Martin-Luther-Universität Halle-Wittenberg
Naturwissenschaftliche Fakultät III
Institut für Informatik

Seminar

Informatik und Gesellschaft

Sommersemester 2025

geleitet durch Prof. Dr. Paul Molitor

Der EU Artificial Intelligence Act

Leonhard Müller & Vincent Kuqi

Inhaltsverzeichnis

1 Einleitung **3**

2 Rechtlicher Hintergrund und Begriffsklärung **4**
2.1 Rechtsakte in der EU 4
2.2 Organe in der europäischen Union 5

3 Überblick über die KI-VO **7**

4 Technische Anforderungen an KI-Systeme **12**
4.1 Begriffsklärung: KI-System und KI-Modell 12
4.1.1 Merkmale von KI-Systemen gemäß der KI-VO 14
4.1.2 Detaillierte Untersuchung der Definition: KI-System 16
4.2 Risikobasierter Ansatz der EU-KI-VO 19
4.2.1 KI-Systeme mit inakzeptablem Risiko: Verbotene Praktiken . . 19
4.2.2 Hochrisiko-Systeme 22
4.2.3 KI-Systeme mit begrenztem und geringem Risiko: 24
4.3 GPAI-Modelle 25
4.3.1 Rechtliche Anforderungen an GPAI-Modelle 25
4.3.2 Systemische Risken und die Gleitkommaschranke von 10^{25} . . . 26

5 Diskussion **28**
5.1 Wirtschaftliche und Gesellschaftliche Auswirkungen 28
5.2 Auswirkungen auf Informatikerinnen 30

6 Fazit **31**

Gender-Hinweis: Die männliche Form ist der weiblichen Form in dieser Arbeit gleichgestellt; lediglich aus Gründen der Vereinfachung wurde die weibliche Form gewählt. Definitionen und Fachbegriffe sind davon ausgenommen.

1 Einleitung

Künstliche Intelligenz (KI) hat sich in den letzten Jahren von einer Nischentechnologie zu einem zentralen Bestandteil der digitalen Gesellschaft entwickelt. Anwendungen reichen von Sprachassistenten und Empfehlungssystemen bis hin zu medizinischer Diagnostik und autonomen Fahrzeugen. Mit dieser rasanten Entwicklung gehen jedoch auch erhebliche Risiken einher, etwa im Hinblick auf Datenschutz, Diskriminierung, Transparenz und die Sicherheit der Nutzerinnen und Nutzer.
Vor diesem Hintergrund hat die Europäische Union den sogenannten *Artificial Intelligence Act* (AI Act) entworfen. Wir werden den deutschen Kurzbegriff: KI-Verordnung in dieser Arbeit mit **KI-VO** abkürzen. Das Ziel der Verordnung ist es, ein rechtlich verbindliches Rahmenwerk zu schaffen, das sowohl die Innovationskraft in Europa stärkt als auch Grundrechtsgüter wie Persönlichkeits- und Freiheitsrechte schützt.
Diese Arbeit beschäftigt sich mit den zentralen Aspekten der KI-VO aus informationstechnischer, gesellschaftlicher und juristischer Sicht. Darauf aufbauend wird der Einfluss der Regulierung auf Gesellschaft, Wirtschaft und Forschung diskutiert.
Informatikerinnen tragen eine besondere gesellschaftliche Verantwortung. Eine gründliche Auseinandersetzung mit den, möglicherweise auch negativen Folgewirkungen, der eigens entwickelten Softwareprodukte oder Technologien war schon immer ein wichtiger Bestandteil dieses Berufs. Mit der KI-VO kommen neue rechtliche Rahmenbedingungen hinzu, deren wesentliche Inhalte Informatikerinnen, welche sich an der Entwicklung von KI-Systemen beteiligen, dies planen oder mit der Thematik konfrontiert werden, bekannt sein sollten. Es soll ein Ziel dieser Hausarbeit sein, die wesentlichsten Punkte der KI-VO zu vermitteln, ohne dass dafür spezielle juristische Fachkenntnisse vorausgesetzt werden. Nach einer Einführung in die Grundzüge der Verordnung, insbesondere das zentrale Prinzip der Risikoklassifizierung folgt eine detaillierte Betrachtung ausgewählter Themenbereiche. Lesende sollen ein Bewusstsein dafür erhalten, unter welchen Umständen ein Softwareprodukt ein KI-System gemäß der KI-VO sein könnte, und welche rechtlichen Folgen sich daraus ergeben. Aus diesem Grund liegt ein inhaltlicher Schwerpunkt auf der detaillierten Analyse der Legaldefinition von KI-Systemen in der KI-VO, also wann ein Software-System überhaupt per Gesetz als KI-System gilt. Dabei wird die Definition interdisziplinär aus verschiedenen Blickwinkeln betrachtet und analysiert. Ein weiterer Schwerpunkt sind die in der KI-VO selbst festgelegten Ausnahmeregelungen, denn die KI-VO entfaltet in einigen Bereichen keinerlei oder nur eingeschränkte Gültigkeit. Dabei werden verschiedene Literaturmeinungen aus Ge-

setzeskommentierungen aufgearbeitet, womit eine kompakte und zugleich detaillierte Übersicht über diesen Bereich der Verordnung geschaffen werden soll. Die KI-VO beschreibt teilweise auch technische Details, indem sie für einen Trainingsumfang von GPAI-Modellen eine Schranke von 10^{25} Gleitkommaoperationen benennt, womit Festlegungen über die potentielle Leistungsfähigkeit dieser Modelle getroffen werden. Dieser Punkt wird hauptsächlich aus der Perspektive der Informatik beleuchtet. Es ist keine Übertreibung zu sagen, dass die KI-VO die Rolle der künstlichen Intelligenz in der Rechtsordnung revolutioniert, schließlich handelt es sich um das weltweit erste verabschiedete Gesetz in diesem Bereich [19]. Im Verlauf dieser Arbeit werden einige Stärken und Schwächen der KI-VO aufgezeigt, welche beide in einer abschließenden Diskussion bewertet werden sollen.

2 Rechtlicher Hintergrund und Begriffsklärung

2.1 Rechtsakte in der EU

Um die Bedeutung der KI-VO zu verstehen, ist es zunächst notwendig, den rechtlichen Rahmen der Europäischen Union zu betrachten. Die organisatorische Grundlage für heutige Gesetzgebungsverfahren bildet der Vertrag von Lissabon, der am 1. Dezember 2009 in Kraft trat. Er stärkte die Gesetzgebungs- und Kontrollrechte des Europäischen Parlaments und legte die Kompetenzen der EU-Institutionen klarer fest.
Ein zentrales Element des EU-Rechts ist die Unterscheidung zwischen **Verordnungen und Richtlinien** [6, Art. 288].
Verordnungen haben allgemeine Geltung, sind in allen Mitgliedstaaten unmittelbar anwendbar und müssen grundlegend nicht erst in nationales Recht umgesetzt werden. Sie sind damit direkt verbindlich für Bürgerinnen, Unternehmen und Behörden [6, Art. 288, Abs. 2]. Ausnahmen können bestehen, wenn explizit ein gewisser Ermessensspielraum eingeräumt wird. Ein Beispiel dafür ist der Ermessensspielraum für EU-Staaten im Umgang mit der verbotenen Praktik der Echtzeit-Gesichtserkennung.
Richtlinien legen lediglich verbindliche Ziele fest, überlassen den Mitgliedsstaaten jedoch die Form und Mittel der Umsetzung. Erst durch nationale Rechtsakte werden sie wirksam [6, Art. 288, Abs. 3]. Verstöße gegen die Umsetzungspflicht können zu finanziellen Sanktionen oder Vertragsverletzungsverfahren führen.
Erwägungsgründe werden in europäischen Rechtsakten oftmals den rechtlich verbindlichen Normen vorangestellt. Diese dienen als Begründung für die jeweiligen Nor-

men [20], und sollen für ein besseres Verständnis dieser beitragen. Auch die KI-VO enthält Erwägungsgründe, auf welche in dieser Arbeit regemäßig Bezug genommen wird.
Die KI-VO ist eine EU-Verordnung und entfaltet damit unmittelbare Geltung in allen Mitgliedstaaten, ohne dass es einer Umsetzung in nationales Recht bedarf. Dies soll sicherstellen, dass ein einheitlicher Rechtsrahmen für KI-Systeme im gesamten Binnenmarkt entsteht und Rechtsfragmentierung vermieden wird. Besonders im Technologiebereich, in dem Unternehmen oft grenzüberschreitend agieren, ist dieser Harmonisierungsansatz von hoher praktischer Bedeutung [6, Art. 179].
Darüber hinaus entfaltet die Verordnung eine extraterritoriale Wirkung. Grundsätzlich gilt die Verordnung für alle KI-Systeme, welche in der EU auf den Markt gebracht werden. Die KI-VO gilt auch, wenn ein KI-System vollständig außerhalb der EU betrieben oder in den Verkehr gebracht wird, sich jedoch faktisch an den EU-Markt richtet und beispielsweise über das Internet in EU-Mitgliedsstaaten verfügbar und nutzbar ist. Die Methoden zur Durchsetzung sind diesbezüglich vielschichtig. Grundlegend ist die EU im Jahr 2025, gemessen am Bruttoinlandsprodukt, die zweitgrößte Volkswirtschaft der Welt [22]. Für Herstellerinnen und Anbieterinnen von KI-Systemen ist dieser Markt oft unumgänglich, was mit entsprechenden Sanktionen als Hebel zur Durchsetzung der Verordnung dienen kann. Auf weitere Details zur Durchsetzung soll an dieser Stelle nicht eingegangen werden.

2.2 Organe in der europäischen Union

Im Verlauf dieser Arbeit wird speziell auf einige Kompetenzen der Europäischen Kommission eingegangen, diese ist ein Organ der EU. Es ist wichtig die Rollen der verschiedenen Organe der Europäischen Union unterscheiden zu können sowie deren grundlegendes Zusammenspiel im Zusammenhang mit der KI-VO zu verstehen. Vor dem Vertrag von Lissabon beschrieb man die Europäische Union oft über ihre drei Grundsäulen (siehe Abbildung 1), welche heute faktisch in die bestehenden Organe integriert sind. Eine Grundlage für Gesetzgebung und Rechtsprechung ist gut erkennbar, und in ihren Grundzügen mit ihrem Pendant auf Staatenebene vergleichbar. Hinzuzufügen ist die Besonderheit, dass allein die Europäische Kommission Gesetzesvorschläge einbringen kann, über welche der Rat der Europäischen Union und das Europäische Parlament dann verhandeln [25]. Formen der Exekutive gestalten sich auf der supranationalen Ebene der EU natürlich anders als auf Staatenebene, teilweise übernimmt auch

