

Blick in die Zukunft: KI in der Strafverfolgung

Valbella, 25. Oktober 2024

«It is difficult to predict, especially the future.»

Ignazio Cassis, Rede «Blick in die Zukunft» am 4.11.2021 in Luzern, zitiert den dänischen Physiker Niels Bohr



«It is difficult to predict, especially the future.» [...] Selbst die beste Strategieschöpfung fusst in der Vergangenheit, wenn sie sich bloss auf gesicherte Daten und bewährte Praxis abstützt.»

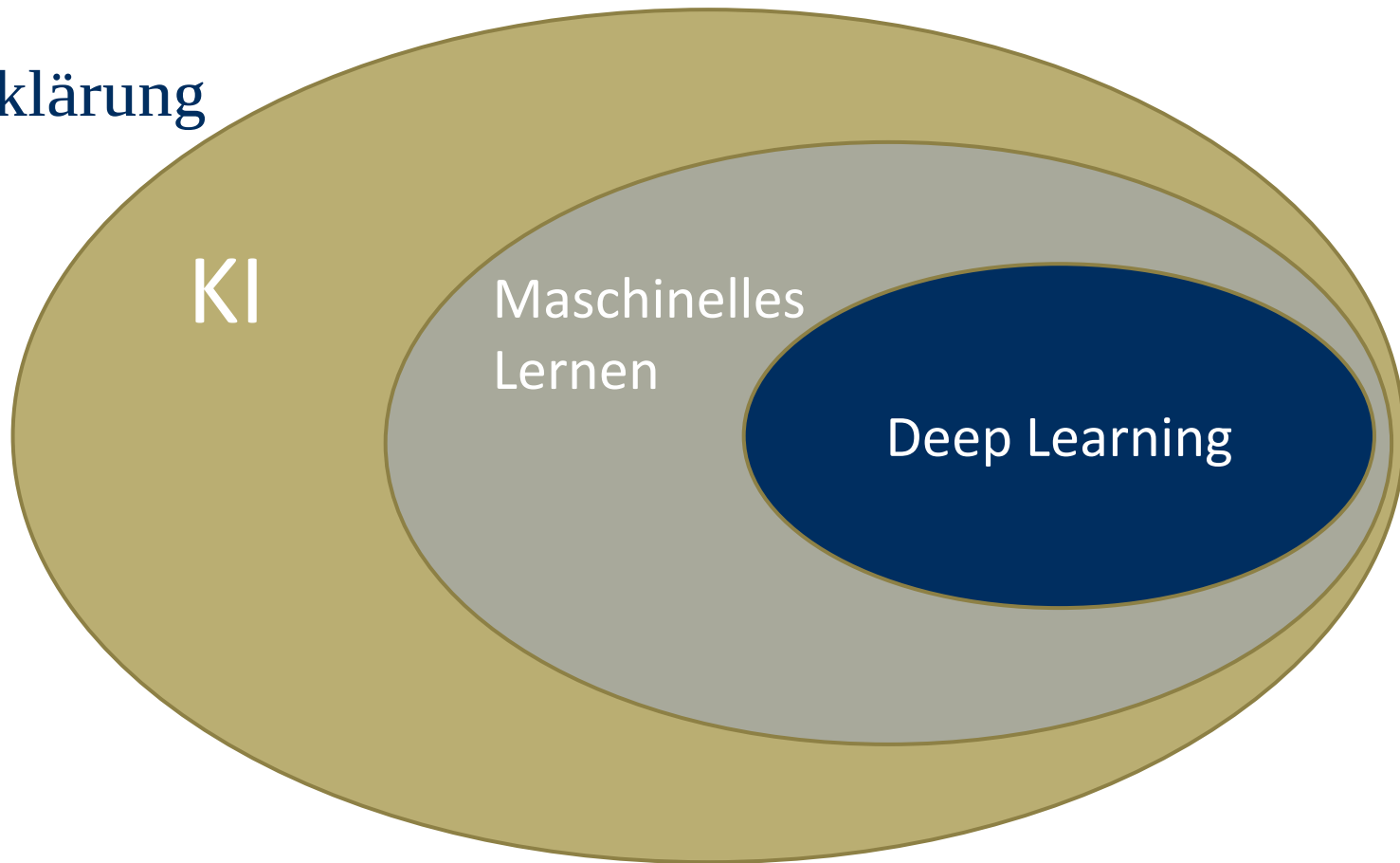
Ignazio Cassis, Rede «Blick in die Zukunft» am 4.11.2021 in Luzern



