Dr. Stefan Els

Erlangen, November 2021

Stellungnahme

Zum Konsultationsverfahren

des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit

zum Thema:

Einsatz von Künstlicher Intelligenz im Bereich der Strafverfolgung und der Gefahrenabwehr

Vorbemerkungen

Um zu beurteilen, welche Anforderungen an Verarbeitungen mit KI Unterstützung zu stellen sind, muss Klarheit über die Begrifflichkeit herrschen.

Wie unscharf der Begriff ist, zeigt sich schon an den Versuchen in schwache und starke KI zu unterscheiden. Der Begriff mäandert entlang der technischen Entwicklung, er beinhaltet sowohl das was Algorithmen bereits leisten, wie auch die Phantasie, was sie in Zukunft voraussichtlich zu leisten in der Lage sind. Statt von KI spricht man auch oft von maschineller Entscheidung (ADM) oder maschinellem Lernen (ML).

Es handelt sich um eine eminent leistungsstarke Entwicklung, die ihr Potential bereits bei den ersten Schritten autonomen Fahrens, Fliegens, der medizinischen Bildauswertung bis hin zur Annäherung an physikalische Chaostheorien unter Beweis gestellt hat. Zugleich haben die Anwendungen aber auch diverse Schwachstellen zu Tage gefördert, die von der Presse genüsslich aufgegriffen wurden (Z.B. Fehleinschätzung der Bahnauslastung, nicht validen Resultaten bei Assessmentverfahren, fehlerhaften Prognosen bei Strafaussetzung zur Bewährung). AlgorithmWatch durchforstet die Ergebnisse weltweit und berichtet über Auswirkungen und Entgleisungen.

Am Horizont bilden sich bereits Entwicklungen in Richtung Quantentechnik, 6G und holographische Verarbeitungen ab.

Wie jede Technik, kann auch ML zu guten, wie zu bösen Zwecken zum Einsatz bzw. zum Missbrauch gebracht werden. Die Hochschulen werden zunehmend mit Wissenschaftlern besetzt, die den Anschluss der BRD an die globale Entwicklung sichern sollen. So ist nicht verwunderlich, dass sich nicht nur die Datenschutzbehörden, sondern auch die Wissenschaft mit der Frage ethischen Implementierungen bei der Entwicklung befassen, und es in der Folge bereits eine Fülle von Veröffentlichungen zu diesem Thema gibt. Dabei gibt es ausreichend Anlass über ethische Grundsätze nachzudenken. Sollen unsere Gemütszustände anhand von Bildauswertungen ausgeforscht werden dürfen oder ist es legitim, dass Versicherer mittels BigData –Analysen das Solidarprinzip aushebeln, indem sie individuelle Risiken ermitteln?

K. Zweig fasst es populär zusammen unter dem Titel *„Ein Algorithmus hat kein Taktgefühl“* und holt uns so auf den Boden der Tatsachen. KI ist Menschenwerk und wir entscheiden, was erlaubt ist und wo die Grenzen sind.

Bei staatlichen Eingriffen geht es um Grundrechtsschutz. Bei staatlichen Eingriffen im polizeilichen Bereich geht es um besonders hohe Anforderungen, die deshalb einer umfänglichen gerichtlichen Kontrolle unterliegen. Fraglich ist inwieweit dies auch beim Einsatz neuer digitaler Technologien gewährleistet ist, wenn es um die automatisierte Verarbeitung von **Personendaten** geht. Denn hier begeben wir uns auf Bereiche des Datenschutzes, die bislang nur gering erschlossen sind und wenig ausgeleuchtet erscheinen.

Polizeiliches Handeln ist ein Gütesiegel für rechtstaatliches Handeln, Gewaltenteilung und Demokratieverständnis. Ein strafrechtlicher Verdacht, der sich verdichtet, kann schnell existenzielle Folgen auslösen. Falsche Einschätzungen haben dann für die betroffene Person fatale Folgen.

Wie stets, geht es beim Grundrechtsschutz um eine Güterabwägung.

Es könnte unterstellt werden, dass ein umfänglicher Fundus von Daten mit Hilfe von KI / ADM zur effizienten Kriminalitätsbekämpfung beiträgt. KI ist schnell, wertet komplexe Datenberge aus, erkennt Muster und beseitigt damit „blinde Flecke“, durch Kategorien und Score-Werte.