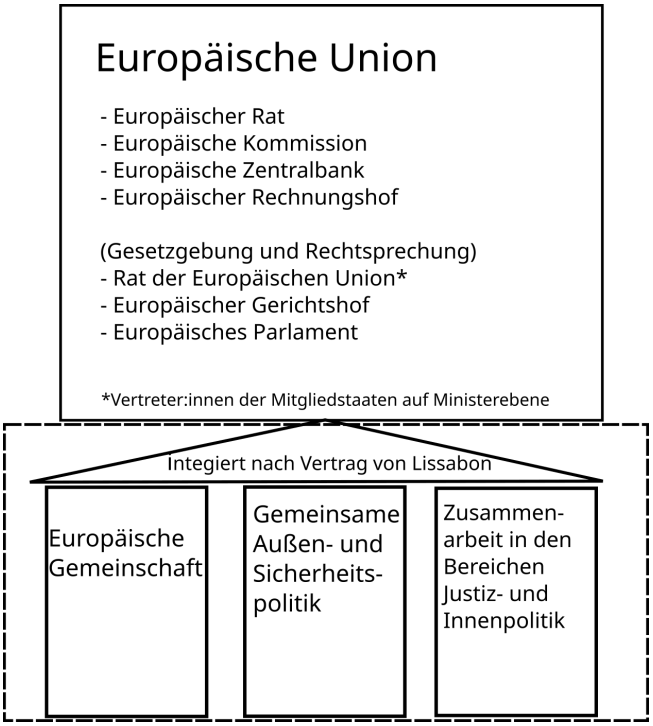

Abbildung 1: Skizze zur Europäischen Union

die Kommission derartige Aufgaben. Weiterhin ist die EU-Kommission für die Haushaltsplanung zuständig, und vertritt die EU auf internationaler Ebene [26]. Die EU-Kommission erlässt außerdem Leitlinien, welche die Mitgliedsstaaten bei der Umsetzung von Rechtsakten unterstützen. Dies ist der Fall für die Klassifikation von verbotenen KI-Praktiken, als auch bei der Auslegung der Definition von KI-Systemen [21] [24]. Diese Leitlinien haben jedoch keine verbindliche Rechtskraft, sondern sind eher als Hilfestellungen und Empfehlungen zu betrachten. Im Einzelfall entscheidet der Europäische Gerichtshof über etwaige Auslegungen [24], dessen Entscheidungen entfalten wie bei gerichtlichen Entscheidungen auf Staatenebene eine richtungsweisende Wirkung. Der EU-Kommission untergegliedert ist das KI-Büro, welches eine zentrale Koordinierungs- und Überwachungsfunktion für die KI-VO übernimmt.
Die übrigen Organe der EU sind für die in dieser Arbeit geführten Diskussionen und Erläuterungen zur KI-VO nicht von zentraler Bedeutung, weshalb auf weitere Erklärungen verzichtet wird. Diese werden jedoch der Vollständigkeit wegen in der Skizze erwähnt.

3 Überblick über die KI-VO

Die KI-VO (offiziell: Verordnung zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz) ist der erste umfassende Rechtsrahmen für KI-Systeme weltweit. Er wurde von der Europäischen Kommission im April 2021 vorgeschlagen und im Jahr 2024 verabschiedet [7, 23]. Die Verordnung verfolgt mehrere zentrale Ziele: die Gewährleistung des reibungslosen **Funktionierens des Binnenmarktes**, den **Schutz von Gesundheit, Sicherheit und Grundrechten** vor negativen Auswirkungen von KI-Systemen sowie die Förderung einer **menschenzentrierten und vertrauenswürdigen KI** [7, Art. 1].
Diese Arbeit widmet sich hauptsächlich der entfaltenden Schutzwirkung der KI-VO. Art. 1 Abs. 1 der KI-VO macht diesbezüglich die Zielstellung der Verordnung deutlich, diese soll Schutz bieten vor Risiken für Gesundheit, Sicherheit und Grundrechten sowie für kollektive Rechtsgüter wie Demokratie, Rechtsstaatlichkeit und Umweltschutz ausgehend von KI-Systemen.
Zentral ist dabei durchgehend der **risikobasierte Ansatz**. Dazu gehört die Einteilung von KI-Systemen und KI-Modellen in bestimmte Risikoklassen. Verallgemeinert lässt sich sagen, je mehr Risiken ein KI-System oder KI-Modell für die oben genannten Rechtsgüter birgt, desto mehr Regularien trifft die KI-VO. Dies reicht von gänzlich entfallenden Vorschriften bis hin zum Verbot einiger Praktiken.
Wesentliche Inhalte der KI-Verordnung sind die folgenden [16, S. 3]

- Harmonisierte Vorschriften für Inverkehrbringen und Verwendung von KI-Systemen in der Union [7, Art. 1]
- Explizite Verbote bestimmter Praktiken [7, Art. 5]
- Hochrisiko-KI-Systeme Besondere Anforderungen und Pflichten für zugehörige Akteure [7, Art. 6 ff.]
- Transparenzvorschriften für bestimmte KI-Systeme [7, Art. 50]
- Transparenz für KI-Modelle mit allgemeinem Verwendungszweck [7, Art. 51 ff.]
- Marktüberwachung Vorschriften zur Marktbeobachtung, Governance, Durchsetzung [7, Art. 54 ff.]
- Innovationsförderung Maßnahmen für KMU und StartUps [7, Art. 57 ff.]

Der risikobasierte Ansatz der KI-VO unterteilt KI-Systeme in die folgenden **vier Risikoklassen** [16, S. 4]:

- **Inakzeptables Risiko:** Systeme, deren Einsatz mit erheblichen Gefahren für Sicherheit und Grundrechte verbunden ist (z. B. Social Scoring, Echtzeit-Gesichtserkennung im öffentlichen Raum). Diese Praktiken sind verboten [7, Art. 5].
- **Hohes Risiko:** Systeme in sicherheitskritischen Bereichen wie Biometrie, kritische Infrastrukturen oder Strafverfolgung. Sie sind zulässig, unterliegen jedoch strengen technischen und organisatorischen Anforderungen [7, Art. 6].
- **Begrenztes Risiko:** Systeme mit moderatem Risiko, für welche Transparenzpflichten gelten [7, Art. 50].
- **Minimales Risiko:** Systeme ohne signifikantes Gefahrenpotenzial, für die keine verbindlichen Pflichten vorgesehen sind [7, Art. 9].

Neben der Risikoklassifizierung benennt die Verordnung verschiedene **Adressaten**, unter anderem **Anbieter, Betreiber**, Importeure und Händler. Dabei handelt es sich jeweils um die Rolle eines Akteurs im Zusammenhang mit KI-Systemen. Für jeden dieser Adressaten sind spezifische Pflichten definiert, die sowohl technische Spezifikationen (z. B. Genauigkeit, Robustheit, Cybersicherheit) als auch organisatorische Maßnahmen (z. B. Risikomanagement, Dokumentationspflichten) umfassen. So gelten *Software-Entwicklerinnen* zumeist als *Anbieter* der KI-Systeme bzw. -Modelle, sowie die *Bereitstellenden oder Nutzer des Systems* als *Betreiber*, wobei dies stark von der Art des KI-Systems abhängt, ob dieses vollständig öffentlich oder beispielsweise firmenintern verwendet wird. Anbieter und Betreiber erhalten dabei in der KI-VO die meisten verpflichtenden Regulatorien. Dabei handelt es sich auch um jene Regulierungen, welche im Verlauf der Arbeit hauptsächlich behandelt werden.

Ausnahmeregelungen

Die KI-VO selbst sieht in Art. 2 auch Ausnahmeregelungen für KI-Systeme und deren Betrieb vor. Diese umfassen folgende Anwendungsbereiche:

- KI-Systeme, die ausschließlich für **Militär, Verteidigung oder nationale Sicherheit** eingesetzt werden
- **Forschungs-, Test- und Entwicklungszwecke**
- **Open-Source-Systeme**
- **Persönliche Nutzung im persönlichen oder familiären Umfeld**

Ausnahme Militär und nationale Sicherheit nach Art. 2 Abs. 3

Die KI-VO sieht gemäß Art. 2 Abs. 3 eine gänzliche Ausnahme für KI-Systeme vor, die ausschließlich für militärische Zwecke, Verteidigungszwecke oder Zwecke der nationalen Sicherheit verwendet werden, unabhängig davon, ob diese Systeme nun innerhalb oder außerhalb der EU betrieben werden. Der erste Satz des Absatzes 3 stellt dabei klar, dass die EU keine Regulatorien bezüglich der nationalen Sicherheit ihrer Mitgliedsstaaten trifft. Eine Zweckentfremdung beispielsweise für den Bereich der Strafverfolgung oder öffentlichen Sicherheit hebt diese Schutzwirkung jedoch auf [17, S. 227, Rn 54]. Die nationale Sicherheit wird auch als äußere Sicherheit bezeichnet und dient dem Schutz, wenn es um die Abwehr von Bedrohungen geht, die sich von außen gegen den Staat und seine Entwicklungsfähigkeit richten. Die innere Sicherheit (oder öffentliche Sicherheit) gilt der Abwehr von Gefahren, die ihren Ursprung innerhalb des Staates haben. Historisch und konzeptionell ist die deutsche Sicherheitspolitik von einer Trennung der beiden Felder geprägt. [27] Der Einsatz von KI-Technologien beispielsweise von Behörden im Rahmen der inneren Sicherheit, speziell den Strafverfolgungsbehörden erscheint derzeit von großem öffentliche Interesse. So ist die umstrittene US-Software Palantir mit Stand vom 14.04.2025 bereits bei den Polizeien der Bundesländer Bayern, Hessen und Nordrhein-Westfalen im Einsatz. [28]. In der Polizei Hessen galt die Software im Juni 2025 bereits als „Kernstück der Ermittlungsarbeit“ [29]. Im Wesentlichen soll die Software zur Datenanalyse dienen, und dabei nicht nur Verknüpfungen zwischen polizeilichen und sonstigen Datenbanken oder Datensammlungen schließen, sondern diesbezüglich auch die notwendigen Schlüsse für ein Ermittlungsverfahren, wie relevante Zusammenhänge und Muster automatisiert liefern. [30] Da die Strafverfolgungsbehörden in der Bundesrepublik, damit auch sämtliche Polizeien der Länder und des Bundes, nur zum Zwecke der Strafverfolgung oder zur Aufrechterhaltung der inneren Sicherheit tätig werden, erscheint diese Ausnahme gemäß Art. 2 Abs. 3 ausgeschlossen. Auch wenn der Fokus des öffentlichen Interesses teilweise auf den einzelnen Behörden selbst liegt, stellt Art. 2 Abs. 3 zusätzlich klar, dass die Tätigkeit oder Kerntätigkeit der Einrichtung, welche ein KI-System anwendet keine Rolle bei dieser Ausnahmeregelung spielt. Entscheidend ist ob die Software im Einzelfall ausschließlich für militärische Zwecke, Verteidigungszwecke oder Zwecke der nationalen Sicherheit eingesetzt wurde. Damit sollen vermutlich Komplikationen vermieden werden, zum Beispiel in Behörden wie den Verfassungsschutzbehörden (Inlandsgeheimdienst in Deutschland) zu deren Aufgabe auch die Abwehr und Verhinderung von Auslandsspionage gehört, und welche

sich wohl zu diesem Zwecke beim Einsatz von KI-Systemen auf die Ausnahme des Art. 2 Abs. 3 KI-VO berufen könnten. Der Verfassungsschutz ist jedoch auch im Bereich der inneren Sicherheit tätig, und kann Strafverfahren beim Generalbundesanwalt anregen [31].
Abschließend kann also gesagt werden, dass mindestens die Anwendung von KI-Systemen bei den Polizeien und anderen Strafverfolgungsbehörden ausnahmslos unter die Regularien der KI-VO fallen dürfte, aufgrund der Zweckgebundenheit dieser Behörden an die innere Sicherheit. Die Ausnahmeregelung nach Art. 2 Abs. 3 bestimmt sich alleinig über den Zweck der Nutzung des jeweiligen KI-Systems und richtet sich nicht nach der Einrichtung, welche das KI-System einsetzt. Jede Einrichtung, welche im Einzelfall unter den Voraussetzungen des Art. 2 Abs. 3 tätig wird, ist in diesem Fall von der KI-VO ausgenommen.

