Die neue Verordnung der EU zur Künstlichen Intelligenz und deren Bedeutung

Stephan Holländer

Am 13. März 2024 verabschiedete das Europäische Parlament den AI-Act (KI-Verordnung). Damit wurde eine gesetzgeberische Lücke geschlossen, denn Künstliche Intelligenz (KI) wirkt sich bereits auf viele Bereiche des Lebens aus. Für den Einsatz von KI sollen in der EU künftig strenge Regeln gelten. Unterhändlerinnen und -händler von Europaparlament und EU-Staaten verständigten sich in Brüssel nach langen Verhandlungen auf diese KI-Verordnung. Sie bildet einen Teil eines Gesamtpakets, das weitere Regulierungen des digitalen Marktes beinhaltet wie die Datenschutz-Grundverordnung (DSGVO), das Gesetz über digitale Märkte (Digital Markets Act DMA) – beide Regelwerke sind bereits in Kraft – sowie das Gesetz über digitale Dienste (Digital Services Act DSA).

Wie ist die KI-Verordnung entstanden?

Mit der Gesetzgebungsarbeit war bereits 2021 begonnen worden. Als im November 2022 ChatGPT auf den Markt kam und einen Hype auslöste, beflügelte dies in Brüssel die gesetzgeberische Arbeit an einem KI-Gesetz. Der Wunsch nach Regelungen zur Anwendung der KI-Technologie auch für breite Kreise wurde offensichtlich. Eine Diskussion darüber, wie weit die Regulierung gehen sollte, begleitete die Ausarbeitung und Beratung des Gesetzes bis zu dessen Verabschiedung durch das EU-Parlament. Der deutsche Digitalminister Volker Wissing wollte eine zu enge Regulierung verhindern, um europäische Unternehmen bei der Entwicklung von KI-Anwendungen gegenüber amerikanischen Konkurrenten nicht ins Hintertreffen geraten zu lassen. Befürchtet wurde, dass Start-ups wie Aleph Alpha aus Deutschland und Mistral AI in Frankreich in ihrer Entwicklung behindert werden könnten, bevor die Entwicklung überhaupt Schwung aufnimmt. Mit dieser Ansicht konnte sich der Minister in der Ampel-Regierung allerdings nicht durchsetzen. Die deutsche Bundesregierung wie auch alle übrigen 26 Mitgliedsländer der EU stimmten dem Gesetzentwurf zu.

Im Fokus des Gesetzes stehen Regelungen für Wirtschaftsunternehmen, die KI-Systeme programmieren oder diese Systeme benutzen. Bibliotheken und weitere Kulturinstitutionen sind von der Nutzung von KI-Anwendungen auch betroffen, stehen aber wie Einzelpersonen, die solche Systeme verwenden, nicht im Vordergrund.

Was ist in der KI-Verordnung geregelt?

Kerngehalt der neuen KI-Verordnung ist die Einteilung von KI-Anwendungen in vier Risikoklassen:

1. KI-Systeme mit niedrigem Risiko

Für Anwendungen, die in die Risikoklasse „Niedriges Risiko" fallen, sind derzeit keine rechtlichen Anforderungen vorgesehen. Hierzu zählen zum Beispiel Spamfilter oder Systeme im Bereich vorausschauender Unterhalt (Predictive Maintenance).

Um allerdings als Anwendung mit niedrigem Risiko eingestuft zu werden, sind eine technische Dokumentation sowie eine Risikobewertung notwendig.

2. KI-Systeme mit begrenztem Risiko

Zu den Anwendungen, die ein begrenztes Risiko aufweisen, gehören KI-Systeme, die mit Menschen interagieren. Beispiele hierfür sind Emotionserkennungssysteme und biometrische Kategorisierungssysteme. Hinsichtlich dieser Anwendungen müssen Anbieter sicherstellen, dass betroffene Personen darüber informiert werden, dass sie mit einem KI-System interagieren. Dies muss für Nutzende durch den Kontext der Anwendung deutlich ersichtlich sein.

