November 2024
12. Jahrg.
84364

Seite 137–204

InTeR

Zeitschrift zum Innovations- und Technikrecht

4

dfv Mediengruppe · Frankfurt am Main

gungsgrund 107). Eine Offenlegung der gesamten Trainingsdaten wäre angesichts der schieren Datenmenge, die für das Training eines GPAI-Modells verwendet wird, ohnehin nicht praktikabel.

Auch die im Rahmen der gem. Art. 53 Abs. 1 lit. a) und lit. b) KI-VO zur Verfügung zu stellenden Informationen über Trainingsdaten erfordern wohl keine Offenlegung von Geschäftsgeheimnissen. Die Informationen müssen lediglich „gegebenenfalls" zur Verfügung gestellt werden. Dies könnte als Einfallstor für den Einwand gesehen werden, dass mit der Weitergabe ein Geschäftsgeheimnis offenbart werden müsste. Es bleibt jedoch unklar, ob mit „Informationen über die für das Trainieren, Testen und Validieren verwendeten Daten" die gesamten Trainingsdaten des GPAI-Modells gemeint sind oder ähnlich wie in lit. d) eine Zusammenfassung ausreichend ist.

III. Ergebnis

Letztendlich zeigt sich, dass die ohnehin schon schwierige Frage nach der Möglichkeit rechtlicher Absicherung von KI jedenfalls in Bezug auf GPAI durch die KI-VO durchaus um weitere Problemkreise erweitert wird. Es sollte deutlich geworden sein, dass infolge der nur zum Teil bestehenden Möglichkeiten urheberrechtlichen Schutzes von KI dem Geschäftsgeheimnisrecht eine wesentliche primäre und/oder komplementäre Bedeutung zukommt, um Investitionen in große KI-Modelle rechtlich schützen zu können. Im Dickicht der umfassenden Regelungen der KI-VO fällt auch nicht auf den ersten Blick auf, dass der Bestand auch des Geschäftsgeheimnisschutzes durch Informationspflichten auszuhöhlen droht.

Insgesamt lässt sich jedoch festhalten, dass es zu deutlich weniger Kollisionen zwischen den Informations- und Dokumentationspflichten der KI-VO und als Geschäftsgeheimnis geschützten Informationen der Anbieter von GPAI-Modellen kommt, als es auf den ersten Blick erscheinen mag. In den Fällen, in denen es dennoch zu einer Kollision kommt, was vor allem die Architektur bzw. Hyperparameter der GPAI betrifft, bestehen jedoch erhebliche Unsicherheiten.

Damit stellt sich die vielfach bemühte Folgefrage, ob der AI Act tatsächlich die von der EU-Kommission intendierten Innovationen in der KI-Branche zu fördern vermag oder ob das Problem etwaig verkürzten Rechtsschutzes der Branche nicht zusätzlich zusetzen wird. Man wird jedenfalls den Eindruck nicht los, dass ein gewaltiges Regulierungswerk in die Welt gesetzt wurde, welches vor allem vom politischen Willen getragen war, um in jedem Fall die weltweit erste KI-Regulierung zu etablieren, so dass Reibungsverluste in Kauf genommen wurden und nicht jeder Aspekt hinreichend überlegt war.

Als Trost mag insofern dienen, dass mit den Informations- und Dokumentationspflichten des Art. 53 KI-VO – jedenfalls bislang – nur die großen Anbieter von GPAI adressiert werden, von denen es bislang nicht allzu viele gibt und bei denen man davon ausgehen kann, dass die Kosten für die notwendige KI-Compliance ebenso getragen werden können wie Maßnahmen zur Absicherung der mühsam entwickelten KI-Modelle. Ob die Informations- und Dokumentationspflichten aber nicht zu einem späteren Zeitpunkt ausgeweitet werden und die in diesem Beitrag beschriebenen Probleme damit ggf. vergrößert werden, bleibt abzuwarten. Denn nur eines scheint gewiss: Irgendwo in Brüssel wird bereits die nächste Regulierung erdacht.

Kristian Borkert, Waiblingen und Anastasia Nomerowskaja, Gießen*

Regulation eats Innovation for Breakfast: KI-basierte SaaS-Lösung unter dem Regime des EU AI Acts in der Praxis

Als einer der ersten Gesetzgeber hat sich die EU entschieden künstliche Intelligenz (KI) zu regulieren. Die KI-Verordnung steht am Ende eines langen und komplexen Einigungsprozesses. Sie trat am 01. August 2024 in Kraft. Der KI-Verordnung wurde im Gesetzgebungsverfahren mehrfach vorgeworfen, dass sie KI-Innovationen in Europa verhindere bzw. sehr erschwere. Europa werde dadurch im internationalen Rennen um die Dominanz in diesem Technologiefeld weiter zurückgeworfen. Ziel der KI-Verordnung ist es, das Spannungsfeld zwischen Menschen- und Freiheitsrechten in der EU mit dem disruptiven Potential der KI-Technologie in Ausgleich zu bringen und einen einheitlichen Rechtsrahmen im Einklang mit den Werten der Union im europäischen Binnenmarkt zu schaffen.

Die nachfolgende Analyse der Klassifizierung einer KI-Anwendung eines KMU in der Praxis zeigt Regelungslücken und Unklarheiten auf. Teilweise lässt sich auf technischer, organisatorischer und vertraglicher Ebene gegensteuern. Daraus wird insgesamt aber ein eher zurückhaltender, risikoaverser Umgang mit KI resultieren, zumindest bis sich eine einschlägige Rechtsprechungspraxis herausgebildet bzw. der EU-Gesetzgeber die KI-Verordnung konkretisiert und nachgebessert hat.

I. Einführung

Die Vorstellung von einer mächtigen künstlichen Intelligenz ist ebenso wenig neu wie die Notwendigkeit sie regulieren zu müssen. Bereits im März 1942 legte Isaac Asimov seine Ideen zu Robotergesetzen in einer Kurzgeschichte nieder[1]. Zahlreiche bekannte Werke der Unterhaltungsin-

* Dieser Beitrag beruht auf einem Vortrag bei der DSRI-Herbstakademietagung 2024. Mehr über die Autor:innen erfahren Sie auf S. III.

1 *Asimov*, Runaround, S. 94, abrufbar unter https://archive.org/details/Astounding_v29n01_1942-03_dtsg0318/page/n3/mode/2up?view=theater, (abgerufen am: 28.6.2024).

dustrie enthalten diverse mächtige KI, wie beispielsweise HAL 9000[2], Skynet[3], WOPR[4] oder Deep Thought[5], die eine Regulierung zum Schutz der Menschheit und der Menschenrechte wünschenswert erscheinen lassen.

Der Begriff „Künstliche Intelligenz" bzw. „Artificial Intelligence" wurde wohl erstmals in einem Forschungsantrag im Jahr 1955 verwendet[6]. In den darauffolgenden Jahren war die Forschung stark geprägt vom „Maschinellen Lernen", also der Nutzung von mathematischen Prozeduren (Algorithmen) zur Analyse von Daten[7]. Häufig werden maschinelles Lernen und Künstliche Intelligenz synonym gebraucht. Dabei ist maschinelles Lernen, auch wenn es eine Schlüsseldisziplin ist, nur eine von mehreren Disziplinen im Feld der Künstlichen Intelligenz.[8]

Obwohl sich die Forschung und Literatur seit mehr als 50 Jahren mit Künstlicher Intelligenz beschäftigt, ist der Begriff weiterhin unscharf und genauso wenig zu greifen wie menschliche Intelligenz. Steven Finlay definiert z. B. Künstliche Intelligenz als die Replikation von menschlichen Fähigkeiten zur Analyse und/oder Entscheidungsfindung[9].

