„Mit dem KI-Verordnungsentwurf unternimmt die Kommission einen mutigen Versuch der weltweit ers-ten umfassenden KI-Regulierung.“

Aufsatz

Der AIA und Legal Tech – Der (goldene) Käfig für Künstliche Intelligenz?

Isabel Ecker und Philipp Mahlow

Open Peer Review

Dieser Beitrag wurde lektoriert von: Lisa Krebber und Michelle Duda

Isabel hat Jura an der Universität zu Köln studiert. Sie schreibt nun ihre Promotion im Bereich des Wirtschaftsstrafrechts bei Herrn Professor Waßmer und ist Promotionsstipendiatin der Studienstiftung des deutschen Volkes. Zudem ist sie Vorstandsmitglied des Legal Tech Lab Cologne.

Philipp hat Jura an der Universität zu Köln mit dem Schwerpunkt Geistiges Eigentum und Wettbewerbsrecht studiert. Er bereitet zur Zeit seine Promotion im KI-Recht vor. Er ist Redakteur für die CTRL.

Der am 21.04.2021 vorgestellte KI-Verordnungsentwurf (KI-VO-E)[1] der Europäischen Kommission[2] stellt den Abschluss einer langjährigen europäischen Beschäftigung mit Künstlicher Intelligenz dar. Bereits mit seinem Entschluss vom 16.02.2017[3] forderte das Europäische Parlament die Kommission dazu auf, einen Vorschlag für eine Richtlinie über „zivilrechtliche Regelungen im Bereich Robotik zu unterbreiten“. Ferner solle die Kommission zur Überprüfung angehalten werden, ob

1 Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union Legislative Acts, COM(2021) 206 final, fortan als “KI-VO-E”, “KI-Verordnungsentwurf” oder “Entwurf” bezeichnet.

2 Fortan bezeichnet als “Kommission”.

3 Entschließung des Europäischen Parlaments vom 16.02.2017 mit Empfehlungen an die Kommission zu zivilrechtlichen Regelungen im Bereich Robotik (2015/2103(INL)).

die Gründung einer EU-Agentur für Robotik und Künstliche Intelligenz sinnvoll sei. Die Kommission reagierte mit der Veröffentlichung einer KI-Strategie: „Künstliche Intelligenz für Europa“,[4] einem „Koordinierten Plan für Künstliche Intelligenz“[5] und der Einrichtung der Hochrangigen Expertengruppe für Künstliche Intelligenz[6]. Diese Gruppe erarbeitete Ethik-Leitlinien[7], die ein KI-System beachten sollte, um als vertrauenswürdig zu gelten.[8]

Schließlich stellte die Kommission im Februar 2020 ein Weißbuch „Zur Künstlichen Intelligenz – ein europäisches Konzept für Exzellenz und Vertrauen“[9] vor. Allein die Menge an vorgestellten regulatorischen Ergebnissen innerhalb einer Zeitspanne von nur vier Jahren zeigt den Stellenwert, den die EU der KI-Regulierung beimisst. Die Kommission selbst betont mehrfach die rapide Entwicklung der KI-Technologie.[10] Diese schnellen technischen Entwicklungen in Verbindung mit den potenziell großen Gefahren künstlich intelligenter Systeme für die Europäischen Grundwerte[11] veranlassten die Kommission nun, diesen Herausforderungen mit dem KI-VO-E zu begegnen.

A. Regulatorische Ziele der Kommission

Die Regulierung von Künstlicher Intelligenz spielt sich in einem „Motivdreieck“[12] verschiedener Interessen ab. Zunächst möchten KI-Unternehmen die größtmögliche Freiheit zur Innovation der Technologie genießen, ohne unnötigem Compliance-Aufwand und gesetzlichen Grenzen ausgesetzt zu sein. Dies soll letztlich zu einer optimalen Monetarisierung des eingebrachten Entwicklungsaufwands führen. Daneben sollen die Grundrechte der europäischen Bevölkerung vor der Realisierung dystopisch anmutender Szenarien[13] durch missbräuchliche oder unvorsichtige Nutzung von KI-Systemen geschützt zu werden. Zuletzt hat die Europäische Union als Wirtschaftsstandort das Bedürfnis, für Entwickler[14] und Verwender dieser zukunftsweisenden Technologie attraktiv zu bleiben, um ihren geopolitischen Einfluss in Wirtschaftsfragen zu sichern.

Um diesen unterschiedlichen Interessen zu begegnen, legt die Kommission drei Ziele des KI-VO-E fest: Zum einen darf der KI-VO-E keinen innovationshemmenden, unverhältnismäßigen Verwaltungsaufwand für die KI-Erzeuger und -Verwender bedeuten.[15] Zweitens muss die entsprechende Regulierung die Berücksichtigung der europäischen Werte, insbesondere der europäischen Grundrechte, sicherstellen.[16] Somit soll dann das von der Kommission mehrfach angesprochene „Vertrauen“[17] der Bürger in die Technologie gestärkt werden.

Letztlich bleibt zu beachten, dass die EU nicht verheimlicht, ihre Werte „in die Welt hinaus exportieren“[18] zu wollen. Dieser von ***Bradford*** als „***Brussels Effect***“[19] beschriebene internationale Einfluss Europas durch das Einnehmen einer regulatorischen Vorreiterrolle kann klar am Beispiel der DSGVO aufgezeigt werden. Seit deren Inkrafttreten im Mai 2018 haben fast 120 Länder von der DSGVO inspirierte Datenschutzgesetze erlassen.[20] Ähnliche internationale Wirkung scheint die Kommission auch mit dem KI-VO-E erreichen zu wollen.[21]

