KI Paper-Kurzversion mit Empfehlungen (Barbara Ferrarese):

Der Einfluss künstlicher Intelligenz auf menschliche Selbstbestimmung – Potenziale nutzen, Risiken minimieren

Forum Privatheit veröffentlicht neues Policy-Paper über Chancen und Risiken KI-basierter Technologien. Mit 15 Empfehlungen, wie die menschliche Selbstbestimmung trotz Künstlicher Intelligenz nicht nur erhalten, sondern sogar gefördert werden kann.

Im Gesundheitswesen kann Künstliche Intelligenz ein selbstbestimmtes Leben fördern
Es gibt verschiedene Bereiche, in denen KI-Technologien die menschliche Selbstbestimmung fördern kann. So kann der Einsatz von KI-Technologien im Gesundheitswesen die Diagnosemethoden erheblich verbessern. Menschen mit Seh- oder Hörbehinderungen können mit KI-Technologien die gesprochene Sprache in Texte umwandeln, Wahrnehmungseinschränkungen ausgleichen oder zumindest verbessern. Digitale Assistenzsysteme für Pflege und Gesundheit fördern ebenfalls ein selbstbestimmtes Leben, sowohl in der häuslichen Pflege als auch in Pflegeeinrichtungen. Menschen können zudem mehr Freiheit erlangen, indem sie lästige, gefährliche oder anderweitig unerwünschte Aufgaben an KI-Systeme abgeben. In diesen und anderen Bereichen wirkt sich KI positiv auf die Selbstbestimmung von Menschen aus.

Künstlich erzeugte Bilder, die täuschend echt wirken, können Sachverhalte verzerren
Doch neben positiven Einflüssen auf Selbstbestimmung können KI-Technologien auch einschränkend wirken. Vor allem die Herstellung synthetischer Medien hat sich in den letzten Jahren durch KI rasant weiterentwickelt. So sind selbstlernende Computersysteme mittlerweile in der Lage, täuschend echte Bilder, Texte, Audio-Dateien oder Videos synthetisch herzustellen. Dabei arbeiten zwei neuronalen Netze „gegeneinander“, von denen das erste ein künstliches Bild erstellt, während das zweite auf der Basis eines Trainingsdatensatzes mit „echten“ Bildern den „Realitätsgrad“ des artifiziellen Bildes beurteilt und optimiert. Am Ende erkennt man kaum noch, dass diese Produkte ein computergeneriert sind. Auf diese Weise können massenhaft synthetische Medien erzeugt und beispielsweise durch soziale Medien in Umlauf gebracht werden. Deren Zweck ist es häufig, Sachverhalte zu verzerren, Meinungen zu beeinflussen, Ängste und Konflikte zu schüren und politische Gegner zu diskreditieren. Diese Entwicklungen stellen ein Problem sowohl für den Wert der individuellen Selbstbestimmung als auch der kollektiven Selbstorganisation von Demokratien dar.

Das Verhalten von Menschen wird ausgelesen, um es dann zu beeinflussen
Dass KI-gestützte Massenbeeinflussung in der Praxis funktioniert, ist durch verschiedene Studien deutlich geworden. In einer Studie wurden beispielsweise mehr als drei Millionen Facebook-Nutzer*innen mit personalisierter Werbung angesprochen, die in Abhängigkeit von psychometrisch ermittelten Persönlichkeitseigenschaften individualisiert wurde. Bei Werbung, die auf das psychologische Profil, also etwa die gemessene Extra- oder Introvertiertheit einer Person abgestimmt war, ergab sich eine signifikant höhere Klick- und Kaufrate als bei nicht-individualisierter Werbung. Dass ein auf Gefühle oder Instinkte abzielendes „Micro-Targeting“ im großen Stil funktioniert, zeigen auch die Wahlbeeinflussungen der vergangenen Jahre, sei es in der Leave.EU-Kampagne in Großbritannien oder dem US-Wahlkampf der Republikanischen Partei 2016. Unternehmen wie Cambridge Analytica haben

sich auf diese Art der Wahlbeeinflussung spezialisiert. Maschinelles Lernen hilft bei der digitalen Psychografie, also der genauen Auslesung der Persönlichkeit eines Menschen. Wer diese kennt, kann Menschen manipulieren. Ängste, Schwächen oder Erwartungen können ausgenutzt werden. KI-gestütztes psychometrisches Vermessen von Persönlichkeiten und das daraufhin erfolgende Anpassen und Individualisieren von Marketingbotschaften oder Wahlkampfmotiven steht in fundamentalem Widerspruch zur Idee menschlicher Selbstbestimmtheit.