Eine klare Definition des regulierten Gegenstandes ist wiederum Voraussetzung für die Rechtssicherheit der Betroffenen bei der Umsetzung der Regulierungsinhalte. Die folgende Untersuchung wird an einem praktischen Fall zeigen, ob die KI-Verordnung der EU (nachfolgenden KI-VO)[10] diesem Anspruch gerecht wird.

1. Überblick über das Thema und die Bedeutung von KI-Technologie als SaaS-Lösung

Die Einführung von ChatGPT[11] markierte einen Höhepunkt in der Entwicklung der KI und löste eine Welle von Innovationen und Anpassungen in der Technologiebranche aus. Aktuell kommt kaum ein Unternehmen ohne eine KI-Strategie aus.

ChatGPT und andere KI-Lösungen werden regelmäßig als Software-as-a-Service-Lösungen (SaaS-Lösungen) angeboten. Dabei handelt es sich, vereinfacht dargestellt, um browserbasierte Software-Anwendungen, die dem Nutzer via Internet bereitgestellt werden.[12] Damit kann der Nutzer die KI-Anwendung auf seinem Laptop oder Mobiltelefon nutzen, ohne über besonders leistungsfähige Rechenkapazitäten zu verfügen oder eine komplexe IT-Infrastruktur betreiben zu müssen. Die KI passt in die Hosentasche.

Durch den niedrigschwelligen Zugang zur Technologie ermöglicht SaaS die schnelle Skalierung in die Breite. Privatpersonen und kleine Unternehmen können mit KI-Technologie als SaaS fortschrittliche Lösungen nutzen, die bisher größeren Organisationen vorbehalten waren. Dies eröffnet neue Perspektiven und Geschäftsfelder.

2. EU AI Act – Hintergründe und Sachstand

Mit der Veröffentlichung der KI-VO am 14. Juli 2024 im Amtsblatt der Europäischen Union bezweckt die EU, die Entwicklung und den Einsatz sicherer, vertrauenswürdiger und ethischen Prinzipien entsprechender KI-Systeme zu fördern.[13] Dazu schafft sie die harmonisierten Vorschriften für künstliche Intelligenz.[14] Sie möchte sowohl die Vorteile als auch die Risiken von KI angemessen regeln.[15] Dazu zielt die KI-VO u. a. darauf ab, Herausforderungen wie Undurchsichtigkeit, Komplexität, systemischen Bias sowie das teilweise autonome Verhalten und die Unberechenbarkeit verschiedener KI-Systeme wirksam zu regulieren.

Die KI-VO knüpft an die Prinzipien des Produkthaftungsrechtes insbesondere an die dort verwendeten Begrifflichkeiten, wie Anbieter, Betreiber und Hersteller an und nimmt eine Risikoqualifikation des KI-Produktes vor. Zusammen mit der aktuell neu überarbeiteten Produkthaftungsrichtlinie und der geplanten KI-Haftungsrichtlinie[16] bildet die KI-VO den Rahmen für die zukünftige Produkthaftung und Verantwortlichkeit bei KI. Mit der KI-VO soll ein flexibler, dynamischer und zukunftssicherer Rechtsrahmen geschaffen werden, in dem die Anforderungen an die KI-Systeme in einem angemessenen Verhältnis zu den potenziellen Risiken des jeweiligen Systems und den technologischen Entwicklungen stehen.[17] Im Folgenden wird am Beispiel des KI-Produktes „Vektrus" untersucht, ob dies gelungen ist.

3. Vorstellung des KI-Produkts „Vektrus" und dessen Einsatzbereiche

Das KI-System „Vektrus" ist eine SaaS-Lösung, die auf dem Large Language Model von OpenAI's ChatGPT Version 3.5 basiert. „Vektrus" wurde speziell entwickelt, um Social Media-Texte und Content-Pläne zu erstellen und richtet sich primär an Unternehmen, die ihre Social Media-Präsenz er-

2 Der Computer HAL 9000 zeigt in dem Kinofilm 2001 Odyssee im Weltraum (1968) von Stanley Kubrick während der Reise zum Planeten Jupiter zunehmend eine Art neurotisches Verhalten.
3 Die zentrale Maschineninstanz Skynet in der Terminator-Filmreihe (ab 1984) übernimmt die Erde und kämpft gegen die Menschheit.
4 Der lernfähige Computer WOPR (War Operation Plan Response) bringt die Menschheit in WarGames – Kriegsspiele (1983) an den Rand eines Atomkrieges bis er lernt, dass er das Spiel nicht gewinnen kann.
5 Der Computer Deep Thought gibt in der Romanreihe „Per Anhalter durch die Galaxis" des englischen Autors Douglas Adams mit „42" die Antwort auf die Frage nach dem Universum, dem Leben und dem ganzen Rest.
6 J. McCarthy et al., A PROPOSAL FOR THE DARTMOUTH SUMMER RESEARCH PROJECT ON ARTIFICIAL INTELLIGENCE, abrufbar unter https://www-formal.stanford.edu/jmc/history/dartmouth/dartmouth.html (abgerufen am 20.6.2024).
7 *Finlay,* Artificial Intelligence and Maschine Learning for Business, Relavistic Books, 2017, S. 5
8 *Finlay* (Fn. 7), S. 9.
9 *Finlay* (Fn. 7), S. 10.
10 Diese Untersuchung basiert auf der Verordnung (EU) 2024/1689 des Europäischen Parlaments und des Rates vom 13. Juni 2024 zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz und zur Änderung der Verordnungen (EG) Nr. 300/2008, (EU) Nr. 167/2013, (EU) Nr. 168/2013, (EU) 2018/858, (EU) 2018/1139 und (EU) 2019/2144 sowie der Richtlinien 2014/90/EU, (EU) 2016/797 und (EU) 2020/1828 (Verordnung über künstliche Intelligenz).
11 Vgl. zur Definition Prof. Dr. Oliver Bedel in Gabler Wirtschaftslexikon „ChatGPT" steht für „Chat" (dt. „Schwatz") und „Generative Pre-trained Transformer". Es handelt sich um einen Chatbot (bzw. ein System zum Produzieren von Content) von OpenAI, dem das Sprachmodell GPT-3.5 bzw. GPT-4 desselben Unternehmens zugrunde liegt. Die Trainingsdaten stammen u. a. aus Foren, Artikeln und Büchern sowie gesprochener Sprache. Benutzt wird eine spezielle Form von Machine Learning, nämlich Reinforcement Learning from Human Feedback (RLHF). Dabei sind Menschen involviert, die bestimmte Antworten für gut und richtig befinden. Mit ihrem Feedback wird ein Belohnungssystem trainiert, das wiederum den Chatbot trainiert. Herunterladbar unter https://wirtschaftslexikon.gabler.de/definition/chatgpt-124904/version-389664 (abgerufen am 28.6.2024).
12 *Czychowski/Siesmayer,* in: Taeger/Phole ComputerR-HdB, 20.4 Urheberrecht, 2023, Rn. 145.
13 PE/24/2024/REV/1 S. 2.
14 PE/24/2024/REV/1 S. 1.
15 PE/24/2024/REV/1 S. 1.
16 Vgl. Vorschlag für eine Richtlinie über KI-Haftung, COM (2022) 496 final, vom 28.9.2022.
17 PE/24/2024/REV/1 S. 2.

folgreich verstärken möchten, ohne über entsprechendes Know-how zu verfügen. Das KI-System ermöglicht es den Nutzern, ansprechende Inhalte zu erstellen und diese zu optimalen, reichweitenstarken Zeiten zu veröffentlichen.