4 Mitteilung der Kommission, Künstliche Intelligenz für Europa, COM(2018) 237 final.
5 Mitteilung der Kommission, Koordinierter Plan für künstliche Intelligenz, COM(2018) 795 final.
6 Die Einrichtung erfolgte durch die Kommission am 09.03.2018, siehe hierzu die Pressemitteilung vom selbigen Tage, hier abrufbar (Stand: 15.12.2021).
7 Hier abrufbar (Stand: 15.12.2021).
8 Insbesondere diese sieben Schlüsselkriterien: 1) Vorrang menschlichen Handelns und menschliche Aufsicht, 2) technische Robustheit und Sicherheit, 3) Schutz der Privatsphäre und Datenqualitätsmanagement, 4) Transparenz, 5) Vielfalt, Nichtdiskriminierung und Fairness, 6) gesellschaftliches und ökologisches Wohlergehen sowie 7) Rechenschaftspflicht.
9 Weißbuch zur Künstlichen Intelligenz – ein europäisches Konzept für Exzellenz und Vertrauen, COM(2020) 65 final.
10 Siehe z.B. in Zur Künstlichen Intelligenz – ein europäisches Konzept für Exzellenz und Vertrauen, COM(2020) 65 final, S. 1; KI-VO-E, COM(2021) 206 final, S. 1.
11 KI-VO-E, COM(2021) 206 final, S. 12 f.
12 *Valta/Vasel*, ZRP 2021, 142.
13 Ebd., 143.
14 Zum Zwecke der besseren Lesbarkeit wird bei personenbezogenen Hauptwörtern nur die männliche Form verwendet. Diese Begriffe sollen jedoch für alle Geschlechter gelten.
15 Dies kann Erwägungsgrund 71 entnommen werden, der einen „innovationsfreundlichen […] Rechtsrahmen“ verspricht.
16 KI-VO-E, COM(2021) 206, S. 12 f.; *Geminn*, ZD 2021, 354 (356), der jedoch kritisiert, dass die Rolle der Grundrechte „darauf reduziert [wird], an ihrem Maßstab eine Risikobewertung vorzunehmen“.
17 So z.B. KI-VO-E, COM(2021) 206 final, “1.1. Gründe und Ziele des Vorschlags und Erwägungsgrund 5“; COM(2020) 65 final, S. 2, 3, 10 ff.
18 *Gaumond*, “AIA: What is the European Approach for AI?”, hier abrufbar: (Stand: 15.12.2021).
19 *Bradford*, The Brussels Effect, Northwestern University Law Review, Vol. 107 (1), 2012, S. 25 ff.; *Dies.*, The Brussels Effect – How Europe Rules the World, 2020.
20 Ebd.
21 Zweifel daran äußern *Valta/Vasel*, ZRP 2021, 142 (144 f.).

B. Anwendungsbereich

Gem. Art. 2 I KI-VO-E gilt der Entwurf für Anbieter und Nutzer von KI-Systemen. Obgleich Art. 2 und 3 KI-VO-E die zentralen Begriffe zur Bestimmung des Anwendungsbereichs definieren, sind große Diskussionen um die verwendeten Definitionen entstanden.[22] Gem. Art. 3 Nr. 1 versteht der KI-VO-E unter künstlich intelligenten Systemen:

„Software, die mit einer oder mehreren der in Anhang I aufgeführten Techniken und Konzepte entwickelt worden ist und im Hinblick auf eine Reihe von Zielen, die vom Menschen festgelegt werden, Ergebnisse wie Inhalte, Vorhersagen, Empfehlungen oder Entscheidungen hervorbringen kann, die das Umfeld beeinflussen, mit dem sie interagieren"

Im Anhang I zum KI-VO-E werden dann als künstlich intelligent verstandene Techniken und Konzepte aufgeführt.[23] Trotz dieser Konkretisierung wird die Definition zu Recht als denkbar weit bezeichnet.[24] Der Kommission ist zuzugestehen, dass keine allgemein akzeptierte Definition von KI existiert, auf die hätte zurückgegriffen werden können.[25] Die Kommission definiert KI-Systeme so „technologieneutral und zukunftstauglich wie möglich"[26] und behält sich gem. Art. 4, 73 KI-VO-E vor, den Anhang I an Marktentwicklungen und technische Entwicklungen anzupassen.

> „Der KI-Begriff ist schlicht zu weit und grenzt künstlich intelligente Systeme nicht trennscharf genug von unintelligenten Software-Systemen ab."

Dieser Kunstgriff ist regulierungstechnisch insoweit zu begrüßen, da so der jeweilige tatsächliche Stand der Technik berücksichtigt werden kann. Zu Recht wird jedoch einerseits kritisiert, dass bereits die Definition Kriterien enthält, die nicht nur KI-Systeme, sondern grundsätzlich auch nicht künstlich intelligente Software erfasst.[27] Andererseits verwundert, dass weder die Definition, noch der Anhang I tatsächlich KI-spezifische Funktionen oder Eigenschaften enthalten.[28]

Vorteilhafter könnte es sein, statt einer positiven Definition von KI-Systemen eine negative Abgrenzung zu anderer Software anhand dessen vorzunehmen, ob das System regelbasiert oder regelunabhängig funktioniert.[29] Zumindest scheint sich abzuzeichnen, dass die Kommission den KI-Begriff in seiner Reichweite beschränken wird.[30]

C. Kategorisierung von KI

In Ermangelung sinnvoller Alternativen hat die Kommission einen besonderen Regulierungsansatz gewählt: Statt sektorspezifisch jedes Anwendungsgebiet Künstlicher Intelligenz zu regulieren, wählt die Kommission einen sektorübergreifenden, also horizontalen[31] Regulierungsansatz. Dieser knüpft Rechtsfolgen an die Einordnung der Anwendung des jeweiligen KI-Systems in eine entsprechende Risikogruppe.

22 Beschränkt werden soll sich auf die Erläuterung der Diskussion des zentralen KI-Begriffs des KI-VO-E. Zum Problem der rückwirkenden Anwendbarkeit der KI-VO auf außer-europäisch hergestellten KI-Output, welcher ohne Kenntnis oder Zutun des Herstellers in den EU-Binnenmarkt eingeführt wird siehe: *BVMED*, MPR 2021, 176 (179); *Geminn*, ZD 2021, 354 (356).

23 „a) Konzepte des maschinellen Lernens, mit beaufsichtigtem, unbeaufsichtigtem und bestärkendem Lernen unter Verwendung einer breiten Palette von Methoden, einschließlich des tiefen Lernens (Deep Learning); b) Logik- und wissensgestützte Konzepte, einschließlich Wissensrepräsentation, induktiver (logischer) Programmierung, Wissensgrundlagen, Inferenz- und Deduktionsmaschinen, (symbolischer) Schlussfolgerungs- und Expertensysteme; c) Statistische Ansätze, Bayessche Schätz-, Such- und Optimierungsmethoden."

24 *BVMED*, MPR 2021, 176 (177 f.); *Engelmann/Brunotte/Lütkens*, RDi 2021, 317 (318 f.).

25 *Ebers/Heinze u.a.*, Künstliche Intelligenz und Robotik, 2020, § 3 Rn. 4; *Kaulartz/Braegelmann*, Rechtshandbuch Artificial Intelligence und Machine Learning, 2020, Kap. 1 Rn. 2 ff.; *Hacker*, NJW 2020, 2142, (2142 f.), der sich dafür ausspricht, statt von KI von Maschinellem Lernen zu sprechen.

26 KI-VO-E, COM(2021) 206 final, S. 14.

27 Mit Bezug auf den zweiten Satzteil: *„Software, die … im Hinblick auf eine Reihe von Zielen, die vom Menschen festgelegt werden, Ergebnisse wie Inhalte, Vorhersagen, Empfehlungen oder Entscheidungen hervorbringen kann, die das Umfeld beeinflussen, mit dem sie interagieren": Bomhard/Merkle*, RDi 2021, 276 (277) die von einer „Leerformel" sprechen; *BVMED,* MRP 2021, 176 (177).

