Teil I. Technischer Hintergrund und Anwendungsfälle von KI

Lukas Lehner

1. Einleitung

„Was ist KI eigentlich?" – Angesichts der Prävalenz des Begriffs in Alltag und Beruf und der stetig zu steigen scheinenden Relevanz der dahintersteckenden Technologie für ebenjenen Alltag und unser Berufsleben könnte man meinen, jedes Kind müsste mittlerweile eine Antwort auf diese Frage aus dem Ärmel schütteln können. Aber im Gegenteil: Es scheint, als ob sich nicht einmal die Experten dieses Gebiets auf eine griffige Antwort einigen können[1] und sich auch Antworten wie „Ist nur ein Marketing-Begriff"[2] finden lassen, was den Nutzen des Begriffs infrage stellt. Unter anderem deshalb wird im folgenden Kapitel versucht, stattdessen die Frage „Ist das schon KI?" – angewandt auf verschiedenste Beispiele – zu beantworten.

Dem Leser werden diese Beispiele vor allem aus technischer Sicht vorgestellt. Dabei wird versucht – ganz im Sinne von „iudex non calculat" – die Technik unter Verwendung geringstmöglicher Mathematik zu erklären. Weiters sei Folgendes angemerkt: Da hier aus technischer Sicht beleuchtet wird, was KI ist und was nicht, ist der Leser angehalten, eventuelle technische Definitionen nicht mit rechtlichen Definitionen zu vermischen oder sie als solche aufzufassen.

2. Klassische Anfänge

Zunächst werden grundlegende Begriffe wie *KI-Methode, Algorithmus, KI-Modell, KI-System, Entscheidung, Datenset* sowie *Input* und *Output* anhand eines einfachen Beispiels erklärt – und zwar mittels eines alten Bekannten: des arithmetischen Mittels.

2.1. Das Arithmetische Mittel – Don't Be Mean

Sollten Sie sich fragen, was dieser umgangssprachlich genannte Durchschnitt mit KI zu tun hat, hier gleich die Antwort: direkt nicht viel, aber als Platzhalter eignet er sich hervorragend. Beginnen wir damit, den Durchschnitt von etwas zu berechnen. Als Beispiel für so ein *etwas* nehmen wir hier die Länge einer Kaffee-

1 *Russell/Norvig*, Artificial intelligence: a modern approach (4th Global Edition) (2022) 19.

2 *Belsky*, Is It Time We Stop Saying AI? 23.8.2023, https://www.forbes.com/councils/forbestechcouncil/2023/08/23/is-it-time-we-stop-saying-ai/ (20.12.2024).

2.1. Rechtsvorschriften

Die zentrale Rechtsvorschrift zum Datenschutz in der EU ist die VO (EU) 2016/679 (**Datenschutzgrundverordnung – DSGVO**).[4] Sie gilt seit 25.5.2018 und ist in allen EU-Mitgliedstaaten unmittelbar anwendbar. Die DSGVO lässt den EU-Mitgliedstaaten allerdings die Möglichkeit, einzelne Bereiche der DSGVO noch genauer zu regeln, und enthält sog Öffnungsklauseln. Österreich hat davon teilweise Gebrauch gemacht und dazu das **Datenschutzgesetz (DSG)** erlassen,[5] das gemeinsam mit der DSGVO anzuwenden ist. Es gibt aber auch in **weiteren Gesetzen**, zB im Forschungsorganisationsgesetz (FOG),[6] datenschutzrechtliche Vorschriften, die auf Öffnungsklauseln oder Bereichsausnahmen in der DSGVO zurückgehen.[7]

Grundsätzlich sind alle von der DSGVO erfassten Datenverarbeitungen verboten, solange sie nicht unter einen Erlaubnistatbestand fallen. Für besondere Kategorien personenbezogener Daten (zB Gesundheitsdaten, Daten über politische oder religiöse Zugehörigkeit) sind diese Erlaubnistatbestände strenger ausgestaltet als für „normale" personenbezogene Daten.