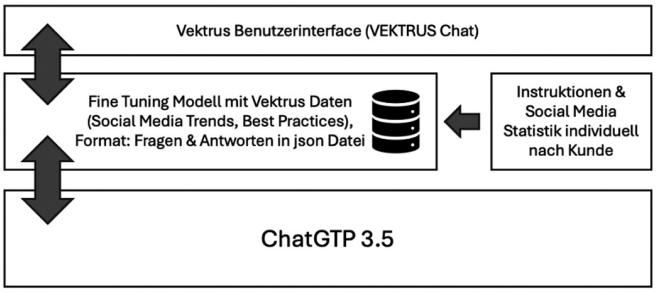

Abb. 1: IT-Architektur „Vektrus", Quelle: Eigene Darstellung

Wie in der Abb. 1 gezeigt, nutzt „Vektrus" OpenAI's Fine-Tuning-Modell, das mit von den Entwicklern gesammelten Informationen über Social Media Marketing-Strategien, Trends und Best Practices trainiert wurde.

Beim Fine-Tuning-Modell wird, grob skizziert, eine Schicht um das Large Language Model (LLM) gelegt und mittels dieser Schicht das LLM aufgabenspezifisch trainiert und sodann „eingefroren". Dieses Training nutzt individuelle Datensätze sowie eine begrenzte Anzahl trainierbarer Parameter, die als Adapter bezeichnet werden. Bildlich gesprochen lässt sich das Fine-Tuning-Modell mit dem Tragen einer rosa Brille vergleichen: Während ChatGPT wie eine normale Brille funktioniert, durch die der Betrachter das gesamte Farbspektrum sehen kann, lässt das Fine-Tuning-Modell alles durch einen rosa Filter erscheinen. Demensprechend limitiert das Fine-Tuning-Modell ChatGPT auf das spezifische Training. Im Falle von „Vektrus" bedeutet das, alles durch eine spezielle Social Media-Brille zu betrachten. Nach diesem Trainingsdurchgang werden die Konten der jeweiligen Kunden individuell mit weiteren Daten angereichert, darunter Statistiken der genutzten Social Media-Kanäle und die entsprechenden Unternehmensinformationen. Diese Datensätze werden monatlich manuell aktualisiert. Dadurch ist es „Vektrus" möglich, mit einigen wenigen Informationen in Form eines Prompts einen auf den Kunden zugeschnittenen Text basierend auf der aktuellen allgemeinen Wissensbasis und den hochgeladenen Dateien zu generieren (siehe Abb. 2).

Für die Zukunft ist geplant, dass „Vektrus" Beiträge semiautomatisch veröffentlichen kann, wobei der Kunde die finale Freigabe erteilt. Zusätzlich soll das System in der Lage sein, Bilder und Videos für den Social Media-Content zu generieren und anzupassen. Um „Vektrus" als bedeutende strategische Investition zu schützen, soll frühzeitig untersucht und sichergestellt werden, dass „Vektrus" in Einklang mit den Vorschriften der KI-VO ist.

Abb. 2: „Vektrus" Chat, Quelle: Von Autoren erstellter Screenshot

II. Prüfung nach EU AI Act

1. Überblick und relevante Bestimmungen des EU AI Acts

Die KI-VO stellt einen umfassenden Rechtsrahmen dar, der darauf abzielt, die Entwicklung und Nutzung von KI in der EU zu regeln, um sowohl Innovation zu fördern als auch ein hohes Schutzniveau vor schädlichen Auswirkungen von KI-Systemen zu gewährleisten (vgl. Art. 1 I KI-VO). Sie gilt für alle Anbieter, die KI-Systeme in der EU auf den Markt bringen oder in Betrieb nehmen, unabhängig davon, ob sie ihren Sitz in der EU oder in einem Drittland haben.

Für KI-Anwendungen wie „Vektrus" gilt es zunächst zu prüfen, ob die KI-VO auf sie anwendbar ist (Art. 2 KI-VO). Dabei ist u. a. festzustellen, in welcher Rolle das Unternehmen „Vektrus" auf den Markt bringt und ob es sich bei „Vektrus" um ein KI-System oder ein KI-Modell mit allgemeinem Verwendungszweck handelt. Sodann ist die Frage zu klären, in welche Risikoklasse „Vektrus" einzuordnen ist, insbesondere ob „Vektrus" eine verbotene KI (Art. 5 KI-VO) oder eine Hochrisiko-KI (Abschnitt 1, Art. 6 ff. KI-VO) ist. Für letztere gelten erhebliche Transparenz-, Dokumentations- und Meldepflichten. Schließlich stellt sich die Frage, ob es sich um ein bestimmtes KI-System nach dem Auffangtatbestand Art. 50 KI-VO mit den dort festgelegten Transparenzpflichten handelt. Sofern es sich um ein KI-Modell mit allgemeinem Verwendungszweck handelt, sind die besonderen Regelungen des Kapitels V (Art. 51 ff. KI-VO) zu beachten.

2. Eröffnung des Anwendungsbereiches der KI-VO

Bevor das KI-System „Vektrus" im Rahmen der KI-VO kategorisiert wird, muss die Frage nach dem Anwendungsbereich der KI-VO geklärt werden. Art. 2 I KI-VO führt zunächst an, für welche Anbieter und Nutzer von KI-Systemen die KI-VO gilt. Als Anbieter wird dabei gem. Art. 3 Nr.3 KI-VO eine natürliche oder juristische Person, Behörde, Einrichtung oder sonstige Stelle bezeichnet, die ein KI-System oder ein KI-Modell mit allgemeinem Verwendungszweck entwickelt oder entwickeln lässt, um es unter eigenem Namen oder eigener Handelsmarke in Betrieb zu nehmen.

Die Entwickler von „Vektrus", eine deutsche GbR, die „Vektrus" erstmals in Deutschland auf den Markt gebracht hat, gelten nach Art. 3 Nr.3 KI-VO als Anbieter und fallen somit unter die Regelungen der KI-VO.

Das hinter „Vektrus" stehende KMU könnte zudem Produkthersteller nach Art. 2 lit. e) KI-VO sein. Es ist nicht klar, was ein Produkthersteller im Sinne der KI-VO ist. Anders als für die Begriffe Anbieter, Betreiber, Einführer, Händler oder nachgelagerter Anbieter findet sich dafür keine explizite Definition in Art. 3 KI-VO. Jedoch könnte die Beschreibung des Produktherstellers in Art. 2 I lit. e) KI-VO im Rahmen des Anwendungsbereiches der KI-VO herangezogen werden, nach der Produkthersteller diejenigen sind, „die das KI-System zusammen mit ihrem Produkt in eigenem Namen oder ihrer Handelsmarke in Verkehr bringen oder in Betrieb nehmen". Da das hinter „Vektrus" stehende KMU jedenfalls Anbieter im Sinne des Art. 3 Nr. 3 KI-VO ist, ist diese auf „Vektrus" anwendbar und eine weitere Diskussion kann an dieser Stelle dahinstehen.