28 *BVMED,* MRP 2021, 176 (177); *Geminn,* ZD 2021, 354 (355) nennt z.B. „eine gewisse Anpassungsfähigkeit und auch Autonomie des technischen Systems, die in unterschiedlichem Maße zur Unvorhersagbarkeit seiner Handlungen führen"; *Kaulartz/Braegelmann* nennen Eigenschaften, welche erfüllt sein müssen, damit ein System als künstlich intelligent angesehene werden könne: "Wahrnehmen, Verstehen, Handeln und Lernen", *Kaulartz/Braegelmann* in: Kaulartz/Braegelmann ‚Rechtshandbuch Artificial Intelligence und Machine Learning, 2020, Kapitel 1 Rn. 9.

29 *Bomhard/Merkle*, RDi 2021, 276 (277 f.).

30 *Kayser-Bril*, European Council and Commission in agreement to narrow the scope of the AI Act, hier abrufbar (Stand: 30.12.2021).

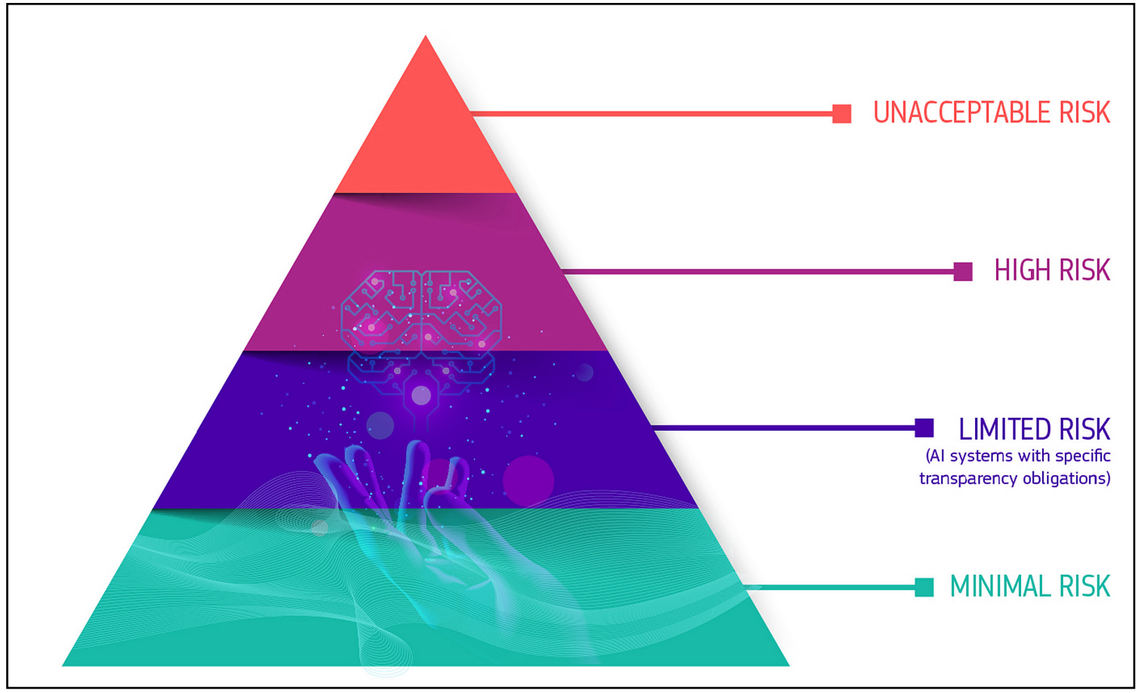
31 Zum Begriff der horizontalen Regulierung: *Grützmacher/Füllsack*, ITRB 2021, 159 (160).

Im Rahmen dieses risikobasierten Ansatzes[32] unterteilt der europäische Gesetzgeber die Künstliche Intelligenz in folgende Risikogruppen: unannehmbares Risiko, Hochrisiko-KI, KI mit geringem Risiko und KI mit minimalem Risiko.[33] Je nach Risikostatus des KI-Einsatzes gelten unterschiedlich hohe Anforderungen an den Einsatz bzw. an das Inverkehrbringen. Herzstück des Entwurfs bilden die Regelungen rund um die Regulierung der Hochrisiko-KI.

I. KI mit unannehmbarem Risiko

Zunächst beschäftigt sich die Verordnung in Art. 5 KI-VO-E jedoch mit KI-Systemen, die ein unannehmbares Risiko mit sich bringen. Das Risiko, das durch die Verwendung oder das Inverkehrbringen der verschiedenen abschließend aufgezählten Systeme entsteht, schätzt die Europäische Kommission als so hoch ein, dass sie die Systeme vollständig verbietet.

Grund für das generelle Verbot ist die Annahme, dass die verbotenen Praktiken die Werte der Union, insbesondere die europäischen Grundrechte, verletzen würden.[34] Hierunter fallen beispielsweise gem. Art. 5 I a) KI-VO-E Systeme, die eine potenziell körperlich oder psychisch schädigende Technik der unterschwelligen Beeinflussung nutzen, um das Verhalten einer Person auf diese Weise zu steuern (Verhaltensbeeinflussung).[35] Dieses Verbot soll das Selbstbestimmungsrecht jedes EU-Bürgers und damit einen wesentlichen Kern der individuellen Freiheit schützen.[36] Hierbei wird nicht nur das Inverkehrbringen des Systems umfasst, sondern auch die Inbetriebnahme eines solchen sowie dessen Verwendung.



© Europäische Kommission

Die Risikopyramide des KI-VO-E

Auch die behördliche Bewertung von persönlichen Eigenschaften oder menschlichem Verhalten, um dieses zu vergleichen (Social-Scoring-Anwendung)[37] wird gem. Art. 5 I c) KI-VO-E verboten. Das Verbot des Social Scoring könnte künftig auch Teile der Polizeiarbeit betreffen, zum Beispiel im Rahmen des Predictive Policing.[38] Für Strafverfolgungszwecke besonders interessant gestaltet sich zudem das Verbot des Art. 5 I d) KI-VO-E. Hiernach ist die Verwendung biometrischer Echtzeit-Fernidentifizierungssysteme[39] in öffentlich zugänglichen Räumen zu Strafverfolgungszwecken verboten. Hierunter fällt beispielsweise die Videoüberwachung mit automatisierter Gesichtserkennung. Allerdings ist nicht jeglicher Überwachungseinsatz untersagt. Art. 5 I d) KI-VO-E erlaubt den Einsatz der Echtzeit-Fernidentifizierung in Ausnahmefälle, wie zum Beispiel zur Abwendung eines Terroranschlags oder der

