Der EU AI Act zur Künstlichen Intelligenz bietet keine umfassende Sicherheit – vielmehr könnten sich bekannte Großunternehmen einen Anstrich von Transparenz und regulierter Künstlicher Intelligenz geben, ohne tatsächlich nach diesen Prinzipien zu handeln. Es braucht aber Regeln, die konsequent und für alle gleichermaßen gelten. Von **Günther Burbach.**

Dieser Beitrag ist auch als Audio-Podcast verfügbar.

https://www.nachdenkseiten.de/upload/podcast/241031-EU-AI-Act-NDS.mp3

Podcast: Play in new window | Download

Am 21. Mai 2024 wurde der EU AI Act beschlossen. Was als beispielhafte und einmalige Richtlinie angepriesen wird, ist in Wirklichkeit nur ein Papiertiger. Auch wenn der Wille zur Regulierung im Bereich der Künstlichen Intelligenz (KI) scheinbar vorhanden ist, mangelt es deutlich an einer konsequenten Umsetzung. Zu einzelnen Punkten wird weiterhin verhandelt und teilweise nachgebessert. Doch eines ist bereits klar: Die grundlegenden Prinzipien stehen fest. KI-Systeme sollen nach Risikoklassen eingeteilt werden. Hochrisiko-Anwendungen unterliegen dabei strengen Auflagen, während Systeme mit niedrigem Risiko kaum Einschränkungen fürchten müssen.

Natürlich ist der EU AI Act einzigartig und sollte durchaus als Vorbild dienen. Schließlich ist eine schlechte Regulierung immer noch besser als gar keine. Doch künftig sollten weniger Lücken und Schlupflöcher bestehen. Betrachtet man die Regelungen im Detail, drängt sich der Verdacht auf, dass auch große Lobbyorganisationen Einfluss auf die Verhandlungen genommen haben könnten. Zwar wurden die Risiken unregulierter KI offensichtlich erkannt – jedenfalls von einigen Abgeordneten in Brüssel. Doch wirklich schmerzhaft einschränken möchte man anscheinend niemanden. Mächtige Interessengruppen könnten immer noch gesetzliche Lücken nutzen, um ihre Geschäftsmodelle abzusichern.

Eine entscheidende Rolle spielt die Kategorisierung, bei deren Definition genau diese Interessengruppen ihren Einfluss geltend gemacht haben und weiterhin machen. Den Bürgern der EU wird erneut vor Augen geführt, wie gutgemeinter politischer Wille im Konflikt mit großem Kapital steht. Die Einstufung als vermeintlich geringes Risiko kann dabei bares Geld wert sein – besonders, wenn es gelingt, durch das Dauerfeuer der Lobbyverbände das eigene Geschäftsmodell in

die niedrigste Risikoklasse einzuordnen.

Datenmissbrauch durch soziale Medien

Anwendungen mit geringem Risiko werden oft von sozialen Medien oder für personalisierte Werbung genutzt. Die großen Unternehmen hinter diesen „Datenkraken“ stellen solche Systeme als überwiegend harmlos dar und werden dabei von einer starken Lobby unterstützt. Für uns als Verbraucher stellt sich also die Frage: Ist das wirklich so unbedenklich, wie es von den Profiteuren dieser Einstufung dargestellt wird?

Gerade die Firmen, die als „geringes Risiko“ eingestuft werden, prägen unseren Alltag erheblich. Wer ist heutzutage nicht auf einer der großen Plattformen, um sich zu vernetzen, zu spielen oder einen neuen Partner zu finden? Doch überall werden Daten erhoben, die das Fundament für Nutzeranalysen und Microtargeting bilden. Diese scheinbar harmlosen Anwendungen dringen immer tiefer in unsere Privatsphäre ein und eröffnen ein großes Potenzial für Manipulation durch gezielte Werbung. Die erhobenen Daten könnten außerdem von Drittanbietern oder sogar staatlichen Stellen genutzt werden. Ohne stärkere Regulierung können Unternehmen umfassende Verhaltensprognosen ihrer Nutzer erstellen, was Manipulationen durch gezielte Einflussnahme Tür und Tor öffnen könnte. Ein öffentlich gewordener Fall ist der Skandal um Cambridge Analytics, wo Daten von Millionen Facebook-Nutzern ohne deren Zustimmung benutzt wurden, um politische Kampagnen zu beeinflussen.