Die Ausnahmefälle des Art. 2 II-IV KI-VO, z. B. Hochrisiko-KI-Systeme, die unter die Regelungen der in Anhang I Abschnitt B aufgeführten Harmonisierungsrechtsvorschriften der Union fallen oder KI-Systeme, die ausschließlich für militärische Anwendungen entwickelt wurden (siehe Art. 2 III KI-VO), sind für „Vektrus" nicht einschlägig. Bei „Vektrus" handelt es sich lediglich um eine Social Media KI für geschäftliche und private Anwendung.

Bei „Vektrus" müsste es sich aber auch um ein KI-System und/oder ein KI-Modell mit allgemeinem Verwendungszweck handeln. Nach Art. 3 Nr.1 KI-VO wird ein KI-System als „ein maschinengestütztes System definiert, das für einen in unterschiedlichem Grade autonomen Betrieb ausgelegt ist und das nach seiner Betriebsaufnahme anpassungsfähig sein kann und das aus den erhaltenen Eingaben für explizite oder implizite Ziele ableitet, wie Ausgaben wie etwa Vorhersagen, Inhalte, Empfehlungen oder Entscheidungen erstellt werden, die physische oder virtuelle Umgebungen beeinflussen können." Diese Definition ist nur schwer verständlich und wurde im Vorfeld zu Recht bereits mehrfach kritisiert[18].

„Vektrus" basiert auf ChatGPT 3.5. Damit basiert es auf einem KI-System, welches als „Generative Pretrained Transformer" qualifiziert wird und eine spezielle Form von Machine Learning, nämlich Reinforcement Learning from Human Feedback (RLHF), einsetzt[19]. Basierend auf den Eingaben durch sog. Prompts erzeugt das System die in der Definition genannten Ausgaben. „Vektrus" ist mithin ein KI-System. Ob „Vektrus" ein KI-Modell mit allgemeinem Verwendungszweck ist, kann für die Bestimmung des Anwendungsbereiches ergo dahinstehen.

Somit gilt die KI-VO uneingeschränkt für das KI-System „Vektrus".

3. Kategorisierung des KI-Systems

Mit der Einführung der KI-VO wird ein risikobasierter Ansatz zur Kategorisierung von KI-Systemen implementiert. Dabei wird zwischen KI-Systemen und KI-Modellen unterschieden, die (1) ein unannehmbares, (2) ein hohes, (3) „Transparenz" oder (4) geringes bzw. minimales Risiko darstellen. Je nach Risikostufe des jeweiligen Systems variieren die zu ergreifenden Maßnahmen und die zu erfüllenden Anforderungen. Die richtige Kategorisierung des Systems ist dabei nicht immer trivial. Abhängig von der Einstufung des Systems entscheidet sich, ob das KI-System aufgrund seines unannehmbaren Risikos gänzlich verboten ist oder in welchem Ausmaß dieses die dargestellten rechtlichen Anforderungen erfüllen muss.

a) Keine verbotene Praktiken im KI-Bereich (Art. 5 KI-VO)

Zunächst ist festzustellen, ob es sich bei dem zu kategorisierenden KI-System um eine Software handelt, die als unannehmbar gilt, weil sie die Werte der EU, wie beispielsweise die Charta der Grundrechte der Europäischen Union, verletzt. Ist dies der Fall, gehört diese zu den verbotenen KI-Systemen und darf bis auf einige wenige Ausnahmen nicht auf den Markt gebracht werden. Von diesem Verbot werden insbesondere solche Praktiken erfasst, die ein erhebliches Potenzial haben, Personen zu manipulieren (vgl. Art. 5 I lit. a) KI-VO) oder die Schwächen bestimmter schutzwürdiger Gruppen wie Kinder ausnutzen, sodass diese Schäden psychischer oder physischer Natur erleiden (vgl. Art. 5 I lit. b) KI-VO). Weiterhin zählt auch das sog. Social-Scoring und der Einsatz von biometrischen Echtzeit-Fernidentifizierungssystemen in öffentlich zugänglichen Räumen bis auf die Ausnahmen nach Art. 5 I lit. c) – h) KI-VO zu den verbotenen Praktiken. „Vektrus" übt keine der oben aufgeführten verbotenen Praktiken aus. „Vektrus" ist also keine verbotene KI nach Art. 5 KI-VO.

b) Hochrisiko KI nach Art. 6 KI-VO

„Vektrus" könnte entsprechend seiner Zweckbestimmung gemäß den bestehenden EU-Produktsicherheitsvorschriften[20] als Hochrisiko-KI-System nach Art. 6 KI-VO klassifiziert werden. Die KI-VO definiert demnach innerhalb der Regelungen des Kapitels III neben den Einstufungsvoraussetzungen auch zwei Hauptkategorien für Hochrisiko-KI-Systeme: Zum einen KI-Systeme, die als Sicherheitskomponenten in Produkten fungieren, welche einer Konformitätsbewertung im Hinblick auf das Inverkehrbringen oder die Inbetriebnahme durch Dritte unterzogen werden müssen, wie in Art. 6 I KI-VO beschrieben. Zum anderen eigenständige KI-Systeme, die in Anhang III explizit aufgeführt sind und die insbesondere Auswirkungen auf die Grundrechte haben, gemäß Art. 6 II KI-VO.

aa) KI ist Sicherheitsbauteil eines harmonisierten Produktes nach Anhang I oder ist ein solches Produkt

Wie bereits erläutert, umfasst die erste Hauptkategorie der Hochrisiko-KI-Systeme u. a. solche, die Sicherheitskomponenten von Produkten darstellen, wie in Anhang I aufgeführt. Diese Kategorie schließt KI-Systeme ein, die eine der zwanzig in der Liste des Anhang I aufgeführten Harmonisierungsrechtsvorschriften der Union fallen, die unterschiedliche Regelungsgegenstände von Spielzeug bis zu Fahrzeugen abdecken. „Vektrus" stellt jedoch keine Sicherheitskomponente eines Produkts im Sinne von Anhang I dar, sondern ein eigenständiges Produkt, welches mithin nicht der Erfüllung von Sicherheitsanforderungen dient.

bb) In Katalog von Anhang III als KI-System aufgezählt und keine Ausnahme nach Abs. 3

Bei den in Anhang III aufgeführten KI-Systemen handelt es sich unter anderem um solche, bei denen es sich bereits gezeigt hat oder absehbar ist, dass die Risiken tatsächlich eintreten. Als Hochrisiko-KI-Systeme gelten demnach solche, die in spezifischen, kritischen Bereichen eingesetzt werden: Diese umfassen die biometrische Identifizierung und Kategorisierung natürlicher Personen (Anhang III Nr.1 KI-VO), den Einsatz in kritischer Infrastruktur (Anhang III Nr. 2 KI-VO), in allgemeiner und beruflicher Bildung (Anhang III Nr.3 KI-VO), im Bereich Beschäftigung, Personalmanagement und Zugang zur Selbständigkeit (An-

18 Beispielhaft *Spies,* KI Act: Definition umstritten. Was ist überhaupt AI (KI)?, beck-blog vom 31.8.2023, aufrufbar unter https://community.beck.de/2023/08/31/ki-act-definition-umstritten-was-ist-ueberhaupt-ai-ki#:~:text=Juristen%20sind%20selbstredend%20besonders%20besorgt,Berechnungen%20in%20einer%20Tabellenkalkulation%20einschlie%C3%9Ft., zuletzt aufgerufen am 28.6.2024.

