

### **Welche Rolle kann KI zukünftig in Strafprozessen spielen? Welche Vorteile bietet ihr Einsatz, und welche Konflikte können dadurch entstehen?**

KI-Systeme bieten auch im Strafprozess Potenzial. Dabei geht es nicht um die dystopische Vorstellung eines Roboter-Richters, sondern um Ansätze für Unterstützungssysteme, die den Gerichten die alltägliche Arbeit erleichtern können. In Betracht kommt zum Beispiel eine Unterstützung bei der idealen Prozessplanung oder Terminansetzung, aber auch eine Unterstützung bei der Entscheidung selbst durch sogenannte «Decision Support Systeme (DSS)» ist denkbar. Diese können etwa darauf ausgerichtet sein, die Effizienz der Entscheidung zu steigern, und sei es «nur» durch intelligente Textbausteine, die sich den bevorzugten Formulierungen bei der Entscheidungsbegründung an-

passen. Aber auch qualitative Verbesserungen der gerichtlichen Entscheidungen sind im Grundsatz vorstellbar. Erhebliches Verbesserungspotenzial besteht dabei in Deutschland etwa im Bereich der Strafzumessung, bei der die grossen regionalen Unterschiede in der Strafhöhe für an sich vergleichbare Delikte seit Jahrzehnten bekannt sind. Hier könnten Entscheidungs-Unterstützungssysteme genutzt werden, um die üblicherweise für eine Tat verhängte Sanktion transparent zu machen und so als zusätzliche Entscheidungsgrundlage zu mehr relativer Sanktionsgerechtigkeit beizutragen. Auch hier bleibt jedoch Vorsicht geboten, da aus psychologischen Studien bekannt ist, dass es dem Menschen schwerer fällt, sich über von «Technik» – scheinbar objektiv – generierte Werte hinwegzusetzen: der sogenannte «Automation

Bias». Um im grundrechtssensiblen Strafverfahren zum Einsatz kommen zu können, müssen Transparenz, Datenschutz und Qualitätssicherung der Systeme gewährleistet werden. Zudem muss auch bei Zuhilfenahme von Unterstützungssystemen die menschliche Letztentscheidung gewahrt bleiben.

### **Warum muss die letzte Entscheidung über eine gerechte Strafe für menschliche Verfehlungen in menschlicher Hand bleiben?**

Weil eine KI keine Verantwortung für die getroffene Entscheidung übernehmen kann, egal wie leistungsfähig sie noch werden mag. Sie kann die Bedeutung einer Sanktion nicht kennen, das kann allenfalls simuliert werden. Und weil es in spezialpräventiver Hinsicht den Diskurs braucht, der im menschlichen Urteil liegt.

# Künstliche Intelligenz und Kriminalität

Die jüngsten Entwicklungen im Bereich der KI können als problematisch angesehen werden, vor allem bezüglich ihrer Kontrollierbarkeit. Eine Sorge ist, dass KI genutzt wird, um insbesondere Cybercrime-Delikte zu begehen. Allerdings kann KI, wie der Kriminologe Dirk Baier in seinem Beitrag zeigt, nicht nur ein neues Kriminalitätsproblem, sondern auch ein Teil der Lösung von Kriminalitätsproblemen sein.

Künstliche Intelligenz (KI) ist spätestens seit der Veröffentlichung von ChatGPT im November 2022 zu einem Thema geworden, welches grosse Teile der Gesellschaft beschäftigt. Dass Computer algorithmengestützt Gespräche führen und Fragen beantworten, letztlich auch logisch denken, lernen, Neues

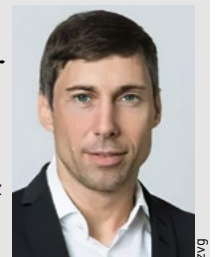
entwickeln und kreativ sein können und damit dem Menschen immer ähnlicher werden, ist seitdem vielen bewusst geworden. Doch letztlich ist KI kein gänzlich neues Phänomen. Wenn KI sehr allgemein als Instrument definiert wird, welches aus vorhandenen Daten neu strukturierte Daten, neue Erkenntnisse

generieren kann, dann geschieht genau dies seit Beginn der empirischen kriminologischen Forschung. Wurden anfänglich noch einfache Zusammenhänge zwischen Phänomenen statistisch untersucht, wurden die Erkenntnismöglichkeiten mit der Weiterentwicklung informationstechnischer Infrastruktur umfassender. Maschinengestütztes Lernen, Mustererkennung, Prognosen usw. kommen daher bereits seit vielen Jahren u.a. in der Kriminalanalyse zur Anwendung. Und das Internet und andere Infrastrukturen werden auch seit vielen Jahren genutzt, um Kriminalität zu begehen. ChatGPT und vergleichbare KI-Anwendungen läuten daher keine

### **Autor**

#### **Prof. Dr. Dirk Baier**

Universität Zürich,  
Kriminologisches  
Institut; ZHAW,  
Institut für Delinquenz  
und Kriminalprävention



komplett neue Ära der Kriminalität ein; sie beschleunigen aber Entwicklungen und sind vor diesem Hintergrund zweifellos sehr bedeutsam.