3. KI-Systeme mit hohem Risiko

Eine Anwendung gilt als Hochrisiko-KI, wenn sie ein potenziell hohes Risiko für die Gesundheit, die Sicherheit oder die Grundrechte von Personen darstellt. Systeme, die hierunter fallen, sind zum Beispiel

- KI-Systeme, die für die biometrische Identifikation von Personen verwendet werden,
- KI-Systeme, einschließlich Emotionserkennungssysteme, die Rückschlüsse auf persönliche Merkmale von Personen zulassen,
- KI-Systeme, die für die Verwaltung und den Betrieb von kritischen Infrastrukturen eingesetzt werden,
- KI-Systeme für die Bildung oder Ausbildung mit Bezug auf Bewertung und Beurteilung von Prüfungen und des Bildungsniveaus sowie
- KI-Systeme, die das Screening oder Filtern von Bewerbungen oder Änderungen des Arbeitsverhältnisses oder der Aufgabenzuweisung betreffen.

4. KI-Systeme mit inakzeptablem Risiko

KI-Systeme, die in diese Risikoklasse fallen, werden gemäß AI-Act künftig grundsätzlich verboten. Sie bergen

ein erhebliches Potenzial zur Verletzung von Menschenrechten oder Grundprinzipien.
Hierzu zählen Anwendungen, die

- Menschen durch unterschwellige Techniken manipulieren oder ihnen körperlich bzw. physisch schaden könnten,
- Schwächen von bestimmten Personengruppen aufgrund ihres Alters oder von körperlichen sowie geistigen Beeinträchtigungen ausnutzen, um sie bewusst zu beeinflussen,
- Beurteilungen oder Einstufungen der Vertrauenswürdigkeit von Personen über einen bestimmten Zeitraum hinweg auf der Grundlage ihres Sozialverhaltens oder persönlichkeitsbezogener Merkmale vornehmen, die zu einer nachteiligen sozialen Bewertung für die Betroffenen führen könnten oder
- eine biometrische Identifizierung von Menschen in öffentlich zugänglichen Räumen in Echtzeit aus der Ferne heraus erlauben (Ausnahme: Strafverfolgung).

In der KI-Verordnung sind auch die Sanktionen gegen Verstöße festgelegt. Die Nichteinhaltung der Verordnung hat erhebliche Sanktionen zur Folge, die schwerwiegende Auswirkungen auf das Geschäft des Anbieters oder Anwenders nach sich ziehen. Abhängig von der Schwere des Verstoßes bewegen sich die Geldstrafen zwischen 10 und 40 Millionen Euro oder 2 bis 7 Prozent des gesamten weltweiten Jahresumsatzes im vorangegangenen Geschäftsjahr. Daher ist es für alle Beteiligten von größter Bedeutung, dass sie die KI-Verordnung gut kennen und ihre Bestimmungen einhalten können.

Wie lauten die Vorschriften für besonders leistungsfähige Anwendungen der KI?

Dabei geht es um Anwendungen, die mit umfassenden Sprachmodellen und leistungsfähiger KI arbeiten und für bestimmte Anwendungen vorgängig trainiert werden müssen oder die bereits eingegebene Metadaten enthalten. Hierunter fallen Anwendungen wie ChatGPT 4 und Transkriptionsanwendungen wie etwa Transkribus, eine KI-gestützte Plattform zur Erkennung von handgeschriebenem Text zum Beispiel in altdeutscher Schrift. Gemeint sind aber auch sogenannte KI-Basismodelle (foundation models), die etwa in Personalabteilungen eingegangene Bewerbungen auswerten und deren Eignung für ein vorgegebenes Stellenprofil prüfen. Es besteht die Gefahr, dass ein solches System eine Fehlentscheidung aufgrund einer falschen Anwendung oder wegen eines Software-Fehlers im Basismodel trifft. Damit die Unternehmen oder Institutionen solche Fehler aufspüren und nachverfolgen können, müssen die Entwickler wie beispielsweise Open AI oder Mistral so viele technische Details ihrer Anwendungen offenlegen, dass die Anwender ein genügend großes Verständnis ihres KI-Basissystems erwerben können, um die Möglichkeiten und Grenzen dieses Systems einschätzen zu können.