19 Siehe Definition ChatGTP a. a. O.

20 Verordnung (EU) 2023/988 des Europäischen Parlaments und des Rates vom 10. Mai 2023 über die allgemeine Produktsicherheit, zur Änderung der Verordnung (EU) Nr. 1025/2012 des Europäischen Parlaments und des Rates und der Richtlinie (EU) 2020/1828 des Europäischen Parlaments und des Rates sowie zur Aufhebung der Richtlinie 2001/95/EG des Europäischen Parlaments und des Rates und der Richtlinie 87/357/EWG des Rates.

hang III Nr. 4 KI-VO), zur Zugänglichkeit und Inanspruchnahme grundlegender privater und öffentlicher Dienste und Leistungen (Anhang III Nr. 5 KI-VO), in der Strafverfolgung (Anhang III Nr. 6 KI-VO), in Migration, Asyl und Grenzkontrolle (Anhang III Nr. 7 KI-VO) sowie in der Rechtspflege und bei demokratischen Prozessen (Anhang III Nr. 8 KI-VO).

Fällt ein KI-System nicht unter Anhang III, weist aber ein entsprechend hohes Risiko auf, ist die KI-VO so konzipiert, dass sie anhand einer festgelegten Methodik für die Risikoabschätzung und einer Reihe von Kriterien flexibel auf neue Einsatzbereiche und Anwendungen von KI reagieren kann (vgl. Art. 6 VI – VIII KI-VO).[21]

Nach Art. 6 III KI-VO wird ein in Anhang III aufgeführtes KI-System nicht als hochriskant eingestuft, wenn es kein signifikantes Risiko einer Beeinträchtigung der Gesundheit, Sicherheit oder Grundrechte natürlicher Personen darstellt, insbesondere wenn es den Ausgang von Entscheidungsprozessen nicht wesentlich beeinflusst. Dies ist der Fall, wenn seine Funktionen spezifisch darauf ausgerichtet sind, bestimmte Aufgaben, wie sie in Art. 6 III lit. a)-d) KI-VO näher aufgeführt werden, zu erfüllen. Dies beinhaltet KI-Systeme, die dazu bestimmt sind, eine eng gefasste Verfahrensaufgabe durchzuführen oder das Ergebnis einer bereits abgeschlossenen menschlichen Tätigkeit zu verbessern. Des Weiteren umfasst es Systeme, die entwickelt wurden, um Entscheidungsmuster oder Abweichungen von früheren Entscheidungsmustern zu erkennen, ohne dabei die vorausgegangene menschliche Bewertung zu ersetzen oder ohne angemessene menschliche Überprüfung zu beeinflussen. Zudem betrifft es KI-Systeme, die vorbereitende Aufgaben für Bewertungen ausführen, die für die in Anhang III aufgeführten Anwendungsfälle relevant sind. Die Verwendung von in Anhang III aufgeführten KI-Systemen zum Profiling natürlicher Personen wird weiterhin als hochriskant eingestuft und ist demnach nicht von den Ausnahmeregelungen umfasst.

„Vektrus" ist ein KI-System, das speziell für den Einsatz im Bereich Social Media entwickelt wurde. Es kann basierend auf wenigen Eingaben diverse Inhalte generieren, darunter Beiträge über Mitarbeiter, ansprechende Posts zu den Hauptthemen der Unternehmensaktivitäten oder Stellenausschreibungen. Das Hauptziel von „Vektrus" ist die Erhöhung der Reichweite der jeweiligen Social Media-Accounts. Gerade durch die vielfältigen Einsatzmöglichkeiten von „Vektrus" berühren einige seiner Anwendungsmöglichkeiten kritische Bereiche, die in Anhang III KI-VO aufgeführt sind. Nach Nr. 4a) im Anhang III gelten zu den Hochrisiko-KI-Systemen u. a. solche, „die bestimmungsgemäß für die Einstellung oder Auswahl natürlicher Personen verwendet werden sollen, insbesondere für die Bekanntmachung freier Stellen (…)". Ein KI-System, welches die Möglichkeit hat, ansprechende Stellenausschreibungen zu verfassen, könnte demnach ein Hochrisiko-KI-System darstellen (Abb. 3).

Fraglich ist, ob das bloße Tangieren eines solchen kritischen Bereiches ausreicht, um das System als Hochrisiko-KI-System zu qualifizieren. Zur Beantwortung dieser Frage muss zunächst der Begriff der „bestimmungsgemäßen Verwendung" in Nr. 4a) im Anhang III ausgelegt werden.

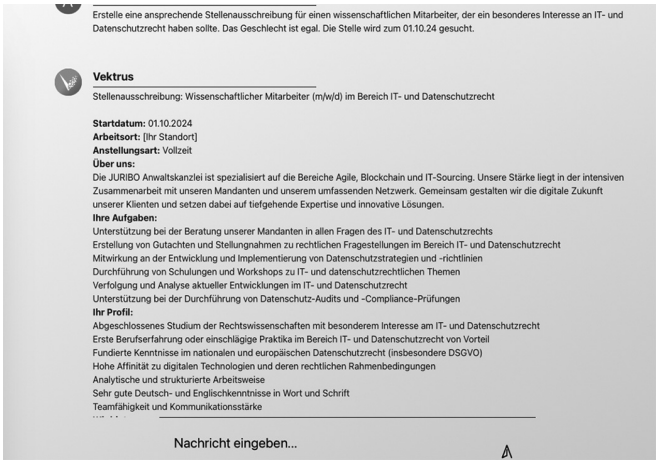

Abb. 3: „Vektrus" Stellenausschreibung, Quelle: Von Autoren erstellter Screenshot

cc) Auslegung „bestimmungsgemäße Verwendung"

Die Verwendung des Wortes „bestimmungsgemäß" zieht sich durch die gesamte KI-VO. Meist wird in diesem Kontext die Verwendung eines KI-Systems in einem bestimmten Anwendungsbereich thematisiert. Wird dies bei der Auslegung des Wortes berücksichtigt, kann schnell festgestellt werden, dass es sich bei der bestimmungsgemäßen Verwendung, um die „Zweckbestimmung" i. S. d. Art. 3 Nr. 12 KI-VO handelt. Der Begriff der „Zweckbestimmung" wird danach definiert als die Verwendung, die für ein KI-System gemäß den Angaben des Anbieters vorgesehen ist. Dies umfasst die spezifischen Einsatzumstände und -bedingungen, wie sie in der Gebrauchsanweisung, in Werbe- oder Verkaufsmaterialien sowie in entsprechenden Erklärungen und der technischen Dokumentation des Anbieters beschrieben werden. Damit richtet sich die Klassifizierung des Systems zu bestimmungsgemäßen Verwendung in Nr. 4a) im Anhang III nach der Zweckbestimmung durch den Anbieter.

