Arbeitsübersetzung unter Zuhilfenahme maschineller Übersetzungstools aus dem Englischen: „Advanced Technologies and Data Security ", 12. Mai 2025. Kein offizielles G7- bzw. S7-Dokument.

Spitzentechnologien und Datensicherheit

Definition des Themas

In den letzten zwei Jahrzehnten haben Anzahl, Umfang, Nutzen und Einsatz von Datenerfassungssystemen,[1] Datenverarbeitungs- und Datenarchivierungstechnologien, einschließlich Systeme mit Künstlicher Intelligenz (KI), die Daten nutzen, um Schlussfolgerungen zu ziehen oder Handlungen auszuführen, erheblich zugenommen. Laut dem *International Scientific Report on the Safety of Advanced AI* stehen dem Potenzial der KI zum Nutzen der Menschheit potenziell schwerwiegende Risiken gegenüber.[2] Daher ist ein mehrstufiger, ganzheitlicher, auf den Menschen ausgerichteter und intelligenter Governance- und Regulierungsansatz erforderlich, um die Vorteile dieser Technologien nicht zu schmälern und gleichzeitig die Probleme anzugehen. Im Folgenden wird der Begriff „Datensicherheit" verwendet, um diese miteinander verknüpften Anliegen zu beschreiben.

Hintergrund

Wie das Panel des *International Scientific Report on the Safety of Advanced AI* dargelegt hat, stehen dem enormen Potenzial der erwarteten Fortschritte im Bereich der KI und dem Bedarf an Verfügbarkeit und Qualität von Daten für legitime Zwecke wie die Forschung in Bereichen, die für das Wohlergehen der Menschheit von entscheidender Bedeutung sind, potenziell schwerwiegende Risiken gegenüber, die sich aus vorsätzlichem Missbrauch (z.B. Desinformation und andere Bedrohungen der Demokratie), Kontrollverlust, Menschenrechtsverletzungen, Umbrüchen des Arbeitsmarkts und Verlust von Existenzgrundlagen sowie Klima- und Umweltschäden ergeben können. Sowohl das Ausmaß der möglichen Störungen als auch ihr zeitlicher Ablauf sind mit großen Unsicherheiten behaftet, aber es besteht Einigkeit darüber, dass Wissenschaft, Entwicklerinnen und Entwickler sowie Politik nicht ausreichend vorbereitet sind. Im Sinne des Vorsorgeprinzips ist es daher von entscheidender Bedeutung, in die Datensicherheit zu investieren und zu erforschen, wie fortgeschrittene KI-Systeme nutzbar gemacht und kontrolliert werden können. Soziale, politische und technologische Innovationen sind auf allen Ebenen erforderlich, um den kollektiven Nutzen zu erkennen und zu maximieren und um sicherzustellen, dass die Leitplanken kontinuierlich aufrechterhalten und aktualisiert werden, um Risiken zu antizipieren, zu verhindern und zu mindern.

Spezifische nationale und internationale Governance- und Regulierungsmaßnahmen sowie deren Koordinierung spielen eine wichtige Rolle bei der Minderung dieser Risiken. Governance- und Regulierungsgremien sollten technische und organisatorische Erwartungen und Leitlinien festlegen, um sicherzustellen, dass Risiken und Nutzen angemessen ermittelt und behandelt werden. Sie sollten reaktionsfähige Einhaltungs- und Durchsetzungssysteme einführen, die die Menschen und den Planeten schützen, ohne Innovation zu behindern und wirtschaftlichen Wohlstand zu gefährden. Wir verstehen eine effektive Governance und Regulierung als notwendige, politische Innovation, die eine gerechtere Verteilung der Vorteile über die gesamte Gesellschaft ermöglicht und einen Rahmen für verantwortungsvolle Innovation und den Einsatz von Technologie zur Erreichung gesellschaftlicher Ziele bietet. Zu den Akteuren im Bereich der Datensicherheit gehören Praktikerinnen und Praktiker (z.B. aus der Industrie und dem öffentlichen Sektor), Wissenschaftlerinnen und Wissenschaftler und die Öffentlichkeit, entweder als Einzelpersonen oder als (selbst-) identifizierte Gruppen.

