

SWP-Aktuell

NR. 52 OKTOBER 2026

KI als Risiko für die Demokratie

Wie Künstliche Intelligenz den digitalen Autoritarismus zu fördern droht

Daniel Voelsen/Stella Schade

In vielerlei Hinsicht ist Künstliche Intelligenz (KI) eine »normale« Technologie. Sie kann wie andere Technologien für unterschiedliche Zwecke eingesetzt werden, auch in politischer Hinsicht. Die enormen Entwicklungssprünge der KI in den letzten Jahren verstärken insofern Herausforderungen, mit denen Demokratien schon zuvor konfrontiert waren. Insbesondere erlauben KI-Systeme qualitativ wie quantitativ eine neue Stufe an Überwachung und Manipulation. Hinzu kommt jedoch eine Eigenschaft, die über bisher bekannte Technologien hinausgeht, nämlich die immer deutlicher hervortretende Fähigkeit von KI-Systemen, sich eigenständig weiterzuentwickeln. Wird diese Fähigkeit nicht effektiv eingehegt, droht demokratischen Systemen ein massiver Kontroll- und Handlungsverlust.

Als das US-Softwareunternehmen OpenAI im November 2022 den KI-Assistenten ChatGPT veröffentlichte, markierte dies eine Zäsur in der Geschichte der Künstlichen Intelligenz. Erstmals wurde in der Breite erfahrbar, wie groß das Potential von »large language models« (LLMs) ist. In der Folge konnten insbesondere die auf diesem Feld führenden Firmen aus den USA enorme finanzielle Ressourcen mobilisieren, was die Dynamik der technologischen Weiterentwicklung noch einmal steigerte.

Angesichts der beeindruckenden Fähigkeiten aktueller KI-Systeme ist international ein Wettstreit um den Zugang zu den fortschrittlichsten Modellen entbrannt. Auch wenn deren Entwicklung in den Händen privater Unternehmen liegt, sehen die US-amerikanische wie die chinesische Regierung in KI eine wesentliche Grundlage ihrer

zukünftigen außenpolitischen Machtposition. Viel diskutiert wird daher, wie Europa sich zu diesem Wettbewerb verhalten sollte. Vergleichsweise wenig Beachtung findet hingegen die Frage, wie sich die technischen Möglichkeiten von KI auf politische Systeme auswirken – und damit auch auf das Verhältnis zwischen Demokratien und Autokratien.

KI-gestützte Überwachung durch autoritäre Regime

In autoritären Systemen gibt es seit Jahren einen deutlichen Trend, digitale Technologien zur Überwachung der eigenen Bevölkerung einzusetzen. Aus Sicht der Machthaber bietet sich damit die Möglichkeit, mit weniger Personalaufwand eine noch umfas-



sendere und zugleich individuellere Kontrolle zu gewährleisten. Während einige autoritäre Staaten wie China und Russland entsprechende Technologien selbst entwickeln, setzen Regierungen anderer Länder zumeist auf kommerzielle Angebote.

Durch die aktuellen Entwicklungen im Bereich von KI wird der Trend noch verstärkt, Technologie als Mittel zur Repression zu nutzen. Die derzeit verfügbaren Systeme sind unter anderem besonders gut dafür geeignet, Muster in umfangreichen und diversen Datenbeständen zu finden. Für Zwecke der Überwachung erlaubt dies etwa, mit hoher Geschwindigkeit große Mengen an Kommunikationsinhalten oder Bildaufnahmen auszuwerten. Beispielsweise wird in China die öffentliche Überwachung, die bisher schon großflächig erfolgte, mit Künstlicher Intelligenz immer weiter ausgebaut. Über KI-basierte Gesichtserkennung lassen sich so die Standorte von Personen noch engmaschiger verfolgen.

Mit der Entwicklung von KI-Agenten, die Aufgaben zunehmend autonom ausführen, wird diese Praxis noch einmal auf eine neue Stufe gebracht. Vorstellbar ist, dass sich Künstliche Intelligenz schon sehr bald gezielt darauf ansetzen lässt, einzelne Personen oder Gruppen kontinuierlich zu beobachten. Die technologische Entwicklung weist damit über die vielfach bemühte Metapher des »Panoptikums« hinaus. Während im Panoptikum die Überwachung des Einzelnen immer eine latente *Möglichkeit* war, die sich aber nicht zu jedem Zeitpunkt nutzen ließ, erwächst mit KI-Agenten die Aussicht auf eine räumliche und zeitliche Rundum-Observation.

Angesichts dieser technischen Optionen ist zu erwarten, dass autoritäre Regime ihre Macht gegenüber der Bevölkerung unter Rückgriff auf KI-Systeme weiter ausbauen werden. Entsprechende Technologie zu beschaffen ist für Regierungen vergleichsweise einfach, insbesondere über kommerzielle Anbieter. Hinzu kommt, dass für diese Art von Einsatz der Zugang zu den allerneuesten KI-Modellen (den »frontier models«) wohl nicht notwendig ist. Frei verfügbare

»open source«-Modelle sind dafür vermutlich schon heute gut genug.

