Oktober 2020

AK POLICY PAPER

KÜNSTLICHE INTELLIGENZ (KI) UND VERBRAUCHERSCHUTZ

AUF EINEN BLICK

- Unreguliert ist KI eine Blackbox, bei der Dateneinsatz, Logik und Entscheidungen intransparent und unverständlich bleiben. Sie kann Nutzen stiften, aber auch Alltagsverhalten überwachen, durch Klassifizierung KonsumentInnen benachteiligen oder als Informationsfilter Meinungsvielfalt bedrohen.
- Zum Schutz der Menschenwürde und der Freiheitsrechte ist überall, wo KonsumentInnen mit KI in Berührung kommen, vorbeugender Schutz durch strikte Regulierung, fachkundige Marktaufsicht und wirksamen Vollzug nötig.
- Das ist möglich, ohne Innovation zu verhindern.

Software, die eigenständig Probleme bearbeitet, gilt für manche bereits als „Künstliche Intelligenz". Vorsichtige sprechen lieber vom „maschinellen Lernen". Intelligenz ist letztlich schwer definierbar. Algorithmen können zunehmend Muster in Daten erkennen und Vorhersagen treffen. Das EU-Weißbuch zu KI benennt viele Risiken, bleibt aber bei den Schutzmaßnahmen hinter den Erwartungen zurück.

In ihrem im Februar veröffentlichten Weißbuch erklärt die EU-Kommission: KI muss vertrauenswürdig sein! Sie macht kein Hehl daraus, dass Nutzen und Gefahren dicht beieinanderliegen. So richtig der Befund, so schwach die Rechtsinstrumente, die die EU-Kommission schlussendlich erwägt. Der vorgeschlagene risikobasierte Ansatz schützt Betroffene unzureichend: Pflichten soll es nur bei „high-risk" KI-Anwendungen geben. Für alles andere muss ein freiwilliges Gütezeichen reichen.

KI kann je nach Einsatzgebiet und Betrachtungswinkel Nutzen stiften. Sie wirft aber elementare Fragen der Ethik, Moral, Demokratie und Menschenrechte auf – vor allem, wenn Algorithmen Entscheidungen vorbereiten oder treffen, die Menschen berühren. Mathematische Formeln können die vielen Facetten des Lebens nicht abbilden. Ohne strikte Ge- und Verbote werden Betroffene in unzähligen KI-Testfeldern zu Versuchskaninchen, die diskriminierend klassifiziert, benachteiligend behandelt und mit ihren Einwänden nicht gehört werden. KI verspricht Effizienzgewinne. Als Blackbox, die nicht nachvollziehbare Bewertungen auswirft, hat sie aber das Potential, die Gesellschaft zu spalten, statt ihren Zusammenhalt zu fördern. Es braucht maximale Trans- →

Autorin: Daniela Zimmer

arbeit.digital AK WIEN

parenz, menschliche Aufsicht und klare Vorgaben für die Zurechnung, Verantwortung und Haftung für fehlerhaftes Handeln von KI – auch bei Anwendungen außerhalb der Kategorie „hoch riskant".

Die ambivalente Rolle der EU

Die EU-Kommission verkennt die Risiken nicht und zählt in ihrem Weißbuch Bedrohungsszenarien (Personenschäden, Missbrauch zu kriminellen Zwecken etc) auf. Dieses Risikobewusstsein spiegelt sich in der Zusammensetzung ihres Beratungsorgans, der High-Level Expert Group on Artificial Intelligence, nicht wieder. Die EU-Menschenrechtsagentur und der europäische Verbraucherverband Beuc treten gegen ein Großaufgebot an Unternehmen an. Ganz in deren Sinn betont die EU-Kommission, es dürfen keine unverhältnismäßigen Bürden für Entwickler und Verwender entstehen. Ihr regulatorisches Ziel beschränkt sich auf Risikotests und Pflichtnormen für besonders risikobehaftete Anwendungen. Mangels (abgestufter) Pflichtauflagen für alle KI-Anwendungen würden viele verbraucherrelevante Anwendungen unreguliert bzw. bloßer Branchenselbstregulierung überlassen bleiben.

