KI als neues Wahlkampfinstrument

Offene Flanke der KI-Regulierung?

Lennart Laude & Andreas Daum

03.05.2024 doi: 10.59704/9e96c5f69bbfa94c

KI-Systeme werden auch in Deutschland verstärkt zur Erzeugung von politischen Inhalten verwendet. Politische Parteien nutzen die Fähigkeiten Künstlicher Intelligenz, um unwahre Inhalte über den politischen Gegner zu generieren und zu verbreiten. Eine Überprüfung zeigt, dass die neue europäische Digitalregulierung nicht auf politische Sachverhalte zugeschnitten ist. Insbesondere erfasst die verabschiedete KI-Verordnung eher wirtschaftliche Risiken als solche für den demokratischen Prozess. Dabei haben manche Parteien mit den von ihnen verbreiteten KI-Inhalten schon jetzt allgemeine verfassungsrechtliche Vorgaben klar verletzt. Angesichts der rasanten technischen Entwicklung ist eine zeitnahe Schaffung spezifischer Regeln für den KI-Einsatz im demokratischen Prozess notwendig.

Fakes ohne Grenzen

Der Oppositionsführer im britischen Unterhaus, Keir Starmer, war im Oktober 2023 Leidtragender des „ersten Deepfake Moments“ im Vereinigten Königreich. Ein KI-generiertes Video zeigte den Labour-Chef vermeintlich pöbelnd gegenüber Mitarbeitern. Eine Klarstellung konnte die Wirkungen nicht einfangen: Binnen weniger Tage hatte der Deepfake Millionen Aufrufe erzielt. Für den demokratischen Prozess stellt sich die grundsätzliche Frage, inwieweit Parteien, Politiker und Amtsträger zukünftig KI-Systeme zur Kommunikation mit dem Volk verwenden dürfen. Es überrascht wenig, dass die AfD in Deutschland als erste Partei die Grenzen des technisch und rechtlich Möglichen erprobt. In ihrem „Ampel-Adventskalender“ konnten täglich Äußerungen von Mitgliedern der Ampelregierung abgerufen werden – vermeintlich. Tatsächlich wurden Deepfake-Stimmen u.a. von Olaf Scholz, Annalena Baerbock und Friedrich Merz präsentiert – (natürlich) ohne jegliche Hinweise auf die Herkunft und auf den unwahren Charakter der Inhalte. Auch die FDP-Fraktion im nordrhein-westfälischen Landtag offenbarte ein sehr liberales Verständnis KI-basierter politischer Kommunikation, als sie – wiederum ohne jegliche Hinweise – ein gefälschtes Bild von Ministerpräsident Wüst verbreitete.

Es wäre leicht, diese Deepfakes als Spielerei oder übliche Härte des politischen Wettbewerbs abzutun. Diese Sicht ignoriert indes, dass die Auswirkungen und Gefahren für die Demokratie mindestens unklar sind. Angesichts der beständig festgestellten schwachen Medienkompetenz der Deutschen kann nicht darauf vertraut werden, dass KI-basierte Falschkommunikation als solche erkannt wird. Auch ist nicht absehbar, wie ungleich bessere KI-Systeme zukünftig wirken könnten.

Lücken der KI-Verordnung

Bei der Frage nach den rechtlichen Grenzen KI-basierter politischer Kommunikation und Mechanismen zu ihrer Überprüfung liegt zuerst der Blick nach Brüssel nahe, wo das Europäische Parlament Mitte März der KI-Verordnung (AI Act) zustimmte. Das Ziel der Verordnung ist die Förderung von „menschenzentrierter und vertrauenswürdiger künstlicher Intelligenz“ sowie die Etablierung eines „hohen Schutzniveaus in Bezug auf […] Grundrechte, Demokratie [und] Rechtsstaatlichkeit“ (vgl. Erwägungsgrund 1).