Selbstlernende Systeme

Eine weitere, sehr ernst zu nehmende Lücke im EU AI Act zeigt sich im Bereich selbstlernender und autonomer Systeme. Der Act sieht zwar vor, dass Systeme vor ihrem Einsatz geprüft und klassifiziert werden – ein guter Ansatz, der jedoch für autonome und selbstlernende Systeme nicht weit genug geht. Diese Systeme entwickeln sich eigenständig weiter und könnten innerhalb kürzester Zeit ihre Risikostufe verändern, ohne dass eine erneute Prüfung erforderlich wäre.

Das bedeutet, dass sich die Algorithmen autonomer Systeme möglicherweise so verändern, dass sie profitabler, aber zugleich unethischer werden. So könnte beispielsweise ein Algorithmus, der auf die Daten einer Krankenversicherung zugreift, entscheiden, Personen ab fünfzig Jahren eine Selbstbeteiligung für kostenfreie Leistungen zu berechnen. Dies könnte schlicht auf der Grundlage

geschehen, dass diese Altersgruppe statistisch häufiger Leistungen in Anspruch nimmt als jüngere Menschen.

Autonome Waffensysteme

Die kritischste und gefährlichste Schwachstelle im EU AI Act liegt jedoch im Bereich autonomer Waffensysteme. Zuvor eingestufte Systeme könnten zweckentfremdet werden, eine ursprünglich harmlose Überwachungsdrohne könnte etwa zu einer Angriffsdrohne umprogrammiert werden. Angesichts der erheblichen Investitionen in autonome Waffentechnologien durch global agierende Großunternehmen kann man nur mutmaßen, was mit diesen Systemen tatsächlich möglich ist. Zu befürchten ist jedoch, dass die Fortschritte autonomer Systeme letztlich katastrophale Folgen haben könnten. Beispielhaft dafür könnten autonome Drohnen sein, die unabhängige Entscheidungen über Zielangriffe treffen können, was zu unvorhersehbaren Konsequenzen, gerade in Kriegsgebieten, führen könnte.

Begrenzte Reichweite

Ein weiterer Schwachpunkt des EU AI Acts liegt in seiner begrenzten Reichweite. Die Vorschriften gelten ausschließlich für Unternehmen mit Sitz in der EU und für Firmen, die gezielt Produkte und Dienstleistungen in die EU liefern. Internationale Konzerne mit Datenzentren oder Entwicklungsabteilungen außerhalb der EU könnten jedoch genau diese Lücken nutzen. Auch in der EU ansässige Unternehmen könnten Standorte in Drittländern aufbauen, in denen keine strengen KI-Regulierungen bestehen. So könnten sie Daten und Modelle außerhalb der EU weiterentwickeln und anschließend in die EU importieren und die europäischen Vorschriften so weitgehend umgehen.

Diese Strategie erinnert an das bekannte Vorgehen: „Wenn ich meine eigenen Landsleute nicht ausspionieren darf, beauftrage ich eben einen anderen Staat damit und lasse mir die Informationen übermitteln.“

Transparenz

Was nützt die beste Regulierung, wenn es an Transparenz fehlt? Da der EU AI Act die Transparenzanforderungen nicht universell festlegt, können Unternehmen in bestimmten Fällen die Details ihrer Systeme geheimhalten, unter Berufung auf den Schutz von Betriebsgeheimnissen. So verständlich es ist, dass große Marktführer ihre internen Abläufe schützen möchten, birgt genau diese Intransparenz erhebliche

Risiken. Große Plattformen könnten sich auf den Schutz ihrer Betriebsgeheimnisse berufen, um die Transparenzvorgaben zu umgehen. Dadurch wäre es ihnen möglich, tiefgreifende Nutzeranalysen und Manipulationsstrategien zu entwickeln, ohne dass Benutzer oder Behörden die Mechanismen dahinter nachvollziehen können.