Die bestimmungsgemäße Verwendung von „Vektrus" ist die Generierung von Social Media-Inhalten und Content-Plänen zur Erhöhung der Reichweite des jeweiligen Nutzers. Obwohl das KI-System die Möglichkeit des Verfassens von Stellenausschreibungen hat, ist dies nicht der eigentliche Zweck des Systems. Es wird nicht zur Personalgewinnung beworben und soll bestimmungsgemäß nicht dafür eingesetzt werden. Dementsprechend verbieten die geplanten, nachstehend näher erläuterten Nutzungsbedingungen dem Nutzer den Einsatz von „Vektrus" für die Einstellung oder Auswahl natürlicher Personen, insbesondere für die Bekanntmachung freier Stellen. Der Art. 13 III lit. b) iii) KI-VO verlangt darüber hinaus aber, dass Anbieter auch die vernünftigerweise vorhersehbare Fehlanwendung i. S. d. Art. 3 Nr. 13 KI-VO ihrer (Hochrisiko-KI-)Systeme berücksichtigten und die bekannten oder vorhersehbaren Umstände der Verwendung in der Betriebsanleitung dokumentieren.[22] Dies bedeutet, dass eine über die ursprüngliche Zweckbestimmung des KI-Systems hinausgehende Nutzung durch den Anwender nicht zur Neukategorisierung des KI-Systems führt, solange die zweckbestimmte Verwendung ausreichend verständlich dargelegt wurde. Die Anbieter müssen alle Nutzungsszenarien ihres Systems bedenken

21 Vgl. PE/24/2024/REV/1 S. 43.
22 PE/24/2024/REV/1 S. 19.

und diese explizit in der Betriebsanleitung, sowie in Werbe- und Verkaufsmaterialien, entsprechenden Erklärungen sowie der technischen Dokumentation adressieren. Dies kann durch die Nutzungsbedingungen zusätzlich organisatorisch verankert werden. Die Nutzungsbedingungen wurden im Einklang mit der Betriebsanleitung soweit ausgestaltet, dass sowohl erwünschte als auch ausdrücklich untersagte Nutzungsszenarien, sog. Dos & Don'ts, im Rahmen der Verwendung von „Vektrus" definiert wurden. Zur Förderung des Nutzerverständnisses wurden diese Szenarien zudem in der Betriebsanleitung durch gezielte Beispiele und visuelle Darstellungen ausführlich erläutert. Bei „Vektrus" handelt es sich damit nicht um ein Hochrisiko-KI-System i. S. d. Art. 6 KI-VO.

c) KI-Modell mit allgemeinem Verwendungszweck Art. 51 ff.KI-VO, ggfs. Qualifikation „systemische Risiko"

Für „Vektrus" könnten, als auf ChatGPT 3.5 basierendes KI-System, die Regelungen für die KI-Modelle mit allgemeinem Verwendungszweck gelten. Solche KI-Modelle werden innerhalb der KI-VO in einfache KI-Modelle mit allgemeinem Verwendungszweck (vgl. Art. 51 II KI-VO) und solche mit systemischem Risiko (vgl. Art. 51 I KI-VO) unterschieden. Diese Modelle sind von den zuvor erwähnten KI-Systemen zu trennen.[23] Es ist an dieser Stelle klarzustellen, dass KI-Modelle grundsätzlich wesentliche Komponenten von KI-Systemen sind und erst durch bspw. das Hinzufügen einer Nutzerschnittstelle zu KI-Systemen werden.[24] Im Rahmen dieser Betrachtung sind daher auch KI-Modelle zu berücksichtigen, da die KI-VO klarstellt, dass die spezifischen Vorschriften für die KI-Modelle auch gelten, wenn diese in ein KI-System integriert oder ein Teil davon sind.[25]

Ein KI-Modell mit allgemeinem Verwendungszweck ist nach Art. 3 Nr. 63 KI-VO „ein KI-Modell – einschließlich der Fälle, in denen ein solches KI-Modell mit einer großen Datenmenge unter umfassender Selbstüberwachung trainiert wird –, das eine erhebliche allgemeine Verwendbarkeit aufweist und in der Lage ist, unabhängig von der Art und Weise seines Inverkehrbringens ein breites Spektrum unterschiedlicher Aufgaben kompetent zu erfüllen, und das in eine Vielzahl nachgelagerter Systeme oder Anwendungen integriert werden kann, ausgenommen KI-Modelle, die vor ihrem Inverkehrbringen für Forschungs- und Entwicklungstätigkeiten oder die Konzipierung von Prototypen eingesetzt werden." Eingeschlossen davon sind ebenso die Fälle, in denen ein solches KI-Modell mit einer großen Datenmenge unter umfassender Selbstüberwachung trainiert wird. Die allgemeine Verwendbarkeit wird dabei u. a. auch bei der Verarbeitung von mindestens einer Milliarde Parameter angenommen.[26]

Ein „systemisches Risiko" i. S. d. Art. 3 Nr. 65 KI-VO durch das KI-Modell liegt hingegen bei einem Risiko vor, „das für die Fähigkeiten mit hoher Wirkkraft von KI-Modellen mit allgemeinem Verwendungszweck spezifisch ist und aufgrund der Reichweite oder aufgrund tatsächlicher oder vernünftigerweise vorhersehbarer negativer Folgen für die öffentliche Gesundheit, Sicherheit, öffentliche Sicherheit, Grundrechte oder Gesellschaft insgesamt erhebliche Auswirkungen auf den europäischen Markt hat, die sich in großem Umfang über die gesamte Wertschöpfungskette hinweg verbreiten können." Die genauen Einstufungsbedingungen werden in Art. 51 I KI-VO ausgeführt. Ist der geltende Schwellenwert für Fähigkeiten mit hoher Wirkkraft (vgl. Art. 3 Nr.64 KI-VO & Anhang XIII) erreicht, ist anzunehmen, dass ein systemisches Risiko vorliegt.[27]

Wie bereits eingangs erwähnt, stellt „Vektrus" ein KI-System dar, das über eine API-Schnittstelle zu ChatGPT verfügt. ChatGPT stellt damit eine wesentliche Komponente des KI-Systems dar. Bei ChatGPT handelt es sich um ein Multimodal Large Language Model, welches ca. 200 Milliarden Parameter verarbeitet.[28] ChatGPT hat somit eine erhebliche allgemeine Verwendbarkeit, wodurch es in der Lage ist unterschiedliche Aufgaben kompetent zu erfüllen und in solch nachgelagerte Systeme wie „Vektrus" integriert zu werden. Folglich fällt ChatGPT unter die Definition eines KI-Modells mit allgemeinem Verwendungszweck. Zudem kann den Erwägungsgründen in Absatz 99 und 105 der KI-VO entnommen werden, dass insbesondere große generative KI-Modelle als typisches Beispiel für diese Klassifizierung herangezogen werden.[29] Trotz der Leistungsstärke des Generative Foundation-Modells ChatGPT, welches den oben erwähnten Schwellenwert überschreitet, gilt das Modell nach Einschätzung der EU nicht als risikoreich, ist aber gründlich zu bewerten und Vorfälle sind zu melden.[30]

Im Gegensatz zu dem dargestellten KI-Modell handelt es sich bei „Vektrus" bereits nicht um ein KI-System mit allgemeinem Verwendungszweck, wie sie in Art. 3 Nr.66 KI-VO definiert wird. Dem KI-System fehlt es an dieser Stelle an der Möglichkeit einer Vielzahl von Zwecken[31] zu dienen.[32] Weiterhin überschreitet „Vektrus" nicht den geltenden Schwellenwert für Fähigkeiten mit hoher Wirkkraft. „Vektrus" und das zugrunde liegende ChatGPT Fine-Tuning-Modell überschreiten nicht die Schwelle der kumulierten Menge der für das Training verwendeten Berechnungen von mehr als 10^{25} Gleitkommaoperationen.