Stock-Fotografie-ID_1706485451_Bildnachweis_Rafmaster

Bei technisch ausgereiften Großsystemen kommen weitere Regeln zur Anwendung, welche die Cybersicherheit betreffen. Maßnahmen zur Cybersicherheit waren von KI-Fachleuten eingefordert worden, da größere Systeme und damit solche, die über eine größere Rechenleistung und umfangreiche Sprachmodelle verfügen, das Risiko für Fehler beim Trainieren der Module mit möglicherweise zu wenig gut kuratierten Daten erhöhen. Die Anforderungen an die Cybersicherheit liegen im Moment so hoch, dass keines der aktuell am Markt erhältlichen Systeme diese Anforderungen erfüllt. Mit den Anforderungen sollen die europäischen Start-up-Unternehmen wie beispielsweise Aleph Alpha, die auch selber Basismodelle entwickeln möchten, dazu ermutigt werden, sodass sie mit den amerikanischen und chinesischen Großkonzernen auf diesem Gebiet Schritt halten können.

Wie rechtssicher ist die jetzt verabschiedete Fassung der KI-Verordnung?

Es ist der EU gelungen, ein komplexes Gesetz zu schaffen, das eine zweckmäßige Regulierung der KI für Produzenten solcher KI-Anwendungen, aber auch für deren Nutzende bewirkt. Eine Rechtslücke wird damit geschlossen. Auch die Normen der durch die Organisation for Economic Co-operation and Development (OECD) unterstützten Organisation Global Partnership on Artificial Intelligence (GPAI) sind nach den intensiven Diskussionen in der EU bezüglich der biometrischen Echtzeit-Fernidentifizierung zu begrüßen, wurden doch damit klare gesetzliche Regeln aufgestellt. Anderes wird wohl erst vor dem EU-Gerichtshof in Luxemburg zu klären sein, so etwa die Transparenzverpflichtung in der Verordnung, gemäß der Unternehmen ihre Trainingsdaten offenlegen müssen. Bisher haben die großen Unternehmen, die sich der Entwicklung von KI-Systemen widmen, ihre Trainingsdaten

geheim halten können, woraus auch Wettbewerbsvorteile resultierten. Die EU-Gesetzgeber haben die Hoffnung, dass es den Anbietern, Betreibern und sonstigen Nutzenden von KI-Systemen dank der Verordnung mit technischer und juristischer Unterstützung sowie mit den angekündigten Leitlinien der EU-Kommission gelingen wird, den europäischen Markt für KI-Systeme attraktiv zu machen, ohne dass die Grundrechte der Nutzenden auf Privatsphäre und Recht an den eigenen Daten infrage gestellt sind.

Wann tritt die Verordnung in Kraft?

Die KI-Verordnung wurde am 13. März dieses Jahres verabschiedet und muss nun noch formell vom Europäischen Rat angenommen werden. Kurze Zeit später wird die KI-Verordnung im EU-Amtsblatt veröffentlicht werden und tritt dann am 20. Tag nach der Veröffentlichung in Kraft, voraussichtlich im Juni 2024. Von der EU ist ein abgestuftes Verfahren für die Anwendung der Regelungen vorgesehen:

iStock-ai-generated

- 6 Monate nach Inkrafttreten (voraussichtlich im Dezember 2024) müssen alle durch die KI-Verordnung verbotenen KI-Systeme abgeschaltet werden.
- 12 Monate nach Inkrafttreten (voraussichtlich im Juni 2025) werden die Normen der GPAI für KI-Systeme verbindlich und anwendbar.
- 24 Monate nach Inkrafttreten (voraussichtlich im Juni 2026) werden alle Vorschriften der KI-Verordnung anwendbar, insbesondere jene für Hochrisiko-KI-Systeme.
- 36 Monate nach Inkrafttreten (voraussichtlich im Juni 2027) werden die Vorschriften für Hochrisiko-KI-Systeme verpflichtend anwendbar.

Wen betrifft die KI-Verordnung?

