Hinweisen, Mustern, Unstimmigkeiten und Zusammenhängen ist äußert zeitaufwendig und es besteht ein hohes Risiko, dass wichtige Details übersehen werden. Erschwert wird dieser Umstand dadurch, dass Ermittler oft großen Zeitdruck haben und innerhalb 24 Stunden eine grobe Einschätzung von Fällen vornehmen sollten. [3, 16]

In Zusammenarbeit mit Microsoft wurde deshalb ein cloudbasiertes KI-Programm entwickelt, das hilft, bei großen Ansammlungen von Daten Licht ins Dunkel zu bringen und wichtige Informationen und Muster auf zuverlässige Weise aufzudecken. Der Einsatz ist erfolgreich: Die Software entnimmt den Daten relevante Informationen, analysiert Texte und Bilder, erkennt Zusammenhänge und ist in der Lage, die Arbeit mehrerer Monate auf ein paar Stunden zu reduzieren. Darüber hinaus hilft die Plattform bei der Übersetzung fremdsprachiger Texte, was den Prozess noch weiter beschleunigt. [16]

Laut dem Inspective Detector der WAPF, welcher an dem Projekt maßgeblich beteiligt war, hat die Geschwindigkeit, Effizient und Genauigkeit, welche die Plattform bietet, enormes Potenzial. Softwarelösungen dieser Art entlasten Analysten und Ermittler und unterstützen sie in ihrer Arbeit. [16]

3.3 Erkennung von Dokumentenfälschungen

Ein Delikt, das im Zusammenhang mit diversen kriminellen Aktivitäten auftritt, ist die Fälschung von Dokumenten wie beispielsweise Identitätsnachweisen. Gefälschte Dokumente erlauben es Kriminel-

len etwa, Straftaten oder deren Planung zu verschleiern. Im Rahmen des Forschungsprojekts DOKIQ soll deshalb untersucht werden, inwiefern KI-basierte Software helfen kann, Fälschungen zu erkennen und wie sie in die Polizeiarbeit integriert werden kann. Beteiligte Projektpartner sind neben dem Landeskriminalamt Baden-Württemberg, der Bundesdruckerei Berlin und den Landeskriminalämtern Bayern und Hessen auch die Hochschule der Medien Stuttgart mit ihrem Institut für Angewandte Künstliche Intelligenz (IAAI). Die Kooperation, die im April 2020 begann, dauert voraussichtlich bis Juli 2022. [17, 18]

Im Projekt soll untersucht werden, welche Möglichkeiten bei der automatisierten Erkennung von Fälschungen bestehen. Eine weitere Herausforderung ist die Integration des Domänenwissens der polizeilichen Sachbearbeiter in das durch Deep Learning modellierte, datenbasierte Wissen. Da die bei der Fälschung eingesetzten Methoden immer komplexer und technisch anspruchsvoller werden, bedeutet ein KI-basiertes Assistenzsystem einen großen Fortschritt auf diesem Gebiet. [19]

4 Fazit

In den vorangehenden Kapiteln wurde anhand diverser Anwendungsfälle aufgezeigt, wie Methoden der künstlichen Intelligenz eingesetzt werden können, um Polizeiarbeit zu unterstützen und Kriminalität zu bekämpfen.

Es zeigt sich, dass die Einsatzzwecke sehr vielfältig sind – KI-basierte Systeme setzen bereits bei der Prävention von Straftaten an und sollen ermöglichen, kriminelle Aktivitäten vorherzusagen und zeitnah einzugreifen. Doch auch auf andere Weise können Ermittlungen unterstützt werden: Beispielsweise durch Analyse von Bild- und Videomaterial, Gesichtserkennung, der Auswertung von Beweismaterial oder der automatisierten Erkennung gefälschter Dokumente.

KI eröffnet dadurch eine ganze Reihe neuer Möglichkeiten: Ermittlungen können enorm beschleunigt werden, Ressourcen und Einsatzkräfte können gezielter eingesetzt werden und es können Muster und Zusammenhänge aufgedeckt werden, die für Menschen nur schwer erkennbar sind. [6, 16]

Ermittler, die sich mit KI-basierten Assistenzsystemen auseinandergesetzt haben, sprechen etwa von einem Paradigmenwechsel und sind der Ansicht, dass die Polizeiarbeit dadurch unterstützt, verbessert und zukunftsorientiert ausgerichtet werden kann. [2, 16]

Trotz der vielen Stärken ist es wichtig, auch die Nachteile im Blick zu behalten. Unternehmen wie Clearview AI sammeln Unmengen persönlicher Daten und agieren auf eine ethisch und datenschutzrechtlich fragwürdige Art und Weise. Darüber hinaus neigen einige präventive KI-Systeme aufgrund von statistisch verzerrten Trainingsdaten dazu, Vorhersagen zu treffen, die schwarze Menschen deutlich benachteiligen, wie in Kapitel 2 angesprochen wurde.

Vor diesem Hintergrund ist es beim Einsatz von künstlicher Intelligenz im Bereich der Bekämpfung von Kriminalität wichtig, eine sorgfältige Abwägung zwischen Chancen und Risiken vorzunehmen. Das erleichterte Verhindern und Aufklären von Straftaten ist durchaus erstrebenswert – es beschleunigt die Arbeit von Ermittlern und ermöglicht einen gezielteren Einsatz von Personal und Ressourcen.