Die Integration von ChatGPT 3.5 als KI-Modell mit allgemeinem Verwendungszweck hat folglich keine weiteren Auswirkungen auf die Kategorisierung von „Vektrus" als KI-System gem. Art. 53 ff. KI-VO.

d) Bestimmte KI-Systeme nach Art. 50 KI-VO

Art. 50 KI-VO verzichtet auf eine umfangreiche Definition der dort genannten KI-Systeme. Stattdessen legt er eine Transparenzpflicht für bestimmte Typen von KI-Systemen fest. Explizit werden vier Arten von KI-Systemen genannt, die besonderen Transparenzanforderungen unterliegen. Zunächst wird die Transparenzpflicht KI-Systemen auferlegt, die für die direkte Interaktion mit natürlichen Personen entwickelt wurden (Art. 50 I KI-VO), wie beispielsweise Chatbots. Diese Pflicht erstreckt sich auch auf KI-Systeme, die synthetische Audio-, Bild-, Video- oder Textinhalte erzeugen sowie auf KI-Systeme mit allgemeinem Verwendungszweck (Art. 50 II KI-VO). Des Weiteren

23 PE/24/2024/REV/1 S. 26.
24 PE/24/2024/REV/1 S. 26.
25 PE/24/2024/REV/1 S. 26.
26 PE/24/2024/REV/1 S. 26.
27 PE/24/2024/REV/1 S. 29.
28 Abrufbar unter https://chatopenai.de (abgerufen 26.6.2024).
29 PE/24/2024/REV/1 S. 26.
30 Abrufbar unter https://www.europarl.europa.eu/topics/de/article/20230601STO93804/ki-gesetz-erste-regulierung-der-kunstlichen-intelligenz (abgerufen 26.6.2024).
31 Siehe Definition der Zweckbestimmung gem. Art. 3 Nr.12 KI-VO.
32 PE/24/2024/REV/1 S. 26.

schreibt Art. 50 III KI-VO spezifische Transparenzanforderungen für Systeme zur Emotionserkennung, biometrische Kategorisierungssysteme und KI-Systeme, die Deepfake erzeugen (Art. 50 IV KI-VO), vor.

Der Hintergrund der Einführung spezifischer Transparenzanforderungen für KI-Systeme nach Art. 50 II KI-VO ist, dass die zunehmende Menge an synthetisch erzeugten Inhalten es immer schwieriger macht, diese von Menschen geschaffenen und authentischen Inhalten zu unterscheiden.[33] Insbesondere die breite Verfügbarkeit und die fortgeschrittenen Fähigkeiten dieser Systeme haben erhebliche Auswirkungen auf die Integrität des Informationsökosystems und das Vertrauen, das ihm entgegengebracht wird.[34] Dies führt unter anderem zu Risiken hinsichtlich der Verbreitung von Fehlinformationen und der Manipulation von Inhalten in großem Maßstab, beispielsweise in Form von Betrug oder Täuschung der Verbraucher.[35]

Bei „Vektrus" handelte es sich nach alledem um ein bestimmtes KI-System, welches aktuell synthetische Textinhalte erzeugt. Zukünftig soll dieser Funktionsumfang zudem um das Erzeugen von synthetischen Bild- und Videoinhalten erweitert werden. Folglich treffen die Anbieter von „Vektrus" die Pflichten des Art. 50 II KI-VO über die Transparenz- und Informationspflichten für entsprechende KI-Systeme. Auch muss „Vektrus" das europäische Urheberrecht[36] berücksichtigen und einhalten. Denn das Urheberrecht und die KI-VO stehen in einem parallelen Verhältnis zueinander.

4. Anforderung an Transparenz, Datenschutz und Sicherheit

Fällt das KI-System in die Kategorie der KI-System mit geringem Risiko nach Art. 50 I, II KI-VO, treffen den Anbieter nur wenige Anforderungen. Das in diesem Rahmen betrachtete KI-System gehört wie oben erläutert zu einem solchen bestimmten KI-System.

Anbieter generativer KI-Systeme i. S. d. Art. 50 II KI-VO müssen sicherstellen, dass technische Lösungen integriert werden, die die Kennzeichnung in einem maschinenlesbaren Format und die Feststellung ermöglichen, dass die Ausgabe von einem KI-System und nicht von einem Menschen erzeugt oder manipuliert wurde. Dabei kann Ausgabe grammatikalisch grundsätzlich weit verstanden werden, d. h. es könnte auch die Weitergabe von Ausgaben an Dritte einschließen und eine entsprechende Kennzeichnungspflicht auslösen. Jedoch ist die Kennzeichnungspflicht in Art. 50 II KI-VO systemisch von der Offenlegungspflicht der Anbieter bei Deepfakes in Art. 50 IV KI-VO zu unterscheiden. Während bei ersterer die Kennzeichnung der Ausgabe des KI-Systems verlangt wird, entscheidet sich der Gesetzgeber bewusst für die Begriff der „Offenlegung". Dies weist darauf hin, dass die unmittelbare Erkennbarkeit von künstlich erzeugten Inhalten nach Art. 50 IV KI-VO durch beliebige Dritte gewährleistet sein muss, u. a. durch Wasserzeichen, Protokollierungsmethoden oder andere Techniken, oder eine Kombination solcher Techniken.[37].

Für diese Auslegung spricht zudem die Anforderung bei Deepfakes, bei offensichtlich künstlerischen, kreativen, satirischen, fiktionalen oder analogen Werken oder Programmen die Offenlegung in einer Weise vorzunehmen, dass die Darstellung und der Genuss des Werkes nicht beeinträchtigt werden. Entsprechend verhält es sich bei Texten, die die Öffentlichkeit über Angelegenheiten von öffentlichem Interesse informieren. Die Anforderungen in Art. 50 II KI-VO sind demgegenüber viel toleranter. Dort wird keine Neutralität der Kennzeichnung in Bezug auf die Darstellung des Werkes gefordert, obwohl auch an dieser Stelle Audio-, Bild-, Video-, und Textinhalte ausgegeben werden. Dementsprechend beschränkt sich die Kennzeichnungspflicht nach Art. 50 II KI-VO lediglich auf die unmittelbare Ausgabe und könnte ggfs. sogar mit einem einfachen Hinweistext umgesetzt werden.

Bei der Umsetzung der Transparenzverpflichtung werden u. a. die spezifischen Eigenschaften und Beschränkungen verschiedener Inhaltsarten ebenso berücksichtigt wie die Umsetzungskosten sowie einschlägigen technologischen und marktbezogenen Entwicklungen in diesem Bereich, wie insbesondere der aktuelle Stand der Technik.[38] Die entsprechenden Techniken können dabei sowohl auf der Ebene des KI-Systems als auch des verwendeten KI-Modells implementiert werden.[39]

Für die Anbieter von „Vektrus" bedeutet dies, dass sie eine klare und den Barrierefreiheitsanforderungen (vgl. Art. 50 V KI-VO) entsprechende Kennzeichnung gegenüber den Betreibern vornehmen müssen. In der Praxis könnte dies durch einen Disclaimer realisiert werden, der ähnlich wie bei ChatGPT dauerhaft unterhalb des Eingabefeldes platziert wird. Dieser könnte beispielsweise lauten: „Die von Vektrus generierte Antwort basiert auf künstlich erzeugten/manipulierten Inhalten. Die zugrundeliegende Informationsbasis basiert auf dem Stand von September 2024. Eine Garantie für die Richtigkeit der Inhalte wird nicht übernommen." Zusätzlich könnte beim Aufruf der Chatseite von „Vektrus" ein Popup-Fenster eingesetzt werden, das zu Beginn jeder Sitzung erscheint. Der Betreiber müsste dann die Kenntnisnahme des Disclaimers durch einen Klick bestätigen.