Die KI-Verordnung richtet sich an eine breite Gruppe von Produzenten und Anwendern in der EU:

- KI-Entwickler und -Anbieter: Das sind Unternehmen und Organisationen, die KI-Systeme in der EU entwickeln oder anbieten.
- Nutzer und Betreiber von KI-Systemen: Unternehmen und Organisationen, die KI-Systeme in der EU nutzen oder betreiben.
- Aufsichtsbehörden und noch zu schaffende nationale Behörden: Das sind in erster Linie die nationalen Behörden in den EU-Mitgliedsländern. Sie werden für die Durchsetzung der Verordnung verantwortlich sein und müssen sicherstellen, dass die in ihren jeweiligen Ländern eingesetzten KI-Systeme die in der Verordnung festgelegten Anforderungen und Pflichten erfüllen. Als übergeordnetes Organ auf EU-Ebene dient der Sonderausschuss zu Künstlicher Intelligenz[1] als Aufsichtsbehörde, welche die nationalen Behörden in allen Belangen anleiten und unterstützen soll.
- Nutzende und Bürger/-innen der EU: Die KI-Verordnung zielt darauf ab, die Rechte und Interessen der Konsument/-innen und Bürger/-innen in der EU zu schützen, die mit KI-Systemen zu tun haben.

Was macht die Schweiz als Nicht-EU-Mitglied?

Die Schweiz gehört nicht zur EU. Dennoch wird die KI-Verordnung auch auf Schweizer Firmen Auswirkungen haben, die am EU-Markt teilnehmen.

Über KI-Regulierungen diskutiert wird auch außerhalb der EU. Die Schweiz ist seit 1963 Mitglied des Europarats, und eine Option ist, dass sie dessen KI-Konvention folgen wird, die sich in Ausarbeitung befindet und im Mai im Ministerkomitee[2] beraten und verabschiedet werden soll. Mit Thomas Schneider hat die Schweiz den Vorsitz („Chair") im KI-Komitee des Europarats inne. Schneider ist Vizedirektor des Bundesamts für Kommunikation. Da dem Europarat unter anderen auch die USA, Kanada, Japan, Israel und Mexiko als Beobachter angehören, dürfte dessen Regelung in ihrer Wirkung über Europa hinausgehen.

In der Schweizer Bundesverwaltung begann man bereits 2016, sich mit dem Potenzial möglicher KI-Anwendungen in der Verwaltung auseinanderzusetzen. 2019 hat die Schweizer Regierung (Bundesrat) eine erste Beurteilung vorgenommen und beschlossen, dass die Schweiz mit einer eigenen KI-Regulierung erst mal abwartet. Zwar wurden dann 2020 interne Richtlinien für die Bundesverwaltung erlassen, die erste Anwendungen möglich machten, um Erfahrungen damit zu sammeln. Ende 2022 wurde man jedoch vom Erscheinen von ChatGPT am Markt überrascht. Der Bundesrat gab in der Folge einen Auftrag zu einem Bericht über die laufenden KI-Regulierungen in

1 https://www.europarl.europa.eu/committees/de/aida/about

2 https://www.euractiv.de/section/innovation/news/ki-konvention-des-europarats-unklare-verpflichtungen-des-privatsektors/

anderen Ländern in Auftrag. Wie das zuständige Regierungsmitglied, Bundesrat Beat Jans, auf einer Veranstaltung der Universität St. Gallen in Zürich ausführte, wird die Regierung aufgrund einer Auslegeordnung Ende November dieses Jahres eine erneute Evaluation zur Notwendigkeit einer KI-Regulierung vornehmen.

Was müssen von der KI-Verordnung betroffene Anwender tun, um KI-Anwendungen rechtssicher einsetzen zu können?

Die Antwort auf diese Fragen lässt sich mit den folgenden vier Phasen beantworten.

1. Phase: Sich eine Übersicht über die bereits eingesetzten KI-Anwendungen verschaffen

Unternehmen und Institutionen sollen zunächst prüfen, ob und wenn ja welche KI-Anwendungen bereits im Einsatz sind, sich noch in Entwicklung befinden oder von externen Anbietern beschafft werden müssen. Dann soll ein Verzeichnis über bereits im Einsatz befindliche oder geplante KI-Modelle erstellt werden. Dazu kann man die Unterlagen der Hersteller benutzen oder muss sich im jeweiligen Geschäftsfeld bei den Anbietern erkundigen.