32 KI-VO-E, COM(2021) 206 final, S. 11.
33 Der KI-VO-E benennt die Risikogruppen in der Originalfassung mit „[…] *AI that create (i) an unacceptable risk, (ii) a high risk, and (iii) low or minimal risk*.“, s. KI-VO-E 5.2.2., S. 12; Einen guten Überblick über die verschiedenen Gruppen bietet die Kommission, hier abrufbar (Stand: 15.11.2021).
34 KI-VO-E, COM(2021) 206 final, S. 12 f.
35 Nicht erfasst aufgrund des Erfordernisses eines physischen oder psychischen Schadens ist beispielsweise die Konsumentenbeeinflussung durch die großen Digitalkonzerne, da dies nur zu finanziell spürbaren Auswirkungen führt, s. hierzu *Valta/Vasel*, ZRP 142 (143).
36 *Rostalski/Weiss*, ZfDR 2021, 329 (338).
37 *Ballestrem*, DB 2021, M4 -M5.
38 Zum Begriff des Predictive Policing s. *Scholz*, CTRL 2/2021, 110.
39 Zum Begriff s. Erwägungsgrund 8 KI-VO-E, COM(2021) 206 final, S. 19.

dringenden Suche nach vermissten Kindern oder Opfern von Straftaten. Bei genauerer Betrachtung der weiteren Ausnahmen fragt sich, ob das Verbot tatsächlich noch so generell ist, wie der KI-VO-E dies suggeriert.[40]

II. Hochrisiko-KI

Auf einer zweiten Stufe stehen Hochrisiko-KI-Systeme, worunter Anwendungen fallen, die erhebliche Risiken für die Gesundheit und Sicherheit oder die Grundrechte der EU-Bürger bergen.[41] Systeme mit hohem Risiko werden zwar nicht grundsätzlich verboten, unterstehen jedoch strenger Regulierung, woraus sich gem. Art. 8 ff. KI-VO-E erhöhte Pflichten für die Entwickler und Verwender ergeben. Unter den Begriff der KI mit hohem Risiko fallen gem. Art. 6 I KI-VO-E KI-Systeme, die als Sicherheitskomponente eines Produkts[42] verwendet werden oder selbst ein in Anhang II[43] gelistetes Produkt darstellen (lit. a) und einer Konformitätsbewertung durch Dritte unterzogen werden müssen (lit. b). Unabhängig hiervon fallen gem. Art. 6 II KI-VO-E zusätzlich solche Systeme in den Hochrisiko-Bereich, die enumerativ in Anhang III zum KI-VO-E aufgeführt werden. Die in Anhang III aufgeführten Bereiche betreffen hierbei unterschiedliche Sektoren, insbesondere jedoch all jene Bereiche der kritischen Infrastruktur. Im Hinblick auf die Anwendung Künstlicher Intelligenz im juristischen Bereich ist insbesondere Anhang III Nr. 6 interessant, der sich erneut dem KI-Einsatz im Rahmen der Strafverfolgung[44] widmet. Darüber hinaus nennt Anhang III Nr. 8 den KI-Einsatz im Rahmen der Rechtspflege.

Wird künftig ein Hochrisiko-KI-System entwickelt, vertrieben oder eingesetzt, gilt es, einen umfangreichen und dezidierten Maßnahmenkatalog nach den Art. 8 ff. KI-VO-E einzuhalten, um der andernfalls mit einem Verstoß einhergehenden Sanktionsgefahr[45] zu entgehen. Zunächst müssen die KI-Systeme mit hohem Risiko künftig einer Konformitätsprüfung nach den Art. 11, Art. 16 a), c), d), g), j), Art. 18 und Art. 43 KI-VO-E genügen und bedürfen einer CE-Zertifizierung.[46] Hierdurch soll sichergestellt werden, dass das System den Anforderungen einer vertrauenswürdigen KI gerecht wird.[47] Darüber hinaus setzt Art. 9 KI-VO-E die Einrichtung eines Risikomanagementsystems voraus. Hierdurch sollen die der Anwendung innewohnenden Risiken benannt und eingeschätzt werden, wobei anschließend Maßnahmen zur Minimierung und zum Management dieser Risiken entwickelt werden.[48] Nähere Vorgaben zur genauen inhaltlichen Umsetzung des Risikomanagements wurden hingegen nicht getroffen. Art. 10 KI-VO-E widmet sich der Verwendung von Daten und Data-Governance. Kernanliegen ist, dass die Trainings-, Validierungs- und Testdatensätze für Hochrisiko-KI hinreichend relevant, repräsentativ, fehlerfrei und vollständig sein sollen. Vorgeschrieben wird an dieser Stelle zudem in Art. 10 II f) KI-VO-E, dass die Daten auf mögliche Verzerrungen untersucht werden müssen („***examination in view of possible biases***“). Diese Vorschrift dient dem Ziel der Kommission, durch gute Data-Governance Diskriminierungen durch KI-Einsatz vorzubeugen.[49]

Im Anschluss setzt Art. 12 KI-VO-E Aufzeichnungspflichten für Hochrisiko-KI-Systeme fest. Es geht insbesondere um die Ermöglichung der automatisierten Protokollierung, um die inneren Vorgänge und den Betrieb des Systems nachvollziehen und Ergebnisse des Systems zurückverfolgen zu können. Diese Nachvollziehbarkeit der inneren Wirkweise ist unerlässlich, um überprüfen zu können, ob das System tatsächlich die inhaltlichen Anforderungen an KI-Systeme mit hohem Risiko einhält.[50] Zu mehr Transparenz soll auch die Regelung des Art. 13 KI-VO-E beitragen. Nach Art. 13 I KI-VO-E sollen die Hochrisiko-Systeme so entwickelt werden, dass die Nutzer die Ergebnisse verstehen und verwenden können. Art. 13 II KI-VO-E schlägt hierfür die Bereitstellung von Gebrauchsanweisungen für den Nutzer vor. Die Schaffung von mehr Transparenz ist gerade im Hinblick auf den Schutz der Grundrechte des Einzelnen besonders wünschenswert. Gleichzeitig bestehen Bedenken hinsichtlich

40 *Rostalski/Weiss*, ZfDR 2021, 329 (343); *Spindler*, CR 2021, 361 (365).
41 KI-VO-E, COM(2021) 206 final, S. 3.
42 Auch hier wird auf die in Anhang II des KI-VO-E genannten Vorschriften verwiesen.
43 Annexes to the Proposal for a Regulation of the European Parliament and of the Council, COM(2021) 206 final Annexes 1 to 9, hier abrufbar (Stand: 19.11.21).
44 Zum KI-basierten Legal-Tech-Einsatz im Strafprozess generell s. *Ecker*, CTRL2/2021, 114 (115 ff.).
45 Art. 71 KI-VO-E; COM(2021) 206 final.
46 *Grützmacher/Füllsack*, ITRB 2021, 159 (160).
47 “Those AI systems will have to comply with a set of horizontal mandatory requirements for trustworthy AI and follow conformity assessment procedures […]”, vgl. COM(2021) 206 final, S. 3.
48 Vergleichbar mit einem Compliance-Management-System.
49 Erwägungsgrund 44 KI-VO-E, COM(2021) 206 final, S. 29 .
50 Erwägungsgrund 46 KI-VO-E, COM(2021) 206 final, S. 30.