Ausnahme Forschungs-, Test- und Entwicklungszwecke nach Art. 2 Abs. 6 und Art. 2 Abs. 8

Diese beiden Absätze werden hier für eine bessere Verständlichkeit gemeinsam betrachtet und gegenübergestellt.

- **Art. 2 Abs. 6** umfasst den Einsatz von KI-Systemen zu **allgemeinen** Forschungs-, und Entwicklungszwecken in jedem wissenschaftlichen Bereich. Die Ausnahme dient damit hauptsächlich der Wahrung der Freiheit der Wissenschaft.
- **Art. 2 Abs. 8** umfasst Forschungs-, Test- und Entwicklungstätigkeiten **explizit von KI-Systemen** vor deren Inbetriebnahme oder Inverkehrbringen. Damit gilt die Ausnahme in erster Linie der Innovationsförderung im Bereich von KI.

Notwendige Voraussetzung für **Art. 2 Abs. 6** ist, dass ein KI-System von Beginn an sowie alleinig zum Zwecke der Forschung und Entwicklung entwickelt und in Betrieb genommen wurde. Der Betrieb von KI-Systemen, welche zusätzlich zu anderen Zwecken verwendet oder entwickelt wurden, ist nicht von der Ausnahme erfasst [17, S. 230, Rn 66]. Der Hintergrund dieser Ausnahme sollte in der Verfassungskonformität der KI-VO liegen. Bei gewünschter Schutzwirkung muss die KI-VO gleichermaßen im Einklang mit bereits gültigen Gesetzen, an erster Stelle natürlich den Verfassungen der EU-Mitgliedsstaaten stehen. In Deutschland ist die Wissenschaftsfreiheit nach *Art. 5 Abs. 3 S. 1, 2. Alternative* des Grundgesetzes geschützt [32]. Jede Regulierung der KI-VO würde einen Eingriff in die Wissenschaftsfreiheit darstellen, womit mittels der Ausnahmeregelung des Absatzes 6 entgegengewirkt wird.

Der **Art. 2 Abs. 8** zieht hingegen eine klare Trennlinie für KI-Systeme vor, und nach deren Teilnahme am EU-Binnenmarkt. Es handelt sich also um eine gänzliche andere Art von Ausnahmeregelung. Vor der Teilnahme, also vor dem Inverkehrbringen eines KI-Systems trifft die KI-VO noch keine Regulierungen [17, S. 232, Rn 78]. Ausdrücklich ausgenommen von dieser Ausnahme sind Tests unter Realbedingungen [17, S, 232, Rn 79]. Die Ausnahme vermeidet damit standortbedingte Nachteile für Anbieter von KI-Systemen in der EU. Ohne einer solchen Ausnahmeregelung hätten Entwicklerinnen von KI-Systemen außerhalb der EU vor dem Inverkehrbringen eines KI-Systems möglicherweise mildere Regularien, und damit einen Vorteil. Die Ausnahmeregelung nach Absatz 8 dient damit der Innovations- und Standortgerechtigkeit, und soll einen globalen fairen Wettbewerb sichern

Betrieb für persönliche Zwecke Art. 2 Abs. 10

Diese Ausnahmeregelung gilt speziell für Betreiber von beliebigen KI-Systemen und findet Anwendung, insofern die Verwendung von KI-Systemen oder Modellen ausschließlich für private Zwecke geschieht. Dafür liefert die KI-VO selbst keine Beispiele, und es erscheint schwierig mögliche hypothetische Beispiele zu finden. Als Orientierung für eine Abgrenzung zwischen ausschließlich privater und beruflicher Tätigkeit kann hier der Vergleich zum *Haushaltsprivileg* der DGSVO gezogen werden. Darunter fiele dann jede Verwendung zu privaten oder familiären Zwecken [17, S. 234, Rn 88]. Die Ausnahme kann damit nur für natürliche Personen, und nicht für juristische Personen wie zum Beispiel Firmen gelten. Die Nutzung von privaten Endgeräten für berufliche Zwecke führt nach gängiger Annahme nicht zum Greifen der Ausnahmeregelung [14, 1. Kapitel, Rz47]. Gleichermaßen könnte nach dieser Auffassung der Betrieb auf Servern von dritten Personen ausgelagert werden, wobei es sich nicht um natürliche Personen handeln muss.
Entscheidend erscheint ausschließlich der private Zweck des Betreibens, und damit auch ein Ausschluss von Dritten, wenn abzusehen ist, dass diese das System für nicht private Zwecke nutzen oder betreiben werden. Dies könnte beispielsweise durch eingeschränkte Zugriffsrechte auf das KI-System erfolgen.

Ausnahme Open-Source-Modelle Art. 2 Abs. 12

Eine eingeschränkte Ausnahmeregelung genießen auch Open-Source-Modelle, also KI-Modelle mit freien und quelloffenen Lizenzen [39].

Diese Einschränkung gilt jedoch nicht für Hochrisiko-Systeme, oder gar den Bereich der verbotenen Praktiken. Ebenfalls erfolgt keine Rücknahme von einigen bestimmten kritischen Transparenzpflichten, insbesondere im Bereich von synthetischen Inhalten [17, S. 236, Rn 96]. Der Absatz 12 schafft also keine weitreichenden Ausnahmeregelungen, sondern bringt lediglich Erleichterung in Bezug auf die weniger kritischen Transparenzpflichten der KI-VO. Dies erscheint nachvollziehbar, da mögliche Risiken, auch jene von kritischen Systemen ungeachtet von Quelloffenenheit oder der Art der Softwarelizenzen existieren. Ebenso können auch freie, quelloffene KI-Systeme täuschend echte synthetische Inhalte erzeugen, deren Verbreitung selbstverständlich gleichermaßen durch die KI-VO reguliert werden sollte.
Die Ausnahmeregelung nach Absatz 12 hilft damit der Ermöglichung des Fortbestehens, sowie der Förderung von freien Open-Source-Projekten. Die Grundbedingungen und Parameter in solchen Projekten sind oftmals anderes als in kommerziellen, hochmonetarisierten Projekten. Zu starke Regulierungen der KI-VO könnten diese Projekte gefährden, unattraktiv gestalten und somit langfristig diesen bereits in ihrer Entstehung entgegenwirken. Ferner ist zu erwarten, dass freie Open-Source-Produkte künftig das geforderte Maß an Transparenz verschiedener Vorschriften, einschließlich der KI-VO, tendentiell überschreiten werden. Von daher birgt die Ausnahmeregelung in ihrer Ausgestaltung keine offensichtliche Schwächung der Schutzwirkung der KI-VO.

4 Technische Anforderungen an KI-Systeme

4.1 Begriffsklärung: KI-System und KI-Modell

Im Rahmen der KI-VO versteht man unter einem KI-System ein *maschinengestütztes System*, das so konzipiert ist, dass es mit unterschiedlichem Grad an *Autonomie* betrieben werden kann, nach seiner Einführung *Anpassungsfähigkeit* zeigt und aus den Eingaben, die es erhält, explizite oder implizite Ziele *ableitet*, um Ausgaben wie Vorhersagen, Inhalte, Empfehlungen oder Entscheidungen zu generieren, die *physische oder virtuelle Umgebungen beeinflussen* können [7, Art. 3, Abs. 1].
Auf die genauen Bestandsmerkmale eines KI-Systems wird im Kapitel 4.1.1 eingegangen. Zunächst wollen wir zwischen

- **KI-Modell**
- **GPAI-Modell** gemäß Art. 3 Abs. 63

- **GPAI-Systems** gemäß Art. 3 Abs. 66

unterscheiden.
Bei einer Abgrenzung zwischen den Begriffen können die Konzepte aus dem Software-Engineering helfen:

- Unter einem KI-**System** kann man sich das **fertige Produkt im Softwarelebenszyklus** vorstellen. Dieses fertige Produkt kann in Verkehr gebracht, betrieben und genutzt werden.

Der Begriff des KI-Modells ist in der KI-VO nicht legaldefiniert. Lässt sich jedoch wie folgt erklären:

- Ein KI-**Modell** kann als **Komponente oder Microservice** eines Softwareproduktes aufgefasst werden. In jedem Fall ist es **maximal entkoppelt** *(im Sinne des SW-Engineerings)* vom restlichen Softwaresystem, und kann in verschiedenen KI-/ beziehungsweise Softwaresystemen verwendet werden.

Auf dieser Grundlage lässt sich der legaldefinierte Begriff des GPAI-Modells (KI-Modell mit allgemeinem Verwendungszweck) einordnen. Es handelt sich um besondere KI-Modelle, welche die Bestandsmerkmale des Art. 3 Abs. 63 erfüllen. Diese Merkmale wurden im folgenden Absatz hervorgehoben:

- Ein GPAI-**Modell** ist eine spezielle Form eines KI-Modells, mit **erheblicher allgemeiner Verwendbarkeit**, welches **unabhängig von der Art und Weise seines Inverkehrbringens ein breites Spektrum unterschiedlicher Aufgaben kompetent erfüllt,** sowie **in eine Vielzahl nachgelagerter Systeme oder Anwendungen integriert werden kann**.

Abschließend betrachten wir den Begriff des **GPAI**-Systems (KI-System mit allgemeinem Verwendungszweck) gemäß Art. 3 Abs. 66:

- Ein GPAI-**System** ist eine spezielle Form eines KI-Systems, welches auf einem **GPAI-Modell** beruht.

Der Art. 3 Abs. 66 fordert zusätzlich, dass ein GPAI-System *in der Lage ist, einer Vielzahl von Zwecken sowohl für die direkte Verwendung als auch für die Integration in andere KI-Systeme zu dienen.* Damit wird eine breite Verwendbarkeit auch für das GPAI-System selbst, nicht nur für das zugrundeliegende GPAI-Modell gefordert. Warum vom Gesetzgeber zusätzlich die Fähigkeit der Integration in andere KI-Systeme gefordert wird, erscheint nicht unmittelbar ersichtlich. Man dürfte sich hier erneut auf die breite Anwendungsmöglichkeit von GPAI-Systemen beziehen, um diese damit von

KI-Systemen mit sehr spezieller Funktionalität unterscheiden zu können. Die Integrierbarkeit im Sinne des Software-Engineerings, speziell der damit verbundene technische Aufwand, dürfte nicht gemeint sein.

4.1.1 Merkmale von KI-Systemen gemäß der KI-VO

Die Definition eines KI-Systems gemäß der KI-VO orientiert sich an der Definition der OECD [41], tatsächlich sind die Definitionen der KI-VO und der OECD, mit Ausnahme eines Zusatzmerkmals (autonomer Betrieb), identisch. Insgesamt ergeben sich nach Art. 3 Abs. 1 der KI-VO die folgenden fünf folgenden Tatbestandsmerkmale für KI-Systeme:

- **maschinengestütztes** System
- in unterschiedlichem Grade ausgelegt für **autonomen Betrieb**
- **Anpassungsfähigkeit** nach Inbetriebnahme
- **Ableitungsfähigkeit**
- kann physische oder virtuelle Umgebungen **beeinflussen**

Der Begriff **maschinengestützt** umfasst hier jede Form von funktionsfähigen Software- oder Hardwareprodukten.