Um dieser Entwicklung politisch entgegenzuwirken, bietet sich ein Instrumentarium an, wie es auch bisher schon im Umgang mit digitaler Überwachung angezeigt ist. Demokratische Regierungen sollten sich insbesondere dafür einsetzen, dass der kommerzielle Markt für Überwachungstechnologie soweit wie möglich reguliert wird, um autoritären Regierungen den Zugang zu einschlägigen Produkten zu erschweren. Möglich wäre dies durch verschärfte Exportkontrollen. Vor allem sollten demokratische Regierungen die Nachfrage nicht selbst als Kunden problematischer Firmen weiter befeuern.

Speziell mit Blick auf KI liegt aus dieser Perspektive auch nahe, den vollkommen unregulierten Zugang zu immer leistungsfähigeren »open source«-Modellen zu überdenken. Umgekehrt wäre vorstellbar, gerade demokratischen Kräften in autoritären Staaten den Zugang zu den fortschrittlichsten KI-Modellen zu erleichtern. Im digitalen Wettrüsten zwischen Regierung und Opposition könnte dies im Einzelfall eine entscheidende Wirkung haben.

Manipulation durch KI in Demokratien

Auch demokratische Staaten setzen zunehmend KI-basierte Überwachungssysteme ein – für Zwecke der Strafverfolgung, bei der Terrorismusabwehr und in der nachrichtendienstlichen wie militärischen Aufklärung. Während sich die technologische Grundlage hier wenig von jener in autoritären Ländern unterscheidet, soll der rechtliche Rahmen demokratischer Systeme eine unzulässige Machtausübung seitens der Regierung verhindern. Wie etwa der 2023 erschienene Bericht des Europäischen Parlaments zum Einsatz der Spyware »Pegasus« durch Regierungen von EU-Staaten zeigt, ist diese rechtliche Einhegung in gewissem Maße aber auch in Demokratien prekär; sie muss deshalb immer wieder politisch neu verteidigt werden.

Darüber hinaus erweist sich Künstliche Intelligenz schon heute als wirksames Instrument all jener Akteure, die darauf zielen, demokratische Systeme von innen heraus auszuhöhlen. Insbesondere erlauben heutige KI-Programme das massenhafte und kostengünstige Erstellen falscher Informationen in Form von Texten, Bildern und Videos. Solcherart generierte Informationen werden verwendet, um über digitale Plattformen den öffentlichen Diskurs zu beeinflussen. Das Problem von Desinformation ist nicht neu, verschärft sich aber durch den verstärkten Einsatz von KI-Agenten.

Im Fall der heute vielgenutzten Chatbots kommt als weitere Dimension hinzu, dass ihre Aussagen mitunter bestimmte politische Sichtweisen begünstigen. Dies kann Ergebnis bewusster Konfiguration sein, etwa wenn sich chinesische KI-Modelle an den Zensurvorgaben der eigenen Regierung orientieren. Eine inhaltliche Schlagseite kann aber auch schlicht dadurch entstehen, dass KI-Systeme sich selektiv auf bestimmte Medien stützen und dabei deren Ausrichtung übernehmen.

Brisant ist zudem, dass der Markt für Künstliche Intelligenz hochkonzentriert ist und einige der hier dominierenden US-Unternehmen explizit politisch agieren. Zu Recht sind darum die »tech bros« – wie die Führungspersonen der einflussreichsten KI-Firmen teils noch immer verniedlichend genannt werden – in den Fokus gerückt. Einige von ihnen haben ein zumindest angespanntes Verhältnis zu demokratischen Prinzipien und wirken partiell als »Erosionsakteure«, also Kräfte, die durch ihr Handeln demokratische Strukturen und Verfahren unterminieren.

In der Summe ergibt sich hier ein ähnlicher Effekt wie in autoritären Staaten. Als Weiterentwicklung bisheriger Technologien verstärkt KI die damit verbundenen Konflikte – und erhöht so den Druck, gegebene Handlungsmöglichkeiten zu nutzen. Im Rahmen demokratischer Systeme reicht das Spektrum denkbarer Reaktionen dabei von einem schärferen Wettbewerbsrecht über verbindlichere Vorgaben zur »content moderation« bis hin zur Förderung

von Medienkompetenz über klassische Bildungspolitik.

Selbstlernende KI-Systeme

Jenseits der beschriebenen Verstärkungseffekte geht Künstliche Intelligenz in einer wesentlichen Dimension über das Fähigkeitsspektrum »normaler« Technologien hinaus. Nach jetzigem Stand deutet vieles auf eine Zukunft, in der sich KI-Systeme in einer bislang ungekannten Weise eigenständig weiterentwickeln werden (»rekursive Selbstverbesserung«).