der praktischen Umsetzbarkeit dieses Ziels im Hinblick auf die bisher bestehende „***Black-Box***"-Problematik[51]. Dem praktischen Problem bezüglich der Umsetzung aller Transparenzvorgaben könnten neuere Entwicklungen auf dem Gebiet der Explainable AI (XAI)[52] Abhilfe schaffen.[53]

Einen weiteren Baustein der Nachvollziehbarkeit bildet Art. 14 I KI-VO-E, der eine wirksame menschliche Beaufsichtigung des KI-Systems fordert. Diese menschliche Aufsicht verfolgt zum einen erneut die Aufgabe, Risiken für einen unverhältnismäßigen Eingriff in die Rechte des Einzelnen zu minimieren. Zum anderen bildet sie einen wichtigen Grundpfeiler im Rahmen der Wahrung menschlicher Autonomie auch bei einem KI-Einsatz. Allerdings bestehen an dieser Stelle ebenfalls Bedenken hinsichtlich der praktischen Umsetzbarkeit der Regelung, da es oftmals nur einen sehr kleinen Personenkreis geben wird, der überhaupt die Möglichkeit hat, die Wirkweise des Systems ausreichend nachzuvollziehen. Welche genauen Wissensanforderungen an den Anwender zu stellen sind und wie etwaige Geschäftsgeheimnisse effektiv geschützt werden sollen, bleibt ebenfalls offen.[54]

„Es verwundern einige Einordnungsentscheidungen, wie die Zuordnung von Deepfakes zu Systemen mit geringem Risiko."

III. KI mit geringem Risiko

Eine Stufe darunter werden KI-Systeme mit einem lediglich geringen Risiko für die Rechte des Einzelnen eingestuft. Für KI-Systeme mit einem solch geringen Risiko sollen gem. Art. 52 KI-VO-E lediglich besondere Kennzeichnungspflichten gelten.

Hierunter fallen beispielsweise KI-Anwendungen, die mit den einzelnen Personen interagieren (z.B. Chatbots[55]), bei denen dem Nutzer künftig explizit mitgeteilt werden soll, dass er mit KI interagiert. Ebenfalls als KI-System mit geringem Risiko werden Deepfakes[56] eingestuft. Die Ersteller müssen von nun an offenlegen, dass der Videoinhalt künstlich erzeugt oder manipuliert wurde. Ziel ist es, den Nutzern die Erkenntnis zu ermöglichen, dass sie mit einem KI-System interagieren, was durch die Informationspflichten praktisch gut umsetzbar erscheint.

IV. KI mit minimalem Risiko

Alle sonstigen Anwendungen, die nicht einmal ein geringes Risiko für die Anwender bergen, fallen nicht unter die Verordnung und können demzufolge ohne weitere Einhaltung zusätzlicher Vorschriften entwickelt und eingesetzt werden, vgl. Art. 69 KI-VO-E. Lediglich die sonstig bereits geltenden Rechtsvorschriften sind einzuhalten. KI-Anwendungen mit einem derartig minimalen Risiko sollen auch künftig der Selbstregulierung überlassen werden.[57]

D. Auswirkungen des KI-VO-E auf Legal-Tech-Anwendungen

Wird diese Risiko-Kategorisierung des KI-VO-E auf den Bereich der Legal-Tech-Anwendungen[58] übertragen, fragt sich, welche Implikationen der KI-VO-E für einzelne Entwicklungen in den verschiedenen juristischen Einsatzgebieten haben wird. Zwar geht der KI-VO-E von einem risikobasierten Ansatz aus und vermeidet demnach eine Sektorenanknüpfung. Zum Zwecke der Übersichtlichkeit sollen hier

51 Hierzu *Leeb/Schmidt-Kessel*, in: Braegelmann/Kaulartz, Rechtshandbuch Artificial Intelligence und Machine Learning, 2020, Kap. 10, Rn. 27 ff.
52 XAI soll dazu dienen, die Entscheidungsfindung durch KI transparent und nachvollziehbar zu gestalten; Hierzu ausführlich *Käde/Maltzan*, CR 2020, 66 ff.
53 *Bomhard/Merkle*, RDi 2021, 276 (280).
54 *Bomhard/Merkle*, RDi 2021, 276 (281).
55 KI-VO-E, COM(2021) 206 final, S. 3; zum Begriff der Legal Chatbots s. *Duda/Lilienbeck*, CTRL 2/2021, 168.
56 Deepfakes sind Bilder oder Videos, die mithilfe von KI erstellt werden und echt wirken; Zum Begriff z.B. *Lantwin*, MMR 2019, 574; Kritik an der Einordnung üben *Valta/Vasel*, ZRP 2021, 142.
57 *Grützmacher/Füllsack*, ITRB 2021, 159 (160).
58 Was unter den Legal-Tech-Begriff zu fassen ist, wird nicht durchweg einheitlich beurteilt, s. hierzu *Frink*, CTRL 1/21, 62; Für die Zwecke dieses Beitrags soll der Begriff weit verstanden werden.

jedoch einige Beispiele je nach Sektor und Einsatzgebiet beleuchtet werden.

I. KI-Einsatz im Bereich der Justiz

Im Bereich der Justiz erkennt der KI-VO-E bereits selbstständig gewisse Besonderheiten an. Der Entwurf legt in Erwägungsgrund 40 fest, dass der KI-Einsatz im Bereich der Justiz besonders grundrechtssensibel sein kann, insbesondere wenn das KI-System dabei helfen soll, Sachverhalte und Rechtsvorschriften zu ermitteln und auszulegen sowie das Recht auf konkrete Sachverhalte anzuwenden. Art. 6 II KI-VO-E i.V.m. Anhang III Nr. 8 lit. a) stuft all diese Systeme im Bereich der Justiz als grundsätzlich hochriskant ein. Ausgenommen sind KI-Systeme, die sich auf rein begleitende Verwaltungstätigkeiten beziehen. Gerade für besonders zukunftsorientierte Projekte im Bereich der Justiz kann diese Kategorisierung zur Herausforderung werden. Wird beispielsweise das Smart Sentencing-Tool[59] zur Förderung einer einheitlichen Strafzumessung in ganz Deutschland betrachtet, stellt sich die Frage, ob auch eine solche Anwendung als Hochrisiko-KI einzustufen ist. Im Rahmen des Tools soll eine Software nach der Eingabe von Urteilen die darin enthaltenen Strafzumessungserwägungen erkennen und mit dem daraus resultierenden Strafmaß in Relation setzen.[60] Die so entstehende Datenbank kann anschließend zur Abfrage von Statistiken aufgrund der jeweiligen Strafzumessung genutzt werden. Ob das Einsatzgebiet der Strafzumessung bereits unter den Wortlaut des Anhangs III Nr. 8 a) zu fassen ist, lässt sich je nach genauem Wortverständnis unterschiedlich beurteilen.[61] Allerdings soll die Strafzumessung alle wertenden Tatumstände erfassen, korreliert demnach unmittelbar auch mit dem zugrundeliegenden Tathergang und der Schuld des Angeklagten.[62] Sie stellt ferner einen Kern der richterlichen Entscheidungsfindung dar und wird daher klar vom Sinn der Nr. 8 erfasst. Zudem stellt die Strafzumessung einen besonders sensiblen Bereich des Strafverfahrens dar, da sich die Höhe der Strafe unmittelbar auf die Freiheit des Einzelnen auswirkt. Demnach läge es nahe, auch die konkrete Stützung der Strafzumessungserwägungen durch ein statistisch selbstständig arbeitendes System, das die Anwendung des Rechts auf den konkreten Sachverhalt unterstützen soll, als ein KI-System nach Anhang III Nr. 8 lit. a) zu qualifizieren. Entwicklungen im Hinblick auf die Strafzumessung müssten sich demnach auf das bereits angesprochene umfangreiche Zertifizierungsverfahren einstellen.

