bitkom

KI in der Polizei – Einsatzpotentiale und Lösungsansätze zur Implementierung

Herausgeber
Bitkom e. V.
Albrechtstraße 10
10117 Berlin
T 030 27576-0
bitkom@bitkom.org
www.bitkom.org

Ansprechpartner
Stephan Ursuleac | T 030 27576-126 | s.ursuleac@bitkom.org
Bereichsleiter Verteidigung & Öffentliche Sicherheit

Kai Beerlink | k.beerlink@bitkom.org
Referent Künstliche Intelligenz

Verantwortliches Bitkom-Gremium
AK Verteidigung

Layout
Anna Stolz | Bitkom e.V.

Auf einen Blick

Ausgangslage

Spätestens mit ChatGPT sind Anwendungen zur Künstlichen Intelligenz (KI) in aller Munde. Dabei unterlag die Technologie in den vergangenen 70 Jahren immer wieder Wellenbewegungen der Aufmerksamkeit. KI hat das Potential die Leistungsfähigkeit der Polizeibehörden erheblich zu steigern. Daten in guter Qualität sind die Grundlage für erfolgreiche KI-Anwendungen und erfordern ein intelligentes Datenmanagement als solides Fundament. Die digitale Transformation bietet Chancen, stellt jedoch die Gesellschaft und die Sicherheitsbehörden gleichzeitig vor enorme Herausforderungen. Sie verändert die Kriminalitätsformen der analogen Welt und beeinflusst immer stärker die operative und strategische Arbeit der Polizei. Über Jahrzehnte in der analogen Welt erprobte Prozesse und Strukturen, kommen immer stärker an ihre Grenzen oder erreichen ihre Obsoleszenz. Der technologische Wandel vollzieht sich zudem in immer schnelleren Zyklen und erfordert oft neue Ansätze, Plattformen und Lösungen. Die Komplexität von Prozessen und die sie abbildenden Verfahren nimmt zu und ist nicht immer anwendbar für:

- die Menge gespeicherter Daten
- die Wichtigkeit von Informationen zur und während der Verarbeitung
- Personalressourcen für Verfahrensbearbeitung sind begrenzt und werden zunehmend geringer
- Ergebnisse aus Verfahrensbearbeitungen werden zunehmend zeitkritischer und bedürfen analytischer
- und kognitiver Unterstützung beim Prozess der Entscheidungsfindung – erfahrungsgestützt!
- Sogenannte Robotics-Szenarien werden zunehmend diskutiert, befinden sich in der Erprobung
- Die Gerichtsverwertbarkeit
- Die umfassende Fortbildung der Mitarbeitenden

Bewertung

Der KI-Thematik begegnen die Behörden, bzw. der beauftragende politische Raum noch mit Skepsis. Teilweise ist die Debatte aufgrund von fehlendem Know-How durch Angst geprägt. Aspekte wie Ethik und Datenschutz werden als Alibi einer verlangsamten Bearbeitung herangezogen. Dies ist jedoch nicht nötig.

KI-Anwendungen dienen der Befähigung der Polizeibehörden, u. a. zur Erhöhung der Entscheidungsqualität, am Ende von Bearbeitungsprozessen, und der Verarbeitungs-

geschwindigkeit. So kann die Integration von KI-Anwendungen zur Optimierung bestehender Arbeits- und Lösungsstrukturen dienen, aber auch zur Flexibilität beitragen. Arbeitsprozesse lassen sich somit skalieren und standardisieren, immer mit der Vorgabe, jederzeitiger Nachvollziehbarkeit und Transparenz von Logiken und Algorithmen zu gewährleisten. Das kann die Qualität steigern und Kosten und Zeit für Bearbeitungsschritte einsparen. Zudem unterstützt KI den Schutz von Grundrechten, weil irrelevante Daten erst gar nicht von einem Sachbearbeiter/einer Sachbearbeiterin gesichtet werden müssen.

Grundsätzlich bedarf es der Untersuchung für welche Arbeitsabläufe und Verfahren KI-Anwendungen eine sinnvolle Ergänzung und Unterstützung bedeuten könnten. Dies bedarf der Durchführung einer Grundlagenarbeit für eine Sachstandsfeststellung, die über Abläufe, deren Kritikalität (zeitliche und inhaltlich) und deren Bedeutung Aussagen trifft. Der weitere Schritt wäre dann ein entsprechendes Clustering, um so eine Priorisierung hinsichtlich des Einsatzes von KI-Anwendungen durchzuführen und das intelligente Datenmanagement danach auszulegen. Es gilt zu klären, welche relevanten Informationen und Entscheidungsparameter dargestellt, verarbeitet und für die fachlichen Bedarfe adaptiert werden können. Dabei können marktverfügbare Funktionalitäten adaptiert werden. Dies erfordert eine engere kooperative Zusammenarbeit zwischen Polizei, IT-Bedarfsträgern, Wissenschaft und Wirtschaft Schließlich gilt es zu klären welche beschaffungsrelevanten Rahmenbedingungen für den Einsatz von KI zu klären sind.

Zudem kann eine Marktschau helfen, bereits vorhandene Lösungen den eigenen Bedürfnissen anzupassen, bevor eine neue KI-Lösung entwickelt wird.

