Einleitung: Künstliche Intelligenz, Demokratie und Privatheit

Michael Friedewald und Alexander Roßnagel

Zum Thema dieses Bandes

Die digitale Transformation von Gesellschaften weltweit hat in den letzten Jahren nicht nur weiter an Dynamik gewonnen, sondern auch immer deutlicher spürbar globale Wirkungs- und Problemzusammenhänge ausgebildet. Heute sind es vor allem allgegenwärtige Systeme der Künstlichen Intelligenz (KI), die im Zentrum des wissenschaftlichen, politischen, ökonomischen, normativen und regulatorischen Interesses stehen. Von besonderer Bedeutung sind hier algorithmische Datenauswertungen zur Steuerung wirtschaftlichen und gesellschaftlichen Verhaltens, die eine Bedeutung für die politische Entscheidungsfindung und die Strukturierung öffentlicher Kommunikation haben und so die Lebenswirklichkeit der Bürgerinnen und Bürger mitgestalten.

Die heute diskutierten KI-Systemen sind überwiegend Vertreter der so genannten „schwachen KI", bei der es darum geht, einzelne kognitive Fähigkeiten, vor allem Erkennen und Klassifizieren innerhalb eines engen Aufgabenbereichs in einem Computersystem nachzubilden. Eine solche Nachbildung bestimmter, als „intelligent" bezeichneter Funktionen umfasst aber kein Verständnis für die dahinterliegenden Konzepte. Die dazu heute meist genutzten Verfahren sind statistischer bzw. probabilistischer Natur, die auf einer Modellierung des betrachteten Problems basieren und weitgehend nicht durch einfache Regeln erklärt werden können. Zur Erstellung der Modelle und das „Training" der Funktionalität werden in der Regel große Datenbestände benötigt, so dass die Voraussagen, Klassifizierungen oder Entscheidungen einer KI höchstens so gut sein können wie die Qualität der „Trainingsdaten". Solche, auf „maschinellem Lernen" basierende Anwendungen haben in den letzten Jahren erheblich an (technischer) Reife gewonnen.

Unternehmen und Politik betrachten KI seit einigen Jahren als so genannte Schlüsseltechnologie und hegen hohe Erwartungen an die Möglichkeiten der ökonomischen Verwertung und administrativen Nutzung

zu Zwecken des Gemeinwohls.[1] Andere warnen eher vor den disruptiven ökonomischen Effekten und den unintendierten Folgen dieser gar nicht mehr so neuen Technologie für Gesellschaft und Demokratie. Auf der nationalstaatlichen Regulierungsebene ist es nach wie vor schwierig, die damit einhergehenden Herausforderungen in den Griff zu bekommen. Unter dem Eindruck einer „überwachungskapitalistischen" Implementierung von KI-Systemen einerseits und „überwachungsstaatlichen" Verwendung solcher Systeme andererseits stehen Selbstbestimmung und Privatheit als Grundwerte der demokratischen Gesellschaft einmal mehr vor einer Bewährungsprobe. Auch die Meinung in der deutschen Bevölkerung bildet diese beiden Pole ab. Laut einer Umfrage des Branchenverbands BITKOM aus dem Jahr 2021 betrachten über 70 % der deutschen Bürgerinnen und Bürger KI vor allem als Chance, während immerhin fast 30 % die Risiken überwiegen sieht.[2]

Die mit der KI entstehenden Formen der Datafizierung ändern nicht nur die zum Schutz von Privatheit und Selbstbestimmung erforderlichen Konzepte, sondern stellen auch das Verständnis und den Stellenwert von Privatheit und Selbstbestimmung selbst in Frage. Bislang wurde ihr Wert meist so begründet, dass Privatheit und Selbstbestimmung den Einzelnen vor illegitimer Beobachtung, Einflussnahme und Fremdbestimmung schützen und dadurch eine Grundlage für individuelle Autonomie, Selbstverwirklichung sowie freie Meinungs- und Willensbildung bieten soll.

Negative Einflüsse wurden entsprechend an überwachend oder „manipulativ" wirkenden Technologien festgemacht. Verwiesen sei an dieser Stelle auf Schlagworte wie „Gesichtserkennung", „intelligente Videoüberwachung", „Big Nudging", „Micro Targeting", „Predictive Policing" und ähnliche Nutzungsformen der KI. Tatsächlich bringen derartige Technologien und die damit einhergehenden Datenverarbeitungen in zunehmendem Maße neue, auch gruppenbezogene und gesamtgesellschaftliche Risiken mit sich. Während beispielsweise die von einer personenbezogenen Datenverarbeitung konkret Betroffenen immerhin verschiedene rechtliche Möglichkeiten zur Durchsetzung ihrer Rechte offenstehen, können sich die Mitglieder einer algorithmisch generierten Gruppe weder über ihre Zughörigkeit zu dieser Gruppe noch über die sie persönlich betreffenden Auswirkungen im Klaren sein. Möglich wird eine solche Zuordnung,

1 Vgl. z.B. die KI-Strategie der Bundesregierung. https://www.ki-strategie-deutschland.de/home.html.

2 https://www.bitkom.org/Presse/Presseinformation/Kuenstliche-Intelligenz-als-Chance (zuletzt zugegriffen: 06.07.2022)

wenn Datenverarbeitungen zunächst auf konkret zu einer natürlichen Person zuordenbare Daten verzichten und stattdessen nicht-personenbezogene Daten (bestimmte Nutzungs- oder Verhaltensweisen bzw. Attribute) als Bezugspunkt nehmen. Durch einen solche Verarbeitung der Daten werden etwa aus Surfgewohnheiten einzelner Individuen Informationen gewonnen, die in der Folge dann zur Personalisierung von Werbung oder Newsfeeds eingesetzt werden können. Indem derartige Verfahren oft jenseits etablierter Schutzkonzepte operieren, weil statistische Verfahren häufig nicht mit „personenbezogener Daten" im datenschutzrechtlichen Sinne arbeiten, laufen die Regelungen des Datenschutzes ins Leere. Künstliche Intelligenz ermöglicht so nicht nur algorithmengestützte Entscheidungen, die zur Steuerung und Organisation sozialer Systeme verwendet werden, sondern auch die Extraktion „emergenter", privater Informationen aus „unverdächtigen" Datensätzen.