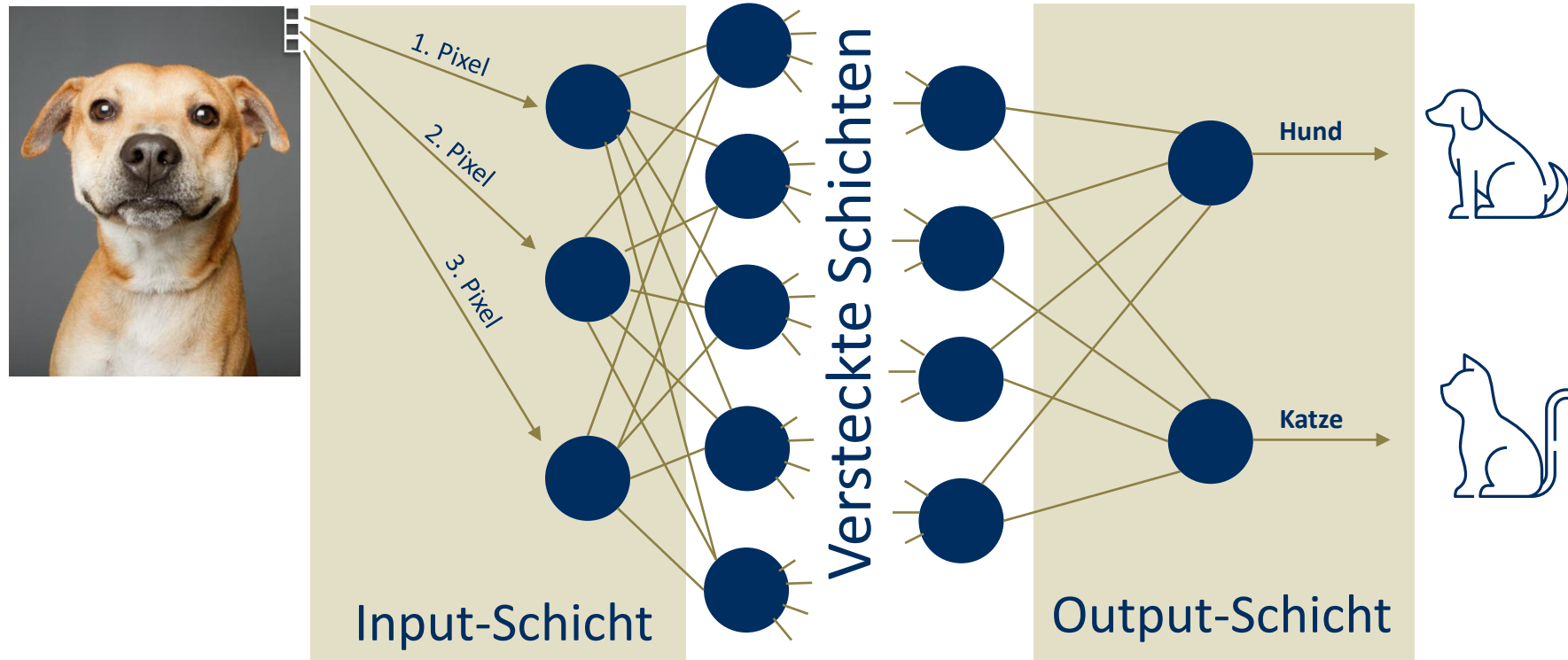
Gesicherte Daten?

Einführung in Künstliche Intelligenz

Begriffsklärung



Künstliche Neuronale Netze



Chihuahua oder Muffin?



Source: www.freecodecamp.org

Die (bewährte?) Praxis

in der Schweiz und im Ausland



NZZ

Einbruchsalgorithmus schlug zu wenig Alarm: Erstes Polizeikorps setzt umstrittene Analyse-Software ab

Eine Software, die nach Mustern bei Einbruchsdiebstählen sucht, soll bei der Entdeckung von Serientätern helfen. Wie gross der Nutzen ist, ist aber nicht klar. Und Corona hat das Tool zusätzlich geschwächt.