Politikempfehlungen

<u>Empfehlung 1</u>

Da Spitzentechnologien schnell zu kritischen Infrastrukturen werden können, ist es von entscheidender Bedeutung, dass ihre Verwaltung weder den Unternehmen, die sie entwickeln, noch den Märkten, der sozialen Anpassung oder der allgemeinen und beruflichen Bildung überlassen wird, um die Gesamtverantwortung auf die Menschen zu übertragen. Unternehmen, Märkte und Bildung spielen alle eine wichtige Rolle, aber Governance und Regulierung sind unerlässlich:

a. um diejenigen zu schützen, die von den verschiedenen Möglichkeiten und Auswirkungen der neuen Technologien negativ betroffen sind; und
b. um sicherzustellen, dass diese Technologien nicht fortwährend wirtschaftliche und politische Macht konzentrieren und bestehende Ungleichheiten verschärfen.

Empfehlung 2

Die Regelung der Datenerhebung und -speicherung stellt sowohl eine rechtliche als auch eine ethische Herausforderung dar. Sind die Daten erst einmal erhoben, müssen zwei entscheidende Aspekte der Datennutzung sorgfältig geregelt werden: die Verhinderung unbeabsichtigter Datenlecks und die Gewährleistung der Datenqualität. Aufkommende Regelungen wie der *EU AI Act*[3] erkennen diese Bedenken an, weisen jedoch Lücken auf. Die Verordnungen empfehlen beispielsweise

a. die Pseudonymisierung von Daten, um unbeabsichtigte Datenlecks zu verhindern – obwohl Datenschutzexpertinnen und -experten gezeigt haben, dass dies oft nicht ausreicht und stärkere Maßnahmen wie ein differenzierter Datenschutz erforderlich sind; und
b. sicherzustellen, dass die demografische Verteilung in Daten, die für nützliche Schlussfolgerungen verwendet werden (z.B. um ein KI-Modell zu trainieren), mit der Bevölkerung übereinstimmt, für die sie bestimmt sind – allerdings ohne dabei anzugeben, wie dies geschehen kann, ohne die Vertraulichkeit der Daten zu verletzen.

Um diese Lücken zu schließen, sollten die politischen Entscheidungsträgerinnen und -träger enger mit Fachleuten, einschließlich Wissenschaftlerinnen und Wissenschaftlern, und Mitgliedern der Gesellschaft zusammenarbeiten, von denen diese Daten stammen. Die Kommunikation in beide Richtungen sollte die Auslegung der Gesetzgebung auf technische Aspekte lenken, wie z.B. die Sicherstellung, dass relevante demografische Daten (z.B. Sprache, Alter, ethnische Zugehörigkeit, Geschlecht) angemessen erhoben und gesichert werden, um Ungleichheiten nicht zu verstärken. Sie sollte auch aufzeigen, in welche Richtung sich die akademische und industrielle Forschung vorrangig bewegen sollte, um Technologien zu entwickeln, die die Einhaltung der Vorschriften durch die Praktikerinnen und Praktiker und die Durchsetzung durch die Regulierungsbehörden erleichtern (z.B. durch die Entwicklung von Datenanalyseverfahren, die überprüfbare Garantien bieten).

Empfehlung 3

Mit dem Einzug datengetriebener Systeme in alle Bereiche menschlichen Handelns hat sich die „Bedrohungsfläche“ solcher Systeme drastisch vergrößert. Menschen aus allen Lebensbereichen sind nun an der Nutzung und Management dieser Systeme beteiligt. Ihre Handlungen, Unterlassungen und Fehler können zu Sicherheitsverletzungen führen. Die Zahl der Fälle, in denen menschliches Versagen zu Ransomware oder anderen Angriffen auf kritische Infrastrukturen wie Krankenhäuser geführt hat, verdeutlicht das Ausmaß des Problems. Es bedarf breit angelegter und kontinuierlicher Anstrengungen, um eine „Literacy“ im Bereich Sicherheit/Privatsphäre zu erreichen. Politische Entscheidungsträgerinnen und -träger sollten Anreize für die kontinuierliche Entwicklung von Werkzeugen und Schulungsprogrammen schaffen, um dieses Wissen zu vermitteln und kontinuierlich zu verbessern, sowie für die Entwicklung alternativer „Backup“-Systeme und -Verfahren, um menschliche Fehler zu abzufedern.