Die Definition der KI-VO ergänzt die Variante der OECD um das Merkmal des **autonomen Betriebs**. Nach Erwägungsgrund 12 bedeutet dies, *dass sie bis zu einem gewissen Grad unabhängig von menschlichem Zutun agieren und in der Lage sind, ohne menschliches Eingreifen zu arbeiten* [33]. Eine nachvollziehbare Annahme für die zusätzliche Forderung ist, dass Systeme verschiedenster Autonomiestufen von der Definition erfasst sein sollen [15, S. 156, Rn 30]. Konkret bedeutet dies, dass von völlig unautonomen und permanent menschlich gesteuerten Systemen bis hin zu gänzlich autark laufenden Systemen alle Varianten eingeschlossen wären. Nach dieser Auffassung handelt es sich nicht um eine strenge zusätzliche Forderung, welche kaum Systeme ausschließen sollte. Diese Ansicht steht auch mit dem zentralen Prinzip des risikobasierten Ansatzes der Verordnung im Einklang. Hochriskante KI-Systeme müssen nicht zwangsläufig autonom betrieben werden können.

Bei der **Anpassungsfähigkeit** handelt es sich um eine Kann-Bestimmung. Das heißt im Wortlaut, dass dieses Merkmal nicht vorhanden sein muss, damit ein System als

KI-System gemäß der KI-VO gilt. Es dürfte sich also eher um ein Merkmal zur Veranschaulichung handeln [15, S. 156, Rn 30]. Im Erwägungsgrund 12 bezieht man sich auf die **mögliche Lernfähigkeit** eines Systems, welches dieses **während der Verwendung** verändern kann [33]. Dies betrifft beispielsweise die Fähigkeit eines Systems, durch Lernen nach der Inbetriebnahme seine Leistungsfähigkeit zu steigern.

Ableitungsfähigkeit umfasst nach Erwägungsgrund 12 Prozesse, die über **einfache Datenverabeitung** hinausgehen, und damit die Ermöglichung von **Lern-, Schlussfolgerungs- und Modellierungsprozessen** durch das System. Dies umfasst die Fähigkeit eines Systems **Vorhersagen, Inhalte, Empfehlungen oder Entscheidungen, [...], Modelle oder Algorithmen** anhand einer Nutzereingabe oder gegebenen Daten abzuleiten. Dabei erfolgt auch die Bezugnahme auf Techniken wie **maschinelles Lernen, sowie logik- und wissensgestützte Konzepte**. Der Formulierung im Erwägungsgrund 12 ist zu entnehmen, dass diese Aufzählung von Techniken nicht abschließend ist [33]. Als klares Unterscheidungsmerkmal dürfte die *einfache Datenverabeitung* zu verstehen sein. Beschränkt sich ein Softwaresystem darauf, so ist eine Ableitungsfähigkeit mit Sicherheit abzulehnen. Wann genau lediglich eine *einfache Datenverabeitung* vorliegt, ist strittig und wird anhand eines konkreten Beispiel zu mathematischen Regressionsmethoden im Kapitel 4.1.2 diskutiert. Die im Erwägungsgrund genannten Techniken: *maschinelles Lernen, sowie logik- und wissensgestützte Konzepte* sollten jedoch ein guter Indikator sein, ob ein System über die *einfache Datenverarbeitung* hinausgeht. Die bloße Verwendung dieser Techniken allein kann dem Erwägungsgrund 12 folgend, noch keine Ableitungsfähigkeit begründen. Dort werden diese als Techniken benannt, welche ein *Ableiten ermöglichen.*

Die Fähigkeit der **Beeinflussung physischer oder virtueller Umgebungen** kann restriktiv erscheinen, insbesondere da der überwiegende Teil von praktisch eingesetzter Software nicht unmittelbar das physische Umfeld, beispielsweise mit einem Roboterarm oder Vergleichbarem, beeinflusst. Entscheidend für das Vorliegen diese Merkmals dürften aber bereits **physische Kausalzusammenhänge** sein, zum Beispiel wenn ein Mensch einer KI-Handlungsempfehlung folgt [11, Gless/ Janal, S. 22, RN 24]. Die Beeinflussung virtueller Umgebungen ist wahrscheinlich bereits mit jeder Software- oder Komponentenschnittstelle gegeben.

4.1.2 Detaillierte Untersuchung der Definition: KI-System

Eine detaillierte Betrachtung der Definition zeigt auf, dass diese sowohl sehr präzise, als auch funktional getroffen wurde [13]. Das bedeutet, dass die Funktionalität des Systems im Vordergrund steht. Damit wird auch klar, die rein technische Umsetzung (oder Implementierung) für sich betrachtet, erscheint für die Definition eines KI-Systems weitestgehend nebensächlich. Ein verdeutlichendes Extrembeispiel wäre die Addition zweier beliebiger natürlicher Zahlen unter Nutzung der Vorhersage eines künstlichen neuronalen Netzes. Ein Programm, das dies und nur dies auf genannte Art und Weise leistet, zählt dann per Definition nicht als KI-System. Die Funktionalität beschränkt sich schließlich auf die Addition zweier natürlicher Zahlen, dies lässt sich nicht unter den Merkmalen eines KI-Systems subsumieren.
Eine Kombination aus einem hohen Grad an Präzision und Funktionalität hat zur Folge, dass die aktuelle Definition eines KI-Systems in der KI-VO sehr weitreichend ist [13]. Dies erscheint aus verschiedenen Blickwinkeln sinnvoll und lässt die Vermutung zu, dass diese bewusst vom Gesetzgeber so gewählt wurde. Sie deckt eine Vielzahl an Systemen ab und lässt keine semantischen Lücken, die durch eine geschickte Wahl von Programmfunktionalität oder Funktionalitätsbeschreibung umgangen werden könnte. Es werden keine Hintertüren durch technische Lücken geöffnet, so lässt sich die Definition nicht durch den Einsatz von Nischentechnologien umgehen. Gleichermaßen werden auch künftige Technologien und Entwicklungen abgedeckt.
Allerdings können damit auch ältere Softwaresysteme und Technologien unerwartet unter den Begriff des KI-Systems fallen. Dies verdeutlichen die Leitlinien der EU-Kommission [21], welche explizit *Systeme zur Verbesserung der mathematischen Optimierung oder zur Beschleunigung und Annäherung traditioneller, gängiger Optimierungsmethoden wie* ***lineare oder logistische Regressionsmethoden*** vom Anwendungsbereich der Definition ausnehmen und diese als nicht über den Bereich der *grundlegenden Datenverarbeitung hinausgehend* einordnen. Vor dem Hintergrund der hier geführten Diskussion über die potentielle Einklassifizierung älterer und konsolidierter Systeme als KI-System, könnte es sich dabei um eine Art Klarstellung bezüglich deren Einordnung handeln. Die einfachste Form der linearen Regression im eindimensionalen Raum soll zunächst kurz zur Verdeutlichung angesprochen werden.
Im Beispiel von Abbildung 2 sind die Funktionseingabewerte $\{1, 2, 3, 4, 6\}$ gegeben. Der Wert für $x = 5$ fehlt. Mittels linearer Regression lässt sich ein Funktionswert $f(5) \approx 10,09$ vorhersagen. Die abgebildete Gerade ist die sogenannte Regressions-

gerade. Diese wurde so bestimmt, dass *alle* bekannten Funktionswerte so wenig wie möglich von dieser abweichen. Diese Abweichung wird häufig auch Kostenfunktion genannt, welche im Verfahren minimiert wird. Die Suche nach einem Minimum unter verschiedenen Parametern, hier Startpunkt und Anstieg der Gerade, ist ein klassisches *Optimierungsproblem*. Dieses Verfahren ist vermutlich bereits seit den 90er Jahren in der bekannten Software Microsoft Excel implementiert [34]. Mit diesem erklärenden Beispiel lassen sich natürlich keine beeindruckenden Vorhersagen treffen, es bildet jedoch die Grundlage für die Verallgemeinerung auf höhere Dimensionen oder Daten, welche nicht linear korrelieren.

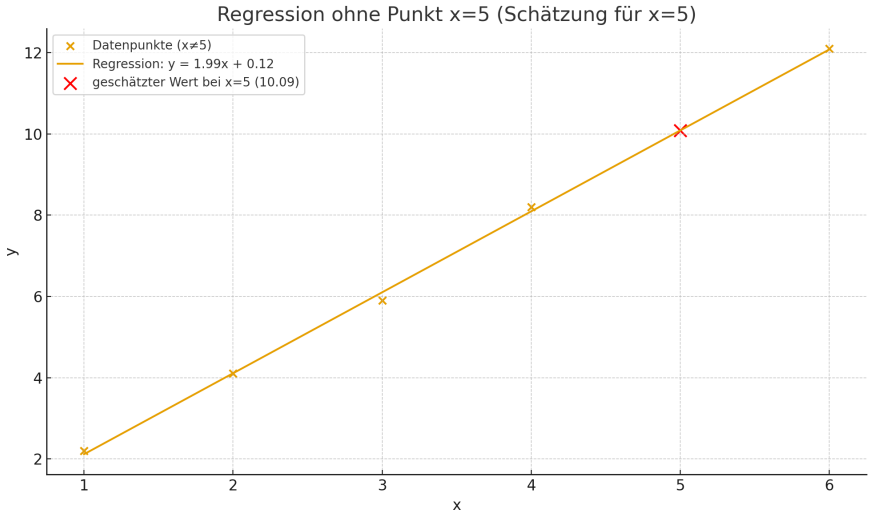

Abbildung 2: Ein sehr einfaches Beispiel für lineare Regression

Würde man entgegen der EU-Leitlinien also genannte Regressionsverfahren, einschließlich Systeme, die unser Beispiel in Abbildung 2 lösen, als KI-System klassifizieren, dann wäre streng genommen jegliche Form von Interpolation (Bestimmen von Funktionswerten zwischen bekannten Eingabewerten) oder Extrapolation (Bestimmen von Funktionswerten größer oder kleiner als bekannte Eingabewerte) eine Form von *Ableitungen treffen* gemäß der KI-Verordnung. Die exakte analytische Berechnung folgt jedoch strikt einem mathematischen Verfahren, welches im Falle einer eindeutigen Regressionsgleichung über den Eingabedaten zusätzlich deterministisch ist und entzieht sich damit dem Charakter der Ableitungsfähigkeit im Sinne einer künstlichen Intelligenz. Dies macht die Positionierung der EU-Kommission als *grundlegende Datenverarbeitung*