Inhalt

1 Begriffsbestimmung Künstliche Intelligenz (KI)

Künstliche Intelligenz ist als Begriff nicht einheitlich definiert. Vor allem, da sie sich schon seit der Begriffsbildung Ende der 1950er Jahre als interdisziplinäre Forschungsrichtung entwickelt und sich in ihrer Deutung stets an die technischen Möglichkeiten angepasst hat. Für die praktische Anwendung hat sich folgende Definition als nützlich erwiesen: Künstliche Intelligenz beschreibt Informatik-Anwendungen, deren Ziel es ist, menschenähnliches intelligentes Verhalten zu zeigen. Dazu sind in unterschiedlichen Anteilen bestimmte Kernfähigkeiten notwendig: Wahrnehmen, »Verstehen« (Erkennen), Handeln und Lernen. Diese vier Kernfähigkeiten stellen die größtmögliche Vereinfachung eines Modells zur modernen KI dar. Wahrnehmen – Verstehen– Handeln erweitert das Grundprinzip aller EDV-Systeme: Eingabe – Verarbeitung – Ausgabe. Das wirklich Neue ist das Lernen. Heutzutage gängige KI-Systeme haben gemeinsam, dass sie in der Verarbeitungsfähigkeit auch trainiert werden und damit lernen können. Angelernte Systeme haben mittlerweile eine gleichbleibende Performance mit einer Treffsicherheit von über 90 Prozent, z. B. bei der Bilderkennung und können zunehmend mit neuen Sachverhalten, die nicht Teil des Trainingsdatensatzes waren, umgehen. So erzielen sie bessere Ergebnisse als herkömmliche Verfahren, die nur auf starren, klar definierten und fest programmierten Regelwerken basieren.

Heute verfügen wir über eine sogenannte »schwache« KI, die den Menschen beim Erreichen seiner Ziele unterstützen soll – also smarte Mensch-Maschine-Interaktion und -Kollaboration. Die neueste Phase von KI-Systemen versucht daher, Lernverfahren mit Expertenwissen zu verbinden, um das Beste aus beiden Welten zu nutzen: Kontrolle, explizites Wissen, und menschliche Erfahrung mit der Kraft von Lernalgorithmen, die riesige Informationsmengen dynamisch für Menschen aufbereiten können.

Die »starke« KI – also eine wahre künstliche Intelligenz, die eine vollständige Imitation des Menschen darstellt – ist bisher jedoch Science Fiction.

2. Allgemeine Anwendungsmöglichkeiten von KI

Beim Einsatz von Künstlicher Intelligenz sind deutsche Unternehmen und Behörden noch sehr zurückhaltend. Oftmals fehlt es an Know-How. Das liegt häufig auch daran, dass es Unsicherheiten darüber gibt, was sich genau hinter dem Begriff KI verbirgt und welcher konkrete Nutzen sich daraus ziehen lässt. Um hier für mehr Übersicht zu sorgen, hat der Digitalverband Bitkom bereits 2019 ein »Periodensystem der Künstlichen Intelligenz erstellt«[1], dass die zahlreichen Einsatzszenarien von KI erklärt. Das KI-Periodensystem liefert einen guten Überblick über eine ganze Reihe von KI-Technologien und ihren praktischen Nutzen. Insgesamt werden in dem Periodensystem 28 Elemente vorgestellt, die Teil von Künstlicher Intelligenz sind. Die Spannbreite reicht dabei von Spracherkennung bis zum Relationship Learning. Für jedes Element gibt die Website unter anderem eine Antwort darauf, was es leistet, wie es eingesetzt werden kann, woran man seine Bedeutung erkennen kann und auch wer entsprechende Technologien und Lösungen anbietet. Zugleich werden auch mögliche Hürden beim Einsatz der Technologie im Alltag erläutert. Datenanalyse und Künstliche Intelligenz sind zwei Schlüsseltechnologien, die künftig nicht nur über den Erfolg einzelner Unternehmen und Behörden, sondern über die Zukunft ganzer Volkswirtschaften entscheiden werden. Beim Thema Künstliche Intelligenz dürfen wir nicht bei Appellen und Absichtserklärungen stehenbleiben. Wir müssen Künstliche Intelligenz jetzt gestalten – das heißt, die Technologie hierzulande weiterentwickeln und Anwendungen in die Praxis bringen.

> Beim Thema KI dürfen wir nicht bei Absichtserklärungen stehenbleiben. Datenanalyse und KI sind zwei Schlüsseltechnologien, die über den Erfolg von Behörden entscheiden werden.

[Das Periodensystem der Künstlichen Intelligenz]

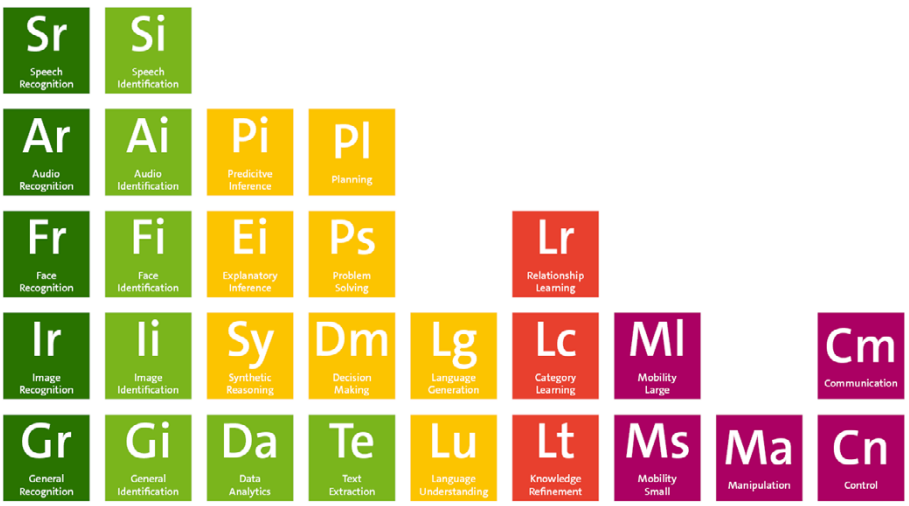


Abbildung 1: Periodensystem der KI

1 ↗ Periodensystem der KI erklärt Künstliche Intelligenz | Presseinformation | Bitkom e. V.