### KI und Kriminalität – Ausgewählte Themen

Es finden sich bereits einige Übersichtsarbeiten zum Zusammenhang von KI und Kriminalität (u.a. Blauth et al. 2022, Hayward & Maas 2020) sowie Studien, die spezifische Aspekte vertieft betrachtet haben. Ohne Anspruch auf Vollständigkeit sollen aus diesem Forschungsstand verschiedene Themen im Folgenden näher beleuchtet werden.

Ein zentrales Thema bzgl. KI und Kriminalität ist das *Begehen von Straftaten*. Hierbei ist zu unterscheiden zwischen *Straftaten gegen KI* und *Straftaten mittels KI*. Straftaten gegen KI umfassen Angriffe auf KI-Systeme (AI-Hacks), um deren Tätigkeiten zu manipulieren. Ein bekanntes Beispiel ist die Manipulation des Microsoft-Chatbots «Tay», der auf «X» (ehem. Twitter) Tweets erzeugen sollte, die nicht von einem menschlichen Akteur zu unterscheiden waren. Wenige Stunden nach der Veröffentlichung gab es einen koordinierten Angriff, bei dem User beleidigende Wörter und Sätze twitterten, die dann von Tay reproduziert wurden. Das Konto musste von Microsoft nach weniger als 16 Stunden gesperrt werden. Weitere Formen von «AI-Hacks» sind denkbar: So können über intelligente Spracherkennungssystemen wie Alexa oder Siri gezielt versteckte Sprachbefehle verschickt werden, damit diese spezifische Telefonnummern wählen oder Websites öffnen; dies kann Angriffe auf «smart homes» ermöglichen (Hayward & Maas 2020, S. 8f).

Je mehr KI in verschiedenen Bereichen wie dem Börsenhandel, dem Gesundheitssystem u.a.m. zum Einsatz kommt und Grundlage für Entscheidungsfindungen ist, umso attraktiver wird es, sie anzugreifen und gezielt zu verändern. Eine Herausforderung im Zusammenhang mit KI ist, dass anhand bestehender Daten ein Entscheidungs-

algorithmus trainiert werden muss, d.h. KI ist einerseits auf umfassende Daten und andererseits auf ein möglichst neutrales Regelwerk zur Entscheidungsfindung angewiesen. Liegen nicht ausreichende oder verzerrte Daten vor, beeinflusst dies die KI-Aktivitäten.