2.2. Herausforderung Datenschutz und KI

Beim maschinellen Lernen und Trainieren von KI-Algorithmen werden große Datenmengen analysiert, die auch personenbezogene Daten enthalten. Damit ist der Anwendungsbereich der DSGVO grundsätzlich eröffnet. Die Verwendung von KI, insb auch von General-Purpose-AI (GPAI), das sind KI-Systeme, die für ganz verschiedene Zwecke eingesetzt werden können (zB ChatGPT von OpenAI), birgt massive datenschutzrechtliche Herausforderungen. Bereits das **Konzept, unzählige Daten aus unterschiedlichen Quellen** zu sammeln, die zu welchen Zwecken auch immer erhoben wurden, widerspricht von Grund auf der DSGVO. Nach deren Regelungsziel soll die Verarbeitung personenbezogener Daten ja eher die Ausnahme als die Regel sein.

Beispiel

Dies zeigte sich zuletzt auch in der Entscheidung der italienischen Datenschutzbehörde, die es *OpenAI* vorübergehend untersagte, ihr KI-System ChatGPT in Italien anzubieten. Gründe dafür waren unter anderem (1) die fehlende Zurverfügungstellung von Information an die Nutzer, deren personenbezogene Daten durch OpenAI verarbeitet werden, (2) dass OpenAI keine legitime Rechtsgrundlage für die massenhafte Verarbeitung

4 VO (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27.4.2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung – DSGVO), ABl L 2016/119, 1.
5 Datenschutzgesetz (DSG) BGBl I 1999/165 idF BGBl I 2024/70.
6 Forschungsorganisationsgesetz (FOG) BGBl 1981/341 idF BGBl I 2023/52.
7 *Haimberger*, Datenschutz in der medizinischen und pharmazeutischen Forschung (2021) 18 ff.

4. KI im Kontext der Erfüllung der Betroffenenrechte

4.1. Einleitendes zum Thema

Beim Einsatz von Anwendungen, die auf Grundlage oder bloß teilweise mit einer künstlichen Intelligenz funktionieren, wird der Anwender wegen der Einhaltung des geltenden Datenschutzrechts unter Umständen vor erhebliche Herausforderungen gestellt. Insbesondere die effektive Wahrung der Betroffenenrechte nach dem 3. Kapitel der DSGVO führt durch die zunehmend komplexen und undurchsichtigen Entscheidungsprozesse von KI-Systemen für Betreiber und Verantwortliche zu besonderen Herausforderungen. Die Rechte auf Auskunft, Berichtigung, Löschung, Datenübertragbarkeit und Einschränkung der Verarbeitung sowie das Widerspruchsrecht stehen zudem in direktem Zusammenhang mit den datenschutzrechtlichen Grundsätzen nach Art 5 DSGVO.[95]

Doch gerade die Ermöglichung der Ausübung dieser Rechte wird durch die Black-Box-Natur vieler KI-Anwendungen für Verwender der Systeme – und somit die Verantwortlichen der Datenverarbeitung – erschwert. KI-Modelle, die auf großen Datenmengen basieren und durch maschinelles Lernen autonome Entscheidungen treffen, werfen Fragen auf, wie die Anforderungen der DSGVO in der Praxis effektiv umgesetzt werden können.

Das Kapitel ist wie folgt aufgebaut: Zuerst werden die datenschutzrechtlichen Rahmenbedingungen dargelegt, und es wird darauf eingegangen, welche Rechte die betroffene Person nach der DSGVO besitzt; danach werden die einzelnen Betroffenenrechte detailliert dargestellt, und die Frage nach der Umsetzung für den Verantwortlichen wird untersucht. Zudem werden Lösungsansätze diskutiert, um die Umsetzbarkeit der Betroffenenrechte für den Verantwortlichen trotz der Komplexität der verwendeten KI-Systeme bestmöglich zu gewährleisten.

4.2. Datenschutzrechtlicher Rahmen

Für die Umsetzung der Betroffenenrechte ist – wie bereits eingangs erwähnt – die DSGVO die zentrale Gesetzesbestimmung für Nutzer von datenverarbeitenden KI-Systemen, die sich im Regelfall in der Rolle des Verantwortlichen iSd Art 4 Z 7 DSGVO befinden.[96] Denn wenn sie alleine oder auch gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheiden, nehmen sie die Rolle des Verantwortlichen iSd DSGVO ein[97] und treffen

95 Bei den in Art 5 DSGVO aufgezählten Grundsätzen handelt es sich um den der Rechtmäßigkeit, der Verarbeitung nach Treu und Glauben, der Transparenz, der Zweckbindung, der Datenminimierung, der Richtigkeit, der Speicherbegrenzung, der Integrität und Vertraulichkeit sowie um den Grundsatz der Rechenschaftspflicht des Verantwortlichen.