Empfehlung 4

Die Öffentlichkeit kann nicht als eine einzige undifferenzierte Gruppe betrachtet werden, ob es sich nun um „Nutzerinnen und Nutzer“, „Verbraucherinnen und Verbraucher“ oder „Bürgerinnen und Bürger“ handelt. Gruppen und Einzelpersonen sind in sehr unterschiedlicher Weise von fortgeschrittenen Daten- und Überwachungstechnologien betroffen, mit Auswirkungen, die von trivial bis lebenswichtig reichen können, von geringfügigen Änderungen des Komforts, wie der automatischen Lieferung nach Hause, über unsichtbare Formen der Diskriminierung, wie z.B. die Einbettung von rassistischen und geschlechtsspezifischen Vorurteilen in automatisierte Einstellungsprozesse oder Strafverurteilungen vor Gericht, bis hin zum Ausschluss aus Ländern aufgrund von Flugverbotslisten, die auf

kategorisierten Verdächtigungen beruhen, oder sogar zum Tod im Falle von KI-gestützter Zielauswahl in Waffensystemen. Die Berücksichtigung von „Datengerechtigkeit“ – der gerechten Art und Weise, wie Menschen bei der Erhebung und Nutzung von Daten kategorisiert und behandelt werden – ist daher eine wesentliche Ergänzung zu bestehenden Vorstellungen von rechtlicher, wirtschaftlicher, sozialer und ökologischer Gerechtigkeit.

Empfehlung 5

Spezifische Gruppen mit höherer Vulnerabilität wie sehr junge Menschen, ältere Menschen, insbesondere solche mit kognitiven Beeinträchtigungen, und kranke Menschen müssen ebenfalls adressiert werden, da sie anfälliger für den böswilligen Einsatz von Spitzentechnologien sind, z.B. Betrügerinnen und Betrüger, die ältere Menschen ins Visier nehmen, der Einsatz von Ransomware gegen Krankenhäuser und auch Kriminelle, die es auf Kinder abgesehen haben. Solche Schwachstellen dürfen jedoch nicht als Vorwand für die Ausweitung ungerechtfertigter und flächendeckender Überwachung und die Einschränkung von Menschenrechten dienen. Wenn mehr Sicherheit und Überwachung eingeführt werden, können solche Maßnahmen zur weiteren Marginalisierung genau der Gruppen beitragen, die bereits Opfer von Datenungerechtigkeit sind.

Empfehlung 6

Die Regulierungsbehörden müssen Überlegungen zur Datensicherheit im Zusammenhang mit aufkommenden Technologien in ihre bestehenden Mandate aufnehmen und dementsprechend sicherstellen, dass sie die erforderlichen internen Fachkenntnisse und Kapazitäten sowie Kommunikations- und Koordinierungsfähigkeiten entwickeln. Sowohl auf nationaler als auch auf internationaler Ebene können neue Governance-Systeme und Regulierungsgremien erforderlich sein, um sektor- und interessentenübergreifend durchsetzbare Leitlinien, Standards und bewährte Verfahren zu koordinieren, wenn Spitzentechnologien systemische und disruptive Veränderungen in der Gesellschaft auslösen, wie dies bei der KI der Fall ist. Datensicherheit ist wichtig, weil Daten und Spitzentechnologien heute nicht nur Innovation und Wohlstand, sondern auch Gesundheit, Bildung, Kreativität, Kunst, Meinungsbildung und Wissen ermöglichen.

Empfehlung 7

Es muss Klarheit über die Zuständigkeiten der einzelnen Regulierungsbehörden herrschen, damit neue Regulierungseinheiten nicht zu Ineffizienzen durch eine stärker fragmentierte Regulierungslandschaft führen. Die G7 ist ein solches Koordinationsforum, aber es muss auch eine viel breitere Diskussion stattfinden, an der bestehende, anerkannte Regulierungsgremien (auch wenn die Zuständigkeiten umstritten sind) wie die UNESCO und die Internationale Fernmeldeunion (ITU), die Länder des Globalen Südens und führende Wirtschafts- und Technologieunternehmen außerhalb der G7 beteiligt werden.

