

Artificial Intelligence: Eine Bestandsaufnahme im Jahr 2018

Bericht über die Tagung «ICT – Recht und Praxis: Artificial Intelligence: Was ist möglich? Wie reagiert das Recht?» vom 26. September 2018 in Zürich

MARIO J. MINDER*

- I. Anwendungsfälle von AI
 - 1. Gesundheitswesen
 - 2. Investmentbanking
 - 3. Rückversicherungen
- II. Immaterialgüterrechtlicher Schutz von AI und ihren Ergebnissen
- III. AI und Datenschutzrecht
- IV. AI und Wettbewerbsrecht
- V. Haftung für AI-Ergebnisse
 - 1. Haftungsgrundlagen
 - 2. Anbietersicht
- VI. Potenzial von AI für Wirtschaft und Gesellschaft

Die ICT-Veranstaltungsreihe des Europa Instituts Zürich (EIZ)¹, die vor zwanzig Jahren unter dem Titel «Geschäftsplattform Internet» gestartet war, feierte mit der Tagung zum Thema Artificial Intelligence (AI) ein rundes Jubiläum. Dr. ROLF AUF DER MAUR, der zusammen mit Dr. PETER K. NEUENSCHWANDER als Tagungsleiter fungierte, zeichnete eingangs ein Bild eines Alltags, der bereits unbemerkt von AI durchdrungen worden ist, z.B. mit Suchmaschinen, Sprachassistenten und Bilderkennungsverfahren. Indes wies er darauf hin, dass es schwierig sei, AI zu definieren. Dieser Unsicherheit hinsichtlich des Untersuchungsgegenstands sollte in einem ersten Themenblock mit Anwendungsbeispielen von

AI aus drei Geschäftsbereichen begegnet werden.

I. Anwendungsfälle von AI

1. Gesundheitswesen

Dr. SHERRYL MANALO, Senior Software Development Engineer bei Microsoft, präsentierte insbesondere das unternehmenseigene Forschungsprojekt «InnerEye», das automatisch Tumore erkennen und messen kann. Neben den spezifischen Vorteilen dieses Projekts wie Zeitgewinn oder Erkennung des Krankheitstrends war vor allem eine Erkenntnis MANALOS bemerkenswert: Es wird eine grosse Herausforderung darstellen, AI-Modelle im Gesundheitsbereich zu zertifizieren. Eine AI verändere sich ständig und werde besser oder schlechter, abhängig von der Qualität der Daten, die ihr als Lerngrundlage zugeführt werden.

2. Investmentbanking

JÜRGEN PULM, PhD, CEO von RBS Services Switzerland, stellte im anschließenden Referat die algorithmengesteuerte Kundenberatung «NatWest Invest» vor, bei der ein Kunde nur zahle und die Bank nur hafte, sofern ein Investment getätigt wird. Zukünftig soll es Banken möglich sein, mithilfe von AI die operationale Effizienz zu steigern (z.B. mit Chatbots), das Risikomanagement und die Einhaltung gesetzlicher Bestimmun-

gen zu optimieren sowie dem Kunden ein vollständig personalisiertes Portfolio anzubieten. Von PULM aufgeworfene Fragen wie, wer der Risk Appetite Owner ist, wenn ein Algorithmus die Entscheidungen trifft, werden weiter zu diskutieren sein.

3. Rückversicherungen

Rückversicherer arbeiten mit verschiedensten Datensätzen, welche die Versicherer oftmals in unstrukturierter und nicht anonymisierter Form zur Verfügung stellen, z.B. Eintrittsformulare von Spitälern und Ärzten, wie BIANCA SCHEFFLER, IT-Direktorin bei SwissRe, im nächsten Vortrag erläuterte. AI könne dabei helfen, Risiken im Portfolio eines Versicherers zu erkennen und Personen-daten zu anonymisieren. Wenn AI für den gesamten Prozess der Risikobewertung verwendet wird, d.h. um Daten einzuspeisen, Informationen zu überwachen und Entscheidungen zu treffen, muss für SCHEFFLER insbesondere nachvollziehbar sein, ob das Resultat überhaupt den bereitgestellten Daten geschuldet ist.

II. Immaterialgüterrechtlicher Schutz von AI und ihren Ergebnissen

Im Anschluss an die Vorstellung der Anwendungsfälle prüfte Dr. MATHIS BERGER, Rechtsanwalt in Zürich, kurso-

* MLaw, Zürich.