96 *Ernst* in *Paal/Pauly*, DS-GVO BDSG[3] (2021) Art 4 Rz 55.

97 *Hödl* in *Knyrim*, DatKomm Art 4 DSGVO Rz 77 (Stand 1.12.2018, rdb.at).

4.3.7.4. Praktische Umsetzung und Herausforderungen

Bei der Verwendung von KI-Anwendungen bedeutet das, dass betroffene Personen das Recht haben, nicht einer solchen automatisierten Entscheidung unterworfen zu werden, es sei denn, diese Entscheidung ist für die Erfüllung eines Vertrags erforderlich, gesetzlich zulässig oder erfolgt mit ausdrücklicher Einwilligung der betroffenen Person. Der Verantwortliche muss (auch technisch) sicherstellen, dass in solchen Fällen angemessene Maßnahmen getroffen werden, um die Rechte und Freiheiten sowie berechtigten Interessen der betroffenen Personen zu schützen. Dies umfasst insbesondere das Recht, menschliches Eingreifen zu verlangen, die eigene Sichtweise darzulegen und die Entscheidung nochmalig unter Berücksichtigung dieser zu treffen.

Praxisbeispiele zu Art 22 DSGVO

Gerade Art 22 DSGVO ist für KI-Anwendungen besonders praxisrelevant, da viele KIs auch dafür eingesetzt werden, vollautomatisierte Entscheidungen für den Verwender zu treffen, um Prozesse zu vereinfachen und zu beschleunigen. Um die Relevanz dieser datenschutzrechtlichen Bestimmung im Kontext von KI-Anwendungen zu veranschaulichen, werden nachfolgend einige fiktive Beispiele angeführt:[173]

- **Automatisierte Kreditvergabe:** Eine Bank verwendet eine KI-Anwendung, um die Kreditwürdigkeit von Antragstellern zu bewerten. Basierend auf den eingegebenen Daten wie Einkommen, Schulden und bisherigem Zahlungsverhalten, trifft die KI automatisch und ohne Eingreifen einer natürlichen Person die Entscheidung, ob ein Kredit gewährt wird oder nicht, was erhebliche rechtliche Auswirkungen auf die betroffene Person haben kann.
- **Bewerbungsverfahren:** Ein Unternehmen setzt eine KI-basierte Software zur automatisierten Vorauswahl von Bewerbungen ein. Die KI analysiert die Lebensläufe und Anschreiben der Bewerber und trifft auf dieser Basis eine Entscheidung darüber, welche Bewerber zu einem Vorstellungsgespräch eingeladen und welche abgelehnt werden. Auch hier handelt es sich um eine automatisierte Entscheidung mit potenziell erheblichen Auswirkungen auf die berufliche Zukunft der betroffenen Bewerber.
- **Personalisierte Versicherungstarife:** Eine Versicherungsgesellschaft verwendet KI, um personalisierte Versicherungstarife zu erstellen. Basierend auf dem Verhalten des Versicherungsnehmers, wie beispielsweise Fahrverhalten bei Kfz-Versicherungen oder Lebensstil bei Krankenversicherungen, berechnet die KI automatisch die Prämienhöhe. Diese automatisierte Profilerstellung und Entscheidung kann zu höheren oder niedrigeren Versicherungsprämien führen, was eine wesentliche (finanzielle) Auswirkung auf die betroffene Person hat.
- **Betrugsprävention im E-Commerce-Bereich:** Ein Online-Shop nutzt eine KI-Anwendung zur Betrugserkennung, die automatisch entscheidet, ob eine Transaktion verdächtig ist und deshalb blockiert oder genauer überprüft wird. Die Entscheidung,

173 Disclaimer: Diese Bespiele dienen der Veranschaulichung und können Sachverhalte enthalten, die aus anderen rechtlichen Gesichtspunkten – insb grundrechtlichen – rechtswidrig sein können. Den Autoren geht es dabei darum, zu zeigen, wie weit der Anwendungsbereich des Art 22 DSGVO reichen kann und welche alltäglichen Sachverhalte bei Vorliegen der rechtlichen Voraussetzungen unter Art 22 DSGVO fallen können.