Mangels Pflichtauflagen der EU-Kommission für alle KI-Anwendungen würden viele verbraucherrelevante Anwendungen unreguliert bzw. bloßer Branchenselbstregulierung überlassen bleiben.

Im Detail

Nicht nur der Einsatzbereich von KI muss nach dem Plan der EU-Kommission besonders risikobehaftet sein (zB Gesundheit, Transport), sondern auch die Anwendung selbst: der KI-Einsatz muss Rechtsfolgen oder ähnliche Effekte für KonsumentInnen haben, wodurch die Gefahr „für Rechtsverletzungen, Tod oder erheblichen materiellen oder immateriellen Schaden" bestünde. Nur KI, die Beschäftigte berührt und Überwachungstechnologien (wie Gesichtserkennung) sollen von vornherein als riskant gelten. Für diese Bereiche soll es neue Vorschriften – etwa über die Datenqualität, Dokumentations- und Infopflichten, Nachprüfbarkeit der Verfahren, Fehlerbehebung, menschliche Aufsicht und Zulassungsverfahren – geben.

KonsumentInnen werden algorithmisch kategorisiert, etwa bei Suchanfragen im Internet, zielgerichteter Onlinewerbung, News- und Filmempfehlungen oder auch Bonitätskontrollen.

> **„Unfaire" automatisierte Entscheidungen der KI sind nur schwer nachzuweisen und kaum abzuwehren. Das können etwa algorithmisch gesteuerter Werbung oder Onlinepreisen, die auf Internetprofiling basieren sein.**

Wenig Verbraucherschutz vor Intransparenz, Diskriminierung und Manipulation: Unser Leben wird in viel größerem Maß von automatisierten Verfahren beeinflusst, als die Beispiele des Weißbuches illustrieren. Nicht nur Flugverkehr und Finanzmärkte sind auf komplexe Algorithmen angewiesen. Auch KonsumentInnen werden algorithmisch kategorisiert, etwa bei Suchanfragen im Internet, zielgerichteter Onlinewerbung, News- und Filmempfehlungen oder Bonitätskontrollen, die über Konditionen beim Vertragsabschluss entscheiden. Die EU-Kommission bagatellisiert solche Risiken, wenn sie für vieles lediglich eine freiwillige Selbstverpflichtung empfiehlt. Auch bei der Nutzung „smarter" Konsumgüter bzw. digitaler Dienste sind KonsumentInnen oft in unzumutbarer Weise mit Intransparenz, Grundrechtsverletzungen, Benachteiligungen und Verhaltensmanipulationen konfrontiert.
So sind zB „unfaire" automatisierte Entscheidungen schwer nachzuweisen und abzuwehren. BAK-Studien haben die Folgen nicht nachvollziehbarer Bonitätsscores (Bewertung der Zahlungsbereitschaft und -fähigkeit) gezeigt. Oder die Manipulationsgefahr, die von algorithmisch gesteuerten Empfehlungen – zB von Sprachassistenten wie Alexa – ausgeht. Oder Diskriminierungen durch individualisierte Onlinepreise für verschiedene Kundengruppen, die auf Internetprofiling basieren. Ob dies alles hochriskante Anwendungen im Sinne des Weißbuches sind, ist unklar bzw. darf bezweifelt werden.

Schlupflöcher in der DSGVO für den Einsatz intransparenter Algorithmen

Derzeit sind der Datenschutz-Grundverordnung (DSGVO) zufolge nur vollautomatisierte Einzelentscheidungen, die Rechtsfolgen →