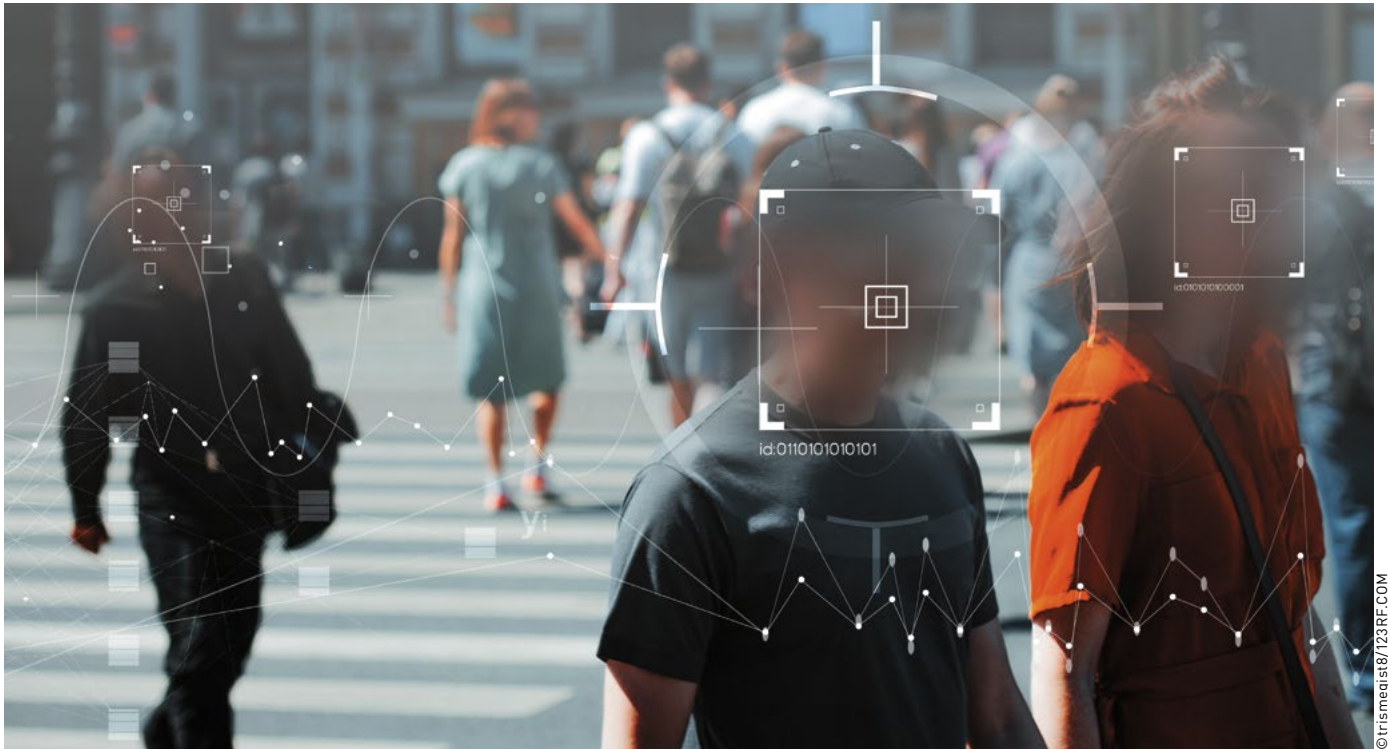
Ausführlich diskutiert werden Straftaten, die mittels KI ausgeführt werden können. Hierbei handelt es sich einerseits um Straftaten, die bereits bekannt sind, aufgrund der neuen KI-Möglichkeiten entweder professionalisiert oder aber von einer grösseren Anzahl an Tatpersonen ausgeführt werden können. Mit letztgenanntem ist gemeint, dass Schadsoftware oder Phishing-Mails nicht mehr selbst programmiert werden müssen, sondern via Auftrag an die KI hergestellt werden können. Professionalisiert werden kann kriminelles Verhalten dadurch, dass bspw. Phishing-E-Mails personalisierter gestaltet werden oder dass neue Phishing-Attacken automatisch von anderen Attacken lernen können (z.B. «DeepPhish»). Es können auch soziale Chatbots programmiert werden, die Betrugsformen, welche auf Social Engineering beruhen, vereinfachen. Unter anderem ist hier der Bereich des Romance Scam angesprochen: Bereits 2007 wurde ein Dating-Chatbot «CyberLover» dazu genutzt, Chatroom-Benutzer dazu zu verleiten, persönliche Informationen preiszugeben oder auf betrügerische Links zu klicken; unter Nutzung von KI kann ein solcher Chatbot sicher noch weit erfolgreicher agieren.

Neben den bereits bekannten Straftaten offeriert KI zugleich die Möglichkeit, bislang in der Form nicht bekannte Straftaten zu begehen (bzw. bislang unbekanntes Mittel zu nutzen). Hier ist vor allem auf die Deepfakes hinzuweisen, also auf Bild- und Videomaterial, welches hochrealistisch gefälscht wurde, um beim Gegenüber bestimmte Reaktionen hervorzurufen. Es kann sich bspw. um pornografisches Material handeln, welches für Erpressungen oder Blossstellungen genutzt wird. Auch Stimmen (Audio-Material) lassen

sich imitieren, so dass Betrugsdelikte (wie «CEO-Betrug») einfacher realisiert werden können. Zwar sind grundsätzlich solche Fälschungen nicht komplett neu (vgl. u.a. Photoshop), doch KI erweitert und vertieft die Möglichkeiten, und Fälschungen sind schwieriger als solche zu erkennen. Zugleich realisiert KI diese Fakes in viel kürzerer Zeit, als es Menschen händisch möglich wäre.

KI-generiertes Material kann dazu eingesetzt werden, dass Menschen Dinge tun, die sie sonst nicht tun würden. Diese Form der Manipulation führt gerade mit Blick auf die Politik dazu, die Gefahren von Fake News zu thematisieren, wobei dies über den eng gefassten Bereich der Straftaten hinausreicht. Auch die Fake News gab es bereits vor der KI; KI führt aber zu einer Potenzierung der Problematik. Durch Liken oder Reposten bestimmter Inhalte können KI-Systeme bspw. den Eindruck erwecken, dass in der Politik bestimmte Kandidat(inne)n oder eine bestimmte Bewegung besonders populär seien, und so die Nutzenden täuschen oder gar zu einem bestimmten Abstimmungsverhalten verleiten. Tools wie ChatGPT können automatisiert Texte mit Fehlinformationen verfassen und diese vielfach reproduzieren und so den Eindruck erwecken, als wären sie von einem Menschen geschrieben und von anderen Menschen verbreitet worden. Die Inhalte können zudem auf eine bestimmte Zielgruppe zugeschnitten werden, um deren Interessen zu bedienen. Das kann zur Folge haben, dass sich Menschen noch stärker in bestimmte «Echo-Kammern» zurückziehen, was die gesellschaftliche Polarisierung vorantreiben könnte.