Beispiel

Ein Finanzdienstleister nutzt einen KI-Algorithmus, um automatisierte Trades durchzuführen. Der Algorithmus agiert autonom und entscheidet aufgrund unerwarteter Marktdatenmuster, eine große Menge an Aktien zu verkaufen, was einen plötzlichen Preissturz auslöst, wodurch andere Marktteilnehmer Verluste erleiden. Der Anbieter des Algorithmus hat ihn umfassend getestet und die gängigen Standards befolgt, konnte jedoch den außergewöhnlichen Markteinfluss der KI nicht vorhersehen.

Zum einen trifft den Anbieter der Software mangels eigenen vorwerfbaren Verhaltens keine deliktische Haftung nach dem ABGB. Eine Zurechnung des Verhaltens der KI etwa mittels analoger Anwendung der Regelungen über die Gehilfenhaftung kommt nach den oben dargelegten Standpunkten ebenfalls nicht in Betracht, und wäre ohnehin die Ersatzfähigkeit von bloßen Vermögensschäden im deliktischen Bereich sehr eingeschränkt.

Dieser Grundgedanke steht im Einklang mit der traditionellen Ausrichtung des Privatrechts und betont insbesondere die individuelle Verantwortlichkeit. Allerdings ist die Verschuldenshaftung nicht der einzige denkbare Ansatz, um rechtliche Verantwortung zu allozieren. So existieren im Bereich der verschuldensunabhängigen Haftung Regelungen, die an der objektiven Gefährlichkeit einer Sache oder eines Verhaltens ansetzen und damit die Ersatzpflicht für Schäden, die durch diese Gefahrenquellen verursacht wurden, dem verantwortlichen Betreiber oder Halter dieser Sachen zuweisen. Diese verschuldensunabhängigen Ansätze vermeiden Beweisprobleme in Bezug auf die Verantwortlichkeit für den Zustand der Gefahrenquelle und finden ihre Ausgestaltung häufig in Form der Gefährdungshaftungstatbestände. Insbesondere angesichts technologischer Neuerungen, die durch hohe Komplexität und Autonomie gekennzeichnet sind, hat sich die Diskussion um alternative Haftungskonzepte neuerlich intensiviert.[90]

Ein prominenter Ansatz in diesem Zusammenhang ist die gerade erwähnte **Gefährdungshaftung**. Anstelle eines schuldhaft handelnden Schädigers tritt der Halter oder Betreiber einer gefährlichen Sache, sofern sich das inhärente Risiko dieser Sache verwirklicht. Die Rechtfertigung dieser Systeme liegt in der besonderen Gefährlichkeit der betroffenen Tätigkeiten oder Gegenstände. Ein besonders relevantes Beispiel ist die Haftung für Kraftfahrzeuge gemäß dem Eisenbahn- und Kraftfahrzeughaftpflichtgesetz (EKHG) sowie die Produkthaftung nach dem PHG, die zumindest Ansätze einer Gefährdungshaftung aufweist. Diese Regime ermöglichen es, komplexe und schwer zu führende Beweisfragen zumindest in Bezug auf ein Verschulden zu umgehen, und stellen sicher, dass Geschädigte dennoch einen effektiven Schadensausgleich erhalten.

90 *Spindler*, Roboter, Automation, künstliche Intelligenz, selbst-steuernde Kfz – Braucht das Recht neue Haftungskategorien? CR 2015, 766; *Wendehorst*, Strict Liability for AI and other Emerging Technologies, JETL 2020, 150; *De Franceschi/Schulze*, Digital Revolution – New Challenges for Law (2019), Introduction, 9 ff; *Zech*, Entscheidungen digitaler autonomer Systeme: Empfehlen sich Regelungen zu Verantwortung und Haftung? Gutachten Teil A zum 73. Deutschen Juristentag (2020) 87 ff; Spindler, Neue Haftungsregeln für autonome Systeme? JZ 2022, 793; siehe auch die Beiträge in *Lohsse/Schulze/Staudenmayer* (Hrsg), Liability for AI (2023).