haben oder KonsumentInnen erheblich beeinträchtigen, grundsätzlich verboten. Unternehmen wenden oft ein, dass Maschinen nicht selbst entscheiden, sondern menschliche Entscheidungen „nur“ vorbereiten. Maschinelle Bewertungen werden von MitarbeiterInnen (allein des hohen Begründungsaufwands wegen) nachträglich aber kaum abgeändert. Der Schutz muss daher auch auf „halbautomatisierte“ Entscheidungen erweitert werden. Außerdem sollten Betroffene über jeden Algorithmus, der mit Daten von KonsumentInnen arbeitet, informiert werden – unabhängig von den Rechtsfolgen oder einer starken Beeinträchtigung der KonsumentInnen, wie es die DSGVO derzeit verlangt. Auch die Erlaubnistatbestände gehen viel zu weit: algorithmische Entscheidungen sind etwa zulässig, wenn sie für den Abschluss oder die Erfüllung von Verträgen nötig sind und der betroffene Konsument eine Chance erhält, seinen Standpunkt zu erklären und die Entscheidung anzufechten. Der Einsatz bei Verbraucherverträgen sollte besonders begründeten Fällen (wie hohes Zahlungsausfallsrisiko bei Krediten) vorbehalten bleiben. Der Einsatz der Technik, die verwendeten Daten und Logik müssen für die Betroffenen nachvollziehbar sein, denn Unternehmen berufen sich bei Auskunftsersuchen momentan allzu oft auf Geschäftsgeheimnisse.

Der Schutz der KonsumentInnen muss auch auf „halbautomatisierte“ Entscheidungen erweitert werden. Der Einsatz der Technik, die verwendeten Daten und Logik müssen für Betroffene nachvollziehbar sein.

Ruf nach mehr Trainingsdaten für KI erfordert mehr Datenschutz

78 Prozent der in einer Eurobarometerumfrage befragten Personen meinen, Onlineanbieter besäßen viel zu viele Kundendaten und 73 Prozent wollten immer um ihre ausdrückliche Zustimmung zur Datennutzung gefragt werden. Die Anliegen einer großen Mehrheit der KonsumentInnen ist bis dato unerfüllt geblieben. Millionen Personendaten werden noch immer de facto unbemerkt und unkontrolliert aus dem Netz gesaugt. Der Entwicklung zu einer Datenökonomie steht – soweit personenbezogene oder nicht verlässlich anonymisierte Daten betroffen sind – der Grundsatz der Datensparsamkeit entgegen. Wann genau Daten als nicht rückführbar anonymisiert gelten, ist nicht geregelt. ExpertInnen gehen davon aus, dass konkrete Personen auch aus anonymisierten Datensätzen durch KI individuell bestimmbar sind. Es ist zu definieren, wann man (überhaupt noch) von Daten ohne Personenbezug reden kann.

Das Anliegen der KonsumentInnen ist bis dato unerfüllt: Millionen Personendaten werden noch immer de facto unbemerkt und unkontrolliert aus dem Netz gesaugt.

Keine Freizeichnung vom Datenschutz für Wissenschaft und Forschung

Damit die optionale Freizeichnung von den Betroffenenrechten der DSGVO für Zwecke von Wissenschaft und Forschung in vertretbarem Rahmen bleibt, müsste hierzulande klarer definiert sein, wer zu den privilegierten Forschungseinrichtungen zählt. Es fehlt eine klare Grenze zu kommerziellen Aktivitäten. Denn auch Internetriesen betreiben Markt„forschung“. Dabei sollte bescheinigt werden, dass der Forschungsgegenstand im wichtigen öffentlichen Interesse liegt. Den Wünschen von Datenökonomen, wie etwa eines „broad consens“ (Einwilligung zur generellen Datennutzung ohne Zweckbindung) oder gar datenschutzfreien „Playgrounds“, sind Absagen zu erteilen. Die Zustimmungen der Betroffenen sollten stets eingeholt werden und nur durch eine Genehmigung der Datenschutzbehörde (DSB) ersetzt werden können (wenn ein herausragendes öffentliches Interesse am Forschungsgegenstand besteht und Zustimmungen schwer eingeholt werden können). In diesen Fällen ist Betroffenen zumindest ein Widerspruchsrecht einzuräumen.

KI lässt sich mit Datenschutzprinzipien schwer vereinbaren

Der immanente Konflikt ist offen anzusprechen. Kaum auflösbare Widersprüche zwischen Grundrechtsansprüchen und dem tatsächlichen Umgang mit Daten sind vor- →