Dennoch darf dies nicht um jeden Preis geschehen. KI-basierte Systeme sollten nicht zulasten des Datenschutzes, gesetzlicher Regelungen oder bestimmter Personengruppen agieren. Es ist daher wichtig, ihre Funktionsweise zu hinterfragen und Transparenz zu schaffen, damit nicht an einer Stelle Probleme gelöst, aber an einer anderen neue geschaffen werden.

Literatur

[1] David Silver u. a. „Mastering the game of go without human knowledge“. In: *nature* 550.7676 (2017), S. 354–359.

[2] Julia Fricke. „Big Data und künstliche Intelligenz – Chancen und Risiken für die Polizeiarbeit der Zukunft“. Diss. URL: https://ksv-polizeipraxis.de/wp-content/uploads/2020/05/Fricke-Big-Data.pdf.

[3] A. Leehealey und A. Chigurula. „Fighting Crime with Artificial Intelligence (AI)“. In: *Proceedings on the International Conference on Artificial Intelligence (ICAI)*. The Steering Committee of The World Congress in Computer Science, Computer …, 2019, S. 284–290.

[4] Rodrigo Ceron, IBM. *AI, machine learning and deep learning: What's the difference?* 5. Dez. 2019. URL: https://www.ibm.com/blogs/systems/ai-machine-learning-and-deep-learning-whats-the-difference/.

[5] Singapore Computer Society (SCS). *Simplifying the Difference: Machine Learning vs Deep Learning*. 2020. URL: https://www.scs.org.sg/articles/machine-learning-vs-deep-learning.

[6] Hope Reese. *What Happens When Police Use AI to Predict and Prevent Crime?* 23. Feb. 2022. URL: https://daily.jstor.org/what-happens-when-police-use-ai-to-predict-and-prevent-crime/ (besucht am 14. 06. 2022).

[7] PredPol Inc. *what. where. when. Predict critical events and gain actionale insights with PredPol, The Predictive Policing Company.* URL: https://www.predpol.com/.

[8] Matt Burgess. *UK police are using AI to inform custodial decisions – but it could be discriminating against the poor*. 1. März 2018. URL: https://www.wired.co.uk/article/police-ai-uk-durham-hart-checkpoint-algorithm-edit.

[9] VoyagerLabs. *Make the Invisible Visible: AI-Based Investigation Solutions*. URL: https://www.voyager-labs.com/.

[10] Johana Bhuiyan und Sam Levin. *Revealed: the software that studies your Facebook friends to predict who may commit a crime*. 17. Nov. 2021. URL: https://www.theguardian.com/us-news/2021/nov/17/police-surveillance-technology-voyager.

[11] Julia Angwin u. a. *Machine Bias*. ProPublica. 23. Mai 2016. URL: https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing (besucht am 27. 06. 2022).

[12] *Algorithmenbasierte Videoüberwachung beim Polizeipräsidium Mannheim gestartet*. 3. Dez. 2018. URL: https://www.baden-wuerttemberg.de/de/service/presse/pressemitteilung/pid/algorithmenbasierte-videoueberwachung-beim-polizeipraesidium-mannheim-gestartet/.

[13] Clearview AI Inc. URL: https://www.clearview.ai/.

[14] Vitaly Vasyukov. „The role of artificial intelligence in crime investigation in Australia“. In: *Materials of the International Scientific and Practical Conference"Development of the doctrine of countering the investigation of Crimes and measures to overcome it in the context of digital transformation", Moscow, Academy of Management of the Ministry of Internal Affairs of Russia*. 21. Mai 2021.

[15] Rahel Lang. *Ukraine will mit Clearview AI russische Gefallene identifizieren*. 25. März 2022. URL: https://netzpolitik.org/2022/gesichtserkennungssoftware-ukraine-will-mit-clearview-ai-russische-gefallene-identifizieren/ (besucht am 27. 06. 2022).

[16] Microsoft News Center. *WA Police use cloud and AI to track criminals' digital footprints*. 7. Juni 2019. URL: https://news.microsoft.com/en-au/features/wa-police-use-cloud-and-ai-to-track-criminals-digital-footprints/.

[17] *Hochschule der Medien kooperiert mit dem Landeskriminalamt Baden-Württemberg*. 24. Apr. 2020. URL: https://www.hdm-stuttgart.de/view_news?ident=news20200423162022 (besucht am 14. 06. 2022).

[18] *Forschungsprojekt DOKIQ zur Erkennung von Dokumentfälschungen*. URL: https://ai.hdm-stuttgart.de/research/dokiq/ (besucht am 14. 06. 2022).

[19] Pressestelle Landeskriminalamt Baden-Württemberg. *Medieninfo: Das Kriminaltechnische Institut des Landeskriminalamts Baden-Württemberg startet in Kooperation mit der Hochschule der Medien Stuttgart die Zukunftsoffensive DOKIQ – Intelligente Fälschungserkennung*. Stuttgart, 23. Apr. 2020. URL: https://www.presseportal.de/download/document/664329-kooperationlkabw-hdmstartetzukunftsoffensivedokiq.pdf.