1.3.3. Musikgenerierende KI-Tools

Auch musikgenerierende KI-Tools haben in den letzten Jahren erhebliche Fortschritte gemacht. Plattformen wie AIVA („Artificial Intelligence Virtual Artist") oder Suno sind inzwischen in der Lage, Musikstücke zu komponieren, die von klassischen Symphonien bis hin zu Songs im Stil aktueller Chart-Hits reichen. Diese KI-Systeme können komplexe Musikstrukturen analysieren und neue Werke schaffen, die den Stil berühmter Komponisten oder ganzer Genres nachahmen. Komponisten und Musikproduzenten können durch diese Technologien entweder Inspiration gewinnen oder KI-generierte Tracks für verschiedene Zwecke wie Werbung, Film oder Videospiele erstellen lassen.

1.3.4. Videogenerierende KI-Tools

Videogenerierende KI-Tools wie RunwayML oder Synthesia haben in den letzten Jahren ebenfalls erhebliche Fortschritte gemacht und ermöglichen es nun, aus einfachen Texteingaben oder Bildern vollständig neue Videos zu erstellen. Mithilfe von KI können sie teilweise realistische Szenen, Animationen und sogar virtuelle Sprecher generieren. Einige dieser Tools wandeln Textbeschreibungen direkt in Videoinhalte um, während andere automatische Videobearbeitungen durchführen, Spezialeffekte hinzufügen oder Stilrichtungen anpassen. Dadurch wird die Erstellung von Videos deutlich zugänglicher und effizienter, sodass selbst Privatpersonen ohne professionelle Ausrüstung oder tiefgreifende Kenntnisse ansprechende Filme produzieren können. Auch Open AI hat nunmehr ein neues Videotool namens Sora gelauncht. Aus rechtlichen Gründen ist dieses Tool auf dem europäischen Markt noch nicht verfügbar.[6]

Beispiel

Ein Beispiel für einen KI-generierten Film ist der Kurzfilm „The Frost", abrufbar auf der Videoplattform YouTube.[7] Darin werden bizarre Szenen einer Eislandschaft gezeigt, inklusive Menschen und Tieren, die sie besiedeln. Für die Produktion von „The Frost" wurde ein Drehbuch von *Josh Rubin* verwendet, sie wurde mit den KI-Tools DALL-E 2 und D-ID, einem Tool zur Animation von Fotos, umgesetzt.[8]

1.3.5. Deepfakes

Die rasante Entwicklung aktueller KI-Tools hat es auch ermöglicht, innerhalb kürzester Zeit und mit minimalem Aufwand täuschend echt wirkende künstlich generierte Fotos, Videos und Audiodateien zu erstellen. Diese Technologien erlauben es, Stimmen von Personen zu imitieren oder ihr Erscheinungsbild in visuellen Medien nachzubilden – die sogenannten Deepfakes.

6 Siehe https://sora.com/ (6.12.2024).
7 Kurzfilm abrufbar unter https://www.youtube.com/watch?v=IgPvoPBrlTE (22.10.2024).
8 *heise online*, Magisch und verstörend: KI-Kurzfilm zeigt Stärken der Technik – und Schwächen, https:// www.heise.de/hintergrund/Die-surreale-Welt-von-DALL-E-jetzt-als-KI-Kurzfilm-9163512.html (22.10.2024).

Teil VI. Geheimnisschutz und KI

Klara Geuer

1. Einleitung

Der Schutz von Geheimnissen ist im privaten (etwa im Hinblick auf Persönlichkeitsrechte und Datenschutz),[1] geschäftlichen und staatlichen Bereich von zentraler Bedeutung. Mit der fortschreitenden Verbreitung von KI in nahezu allen Lebensbereichen gewinnt diese Thematik an Komplexität. Unternehmen und Organisationen stehen vor der Herausforderung, ihre **Geschäftsgeheimnisse** zu wahren, obwohl sie selbst, ihre Beschäftigten, Geschäftspartner und auch Wettbewerber KI-Tools entwickeln und einsetzen, um Produkte und Abläufe zu optimieren. In Berufen mit besonderer Verschwiegenheitspflicht rückt zudem der Schutz von **Berufsgeheimnissen** verstärkt in den Fokus. Dieses Kapitel untersucht den Geheimnisschutz im Kontext von KI.