> **Selbstlernende Systeme suchen in riesigen Datenbeständen nach unerkannten Mustern und Zusammenhängen.**

programmiert. Maschinelles Lernen setzt voraus, dass dem System Unmengen an Trainingsdaten zugeführt werden. Selbstlernende Systeme suchen in riesigen Datenbeständen nach unerkannten Mustern und Zusammenhängen. Sie können aus vorgeblich anonymisierten Datenbeständen auch Einzelpersonen re-identifizieren. Wer KI entwickelt, vertreibt oder einsetzt, muss das Recht auf Schutz des Privatlebens und personenbezogener Daten, die in Art 7 und 8 der EMRK verankert sind, beachten. Datenminimierung, enge Zweckbindung, keine Weiterverarbeitung für mit dem Ursprungszweck nicht kompatiblen weiteren Zwecken, datenschutzfreundliche Voreinstellungen etc. gilt für alle Akteure in der KI-Wertschöpfungskette. Ein Verantwortlicher muss als „Herr der Daten“ in der Lage sein, auf die Verarbeitung jederzeit steuernd einzuwirken. Bestimmt KI selbst, welche Daten sie für welchen Zweck nutzt und entscheidet außerhalb von Entwicklern definierten Bahnen, widerspricht dies fundamental dem Grundsatz der „Accountability“ (Zurechnung, Verantwortung, Haftung). Ein solches Vorhaben kollidiert zudem mit der Pflicht, im Erhebungszeitpunkt den genauen Verwendungszweck der Daten anzugeben.

Wer KI entwickelt, vertreibt oder einsetzt, muss das Recht auf Schutz des Privatlebens und personenbezogener Daten beachten.

KI-basierte Gesichtserkennung

Arbeitspapiere der EU-Kommission enthielten ein mehrjähriges Verbot der KI-Analyse von biometrischen Merkmalen für private wie öffentliche Akteure, um zwischenzeitig eine „solide Methodologie für die Einschätzung der Folgen der Technologie und mögliche Risikomanagementmaßnahmen“ zu entwickeln. Es ist ein fatales Signal, wenn das Weißbuch nun lediglich eine Debatte anstößt, statt sich für ein (zumindest temporäres) Einsatzverbot auszusprechen. Der NGO AlgorithmWatch zufolge nutzt die Mehrheit der EU-Polizeibehörden Software zur Gesichtserkennung oder plant ihren Einsatz. Fast überall mangle es an Transparenz. Automatisierte Gesichtserkennung wird angewandt, um vermisste Kinder zu finden oder gewalttätige Fans im Fußballstadion auszumachen. Die Technologie wirft massive Bedenken auf, die auch von Organisationen wie Privacy International oder Bits of Freedom ausführlich dargestellt wurden. Eine Fehlerrate von 1 Prozent bedeutet etwa: Sind 10.000 Menschen einer Gesichtserkennung ausgesetzt, die polizeilich gar nicht gesucht werden, dann werden 100 von ihnen dennoch als gesucht markiert. Ein Test, der 2018 in London durchgeführt wurde, ergab 104 Übereinstimmungen, von denen nur zwei richtig waren – alle anderen waren Falsch-Positive.

Die Mehrheit der EU-Polizeibehörden nutzt bereits Software zur Gesichtserkennung oder plant ihren Einsatz. Fast überall mangle es an Transparenz.

Einbindung der Betroffenen bei Eingriffen in Grundrechte

Daten- und Privatsphärenschutz sollten wirtschaftlichen Interessen grundsätzlich vorgehen. Wie verhält es sich aber, wenn Eingriffe in diese Rechte mit lebenswichtigen Interessen einzelner Personen, von Gruppen oder der Gesamtgesellschaft begründet werden? Interessenskollisionen sind vorprogrammiert, sobald KI-Anwendungen im Gesundheitssektor Verbesserung bei der Erkennung, Behandlung und Heilung von Krankheiten oder im sicherheitspolizeilichen Einsatz eine bessere Kriminalitätsaufklärung versprechen. Der Preis ist hoch, wenn dabei fundamentale Rechte und Fairness gegenüber großen Bevölkerungsteilen unter die Räder kommen. Vor diesem Hintergrund sollten KI-Anwendungen, die Grundrechte berühren, eine ex ante-Genehmigung durch ein unabhängiges Gremium erfordern. In dieses sind neben Datenschutzbehörden und TechnikexpertInnen auch VertreterInnen betroffener Gruppen (ArbeitnehmerInnen, KonsumentInnen, PatientInnen etc) miteinzubeziehen. Bei der Klärung von Rechtsfragen sind verschiedene Interessen und Werten sorgfältig abzuwägen. Je nach Betroffenheit und weltanschaulichem Hintergrund werden Urteile verschieden ausfallen. Deren gesellschaftliche Akzeptanz steigt, wenn bei der Zusammensetzung der Entscheidungsträ- →

KI-Anwendungen, die Grundrechte berühren, sollen eine ex ante-Genehmigung durch ein unabhängiges Gremium erfordern.

ger auf die Beteiligung der betroffenen Gruppen geachtet wird.