Der Gesetzgeber legt die Messlatte hoch: Die Verordnung verfolgt den Anspruch, die zentralen Risiken und Herausforderungen, die Künstliche Intelligenz für Staat und Gesellschaft mit sich bringt angemessen zu adressieren – und geht damit weit über die bisherigen Vorgaben des Produktsicherheitsrechts hinaus. Allerdings zeigt gerade das Beispiel der KI-generierten

politischen Kommunikation, dass die neue Verordnung den hohen Ansprüchen nicht gerecht werden kann.

Parteien oder andere politische Akteure erwähnt die KI-Verordnung mit keinem Wort. Die Anwendung der KI-Verordnung auf die Parteien ergibt sich aus deren weit gefassten Begriffsdefinitionen. Als „Betreiber" gilt etwa jede *„natürliche oder juristische Person, Behörde, Einrichtung oder sonstige Stelle, die ein KI-System in eigener Verantwortung verwendet"* (vgl. Art. 3 Nr. 4 KI-Verordnung). Als „Einrichtungen" oder „sonstige Stellen" können somit auch politische Parteien als „Betreiber" im Sinne der KI-Verordnung gelten, wenn sie ein KI-System nutzen. Die Verwendung in eigener Verantwortung setzt keinen technischen Betrieb auf eigenen Servern voraus. Es reicht aus, dass der Betreiber ein KI-System auf fremder Infrastruktur für eigene Zwecke einsetzt.

Die KI-Verordnung verfolgt einen „risikobasierten Ansatz", in dem Art und Inhalt der geltenden Pflichten sich nach der Intensität und dem Umfang der Risiken, die von dem jeweiligen KI-System ausgehen, richten. Daher sieht die KI-Verordnung erhöhte Pflichten für die Anbieter von „Hochrisiko-KI-Systemen" (Art. 6 ff.) vor. Die Betroffenen müssen unter anderen spezielle Risikomanagement- und Dokumentationssysteme vorhalten. Als solche besonderen Algorithmen gelten auch „KI-Systeme, die *bestimmungsgemäß* verwendet werden sollen, um das Ergebnis einer Wahl oder das Wahlverhalten zu beeinflussen", (vgl. Art. 6 Abs. 2, Anhang III Nr. 8 KI-Verordnung). Dieser Tatbestand ist jedoch nur einschlägig, wenn das KI-System gerade nach der Bestimmung des Anbieters dazu verwendet werden „soll", das Wahlverhalten zu beeinflussen. Als Anbieter gelten diejenigen Personen, die ein KI-System entwickeln (lassen), in Verkehr bringen oder Betreibern bereitstellen (vgl. Art. 3 Nr. 3 KI-Verordnung), jedoch nicht die Betreiber, die das KI-System lediglich in eigener Verantwortung verwenden (vgl. Art. 3 Nr. 4 KI-Verordnung). Ein „Hochrisiko-KI-System" zur Beeinflussung des Wahlverhaltens läge also (nur) vor, wenn eine Partei ein gänzlich neues KI-System entwickelt, um eine Wahl zu ihren Gunsten zu beeinflussen – etwa durch die automatisierte Verbreitung des Wahlprogramms.

Diese eng gefasste Bestimmung von Hochrisiko-KI dürfte an der Realität der KI-Verwendung durch Parteien vorbeigehen: Die Verantwortlichen der Parteien werden regelmäßig keine eigenen KI-Systeme entwickeln, sondern über das Internet auf (kommerziell) verfügbare KI-Anwendungen wie ChatGPT, Gemini, DallE3 oder Midjourney zugreifen. Bei Zugriff auf diese von Dritten in den Verkehr gebrachten KI-Systeme agieren Parteien lediglich als Betreiber im Sinne der KI-Verordnung. Die strengen Anforderungen an die Anbieter von Hochrisiko-KI-Systeme finden auf die Parteien keine Anwendung.