Die Bedrohung des Gemeinwesens ist gewaltig. OK, Cybercrime, Geldwäsche, Steuerflucht bedrohen unsere Grundordnung. KI kann ein geeignetes Mittel sein, um dem etwas entgegen zu setzen.

In welchem dieser Bedrohungsszenarien und mit welchen Mitteln KI im Bereich der Gefahrenabwehr konkreten Mehrwert erbringen kann, ist jedoch bislang nicht belegt und offenbar auch nicht konkret beschrieben.

Die potentiellen Einsatzfelder sind auch im Konsultationsverfahren nur schemenhaft beschrieben. KI ist schnell, ausdauernd, ermüdungsfrei, erweckt den Anschein von Genauigkeit, bietet Vorhersagen, Strukturanalysen und Muster an.

Mit etwas Phantasie führt uns KI in eine paradiesisch anmutende Vorstellung, was im Bereich der Verbrechensbekämpfung möglich sein könnte. Doch die Bewertung welchen Regeln die von Personendaten mittels KI unterliegt, entscheidet sich am konkreten Vorgang. Insoweit gibt die Konsultation Rätsel auf. (Vergl. Anlage 1)

Bereits an dieser Stelle muss deshalb die Frage erlaubt sein, ob gerade der Bereich der Strafverfolgung, der Prävention und der Forensik ein geeignetes Erprobungsfeld für fortgeschrittene KI sein kann und darf. Die bereits beschrittenen Bereiche der Bildauswertung, der Genbankenanalyse und die Durchforstung von Massendaten haben den Wert elektronischer Verarbeitung bereits belegt, KI /ML gehen aber weit darüber hinaus.

ADM/ML können im Vergleich zu den „herkömmlichen“ geschlossenen Verfahren beachtliche, anders geartete Schwachpunkte haben. Sie lernen nur aus dem, was man dem System bereit stellt. Unausgewogenes Material für die Lernphase hat dann auch zu verwerflichen bis lächerlichen Ergebnissen geführt. KI benötigt klare Vorgaben, Grenzen und Kontrollen. Dazu müsste man aber die Bedrohungen eindeutig identifizieren? Wird ein Risiko durch ethische Erwägungen erschlossen wird die Diskussion allerdings schnell wachsweich.

Denn die Befürchtungen sind diffus und bislang auch nicht ausgeräumt. KI könne sich mittels neuronalem Lernen in unerkannte Bereiche entwickeln (entgleisen), unausgewogene Lerndaten führen zu unzulässigen Ergebnissen, der Begriff der Diskriminierung geistert, einem Popanz gleich, umher. Datenschützer können das Risikopotential kaum vorhersagen, ob die Entwickler oder die Ethiker oder die Soziologen das können, bleibt unbeantwortet.

Dennoch scheint es bei der Konsultation um die Frage zugehen, ob der Startschuss für den Einsatz von KI nun durch gesetzliche Grundlagen unmittelbar bevorsteht.

Lernende Algorithmen machen es nicht leicht, sie in ein verfassungsgemäßes Korsett zu bringen, welches zudem und in allererster Linie die Rechte der Betroffenen sichert. Sie fluktuieren und beglücken uns nur vermeintlich mit dem Anschein von Sicherheit und Objektivität.

Eine fortwährend wiederkehrende Abwägung staatlichen Tuns erfordert deshalb hohes Problembewusstsein bei **allen** Protagonisten, taugliche Werkzeuge zur Vorbeugung, Begleitung und Kontrolle, letztlich auch griffige gesetzliche Vorgaben (vergleiche These 8).

1. These, gesellschaftspolitische, ethische Saldierung

Das Datenschutzrecht hat einen schweren Stand. Die Ursachen darin liegen zum einen in seiner Komplexität und seiner schweren Verständlichkeit, zum anderen in einer Vielzahl ungenauer, auslegungsbedürftiger Begriffe und schließlich an dem Umstand, dass es in einem Abwägungsprozess mit anderen Gütern des Gemeinwohls oft den Kürzeren zieht. Das BDSG befasst sich zudem in weiten Bereichen mit der Begrenzung des Datenschutzes. Die Sicherung datenschutzrechtlichen Terrains gelingt meist nur mit Hilfe der Aufsicht oder mit gerichtlicher Unterstützung (vergl. BfDI Positionspapier vom 06.04.21). Die Entscheidungen des Bundesverfassungsgerichts zur Bemessung des Schadenersatzes und zur hypothetischen Datenneuerhebung haben das belegt.