nachvollziehbar.
Entscheidend erscheint zusätzlich der gewählte Kontext der Leitlinie im Zusammenhang mit *Systemen zur Verbesserung der mathematischen Optimierung*. Die Ausführungen der Richlinien dürften dahingehend so zu deuten sein, dass hier das Lösen eines Optimierungsproblems *innerhalb* eines Regressionsverfahrens gemeint ist, in unserem Beispiel das Finden einer Gerade mit möglichst geringem Abstand zu allen Punkten. Weiterhin wird der Begriff der Heuristik erwähnt, wobei es sich um Lösungsverfahren handelt, welche nicht immer die beste Lösung eines Optimierungsproblems, aber eine möglichst gute Lösung (oder annähernd optimale) Lösung liefern und zugleich wesentlich effizienter durchgeführt werden können.Man könnte beispielsweise in Abbildung 2 auch einfach eine Gerade ziehen, welche den ersten und letzten Wert (hier $x = 1$ und $x = 6$) schneidet. Man würde hier eine ähnlich gute Lösung erhalten, ohne dass es zu starken Qualitätsverlusten bei der Vorhersage bezüglich anderer Eingabewerte kommt. Die Idee in vielen Verfahren ist dann, diese erste Näherungslösung weiter zu optimieren, zum Beispiel durch zufälliges Neigen einer Regressionsgeraden an einem festen Punkt, bis ein hinreichend optimales Ergebnis vorhanden ist. Solche Näherungsverfahren bieten bei gigantisch großen Datenmengen oder sehr hohen Dimensionen oft einen entscheidenden Effizienzvorteil. Vermutlich sind eben jene und ähnliche Methoden in den letzten beiden Sätzen des Absatzes 42 der Richtlinien gemeint.
Die Leitlinie unterstützt nach dieser Auffassung die nach Funktionalität ausgerichtete Definition der KI-VO, indem sie genannte Systeme zur mathematischen Optimierung ausschließt, und dabei notwendigerweise auch auf Funktionsweise und Implementierung etwas genauer eingeht. Dabei werden jedoch teilweise unpräzise Formulierungen getroffen, welche so interpretiert werden sollten, dass die genannten Methoden zur Regression, sowie das Lösen von Optimierungsproblemen in diesem Zusammenhang isoliert betrachtet als einfache Datenverarbeitung gelten. Eine konträre Auslegung, dass Systeme unabhängig von ihrer Mächtigkeit, beispielsweise Software zur Gesichtserkennung, lediglich aufgrund der Nutzung von Regressionsmethoden nicht als KI-System gelten, widerspräche einer auf Funktionalität ausgerichteten Definition. Dies würde den Fokus weg von Programmfunktionalität, und stattdessen auf Implementierungsdetails verlagern. Vorangegangen wurde bereits diskutiert, dass dies offensichtlich nicht bei Gesetzgebung der KI-VO, oder dem Erlass der Richtlinien angedacht war. Stattdessen erscheint der Absatz 42 eher als Klarstellung der Kommission gegen eine mögliche Überregulierung von konsolidierten, teilweise sehr alten mathematischen Verfahren, für die bislang kein Regulierungsbedarf bestand.

4.2 Risikobasierter Ansatz der EU-KI-VO

Gilt ein Softwaresystem als KI-System findet die KI-VO Anwendung und unterteilt solche Systeme in vier Risikoklassen (siehe Kapitel 3). Aus den verschiedenen Risikoklassen folgen dann jeweils unterschiedliche Anforderungen oder auch gänzliche Verbote, speziell konkrete Verbote vom Inverkehrbringen, der Inbetriebnahme oder Verwendung der KI-Systeme. Die Herstellung und Entwicklung solcher Systeme sowie Forschung an diesen bleiben damit grundsätzlich erlaubt. In Kapitel 3 wurde bereits erläutert, aus welchen Gründen die KI-VO in diesen Fällen nicht greift. Die genannten Einschränkungen, wie beispielsweise das Testen unter lediglich eingeschränkten Bedingungen, bleiben jedoch bestehen.

4.2.1 KI-Systeme mit inakzeptablem Risiko: Verbotene Praktiken

Die KI-Verordnung benennt im Art. 5 Abs. 1 insgesamt acht verbotene Praktiken:

- **[Art. 5 Abs. 1 a] Unterschwellige Beeinflussung und Manipulation:** Umfasst den Einsatz sämtlicher Formen von **manipulativer oder täuschender Beeinflussung**, welche die Autonomie und freie Entscheidungsfindung von Personen oder Gruppen untergräbt. Diese Beeinflussung kann sich dabei der Wahrnehmung von Nutzerinnen vollständig entziehen, oder trotz Wahrnehmbarkeit nicht kontrollierbar, oder nur schwer widerstehbar sein [15, S. 254, Rn 37]. Das Verbot greift nur, wenn diese Techniken mit dem Ziel einer **Verhaltensänderung** eingesetzt werden, und konkret dadurch die **Fähigkeit, eine fundierte Entscheidung zu treffen, deutlich beeinträchtigt wird** [15, S. 254, Rn 40]. Infolgedessen muss **Schadenseintritt für diese Person, oder andere mit erheblicher Wahrscheinlichkeit** zumindest drohen.
- **[Art. 5 Abs. 1 b] Ausnutzung von Vulnerabilität und Schutzbedürftigkeit:** Verbiebet KI-Systeme, die die Schutzbedürftigkeit oder Vulnerabilität von Personen (z. B. aufgrund von Alter, Behinderung, Armut oder sozialer/ethnischer Zugehörigkeit) ausnutzen. Auch hier ist das Ziel der **Verhaltensänderung** Voraussetzung für die Wirksamkeit des Verbots, sowie eine hinreichende Wahrscheinlichkeit, dass dieses Verhalten der betroffenen Person selbst, oder einer dritten Person einen **erheblichen Schaden** zufügt.
- **[Art. 5 Abs. 1 c] Soziale Bewertung (Social Scoring) und Diskirminierung:** Verbietet KI-Systeme, zur Bewertung oder Einstufung von natürlichen

Personen oder Gruppen von Personen über einen bestimmten Zeitraum auf der Grundlage ihres sozialen Verhaltens oder bekannter, abgeleiteter oder vorhergesagter persönlicher Eigenschaften oder Persönlichkeitsmerkmalen. Das Verbot greift nur dann, wenn diese Praktiken zu einer **qualifizierten Schlechterstellung oder Benachteiligung** führen [15, S. 260, Rn 69].

- **[Art. 5 Abs. 1 d] Bewertung des Risikos zur Straftatbegehung:** Verbietet sogenanntes *Predictive Policing*, soweit es ausschließlich auf der Grundlage des Profiling einer natürlichen Person oder der Bewertung ihrer persönlichen Merkmale und Eigenschaften basiert. Diese KI-Praktiken sind für die Erstellung einer Risikobewertung, ob eine Person eine Straftat begehen wird, verboten. Nach Erwägungsgrund 42 dient das Verbot dem Einklang mit der Unschuldsvermutung, sodass eine Beurteilung von Personen stets nur auf deren tatsächlichen Verhalten beruht [37] [15, S. 261, Rn 71].
- **[Art. 5 Abs. 1 e] Erstellen und Erweitern von Gesichtsdatenbanken durch ungezieltes Auslesen aus dem Internet und anderen Quellen:** Verbietet KI-Systeme, die Datenbanken zur Gesichtserkennung durch **ungezieltes Sammeln** von Gesichtsbildern aus dem Internet oder Überwachungskameras erstellen oder erweitern. Fraglich ist, ob hier technisch Bezug genommen wird auf sogenanntes *Webscraping* oder *Massenscraping*. Eine solche Maßnahme, beispielsweise zum Zwecke der Strafverfolgung, würde ungeachtet von möglichen Löschfristen eine sehr große Anzahl von unbeteiligten Personen betreffen. Eine Benachrichtigung dieser Betroffenen dürfte je nach Datengrundlage faktisch kaum möglich sein. Benachrichtigungspflichten sind jedoch zumindest in Deutschland bei Maßnahmen nach der Strafprozessordnung oder den Polizeigesetzen regelmäßig vorhanden. In der Kommentierung von *Wendehorst* wird der Begriff **ungezielt** unter anderem mit dem Fehlen eines konkreten Anlassfalls, bespielsweise einem Strafverfahren, beschrieben [15, S. 265, Rn 96]. Die EU-Kommission hingegen betrachtet das *ungezielte* Auslesen ebenfalls auf einer technischen Ebene mit klarem Bezug zu den erhobenen Daten selbst, wenn ein System *so viele Daten und Informationen wie möglich aufnimmt, ohne auf speziell und individuell bestimmte Subjekte für das Auslesen abzuzielen* [24, Abs 228]. Weiterhin wird genannt, dass die Datenbank auch nur *temporär* bestehen braucht, um als Datenbank im Sinne der verbotenen Praktik zu gelten [24, Abs 226]. Das Verbot dürfte dahingehend auch bei konkreten und zeitlich beschränkten Anlässen greifen und bezieht sich

offensichtlich auf die Art und Weise, wie die Daten erhoben werden. Das Vorhandensein einer bestimmten Zielstellung bei der Suche hebt nach den Richtlinen der Kommission dieses Verbot auf [24, Abs 229].

- **[Art. 5 Abs. 1 f] Emotionserkennung am Arbeitsplatz und in Bildungseinrichtungen:** Verbietet KI-Systeme zur Erkennung von Emotionen oder Absichten anhand biometrischer Daten am Arbeitsplatz und in Bildungseinrichtungen. Eine Ausnahme gilt für **medizinische oder sicherheitsrelevante Anwendungen**. Als Beispiel für eine medizinische Ausnahmeregelung nennen die Leitlinien der EU-Kommission die Verwendung für die *Unterstützung von Arbeitnehmern oder Studierenden mit Autismus und zur Verbesserung der Barrierefreiheit für blinde oder gehörlose Menschen* [24, Abs 263].
- **[Art. 5 Abs. 1 g] Kategorisierung anhand biometrischer Daten:** Verbietet KI-Systeme, die aus biometrischen Daten Merkmale beispielsweise Hautfarbe, Religion, sexuelle Orientierung oder politische Einstellungen ableiten, und anhand dessen eine Kategorisierung dieser Personen vornehmen. Eine Rückausnahme besteht für Datensätze, *die im Einklang mit dem Unionsrecht oder dem nationalen Recht anhand biometrischer Daten erworben wurden*, und in einigen Fällen der Strafverfolgung [38].
- **[Art. 5 Abs. 1 h] Echtzeit-Gesichtserkennung in der Öffentlichkeit:** Verbietet die **Verwendung** von KI-Systemen, welche **in Echtzeit** eine Gesichtserkennung und damit folglich die Identifizierung und Echtzeit-Aufenthaltsermittlung einer Person vornehmen. Beispielsweise die Nutzung von Live-Videoüberwachungsdaten für die Gesichtserkennung der darauf abgebildeten Personen. Dieses Verbot gilt nur eingeschränkt, so können beispielsweise nach Art. 5 Abs. 5 der KI-VO EU-Mitgliedsstaaten selbst entscheiden, ob sie unter gewissen Vorgaben der KI-VO eine Ermächtigungsgrundlage für solche Systeme zum Zwecke der Strafverfolgung erlassen.

Für die genannten verbotenen Praktiken **lit. a-g**, gilt ein konkretes Verbot der Inverkehrbringen, der Inbetriebnahme oder der Verwendung entsprechender KI-Systeme. Die Echtzeit-Gesichtserkennung nach **lit. h** ist nur in ihrer Verwendung verboten. Spezielle Regelungen zur Rückausnahme, beispielsweise im behördlichen Einsatz wurden hier nur angedeutet. Die Regulierungen zu diesen Ausnahmeregelungen sind vielschichtig und umfangreich, weshalb auf eine detaillierte Darstellung verzichtet wird.

4.2.2 Hochrisiko-Systeme

Für Systeme mit hohem Risiko ist der Einsatz grundsätzlich erlaubt, dieser unterliegt aber strengen Auflagen. Wann ein KI-System als hochriskant gilt, ist in Artikel 6 Abs. 1 und 2 der KI-VO festgelegt. Der **Absatz 1** bezieht sich dabei auf Produktsicherheitsanforderungen, und umfasst den Einsatz von KI-Systemen im Zusammenhang der Harmonisierungsvorschriften aus Anhang I der KI-VO. Ein KI-System, welches als Sicherheitsbauteil verwendet werden soll, oder selbst ein Produkt nach den Vorschriften des Anhang I ist und welches einer Konformitätsverwertung gemäß dieser Vorschriften unterzogen werden muss, gilt als **hochriskant**. Der Anhang I umfasst unter anderem Vorschriften zu den nachfolgend aufgelisteten Bereichen. KI-Systeme welche wie zuvor beschrieben in den folgenden Branchen eingesetzt werden, sind potentielle Hochrisiko-Systeme:

- Sicherheit von Spielzeug
- Sportboote und Wassermotorräder
- Aufzüge und Sicherheitsbauteile für Aufzüge
- Seilbahnen
- Sicherheit in der Zivilluftfahrt
- ...