Gesichtserkennungstechnologie

Im Bereich der Gesichtserkennung und biometrischen Systeme sieht der EU AI Act zwar Regelungen vor, spricht jedoch kein pauschales Verbot aus. Angesichts des potenziellen Einsatzes zur Massenüberwachung wäre jedoch eine klar formulierte und restriktivere Regelung dringend erforderlich. Ausnahmeregelungen bestehen beispielsweise für private Sicherheitsanwendungen und Systeme zur Strafverfolgung, die private Sicherheitsdienste für ihre Zwecke nutzen könnten. Sie könnten dabei argumentieren, dass das hohe Risiko ihrer Arbeit den Einsatz dieser Technologie rechtfertigt.

Zudem gibt es sprachliche Lücken, die es Sicherheitsunternehmen ermöglichen könnten, Überwachungstechnologien zu etablieren. Wie gefährlich es werden könnte, zeigt sich beim Einsatz von Gesichtserkennung in der Polizeiarbeit. Wie schnell würde eine fehlerhafte Identifikation zu einem persönlichen Drama, das ganze Existenzen vernichten könnte? Hier sollte dringend nachgebessert werden, um eine flächendeckende Überwachung zu verhindern.

Fazit

Die genannten Schwächen machen deutlich, dass der EU AI Act keine umfassende Sicherheit für die Zukunft bietet. Vielmehr könnten sich bekannte Großunternehmen einen Anstrich von Transparenz und regulierter KI geben, ohne tatsächlich nach diesen Prinzipien zu handeln. Es braucht Regeln, die konsequent und für alle gleichermaßen gelten. Betriebsgeheimnisse dürfen nicht als Vorwand für Intransparenz genutzt werden. Unternehmen, die Daten ihrer Nutzer zur Gewinnmaximierung einsetzen, sollten verpflichtet werden offenzulegen, wie diese Daten verwendet werden und welche Gewinne daraus erzielt werden. Vielen Menschen würde dadurch klarer werden, dass angeblich kostenlose Sozial-Media-Plattformen keineswegs selbstlos handeln.

Natürlich hat sich die Politik bei der Erarbeitung dieses Acts auf viele Fachleute verlassen. Es bleibt jedoch die Frage, in wessen Dienst diese Experten stehen. Es

lässt sich durchaus vermuten, dass möglicherweise die Marktakteure selbst darüber entschieden haben, welche Regeln die Politik festlegen sollte. Vergleichbar mit einem verkleideten Wurm, der die Angelzeiten bestimmt.

Es herrscht große Sorge, dass die EU im Bereich der KI-Entwicklung den weltweiten Anschluss verlieren könnte. Diese Angst ist durchaus berechtigt, sollte jedoch nicht dazu führen, dass grundsätzlich gute Ansätze zur Regulierung durch Ausnahmen und Lücken zu einem Schaf im Wolfspelz werden. KI kann insbesondere im Gesundheitssektor erhebliche Fortschritte bringen, die dem Allgemeinwohl zugutekommen können, etwa in der Früherkennung schwerwiegender Krankheiten, wo KI einen unschätzbaren Beitrag leisten könnte. Gleichzeitig dürfen wir aber nicht vergessen, dass Künstliche Intelligenz sich ebenso zur Erstellung von Nutzerprofilen eignet, etwa indem sie aus Kaufverhalten auf ungesunde Lebensweisen schließen könnte.

Zusammenfassend lässt sich sagen, dass der EU AI Act zwar einen ersten Schritt in die richtige Richtung darstellt, jedoch weitreichende Mängel aufweist, die dringend adressiert werden müssen. Die genannten Beispiele, von den Skandalen um Datenmissbrauch bis hin zu den potenziell katastrophalen Folgen autonomer Waffensysteme, verdeutlichen, dass die Risiken unregulierter Künstlicher Intelligenz nicht nur theoretischer Natur sind.