Möglicherweise wird KI in Zukunft auch eigenständig kriminelle Taten begehen, d.h. nicht allein als Instrument eines absichtsvollen Handelns einer Tatperson genutzt werden. Dies wird als «*Crime by AI*» (Hayward & Maas 2020) bezeichnet und führt zu der Frage der Verantwortlichkeit der KI; vergleichbare Diskussionen finden bspw. in Bezug auf das autonome Fahren und mögliche



«Ein Bereich, der hinsichtlich der Frage der Aufklärung von Straftaten (aber auch der Prävention dieser) von besonderem Interesse ist, ist die KI-gesteuerte Überwachung.»

Unfälle, die dabei geschehen, statt. In einem Experiment wurde gezeigt, dass KI-Systeme profitable Handels-Strategien entdecken und erlernen sowie auch anwenden können, die auf Marktmanipulation hinauslaufen (Platzierung falscher Kaufaufträge); KI könnte also u.a. im Bereich der Wirtschaftskriminalität tatsächlich eigensinnig strafbar handeln.

Die Betrachtung des Zusammenhangs von KI und Kriminalität wäre aber unvollständig, wenn sich einzig auf das Begehen von Straftaten konzentriert würde. KI kann daneben auch dafür eingesetzt werden, *Präventionsmassnahmen* zu entwickeln, *Straftaten aufzudecken und aufzuklären*. Ebenso wie KI dafür genutzt werden kann, Phishing-Mails zu erstellen oder Schadsoftware zu programmieren, kann sie genutzt werden, diese zu erkennen und damit die Cybersicherheit von Privatpersonen ebenso wie für Organisationen zu erhöhen und damit präventiv zu wirken (vgl. u.a. Pohlmann 2022, S. 586f). Ebenso kann KI genutzt

werden, Social-Media-Kommunikation mit Blick auf die Verbreitung von Formen problematischen Materials zu durchsuchen. Diese Form der Unterstützung der Aufdeckung von Straftaten durch KI wird bspw. mit Blick auf Hate Speech diskutiert (u.a. Halvani 2023).

Gerade aufgrund von Fortschritten im Bereich des Deep Learnings (DL) und des Natural Language Processings (NLP) weist KI hierfür ein hohes Potenzial auf, wenngleich Formen der Verschleierung von Hate Speech (mittels u.a. Bild und Video, Ironie, Sarkasmus, Memes oder codierter Sprache) weiterhin Herausforderungen für die automatisierte Erkennung darstellen. Daneben ist KI bedeutsam, um über Bild- und Videoanalyse andere Formen von Straftaten aufzudecken, so z.B. sexuellen Kindesmissbrauch. Auch Tools zur Erkennung von Straftatenserien sind in diesem Zusammenhang zu nennen (z.B. PicseI).

Auch bei der weiteren Aufklärung von Straftaten bzw. der Strafverfolgung ergeben sich unterschiedliche Einsatz-

möglichkeiten von KI. Angesprochen sind dabei Anwendungen wie die automatisierte Gesichts- oder Spracherkennung, die KI-gestützte Auswertung von Beweismaterial (wie E-Mails, Textnachrichten, Bilder, Social-Media-Posts), die automatisierte Erkennung von Dokumenten wie Identitätsnachweisen und andere mehr. Diese, wie auch andere KI-Anwendungen, kommen teilweise bereits in der Schweiz zum Einsatz (vgl. Simmler et al. 2023).

Ein Bereich, der hinsichtlich der Frage der Aufklärung von Straftaten (aber auch der Prävention dieser) von besonderem Interesse ist, ist die KI-gesteuerte *Überwachung*. Insofern der öffentliche Raum zunehmend mit Videokameras ausgestattet ist, steht Material zur Verfügung, dass zur Erkennung (des Gesichts, des Verhaltens usw.) genutzt werden kann. Da Gesichter (im Gegensatz zu Fingerabdrücken) schwer zu verbergen sind und aus der Ferne unbemerkt aufgezeichnet und gescannt werden können, liegt in der Gesichtserkennung ein Potenzial für

die Strafverfolgung, wobei hier, wie bei anderen KI-Anwendungen, Fragen des Datenschutzes und der Persönlichkeitsrechte zu klären sind; in China, das auf diese Fragen deutlich weniger Wert legt, sind diese Techniken bereits in der Anwendung (Grzanna 2023). Dystopische Überlegungen gehen zudem davon aus, dass die Kopplung KI-gestützter Videoüberwachung und KI-gestützter Drohnentechnologie die formelle Kontrolle der Bürgerinnen und Bürger auf ein völlig neues Niveau heben könnte (Hayward & Maas 2020, S. 12).