KI eröffnet eine völlig neue Dimension der Datenverarbeitung. Die Entwicklung der Möglichkeiten von KI ist nicht absehbar. Demnach lassen sich derzeit keine exakten Vorhersagen aus der Glaskugel ablesen, mit welchen Mitteln KI im Zaum gehalten werden muss. Erkennbar ist aber, dass die Verarbeitung von Personendaten im Bereich Kriminalitätsbekämpfung geeignet ist, um gravierende Eingriffe in Persönlichkeitsrechte zu bewirken.

KI in der Verwaltung steht am Anfang. KI in der Verwaltung braucht auch ein Experimentierfeld. Dieses Experimentierfeld gerade im Bereich der Gefahrenabwehr zu suchen, ist der am wenigsten geeignete Ort. Dort wo die Gefahren lauern, baut man kein Labor!

Geeignete Rechtsgrundlagen, Achtsamkeit, Akzeptanz der Regularien und die Werkzeuge zur Kontrolle müssen erst noch entwickelt werden.

Dabei ist es auch eine Illusion zu glauben, dass es eine exakte Abwägung zwischen den Interessen des Datenschutzes und der informationellen Selbstbestimmung einzelner Betroffener in der einen Waagschale und den Interessen zum Schutz der Allgemeinheit in der anderen Schale geben wird. Entscheiden wird eine summarische Prüfung und der politische Zeitgeist.

2. These, Rechtsgrundlage

Bei KI in der Verwaltung ist in Bezug auf die Rechtsgrundlage zunächst zu unterscheiden in das Gesetzgebungsverfahren und in die Rechtsgrundlage selbst.

Bei KI geht es darum unterschiedliche Datenbestände unabhängig von ihrem Erhebungsgrund und ihrem Verarbeitungszweck zusammenzuführen um hieraus Erkenntnisse zu Begehungsweisen, und Vorhersagen zu künftigen Entwicklungen oder Verhaltensweisen zu generieren.

Wenn es dabei um die Verarbeitung personenbezogener Daten geht, kommen Art. 22DSGVO und Art. 11 Justizrichtlinie zu den gleichen Ergebnissen: Vom Grundsatz her verboten, es sei denn eine gesetzliche Grundlage und geeignete Garantien gestatten die Verarbeitung.

Die DSGVO und auch die Justizrichtlinie sagen nichts zu BIG Data Auswertungen. Unverkennbar stehen aber die Grundsätze des Datenschutzes KI zumindest im Wege.

Die Datenminimierung kann nicht oder nur eingeschränkt gewährleistet werden und gerade im Bereich der Gefahrenabwehr kann Transparenz nur unzureichend geboten sein. Das Bedürfnis nach großen Datenmengen und Datenverknüpfungen, Schnittstellen und Zugriffsrechten auf entferntere Datensätze begründet sich aus der neuronalen Idee. Was nicht vorhanden ist kann nicht verknüpft werden.
Die klassischen Bereiche des Datenschutzes werden verlassen. Lösungsansätze über HYDANE oder die Interpretation polizeilicher Daten als **einen** Datensatz oder der Umweg über §§ 49,45 BDSG erscheinen gekünstelt und verfassungsrechtlich zu ungenau *(„erforderlich und verhältnismäßig“).* Jedenfalls wäre § 12 BKAG aus dieser Sicht nicht KI-kompatibel.

Die Diskriminierungen geschehen im Verborgenen, sie treten nicht offensiv zu Tage, was die Rechte der Betroffenen zusätzlich gefährdet.

Man kann also feststellen: KI gewährleistet im Verhältnis zu herkömmlichen geschlossenen Verfahren die Rechte der Betroffenen nur eingeschränkt. Deshalb ist KI in der Verwaltung und im Bereich der Strafverfolgung subsidiär.