Weitere spezifische Anforderungen an den Datenschutz und die Sicherheit werden nicht an KI-Systeme i. S. d. Art. 50 II KI-VO gestellt. Selbstverständlich muss die Datenverarbeitung im KI-System auch den bekannten Anforderungen der DSGVO entsprechen (Art. 2 VII KI-VO). Insgesamt bestehen deutliche Erleichterung für die Anbieter von „Vektrus" als i. S. d. Art. 50 KI-VO „bestimmtes" KI-System im Vergleich zu Anbietern und Betreibern von Hochrisiko-KI-Systemen.

III. Hinweise für die Gestaltung der Nutzungsbedingungen der KI-basierten SaaS-Lösung

Anbieter von KI-System jeglicher Art sollten grundsätzlich ihre Betreiber in die Lage versetzen zu verstehen, wie ihr KI-System funktioniert und wo seine Stärken und Grenzen liegen. Die zur Verfügung gestellten Informationen sollen u. a. eine zweckfremde Nutzung des Systems verhindern und stattdessen eine ordnungsgemäße Verwendung er-

33 PE/24/2024/REV/1 S. 34.
34 PE/24/2024/REV/1 S. 34.
35 PE/24/2024/REV/1 S. 34.
36 Vgl. European Commission, „Trends and developments in artificial intelligence", 2020, abrufbar unter: https://op.europa.eu/en/publication-detail/-/publication/394345a1-2ecf-11eb-b27b-01aa75ed71a1/language-en ,abgerufen am 18.10.2024, S. 67.
37 PE/24/2024/REV/1 S. 34.
38 PE/24/2024/REV/1 S. 34.
39 PE/24/2024/REV/1 S. 34.

leichtern. Dabei steht die klar definierte zweckbestimmte Verwendung des KI-Systems im Vordergrund der Ausführungen. Erst diese unmissverständlichen Verwendungsbestimmungen einschließlich der besonderen Umstände und Bedingungen der Verwendung ermöglichen eine saubere und rechtssichere Kategorisierung des KI-Systems innerhalb der KI-VO.

Informationsmedium seitens des Anbieters ist dabei nach Art. 3 Nr.12 KI-VO die Betriebsanleitung, Werbe- oder Verkaufsmaterial, diesbezügliche Erklärungen und die technische Dokumentation. Hinzu treten insbesondere auch die Nutzungsbedingungen für KI-Systeme.

Zu den bereitgestellten Informationen in der Betriebsanleitung gehören Merkmale, Fähigkeiten und Leistungseinschränkungen des entsprechenden KI-Systems.[40] Durch diese Informationen sollen die Nutzer bei der Verwendung des Systems u. a. über die beabsichtigten und ausgeschlossenen Verwendungszwecke informiert werden, um eine korrekte und angemessene Verwendung des Systems zu ermöglichen.[41] Es ist für ein besseres Verständnis empfohlen, anschauliche Beispiele zu den Beschränkungen und ausgeschlossenen Verwendungen anzuführen,[42] Es ist für eine aussagekräftige, umfassende, zugängliche und verständliche Darstellung der Informationen zu sorgen.[43]

Die eingangs genannte technische Dokumentation ist eine Anforderung, die in Bezug auf Hochrisiko-KI-Systemen gestellt und in Art. 11 KI-VO geregelt wird. Sie umfasst unter anderem Informationen über die allgemeinen Merkmale, Fähigkeiten und Grenzen des Systems, die verwendeten Algorithmen sowie die Daten- und Verfahren zu Training, Testung und Validierung.[44] KI-Systeme wie „Vektrus“ müssen diese Anforderungen nicht erfüllen. Daher ist es für Anbieter ratsam, alternative Strategien zu verfolgen, um die zweckbestimmte Verwendung ihres KI-Systems sicherzustellen.

Ergänzend zu den expliziten Regelungen innerhalb der KI-VO steht es den Anbietern frei, eigene Nutzungsbedingungen in ihre Vertragsbeziehung einzubinden und darüber die Nutzung eindeutig festzulegen. Dies kann grundsätzlich in Form von Allgemeinen Geschäftsbedingungen (AGB) oder spezifischen Vertragsklauseln erfolgen. Innerhalb dieser Nutzungsbedingungen besteht die Möglichkeit, ähnlich wie in der Betriebsanleitung, die Verwendungsmöglichkeiten des KI-Systems einzuschränken. Es wird empfohlen, die versprochene Leistung des KI-Systems, seinen dedizierten Anwendungsbereich sowie Anweisungen für eine korrekte und angemessene Nutzung des Systems detailliert auszuführen. Diese Regelungen sollten zusätzlich mit Vertragsstrafen und außerordentliche Kündigungsoptionen für den Fall einer missbräuchlichen Nutzung des KI-Systems abgesichert werden. Trotz der Unschärfen der KI-VO können Anbieter auf diesem Weg zweckfremden Nutzungen entgegenwirken und ihr Risiko sowie ggfs. eine mögliche Höherstufung zur Hochrisiko-KI mit weitreichenden zusätzlichen Pflichten reduzieren.

IV. Abschluss und Ausblick

Insgesamt zeigt sich, dass die KI-VO handwerklich an einigen Stellen verbesserungsbedürftig ist. Insbesondere ist die Definition von KI-Systemen nur schwer verständlich und nicht trennscharf. Auch fehlt es an einer expliziten Definition des Produktherstellers im Vergleich zu anderen Begriffen, wie Anbieter, Betreiber oder Einführer. Der Verzicht auf eine solche Definition wirft eine Unsicherheit auf, die mit Leichtigkeit hätte vermieden werden können. Die weitere Ausgestaltung durch delegierte Rechtsakte sowie Empfehlungen und Verhaltenskodizes des neu zu schaffenden Büros für künstliche Intelligenz sowie ggfs. eine Fortentwicklung durch die Rechtsprechung wird mit Spannung zu verfolgen sein.

In der Praxis empfiehlt es sich für Unternehmen, den Rahmen der KI-VO noch nicht vollständig auszureizen, bis sich eine hinreichende Rechtssicherheit eingestellt hat. Gerade für KMU empfiehlt es sich, die Klassifizierung als Hochrisiko-KI-System über die vorangestellten Wege nach Möglichkeit zu vermeiden.

40 PE/24/2024/REV/1 S. 21.
41 PE/24/2024/REV/1 S. 21.
42 PE/24/2024/REV/1 S. 21.
43 PE/24/2024/REV/1 S. 21.
44 PE/24/2024/REV/1 S. 20.

Report

Prof. Dr. Dagmar Gesmann-Nuissl*

Rechtsprechungsreport „Innovations- und Technikrecht“

I. Aktuelle Rechtsprechung zum Innovationsrecht

1. Text und Data Mining-Schranken beim Erstellen von KI-Trainingsdatensätzen

Das Vervielfältigen von Bilddaten zur Herstellung eines KI-Trainingsdatensatzes kann als Text und Data Mining zum Zweck der wissenschaftlichen Forschung nach § 60d UrhG privilegiert sein, wie das LG Hamburg mit Urteil vom 27.9. 2024 befand (Az. 310 O 227/23).

* Mehr über die Autorin erfahren Sie auf S. III.