Ähnlich umfangreich diskutiert wie die Implikationen von KI für das Begehen von Straftaten, ist der mögliche Nutzen von KI für die *Prognose von Kriminalität*. Dies betrifft einerseits die Prognose des Begehens von Straftaten (predictive policing), in einem bestimmten Zeitraum in einem bestimmten Gebiet. Diese Anwendungen finden sich bereits vor der Einführung neuer KI-Anwendungen, wie die bekannten Beispiele der Programme PreCops oder PredPol zeigen. Studien belegen, dass KI-Technologien bei der Vorhersage von Straftaten wertvolle Informationen liefern können; die KI-Technologie verbessert dabei die Effizienz vor allem bei der Nutzung von Anwendungen zur räumlich-zeitlichen Identifizierung von Kriminalitätsschwerpunkten (u.a. Dakalbab et al. 2022). Zugleich gibt es beim Einsatz solcher Programme fundamentale Aspekte zu beachten, insbesondere die Objektivität des Regelwerks und die Transparenz der genutzten Daten (u.a. Farthofer 2023), um die Gefahr verzerrter Prognosen in der Anwendung zu reduzieren.

Prognosen können sich aber nicht allein auf die Vorhersage von Taten (oder Hotspots) beziehen, sondern ebenso einzelne Personen fokussieren. Bei der individuellen Prognose wird bspw. betrachtet, ob von einer Person eine erhöhte Gefährdung insbesondere für das Begehen von Gewaltdelikten ausgeht. Bewertet werden kann bei einer individuellen Prognose aber auch das Risiko, dass Straftäterinnen und

Straftäter erneut straffällig werden (Rückfall). Auch hierbei gilt, dass Verfahren der individuellen Prognose bereits vor KI in Form strukturierter Einschätzungsinstrumente existiert haben. KI erlaubt aber nun, weitere und vor allem umfassendere Informationen für die Prognose zu gebrauchen. Generell kann auch für den Bereich individueller Prognosen ein gewisser Nutzen festgestellt werden, wenngleich hier verschiedene Probleme noch stärker zu gewichten sind: So können Algorithmen Individuen aufgrund ihrer Zugehörigkeit zu einer spezifischen Bevölkerungsgruppe systematisch diskriminieren (insofern die Trainings-Grundlage der KI entsprechend verzerrt ist); und eine Diskriminierung kann dann «gravierende negative Auswirkungen auf das Leben des Einzelnen haben, wenn er sich mit ständigen gegen ihn gerichteten Massnahmen konfrontiert sieht» (Farthofer 2023, S. 308).

Zuletzt sind noch mindestens zwei weitere Themen zu benennen: KI kann im Bereich des Strafprozesses und insbesondere der *Urteilsfindung* eingesetzt werden. Und KI kann die *wissenschaftliche Untersuchung* der Kriminalität bereichern. Bezüglich des Strafprozesses gilt, dass die Anzahl und ggf. auch die Komplexität von Fällen zuzunehmen scheinen. So titelte bspw. der Tagesanzeiger vom 23.7.2023 «Schweizer Justiz vor dem Kollaps – Über 100 000 offene Fälle». Zugleich gibt es Hinweise darauf, dass gesprochene Urteile von verschiedenen Faktoren abhängig sind, die nicht allein mit den Merkmalen des Falls selbst in Zusammenhang stehen; so ergeben sich immer wieder erstaunliche regionale Unterschiede in der Strafzumessung. KI könnte daher eingesetzt werden, um Informationen zum Verfahren aufzubereiten und gestützt auf landesweit vergleichbare Fälle Vorschläge bzgl. des Urteils zu entwickeln (vgl. hierfür und mögliche Probleme Kaspar et al. 2023).

Auch die wissenschaftliche Analyse kriminellen Verhaltens kann durch KI neue Impulse erhalten. Zu nennen sind

hier bspw. Simulationsstudien, die der Frage nachgehen, unter welchen Bedingungen sich Personen mit bestimmten Eigenschaften (bzw. mit bestimmten, für das KI-Training bereitgestellten Informationen) kriminell verhalten oder nicht. Auch könnte KI bei der Weiterentwicklung von Virtual-Reality-Szenarien eingesetzt werden, die in der Kriminologie zunehmend zum Einsatz kommen, um das Zustandekommen von Straftaten zu untersuchen (u.a. van Gelder & Thielmann 2023). Die kriminologischen Bereiche der Vorhersage kriminellen Verhaltens bzw. des Rückfalls von Straftäterinnen und Straftätern, aber ebenso weitere Themenfelder der forensischen Psychologie (Diagnostik, Therapie, Aussagebeurteilung usw.) dürften ebenfalls weitere Impulse durch KI erhalten.

### Wie sieht die Bevölkerung das Verhältnis von KI und Kriminalität?

Unter Rückgriff auf das Panel des Markt- und Sozialforschungsunternehmens LINK wurde im Februar 2024 eine schweizweit repräsentative Befragung unter 2040 Personen ab 16 Jahren zum Zusammenhang von KI und Kriminalität durchgeführt. Dabei gaben 98,9% der Befragten an, dass sie schon einmal vom Begriff «Künstliche Intelligenz» gehört oder gelesen haben; immerhin 19,5% der Befragten meinten, dass sie viel oder sehr viel über KI wüssten. 88,4% der Befragten hatten schon einmal von ChatGPT oder anderen Chatbots (Google Bard, Bing Chat AI) gehört oder gelesen. Zudem gaben 41,4% der Befragten an, im Alltag schon einmal Anwendungen genutzt zu haben, die mit KI funktionieren; ChatGPT oder andere Chatbots nutzen bereits 31,6% der Befragten. Insofern kann gesagt werden, dass das Wissen über und die Nutzung von KI durchaus in der Schweizer Bevölkerung gegeben ist.