Daniel Gerny

07.11.2021, 08.04 Uhr



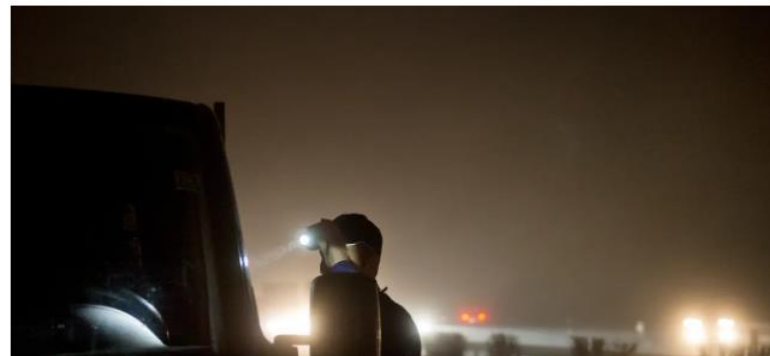
Merken

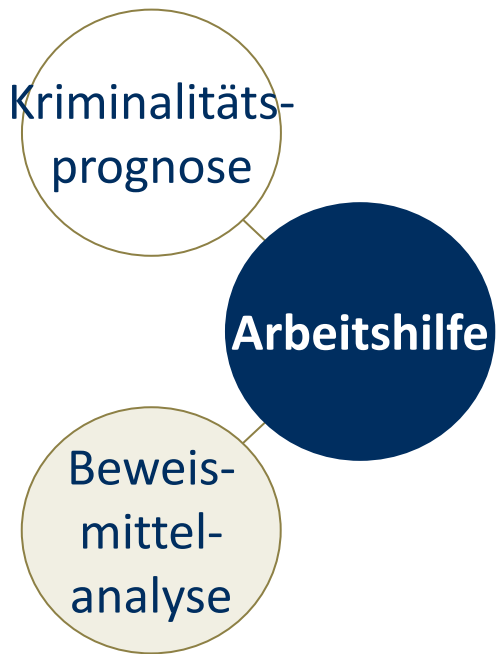


Drucken



Teilen



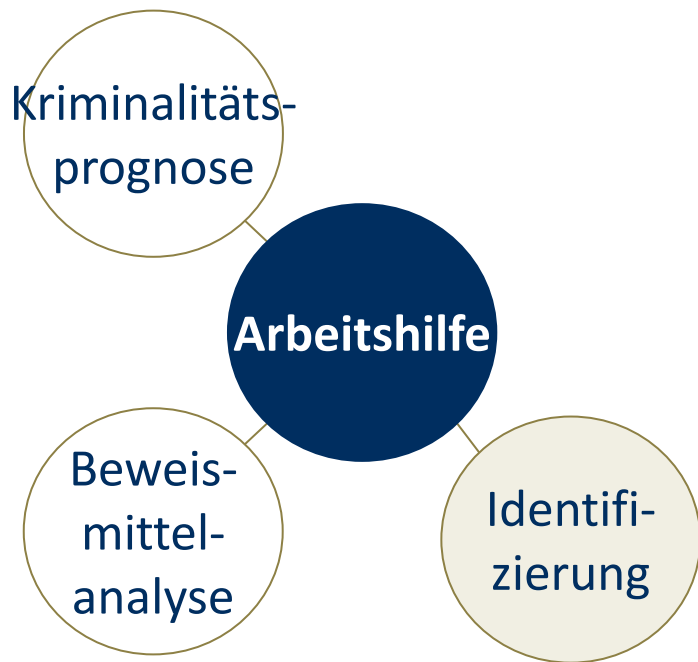


Sicherheit und Prävention

Zürcher Polizei will Terroristen mit künstlicher Intelligenz jagen

Um Terror-Anschläge verhindern zu können, will die Zürcher Sicherheitsdirektion auf künstliche Intelligenz setzen. Sie soll der Polizei helfen, die Daten in geschlossenen Chats und Foren zu sichten. Auch Kontrollschilder sollen automatisch gelesen werden.

Publiziert: 12.09.2024 um 12:04 Uhr | Aktualisiert: 12.09.2024 um 12:23 Uhr



Polizeikorps nutzen automatisierte Gesichtserkennung für die Fahndung: Bald könnte die Software auch nach Demos oder Fanmärschen eingesetzt werden

Mehrere Kantone setzen bereits heute Gesichtserkennungs-Software ein, darunter St. Gallen. Bald könnte die Anwendung ausgeweitet werden – zum Beispiel um gewalttätige Demonstranten zu erkennen. Kritiker warnen vor einer schleichenden Massenüberwachung.

Daniel Gerny

02.07.2022, 05:30 Uhr



Merken



Drucken



Teilen



Der rechtliche Status Quo

in der EU und in der Schweiz



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)

(Text von Bedeutung für den EWR)

DAS EUROPÄISCHE PARLAMENT UND DER RAT DER EUROPÄISCHEN UNION —

gestützt auf den Vertrag über die Arbeitsweise der Europäischen Union, insbesondere auf die Artikel 16 und 114,

auf Vorschlag der Europäischen Kommission,

nach Zuleitung des Entwurfs des Gesetzgebungsakts an die nationalen Parlamente,

nach Stellungnahme des Europäischen Wirtschafts- und Sozialausschusses (*),

nach Stellungnahme der Europäischen Zentralbank (*),

nach Stellungnahme des Ausschusses der Regionen (*),

gemäß dem ordentlichen Gesetzgebungsverfahren (*),

in Erwägung nachstehender Gründe:

- (1) Zweck dieser Verordnung ist es, das Funktionieren des Binnenmarkts zu verbessern, indem ein einheitlicher Rechtsrahmen insbesondere für die Entwicklung, das Inverkehrbringen, die Inbetriebnahme und die Verwendung von Systemen künstlicher Intelligenz (KI-Systeme) in der Union im Einklang mit den Werten der Union festgelegt wird, um die Einführung von menschenzentrierter und vertrauenswürdiger künstlicher Intelligenz (KI) zu fördern und gleichzeitig ein hohes Schutzniveau in Bezug auf Gesundheit, Sicherheit und der in der Charta der Grundrechte der Europäischen Union („Charta“) verankerten Grundrechte, einschließlich Demokratie, Rechtsstaatlichkeit und Umweltschutz, sicherzustellen, den Schutz vor schädlichen Auswirkungen von KI-Systemen in der Union zu gewährleisten und gleichzeitig die Innovation zu unterstützen. Diese Verordnung gewährleistet den grenzüberschreitenden freien Verkehr KI-gestützter Waren und Dienstleistungen, wodurch verhindert wird, dass die Mitgliedstaaten die Entwicklung, Vermarktung und Verwendung von KI-Systemen beschränken, sofern dies nicht ausdrücklich durch diese Verordnung erlaubt wird.
- (2) Diese Verordnung sollte im Einklang mit den in der Charta verankerten Werten der Union angewandt werden, den Schutz von natürlichen Personen, Unternehmen, Demokratie und Rechtsstaatlichkeit sowie der Umwelt erleichtern und gleichzeitig Innovation und Beschäftigung fördern und der Union eine Führungsrolle bei der Einführung vertrauenswürdiger KI verschaffen.
- (3) KI-Systeme können problemlos in verschiedenen Bereichen der Wirtschaft und Gesellschaft, auch grenzüberschreitend, eingesetzt werden und in der gesamten Union verkehren. Einige Mitgliedstaaten haben bereits die Verabschiedung nationaler Vorschriften in Erwägung gezogen, damit KI vertrauenswürdig und sicher ist und im Einklang mit den Grundrechten entwickelt und verwendet wird. Unterschiedliche nationale Vorschriften können zu einer Fragmentierung des Binnenmarkts führen und können die Rechtssicherheit für Akteure, die KI-Systeme entwickeln, einführen oder verwenden, beeinträchtigen. Daher sollte in der gesamten Union ein einheitlich hohes Schutzniveau sichergestellt werden, um eine vertrauenswürdige KI zu erreichen, wobei Unterschiede, die den freien Verkehr, Innovationen, den Einsatz und die Verbreitung von KI-Systemen und damit zusammenhängenden