Diese Aufzählung ist nicht abschließend, insgesamt werden 20 EU-Rechtsakte im Anhang I aufgezählt. Der bloße Einsatz eines KI-Systems in diesen Branchen allein begründet zudem noch kein Hochrisiko-System. Entscheidend ist, ob im Einzelfall die genannte Konformitätsbewertung im jeweiligen Rechtsakt vorgesehen ist. Der sicherheitskritische Einsatz in den aufgezählten Branchen ist jedoch ein verlässlicher Indikator, dass ein KI-System hochriskant gemäß der KI-VO sein könnte.
Im **Absatz 2** wird auf Anhang III der Verordnung verwiesen. Der Anhang III listet verschiedene Einsatzbereiche und allgemeine Anwendungsfälle dieser Bereiche auf. Fällt ein KI-System unter einen solchen Anwendungsfall, gilt es als Hochrisikosystem. Die nachfolgenden acht Einsatzbereiche werden im Anhang III aufgezählt:

- Biometrie
- Kritische Infrastruktur
- Allgemeine oder berufliche Bildung

- Beschäftigung, Personalmanagement und Zugang zur Selbstständigkeit
- Zugänglichkeit und Inanspruchnahme grundlegender privater und grundlegender öffentlicher Dienste und Leistungen
- Strafverfolgung
- Migration, Asyl und Grenzkontrolle
- Rechtspflege und demokratische Prozesse

Für Hochrisiko-KI-Systeme werden in der KI-VO sehr umfassende Anforderungen definiert. Die Benennung dieser konkreten Pflichten bildet den Hauptteil der Verordnung. Dabei handelt es sich unter anderem um die folgenden:

- Art. 9, Pflicht zur Einrichtung, Anwendung, Dokumentierung und Aufrechterhaltung eines **Risikomanagementsystems**
- Art. 10, **Daten und Daten-Governance** - Dies ist eine Forderung an Trainings-, Validierungs- und Testdatensätze von KI-Modellen. Diese müssen gewissen Qualitätskriterien der KI-VO genügen.
- Art. 11, Pflicht zur Erstellung und Aktualisierung einer **technischen Dokumentation**
- Art. 12, **Aufzeichnungspflichten** während des gesamten Lebenszyklus des Systems
- Art. 13, **Transparenz und Bereitstellung von Informationen** von Anbietern für die Betreiber - D.h. hinreichende Transparenz für die Interpretation und Verwendung von Ausgaben, sowie Bereitstellung einer Bediendungsanleitung zum KI-System.
- Art. 14, Wirksame **menschliche Aufsicht** während der gesamten Verwendungsdauer des Systems
- Art. 15, Angemessenes Maß an **Genauigkeit, Robustheit, Cybersicherheit** während des gesamten Lebenszyklus
- ...
- Art. 72 **Beobachtungspflichten** - Pflicht zur Einrichtung eines Systems zur Beobachtung des jeweiligen Hochrisiko-Systems

- Art. 73 Pflicht zur **Meldung schwerwiegender Vorfälle** an die Marktüberwachungsbehörden
- ...
- Art. 86, Recht auf **Erläuterung der Entscheidungsfindung im Einzelfall** für Personen, welche von der Entscheidungsfinung eines Hochrisiko-Systems betroffen waren

Für Informatikerinnen dürften diese Anforderungen künftig eine zentrale Rolle in ihrer Umsetzung spielen. Die KI-VO verankert organisatorische Punkte der Software-Entwicklung wie das Erstellen einer technischen Dokumentation auf einer gesetzlichen Grundlage. Die Anforderungen erscheinen dabei recht umfangreich, weshalb künftige Softwareentwicklungsprozesse sich höchstwahrscheinlich den Vorgaben der KI-VO anpassen werden. Möglicherweise werden die Konzepte von eher traditionellen Entwicklungsprozessen wieder von gesteigerter Bedeutung sein bei der Entwicklung von KI-Software-Systemen. Zudem werden zusätzliche Pflichten im Wirkbetrieb der Software gefordert, zum Beispiel die Beobachtungspflichten oder die Pflicht zur menschlichen Aufsicht. Gerade letztere könnte einen Einfluss auf das künftige Berufsbild von Informatikerinnen haben. Wie genau sich menschliche Aufsicht gestalten wird, ist mit großer Sicherheit stark vom jeweiligen System abhängig. Regelmäßig wird diese als *letztes Sicherheitsnetz* beschrieben, welches den bestimmungsgemäßen Betrieb und die sichere Verwendung eines Hochrisiko-KI-Systems ermöglicht. [9]

4.2.3 KI-Systeme mit begrenztem und geringem Risiko:

Die KI-VO unterscheidet neben verbotenen und hochriskanten Anwendungen auch KI-Systeme mit **begrenztem Risiko** und mit **geringem Risiko**. KI-Systeme mit begrenztem Risiko unterliegen ausschließlich Transparenzpflichten. Nachfolgend werden einige dieser Pflichten aufgezählt und erläutert:

- **Art. 50 Abs. 1 Nutzertransparenz für interaktive Systeme**: Eine interagierende Person muss darüber informiert werden, dass sie mit einem KI-System kommuniziert (klar, verständlich und barrierefrei). Dies betrifft Systeme, die mit Menschen interagieren wie Chatbots oder Sprachassistenten.
- **Art. 50 Abs. 2 Inhaltstransparenz bei Erzeugung/ Veränderung synthetischer Inhalte**: Beinhaltet die Forderung nach einer Kennzeichnung in maschinenlesbaren Format, welche offenlegt, dass synthetisches Material künstlich

erzeugt oder manipuliert ist. Also ein Wasserzeichen oder eine Art elektronische Signatur. Diese technischen Lösungen müssen (soweit möglich) wirksam, interoperabel, belastbar und zuverlässig sein, unter Berücksichtigung der Art des Inhalts, Umsetzungskosten und dem allgemein anerkannten Stand der Technik. Hier könnten Methoden der Steganographie Anwendung finden.

- **Art. 50 Abs. 4 KI-Systeme zur Erstellung oder Manipulation von Medien oder Texten (Deepfakes)**: Trifft zusätzliche Regelungen für Deepfakes (auch legaldefiniert in: Art. 3 Nr. 60 KI-VO), also Inhalte, die nicht unmittelbar als synthetisch erkennbar sind und Menschen bezüglich der Echtheit täuschen können. Betreiber müssen klar und deutlich offenlegen, wenn ein DeepFake verwendet wurde.

KI-Systeme mit **geringem Risiko** machen mit Sicherheit den größten Anteil der Anwendungen aus. Die meisten sind wahrscheinlich bereits seit langem verbreitet und in Nutzung. Dazu zählen etwa Spamfilter, Videospiele mit KI oder Suchalgorithmen. Für diese trifft die KI-VO **keine verpflichtenden Regulierungen**, Anbieter und Betreiber können aber Verhaltenskodizes nach Art. 95 ff KI-VO befolgen.

4.3 GPAI-Modelle

4.3.1 Rechtliche Anforderungen an GPAI-Modelle

Für Anbieter von GPAI-Modellen trifft die KI-VO weitere Regulatorien. Wichtig ist anzumerken, dass für GPAI-Systeme als spezielle Form von KI-Systemen keine gesonderten Forderungen gelten. Die Regulierungen für GPAI-Modelle werden in Art. 51 bis 55; 88 bis 94 und 101 der KI-VO benannt. Im wesentlichen umfassen diese Pflichten:

- Erstellung und Aktualisierung einer **technischen Dokumentation**.
- Die **Erstellung und Aktualisierung von Information und Dokumentation** für Anbieter von KI-Systemen, die eine Integration des Modells beabsichtigen. Dies stellt eine Art **Handlungsanleitung zur Modell-Integration** dar und ist von der *technischen Dokumentation* zu unterscheiden.
- Die Implementierung einer Strategie zur Einhaltung des **Urheberrechts**
- Veröffentlichung einer hinreichend detaillierten **Zusammenfassung der Trainingsdaten**, nach einer durch das KI-Büro bereitgestellten Vorlage

Die eben genannten Pflichten gelten für **alle GPAI-Modelle**. Birgt ein GPAI-Modell ein sogenanntes *systemisches Risiko* kommen nach Art. 51 Abs. 1 der KI-VO weitere Pflichten hinzu. Diese umfassen unter anderem:

- **Angriffstests**
- Die **Bewertung und Minderung möglicher systemischer Risiken**
- Eine **Berichtspflicht bei schwerwiegenden Vorfällen an das KI-Büro und nationale Behörden**
- Die Gewährleistung eines angemessenen Maß an **Cybersicherheit**

4.3.2 Systemische Risken und die Gleitkommaschranke von 10^{25}

Überschreiten die für das Training eines GPAI-Models angewandten Gleitkommaoperationen eine Anzahl von 10^{25}, so wird gemäß KI-VO Art. 51 Abs. 2 ein *hoher Wirkgrad* und folglich ein *systemisches Risiko* des Systems gesetzlich angenommen.
Zwar können Anbieter nach Art. 52 Abs. 2 auch bei Überschreiten des Wertes ein solches systemisches Risiko widerlegen und die Feststellung erfolgt abschließend über Art. 51 Abs. 1a oder b, also über geeignete technische Instrumente, Methoden, Parameter oder der Warnung des wissenschaftlichen Gremiums des KI-Büros. So handelt es sich dennoch um eine der wenigen gesetzlichen Nenngrößen in der KI-VO. Entsprechend ist davon auszugehen, dass diese Zahl zumindest in der nahen Zukunft eine bedeutende Rolle bei der Feststellung eines systemischen Risikos spielen könnte.
Das wird genau dann zum Problem, wenn für potentiell mächtige Modelle kein hoher Wirkgrad angenommen wird, weil diese beispielsweise die Schranke deutlich unterschreiten. Für ein Gesamttraining mit 10^{23} FLOPs, jedoch spätestens ab 10^{22} FLOPs oder geringer könnte man bereits von einem deutlichen Unterschreiten sprechen. Zur Verdeutlichung: Um von 10^{22} auf 10^{25} Operationen zu kommen, ist das 1000-Fache an Ressourcen (Dauer oder Hardware) notwendig. Mit Stand August 2025 sind durchaus einige Modelle in diesem 'niedrigeren' Bereich des Gesamttrainings im Umlauf. Zusätzlich sind 'nur' 22 Modelle bekannt, welche die Schranke von 10^{25} überhaupt überschreiten [35].
Es kann sogar argumentiert werden, dass ein ausgereifteres GPAI-Modell weniger riskante Ausgaben erzeugt [15, Bernsteiner/ Schmitt, S. 798 Rn 38]. Inwiefern diese Kennzahl also tatsächlich das systemische Risiko eines Systems abschätzt, kann nicht pauschal beantwortet werden. Bei Nichtannahme einer hohen Wirkkraft käme es zu einer