2. Geschäftsgeheimnisse

2.1. Ausgangspunkt

Viele KI-Modelle werden mit Geschäftsgeheimnissen und anderen vertraulichen Informationen trainiert. Dies hilft ihnen dabei, den KI-Nutzern bestmögliche Ergebnisse zu liefern. Dabei stellt sich die Frage, ob und wie Geschäftsgeheimnisse geschützt werden können, insbesondere auch dann, wenn KI-Systeme von externen Anbietern bereitgestellt werden und der Nutzer wenig oder keine Kontrolle darüber hat, wie Daten verarbeitet werden.

2.2. Rechtsrahmen

In Österreich befinden sich die Rechtsgrundlagen zum Schutz von Geschäftsgeheimnissen im Bundesgesetz gegen den unlauteren Wettbewerb 1984 (UWG),[2] konkret in den zivilrechtlichen Sonderbestimmungen zum Schutz von Geschäftsgeheimnissen in den **§§ 26a bis 26j UWG**.

EU-rechtliche Basis dieser Bestimmungen ist die **Geheimnisschutz-Richtlinie RL 2016/943/EU** (GG-RL)[3] der EU. Vor einigen Jahren hat der EU-Gesetzgeber erkannt, dass Verletzungen von Geschäftsgeheimnissen oft nicht verfolgt werden,

1 Siehe hierzu „IP- und Persönlichkeitsrechte und KI", V. Teil, 2., sowie „Datenschutz und KI", III. Teil.
2 Bundesgesetz gegen den unlauteren Wettbewerb 1984, BGBl 1984/448 idF BGBl I 2023/99.
3 RL (EU) 2016/943 des Europäischen Parlaments und des Rates vom 8. Juni 2016 über den Schutz vertraulichen Know-hows und vertraulicher Geschäftsinformationen (Geschäftsgeheimnisse) vor rechtswidrigem Erwerb sowie rechtswidriger Nutzung und Offenlegung, ABl L 2016/157, 1.

BEinstG). Auch diese Möglichkeiten stehen dem Arbeitnehmer offen, wenn das Arbeitsverhältnis aufgrund eines geschützten Merkmals beendet wurde und eine KI wesentliches oder sogar einziges Entscheidungstool im Beendigungsprozess war.

4. Pflichten des Arbeitgebers bzw Arbeitnehmers beim Einsatz einer KI

Durch den Einsatz von KI durch Arbeitgeber in ihren Betrieben sowie durch Arbeitnehmer im Zuge der Arbeitsverrichtung kann die Sicherstellung eines **effektiven Beschäftigtenschutzes** erforderlich sein sowie ein Eingriff in allfällige Rechte des Betriebsrates vorliegen. Die aus den Fürsorgepflichten des Arbeitgebers abgeleiteten Informationspflichten des Arbeitgebers wurden in Punkt 3.2. behandelt.

Auf alle auf einem privatrechtlichen Vertrag beruhenden Arbeitsverhältnisse ist das Arbeitsverfassungsgesetz (ArbVG) anwendbar. Nach diesem kommen dem Betriebsrat grundsätzlich die Rechte der Information, Beratung und Mitbestimmung zu. Für die Anwendbarkeit dieser Rechte des Betriebsrates auf den Einsatz von KI durch den Arbeitgeber oder Arbeitnehmer sind daher allfällige rechtliche Bestimmungen des ArbVG zu berücksichtigen.

Durch die datenschutzrechtlichen Vorgaben der DSGVO ergeben sich darüber hinaus Pflichten, die ein Arbeitgeber – als Verantwortlicher einer Datenanwendung – beachten muss. Dazu Näheres in Punkt 4.4.