3. Anwendungsmöglichkeiten und Sachstand in der Polizei

In den USA oder Großbritannien ist der Einsatz von KI-Systemen in der Polizei Standard. Insbesondere die vorbeugende Datenanalyse ermöglicht im Rahmen des Predictive Policing die Erkennung möglicher Kriminalitätsschwerpunkte, auffälliger Aktivitäten oder die Erkennung von Mustern, sodass Einsatzkräfte gezielt dislozíert werden können. In Deutschland findet der Einsatz von KI partiell im Bereich der Strafverfolgung und der Gefahrenabwehr statt. Die meisten Anwendungen und Projekte laufen im Rahmen des Bundeskriminalamtes (BKA), aber auch in den Landespolizeien. Beispiele sind u. a. bei der Auswertung von Kinderpornografie, intelligenter Videoüberwachung von öffentlichen Räumen (was derzeit auf EU-Ebene kritisch diskutiert wird) oder der Schuhspuranalyse zu finden. Das Bundesverfassungsgericht schränkte jedoch unlängst die automatisierte Datenauswertung (Data-Mining) zur Vorbeugung von Straftaten (Predictive Policing) ein. Hintergrund ist der mögliche Eingriff in die informationelle Selbstbestimmung, gemäß Artikel 2 Absatz 1 i.V.m. Artikel 1 Absatz 1 des Grundgesetzes. Solche Systeme dürften jedoch Verwendung finden, wenn eine Gefahr für Leib und Leben oder die Freiheit von Personen, bzw. der Schutz überragend wichtiger Rechtsgüter (z. B. ein Angriff auf den Fortbestand der Bundesrepublik Deutschland) bestehe – also einer hinreichend konkretisierten Gefahr.[2]

Sicherheitsbehörden sehen sich steigenden Herausforderungen gegenüber, die eine Steigerung der Effektivität erfordern. Zum einen sinkt in den kommenden 15 Jahren die Anzahl erwerbstätiger Menschen.[3] Das seit Jahrzehnten geltende Grundkonzept von Verwaltungs- und Sicherheitsbehörden, bei unzureichenden Ressourcen einfach personell zu wachsen, um auf neue Herausforderungen zu reagieren, geht dann folglich nicht mehr auf.

Zum anderen steigt das Datenaufkommen. Bereits heute stellt dies eine große Herausforderung für die Sicherheitsbehörden dar, da der Großteil davon unstrukturierte Daten sind. Allein in der Polizei Niedersachsen sind etwa 7,5 Petabyte Daten gespeichert. Diese Menge an Daten würde etwa 150 Millionen Aktenschränke füllen.[4] Durch den weiteren Anstieg an Sensoren, mobilen Endgeräten (Smartphones, Tablets, etc.) sowie den Kapazitäten auf Speichermedien, wird diese Herausforderung weiter steigen. Hinzu kommt, dass sich Kriminalitätsphänomene immer weiter in den digitalen Raum verlagern und Sicherheitsbehörden stärker mit Daten in digitaler Form konfrontiert sind. Dies erfordert den Aufbau von weiteren Behördenkompetenzen, u. a. in der digitalen Forensik und Open Source Intelligence (OSINT). Es stellen sich technische Fragen nach Speicherkapazitäten, Rechenkapazitäten sowie geeigneter Software zur Auswertung dieser Daten. Diese Herausforderungen können nur im Dreiklang aus Politik (Rahmensetzung), Behörden (Durchführung) und Wirtschaft (digitale Kompetenzen und Ressourcen) konstruktiv und kooperativ gelöst werden. Der mögliche Einsatz von KI-Systemen gemäß der Abbildung 2 stellt eine Lösung der Herausforderung dar.

2 ↗ Bundesverfassungsgericht - Entscheidungen - Regelungen in Hessen und Hamburg zur automatisierten Datenanalyse für die vorbeugende Bekämpfung von Straftaten sind verfassungswidrig
3 ↗ 2035 werden in Deutschland 4 Millionen mehr ab 67-Jährige leben - Statistisches Bundesamt (destatis.de)
4 ↗ Niedersachsens Polizei kämpft gegen Datenmengen: Hilft KI? | NDR.de - Nachrichten - Niedersachsen

KI-Anwendungsmöglichkeiten in der Polizei

Führung

Lagezentrum/Systeme zur Entscheidungsunterstützung: Automatisierte Lagebilderstellung und -bewertung | Situationssimulation | Systeme zur Entscheidungsunterstützung in der Einsatzführung | Identifizierung/Abgleich anhand von Mustererkennungen | Ereignismonitoring und strukturierte Risikoanalyse | Geoanalysen für den operativen Bereich | Radarsysteme (u. a. automatisierte Kennzeichenerfassung | Feststellung von Verkehrsverstößen)