Die KI-Verordnung kategorisiert die genannten Anwendungen als „KI-Modelle mit allgemeinem Verwendungszweck" und sieht für deren Anbieter (nicht jedoch deren Betreiber) spezielle Regelungen vor (vgl. Art. 3 Nr. 63, Nr. 66, Art. 53 ff. KI-Verordnung).

Kennzeichnungspflichten für KI-Inhalte und Deepfakes

Das wichtigste Instrument für die Regulierung von KI-basierter Kommunikation im politischen Bereich wird daher wohl die Kennzeichnungspflicht zu KI-Inhalten nach Art. 50 KI-Verordnung sein. Eine Analyse zeigt, dass genau an dieser Stelle erhebliche Unklarheiten in der Konkretisierung und Durchsetzung der Pflichten bestehen.

Eine zentrale Vorgabe ist Art. 50 Abs. 4 KI-Verordnung, nach dem die Betreiber eines KI-Systems, *„das Bild-, Ton- oder Videoinhalte erzeugt oder manipuliert, die ein Deepfake sind"*, offenlegen müssen, dass die Inhalte künstlich erzeugt oder manipuliert wurden. Die scheinbar einfache wie klare Regelung hat jedoch deutliche Schwächen. Zunächst weist die gesetzliche Definition des „Deepfakes" starke subjektive Elemente auf. Nach Art. 3 Abs. 60 KI-Verordnung kommt es darauf an, dass der Bild-, Ton- oder Videoinhalt einer Person fälschlicherweise als echt oder wahrheitsgemäß erscheinen würde. Bei Wahrnehmenden wird in Abhängigkeit von Alter, Sozialisierung und digitaler Affinität die Beurteilung von falschen KI-Inhalten jedoch vielfach unterschiedlich ausfallen. Die Definition des „Deepfakes" vermittelt eine vermeintliche Objektivität, die in einem diversen Publikum nicht besteht. Darüber hinaus präsentiert die KI-Verordnung

ein Schlupfloch für einen böswilligen Betreiber, der falsche politische KI-Inhalte verbreiten will: Soweit der Inhalt nach Art. 50 Abs. 4 S. 3 KI-Verordnung *„Teil eines offensichtlich künstlerischen, kreativen, satirischen, fiktionalen analogen Werks oder Programms*“ ist, beschränken sich die Transparenzpflichten darauf, dass Betreiber auf den Ursprung der Inhalte in geeigneter Weise hinweisen, *„die die Darstellung oder den Genuss des Werks nicht beeinträchtigt*.“ Es braucht nicht viel Fantasie, dass vor allem Parteien sich auf den bereits viel bemühten satirischen Zweck der falschen KI-Inhalte berufen werden und den Hinweis auf den „künstlichen“ Ursprung des Inhalts kaum wahrnehmbar platzieren.

Keine ausreichende Verzahnung von KI-Verordnung und DSA

Überdies ist der Durchsetzungsmechanismus für die Kennzeichnungsregeln des Art. 50 Abs. 2, Abs. 4 KI-Verordnung unklar. Sind ungekennzeichnete KI-Inhalte im Einzelfall als rechtswidrig zu entfernen, wenn sie in einer Online-Plattform verbreitet werden? Naheliegend wäre, hier eine Verzahnung zwischen der KI-Verordnung und dem Digital Services Act (DSA) als zentralem Baustein der europäischen Plattformregulierung zu schaffen. Nach Art. 16 ff. DSA müssen Hostingdienste und Online-Plattformen ein Notice-und-takedown-Verfahren implementieren, mit dem rechtswidrige Inhalte gemeldet und entfernt werden.