4.1. Rechte des Betriebsrates nach dem ArbVG

Dem ArbVG ist die Begrifflichkeit der „künstlichen Intelligenz" zumindest nicht wörtlich entnehmbar, jedoch gibt es Bestimmungen, unter welche auch eine KI subsumiert werden könnte. Allenfalls einschlägige Bestimmungen könnten § 91 ArbVG, § 92a ArbVG, § 96 ArbVG, § 96a ArbVG sowie § 109 ArbVG sein. Diese Normen waren entweder bereits in der Stammfassung des ArbVG aus dem Jahr 1973 enthalten oder fanden durch einen Initiativantrag im Jahr 1986 bzw durch eine Regierungsvorlage im Jahr 1994 Einzug in das ArbVG – somit lange bevor KIs auch nur in ihrer potenziellen Möglichkeit diskutiert wurden. Fraglich ist daher, ob diese alten Regelungen „jung" geblieben sind und daher auch auf den aktuellen Stand der Technik, inklusive KI, anwendbar sind oder ob eine Überholung der gesetzlichen Regelungen durch den Gesetzgeber zwingend und vor allem zeitnah erforderlich ist.

Nach **§ 91 Abs 1 ArbVG** ist der Arbeitgeber jedenfalls verpflichtet, dem Betriebsrat über alle Angelegenheiten Auskünfte zu erteilen, welche die wirtschaftlichen, sozialen, gesundheitlichen oder kulturellen Interessen des Arbeitnehmers berühren. In **§ 91 Abs 2 ArbVG** ist außerdem normiert, dass der Arbeitgeber den

3.1.1.1. Verfassungsrecht

Die Frage, ob KI im Rahmen der Strafgerichtsbarkeit als eigenständiger **„Richter"** fungieren könnte, stößt auf klare rechtliche Grenzen. Gemäß den Art 82 ff B-VG[234] ist die ordentliche Gerichtsbarkeit, zu der auch die Strafgerichtsbarkeit gehört, ausschließlich durch **menschliche Richter** besetzt. Obwohl der Begriff „Richter" auf den ersten Blick technikneutral erscheinen mag, wird durch die verfassungsrechtlichen Bestimmungen eindeutig festgelegt, dass Richter Menschen sein müssen.[235] Dies wird unter anderem durch die Regelung, dass Richter vom Bundespräsidenten oder einem ermächtigten Bundesminister ernannt werden, sowie durch den Verweis auf Altersgrenzen und Ruhestandspflichten in Art 88 B-VG unterstrichen. Diese Bestimmungen machen deutlich, dass der Gesetzgeber bei der Schaffung der Verfassung explizit auf natürliche Personen abzielte. Nach dem aktuellen Verfassungsrecht ist der Einsatz von KI als vollwertiger „Richter" in der Strafgerichtsbarkeit **unzulässig**.[236] Algorithmen und KI-Systeme, die bislang weder als natürliche noch als juristische Personen anerkannt sind, können daher nicht die Position eines Richters einnehmen. Diese Beschränkung gilt nicht nur für Richter, sondern auch für andere Akteure im Strafprozess wie Staatsanwälte oder andere nichtrichterliche Bundesbedienstete[237] sowie Verteidiger. Das bestehende verfassungsrechtliche Fundament zieht somit eine klare Grenze, die den Einsatz von KI in richterlicher Funktion im Strafprozessrecht ausschließt, unabhängig von den technologischen Fortschritten und den potenziellen Fähigkeiten solcher Systeme.

3.1.1.2. Weitere rechtliche Bedenken

Neben den verfassungsrechtlichen Bedenken stellt auch die geltende **Gesetzeslage außerhalb der StPO**[238] erhebliche Hürden für den Einsatz eines KI-Strafrichters dar. Ein KI-Strafrichter wäre ein Algorithmus, der eigenständig und vollautomatisiert die Ermittlung des Sachverhalts, die Beweiswürdigung, die rechtliche Subsumtion und schließlich die Entscheidung über eine strafrechtliche Anklage übernehmen würde.[239] Diese Form der automatisierten Entscheidungsfindung ist jedoch streng reglementiert, insb durch § 41 DSG[240], der auf der EU-Datenschutzrichtlinie für Polizei und Justiz (Art 11 DSRL-PJ)[241] basiert.