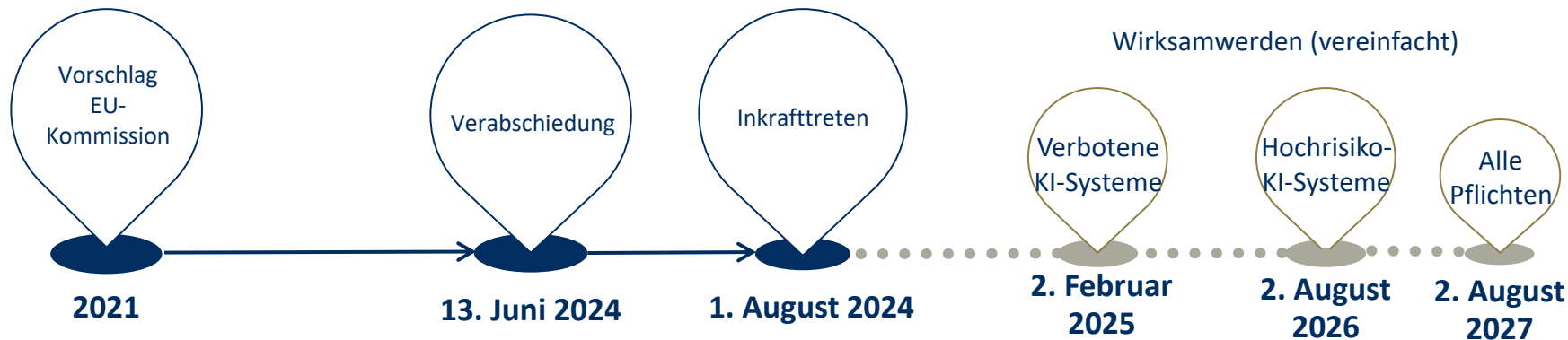
(*) ABL C 517 vom 22.12.2021, S. 56.

(*) ABL C 115 vom 11.3.2022, S. 5.

(*) ABL C 97 vom 28.2.2022, S. 60.

(*) Standpunkt des Europäischen Parlaments vom 13. März 2024 (noch nicht im Amtsblatt veröffentlicht) und Beschluss des Rates vom 21. Mai 2024.

KI-VO: Inkrafttreten / Wirksamwerden



KI-VO: Personell-räumlicher Anwendungsbereich

- Verordnung = unmittelbar anwendbar in EU-Mitgliedstaaten
- KI-System wird in der EU in Verkehr gesetzt oder in Betrieb genommen
- Auch: Extraterritoriale Wirkung
 - Marktortprinzip
 - Anbieter und Betreiber von KI-Systemen, die in einem Drittland niedergelassen sind, soweit beabsichtigt wird, die von diesem System erzeugte Ausgabe in der Union zu verwenden



KI-VO: Personell-räumlicher Anwendungsbereich

- Nicht anwendbar auf:
 - Behörden eines Drittlands
 - im Rahmen der Zusammenarbeit oder internationaler Übereinkünfte für die Zusammenarbeit im Bereich der Strafverfolgung und der justiziellen Zusammenarbeit
 - Voraussetzung: Garantien für den Schutz der Grundrechte und -freiheiten
 - Empfangende Stellen, die Output in der Union verwenden, müssen sicherstellen, dass ihre Verwendung mit Unionsrecht vereinbar ist

- ➔ KI-VO für schweizerische Behörden *grundsätzlich* nicht anwendbar
- ➔ Anpassung internationaler Übereinkünfte?
- ➔ Jedenfalls Ausstrahlungswirkung auf die Schweiz zu erwarten (Brüssel-Effekt)



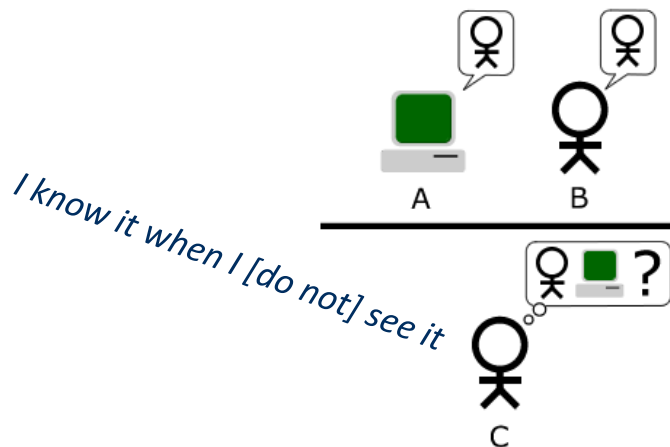
KI-VO: Sachlicher Anwendungsbereich

Art. 3 Nr. 1 KI-VO

«[...] bezeichnet der Ausdruck 'KI-System' ein maschinengestütztes System, das für einen in unterschiedlichem Grade autonomen Betrieb ausgelegt ist und das nach seiner Betriebsaufnahme anpassungsfähig sein kann und das aus den erhaltenen Eingaben für explizite oder implizite Ziele ableitet, wie Ausgaben wie etwa Vorhersagen, Inhalte, Empfehlungen oder Entscheidungen erstellt werden, die physische oder virtuelle Umgebungen beeinflussen können»