Produkthaftungsregeln aktualisieren

Die Produkthaftungs-RL aus dem Jahr 1985 hat für digitale Trends wie KI keine Antworten parat. Eine überarbeitete RL muss auf alle (nicht) materiellen Sachen, digitale Dienste und digitale Inhalte anwendbar sein. Als „defekt" sollten Produkte gelten, von denen Cybersicherheitsrisiken ausgehen, die erforderliche Updates nicht erhalten oder die nicht DSGVO-konform sind. Die Fähigkeit, selbst zu lernen und autonome Entscheidungen zu treffen, sollte als „Defekt" gelten, wenn dadurch Schäden bei NutzerInnen oder Dritten verursacht werden.

Überholte Produktsicherheits-RL

Die RL aus dem Jahr 2001 verpflichtet Hersteller, Gefahren, die von ihren Produkten ausgehen, selbst zu erkennen und Vorkehrungen zu treffen einschließlich der Rücknahme des Produkts vom Markt und des Rückrufs beim Verbraucher. Klarzustellen ist, dass die RL auf alle Produkte, Dienste und Software, die Algorithmen enthalten, anwendbar ist. Alle mit KI verbundenen Risiken müssen durch die Produktsicherheits-RL abgedeckt sein. KI-basierte Anwendungen sollten auf Cybersicherheit hin geprüft werden, bevor sie auf den Markt kommen dürfen.

Fazit

Das Thema spaltet. Jürgen Schmidhuber, bekannter KI-Forscher, glaubt, dass in wenigen Jahrzehnten KI „den Menschen transzendiert und ein besserer Problemlöser nicht nur in speziellen Teilgebieten, sondern quer durch die Bank sein wird". Bedrohlich findet er das Szenario nicht: „Die Menschen werden wegen KI nicht untergehen. Sie werden nur nicht mehr so wichtig sein." Für den Philosophen Richard David Precht gefährlicher Unfug, vergleichbar dem transhumanistischen Credo, KI sei eine unabwendbare Stufe der Evolution. Profanes Ziel nahezu aller KI sei, „mehr Kontrolle zu gewinnen und größere Gewinne zu erwirtschaften; sei es durch Medizin- oder Militärtechnik, effizientere Produktion, geringere Kosten und eine noch bessere Kenntnis des Bürgers oder Kunden." KI dringe in viele Bereiche ein und errechne anhand statistischer Korrelationen Lösungen, für die sie keine Gründe nennt. Entscheidungen ohne nachvollziehbare Begründung sind zutiefst undemokratisch. Für ihn läuft der Trend deshalb entweder auf strenge Grenzen für den KI-Einsatz hinaus oder auf das Ende der Demokratie. Aus Verbrauchersicht eine von vielen einprägsamen, dystopischen Ermahnungen, den Einsatz von KI verantwortungsvoll abzustecken und Digitalisierung gemeinnützig auszurichten. ☐

EMPFEHLUNGEN

- ☐ Mit einem zwei-Klassen-Schutzniveau, das wichtige Bereiche des Verbraucheralltags unreguliert lässt, wird das Vertrauen der KonsumentInnen verspielt. Diese wünschen sich präventiven Schutz statt bloßer Schadenersatzansprüche.
- ☐ Was muss mir meine Bank offenlegen, wenn mir ihr Bonitätsalgorithmus keinen Kredit gewährt? Wofür sind Hersteller, Softwareproduzent oder Fahrer eines autonomen Fahrzeuges verantwortlich? Kann ich profilabhängige Empfehlungen auf Internetplattformen deaktivieren? Wo beschwere ich mich über intransparente, unfaire KI-Verfahren?