§ 41 DSG legt fest, dass automatisierte Entscheidungen im Einzelfall, die nachteilige Rechtsfolgen für eine betroffene Person haben oder sie erheblich beeinträch-

234 Bundes-Verfassungsgesetz BGBl 1930/1 idF BGBl I 2024/89.
235 Vgl dazu *Reindl-Krauskopf*, Grundrechtliche und strafprozessrechtliche Grenzen: Welche rote Linien zieht das Recht? AnwBl 2024, 35 (35).
236 *Mayrhofer/Parycek*, Digitalisierung des Rechts – Herausforderungen und Voraussetzungen, in ÖJT (Hrsg), Verhandlungen des 21. ÖJT IV/1 (2022) 3, 81 ff; *Matejka*, Mensch versus Maschine, RZ 2019, 134 (135 f); *Reindl-Krauskopf*, AnwBl 2024, 35 (35).
237 *Reindl-Krauskopf*, AnwBl 2024, 35 (35).
238 Strafprozßordnung 1975 BGBl 1975/631 idF BGBl I 2024/157.
239 In diese Richtung argumentierend *Reindl-Krauskopf*, AnwBl 2024, 35 (35).
240 Datenschutzgesetz BGBl I 1999/165.
241 BGBl I 2017/120; ErläutRV 1664 BlgNR 25. GP 16.

Teil IX. Ethik und Recht und KI

Lukas Madl

1. Einleitung

Um eine vertrauenswürdige KI zu ermöglichen, benötigt es eine enge Integration zwischen Ethik und Recht. Eine Domäne allein wird die Herausforderungen nicht bewältigen können. Ethische Kompetenz für alle Akteure wird daher immer wichtiger.

„*In civilized life, law floats in a sea of ethics*" ist ein Zitat des ehemaligen Obersten Richters der Vereinigten Staaten *Earl Warren.*[1] Er bringt damit zum Ausdruck, dass die Gesetzgebung einer ständigen Reflexion über Werte bedarf. Denn sie sind die Orientierungslichter, die erkennen lassen, was im Leben gut, richtig, wichtig und schützenswert ist.

Die rasanten Entwicklungen rund um KI werden daher von vielschichtigen ethischen Debatten begleitet. Die Gesellschaft steht vor der grundlegenden Herausforderung, KI an menschliche Ziele und Werte auszurichten[2] und Ökosysteme zu schonen (zB durch Energieeffizienz oder nachhaltige Anwendungen). Was braucht es, damit KI zu einer besseren Welt beiträgt und nicht als dystopische Triebkraft wirkt? Das ist eine existenzielle Frage.

Denn die KI verändert heute unser Weltgefüge enorm. Sie ist dabei, fast alles zu revolutionieren: wie wir arbeiten, wie wir schreiben, wie wir spielen, wie wir leben, wie wir Entscheidungen treffen; wie wir unsere Talente verkümmern lassen oder sie nutzen, etwa durch Tools, die Musik, Kunst oder Design leichter zugänglich machen. Aber gleichzeitig besteht auch die Gefahr, dass wir unsere Fähigkeiten verlernen, wenn wir uns zu sehr auf KI verlassen, etwa bei der der Problemlösung und Entscheidungsfindung oder beim Texte-Schreiben.

KI kann Produktionsprozesse effizienter machen, zum Klimaschutz beitragen, Krankheiten früher diagnostizieren.[3] Sie kann aber auch politische Debatten in sozialen Medien manipulieren, menschliche Vorurteile in algorithmischen Entscheidungsprozessen reproduzieren und den ökologischen Fußabdruck der Menschheit weiter vergrößern. Und mit KI können auch verheerendere Tötungsmaschinerien durch autonome Waffensysteme etabliert werden.

1 *Henz*, Ethical and legal responsibility for Artificial Intelligence, Discover Artificial Intelligence 1, 22.9.2021, https://doi.org/10.1007/s44163-021-00002-4 (26.7.2024), 1.

2 Vgl *Han/Kelly/Nikou/Svee*, Aligning artificial intelligence with human values: reflections from a phenomenological perspective, AI & SOCIETY 37, 20.7.2022, https://doi.org/10.1007/s00146-021-01247-4 (30.7.2024), 1383–1395.

3 ZB durch KI-gesteuerte Energiemanagementsysteme oder die medizinische Bildanalyse.