Die Befragten wurden daneben gebeten, einzuschätzen, wie aus ihrer Sicht KI Kriminalität in der Gesellschaft verändern wird. In Abbildung 1 ist die

## KÜNSTLICHE INTELLIGENZ UND KRIMINALITÄT

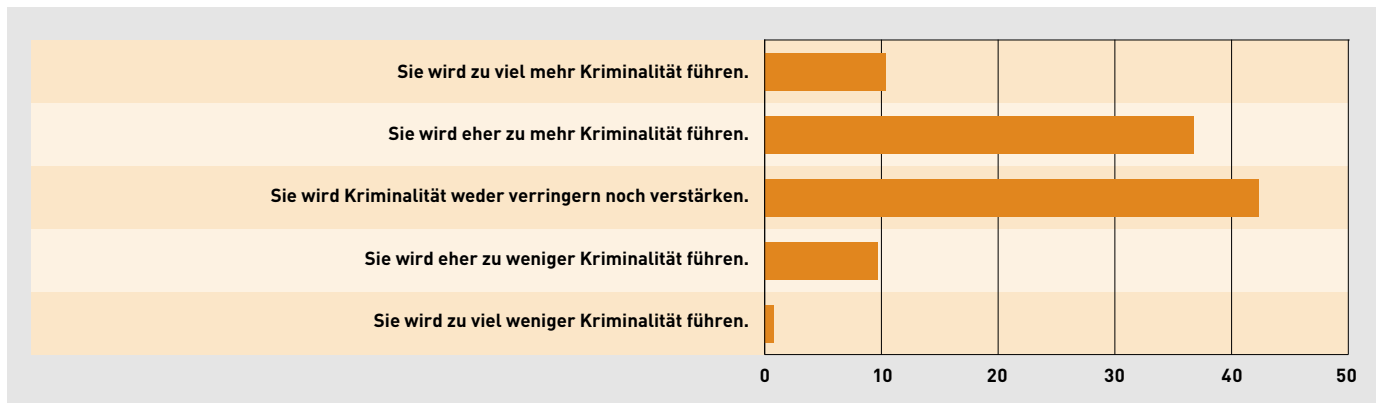


Abbildung 1: Antwortverteilung auf die Frage «Was glauben Sie, wie wird Künstliche Intelligenz Kriminalität in der Gesellschaft verändern?» (n = 1876; gewichtete Daten)