Aufklärung/ Informationsbeschaffung

Hotspotfrüherkennung i. V. m. Lagesystemen| Predictive Policing (u. a. Früherkennung von Straftaten | Kriminalitätsauswertung | Bild- und Mustererkennung) | automatisierte Aufklärungssysteme i. S. v. polizeilichem Internetmonitorig | Drohnenüberwachung bei Veranstaltungen oder sonstigen Lagen | Mapping Organisierte Kriminalität | Videoüberwachung auf öffentlichen Wegen und Plätzen

Informationsmanagement-/ -aufbereitung/ -auswertung/-analyse

Massendatenauswertung in OSINT (Nachrichten | Chats | PC/Smartphones, Social Networks/ | Erkennung von Hasskriminalität und ggf. Steuerung der Kommunikation | Sprechererkennung | Erkennung und Auswertung Audiodaten | Erkennung Social Engineering) | Abwehr und Aufklärung von Cyberangriffen |Geldflussnachverfolgung | Verknüpfung relevanter Informationen i. S. d. »intelligenten Beweismittelsicherung« zwecks Speicherplatzreduzierung | Bild- und Mustererkennung | Vorklassifizierung von Straftaten/Erkennung relevanter Paragraphen) | »intelligente Verknüpfung« von Informationen | allgemein großes KI-Potential mit diversen Anwendungsfällen

Kriminaltechnik

(teil)automatisierte Asservatenlager und Labors | automatisierte oder durch Assistenten geführte Erzeugung von (digitalen) Beweismitteln oder Fotos o. ä. | teilautomatisierte Auswertung | Data-Carving | Analyse biotechnischer Signale | Bild- und Mustererkennung

Unterstützung

Robotiksysteme | Intelligentes Routing (i. V. m. Smart Cities) | automatisierte logistische Prozesse | Delikt-/Straftatenvorschlag anhand Sachverhalt | EG/ BAO-Überwachung (i. S. eines HRM-Systems) | Auswertung Kinderpornographie (u. a. Szenenerkennung und Re-Identifizierung von Videodaten) | Analyse & Aufbereitung von Daten für die Justiz | Vernehmungen aufbereiten | SV/Gutachtenerstellung (selbstschreibende KI anhand von Stichworten, Passagenvorschrieb, intelligente Verknüpfung von Text mit Bildern, Beweismitteln, Laborergebnissen)

Personal

Besoldung | Beihilfe | Personalstrategie | Recruitment | Personalmanagement | Smart Personal Assistants (Chatbots) | Personalselektion für Aufgaben (EG,Einsätze)

Ausbildung/Übung/Einsatz

Übungsaus- und bewertung (Big Data) | simulationsbasierte Ausbildung | Augmented Reality in der Ausbildung | individualisierte Ausbildung | Real-Time Health Care System

Material und Ausrüstung

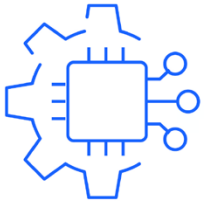
Fahrassistenten | autonomes Fahren | Predictive Maintainance | Flotten- und Mobilitätsmanagement

Infrastruktur

Sicherheitssysteme für Liegenschaften & IT | Liegenschaftsmanagement- und Wartung | Asservatenlagerung

Methoden und Verfahren

Informationsmanagement | Analyse großer Datenmengen | verbessertes Risikomanagement | medizinische Überwachung und Diagnoseunterstützung | personalisierte medizinische Unterstützung/predictive health care | Ordermanagement/dezentrale Beschaffung | Prozessautomatisierung | Schuhspuranalyse



Konzeption und Konzepte

Analysemethoden | Prozessmanagement und -optimierung in Planung, Beschaffung und Nutzung

Abbildung 2: KI-Use Cases in der Polizei

KI kann auf allen Ebenen der (Massen-)Datenverarbeitung eingesetzt werden, insbesondere bei spezialisierten und sich wiederholenden Aufgaben. Das bedeutet Daten zu erheben, zu speichern und zu analysieren. Dadurch können eine große Datenmenge strukturiert und handhabbar gemacht sowie Zusammenhänge aufgedeckt werden. KI kann als digitaler Assistent dienen, Muster erkennen und eine Vorauswahl für eine menschliche Entscheidung treffen. Dabei sollte der Mensch grundsätzlich das Recht auf eine finale Entscheidung behalten.

3.1. Hürden bei der Implementierung

Der Einsatz von KI in den Sicherheitsbehörden bedarf eines gesetzlichen Rahmens, insbesondere wenn personenbezogene Daten verarbeitet werden. Das damit verbundene Recht auf informationelle Selbstbestimmung ist bei den meisten Anwendungen betroffen. Eingriffe in dieses Recht können auch dann vorliegen, wenn das Ergebnis einer Analyse einen »Nichttreffer« erzeugt und die Daten umgehend gelöscht werden. Eine hohe Eingriffsintensität stellen in diesem Zusammenhang KI-Anwendungen dar, die verdachtslos und mit einer großen Streubreite agieren. Dabei werden diverse Personen involviert, die in keinem Zusammenhang zu einem Sachverhalt stehen, bzw. durch ihr Verhalten keinen Anlass einer Überprüfung gegeben haben. Ebenso ist eine vollständige »Durchleuchtung« von Personen mit der Verfassung nicht vereinbar.