Damit ergeben sich für das Gesetzgebungsverfahren folgende Anforderungen:

- Beleg der Subsidiarität (Nachweis, dass KI /ML zu besseren Ergebnissen führt,
- Gesetzesfolgenabschätzung mit vertiefter Betrachtung auf mögliche Diskriminierungen (eine DSFA käme viel zu spät)
- Begleitung mit einem Gutachten der DEK

Für die Rechtsgrundlage selbst ergeben sich folgende Anforderungen:

- Klare Vorgaben zur Lernphase, d.h.: Prüfung der Orientierung an der Zweckbindung
- Echtdatenverwendung zulassen
- Anonymisierte Daten mit Transparenz-Anforderungen
- hinreichende Prüfung der Zwischenergebnisse
- Bezeichnung der eingespielten/verknüpften Daten
- **Klärung, inwieweit es möglich ist nur „Kontextdaten" (ohne Personenbezug) zu verwenden**

Die Rechtsgrundlage muss auch die Überwachung des Echtbetriebs abdecken:

- Genaue Vorgaben, welche Daten in die Auswertung einbezogen werden sollen
- Anforderung einer Zertifizierung vor Inbetriebnahme werden erstellt (und zwar eigenständig national, ohne endloses Zuwarten auf Entscheidungen der Kommission)
- DSFA vor Inbetriebnahme (Art der DSFA vergl. unten These 7)
- Regelung der Aufsicht mit Einbeziehung einer Fachexpertise
- Festlegung der Mindestanforderungen an die Aufsicht
- Verlaufskontrolle / Monitoring
- **Verordnungsermächtigung** zur Festlegung und einfacheren Anpassung der
    - Errichtungsanordnung
    - der TOM
    - der Anweisung an den Entwickler

Bei Betrachtung solch umfangreicher Anforderungen stellt sich die Frage, ob der Aufwand lohnt und ob insbesondere im Bereich der Forensik auch KI Anwendungen denkbar sind, die ohne personenbezogene Daten auskommen.
Die Anknüpfung an Begehungsformen, die Auswertung der Modi Operandi, Sprach- und Genanalysen zur Eingrenzung von Suchmerkmalen könnte als sog. „Kontextanalyse“ auch ohne Personenbezug mittels KI wertvolle Hinweise bei der Aufklärung von Straftaten geben. (Vergl. Anlg.1)

3. These Datenschutzgrundsätze und Rechte von Betroffenen

Die Bewahrung der Betroffenenrechte steht im Zentrum der Nagelprobe. Die Transparenz stößt bei polizeilichen Ermittlungsmethoden nachvollziehbar schnell an Grenzen. Im Gegenzug dürfen Fehlentwicklungen, Diskriminierungen und auch die sog. Kinderkrankheiten nicht verschwiegen werden. Proaktiv die Betroffenenrechte zu wahren, hieße auf die Aufsichtsbehörden und soweit möglich auf die Betroffenen zugehen. Erwägungsgründe 38,39 zur Justizrichtlinie weisen die Richtung.

Anforderungen lassen sich leicht benennen:

- Überarbeitung der Löschroutinen
- Regelmäßige Ergebniskontrolle mit nachvollziehbarer Einbeziehung einer menschlichen Entscheidung
- Einbindung der Vorgesetzten beim Einsatz von KI Verarbeitung
- Unabhängige Überprüfung der Ergebnisse, insb. bei Berührung der grundrechtlichen Kernbereiche
- Auswertbare Protokollierung
- Nachvollziehbare Zugriffsrechte mit regelmäßiger Überwachung!
- Entschlackung der von der DSK vorgeschlagenen TOM auf ein umsetzbares Maß
- Schulung der Mitarbeiter insbesondere zu der Frage, wie und an welcher Stelle eines Entscheidungsprozesses die Ergebnisse der KI eingehen (Stichwort: gesunde Skepsis)
- Benachrichtigung betroffener Personen im Schadensfall (Diskriminierung inbegriffen) Überarbeitung von § 67 BDSG.

- Transparente Einbeziehung der KI Resultate in den Entscheidungsprozess
- Transparenz soweit wie möglich umsetzen (Logik erklären, Gutachten der DEK veröffentlichen)
- Transparenz in Bezug auf Anonymisierung auch in Bezug auf die weitere Verwendung
- Transparenz-Portal mit abstrakter Darstellung der Schadensfälle
- Proaktiver Schadensausgleich mit Gefährdungshaftungstatbestand
- Ombudsstelle zur Vermittlung des Schadensausgleichs

4. These Datenqualität

Die Verlässlichkeit der eingesetzten Daten, ihre Qualität und ihre Interpretation sind seit jeher ein wesentliches Qualitätsmerkmal. „Unsaubere“, überholte Daten können bei ML/ADM aber zu besonders fatalen Folgen führen. Nachhaltigkeit ist in aller Munde, weshalb nicht auch bei polizeilicher Datenverarbeitung?