  Abgestufte, aber verbindliche Regeln sind für alle Risikoklassen erforderlich. Transparenz, Menschenrechte, Nichtdiskriminierung und niedrigschwellige Abwehrrechte müssen mehr als reine Lippenbekenntnisse in allen Bereichen sein, in denen KI ausprobiert wird,

sei es Arbeitswelt, Bildung, Finanzdienste, Gesundheit, Internet (der Dinge), Medien, öffentliche Sicherheit, Verkehr, Verwaltung u.v.m.

- ☐ Bezüglich der Analyse biometrischer Merkmale (wie Gesichtserkennungssoftware) stößt das Weißbuch eine Debatte an, statt ein Anwendungsverbot auszusprechen. Die EU-Kommission erntete zu Recht Kritik für ihr fehlendes Grundrechtsbewusstsein.
- ☐ Wenn Entwickler einräumen, dass sie ihre selbstlernende Software selbst nicht verstehen bzw. erklären können, überfordert die Beurteilung komplexer Algorithmen auch Aufsichtsbehörden. Alle Entscheidungen, die auf Algorithmen basieren, müssen deshalb erklär- und überprüfbar bleiben, vor allem in Hinblick auf unzulässige Diskriminierung, Benachteiligung, Verhaltensmanipulation oder Betrügereien. Behördlichen ex-Ante-Genehmigungen ist gegenüber nachträglichen Prüfungen im Schadensfall der Vorzug zu geben.
- ☐ Haftung muss eindeutig und abschreckend geregelt sein. KonsumentInnen dürfen bei einer Vielzahl an Beteiligten (Entwicklern, Herstellern, Anwendern, Dienstleistern) nicht zum Spielball unklarer Verantwortlichkeiten werden. Sie sollen im Sinne einer Solidarhaftung Unterlassungs- und Schadenersatzansprüche gegen jeden Beteiligten der Wertschöpfungskette richten können.

Weiterführende Literatur und Links

Weißbuch zu Künstlicher Intelligenz COM(2020) 65 final:
https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_de.pdf

Verbraucherpolitische Forderungen der BAK zu KI (2020): https://www.arbeiterkammer.at/kuenstliche-intelligenz

Datenschutz-Anliegender BAK anlässlich des zweijährigen Bestehens der DSGVO (2020):
https://www.akeuropa.eu/de/evaluation-der-datenschutz-grundverordnung-dsgvo

Position des europäischen Verbraucherverbands BEUC (2019/2020): http://www.beuc.eu/general/artificial-intelligence

Position des deutschen Verbraucherverbands VZBV (2019):
https://www.vzbv.de/dokument/faktenblatt-zu-kuenstlicher-intelligenz

Mitglieder der High-Level Expert Group on Artificial Intelligence der EU-Kommission:
https://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetail&groupID=3591

Auswahl kritischer Stimmen zu KI-Gesichtsanalysen:
https://algorithmwatch.org/story/polizei-gesichtserkennung-europa
https://privacyinternational.org/learn/facial-recognition
https://www.bitsoffreedom.nl/2020/01/29/facial-recognition-a-convenient-and-efficient-solution-looking-for-a-problem/

Googles KI Code of Conduct: https://deepmind.com/safety-and-ethics

Schmidhuber, Jürgen, Interview pwc next – das Magazin für Vorausdenker (3/2017);
https://next.pwc.de/2017-03/interview-schmidhuber.html

Precht, Richard David, Künstliche Intelligenz und der Sinn des Lebens, (2020) Goldmann V.

IMPRESSUM:

Herausgeberin und Medieninhaberin Kammer für Arbeiter und Angestellte für Wien, 1040 Wien, Prinz Eugen Strasse 20-22 · **Redaktion** Büro für Digitale Agenden · **Kontakt** arbeit.digital@akwien.at · **Verlags- und Herstellungsort** Wien · **DVR** 0063673 AKWien · **Grafik** Jakob Fielhauer · **Verlags- und Herstellungsort** Wien · **Offenlegung gem § 25 des Mediengesetzes** siehe wien.arbeiterkammer.at/offenlegung · **Blattlinie:** Die Meinungen der AutorInnen

Genug vom Fischen im Trüben?

A&W blog

awblog.at