Dies stellt Ermittlerinnen und Ermittler in der Praxis jedoch auch vor Herausforderungen. Gerade im extremistischen Umfeld kann es sinnvoll sein, alle Informationen zu einer Person für eine Lageanalyse zu erhalten, darunter auch deren emotionalen Zustand (z. B. bei Geiselnehmenden oder Gewalttäterinnen und -tätern).

Schließlich sind europäische Richtlinien zu beachten. Eine mittels KI automatisierte Entscheidungsfindung ist aufgrund Artikel 11 Abs. 1 und Abs. 2 der Richtlinie der EU 2016/680 möglich. Ein Profiling, das natürliche Personen auf Basis definierter Datenkategorien diskriminiert, ist hingegen nach Absatz 3 verboten.[5] Vor diesem Hintergrund ist es geboten, vor und während der Einführung von KI-Anwendungen in den Sicherheitsbehörden die Datenschutzbeauftragten einzubinden, um rechtskonform zu agieren. Dies ist auch gemäß Paragraph 69 Abs. 1 Bundesdatenschutzgrundverordnung (BDSG) nötig, um die Rechtmäßigkeit der angestrebten Verarbeitung zu gewährleisten. Auch Paragraph 67 Absatz 1 der BDSG fordert bei der »Verwendung neuer Technologien« eine Datenschutz-Folgenabschätzung. Aktuell stellt die Einhaltung der datenschutzrechtlichen Grundsätze Transparenz, Zweckbindung und Datenminimierung eine Herausforderung in der Praxis dar, die ggf. zu gesetzlichen Anpassungen führen muss. Der Gesetzgeber schätzt KI in Sicherheitsbehörden als besonders risikoreich ein und versieht sie daher mit Auflagen.

KI in der Polizei dient nicht gläsernen Bürgerinnen und Bürgern.

Die Europäische Union (EU) nimmt sich dem Thema im Rahmen des Artificial Intelligence Acts (AI Act) an, welcher voraussichtlich Ende 2023 verabschiedet wird. Dort werden KI-Anwendungen in Kategorien (unannehmbares, hohes, geringes, oder minimales Risiko) mit entsprechenden Auflagen (etwa Transparanz- und Kontrollanforderungen) eingestuft). Die Regularien des AI Act und die nach dem Entwurf der EU-Kommission vorgesehenen Haftungsregelungen für KI (AI Liability Directive – AILD) stellen Entwickler bestimmter KI-Anwendungen in Europa vor neue Herausforderungen. Strenge Regularien für KI, u. a. beim Aufbau von Qualitätsmanagementsystemen, bei technischen Dokumentationen, bei Datenanforderungen, etc., ergeben eine rechtliche Komplexität und damit erhöhte Kosten. Aufgrund der Komplexität und erschwerten Nachvollziehbarkeit von Entscheidungen von KI-Systemen, erhalten potenziell geschädigte Personen verhältnismäßig leichten Zugang zu Klagemöglichkeiten gegen Betreiber von KI-Systemen. Diesen droht nach dem aktuellen Entwurf der AILD gar die gerichtlich angeordnete Offenlegung von Informationen, wie etwa dem Quellcode. Dies greift in die Geschäftsgeheimnisse ein und bietet erhebliches Erpressungspotenzial. Auch könnten Trainingsdatensets gesperrt werden, wenn diese bestimmte persönliche Daten enthalten. Hinzu kommt, dass KI zudem in den Anwendungsbereich der überarbeiteten Produkthaftungsrichtlinie aufgenommen worden ist (Entwurf der Kommission aus September 2022). Da nach dem Entwurf keine Haftungshöchstsummen mehr für Schäden vorgesehen sind, stellen KI-Lösungen ein nicht kalkulierbares Risiko für Unternehmen dar. Insbesondere innovative Startups und mittelständische Unternehmen können diese Risiken und Regularien nicht übernehmen.

5 ↗ RICHTLINIE (EU) 2016/ 680 DES EUROPÄISCHEN PARLAMENTS UND DES RATES - vom 27. April 2016 - zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/ 977/ JI des Rates (europa.eu)

Auf Vorschlag der Kommission wird der AI Act voraussichtlich KI Anwendungen in Behörden verbieten, die folgende Punkte umfassen:

- Manipulation von Personen
- Exploitation (Ausbeutung von Personen)
- ein Social Scoring (u. a. Einbeziehung von Persönlichkeitsmerkmalen oder sozialem Verhalten zur Analyse der Vertrauenswürdigkeit von Personen)
- biometrische Identifizierung mittels Echtzeit-/Fernidentifizierungssystemen in öffentlich zugänglichen Räumen zur Strafverfolgung (Ausnahmen: Suche nach bestimmten Verdächtigen, Täterinnen und Tätern sowie Opfern und Abwendung unmittelbarer Gefahren)

Die laufende Debatte um konkrete Verbote wird jedoch voraussichtlich erst zum Ende dieses Jahres ihren Abschluss finden. Dafür erfordert es eine umfassende Einigung in den Trilogverhandlungen zwischen der EU Kommission, dem Rat sowie dem EU Parlament, die ebenfalls eigene Änderungen eingebracht haben.