Minderung der Schutzwirkung der KI-VO, da einige Pflichten und Anforderungen im Sicherheitsbereich nach Art. 55 Abs. 1 KI-VO entfielen.
Gleitkommaarithmetik bildet derzeit den Standard im Deep-Learning-Bereich und ist damit fundamental für das Training aller relevanten GPAI-Modelle. Derzeit ist kein bedeutender Trend zu beobachten, die Schranke potenziell vollständig zu umgehen, indem ausschließlich Modelle mit Festkomma- oder Ganzzahlen trainiert werden. Beim Training werden in der Regel Zahlenwerte verarbeitet, welche stark schwanken, von sehr kleinen gebrochenen Werten bis hin zu sehr großen Werten. Für so einen breiten Anwendungsfall bietet die Darstellung in Form von Gleitkommazahlen deutliche Vorteile. Es gibt jedoch einige Workarounds, und damit Ansätze diese Probleme zu umgehen, in welchen Teile des Trainings tatsächlich in Ganzzahlarithmetik durchgeführt werden [8]. Die Motivation dahinter entspringt jedoch sicherlich dem möglichen Energieeffizienzvorteil gegenüber Berechnungen in präziseren Zahlenformaten. Interessant in diesem Zusammenhang ist, dass in den letzten Jahren und damit vermutlich im Rahmen des großen Durchbruchs von KI-Modellen der Trend zu geringeren Präzisionen in Gleitkommadarstellungen zu erkennen war. So galt IEEE Single-Precision offenbar lange als Standard [36]. Nehmen also Ganzzahloperationen zusätzlich eine nicht zu vernachlässigende Rolle im Training von GPAI-Modellen ein, so erscheint eine Anpassung des Art. 51 Abs. 2 KI-VO ohnehin unumgänglich. Eine solche Anpassung mittels deligiertem Rechtsakt der Kommission wäre per Art. 51 Abs. 3 möglich. Dieser Absatz wurde, möglicherweise vorausschauend, eingeführt um auf technologische Entwicklungen reagieren zu können.
Ein weiteres zentrales Problem der 10^{25}-Schranke ist, dass sie lediglich den quantitativen Trainingsaufwand misst, nicht jedoch die qualitativen Eigenschaften des Modells. Moderne KI-Modelle können nicht vorhersehbare Fähigkeiten entwickeln, die nicht direkt proportional zum Trainingsaufwand sind [12]. Effiziente Architekturen, sparsames Training oder multimodale Ansätze ermöglichen es, gleiche oder sogar höhere Fähigkeiten bei deutlich geringerem Rechenaufwand zu erreichen. Folglich kann ein Modell mit 10^{23} FLOPs Fähigkeiten besitzen, die von der Regulierung fälschlicherweise als unproblematisch eingeschätzt würden. Zudem berücksichtigt die FLOP-Schranke nicht, ob ein Modell gezielt auf Stabilität, Sicherheit oder Fairness trainiert wurde. Zwei Modelle mit identischem Trainingsaufwand können völlig unterschiedliche Risikoprofile aufweisen, abhängig von Trainingsdaten, Regularisierungsmethoden oder Optimierungstechniken. Dadurch entsteht eine Diskrepanz zwischen regulatorischer Einstufung (basierend auf FLOPs) und tatsächlichem systemischen Risiko.

Um die Gleitkommaschranke wirksam einzusetzen, muss sie Teil eines adaptiven, mehrstufigen Governance-Systems sein. Der Rechenaufwand kann als erster Hinweis dienen, danach sollten qualitative Analysen, Sicherheitsbewertungen und simulationsbasierte Risikoabschätzungen erfolgen. Nur so lässt sich gewährleisten, dass die Schutzwirkung der KI-VO nicht durch technische Limitationen oder die Diskrepanz zwischen Rechenaufwand und Fähigkeiten abgeschwächt wird. Gleichzeitig ermöglicht dieses System, die Innovationsfähigkeit zu erhalten, da Modelle nicht allein aufgrund hoher FLOPs reguliert werden.
Insgesamt ist die 10^{25}-Schranke ein nützlicher, aber unvollständiger Indikator. Sie lenkt die Aufmerksamkeit auf potentielle Hochrisikomodelle, ersetzt jedoch keine umfassende Risikobewertung. Eine robuste KI-Governance erfordert daher die Kombination aus quantitativen Schwellen, qualitativen Analysen, Sicherheitsprüfungen und adaptiven Bewertungsprozessen, um ein ausgewogenes Verhältnis zwischen Schutzwirkung und Innovationsfähigkeit zu gewährleisten. Es sei zu erwähnen, dass die KI-VO mit Art. 51 Abs. 1a und b die Grundlage für eine solche vielschichtige Risikobewertung bildet. Wichtig ist, dass diese bei der praktischen Umsetzung durch die Kommission berücksichtigt werden und die gesetzlich und damit hochangebundene 10^{25}-Schranke nicht zur Hintertür für gefährliche GPAI-Modelle mit 'geringer' Gesamttrainingsdauer wird.

5 Diskussion

5.1 Wirtschaftliche und Gesellschaftliche Auswirkungen

Die wirtschaftlichen und gesellschaftlichen Folgen der KI-VO zeigen ein Spannungsfeld zwischen Innovationsförderung, Grundrechtsschutz und ökonomischen Machtstrukturen. Das Gesetz wird zunächst zu erheblichen Anpassungskosten führen, da vor allem Anbieter von Hochrisiko-KI-Systemen umfassende Anforderungen an Risikomanagement, Datenqualität, Dokumentation, Transparenz und menschlicher Aufsicht erfüllen müssen. Alle anderen Akteure werden von größeren Compliance-Aufgaben größtenteils verschont bleiben. Allerdings können schon diese Vorgaben insbesondere für kleine und mittlere Unternehmen (KMU), die den Großteil der Unternehmen in der EU ausmachen, sowie Start-ups hohe Eintrittsbarrieren schaffen und die Innovationsgeschwindigkeit kurzfristig bremsen. Studien zeigen, dass der Aufbau von Compliance-Strukturen und Zertifizierungsprozessen erhebliche Ressourcen bindet. Kritikerinnen befürchten trotz vorhandener Ausnahmeregelungen eine Verlagerung von Forschung

und Entwicklung in weniger regulierte Regionen, was wiederum die technologische Souveränität Europas schwächen könnte [1, 4]. Andere Stimmen betonen jedoch mögliche langfristige Vorteile: Einheitliche Standards schaffen Investitionssicherheit, stärken den europäischen Binnenmarkt und könnten es der EU ermöglichen, globale Normen zu setzen, ähnlich wie es mit der Datenschutz-Grundverordnung (DSGVO) gelungen ist. Aus dieser Perspektive erscheint Regulierung als strategisches Instrument, um Europas Wettbewerbsfähigkeit zu sichern und vertrauenswürdige KI als Markenzeichen zu etablieren. Befürworterinnen argumentieren, dass eine stringente Regulierung Vertrauen schafft, was zu einer höheren Qualität des Datenaustauschs führen und Firmen dazu anregen kann, sich in datenschutzfreundlichen Techniken wie Federated Learning hervorzutun [4].

Von zivilgesellschaftlichen Organisationen wurde stellenweise Kritik geübt. Diese kritisieren, dass die KI-VO zentrale soziale Probleme trotz seiner hohen Ambitionen nicht ausreichend adressiert. Sei es durch Unwillen oder auch durch die breite Untergrabung zentraler Punkte durch Lobbyarbeit. Ein prominentes Beispiel dafür ist das Zuwirken von Deutschland und Frankreich im Bezug auf die Einordnung von GPAI-Systemen. Die beiden KI-Firmen *Mistral AI* und *Aleph Alpha* lobbyierten für weniger strenge Auflagen und plädierten für mehr Selbstkontrolle und verwässerten somit den Gesetzestext [5]. Weiterhin erlaubt das Gesetz beispielsweise den Einsatz biometrischer Echtzeit-Überwachungstechnologien in bestimmten Ausnahmefällen, etwa bei der Strafverfolgung [3, 40]. Kritikerinnen warnen, dass diese Ausnahmen Schlupflöcher für Massenüberwachung schaffen und Grundrechte wie Datenschutz, Versammlungsfreiheit und das Recht auf Nichtdiskriminierung untergraben könnten. Auch die vorgesehene Risikoklassifizierung wird bemängelt: Viele Anwendungen, die erhebliche gesellschaftliche Auswirkungen haben könnten über Schlupflöcher nicht unter die Kategorie „Hochrisiko“ fallen [3, 40]. Ein anderes Beispiel ist der Export von Technologien. Die KI-VO behandelt zwar die extraterritoriale Wirkung von KI-Systemen. Sie bezieht sich jedoch nur auf Systeme, die außerhalb der EU entwickelt wurden und in der EU zum Einsatz gebracht werden. Technologien, die aus der EU in Drittstaaten exportiert werden, bleiben in der Betrachtung allerdings außen vor [2]. Dies wirft auch Fragen zur globalen Verantwortung europäischer Unternehmen auf. Werden die innerhalb der EU geltenden Standards, die für Vertrauen und Sicherheit sorgen sollen, bei Exporten umgangen, drohen negative Auswirkungen auf die Menschenrechte und ethische Standards in anderen Regionen. Menschenrechtsorganisationen fordern daher strengere Kontrollmechanismen für den Export von KI-Systemen, insbesondere für Anwendungen, die zur

Überwachung, Diskriminierung oder Unterdrückung eingesetzt werden könnten [2, 40]. Abschließend zeigt sich bei der KI-Verordnung ein Spannungsfeld zwischen wirtschaftlichem Erfolg und dem Schutz der Menschenrechte. Die Verordnung erhöht die Compliance-Anforderungen erheblich, was insbesondere KMU und Start-ups belastet und die Innovationsgeschwindigkeit kurzfristig hemmen kann. Ergänzende regulatorische Rahmenwerke wären hier notwendig, um kleinere Unternehmen zu entlasten und gleichzeitig gesellschaftliche Risiken wie Diskriminierung oder Missbrauch besser zu adressieren.
Die KI-VO spiegelt einen Kompromiss wider: Vertrauen und Sicherheit werden angestrebt, wirtschaftliche Effizienz und Wettbewerbsfähigkeit haben jedoch weiterhin ein starkes Gewicht, möglicherweise ist man dabei aber hauptsächlich Großkonzernen entgegengekommen. Fraglich ist, ob die Prioritäten allgemein so gesetzt werden sollten oder ob nicht ein Umdenken erforderlich ist. Hin zu einer weiter menschenzentrierten Auslegung und vor allem auch einer Ausweitung der extraterritorialen Wirkung, um Menschen in anderen Teilen der Welt, die meist die vulnerabelsten Gruppen darstellen, nicht weiter zu gefährden.