Ebenfalls einen klaren Anwendungsfall von Hochrisiko-KI würde ein Prognosesystem darstellen, das eine Rückfallwahrscheinlichkeit der Straftatbegehung vorhersagt, wie ein etwaiges Pendant zum amerikanischen ***COMPAS***-System[63]. Durch das Risikobewertungstool ***COMPAS*** werden Prognosen durch KI getroffen, die eine etwaige Rückfallgefahr sowie die generelle Gefährlichkeit und Fluchtgefahr des Angeklagten betreffen, die dann wiederum dem Richter als Bewertungsgrundlage dienen sollen. Das System arbeitete jedoch nicht neutral und diskriminierte beispielsweise Angeklagte mit dunkler Hautfarbe.[64] Gerade bei derartigen Prognosesystemen ist die Transparenz und Nachvollziehbarkeit sowie die Kontrolle von enormer Bedeutung, um etwaige Ungleichbehandlungen auszuschließen.[65] Nur durch strenge Reglementierung und dauernde Überwachung kann ein ***bias*** (dt. ***Voreingenommenheit***) der KI entdeckt und ausgeschlossen werden. Das Beispiel ***COMPAS*** aus den Vereinigten Staaten hat gezeigt, dass es ohne Überwachung zu einer Diskriminierung bestimmter Gruppen durch das System kommen kann. Wagt man einen noch weiteren Zukunftsblick auf den etwaigen Einsatz von „***Robo-Judges***“[66], also selbstständig arbeitende Subsumtions- und Entscheidungsautomaten, so zeigt sich deutlich, dass solch intelligente Systeme als Paradefall unter Art. 6 II i.V.m. Anhang III Nr. 8 a) zu fassen sind und damit Hochrisiko-Systeme darstellen.

59 Zum Tool *Rostalski/Völkening*, KriPoZ 2019, 265; PM der Universität zu Köln, hier abrufbar (Stand: 13.12.2021).
60 *Rostalski/Völkening*, KriPoZ 2019, 265 (271).
61 Anhang III Nr. 8 lit. a) erfasst: “*AI systems intended to assist a judicial authority in researching and interpreting facts and the law and in applying the law to a concrete set of facts*” . Ob die Strafzumessung tatsächlich unter die Interpretation von Sachverhaltsfakten zu fassen ist, kann dahingestellt bleiben. Jedenfalls zeigt der Wortlaut, dass es im Kern um die Stützung der richterlichen Entscheidung durch KI-Systeme gehen soll.
62 *Streng*, in: Kindhäuser/Neumann/Paeffgen, StGB, 5. Auflage, § 46 Rn. 22 ff.
63 Ausführlich zum COMPAS-System *Nink*, Justiz und Algorithmen, 376 ff.
64 *Steege*, MMR 2019, 715 (716); *Steinrötter/Warmuth*, in: Hoeren/Sieber/Holznagel, Handbuch Multimedia-Recht, 56. EL, Stand Mai 2021, Teil 30 Rn. 61 m.w.N.
65 Vgl. Erwägungsgrund 38 KI-VO-E, COM(2021) 206 final, S. 27.
66 Die vorliegenden Gedanken klammern bewusst die bisher bestehenden technischen und sonstigen Umsetzungsprobleme aus; S. weitergehend hierzu auch *Gless/Wohlers*, in: FS Kindhäuser, 2019, 147; *Hilgendorf*, in: Hoven/Kubiciel, Zukunftsperspektiven des Strafrechts, 2020, 229; *Rostalski*, in: Hoven/Kudlich, Digitalisierung und Strafverfahren, 263; *Timmermann*, Legal-Tech-Anwendungen, 266 ff.; *Ecker*, CTRL2/21, 114 (119 ff.).

Im Ergebnis zeigt sich für die Justiz einerseits, dass viele den Kern der richterlichen Arbeit unterstützenden Anwendungen künftig die hohen Voraussetzungen erfüllen müssen, die an den Einsatz von Hochrisiko-KI geknüpft sind. Andererseits ist der KI-Einsatz im sensiblen richterlichen Entscheidungsprozess nicht per se nach Art. 5 KI-VO-E verboten, was teilweise verwundert.[67] Allerdings kann sich dies bei zukünftig noch weitergehenden technischen Entwicklungen im Bereich der Justiz jederzeit ändern. Die Entscheidung der Kommission gegen ein generelles Verbot ist als positiv zu bewerten, da sie weiterhin Innovationen im Bereich der Justiz ermöglicht, um den Prozess moderner, fairer und schneller zu gestalten. Bestehende Entwicklungen können vorangetrieben werden, müssen sich jedoch auf das umfangreiche Zertifizierungsverfahren einstellen. Durch die erhöhten Voraussetzungen und Zertifizierungsansprüche, die an die Hochrisiko-KI-Systeme gestellt werden, findet zudem die nötige Überwachung des KI-Einsatzes statt. Gerade im justiziellen Bereich ist dies zum Schutz der Grundrechte des Einzelnen unerlässlich. Derzeit bereits genutzte Legal-Tech-Anwendungen jenseits des richterlichen Entscheidungskerns werden auch im Bereich der Justiz weiterhin der Selbstregulierung überlassen bleiben, da sie nicht unter Hochrisiko-KI fallen, sondern lediglich unbedenkliche technische Optimierungen der justiziellen Abläufe fördern. Hierunter könnten künftig beispielsweise das besondere elektronische Anwaltspostfach (beA) oder die e-Akte fallen, soweit auch in diesen Bereichen eine KI gestützte Lösung im Sinne des KI-VO-E eingesetzt würde. Bisher ist dies jedoch noch nicht der Fall. Zwar würden die Lösungen dann keine Hochrisiko-KI darstellen, allerdings könnten diese verwaltungsbegleitenden Anwendungen einer anderen Risikogruppe unterfallen. Diese Klassifizierung hinge wiederum von der genauen Ausgestaltung und Einsatzweise der KI-Lösung ab.