Genau diese Kopplung seiner Regulierungsinstrumente will der Unionsgesetzgeber aber scheinbar vermeiden. So bestimmt Erwägungsgrund 136 KI-Verordnung explizit, dass die fehlende Kennzeichnung die Bewertung der Rechtswidrigkeit von Inhalten nicht berühren soll (*without prejudice*). Die Bewertung der Rechtswidrigkeit von KI-Inhalten soll allein unter Bezugnahme auf die Regelungen zum Äußerungsinhalt erfolgen. Wenngleich angesichts der Bedeutung des Grundrechts der freien Meinungsäußerung (Art. 11 GRCh) eine vorschnelle Löschung von Inhalten vermieden werden muss, wird hierdurch das Vorgehen gegen KI-Inhalte insgesamt erschwert. Bei Verwendung von KI-Systemen können in Sekundenschnelle Inhalte generiert und in Online-Plattformen verbreitet werden. Ist trotz fehlender Kennzeichnung eine Einzelfallprüfung der Rechtswidrigkeit notwendig, kann während der Dauer dieser Prüfung bereits irreversibler Schaden entstanden sein. Das oben zitierte Beispiel zu Keir Starmer zeigt, dass eine ex post- Benennung eines Deepfakes keine effektive Lösung darstellt, wenn der Inhalt zuvor millionenfach rezipiert wurde.

Im Ergebnis zeigt sich, dass die europäische Digitalregulierung das Problem politisch eingesetzter Deepfakes und massenhaft verbreiteter KI-Inhalte nicht hinreichend aufnimmt. Die Regelungen der KI-Verordnung, speziell für Hochrisiko-KI-Systeme und solche mit allgemeinem Verwendungszweck, regeln primär deren kommerzielle Verwendung. Der sensible politischen Bereich wird durch die insoweit wirtschaftlich ausgerichtete KI-Verordnung nur am Rande und eher beiläufig miterfasst. Spezifische Mechanismen zur Entfernung massenhaft verbreiteter, nicht gekennzeichneter KI-Inhalte bestehen nicht.

Die kommunikative Rolle der Parteien unter dem Grundgesetz

Welche Möglichkeiten bleiben von KI-basierter Kommunikation betroffenen Parteien angesichts fehlender spezifischer (unionsrechtlicher) Mechanismen? Wenngleich die regulatorische Wirkung des Verfassungsrechts für technische Fragestellungen regelmäßig überschaubar ist, lassen sich dem Grundgesetz an dieser Stelle wesentliche Vorgaben entnehmen. Wendet man es auf die o.g. Beispiele der AfD und FDP an, zeigt sich, dass ihre KI-basierte Kommunikation im verfassungswidrigen Bereich liegt.

Dem Grundgesetz liegt eine Vorstellung des demokratischen Prozesses zugrunde, in dem den Parteien als Mittler zwischen Staat und Gesellschaft agieren. Sie sollen und müssen in dieser durch Art. 21 Abs. 1 ausgeformten Mittlerfunktion versuchen, die Meinungsbildung der Wähler zu beeinflussen. Im Grundsatz sind Parteien beim Verbreiten ihrer Meinungen daher durch die Meinungsfreiheit des Art. 5 Abs. 1 Satz 1 GG (über Art. 19 Abs. 3 GG) geschützt. Anders als Staatsorgane sind Parteien dabei nicht zur Neutralität verpflichtet. So sind inhaltliche Zuspitzungen wie die Aussage, die CSU sei die „NPD von

Europa“, trotz der darin enthaltenen tatsächlichen Elemente insgesamt als Werturteil eingeordnet und dem Schutzbereich von Art. 5 Abs. 1 GG zugeordnet worden.

Der verfassungsrechtliche Favor hat jedoch Grenzen, soweit die Verantwortlichen der Parteien bewusst unrichtig kommunizieren. Wird ein Sachverhalt nicht vereinfacht, sondern im Kern falsch dargestellt, können sich Parteien nicht darauf zurückziehen, eine Äußerung sei nur polemisch überzogen. Sobald Parteien mithilfe von KI-Systemen vermeintliche Aussagen des politischen Gegners erzeugen, handelt es sich um nachweislich unwahre Information – nämlich dergestalt, dass sich der Gegner in der verbreiteten Form tatsächlich geäußert habe. Die Verbreitung einer unrichtigen Information kann ungeachtet der Motive und des genutzten Forums im Wahlkampf nichts zum Meinungsbildungsprozess beitragen.