5.2 Auswirkungen auf Informatikerinnen

Für Informatikerinnen sollte die KI-VO von Bedeutung sein, da vor allem sie sich mit der Compliance-Arbeit und Einhaltung von Regularien auseinandersetzen müssen. Vor allem für Informatikerinnen im Bereich der Software-Entwicklung von Hochrisiko-KI-Systemen kommt eine Fülle an neuen Aufgaben hinzu, die sich neben die eigentliche Entwicklungsarbeit reiht. Wie schon im Kapitel zu Hochrisikosystemen aufgelistet, dürften Entwicklerinnen künftig eine Vielzahl von Dokumentationspflichten erwarten. Selbiges gilt für Entwicklerinnen von GPAI-Modellen. Diese unterliegen ebenfalls besonderen Transparenz- und Dokumentationspflichten, vor allem wenn sie als „systemisch riskant“ eingestuft werden.
Diese neuen Vorgaben beeinflussen den gesamten Entwicklungsprozess: Bereits in frühen Phasen müssen Entwicklerinnen und Entwickler Risikoanalysen planen, geeignete Datensätze auswählen und Maßnahmen zur Bias-Kontrolle implementieren [18]. Die Pflicht zur Protokollierung, die Kennzeichnung von synthetischen Inhalten und Auditierbarkeit führen zu höherem organisatorischen und finanziellen Aufwand. Besonders kleinere Start-ups oder Forschungsteams ohne große Ressourcen könnten dadurch unter Druck geraten, da Compliance- und Dokumentationspflichten kostspielig sein können [10]. Für Informatikerinnen bedeutet dies nicht nur zusätzliche Pflichten, sondern

auch eine stärkere gesellschaftliche Verantwortung auf einer gesetzlichen Grundlage. Sie müssen jetzt auch rechtliche und soziale Aspekte in ihre Arbeit integrieren. Die KI-VO verlangt, dass KI-Systeme sicher, transparent und diskriminierungsfrei sein müssen. Ein Auftrag, der Informatikerinnen zu zentralen Akteuren bei der Umsetzung europäischer Werte in Technologie macht [18].
Die KI-VO fordert die Informatik dazu auf, sich stärker als bisher mit rechtlichen und gesellschaftlichen Fragen auseinanderzusetzen. Entwicklerinnen übernehmen damit eine Schlüsselrolle bei der Gestaltung einer sicheren und vertrauenswürdigen KI-Landschaft in Europa. Dieser Prozess erfordert zwar zusätzlichen Aufwand und neue Kompetenzen. Kann aber langfristig die Qualität und Akzeptanz von KI-Systemen verbessern.

6 Fazit

Abschließend lässt sich sagen, dass die KI-Verordnung einen wichtigen Schritt hin zu einer klaren und verbindlichen Regulierung von Künstlicher Intelligenz darstellt. Sie schafft Transparenz, legt Pflichten fest und soll das Vertrauen in KI-Systeme fördern, während sie gleichzeitig den Schutz von Grundrechten gewährleistet. Die internationale Entwicklung zeigt zudem, dass immer mehr Länder die Bedeutung einer Regulierung von KI erkennen. Auch wenn die KI-VO nicht perfekt ist und weiterhin Anpassungen notwendig sein werden, stellt sie einen bedeutenden Meilenstein dar. Zum ersten Mal schafft die EU einen einheitlichen und verbindlichen Rechtsrahmen für KI. Damit legt sie die Grundlage für Rechtssicherheit innerhalb Europas und sendet ein wichtiges Signal für die weltweite Diskussion über verantwortungsvolle KI.

Literatur

[1] G. Abako. AI Policy Bulletin. It's too hard for small and medium-sized businesses to comply with EU AI Act – here's what to do. 2024. https://www.aipolicybulletin.org/articles/its-too-hard-for-small-and-medium-sized-businesses-to-comply-with-eu-ai-act-heres-what-to-do. (aufgerufen am 03.09.2025)

[2] Amnesty International. Lawmakers reluctant to stop EU companies profiting from surveillance and abuse through the AI Act. Press Release 05.12.2023. https://www.amnesty.eu/news/lawmakers-reluctant-to-stop-eu-companies-profiting-from-surveillance-and-abuse-through-the-ai-act/ (aufgerufen am 03.09.2025.)

[3] N. Aszódi. EU's AI Act fails to set gold standard for human rights, AlgorithmWatch 2024. https://algorithmwatch.org/en/ai-act-fails-to-set-gold-standard-for-human-rights/ (aufgerufen am 02.10.2025)

[4] R. Csernatoni. The EU's AI Power Play: Between Deregulation and Innovation. Carnegie Endowment for International Peace 2025. https://carnegieendowment.org/research/2025/05/the-eus-ai-power-play-between-deregulation-and-innovation?lang=en (aufgerufen am 03.09.2025.)

[5] F. Duffy. AI Act: Von der KI-Industrie in die Zange genommen. Lobby Control 2024. https://www.lobbycontrol.de/macht-der-digitalkonzerne/ai-act-von-der-ki-industrie-in-die-zange-genommen-114508 (aufgerufen am 11.09.2025)

[6] Europäische Union. Vertrag über die Arbeitsweise der Europäischen Union, 2012. https://eur-lex.europa.eu/resource.html?uri=cellar:2bf140bf-a3f8-4ab2-b506-fd71826e6da6.0020.02/DOC_2&format=PDF (aufgerufen am 02.10.2025)

[7] Europäische Union. Verordnung zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz. Amtsblatt 2024/1689 der Europäischen Union. 2024. https://eur-lex.europa.eu/eli/reg/2024/1689/oj?locale=de

[8] A. Ghaffari, M. S. Tahaei, M. Tayaranian, M. Asgharian, and V. Nia. Is Integer Arithmetic Enough for Deep Learning Training?. In: Proceedings of the 36th Conference on Neural Information Processing Systems (NeurIPS), 2022. Online: DOI: 10.48550/arXiv.2207.08822.

[9] S. Hetmank und P. Meinel. Menschliche Aufsicht in der KI-VO. KIR – Künstliche Intelligenz und Recht, Heft 4, Seiten 113-148, 2024.

[10] H. Hermanns, A. Lauber-Ronsberg, P. Meinel, S. Herz, and H. Zhang. AI Act for the Working Programmer. In: Proceedings of the International Conference on Bridgung the Gap between AI and Reality, pp. 74-98. Lecture Notes in Computer Science, LNCS 15217, Crete, Greece, 2024. DOI: 10.1007/978-3-031-75434-0_6

[11] E. Hilgendorf und D. Roth-Isigkeit. Die neue Verordnung der EU zur Künstlichen Intelligenz. C.H. Beck 2023.

[12] S. Hooker. On the Limitations of Compute Thresholds as a Governance Strategy, 2024. DOI: 10.48550/arXiv.2407.05694

[13] R. Molavi Vasse'i. Die Evolution der KI-Definition von Turings Anthropozentrik zur Funktionsorientierung der KI-VO. KIR – Künstliche Intelligenz und Recht, Heft 5, Seiten 165-212, 2025.

[14] R. Schwartmann, T. Keber und K. Zenner. KI-VO, Leitfaden für die Praxis. C.F. Müller Verlag 2024

[15] C. Wendehorst und M. Martini. KI-VO Kommentar. C.H. Beck 2024.

[16] T. Wybitul. Arbeitsbuch AI Act. Fachmedien Recht un Wirtschaft, Deutscher Fachverlag 2025.

[17] W. Zankl (Hrsg.). KI-VO. Manz'sche Verlags- und Universitätsbuchhandlung 2025.

[18] M. Zderic. What the EU AI Act means for AI software development: everything you need to know. Decode, 2025. https://decode.agency/article/eu-ai-act-software-development (aufgerufen am 11.09.2025)

Internetquellen

[19] Webseite der Bundesregierung, abgerufen am 23.08.2025. https://www.bundesregierung.de/breg-de/aktuelles/ai-act-2285944

[20] Ausarbeitung PE 6- 3000- 83/16 des deutschen Bundestags, abgerufen am 23.08.2025. https://www.bundestag.de/resource/blob/437706/PE-6-083-16-pdf.pdf

[21] EU-Kommission, Veröffentlichungen, abgerufen am 02.08.2025. https://digital-strategy.ec.europa.eu/de/library/commission-publishes-guidelines-ai-system-definition-facilitate-first-ai-acts-rules-application

[22] Webseite, ZDF, abgerufen am 02.08.2025. https://zdfheute-stories-scroll.zdf.de/eu-usa-china-russland-vergleich/index.html

[23] Europäische Kommission, Veröffentlichungen, abgerufen am 02.08.2025. https://digital-strategy.ec.europa.eu/en/library/proposal-regulation-laying-down-harmonised-rules-artificial-intelligence

[24] EU-Kommission, Veröffentlichungen, abgerufen am 02.08.2025. https://digital-strategy.ec.europa.eu/de/library/commission-publishes-guidelines-prohibited-artificial-intelligence-ai-practices-defined-ai-act

[25] Webseite der Bundesregierung, abgerufen am 02.08.2025. https://www.bundesregierung.de/breg-de/aktuelles/eu-kommission-kurz-erklaert-328740

[26] Webseite der EU, abgerufen am 02.08.2025. https://european-union.europa.eu/institutions-law-budget/institutions-and-bodies/search-all-eu-institutions-and-bodies/european-commission_de

[27] Webseite Bundeszentrale für politische Bildung, abgerufen am 02.08.2025.https://www.bpb.de/themen/innere-sicherheit/dossier-innere-sicherheit/190542/das-zusammenwachsen-von-innerer-und-aeusserer-sicherheit/

[28] Webseite Tagesschau, abgerufen am 09.08.2025. https://www.tagesschau.de/investigativ/br-recherche/palantir-polizei-behoerden-analysesoftware-100.html

[29] Webseite Tagesschau, abgerufen am 09.08.2025. https://www.tagesschau.de/investigativ/ndr-wdr/palantir-einsatz-deutschland-100.html

[30] Webseite ZDF, abgerufen am 09.08.2025. https://www.zdfheute.de/wissen/palantir-software-polizei-risiken-faq-100.html

[31] Webseite BfV, abgerufen am 09.08.2025. https://www.verfassungsschutz.de/DE/themen/spionage-und-proliferationsabwehr/rolle-des-verfassungsschutzes/rolle-des-verfassungsschutzes_node.html

[32] Webseite Uni Potsdam, abgerufen am 02.08.2025. https://www.uni-potsdam.de/de/rechtskunde-online/rechtsgebiete/oeffentliches-recht/grundrechte/kunst-und-wissenschaftsfreiheit-art-5-abs-3-gg

[33] Erwägungsgründe der KI-VO, Erwägungsgrund 12, abgerufen am 20.08.2025. https://ai-act-law.eu/de/erwg/12/

[34] Dokumentation MS Excel, abgerufen am 20.08.2025. https://support.microsoft.com/en-us/office/linest-function-84d7d0d9-6e50-4101-977a-fa7abf772b6d

[35] Webseite Epoch AI, abgerufen am 02.08.2025. https://epoch.ai/data/ai-models?view=table

[36] Website Nvidia, abgerufen am 16.08.2025. https://developer.nvidia.com/blog/mixed-precision-training-of-deep-neural-networks/

[37] Erwägungsgründe der KI-VO, Erwägungsgrund 42, abgerufen am 20.08.2025. https://ai-act-law.eu/de/erwg/42/

[38] Erwägungsgründe der KI-VO, Erwägungsgrund 30, abgerufen am 20.08.2025. https://ai-act-law.eu/de/erwg/30/

[39] Erwägungsgründe der KI-VO, Erwägungsgrund 102, abgerufen am 20.08.2025. https://ai-act-law.eu/de/erwg/102/

[40] European Digital Rights (EDRi), abgerufen am 03.09.2025. Artificial Intelligence and Fundamental Rights – Document Pool. 2024. https://edri.org/our-work/artificial-intelligence-and-fundamental-rights-document-pool/und https://edri.org/wp-content/uploads/2024/03/Statement-AI-Act-migration.pdf

[41] Website OECD, abgerufen am 20.08.2025. https://legalinstruments.oecd.org/en/instruments/oecd-legal-0449