Empfehlung 8

Wir erkennen an, dass Spitzentechnologien unweigerlich Fragen der nationalen Sicherheit aufwerfen, aber es liegt in der Verantwortung der Akademien und Regierungen, die Interessen der globalen Menschheit und des Planeten zu berücksichtigen. Zusammenarbeit für Frieden und die globale Sicherheit ist notwendig. Wir würden die Schaffung eines „CERN für KI“ unterstützen, das Forschenden aus der ganzen Welt einen umfassenden und fairen Zugang zu Rechenleistung bietet, ihnen ermöglicht, Datensätze zu erstellen, und auch das gegenseitige Lernen zwischen Forschenden aus dem Globalen Norden und dem Süden fördert.

Empfehlung 9

Wir empfehlen den politischen Entscheidungsträgerinnen und -trägern, Anreize für die Arbeit im Rahmen des Open-Source-Modells zu schaffen, um die Schwierigkeiten bei der Ausbildung geeigneter Expertinnen und Experten für die Durchsetzung zu überwinden. Solche Anreize könnten in Form einer zweckgebundenen Finanzierung und Zuweisung von Ressourcen zur Unterstützung der Open-Source-Gemeinschaft bei der Pflege der Software und ihrer Integrität erfolgen. Populäre Open-Source-Projekte haben gezeigt, dass Offenheit und Transparenz auch zu mehr Sicherheit führen können. Allerdings müssen Entscheidungen über die Zulassung oder Einschränkung des Open-Sourcings leistungsfähiger KI-Systeme einer demokratischen Kontrolle unterliegen und die für proprietäre Systeme geltenden Sicherheitsvorschriften müssen auch für Open-Source-Systeme gelten.

Empfehlung 10

Generative KI-Modelle können Medien von beeindruckender Qualität produzieren und werden zur Täuschung missbraucht. Solche Modelle überschwemmen auch das Internet mit Fehlinformationen, nicht unbedingt mit absichtlicher Täuschung, aber mit falschen Informationen, die dann von KI-Modellen genutzt und wiederverwendet werden können, was sowohl zur Verschlechterung der Modelle als auch zu weiteren Fehlinformationen führt. Regulierungen wie der EU AI Act versuchen, diesem Problem zu begegnen.[4] „Wasserzeichen" – die Einbettung von Mustern in KI-generierte Inhalte, die es ermöglichen, diese als solche zu identifizieren[5] – sind eine Lösung, die jedoch bekanntermaßen anfällig ist. Wasserzeichen, die von den Eigentümern der KI-Modelle verifiziert werden, reichen möglicherweise nicht aus, um den Schaden durch betrügerische KI-generierte Daten einzudämmen, und ändern möglicherweise nicht das Verhalten der Menschen im Umgang mit Daten – insbesondere in stark technologiegetriebenen Gesellschaften. Politische Entscheidungsträgerinnen und -träger sollten die Erforschung verschiedener Techniken zur Überprüfung der Herkunft von Daten fördern.

Empfehlung 11

Schließlich haben Cloud-basierte KI-Technologien wie Large Language Models (LLMs) einen großen direkten Einfluss auf das globale Klima. Beispielsweise ist der Energieverbrauch für eine ChatGPT-Abfrage wesentlich höher als für eine einfache Websuche. Die unbewiesene Behauptung, dass ein höherer Energieverbrauch Anreize für einen schnelleren Umstieg auf nachhaltige Energiequellen schafft, wird hier nicht berücksichtigt. Die Kontrolle und Regulierung von Daten und deren Verarbeitung sollte mit Maßnahmen zur ökologischen und energetischen Nachhaltigkeit koordiniert werden.

Referenzen

1. Dazu gehören Smartphones, tragbare und andere persönliche Geräte, Heim- und Industrieautomatisierung, intelligente Zähler, medizinische Geräte, autonome Fahrzeuge sowie öffentliche und private Überwachungssysteme.
2. International AI Safety Report 2025. DSIT 2025/001. https://www.gov.uk/government/publications/international-ai-safety-report-2025
3. EU AI Act. https://www.europarl.europa.eu/topics/en/article/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence
4. Ebd.
5. Siddarth Srinivasan 2024. Detecting AI fingerprints: A guide to watermarking and beyond. Brookings Institution. https://www.brookings.edu/articles/detecting-ai-fingerprints-a-guide-to-watermarking-and-beyond/