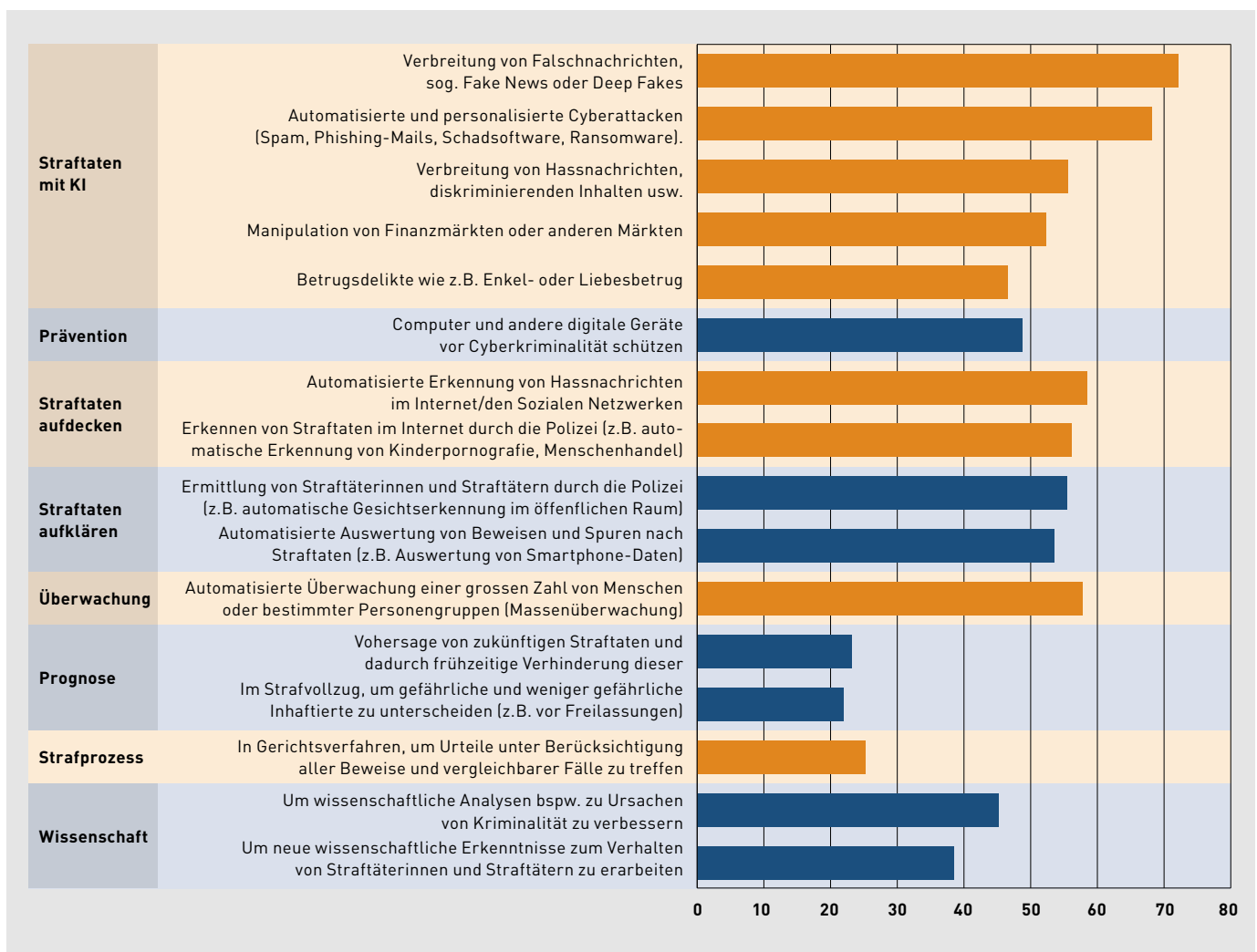


Abbildung 2: Anteil Befragter, die Einsatz von KI als eher wahrscheinlich einstufen (N<sub>Min</sub> = 1750, gewichtete Daten)

Antwortverteilung dargestellt. Nur eine Minderheit (10,5%) geht davon aus, dass KI zu weniger bzw. viel weniger Kriminalität führt. Demgegenüber meinen 47,2% und damit fast die Hälfte

der Befragten, dass KI zu einem Anstieg der Kriminalität führen wird. Eine eher skeptische Haltung gegenüber den kriminalitätsbezogenen Implikationen von KI dominiert also.

Ein kleiner Teil von 4,7% der Befragten gab an, selbst bereits einmal erlebt zu haben, dass KI eingesetzt wurde, um ihnen in krimineller Weise Schaden zuzufügen. Im Wesentlichen handelte



es sich dabei um Betrugsdelikte, wie Eintragungen der Befragten zeigen, wobei letztlich nicht immer klar ist, ob tatsächlich KI zum Einsatz kam: «Bot für Versenden von Spam Mails», «Deep phishing», «Diverse Spam Mails, Hackerangriff auf Kreditkarte», «Ein Telefonanruf klang nach künstlicher Stimme», «Gefälschte Mails/Websites, um geschäftliche Käufe abzuwickeln» oder «Online Betrug».

Entlang der oben dargestellten Themenbereiche sollten die Befragten zudem folgende Frage beantworten: «Als wie wahrscheinlich erachten Sie es, dass Künstliche Intelligenz hierfür zum Einsatz kommt?». Die Antwortvorgaben reichten dabei von «1 – überhaupt nicht wahrscheinlich» bis «10 – sehr wahrscheinlich». Für eine übersichtliche Darstellung wurden die Befragten mit den Antworten 8, 9 und 10 zur Gruppe «eher wahrscheinlich» zusammengefasst. Der Anteil dieser Befragten ist in Abbildung 2 dargestellt. Dabei zeigt sich, dass eine Mehrheit der Befragten es als eher wahrscheinlich einstuft, dass verschiedene Straftaten mit KI begangen werden. Insbesondere wird von der Bevölkerung erwartet, dass Falschnachrichten verbreitet und personalisierte Cyberattacken zunehmen. Der präventive Nutzen von KI wird hingegen von weniger Befragten gesehen: Nur 48,8% meinten, dass es eher wahrscheinlich ist, dass KI eingesetzt wird, um Computer bzw. andere Geräte vor Cyberkriminalität zu schützen.

Daneben zeigt sich zu drei Bereichen, dass jeweils etwas mehr als die Hälfte der Befragten es als wahrscheinlich erachtet, dass KI hier zum Einsatz kommt. Dies betrifft den Bereich der Aufdeckung von Straftaten, der Aufklärung von Straftaten und der Überwachung. 58,5% der Befragten gehen davon aus, dass KI eingesetzt werden kann, um automatisiert Hassnachrichten zu erkennen, 57,8%, dass KI zur Massenüberwachung eingesetzt wird. Deutlich weniger Befragte sind hingegen der Auffassung, dass KI zu

verschiedenen Formen der Prognose bzw. im Strafprozess eingesetzt wird. Ein etwas grösserer Anteil (wenngleich weniger als die Hälfte der Befragten) sieht in KI ein Potenzial, die wissenschaftliche Untersuchung der Kriminalität weiterzuentwickeln.