Algorithmen „entscheiden" über Kreditwürdigkeit und Bildungschancen von Menschen

Bereits Anfang der 2000er-Jahre wurde mit dem Begriff des „Social Sortings", also der „sozialen Sortierung" eine neue Qualität der digitalen Massenüberwachung beschrieben, bei der Menschen durch technische Verfahren in Reputations- oder Risikoklassen eingeteilt wurden. Während die technische Grundlage für das „Social Sorting" noch einfaches „Data-Mining", also „Daten schürfen bzw. Sammeln" war, werden heute zusätzlich Verfahren des maschinellen Lernens eingesetzt. Das „Social Sorting" wurde zum „Social Scoring" ausgebaut. Algorithmische Entscheidungssysteme vergeben Punktwerte für bestimmte Verhaltensweisen, die digital erfasst werden. Besonders problematisch ist dabei, dass diese Verfahren Ergebnisse produzieren, die lediglich wahrscheinliche Projektionen sind, aber nicht die Realität abbilden. Dennoch haben diese Projektionen für Menschen reale Folgen: Bonitäts-Scores, akademische Scores, Rückfälligkeits-Scores und derlei mehr beeinflussen - egal ob faktisch korrekt oder nicht - den Grad möglicher individueller Selbstbestimmung, sei dies im Hinblick auf finanzielle Freiheiten oder auch Bildungschancen. Datenschutzrechtlich gefasst und einem grundsätzlichen Verbot unterworfen sind dabei nur Entscheidungen, die ausschließlich auf einer automatisierten Verarbeitung personenbezogener Daten basieren. Nicht erfasst sind bisher jedoch jene Risiken, die durch eine teilautomatisierte Entscheidung bedingt sind, bei der zwar ein Mensch die finale Entscheidung trifft, dabei jedoch das Ergebnis der automatisierten Entscheidungsvorbereitung faktisch übernimmt und damit nur formal entscheidet. Hier bestehen rechtliche Schutzlücken, die geschlossen werden sollten.

Unternehmen nutzen KI für ihre Zwecke, ohne dass die betroffene Person davon weiß

Ein weiteres wesentliches Problem des Scorings ist seit jeher die Intransparenz des Verfahrens. Hier besteht ein Spannungsfeld zwischen Transparenzpflichten einerseits und dem Geheimhaltungs-interesse des Anbieters des Scoring-Algorithmus andererseits. Solche Algorithmen sind meist als Geschäftsgeheimnis geschützt. Beim Scoring auf Basis von künstlicher Intelligenz, welche die über einen Menschen gesammelten Daten weiterverarbeitet und für Prognosen nutzt, verschärft sich diese Problematik noch. Das Datenschutzrecht fordert gegenüber der betroffenen Person die Offenlegung „aussagekräftiger Informationen über die involvierte Logik". Wie dies gerade bei selbstlernenden Systemen, bei denen vielleicht nicht einmal die Programmierer*innen die Entstehung der Logik nachvollziehen können, realisiert werden kann, bleibt eine offene Frage.

Ausgelesen werden Gesichtsausdrücke, Gangarten oder Körpersprache

Künstliche Intelligenz bewirkt, dass aus „unverdächtigen" Datenspuren wie etwa der Nachverfolgung von Klicks oder Gesichtsabbildungen sehr persönliche und private Informationen über einen Menschen abgeleitet werden. Beispielsweise schließt KI von Gesichtsabbildungen in Verbindung mit Informationen über die jeweilige sexuelle Orientierung dieser Gesichter durch Verarbeitung von Trainingsdaten und Mustererkennung auf die wahrscheinliche sexuelle Orientierung von anderen Personen, von denen nur Gesichtsabbildungen vorliegen. Wenn mit solcher Technologie auf Aspekte wie Drogenkonsum, Beziehungsstatus, Intelligenzquotient, Persönlichkeitseigenschaften und vieles mehr probabilistisch „geschlossen" werden kann, stellt dies eine Gefahr für die Selbstbestimmung von Menschen dar, welche in bestimmten Fällen gerade auf das Nichtwissen von privaten Informationen bei Dritten angewiesen sind, etwa zum Schutz vor Diskriminierung.