Insbesondere das EU Parlament hat noch einige Verschärfungen vorgeschlagen. Gemäß Artikel 5 sind weitere KI-Systeme für ein umfassendes Verbot vorgesehen, die von der EU Kommission vorher noch als Hoch-Risiko eingestuft wurden. Dazu sollen insbesondere KI-Systeme zählen, die:

- auf Grundlage von Persönlichkeitsmerkmalen, Eigenschaften oder früheren kriminellen Verhaltens das Risiko von Personen einschätzen, um straffällig zu werden oder erneut straffällig zu werden
- Datenbanken zur Gesichtserkennung durch das ungezielte Auslesen aus dem Internet oder von Überwachungsaufnahmen erstellen
- zur Ableitung von Emotionen einer natürlichen Person in der Strafverfolgung oder anderen Bereichen dienen

Behörden müssen daher genau definieren, in welchen Szenarien KI-Anwendungen einen konkreten Mehrwert bieten. KI-Anwendungen in der Polizei müssen Aspekten des Datenschutzes und der Datensicherheit entsprechen. Ihre Ergebnisse müssen gerichtsfest sein, auf Basis gesetzlicher Grundlagen. Dies verlangt eine Transparenz der Methodik, eine aktuelle Datenlage sowie eine reglementierte Verfügbarkeit der Daten für bestimmte Personen. Dabei darf auch der Faktor Mensch nicht außer Acht gelassen werden. Für Bedienstete müssen daher Anwendungen leicht bedienbar sein, ohne große technische Vorkenntnisse.

Dabei gilt es strukturell zu vermeiden, dass KI-Projekte in den einzelnen Polizeibehörden parallel laufen und mögliche Synergieeffekte nicht genutzt werden. Eine zentrale Koordinierung wäre ein geeignetes Instrument, um hier Abhilfe zu schaffen.

3.2. Ethische Aspekte

KI in der Polizei anhand von Use Cases ethisch, rechtlich, technisch und sozial bewerten

Bei der Betrachtung von KI-Anwendungen in der Polizei ist Ethik ein zentraler Aspekt. Der Polizei kommt in ihrem Handeln ein Schutzauftrag zu. Die Würde des Menschen ist genau wie das Recht auf informationelle Selbstbestimmung ein zentrales Anliegen. Die Veränderungen, die die KI mit sich bringt, sind grundlegend und unumkehrbar. Sie wirken sich auf das Individuum und die Gesellschaft aus – 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 systemisch) sowie auf die politische Willens- und Meinungsbildung.

Die ethische Debatte darf jedoch nicht missbraucht werden, um die grundsätzliche Skepsis oder Angst vor der Technologie KI zu manifestieren. Um die Sicherheitsbehörden von technologischen Entwicklungen durch langwierige Debatten nicht abzuschneiden, sollten KI-Anwendungen für die Polizei in Fallgruppen kategorisiert werden, um bezogen auf einzelne Use Cases ethisch, rechtlich, sozial, aber auch technisch betrachtet zu werden Eine umfassende ethische Betrachtung zum Thema KI in der Polizei ist zur praktikablen Umsetzung nicht zweckdienlich. Die Nutzung von KI in einem Chatbot ist schließlich anders zu bewerten als im Predictive Policing usw. Dies fördert eine verantwortungsvolle und praktikable Einführung von KI-Anwendungen in der Polizei, um deren Arbeit zu unterstützen.

Was jedoch möglich ist, ist die Einigung über grundlegende ethische Standards. Diese Debatte wird bereits seit Jahrzehnten geführt und gibt kaum noch neue Aspekte her. Es gilt nun ins Machen zu kommen.

Grundsätzliche Überlegungen sind:

- KI sollte eine Technologie sein, die menschliche Fähigkeiten unterstützt, erweitert und verbessert und dem Gemeinwohl dient. Die zentrale ethische Herausforderung besteht darin, intelligente Systeme zu entwickeln, die mit dem menschlichen Leben vereinbar und werteorientiert sind, um das Leben der Menschen zu verbessern, Grundrechte und Autonomie zu wahren und Handlungsoptionen zu erweitern.
- Der Begriff Privatheit ist zentral. Mit Privatheit ist die Kontrolle gemeint, die eine Person darüber haben sollte, wer wann in welchem Maße und Zusammenhang auf etwas zugreift, das zu dieser Person gehört. Privatheit bedeutet, das Individuum in seiner Autonomie und Würde zu schützen und das Prinzip zu achten, dass Individuen in einem Rechtsstaat auch Rechte zum Selbstschutz gegenüber der Staatsmacht haben und behalten müssen. Privatheit dient sowohl dem Schutz der Menschen als auch zum Erhalt von Rechtstaatlichkeit. Privatheit ist Zweckdienlichkeit und Präzision, Schutz sensibler Daten und des Kernbereichs psychischer und emotionaler Belastung von Ermittlern und Ermittlerinnen. Dies ist bei der technischen Entwicklung zu berücksichtigen, genau wie Anonymisierungsverfahren, zur Verhinderung von Datenverfälschungen und Verzerrungen.