- Eingehende Prüfung der Qualität der Daten für die Lernphase
- Klärung, inwieweit Daten nach §§ 72,73 BDSG (vergl. Art. 7 Justizrichtlinie) überhaupt als Lerndaten geeignet sind
- Erforschung der Tauglichkeit von „Kontextdaten“
- Eingehende Prüfung Qualität der Daten die für die Auswertung herangezogen werden

5. These Kernbereiche

Der Kernbereich privater Lebensgestaltung und Menschenwürde dürfen beim Einsatz von KI nicht tangiert werden.

Was für eine Aussage?

Eine Pflichtübung oder ein Hinweis darauf, dass selbst diese Bereiche besonders gefährdet sind. Allein die Aussage provoziert, als ob diese Kernbereiche zur Disposition stünden.

Die Frage sollte eher lauten, wo der Kernbereich beginnt? Was ist schlicht unantastbar, was dagegen kann Gegenstand einer Abwägung sein. Im Bereich der Datenverarbeitung scheint dies eine ungeklärte Frage zu sein, sonst müsste man nicht ständig nach der Ethik fragen.

Die Definition der Kernbereiche der Verfassungsgerichtsbarkeit zu überlassen und die Veröffentlichung von fragwürdigen Ergebnissen der NGO AlgorithmWatch, sind nur zweitbeste Wege.

- Zu den Kernbereichen gehören natürlich das Leben und die Ausformungen etablierter Privatheit, also die Wohnung, der Postverkehr und die Telekommunikation. Aber gehören dazu auch noch die gesetzlich benannten Kategorien sensibler Daten (Art. 9 DSGVO / Art. 10 Richtlinie)? Die Richtlinie gibt in Art. 11 Abs.2 die Antwort: Ja, aber nur bei geeigneten Schutzmaßnahmen. Das hilft für KI nicht weiter, weil diese Maßnahmen erst noch erkundet und errichtet werden müssen. An dieser Stelle wird das Erfordernis der Nacharbeit unübersehbar. Es ist Aufgabe der Bundesdatenschutzbehörde diesen Anpassungsdruck in die Gremien zu tragen. Bislang wurde aber kein Nachbesserungsbedarf erkennbar gemacht.
- Verarbeitung im Kernbereich führt auch zu der Frage, wie man sich den Merkmalen höchstpersönlichen Privatheit nähert. Ergeben sich aus den Kernbereichen auch **Grenzen für die Methoden und Fragestellungen der Auswertung**? Nach derzeitigem Diskussionsstand gehören hierzu die biometrische Auswertung, Bewegungsprofile, Persönlichkeitsprofile, Phrenologie und die Auswertung und Recherche in Big Data. Ernüchterung stellt sich ein, weil gerade in den genannten Bereichen ständig geforscht wird.
- KI liefert Werte. Ihre Interpretation bleibt Sache der Sachbearbeitung. Und wieder steht der Prozess der Verarbeitung, und dem was sich daran anschließt, im Mittelpunkt der Erörterung. Was helfen könnte, ist eine besonders enge Definition des Kernbereichs, damit die Welt wieder in Ordnung scheint. Dabei würden Teile unserer Privatheit und das Gefühl, noch die Herrschaft über unsere Daten zu haben, auf der Strecke bleiben. Die Frage nach der Nutzung aller im Netz und in den Behörden verfügbaren personenbezogenen Daten, und die **Möglichkeit zu deren Verarbeitung in kaum mehr durchschaubarer Weise,** deuten darauf hin, dass sich die Kernbereiche in erheblicher Gefahr befinden. Es scheint nur noch um die Frage des „wie“ nicht mehr um das „ob“ zu gehen.
- Ob die Einschränkungen mit unbeugsamer Absolutheit zu begreifen sind, muss sich noch zeigen. Werden Bereiche zum Kernbereich berührt, muss eine nachvollziehbare Güterabwägung vorangestellt werden, die einen Eingriff in den Kernbereich zu rechtfertigen in der Lage ist.
  In Extremsituationen sind Berührungen von Kernbereichen nicht auszuschließen. Wenn Datenschutz sich der Vernunft entgegenstellt (Verbot der Mautdatenauswertung bei Autobahnmord) geht die Akzeptanz genauso schnell verloren, wie wenn die Schutzmechanismen versagen. Die exakte Vorgabe (Regelung) und die Kontrolle scheinen demnach der Schlüssel zum Erfolg (vergl. Anlage 2). Damit wird es erlaubte und verbotene Verarbeitungsergebnisse geben**. Dies führt im Bereich der Strafverfolgung direkt zur Frage des Verwertungsverbots**.