Wer weiß, dass er beobachtet wird, verhält sich anders

Moderne KI-Technologien bieten darüber hinaus Analysemethoden, bei der nicht nur über tagtägliche Datenspuren, sondern über Eye-Tracking, über Gang- oder Körperspracheanalysen, über Gesichtsausdrücke oder andere physiologische Parameter auf interne Zustände oder intime Persönlichkeitseigenschaften eines Menschen geschlossen werden kann. Basierend auf diesen Technologien ist ein neuer Industriezweig erschlossen worden, der insbesondere durch Sicherheitstechnik Milliardenumsätze macht. Der Erfolg gerade von Gesichtserkennungstechnologien muss jedoch auf zwei Ebenen kritisch betrachtet werden: Zum bei der Beschneidung der Selbstbestimmung, die sich beim Einsatz von Gesichtserkennungstechnologien im öffentlichen Raum durch Selbstzensur-Effekte manifestiert: Wenn man glaubt, beobachtet zu werden, verhält man sich anders. Zum anderen müssen die Technologien methodisch hinterfragt werden. Denn die immer wieder getroffene Behauptung, man könne Emotionen technisch aus Gesichtsausdrücken oder -bewegungen auslesen, ist falsch. Der Link zwischen Gesichtsausdruck und Emotion ist weder spezifisch –derselbe Gesichtsausdruck verweist nicht zuverlässig auf dieselbe Emotion –noch zuverlässig – dieselben Emotionen werden nicht immer durch denselben Gesichtsausdruck angedeutet – oder generalisierbar – es gibt je nach Kontext und Kultur Unterschiede in bestimmten Gesichtsmimiken. In der Emotionspsychologie wird darüber hinaus bereits seit Jahrzehnten auf Basis empirischer Studien debattiert, ob Emotionen und Mimik überhaupt „hartverdrahtet“ verbunden sind oder ob Mimik sich nicht vielmehr nach der sozialen Situation richtet. Diese Feststellung sollte den Einsatzbereich und die Leistungsversprechungen von Gesichtserkennungssoftware stark einschränken bzw. relativieren. Vor allem in Bezug auf die Selbstbestimmung ist dabei relevant, dass die Gefahr falscher Schlüsse wächst, wenn von falschen Voraussetzungen und wissenschaftlich nicht abgesicherten psychologischen Vorstellungen ausgegangen wird.

Fazit und Empfehlungen

Bei allen Technologien liegen Chancen und Risiken dicht beieinander. Erstere gilt es zu fördern, letztere zu minimieren; so auch bei KI-Anwendungen. Das Policy-Paper gibt Empfehlungen, die sich auf die Erhaltung der menschlichen Selbstbestimmung konzentrieren und die sowohl die Selbstbestimmung des Individuums sowie als auch die Selbstbestimmung der Gesellschaft zum Ziel haben.