2. Phase: Risikoeinstufung der KI-Anwendungen anhand der Risikoklassen

Ausgehend vom erstellten Verzeichnis kann eine Risikoeinstufung der KI-Anwendungen aufgrund ihrer Modelle erfolgen. Hochrisiko-KI-Systeme sind gemäß der KI-Verordnung zugelassen, sofern sie gesetzeskonform sind. Um dies festzustellen, ist zu prüfen, ob die gesetzlich vorgeschriebene Transparenzpflicht eingehalten wird. Diese Prüfung erfolgt vor der Markteinführung in der EU durch den Produzenten. Dies bedeutet, dass die Nutzenden darüber informiert sein müssen, dass sie mit von einer KI erzeugten Inhalten interagieren. Als Beispiele hierfür seien Chatbots oder Deepfakes genannt, die nicht als Hochrisiko-Modelle gelten, von denen aber die Nutzenden wissen müssen, dass sie auf KI-Technologien beruhen.

In der Literatur wird empfohlen, dass alle Betreiber von KI-Modellen einen Verhaltenskodex für ethische KI einführen und anwenden.

3. Phase: Vorbereitungsarbeiten vor der Inbetriebnahme der KI-Systeme

Bei Anbietern, Nutzenden, Einführern und Händlern von KI-Systemen muss vor deren Betriebsaufnahme sichergestellt werden, dass die angewandten KI-Praktiken mit der gesetzlichen Regulierung der KI-Verordnung übereinstimmen. Um dies sicherzustellen, sollte die Umsetzung in den folgenden sechs Teilschritten erfolgen: 1. Risikobeurteilung des KI-Systems; 2. Sensibilisierung der Mitarbeitenden, die mit diesen Systemen arbeiten; 3. ethische Regeln ausarbeiten und festlegen; 4. entsprechende Verantwortungen zuweisen; 5. die weiteren Entwicklungen der Technologien und der Rechtsprechung verfolgen; 6. die entsprechenden Regeln der KI-Ethik umsetzen und anwenden.

In Fachkreisen ist es bereits absehbar: Der Aufwand der Unternehmen, um alle Erfordernisse der KI-Verordnung zu erfüllen, wird mindestens so groß wie bei der Einführung der Datenschutz-Grundverordnung der EU sein. Dies kann dazu führen, dass einige Firmen und Institutionen ihre Dateninfrastruktur neu aufsetzen müssen. Ebenso wird eine Verunsicherung bei den Anwendern und Anwenderinnen eintreten und damit eine Vielzahl von Beratungsangeboten erwartet, wie dies bereits bei der DSGVO der Fall war. Im Hinblick auf das Inkrafttreten der KI-Verordnung bereitet sich eine ganze Beraterbranche darauf vor, den Unternehmen und Institutionen bei den geforderten „Risikominderungssystemen" sowie den Protokollierungs- und Dokumentationspflichten zur Seite zu stehen. Aber auch Berufsverbände werden gefordert sein, Entwürfe für Ethikregeln im Umgang mit KI-Systemen bereitzustellen und ihren Mitgliedern Empfehlungen für deren Umsetzung auszusprechen.

Was verspricht sich die EU von der KI-Verordnung?

Die Hoffnung der EU ist, dass die KI-Verordnung Einfluss auf die Gesetzgebung und die Unternehmen außerhalb der EU haben wird, wie dies bei der DSGVO bereits der Fall gewesen ist. Man baut darauf, dass die EU ein attraktiver Markt ist und auch amerikanische und chinesische Konzerne, die KI-Anwendungen entwickeln und anbieten, auf eine Marktteilnahme nicht verzichten möchten. Um nicht Anwendungen nach EU-Standards entwickeln zu müssen, die sich nach Gesetzen in unterschiedlichen Ländern richten, was die Entwicklung erheblich verteuern und zeitlich wesentlich verzögern würde, sollen Eckpunkte der Verordnung weltweit Standards setzen. Ausschlaggebend für die Anbieter ist, wie groß der kommerzielle Erfolg ihrer Systeme in der EU bereits ist oder sein wird. Wenig Einfluss hat dies auf kleine Anwendungen, die speziell für ein Land außerhalb der EU konzipiert wurden. Als Beispiel seien KI-Anwendungen für britische oder amerikanische Behörden genannt, die gleiche Aufgaben wie die deutsche Wirtschaftsauskunftei Schufa in Wiesbaden wahrnehmen. EU-Bürger/-innen sind durch dieses Gesetz auch geschützt, wenn die KI-Anwendung außerhalb der EU zur Verfügung gestellt wird oder wenn sie außerhalb der EU entwickelt wurde.

Stephan Holländer
Lehrbeauftragter, Basel
stephan@stephan-hollaender.ch