Es ist unerlässlich, dass wir als Gesellschaft gemeinsam handeln, um eine Regulierung zu schaffen, die wirklich schützt und nicht nur den Anschein von Sicherheit vermittelt. Eine klare, umfassende und durchsetzungsfähige Regelung ist nicht nur im Interesse der EU-Bürger, sondern auch für den globalen Frieden und die Stabilität von entscheidender Bedeutung.

Die Zeit drängt: In einer Welt, in der technologische Entwicklungen rasant voranschreiten, müssen wir sicherstellen, dass ethische Grundsätze und der Schutz der Menschenrechte nicht auf der Strecke bleiben. Lasst uns gemeinsam für eine Zukunft kämpfen, in der KI verantwortungsvoll eingesetzt wird zum Wohl der Allgemeinheit und gegen die Interessen von Großkonzernen und Lobbyisten. Nur so können wir sicherstellen, dass Künstliche Intelligenz ein Werkzeug für das Gute bleibt und nicht zu einer Bedrohung für unsere Gesellschaft wird.

Titelbild: RaffMaster / Shutterstock

Quellen:

1. **Allgemeine Informationen zum AI Act**
   - Offizielle Website der EU zum Gesetzgebungsverfahren: Europäisches Parlament – AI Act
   - Beschreibung des AI Acts und allgemeiner Überblick: European Commission – Artificial Intelligence Act
2. **Risiko-Kategorisierung und Lücken für „Low Risk“-Systeme**
   - Risikoklassifizierung im AI Act und ihre Schwächen:
     - Details zur **Kategorisierung von KI-Risiken** und deren Ausnahmen (siehe Artikel 52 und folgende des AI Act).
     - Artikel oder Analysen zu Schwächen in „Low Risk“-Regelungen: EDRi (European Digital Rights) – Kritische Analyse des AI Act
     - Fachartikel zum „Low Risk“-Risiko für die Datenethik (gerade für Social-Media-Plattformen relevant):
       - Algorithm Watch – Zur Transparenz von Low-Risk-Algorithmen
3. **Selbstlernende Systeme und Unvorhersehbarkeit von KI-Entwicklungen**
   - Erläuterungen zur Regulierung selbstlernender Systeme und den darin enthaltenen Schwächen:
     - Verschiedene Positionen dazu von KI-Forscher*innen und Fachmagazinen: AI Policy Blog
     - Fachartikel zu den Risiken und Problemen bei lernenden Systemen in regulierten Bereichen: IEEE – KI und die Herausforderungen selbstlernender Systeme
4. **Extraterritoriale Herausforderungen und internationale Lücken**
   - Diskussionen zum Problem der extraterritorialen Anwendungen und den

Problemen durch unzureichende globale Standards:

- Umfangreiche Analysen zur globalen Reichweite und den Extraterritorialitätsproblemen des AI Act: Carnegie Europe – Europe’s Global Tech Policy

- Publikationen zu Schlupflöchern für multinationale Unternehmen und ihre Datenströme:
  - eu – Schlupflöcher in der EU-Regulierung

5. **Transparenzanforderungen und Geschäftsgeheimnisse**
   - Artikel zu Transparenzanforderungen im AI Act und der Möglichkeit, sich auf „Betriebsgeheimnisse“ zu berufen:
     - EDRi (European Digital Rights) sowie Algorithm Watch analysieren diese Schwächen ausführlich:
       - EDRi – Kritische Position zu Transparenz im AI Act
       - Algorithm Watch – Intransparenz durch Geschäftsgeheimnisse

6. **Massenüberwachung und biometrische Systeme**
   - Diskussion zur möglichen Nutzung biometrischer Systeme und den Problemen, die Ausnahmeregelungen schaffen könnten:
     - Fachartikel zur Überwachungsproblematik und der Lockerung der biometrischen Regulierung im AI Act: Privacy International – Gesichtserkennung und Massenüberwachung

     - Kommentare der **Gesellschaft für Freiheitsrechte e.V. (GFF)** zu biometrischer Überwachung in der EU: Gesellschaft für Freiheitsrechte – Stellungnahme zur biometrischen Überwachung