Prinzipien für KI in der Polizei:
Dient dem Wohl von Menschen | muss funktionieren (transparent, erklärbar, robust, prüfbar) keine Diskrimi-nierung Autonomie der Entscheidung beim Menschen

- Über die Prinzipien, die bei der Gestaltung intelligenter Systeme anzuwenden sind, sollte ein interdisziplinärer und transparenter Konsens bestehen. Alle Stakeholder in Wirtschaft, Politik und Gesellschaft müssen die ethische und datenökologische Verantwortung im Hinblick auf eine nachhaltige Datenökonomie übernehmen. Gleichzeitig ist es notwendig, sich auf ethische Standards der Algorithmisierung zu einigen. Für den Kontext von KI-Projekten in der Polizei könnte das heißen: **Anwendungen sollten grundsätzlich dem Wohl von Menschen dienen**. Die Polizei unterliegt dabei dem Grundsatz der Fürsorge und Schadensvermeidung. Hauptauftrag ist nicht die automatisierte Durchleuchtung der Bürgerinnen und Bürger, sondern deren Schutz. **KI-Anwendungen in der Polizei müssen funktionieren**. Das heißt **sie müssen transparent, erklärbar, robust und prüfbar sein. Dies dient der Gerichtsfestigkeit. KI-Anwendungen in der Polizei dürfen keine Diskriminierung von Rasse, Geschlecht, Sexualität oder anderen zu bestimmenden Parametern zulassen**. Der Grundsatz des Human in the Loop, der finalen Entscheidung über Sachverhalte, obliegt den Menschen. Die **KI kann Entscheidungen, bzw. Daten zwar aufbereiten, die Autonomie der Entscheidung obliegt jedoch dem Menschen**. Gerade im Kontext der Strafverfolgung, mit ihren Eingriffsmöglichkeiten in das menschliche Leben, darf keine Maschine finale Entscheidungen treffen. Dabei unterliegen die Anwendungen strengen Qualitätskontrollen. Es gilt Biases zu vermeiden, regelmäßige Kontrollen des Systems durchzuführen und eine Überprüfung der Einsatzzwecke vorzunehmen. Gleichzeitig sind Schulungen der Anwenderinnen und Anwender sowie ein offener Umgang mit Fehlern, Fehlerquellen und Schwächen eines künstlichen Systems anzusetzen. Hier ist ein regelmäßiger Austausch von Staat, Wirtschaft und Wissenschaft nötig.
- Sicherheitsethische Leitlinien sollten sein:
  - Eine Zunahme an Automatisierung soll nicht zu automatisierten Entscheidungen über menschliche Schicksale führen, sondern Entscheidung des Menschen insbesondere durch Filterung vorbereiten und unterstützen.
  - Autonomie und Entscheidungsfreiheit sollten ermöglicht und durch entsprechende Systemarchitektur unterstützt werden.
  - Die Einflüsse der Technik auf die Handlungen, das Denken und die Gewohnheiten des Menschen sollten reflektiert werden: Technikgestaltung ist auch Gesellschaftsgestaltung.
  - Die IT-Sicherheit und der Schutz der Infrastruktur sind Voraussetzungen für den Datenschutz.
- Der Einsatz von Algorithmen und selbstlernenden Systemen muss ethisch bewertet werden. Es muss ein Rahmen für Gesetzgeber, Regulierungsbehörden, Wirtschaft und den öffentlichen Sektor erarbeitet werden. Dazu gehören auch Richtlinien, welche KI-Anwendungen erwünscht sind und welche nicht. Diese Herausforderungen sollten von den politischen Entscheidungsträgern angegangen werden.

4. Lösungsansätze zur Implementierung

Technische Anforderungen an KI

Daten in guter Qualität sind die Grundlage für erfolgreiche KI-Anwendungen. Unzureichende Datensätze führen zu einem verzerrten Lagebild. Der Trainingsphase des Systems kommt somit eine entscheidende Bedeutung zu – insbesondere, um menschliche Einflüsse wie Diskriminierung oder die Korrektheit von Informationen zu gewährleisten. Dies erfordert ein intelligentes Datenmanagement, was die Daten so aufeinander abstimmt und zur Verfügung stellt, dass die jeweilige KI-Anwendung optimal darauf zugreifen kann. Daher müssen Datenmanagement und KI-Anwendung gut koordiniert sein, unter Aspekten der Schnittstellenfähigkeit und Informationssicherheit beim Datenaustausch. Die Komplexität von Prozessen und der sie abbildenden Verfahren nehmen dabei stetig zu. Daher steigt auch das Risiko fehlender Transparenz und Nachvollziehbarkeit bei den angewendeten Methoden. Dies umfasst u. a. die Menge der gespeicherten und übermittelten Daten. Auch die Wichtigkeit von Informationen zur und während der Verarbeitung nimmt durch immer bessere Sensoren weiter zu. Diese Aspekte und die Überprüfbarkeit der Validität, der daraus erzeugten Ergebnisse, sind rechtlich essenziell. Vor Gericht kann es sein, dass auf KI basierende Entscheidungen im Einzelfall vollständig nachvollziehbar sein müssen. Dabei sind die Personalressourcen 'für Verfahrensbearbeitungen begrenzt und werden zunehmend geringer. Daraus gewonnene Ergebnisse müssen gleichzeitig immer schneller bewertet werden und bedürfen analytischer und kognitiver Unterstützung beim Prozess der Entscheidungsfindung. Neben den KI-Anwendungen sollten somit auch Techniken betrachtet werden, die deren Ergebnisse für Anwendende nachvollziehbar machen.

Daten in guter Qualität sind die Grundlage für erfolgreiche KI-Anwendungen.