¹ In Zusammenarbeit mit dem Schweizer Forum für Kommunikationsrecht (SF•FS) und weiteren Partnern.

risch die Möglichkeiten von Schutz für AI und ihre Ergebnisse unter dem URG und dem PatG.

Urheberrechtsschutz für AI als Software sei denkbar, für die Ergebnisse der AI hingegen nicht. Letztere dürften regelmässig keine geistigen Schöpfungen darstellen und für einen allfälligen derivativen Rechtserwerb durch den AI-Entwickler fehle es an einer originären Werkschöpfung durch einen Menschen.

Beim Schutz von AI als solche durch das PatG zeichnete BERGER die bekannten Probleme des Patentrechts mit Software nach. Mit Bezug auf AI-Ergebnisse gebe es insoweit eine Besonderheit, als bei der Beurteilung des Nichtnaheliegens wohl kein menschenbezogener Massstab gelten dürfe. Bei der Erfindernennung gebe es ein Problem, da der Erfinder keine Person sei. Die AI könne weiter nicht als Werkzeug wie z.B. ein Schraubenzieher betrachtet werden, da sie selber erfindetisch tätig werde. Auch ein abgeleiteter Schutz des Ergebnisses der AI schlage fehl, da in der Offenbarung nicht beschrieben werden könne, wie dieses Ergebnis aussieht, und Folgeerfindungen ohnehin kein unmittelbares Verfahrenserzeugnis darstellten.

Die vorgenannten Defizite des geltenden Rechts sollten gemäss BERGER nur behoben werden, wenn ein Marktversagen droht, d.h. wenn AI und Produkte von AI ohne Rechtsschutz nicht mehr hergestellt würden. Aus den derzeit in der Lehre andiskutierten Gesetzesänderungsvorschlägen, die BERGER zum Schluss präsentierte, stach im Bereich Urheberrecht etwa die Forderung nach einer Ausnahme für «non-expressive use» für Machine Learning heraus und im Patentrecht die Abschaffung des Erfinderbezugs, für die sich auch BERGER aussprach. Abgesehen davon stand der Referent einer Auflockerung der Schutzvoraussetzungen eher kritisch gegenüber, da sie zu einer rapiden Zunahme von Schutzrechten führen

würde, was auch der Weiterentwicklung von AI hinderlich sein könne.

III. AI und Datenschutzrecht

MARTINA ARIOLI, Rechtsanwältin in Zürich, begann ihr Referat «Daten als Treibstoff selbstlernender Systeme» mit der Aussage, dass selbstlernende Algorithmen nur mit grossen Mengen an qualitativ guten Daten die erwünschten Resultate liefern können.

Datenschutzrechtliche Vorgaben müssten beachtet werden, wenn Algorithmen Personendaten oder pseudonymisierte Daten bearbeiten, wobei ARIOLI auf die immanenten Widersprüche zwischen datenschutzrechtlichen Vorgaben und Big Data Analytics verwies. Sie erläuterte, dass die Anonymisierung mit verschiedenen Methoden (z.B. Differential Privacy, Federated Learning) erreicht werden könne, wobei die Anonymisierungen selbst eine datenschutzrechtlich relevante Bearbeitung seien und eine Re-Identifizierung nicht immer vollständig ausgeschlossen werden könne. Im Zusammenhang mit den diversen laufenden Initiativen zur Förderung von AI und der Nutzung von Daten (Stichwort «free flow of data» in der EU) betonte sie, dass auch als Sachdaten erachtete Informationen häufig einen Personenzusammenhang aufweisen, insbesondere im Kontext von IoT.

Themenschwerpunkte des Referats bildeten das datenschutzrechtliche Transparenzprinzip, «Algorithmic Accountability» und «Explainability». ARIOLI kam in ihrer Analyse zum Schluss, dass weder die Informationspflicht ex ante (Art. 13 bzw. 14 DSGVO) noch das Auskunftsrecht ex post (Art. 15 DSGVO) ein Recht auf eigentlichen Zugang zum Algorithmus konstituierten. Obschon die Informationspflicht die Pflicht zur Offenlegung des allgemeinen Funktionierens des Algorithmus beinhalte und beim Auskunfts-

recht zusätzlich der Hergang der Entscheidung dargelegt werden müsse, bringe dies keine Überprüfung des Algorithmus mit sich, zumal der Zugang zum Algorithmus auch mit überwiegen- den privaten Interessen (als Geschäftsgeheimnis) verwehrt werden könne. Selbiges gelte auch im Zusammenhang mit Art. 22 DSGVO, wonach die betroffene Person das Recht hat, nicht einer ausschliesslich auf einer automatisierten Verarbeitung beruhenden Entscheidung unterworfen zu werden.