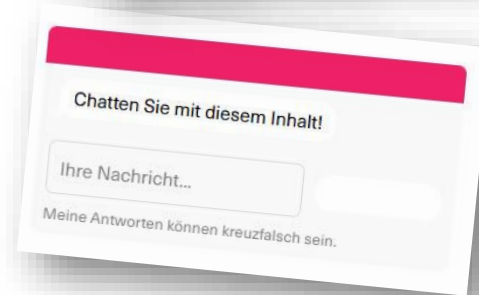
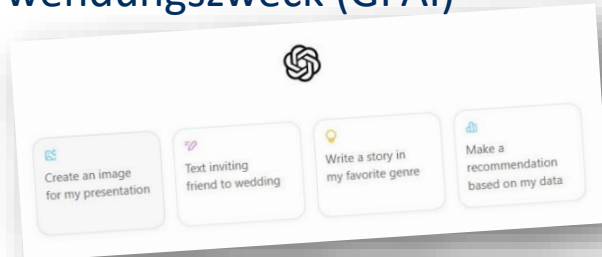
Europäisches Parlament

«Künstliche Intelligenz ist die Fähigkeit einer Maschine, menschliche Fähigkeiten wie logisches Denken, Lernen, Planen und Kreativität zu imitieren»



KI-VO: Funktionsweise

- Risikobasierter Ansatz
 - **Verbotene KI-Systeme**
 - **Hochrisiko-KI-Systeme**
 - KI-Systeme, die zur Interaktion mit Menschen gedacht sind
 - Sonstige KI-Systeme
- KI-Systeme mit allgemeinem Verwendungszweck (GPAI)





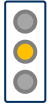
KI-VO: Verbotene Systeme

- Verbotene KI-Systeme (Inverkehrbringen, Inbetriebnahme, Verwendung)
- Auswahl
 - Predictive Policing (mit Ausnahmen)
 - Erstellen von Gesichtserkennungsdatenbanken durch breites Scraping
 - Real-time Gesichtserkennung, ausser unbedingt erforderlich
 - im Zusammenhang mit der Suche nach Opfern bestimmter Straftaten
 - für die Abwehr unmittelbarer Gefahren für Leib und Leben
 - Abwenden der konkreten Gefahr eines Terroranschlags
 - für das Aufspüren/Identifizieren von Verdächtigen, bei Freiheitsstrafe von >4 Jahren



KI-VO: Hochrisiko-KI-Systeme

- Hochrisiko-KI-Systeme: Insbesondere Anhang III
- 8 Fallgruppen mit Unterfallgruppen (z.B. kritische Infrastrukturen, Bildung, Arbeitsbereich, Rechtspflege, Grenzkontrolle)
- Nr. 6: Strafverfolgung, soweit ihr Einsatz nach einschlägigem Unionsrecht oder nationalem Recht zugelassen ist (Auswahl)
 - Lügendetektoren o.Ä.
 - Bewertung der Verlässlichkeit von Beweismitteln
 - Predictive Policing oder Profiling in engem Rahmen



KI-VO: Hochrisiko-KI-Systeme – Pflichten

- Anbieter
 - Training, Testen, technische Dokumentation, QMS
 - Transparenz, Sicherheit, Melden von Vorfällen
 - [...]
- Betreiber
 - Inventarisierung, Protokollierung
 - Handeln entsprechend Anweisung des Anbieters
 - Inputdaten
 - entspr. Zweck des HRAIS
 - Repräsentative Daten
 - Menschliche Überwachung
 - Bei Verdacht auf besonderes Risiko: Information der Marktüberwachungsbehörde (Anbieter und Händler bei festgestelltem besonderem Risiko)
 - [...]

...und in der Schweiz?

Analyse bzgl. Handlungsbedarf und Regulierungsoptionen

- Schweizer KI-Gesetz?
- Sektorenregulierung?

bis Ende
2024

15. März 2024

Abschluss Verhandlungen
zu KI-Abkommen des
Europarats

seit 1.9.2023

Informationspflicht
bei automatisierter
Einzelentscheidung,
Art. 21 DSGVO

Der Blick in die Zukunft

Künstliche Intelligenz in der Strafverfolgung

Use Case 1

Gesichts- erkennung





PinEyes

Search Pricing Blog News Opt-out FAQ

EN

Face Search Engine Reverse Image Search

UPLOAD PHOTO AND FIND OUT WHERE IMAGES ARE PUBLISHED

Upload photo(s)

Or you can take a photo with the device's camera. Don't worry, we will not store it!



Suche nach der RAF-Terroristin mit Gesichtserkennung: warum Journalisten tun, was Polizisten verboten bleibt

Auf der Suche nach Daniela Klette wurde eine Software zur Gesichtserkennung eingesetzt. Das zeigt: Die Lücke zwischen dem, was die Technik kann, und dem, was legal einsetzbar ist, wird immer grösser.