Schon heute ist die konkrete Arbeitsweise von »large language models« für Menschen nur eingeschränkt nachvollziehbar. Diese Systeme sind zu komplex, als dass sich jeder einzelne Schritt ihres Vorgehens zurückverfolgen ließe. Wenn nun möglicherweise schon bald Tausende von KI-Agenten eingesetzt werden, um die nächste Generation von Künstlicher Intelligenz zu entwickeln, wird menschliche Kontrolle praktisch unmöglich. Denn es wird in einem solchen Szenario schlicht nicht mehr genug ausreichend qualifiziertes Personal geben, das überblicken könnte, was die KI-Systeme an Software-Code hervorgebracht haben.

Es gibt bereits hinreichend Beispiele dafür, wie sich KI menschlicher Kontrolle entzieht. Besonders spektakulär ist der Fall eines Modells der Firma OpenAI, das die Begrenzungen seiner Testumgebung umging und anschließend ein anderes Unternehmen hackte. Man muss dabei keine »bewusste Absicht« des Programms unterstellen, kann ein solches Geschehen aber sehr wohl als Vorboten eines drohenden Kontrollverlustes begreifen.

Die Risiken verselbständigter KI-Systeme wurden vielfach beschrieben, bisweilen gar als existentielle Menschheitsbedrohung. Sehr viel unmittelbarer ist dadurch aber schon in absehbarer Zukunft die Demokratie gefährdet. Denn wenn eine Technologie immer weitere gesellschaftliche Bereiche durchdringt und sich zugleich effektiver menschlicher Kontrolle entzieht, beschränkt



Dieses Werk ist lizenziert
unter CC BY 4.0

Das Aktuell gibt die Auf-
fassung der Autoren wieder.

In der Online-Version dieser
Publikation sind Verweise
auf SWP-Schriften und
wichtige Quellen anklickbar.

SWP-Aktuells werden intern
einem Begutachtungsverfahren,
einem Faktencheck und
einem Lektorat unterzogen.
Weitere Informationen
zur Qualitätssicherung der
SWP finden Sie auf der SWP-
Website unter [https://www.
swp-berlin.org/ueber-uns/
qualitaetssicherung/](https://www.swp-berlin.org/ueber-uns/qualitaetssicherung/)

SWP

Stiftung Wissenschaft und
Politik
Deutsches Institut für
Internationale Politik und
Sicherheit

Ludwigkirchplatz 3–4
10719 Berlin
Telefon +49 30 880 07-0
Fax +49 30 880 07-100
www.swp-berlin.org
swp@swp-berlin.org

ISSN (Print) 1611-6364
ISSN (Online) 2747-5018
DOI: 10.18449/2026A52

dies in relevanter Weise die Möglichkeiten
demokratischer Selbstbestimmung und der
dafür nötigen Transparenz.

Ausblick und Handlungs- empfehlungen

Die führenden KI-Unternehmen selbst
haben wiederholt einen politisch bewuss-
teren Umgang mit dem technologischen
Fortschritt eingefordert. Aktuell ist dabei
viel von einem »slowdown« die Rede, also
einem gezielten Verlangsamen der Ent-
wicklung. Auf Ebene der Firmen wie auch
international zwischen Regierungen ent-
steht hier allerdings ein klassisches »collec-
tive action«-Problem. Ohne allgemeinver-
bindliche Vorgaben gibt es starke Anreize
für jeden Einzelakteur, bei allem Bewusst-
sein um mögliche Gefahren für sich selbst
eine Führungsposition anzustreben bzw.
diese zu verteidigen.

In dieser Lage spräche funktional vieles
dafür, eine effektive internationale Gover-
nance zu etablieren. Mit dem amtierenden
US-Präsidenten ist ein solches Ziel jedoch
in weite Ferne gerückt. Donald Trump hat
wiederholt deutlich gemacht, dass er ent-
sprechende Regularien ablehnt; und selbst
wenn er seine Haltung ändern sollte, blie-
ben erhebliche Zweifel, wie verlässlich der
Sinneswandel wäre.

Für die deutsche und europäische Politik
stellt dies eine besondere Herausforderung
dar. Denn sie hat kaum direkten Einfluss
auf eine technologische Entwicklung, die
zu einer grundlegenden Gefahr für die
Demokratie zu werden droht. Umso wich-
tiger ist, die oben genannten Maßnahmen
im Umgang mit digitaler Überwachung und
zum Schutz vor digitaler Manipulation um-
zusetzen, die öffentlich schon lange disku-
tiert werden. Zu prüfen wäre zudem, ob in
sensiblen Bereichen wie der öffentlichen
Verwaltung oder bei Betreibern kritischer
Infrastruktur die Nutzung spezifischer KI-
Modelle rechtlich eingeschränkt werden

muss. Schon jetzt besteht die Möglichkeit,
den Einsatz von Komponenten bestimmter
Hersteller zu untersagen, um Sicherheits-
risiken zu reduzieren. Künftig ließen sich
auch KI-Modelle selbst als solche Kompo-
nenten einstufen. Ein maßgebliches Krite-
rium dafür könnte sein, ob bei ihnen eine
menschliche Kontrolle noch plausibel mög-
lich ist.

*Dr. Daniel Voelsen ist Leiter der Forschungsgruppe Globale Fragen.
Stella Schade ist Forschungsassistentin in der Forschungsgruppe Globale Fragen.*