Zur «Explainability» führte ARIOLI aus, dass die von selbstlernenden Algorithmen erzielten Resultate selbst für Entwickler nicht immer nachvollziehbar seien und deshalb auch nicht erklärt werden könnten. Diese Komplexität dürfe jedoch nicht dazu führen, dass den Betroffenen aussagekräftige Informationen vorenthalten blieben. Ferner dürften Datenverarbeitungen grundsätzlich nicht diskriminierend sein (E. 71 DSGVO), was beim teilweise inhärenten Bias selbstlernender Algorithmen aufgrund unrichtiger oder trädierter Input-Daten nicht immer ausgeschlossen werden könne.

ARIOLI schloss damit, dass Datenschutz allein nicht geeignet sei, sämtliche sich aus AI ergebenden Probleme, wie Erklärbarkeit von AI, Sicherstellung diskriminierungsfreier Resultate oder den ethischen Einsatz von AI zu lösen.

IV. AI und Wettbewerbsrecht

Prof. Dr. PETER GEORG PICHT, Professor für Handels- und Wirtschaftsrecht an der Universität Zürich, prüfte in seinem Referat die Tragfähigkeit geltenden Wettbewerbsrechts, insbesondere des Kartellrechts, zur Beurteilung von AI-Sachverhalten.

Unklar sei etwa die kartellrechtliche Beurteilung von impliziter, algorithmischer Kollusion. Damit gemeint sei eine parallele Ausrichtung des Wettbewerbsverhaltens ohne eine gezielte,

auf Verminderung des Wettbewerbsdrucks ausgerichtete Abstimmung. Vielmehr stütze sich die Anpassung des Wettbewerbsverhaltens auf Beobachtung und Reaktion durch algorithmische Systeme. Diese könnten Verhaltenssignale voneinander deutlich besser lesen als Menschen, was die Wahrscheinlichkeit impliziten Kolludierens in algorithmischen Märkten signifikant erhöhe. Möglicherweise müsse infolgedessen die Zulässigkeit impliziter Kollusion, von der heute ausgegangen wird, überdacht werden. Gestützt auf das aktuelle Fallrecht zum Thema algorithmischer Marktmissbrauch (Google Shopping, Facebook und Lufthansa) sei es schwierig, die Stärken und Schwächen des Wettbewerbsrechts im Umgang mit den neuen Technologien bereits abschliessend abzuschätzen.

Jedenfalls solle das Wettbewerbsrecht nicht vorschnell als Allzweckwaffe eingesetzt werden. Andere Regelungsbereiche wie Finanzmarktrecht und Datenschutzrecht enthielten schon heute algorithmenspezifische Regeln. Bspw. sähen die RTS zu MiFID II vor, dass algorithmisch agierende Finanzmarktteilnehmer eine klare und klar dokumentierte Verantwortlichkeitsstruktur schaffen müssen. Dennoch seien derzeit weder das Wettbewerbsrecht noch andere Rechtsgebiete ausreichend auf die neuen Problemstellungen vorbereitet. Das Wettbewerbsrecht könne und solle von den Instrumenten, die andere Rechtsbereiche bereits entwickelt haben, lernen und sich dadurch für seine kommenden Aufgaben ertüchtigen. In jedem Fall bedürfe es einer besseren empirischen Basis für die (Wettbewerbs-)Rechtsanwendung. Ein wettbewerbsrechtliches Vorgehen gegen unerwünschte Marktergebnisse erscheine angesichts des derzeitigen begrenzten Verständnisses algorithmischer Märkte sachgerecht, das Sanktionsregime müsse aber so ausgelegt werden, dass insgesamt eine

zumutbare Haftungslast für die Marktakteure entstehe.

Mit Blick auf die Zukunft lehnte es PICHT ab, ein AI-Regulierungsgesetz zu schaffen, das bereits heute sämtliche Fragen dauerhaft zu beantworten versucht. Vielmehr plädierte er für eine schrittweise Anpassung des Rechtsrahmens unter Koordination der einschlägigen Rechtsgebiete.

V. Haftung für AI-Ergebnisse

1. Haftungsgrundlagen

Prof. Dr. ROLF H. WEBER, Rechtsanwalt und em. Professor an der Universität Zürich, gab eine Tour d'Horizon über die AI-spezifischen Probleme bestehender Haftungskonzepte.