1.) Algorithmische Entscheidungssysteme sollten demokratisch festgelegten Fairnesskriterien entsprechen. Das Zustandekommen algorithmischer Entscheidungen sollte beispielsweise so transparent und nachvollziehbar wie möglich erklärt werden.
2.) Je größer der Schädigungspotenzial einer KI, desto stärker muss reguliert werden, bzw. muss der Gesetzgeber Schutzmechanismen einbauen, die dieses Schädigungspotenzial verringern.
3.) Darüber hinaus soll auch zivilgesellschaftlichen Initiativen Raum für Ko- und Selbstregulierung gegeben werden.
4.) Verlagerung der Verantwortlichkeit für die Risiken von KI hin zu den Produkt-bzw. Technologieherstellen. Ähnlich wie im Aufsichtssystem der DSGVO wären dann die Unternehmen in der Pflicht, eine erste interne Folgenabschätzung ihrer Systeme vorzunehmen.
5.) Etablierung einer Beratung durch die Aufsichtsstellen
6.) Nichtstaatliche Initiativen als Interessenvertreter zur Überwachung und Kontrolle von KI: Verbraucherschutzorganisationen, Gewerkschaften, (Dach-)Verbände und Berufsvereinigungen sollten die Möglichkeit erhalten, für ihre Gruppe oder ihren Sektor Prüfkriterien und Verhaltensregeln festzulegen.
7.) Das Recht muss die technische Entwicklung von KI kritisch begleiten. Zentrale Frage ist dabei, wie grundrechtlich geschützte Positionen eine konkrete technische Umsetzung erfahren können. Dies ist umso wichtiger, wenn künstliche Intelligenz durch staatliche Stellen zum Einsatz kommen sollte. Spätestens dann muss ein diskriminierungsfreier und die Selbstbestimmung der Bürger*innen wahrender Einsatz sicher gewährleistet werden. Eine besondere Rolle spielt dabei das Verbot, dass staatliche Stellen keinesfalls teilweise oder weitgehend vollständige Persönlichkeitsbilder der Bürger*innen erzeugen dürfen, denn die gänzliche oder teilweise

Registrierung und Katalogisierung der Persönlichkeit stellt einen nicht zu rechtfertigenden Eingriff in die Würde des Menschen dar.

8.) Um den Gestaltungs- und Regelungsbedarf von KI zu eruieren, muss zunächst für jeden Anwendungsbereich bestimmt werden, wie KI die Selbstbestimmung verändert, beeinflusst, einschränkt oder aber erweitert. Gleichzeitig müssen alle anderen verfassungsrechtlich verbrieften Rechte gewährleistet werden.

9.) Vor allem muss sichergestellt sein, dass die betroffenen Personen durch den Einsatz von KI nicht diskriminiert werden, was bereits die Verwendung möglichst diskriminierungsfreier Trainingsdaten erfordert.

10.) KI muss letztlich so gestaltet sein, dass die betroffene Person auch beim Einsatz der KI selbstbestimmt entscheiden kann, ob und welche personenbezogenen Daten verarbeitet werden und ihre Betroffenenrechte geltend machen kann. Ist dies nicht gewährleistet, würde die Person zum bloßen Datenobjekt degradiert. Hierfür müssen verschiedene Grundsätze des Datenschutzes beachtet werden: Der Zweckbindungsgrundsatz, der Grundsatz der Datensparsamkeit, Datenschutz durch Technikgestaltung sowie datenschutzfreundliche Voreinstellungen.

11.) Die Transparenz und Nachvollziehbarkeit algorithmischer Entscheidungen muss gewährleistet werden.

12.) Es sind Ansätze zur kollektiven Beteiligung an der Gestaltung von KI zu entwickeln: Die KI-Gestaltung unterliegt in der Regel ausschließlich dem Bedarf der Datenökonomie. Verbraucher*innen dienen vor allem der Bereitstellung von Trainingsdaten (oft unbewusst und unfreiwillig). Um eine demokratisch gehaltvolle Selbstbestimmung zu ermöglichen, sind indes Ansätze notwendig, welche die kritischen Bewertungskompetenzen von Verbraucher*innen bei der Entwicklung von KI und ihrer Nutzung nicht nur erhalten, sondern auch zielgerichtet fördern.

13.) Weiterhin gibt es einen Bedarf an institutionellen Rahmenbedingungen, damit eine gesellschaftsweite Problematisierung darüber, wie KI zum Wohl der Gesellschaft genutzt werden kann, möglich ist. Hierzu ist eine Stärkung von Datenschutzbehörden oder Verbraucherschutzorganisationen notwendig, die unabhängige Kontrollen durchführen, Zertifikate für vertrauenswürdige KI vergeben und die Öffentlichkeit über Normverstöße in Kenntnis setzen.

14.) Professionsethische Selbstverpflichtungen für KI-Entwickler*innen gewährleisten

15.) Vertraulichkeit sicherstellen mittels technischer und organisatorischer Maßnahmen

Hier finden Sie die ausführliche Version des Papers Risiken künstlicher Intelligenz für die menschliche Selbstbestimmung.