### Schluss

Wie die Auswertungen der Befragung zeigen, findet sich ein eher skeptischer Blick auf KI in der Bevölkerung, wobei an dieser Stelle nur der Kriminalitätsbereich betrachtet wurde. Allerdings zeigt sich auch in Bezug auf andere Bereiche wie bspw. die Arbeitswelt, dass KI eher als Problem wahrgenommen wird («KI wird Arbeitsplätze gefährden»; vgl. z.B. Cousseran et al. 2023, S. 23f). Es wäre daher wichtig, verstärkt positive Einsatzmöglichkeiten der KI, die u.a. in der Prävention oder Straftatenverfolgung und -aufdeckung zu verorten sind, zu untersuchen und öffentlich zu diskutieren.

Zu beachten ist daneben, dass sich diese Einsatzmöglichkeiten der KI permanent und schnell verändern. Die in diesem Beitrag angesprochenen Bereiche sind sicherlich schon teilweise überholt, wenn der Beitrag erscheint. Diese hohe Dynamik des Bereichs ist gerade für Polizei und andere Sicherheitsakteure herausfordernd. Nur die nationale und internationale Vernetzung untereinander und mit weiteren Feldern wie der Wissenschaft garantiert, dass weiterentwickelte oder neue Formen der KI-Kriminalität effektiv verhindert bzw. verfolgt werden können.

Auch die Kriminologie tut gut daran, sich verstärkt mit der KI auseinanderzusetzen. Ein methodischer Ansatz, der dabei verstärkt zur Anwendung kommen könnte, wären Delphi-Studien. Mit diesen könnte versucht werden, zukünftige Einsatzmöglichkeiten der KI im Kriminalitätsbereich auf Basis der systematischen Nutzung von Wissen von Expertinnen und Experten frühzeitig abzuschätzen, was wiederum eine zentrale Grundlage wäre, sich auf diese Möglichkeiten gezielt vorzubereiten.

### Literatur

Blauth, T.F., Gstrein, O.J., Zwitter, A. (2022). *Artificial Intelligence Crime: An Overview of Malicious Use and Abuse of AI*. IEEE Access, 10, 77110-77122. doi: 10.1109/ACCESS.2022.3191790.

Cousseran, L., Lauber, A., Herrmann, S., Brügggen, N. (2023). *Kompass: Künstliche Intelligenz und Kompetenz 2023. Einstellungen, Handeln und Kompetenzentwicklung im Kontext von KI*. München: kopaed.

Dakalbab, F. et al. (2022). Artificial intelligence & crime prediction: A systematic literature review. *Social Sciences & Humanities Open*, 6. doi: 10.1016/j.ssaho.2022.100342.

Farthofer, H. (2023). Der Einsatz von Künstlicher Intelligenz in der Kriminalprävention. In T.-G. Rüdiger, P. S. Bayerl (Hrsg.), *Handbuch Cyberkriminalologie 1* (S. 293-316). Wiesbaden: Springer.

Grzanna, M. (2023). Wie Künstliche Intelligenz in China der Überwachung dient – und zum Exportschlagler wird. *Frankfurter Rundschau* vom 13.8.2023.

Halvani, O. (2023). Möglichkeiten zur Erkennung von Hate Speech. *Datenschutz und Datensicherheit*, 47, 209-214.

Hayward, K.J., Maas, M.M. (2020). Artificial intelligence and crime: A primer for criminologists. *Crime, Media, Culture*, 17, 209-233. doi: 10.1177/1741659020917434.

Kaspar, J., Harrendorf, S., Butz, F., Höffler, K., Sommerer, L., Christoph, S. (2023). Artificial Intelligence and Sentencing from a Human Rights Perspective. In: A. Završnik, K. Simončič (Eds.), *Artificial Intelligence, Social Harms and Human Rights. Critical Criminological Perspectives*. Cham: Palgrave.

Pohlmann, N. (2022). *Cyber-Sicherheit. Das Lehrbuch für Konzepte, Prinzipien, Mechanismen, Architekturen und Eigenschaften von Cyber-Sicherheitssystemen in der Digitalisierung* (2. Aufl.). Wiesbaden: Springer.

Simmler, M., Brunner, S., Canova, G., Schedler, K. (2023). Smart criminal justice: exploring the use of algorithms in the Swiss criminal justice system. *Artificial Intelligence and Law*, 31, 213-237. doi: 10.1007/s10506-022-09310-1.

van Gelder, J.-L., Thielmann, I. (2023). Die Lücken in der kriminologischen Wissensgrundlage schliessen: Eine Forschungsagenda für die kommenden zehn Jahre. *Monatsschrift für Kriminologie und Strafrechtsreform*, 106, 18-28. doi: 10.1515/mks-2022-0030.