Giola da Silva, Ruth Fulterer
04.03.2024, 16:37 Uhr 4 min

Hören Merken Drucken Teilen

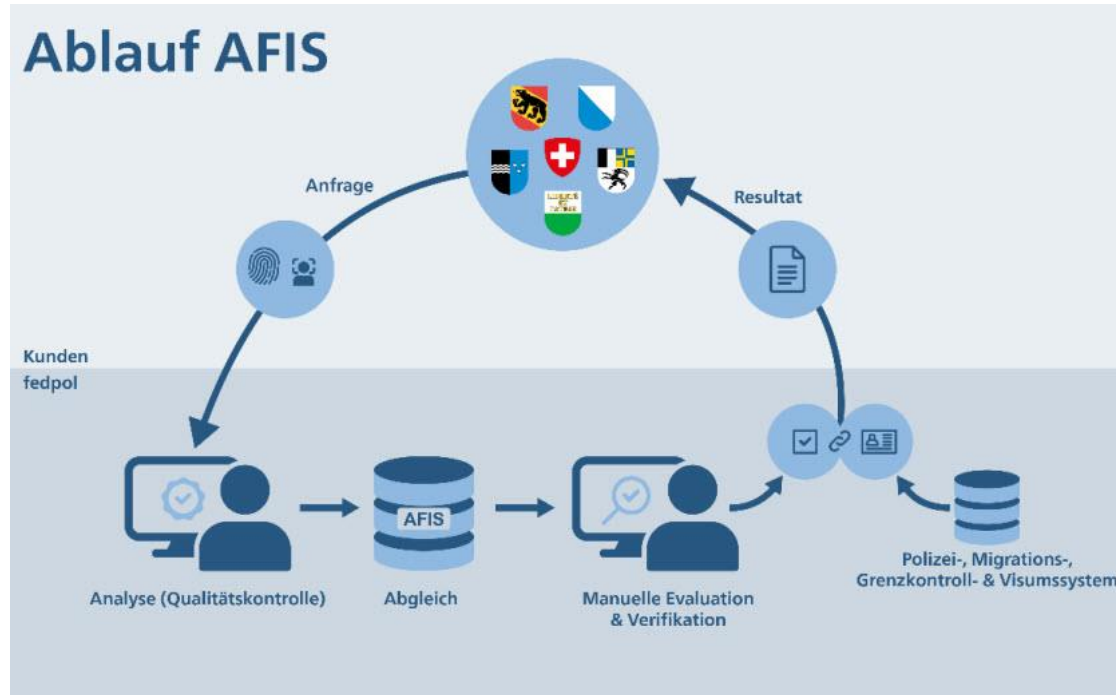
Rechtliche Einordnung: Schweiz

- Rechtsgrundlage erforderlich
 - Biometrische Aufnahme des Gesichts: Besonders schützenswertes Personendatum i.S.d. DSG = formell-gesetzliche Grundlage erforderlich
 - Allgemein: Gesetzesvorbehalt
- Art der Rechtsgrundlage abhängig vom Einsatzbereich (Ort, Zweck)
- Verschiedene Bearbeitungsschritte (vereinfacht)
 - Erstmalige Erfassung des Videomaterials
 - Analyse des Datenmaterials
 - Abgleich
 - Erkennung
 - Speicherung, Austausch mit anderen Behörden
 - [...]

Gesichtserkennung: Rechtsgrundlagen

- Art. 260 StPO: Erkennungsdienstliche Erfassung
 - Es können auch Dritte erfasst werden, wenn
 - Gründe dafür bestehen und
 - die Verhältnismässigkeit gewahrt ist (Schwere des aufzuklärenden Deliktes; Umstand, wie sehr die Sachverhaltsabklärung sonst erschwert würde)
 - z.B.: Unterscheidung von Spuren am Tatort (Dritter vs. Täter)
- Weitere Bearbeitung:
261 StPO, 354 StGB, Art. 14 Abs. 2 BPI,
Art. 2 ED-Verordnung

Automatisiertes Fingerabdruck-Informationssystem



Sitzung vom 10. Juli 2024

789. Anfrage (Einsatz von und Umgang mit Open-Source-Intelligence-Tools bei der Kantonspolizei Zürich)

3. Welche Regelungen kennt die Kantonspolizei im Umgang mit Gesichtserkennungssoftwares, anderen OSINT-Tools oder generell KI bei polizeilichen Ermittlungen? Sind diese Regelungen öffentlich einsehbar? Wenn ja, wo?

Zu Frage 3:

Die Kantonspolizei setzt lokal betriebene KI-Tools ein, um grössere, lokal vorhandene Datenmengen für die weitere Bearbeitung zu sortieren. KI wird beispielsweise eingesetzt, um festzustellen, ob in so gesicherten Daten Kinderpornografie enthalten ist. Die Kantonspolizei setzt auch gängige Suchmaschinen im Internet ein (z. B. Google und Bing). Die Nutzung solcher Software und öffentlich zugänglicher Informationen (Open Source Intelligence [OSINT]) ist in internen Vorschriften geregelt.

4. Sind OSINT-Tools wie PimEyes über die Dienstgeräte der Polizist:innen abrufbar oder gesperrt wie beispielsweise bei der Londoner Polizei?
5. Mindestens über private Geräte sind Tools wie PimEyes frei zugänglich. Wie verhindert die Kantonspolizei Fälle von «Parallel Construction», also dass Polizist:innen solche Tools einsetzen, ohne dies zu dokumentieren? Wird die Plausibilität von Wiedererkennungen geprüft?

Zu Fragen 4 und 5:

PimEyes wird von der Kantonspolizei nicht eingesetzt. Die Dienstgeräte sind zwar nicht für solche Anwendungen gesperrt, jedoch ist der Umgang mit OSINT in internen Vorschriften geregelt. Jegliche Beweisführung muss dokumentiert werden. Resultate aufgrund von rechtlich unzulässigen Ermittlungen sind nicht verwertbar.