Bei der Haftung nach Vertrag – es dürften viele AI-Dienstleistungen als Auftrag zu qualifizieren sein – müsse etwa die sich ohnehin im Gang befindliche Diskussion über die Ausdehnung des Sorgfaltskonzepts weitergeführt werden. Zentrale Bedeutung werde innerhalb des Problemkreises Inhaltskontrolle von AGB der Frage zukommen, ob man sich von der Haftung für Subunternehmen, insbesondere Software-Lieferanten, befreien kann. Im Bereich Deliktshaftung werde sich die Frage stellen, ob die traditionelle Produktbeobachtungspflicht ausreicht, um eine Haftung zu begründen, wenn eine ursprünglich fehlerfreie AI durch Selbstentwicklung zur Gefahrenquelle wird. Zum Thema Gefährdungshaftung wies WEBER auf die europäische Diskussion zur Erweiterung des Produktbegriffs auf Software und gewisse Dienstleistungen hin, die darin münden könnte, dass AI dereinst vom Produkthaftungsgesetz und Produktsicherheitsgesetz erfasst wäre. Allerdings dürften oftmals vorliegende komplexe Produkt- und Dienstleistungs-Value-Chains die klare Zuordnung von Fehlern erschweren.

Für die Zukunft erachtete WEBER es als vorstellbar, Sonderregeln in Spe-

zialgesetzen zu normieren, wie sie z.B. Deutschland neuerdings im StVG für Führer von Fahrzeugen mit vollautomatisierter Fahrfunktion vorsieht. Längerfristig werde sich wohl auch die Frage stellen, ob eine AI in einem Roboter als sog. E-Person haftpflichtig werden kann, was voraussetze, dass solche Systeme mit einer eigenständigen Rechtspersönlichkeit ausgestattet würden.

2. Anbietersicht

DANIEL SCHÖNBERGER, Leiter des Rechtsdiensts von Google Schweiz und Österreich, fragte in seiner Präsentation, wer für das Handeln von AI aus Anbietersicht die «moralische Verantwortung» trägt.

Maschinen und Algorithmen könne philosophisch betrachtet keine «moralische Verantwortung» zugeschrieben werden, da der Begriff integraler Bestandteil des Konzepts der Person bilde, auf dem Moral und Recht basierten. Entsprechend halte Google in seinen AI Principles fest, dass AI «accountable to people» sein soll, wobei der Umfang der menschlichen Kontrolle stark vom Kontext, insbesondere den potenziellen Sicherheitsrisiken, abhängen. Dabei könnten sich die entsprechenden Sorgfaltspflichten durchaus verändern. Hinsichtlich des mit solchen Risiken behafteten Gesundheitsbereichs etwa stellte SCHÖNBERGER die interessante Überlegung an, dass es dereinst Fahrlässigkeit begründen könnte, wenn ein Arzt keine AI-Systeme einsetzt. Das derzeitige allgemeine Haftungsregime erachtete er als genügend. Gleichzeitig schloss er nicht aus, dass sich in risikobehafteten Bereichen dereinst Bedarf ergeben könnte, Spezialgesetze zu ändern.

VI. Potenzial von AI für Wirtschaft und Gesellschaft

ANDY FITZE, Mitbegründer von Swiss-Cognitive, stellte AI in seinem Vortrag

als immense Chance für Wirtschaft und Gesellschaft dar, wies aber gleichzeitig auf Risiken hin. Die Gefahren der missbräuchlichen Verwendung von AI, z.B. im Bereich autonome Waffensysteme, seien enorm und eine Prognose zu den Chancen fast unmöglich. Die meisten Systeme, die heute als auf AI basierend bezeichnet würden, seien in Wirklichkeit keine selbstlernenden Systeme, sondern fussten meist noch auf Regeln. Dennoch würden AI und ihre Produkte sehr schnell auf die Menschheit zukommen. Das liege daran, dass das IoT und

vernetzte Welten derzeit Wachstumsraten von 40 bis 50 Prozent pro Jahr aufwiesen, während das Wachstum der klassischen IT stagniere. Die massiven Datenmengen aus ersterem Bereich seien für uns, anders als für AI, nicht mehr fassbar. AI habe schlicht eine höhere Performance. Dafür dürften Menschen AI im Bereich emotionale Kompetenzen bis auf Weiteres überlegen bleiben.

FITZE richtete einen eindringlichen Appell an Unternehmen, sich bereits heute vertieft mit dem Thema AI

auseinanderzusetzen und nicht bloss zu digitalisieren, sondern digitalneue Geschäftsmodelle zu entwickeln. Sonst bestehe die Gefahr, sich nach dem bevorstehenden «tectonic shift» auf der «falschen Platte» zu befinden.