  Besonders das diffuse Unsicherheitsgefühl bei KI Verarbeitungen führt zu einer erheblichen subjektiv empfundenen Abneigung. Ein weiteres Vordringen in die Kernbereiche der Privatheit stellt eine besondere Gefahr für das Vertrauen in die Verlässlichkeit staatlichen Handelns dar. Spielt sich der Prozess zudem im Bereich der Gefahrenabwehr ab, kann das Ziel, ein Sicherheitsgefühl aufzubauen, auch in das Gegenteil umschlagen.

  Zurückhaltung ist angebracht! Nicht alles was möglich ist, sollte auch erkundet werden und nicht alles was möglich ist, sollte auch unter dem Aspekt der Abwägung zulässig sein.

6. These Aufsicht

Aufsicht über den Datenschutz ist gegeben. Aufsicht über die polizeilichen Daten ist zudem ganz „oben bei der Aufsicht“ angesiedelt (vergl. Art. 46 Richtlinie) Eine weitere Aufgliederung zur Aufsicht über KI-Anwendungen würde nur zu Kompetenzkollisionen führen und den Verwaltungsapparat ungebührlich aufblähen.
Neue Technik erfordert auch neue Formen der Aufsicht. Dieser Herausforderung muss sich auch der BfDI stellen.
Nichts spricht gegen eine Nachschärfung der Richtlinie in Bezug auf Aufsicht über KI/ML/ADM.
Naheliegend wäre auch eine Spezialisierung unter den bestehenden Aufsichtsbehörden. Entwickler und Fachexpertise gehören aber bei der Aufsicht mit an den Tisch. KI führt uns zwingend in das interdisziplinäre Team.
Die Datenschutzbeauftragten der Behörden müssen für die neue Aufgabe ertüchtigt, ermutigt und unterstützt werden! Bundes-und Landesaufsichtsstellen müssen sich mit den behördlichen Beauftragten besser vernetzen. Ohne spezifische Kontrollwerkzeuge wird es keine wirksame Aufsicht geben. Eine Anpassung von Art. 10 DSGVO unter Bezug zu KI ist wünschenswert.

Folgerungen:

- Die Aufsicht wird von den Landesbehörden und der Bundesbehörde (BfDI/LfDI) geleitet und Koordiniert. Die Errichtung einer Sonderbehörde für KI erscheint allein schon wegen Kompetenzüberlagerungen als ungeeignet.
- Die behördlichen Datenschutzbeauftragten werden einbezogen. Sie sind am nächsten am Geschehen. Es erscheint sinnvoll Kompetenzen zu bündeln.
- Das Selbstverständnis des BfDI in Bezug auf die Zusammenarbeit mit den örtlichen Beauftragten muss ausgebaut werden.
- Für akute Fragen muss eine Hotline (Single Point) eingerichtet werden.
- Geeignete Prüfinstrumente für die Aufsicht werden bereits bei der Programmierung berücksichtigt.
- Regelmäßige Prüfprotokolle belegen die Begleitung der Entwicklung besonders nach dem Start in die Praxisphase.
- Die Aufsicht beginnt bereits bei der Begleitung in der Lernphase der Anwendung.
- Die Fluktuation von Mitarbeitern erweist sich als besonders kontraproduktiv. Deshalb sollte eine ausreichende Stellenausstattung (Bewertung) gewährleistet sein.
- Aufsicht ist bezogen auf KI interdisziplinäres Teamwork.