II. KI-Einsatz bei den Ermittlungsbehörden

Der KI-VO-E hält zudem für den KI-Einsatz durch Ermittlungsbehörden Neuerungen bereit. Eine absolute Grenze zieht der KI-VO-E insbesondere beim Einsatz von Gesichtserkennungssoftware zur Strafverfolgung, der bis auf wenige Ausnahmen in öffentlich zugänglichen Räumen zu Strafverfolgungszwecken gem. Art. 5 I lit. d) KI-VO-E grundsätzlich verboten ist. Vor dem Hintergrund des mit der Überwachung verbundenen erheblichen Eingriffs in die Rechte und Freiheit des Einzelnen,[68] ist dieses grundsätzliche Verbot sinnvoll und gerechtfertigt. Neben der Einstufung der Überwachung als inakzeptables Risiko führt der Anhang III Nr. 6 weitere spezielle Felder des KI-Einsatzes im Rahmen der Strafverfolgung auf, die gem. Art. 6 II KI-VO-E als KI mit hohem Risiko eingestuft werden sollen. Aufgeführt werden beispielsweise Systeme, die bei der Strafverfolgung zur individuellen Risikobewertung oder als Lügendetektor eingesetzt werden. Zudem werden Systeme zur Bewertung der Zuverlässigkeit von Beweismitteln im Strafverfahren oder zur Vorhersage des (erneuten) Auftretens von Straftaten auf Grundlage eines Personenprofils aufgelistet. Ebenfalls erfasst werden von Anhang III Nr. 6 lit. g) Systeme, die es ermöglichen, komplexe Datensätze aus verschiedenen Datenquellen oder in verschiedenen -formaten zu durchsuchen, um Datenmuster oder Beziehungen der Daten zueinander aufzudecken. Dies könnte insbesondere für etwaige Programme im Rahmen der Online-Durchsuchung eine Rolle spielen, aber auch soweit ***Technology Assisted Review***[69] eingesetzt wird, um den Sachverhalt aus großen Datenmengen zu extrahieren.[70] Generell lässt sich festhalten, dass viele KI-Systeme insbesondere während strafrechtlichen Ermittlungen in die Gruppe der Hochrisiko-KI fallen werden. Diese Einstufung ist zu begrüßen, da es hier gilt, die Rechte des Beschuldigten besonders zu schützen. Andernfalls könnten die ihm zustehenden Garantien und Rechte wie die Unschuldsvermutung sowie seine Selbstbelastungsfreiheit und Verteidigungsrechte durch den Einsatz von Technik ausgehöhlt werden. Indem der KI-VO-E jedoch auch in diesem Bereich den Einsatz von KI-Systemen nicht grundsätzlich untersagt, sondern viele Systeme als Hochrisiko-KI einstuft, schafft er weiterhin Raum für technische Innovation. Gleichzeitig schafft der Entwurf aber auch an dieser Stelle durch das erforderliche umfangreiche Prüfungsverfahren den notwendigen Grundrechtsschutz.

67 Dies kritisch hinterfragend: *Rostalski/Weiss*, ZfDR 2021, 329 (345).

68 Hierneben wird als Grund auch das sonst drohende Gefühl der ständigen Überwachung für die Bevölkerung aufgeführt; Erwägungsgrund 8 KI-VO-E.

69 Zum Begriff *Ohrloff/Zickert*, ZdiW 2021, 232 (234).

70 *Engelmann/Brunotte/Lütkens*, RDi 2021, 317 (320).

III. KI-Einsatz in der Privatwirtschaft

Nicht nur in der Justiz und bei den Ermittlungsbehörden, sondern auch in der Privatwirtschaft finden KI-basierte Legal-Tech-Anwendungen ihren Einsatz. Zur Zeit beschränkt sich der Anwendungsbereich auf den Einsatz von Legal Chatbots[71] und vereinzelt Dokumentenauswertungs- und -erstellungslösungen. Zukünftig ist jedoch zu erwarten, dass der KI-Einsatz deutlich zunimmt, wodurch die Nachfrage nach Legal-Tech-Intermediären und Legal Engineers/Legal Technologists[72] rapide ansteigen[73] wird. Für KI-Systeme, die mit natürlichen Personen interagieren, schreibt Art. 52 I 1 KI-VO-E besondere Transparenzpflichten vor. Diese treffen insbesondere Betreiber sog. Legal Chatbots. Aktuell wird beim Öffnen der Webseiten einiger Dienste-/Warenanbieter dem Nutzer, meist in einer Ecke des Bildschirms, die Möglichkeit zum Chat mit einem Berater des Webseitenbetreibers angeboten. Oftmals wird auch durch das Anzeigen dreier Punkte vom Webseitenbetreiber vorgespiegelt, die nachfolgende standardisierte Begrüßungsnachricht sei von einem menschlichen Mitarbeiter getippt worden. Diese Punkte werden nämlich in Messengern klassischerweise dazu verwendet, das aktuelle Nachricht-Tippen des Kontakts anzuzeigen. Die Vorstellung des Nutzers, mit einem Menschen zu interagieren, wird weiter verfestigt, indem auf vielen dieser Webseiten ein Foto eines vermeintlich tatsächlich existierenden menschlichen Mitarbeiters als Avatar neben der Nachricht angezeigt wird. Die Realität dürfte hingegen sein, dass diese Nachrichten von einem automatisierten System stammen und erst nach einer Antwort des Webseitenbesuchers ein menschlicher Berater zugeschaltet wird. Diese Praxis wird bei der Verwendung von KI-basierten Chatbots unter dem Regelungskonstrukt des KI-VO-E so nicht mehr aufrecht erhalten werden können.