Die Parteien haben im Rahmen ihrer durch Art. 21 Abs. 1 GG bestimmten Aufgabe die Pflicht, auf die Mitteilung richtiger Informationen zu achten. Sobald sie falsche KI-Inhalte verbreiten, verletzen sie ihren Auftrag zur Förderung des demokratischen Willensbildungsprozesses. Die Verbreitung dieser Inhalte ist nicht vom Schutzbereich der Meinungsfreiheit umfasst.

Prozessuale Geltendmachung

Wenngleich KI-basierte politische Kommunikation (soweit ersichtlich) noch nicht Gegenstand gerichtlicher Verfahren gewesen ist, können verfassungs- und verwaltungsgerichtliche Verfahren eine Möglichkeit zur Überprüfung der beschriebenen Grenzen darstellen. Zunächst können betroffene Personen unmittelbar eine Verletzung ihres Persönlichkeitsrechts geltend machen. Daneben dürfen Fraktionen – in den o.g. Beispielen der AfD und FDP – nach den Maßstäben des öffentlich-rechtlichen Äußerungsrechts nicht bewusst Unwahrheiten verbreiten und haben Sachlichkeitsanforderungen zu beachten. Die Verbreitung KI-basierter Falschinformationen verstößt gegen diese Sachlichkeitsanforderungen und kann einen rechtswidrigen Eingriff in die Chancengleichheit anderer Parteien darstellen. Für die Informationstätigkeit von Fraktionen ist richtigerweise der Verwaltungsrechtsweg eröffnet (Mast in Conrad et al, Handbuch öffentlich-rechtliches Äußerungsrecht, § 6 Rn. 68 ff.). Insoweit könnten in den o.g. Beispielen die betroffenen Fraktionen die KI-basierte Kommunikation verwaltungsgerichtlich prüfen lassen.

Notwendigkeit einer politischen Komponente der KI-Regulierung

Mit Anwendbarkeit der KI-Verordnung – uneingeschränkt (erst) 24 Monate nach Inkrafttreten – wird die Digitalregulierung der EU auch die Verwendung von KI-Systemen erfassen. Nach aktuellem Stand erfasst der risikobasierte Ansatz wirtschaftliche Fragen stärker als den Schutz des demokratischen Prozesses. Insbesondere erschwert die fehlende Verzahnung mit dem DSA die Prüfung (rechtswidriger) KI-Inhalte. Es bedarf spezifischer Mechanismen zur Regulierung der KI-Verwendung im demokratischen Prozess. Unionsrechtlich wird etwa die Möglichkeit bestehen, durch Leitlinien etwa nach Art. 6 (5) KI-Verordnung die Risiken im demokratischen Prozess zu konkretisieren. Auf nationaler Ebene sind Regelungen für Parteien und Fraktionen, etwa im PartG, zu erwägen. Nach ersten Beobachtungen scheint ohne klare rechtliche Vorgaben jedenfalls für einige Parteien das Täuschungspotenzial von KI interessanter als eine transparente Verwendung dieses neuen Wahlkampfinstruments.

AUTOR*INNEN

Lennart Laude
Lennart Laude ist Rechtsanwalt bei Noerr in München und wissenschaftlicher Mitarbeiter im Justiz-Projekt des Verfassungsblogs.
Andreas Daum

EMPFOHLENE ZITATION

Laude, Lennart; Daum, Andreas: KI als neues Wahlkampfinstrument: Offene Flanke der KI-Regulierung?, Verfassungsblog, 03.05.2024, doi: 10.59704/9e96c5f69bbfa94c.

Lizensiert unter CC BY-SA 4.0.

Langzeitarchiviert bei IntRechtDok unter: doi.org/10.17176/20240503-185310-0.