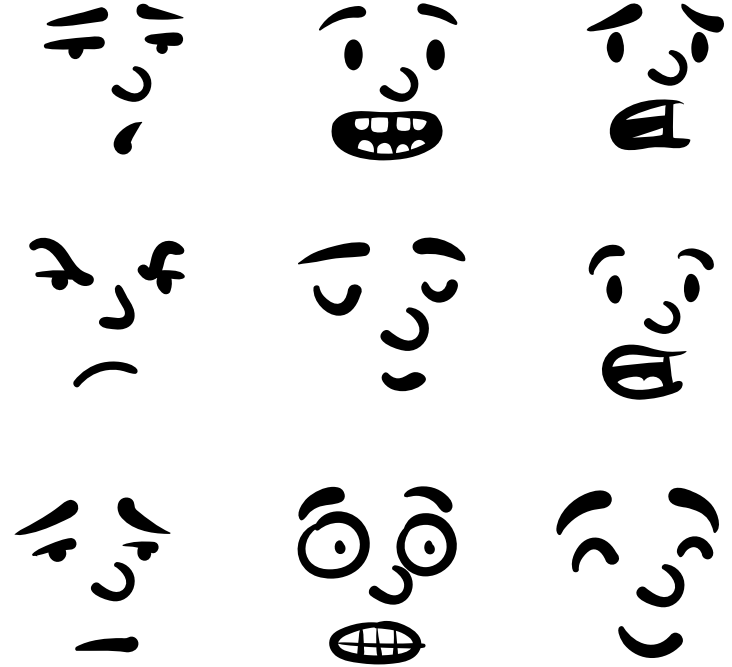
Use Case 2

KI-basierter Lügendetektor



Wie funktionieren KI-basierte Lügendetektoren?

- Grundannahmen
 - Stress, Angst, kognitive Belastung, etc. beeinflussen non-verbales Verhalten einer Person (Mimik, Gestik, Stimmlage etc.)
 - Non-verbales Verhalten ist messbar
 - Schluss von z.B. Gesichtsausdrücken auf Lüge ist möglich (Bestätigung dieser Hypothese steht aus)
- Nicht: physiologischer Erregungszustand wie Schwitzen, erhöhter Puls, etc. (Polygraphentest)



Um welche Art von Beweismittel handelt es sich?

- Sachverständigengutachten, Art. 185 StPO?
- Augenschein, Art. 193 StPO?
- Urkundenbeweis, Art. 192 Abs. 2 StPO?

– Art. 185 Ausarbeitung des Gutachtens

¹ Die sachverständige **Person** ist für das Gutachten **persönlich** verantwortlich.

Eingriff in die Grundrechte der Beschuldigten/Zeugen?

– Persönliche Freiheit, Art. 10 BV?

- (angeblich) «*Eingriff in den Kerngehalt der persönlichen Freiheit*» und «*Einbruch in den seelischen Eigenraum des Menschen*» (BGE 109 Ia 273 E. 7 vom 9.11.1983)
- Keine unzulässige Ausforschung des Unterbewussten, sondern Bewertung äusserlich erkennbarer Umstände
- nicht zu rechtfertigender Eingriff in Kernbereich fragwürdig:
Glaubhaftigkeitsgutachten sind nach h.M. zulässig

– Art. 140 Verbotene Beweiserhebungsmethoden

¹ Zwangsmittel, Gewaltanwendung, Drohungen, Versprechungen, Täuschungen und Mittel, welche die Denkfähigkeit oder die Willensfreiheit einer Person beeinträchtigen können, sind bei der Beweiserhebung untersagt.

² Solche Methoden sind auch dann unzulässig, wenn die betroffene Person ihrer Anwendung zustimmt.

Eingriff in die Grundrechte der Beschuldigten/Zeugen?

- **Informationelle Selbstbestimmung**, Art. 13 Abs. 2 BV?
 - (faktischer) Eingriff in Schutzbereich durch Messung von Personendaten (z.B. Augenbewegung) gegeben
 - Einwilligung entfaltet gemäss ErG 35 RL 2016/680 nicht per se rechtfertigende Wirkung
 - Verhältnismässigkeit entscheidend
 - Keine besonders schützenswerten Daten
 - Erhebt und bearbeitet werden die gleichen Eindrücke wie durch das Gericht, aber ggf. in höherer Geschwindigkeit
 - Eingriff tritt bei möglichem Entlastungsbeweis von schweren Straftaten aber wohl gegenüber drohenden Konsequenzen zurück

*«Bei der Alternative ‚Lebenslang‘ trotz denkbarer Unschuld [...] entscheidet man sich für die Lösung ‚Lebenslang‘.
Absurder geht es kaum noch. Man stelle sich eine Rechtsordnung vor, die bestimmte entlastende Zeugenaussagen vom Prozess ausschließt mit dem Argument, die Zeugen würden zwangsläufig Einzelheiten aus dem Intimbereich des Angeklagten berühren, was man zu seinem Schutz verhindern müsse.» (Schwabe, NJW 1982, 367)*

Eingriff in die Justiz-Grundrechte der Beschuldigten?

- **Nemo tenetur-Grundsatz, Art. 6 EMRK?**
 - «*Öffentliche Interessen können keine Massnahmen rechtfertigen, die zu einer Aushöhlung des Nemo tenetur-Grundsatzes führen*» (BGE 148 IV 205 E. 2.8.5)
 - Gefahr, dass Ablehnung der fraglichen Methode als Verdachtsmoment interpretiert wird (Botschaft revStPO BBl 2006, 1183)
 - Einsatz nur bei Zeugen?

– Art. 185 Ausarbeitung des Gutachtens

¹ Die sachverständige Person ist für das Gutachten persönlich verantwortlich.

² Die Verfahrensleitung kann die sachverständige Person zu Verfahrenshandlungen beiziehen und sie ermächtigen, den einzuvernehmenden Personen Fragen zu stellen.