Die Erlangung technischer Lösungen

Für Sicherheitsbehörden stellt sich somit die Frage, wie sie Zugang zu solchen Technologien erhalten. Dabei bekommen sie oft erst Gelder, nachdem ein Schadensereignis eingetreten ist, welchem nun – meist politisch motiviert – abgeholfen werden muss. Beim anschließenden Aufbau von technischen Kompetenzen stellen sich dann weitere Herausforderungen ein. Vor allem der Zugang zu validen und verlässlichen Test- und Trainingsdaten, die zudem unter Berücksichtigung von ethischen, datenschutz- und allgemeinen rechtlichen und technischen Standards bestehen, ist kritisch. Auch die Einbeziehung externer Akteure, gerade bei Vertrauenssachen, wird hinterfragt. Doch nicht alle in den Polizeibehörden verwendeten Daten unterliegen VS-NfD. Grundlage eines KI-Datenmanagements ist daher die Bildung von Clustern, in denen VS-NfD und offene Daten unterschieden werden. Offene Daten liegen z. B. bei Online-Anzeigen vor, oder bei parallellaufenden Transkripten von Notrufen an Leitstellen. Dies kann helfen die Implementierung zu unterstützen, da somit nicht die schwersten, sondern leichtes-

Um KI in der Polizei einzu-führen, bedarf es klarer Ansprechstellen für KI-Themen

ten Herausforderungen angegangen werden können. Dabei ist der Aufbau eines eigenen Ökosystems aus eigenen Personalressourcen, Wirtschaft und Wissenschaft dringend geboten.

Die Polizei sollte sich auf ihre Kernaufgaben und Kernfähigkeiten fokussieren. Die Entwicklung von Software gehört nicht dazu. Dennoch wird dies durchgeführt, mit dem Ziel den gesetzlichen Auftrag zur Gefahrenabwehr und Strafverfolgung ohne Abhängigkeiten nachkommen zu können. Argumente, dass wirtschaftliche Lösungen zu teuer seien oder man selbst am besten wisse, was man benötigt, stehen immer wieder im Raum. Dabei ist jedoch zu berücksichtigen, dass eigene Expertinnen und Experten bei der Programmierung zu beschäftigen, ggf. teurer sein kann, als eine Marktlösung, die in einem gemeinsamen iterativen Prozess abgestimmt wurde und an die Bedürfnisse der Polizei angepasst ist. Software ist heutzutage so komplex, dass sie nicht mehr vollständig getestet werden kann. Sie wird daher nicht einmalig entwickelt und steht dann unmittelbar zur Verfügung. Vielmehr bedarf es einer ständigen Anpassung, was dann Daueraufgabe der Programmierenden innerhalb der Behörde ist. Deren Unterhalt kann über mehrere Jahre also teurer als eine Auslagerung von Services in die Wirtschaft sein. Auch sollten ggf. Lösungen, die nur zu 80 Prozent den Anforderungen entsprechen, in Betracht gezogen werden, gerade weil die Software stets weiteren Anpassungen unterliegt. Dabei muss Transparenz herrschen, was die KI kann und nicht kann, um ein realistisches Erwartungsmanagement zu betreiben. Dies müsste bei Ausschreibungen Berücksichtigung finden.

Schließlich verfügen viele Marktteilnehmer auch über sicherheitsüberprüfte Zertifizierungen, die sie zum Umgang mit vertraulichen Inhalten befähigen. Im Verteidigungssektor ist diese Zusammenarbeit Standard und daher auch für die Sicherheitsbehörden des Inneren nutzbar. So kann die Technologie auch für die Polizei vollumfänglich adaptiert werden. Durch Leuchtturmprojekte können zudem Erfahrungswerte für Folgeprojekte gesammelt werden. Dabei sollte sowohl in den Bundesländern, als auch auf Bundesebene eine klare Ansprechstelle für BOS-KI-Themen organisatorisch verortet werden, um das KI-Thema fokussiert und abgestimmt voranzutreiben. Somit ließen sich finanzielle und personelle Ressourcen bündeln. Dazu wären auch Modelle der Public-Private-Partnership mit Unternehmen denkbar, die Konzepte erstellen, Ideen sammeln und Projekte mit agilen Methoden koordinieren.

Bitkom vertritt mehr als 2.200 Mitgliedsunternehmen aus der digitalen Wirtschaft. Sie erzielen allein mit IT- und Telekommunikationsleistungen jährlich Umsätze von 190 Milliarden Euro, darunter Exporte in Höhe von 50 Milliarden Euro. Die Bitkom-Mitglieder beschäftigen in Deutschland mehr als 2 Millionen Mitarbeiterinnen und Mitarbeiter. Zu den Mitgliedern zählen mehr als 1.000 Mittelständler, über 500 Startups und nahezu alle Global Player. Sie bieten Software, IT-Services, Telekommunikations- oder Internetdienste an, stellen Geräte und Bauteile her, sind im Bereich der digitalen Medien tätig oder in anderer Weise Teil der digitalen Wirtschaft. 80 Prozent der Unternehmen haben ihren Hauptsitz in Deutschland, jeweils 8 Prozent kommen aus Europa und den USA, 4 Prozent aus anderen Regionen. Bitkom fördert und treibt die digitale Transformation der deutschen Wirtschaft und setzt sich für eine breite gesellschaftliche Teilhabe an den digitalen Entwicklungen ein. Ziel ist es, Deutschland zu einem weltweit führenden Digitalstandort zu machen.

Bitkom e.V.

Albrechtstraße 10
10117 Berlin
T 030 27576-0
bitkom@bitkom.org

bitkom.org

bitkom