7.These DSFA

Die DSFA in der derzeitigen Fassung ist ungeeignet. KI und ML erfordern eine fortlaufende Begleitung. Schwellwertanalyse und einmalige DSFA werden KI im Bereich der Gefahrenabwehr nicht gerecht.

- Die Bestimmungen zur DSFA werden Diskriminierungen nicht gerecht, weil schwer vorhersagbar ist, welche Umstände Diskriminierungen herbeiführen und welche Auswirkungen Diskriminierungen anrichten.
- Bei einer ML- bezogenen DSFA müssten bereits die Ausgewogenheit und Verlässlichkeit der „Lerndaten“ einbezogen werden. Sodann müssten die Ergebnisse der Erprobungsphase betrachtet werden, mithin ein anhaltender Prüfungs-und Begleitungsprozess.
- Ohne eine Anpassung der gesetzlichen Vorgaben sollte KI / ML im Bereich der Gefahrenabwehr nicht zum Einsatz gelangen

Anlage 1

Anwendungsbeispiele

zur Verarbeitung personenbezogener Daten mittels Techniken künstlicher Intelligenz

(Versuch einer Annäherung)

Zweck	Lernziel	Verarbeitung	Ergebnisse	Bewertung
Suche nach einer Person oder Gruppen	Erkennen von Ähnlichkeiten anhand bekannter Eigenschaften	Einbeziehung aller in Betracht kommenden Dateien/ Aufzeichnungen/ Bilder/ etc.	Bezüge zu Orten Personen Bewegungsmustern	Nur auf der Grundlage einer Rechtsgrundlage und einer besonderen Bedrohungslage. Mit richterlicher Anordnung
Erkennen von Begehungsmustern	Auswertung von Begehungsmustern, Tatwerkzeugen, Finanzwerkzeugen	Begehungsdaten werden von den Personen getrennt verarbeite. Nur der Anonymisierungsprozess unterliegt dem Datenschutz	Muster als Grundlage für weitere Verifizierung	Kritische Betrachtung von Vermutungsansätzen. Absicherung die eine Rückverfolgung ausschließt. Dürfte ohne gesonderte Rechtsgrundlage möglich sein.
Erkennen und Vorhersage von Orten, Regionen mit	Auswertung von Begehungsmustern,	Nur relevante Daten werden aus allen verfügbaren	Regionen, Örtlichkeiten denen Attraktivität für	Herkunft der Daten ist zu regeln.

evidenter Kriminalitätsbelastung	Tatwerkzeugen, Finanzwerkzeugen Herkunft der Daten ist zu regeln.	Dateien einbezogen, dabei wird der Personenbezug gesichert vermieden	künftige Kriminalitätsbelastung anhaftet	Kritische Betrachtung von Vermutungsansätzen. Absicherung die eine Rückverfolgung ausschließt. Dürfte ohne gesonderte Rechtsgrundlage möglich sein.
Sprachanalyse zur Ermittlung einer regionalen / ethnischen Zugehörigkeit	Sprachen, Dialekte, Sprachmelodie, Wortwahl wird anhand von Beispielen einer Region oder der Zugehörigkeit einer Gruppe zugeordnet einer Herkunft etc. zugeordnet. Viele Daten versprechen hohe Validität	Hohes KI Potential, weil es sich um sehr mächtige Datenmengen handelt	Zuordnung zu einer Gruppe ermöglicht eine Eingrenzung der Suche nach Tätergruppen	Rechtsgrundlage für die Entwicklung entbehrlich. Notwendigkeit einer Rechtsgrundlage für die Zuordnung auf eine Person müsste geprüft werden. Hohe Diskriminierungsgefahr kann nur durch kritisches Hinterfragen des Ergebnisses erfolgen! Die Lernphase kann auf der Grundlage der Mitwirkung Freiwilliger erfolgen.
Sprachanalyse zur Rekonstruktion des Aussehens (Gesicht/ Geschlecht/Alter)	Neue Entwicklungen forschen zu diesem Anwendungsbereich	Aus Sprache wird ein Gesicht, aus einem Gesicht wird Sprachliche Zuordnung	Gesichtsprofil ermöglicht z.B. die Suche in Täterdateien	Sehr hohes Irrtumspotential Derzeit nur kritisch zu begleiten
Erstellen eines Täterprofils einschließlich Phantomisierung	Erfassung von allen einer Tat anhaftenden Details zur Erstellung eines eingrenzenden Profils, einschl. Erstellen von Phantombildern. Ergebnisse erfordern extrem hohen Aufwand bei der	Verarbeitung zur Erstellung eines eingrenzenden Profils, einschl. Erstellen von Phantombildern. Verknüpfung zu anderen Tätern /Gruppen	Hohes Entwicklungspotential	Hohes Diskrimoinierungspotential. Gemütsverfassungsanalyse sehr kritisch Nur bei Katalogtaten auf Rechtgrundlage zulässig