Chatbot-KIs stellen weder unannehmbare noch hohe Risiken i.S.d. Art. 5 und 6 KI-VO-E dar.[74] Allerdings sind sie für die Interaktion mit natürlichen Personen bestimmt, sodass gem. Art. 52 I 1 KI-VO-E grundsätzlich eine Mitteilungspflicht des Anbieters besteht, die natürliche Person darüber zu informieren, dass sie mit einem KI-System korrespondiert. Eine Ausnahme für diese Pflicht besteht, wenn aus den Umständen und dem Kontext der Nutzung offensichtlich wird, dass es der Nutzer mit einem KI-System zu tun hat.[75] Wann eine solche Offensichtlichkeit vorliegen soll, wird vom KI-VO-E nicht weiter beschrieben. Dem Durchschnittsnutzer dürfte grundsätzlich einleuchten, dass bei großen Internetdiensteanbietern mehrere tausend Webseitenaufrufe pro Sekunde erfolgen können, sodass unmöglich jedem dieser Nutzer ein menschlicher Chatpartner zur Verfügung gestellt werden kann. Allerdings ist es in der Regel für den Durchschnittsnutzer schwer abzuschätzen, ab welcher Größe des Internetauftritts eine Nutzung von KI geboten wäre. Zudem können Chatbots gerade auch durch nicht-KI basierte Softwaresysteme realisiert werden. Somit wäre es für den Nutzer schwer zu differenzieren, ob er mit einem KI-gestützten oder mit einem einfachen Entscheidungsbaum-System kommuniziert. Vor dem Hintergrund des Ziels des KI-VO-E, Transparenz für den Nutzer schaffen zu wollen, um sein Vertrauen in KI-Technologie zu stärken, muss eine Offensichtlichkeit somit abgelehnt werden. Anbieter von KI-basierten Chatbots müssen dem Nutzer künftig gem. Art. 52 I 1 KI-VO-E mitteilen, dass er mit einer KI und gerade nicht mit einem menschlichen Berater kommuniziert.

Dokumentenerstellungs- und Analysehilfen für den kanzleiinternen Gebrauch, wie z.B. Schriftsatzauswertungs- und -erstellungs-Systeme,[76] dürften hingegen zukünftig regulierungsfrei bleiben. Rechtsanwälte sind zwar Organe der Rechtspflege, fallen aber dennoch nicht unter Art. 6 II i.V.m. Anhang III Nr. 8 KI-VO-E, da sie zumindest keine Justizbehörden sind. Auch sind derartige Systeme (noch) ausschließlich für die Anfertigung reiner Entwürfe vorstellbar. Diesen Entwurf macht sich der jeweilige Unterzeichnende zu eigen, sodass auch eine Schriftsatzerstellungs-KI nicht mit natürlichen Personen interagiert. Anders hingegen sind beispielsweise Vertragsgeneratoren zu beurteilen, welche von den Nutzern selbst bedient werden. Diese sind auf die Interaktion mit natürlichen Personen ausgelegt und mithin Art. 52 I 1 KI-VO-E unterworfen.

71 Siehe hierzu: *Duda/Lilienbeck*, CTRL 2/21, 168.
72 Zu den hinter diesen Begriffen stehenden Berufsbildern *Kupfermann/Goral-Wood*, CTRL 1/21, S. 71; *Hartung,* in: Hartung/Bues/Halbleib, Digitalisierung 2018, S. 237, 239 ff; *Müller*, InTeR 2018, 57.
73 *Alschner,* „Trends in AI: What´s to come", in: Artificial Intelligence Future of Legal Profession, hier abrufbar (Stand: 15.12.2021).
74 Im Ergebnis auch *Engelmann/Brunotte/Lütkens*, RDi 2021, 317 (321).
75 Art. 52 I S. 1 Hs. 2 KI-VO-E; COM(2021) 206 final.
76 Eine Übersicht über derartige Tools ist hier abrufbar (Stand: 15.12.2021).

E. Fazit

Mit dem KI-VO-E unternimmt die Kommission einen mutigen Versuch der weltweit ersten umfassenden KI-Regulierung.[77] Sie betritt dabei ein heikles Spannungsfeld aus Schutzinteressen der EU-Bürger, wirtschaftlichen Interessen der KI-Industrie und eigenen Bedeutungsinteressen des Wirtschaftsstandorts Europa. Positiv ist, dass die Kommission dabei einen risikobasierten Ansatz wählt, der praktisch alternativlos erscheint.[78] Geschickt wählt sie zudem die Möglichkeit, über leicht änderbare Anhänge Aufschluss über die weit gewählten Definitionen zu bieten und gleichzeitig die notwendige Flexibilität beizubehalten, den Entwurf ständig an eine sich rapide entwickelnde Technologie anpassen zu können. Dieses Vorgehen bietet für die Adressaten des Entwurfs allerdings auch erhebliche Rechtsunsicherheiten.[79]

Anpassungsbedarf ergibt sich insbesondere noch im Rahmen des zentralen KI-Begriffs. Dieser ist schlicht zu weit und grenzt künstlich intelligente Systeme nicht trennscharf genug von unintelligenten Software-Systemen ab.[80]

Ebenso verwundern einige Einordnungsentscheidungen, wie die Zuordnung von Deepfakes zu Systemen mit geringem Risiko. Der privatwirtschaftliche Legal-Tech-Sektor dürfte sich infolge des KI-VO-E nur geringen weiteren Verpflichtungen ausgesetzt sehen. Größeren Umsetzungsaufwand wird der Entwurf jedoch für die deutlich grundrechtsintensiveren Bereiche der Justiz und Ermittlungsbehörden bedeuten. Diese Anwendungsbereiche dürften regelmäßig als hoch risikobehaftet qualifiziert werden. Zeigen muss sich, ob der KI-VO-E tatsächlich die Attraktivität des Wirtschaftsstandorts Europa für KI-Entwicklung gegenüber der starken Konkurrenz wie den USA steigern wird. Mit Sicherheit lässt sich jedoch voraussagen, dass der KI-VO-E im Bereich Legal Tech die Innovationskraft nicht vollständig hemmen wird.

77 *Spindler*, CR 2021, 361 (373).
78 *Marx*, jurisPR-ITR 19/2021, Anm. 2, S. 4.
79 *Heiss*, NZG 2021, 611 (611 f.).
80 *BVMED*, MPR 2021, 176 (177); *Bomhardt/Merkle*, RDi 2021, 276 (277, Rn. 7); *Engelmann/Brunotte/Lütkens*, RDi 2021, 317 (318); *Spindler*, CR 2021, 361 (373).

Weiterführende Hinweise:

Talking Legal Tech – Folge 45:

Wie Legal Tech der Staatsanwaltschaft bei der Aufdeckung von Cybercrime hilft

Talking Legal Tech – Folge 42:

Smart Sentencing – Gefährdung richterlicher Unabhängigkeit oder Ermöglichung gerechter Strafen, Malte Völkening und Timothée Schmude?

Talking Legal Tech – Folge 28:

Regulierung & Innovation – Wie lässt sich beides vereinbaren, Martin Ebers?

Zurück zum dynamischen Inhaltsverzeichnis?

Zum dynamischen Inhaltsverzeichnis

1/22

2. Jahrgang, 1. Ausgabe
www.legaltechcologne.de/ctrl

CTRL

Cologne Technology & Law Review

Hier geht es zur ganzen Ausgabe

Dort findest Du in 19 Beiträgen alles von Datenschutz bei Connected Cars über Krypto-Auktionen bis hin zum Artificial Intelligence Act und Legal Tech.

LEGAL TECH LAB COLOGNE