Ein anderes Beispiel möglicher gesellschaftlicher Auswirkungen der KI: Wird KI auch zur Entwicklung von Social Bots genutzt, damit diese computergenerierten virtuellen Gesprächspartner möglichst menschenähnlich auftreten, kann dies die Auseinandersetzung über politische Meinungen oder soziale Haltungen wesentlich verändern. Während der Einsatz von Social Bots im Falle der Beantwortung einfacher Kundenfragen noch sinnvoll erscheint, ermöglicht dieselbe Technologie, den Diskussionsteilnehmer in politischen Auseinandersetzungen vorzugaukeln, dass reale Menschen eine bestimmte Meinung vertreten. Indem Bots in Posts oder ähnlichen Äußerungen Zustimmung oder Ablehnung zu einem Vorschlag oder einer Haltung zum Ausdruck bringen, können sie im demokratischen Diskurs Mehrheiten verändern oder bestimmten Meinungen „zum Durchbruch verhelfen". Auf diese Weise kann mit ihrer Hilfe der Effekt ausgenutzt werden, dass viele Menschen Teil der Mehrheit sein wollen und daher der von Bots vertretenen Meinung zustimmen. Mittels des Einsatzes von „Bot-Armeen" sind auf diese Weise sogar großflächige Meinungsmanipulationen möglich.

In diesem Zusammenhang ist auch die für Gesellschaft und Individuen ausgehende und zunehmende Gefahr von Deepfakes und vergleichbaren manipulativen Verfahren einzuordnen. Mittels spezieller künstlicher neuronaler Netzwerke (so genannte „generative adervsarial networks") ist es heute bereits möglich, authentisch wirkende Fälschungen von (Bewegt-)Bild- und Audiomaterial zu generieren. Mittels der auf diese Weise generierten Deepfakes können sich für Individuen Konsequenzen für ihre Privatsphäre entfalten, die sich derzeit insbesondere in Form von Rachepornographie äußern. Die möglichen Verletzungen gesellschaftlicher Werte reichen allerdings weit über das Individuum hinaus, wenn sie bei-

spielsweise zur Manipulation und Irritation politischer Prozesse verwendet werden – wie etwa die gefälschten Anrufe des Kiewer Bürgermeisters Vitali Klitschko bei europäischen Politikern im Juni 2022 gezeigt haben.

Alle diese Technologien können zu einer Gefahr für demokratische Werte werden, wenn etwa Filterblasen zur übermäßigen Verbreitung von Miss- oder Desinformation sowie zu Radikalisierungstendenzen im öffentlichen Diskurs beitragen. Illegitime Informationsbestände, die jedoch eine besonders hohe Popularität unter den Nutzenden sozialer Netzwerke genießen, entfalten häufig eine stärkere Wirkung als Richtigstellungen oder differenzierte und ausgewogene Informationsbestände. Indem Algorithmen die Aussendung von Inhalten steuern, können sie derartige soziale Verhaltensweisen bestärken und zu einer Verschärfung des Problems führen.

Solche Praktiken adressieren in der Regel alle Bevölkerungsgruppen. Es muss aber berücksichtigt werden, dass die Folgen für die Selbstbestimmung aufgrund unterschiedlicher individueller Voraussetzungen für unterschiedliche gesellschaftliche Gruppen verschieden sein können. So ist davon auszugehen, dass es sich etwa bei Kindern und Jugendlichen oder bei älteren Personen um Gruppen handelt, die gegenüber ausforschenden und verhaltenssteuernden Technologien besonders verletzlich sind, da sie auf anderen Kompetenzniveaus agieren, als Gruppen mit höherer „digital literacy". Die Fähigkeiten, Kenntnisse oder Mittel, die diesen Gruppen zum wirksamen Schutz ihrer informationellen Selbstbestimmung zu Verfügung stehen, müssen daher anders bewertet, gefördert und kollektiv abgestützt werden als im Falle der übrigen Gesellschaftsmitglieder. Darüber hinaus ist auch zu berücksichtigen, dass sich Menschen und ihr Umfeld über ihre Lebensspanne erheblich ändern und damit auch die Aussagekraft der über sie gesammelten Daten.

Die aus der Tagung des „Forum Privatheit" im November 2021 hervorgegangenen und in diesem Band gesammelten Beiträge drehen sich entsprechend um die Frage, welche Auswirkungen „Künstliche Intelligenz" auf Privatheit, auf das Recht auf informationelle Selbstbestimmung und auf demokratische Strukturen und Prozesse haben kann und wie diese zu bewerten sind. Darauf aufbauend wird thematisiert, mit welchen Mitteln – von der Regulierung über ökonomische Anreize und soziale Praktiken bis zur Technikgestaltung – auf diese Herausforderungen reagiert werden kann, um eine zukunftsgerechte Gewährleistung von Selbstbestimmung und demokratischer Teilhabe zu gewährleisten.