	Bereitstellung von Lerndaten. Falsche Gewichtung birgt hohes „ Unfugpotential“!			

Anlage 2 (These 8)

Thesen verleiten dazu, Themen zu begrenzen, vielleicht sogar den Blick zu verstellen.

Die 8. These steht daher für eine offene Skala weiterer Anliegen.

- KI mit Personenbezug wird in einer Anfangsphase, gesetzlich vorgeschrieben, nur mit **richterlicher Anordnung** zum Einsatz gebracht. Die Auswertung der Ergebnisse erfolgt unter Einbeziehung der Aufsichtsstelle. Der unzulässige Einsatz von KI führt zur Frage des Verwertungsverbots.
- Die **Zertifizierung** ist ein wesentlicher Schritt in Richtung Verarbeitungssicherheit
- Die Justizrichtlinie und das BDSG müssen auf die neuen Anforderungen angepasst werden.
- **Interdisziplinäre Teamarbeit** aller Protagonisten ist eine Pflichtaufgabe
- Die **Schulung** der Mitarbeiter und der Prüforgane in Bezug auf die Spezifika automatischer Entscheidungen ist unabdingbar und hat Priorität
- Ausgewählte Einsatzfelder sind zu ermitteln, zu erläutern und unter **Laborbedingungen** zu erproben (insb. Erprobung von Kontextdaten)
- Der **Zugriff** auf eingespielte „Lern“-Daten, ohne Berücksichtigung des ursprünglichen Erhebungszwecks muss verhindert werden
- Zum Auffinden möglicher Einsatzbereiche von KI im Bereich der Gefahrenabwehr ist es Aufgabe forensischer Forschung die Tauglichkeit von **„Kontext-Daten“ ohne Personenbezug** zu ergründen.

Stand 16.11. 2021

Literatur:

Zweig Katharina, Ein Algorithmus hat kein Taktgefühl

Misselhorn Catrin, Grundfragen der Maschinenethik

NEGZ Bericht Nr. 16, Potentiale und Herausforderungen einer neuen Datenorientierung im Kontext öffentlicher Aufgabenwahrnehmung

NEGZ Bericht Nr.22 Weniger ist manchmal mehr: Dienstleistungen und Anforderungen für einen No-Stop-Shop (09/2021)

NEGZ Bericht Nr.3 Künstliche Intelligenz in der öffentlichen Verwaltung

Wedde Peter, Automatisierung im Personalmanagement (Abruf über AlgorithmWatch)

Kucklik Christoph, Algorithmische Diskriminierung in Macht im Netz, Vom Cybermobbing bis zum Überwachungsstaat, Reclam 2019

Ballestrem et al., Künstliche Intelligenz- Rechtsfragen und Strategien in der Praxis

Grimm / Keber / Zöllner Digithale Ethik, untertitel: Leben in vernetzten Welten

Wampfler Philippe (Hrsg.) Macht im Netz vom Cybermobbing zum Überwachungsstaat

Nemitz / Pfeffer Prinzip Mensch 1. Aufl. 2020

Von Schirach Ferdinand, Jeder Mensch

Hornung, Schindler, Datenschutz bei der biometrischen Gesichtserkennung
Künstliche Intelligenz und Mustererkennung als
Herausforderung für das Recht, DuD 8/21, S. 515f

Löber, Lange, Roßnagel, Datenschutzfreundliche Algorithmen, DUD 9/21, S. 622f

Schwartmann /Pieper/Mühlenbeck Kommt. zur DSGVO/BDSG, 2.Auflg., Art.6 Rz 281-291

Buijsman Stefan, ADA und die Algorithmen -- Wahre Geschichten aus der Welt der künstlichen Intelligenz