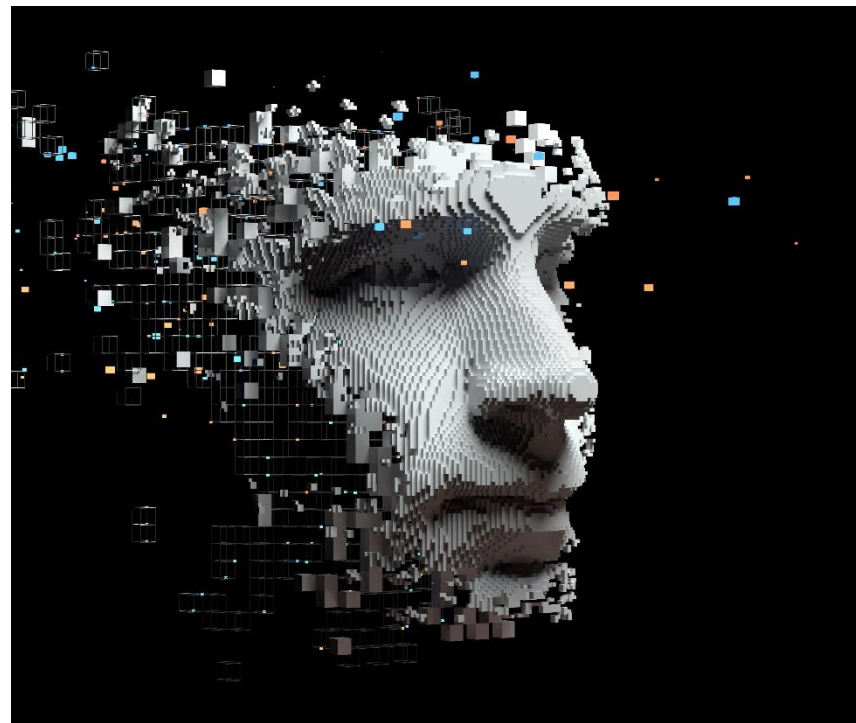
³ Hält die sachverständige Person Ergänzungen der Akten für notwendig, so stellt sie der Verfahrensleitung einen entsprechenden Antrag.

⁴ Die sachverständige Person kann einfache Erhebungen, die mit dem Auftrag in engem Zusammenhang stehen, selber vornehmen und zu diesem Zweck Personen aufbieten. Diese haben dem Aufgebot Folge zu leisten. Weigern sie sich, so können sie polizeilich vorgeführt werden.

⁵ Bei Erhebungen durch die sachverständige Person können die beschuldigte Person und, im Umfang ihres Verweigerungsrechts, Personen, die zur Aussage- oder Zeugnisverweigerung berechtigt sind, die Mitwirkung oder Aussage verweigern. Die sachverständige Person weist die betroffenen Personen zu Beginn der Erhebungen auf dieses Recht hin.

Eingriff in die Justiz-Grundrechte der Beschuldigten?

- **Waffengleichheit**, Art. 6 EMRK?
 - Möglichkeit der Einwirkung auf Beweisverfahren
 - Zugang zu Daten/ Analyse-Programm erforderlich
 - Zusammenhang zwischen Input (Mimik) und Output (Lüge) nicht nachvollziehbar
 - Repräsentative Datenbasis?
 - «Black-Box»-Problem
 - Einhaltung noch kritisch



Darf ein Gericht einen KI-Beweis berücksichtigen?

- nach dem Stand von Wissenschaft und Erfahrung zur Wahrheitsfindung **geeignetes Beweismittel, Art. 139 StPO?**
 - Zuverlässigkeit von ausschlaggebender Bedeutung
 - (Zuverlässigkeits-)Anforderungen entsprechend zu Glaubhaftigkeitsgutachten:
 - Wissenschaftliche Belegung, d.h. empirisch gestütztes theoretisches Fundament; und
 - Darauf gestützte Urteilsbildung gelingt mit hinreichender Zuverlässigkeit
 - Erhöhter Erkenntnisgewinn: richterliche Aussagewürdigung mit KI müsste aussagekräftiger sein als eine ohne KI
- Wissenschaftliche Bestätigung des Zusammenhangs zwischen Mimik und Lüge fehlt, daher (noch) kein geeignetes Beweismittel

Braucht es eine (formell-)gesetzliche Grundlage?

- Bearbeitung von Personendaten durch Bundesorgane bedarf gesetzlicher Grundlage (Art. 34 Abs. 1 DSG)
- Formelles Gesetz erforderlich (Art. 34 Abs. 2 DSG) bei
 - Bearbeitung besonders schützenswerter Daten (Art. 5 lit. c DSG),
 - Profiling (Art. 5 lit. f DSG), oder
 - «jede Art der **automatisierten** Bearbeitung von Personendaten, die darin besteht, dass diese Daten verwendet werden, **um** bestimmte **persönliche Aspekte**, die sich auf eine natürliche Person beziehen, **zu bewerten**, insbesondere um Aspekte [...] dieser natürlichen Person **zu analysieren** oder vorherzusagen»
- schwerwiegendem Grundrechtseingriff.
- Zumindest wegen Profiling formelles Gesetz notwendig.

«Wenn Sie auch nicht Antworten auf alle Fragen haben, dann befinden Sie sich in bester Gesellschaft! Denn erstens kommt es anders, und zweitens als man denkt.»

Ignazio Cassis, Rede «Blick in die Zukunft» am 4.11.2021 in Luzern



Vielen Dank!

Lena Götzing

Lena Götzing
Rechtsanwältin

Direkt: +41 58 658 56 63
lena.goetzing@walderwyss.com



CV / vCard



Hannes Meyle

Hannes Meyle
Dr. iur., Rechtsanwalt
(Rechtsanwaltskammer München)

Direkt: +41 58 658 55 92
hannes.meyle@walderwyss.com



CV / vCard



