BUNDESRECHTSANWALTSKAMMER

Stellungnahme Nr. 52/2021
August 2021
Registernummer: 25412265365-88

Stellungnahme zum Verordnungsentwurf zur Festlegung von harmonisierten Regeln für künstliche Intelligenz

Verteiler: Europäische Kommission
Europäisches Parlament
Rat der Europäischen Union
Ständige Vertretung der Bundesrepublik Deutschland bei der EU
Vertretungen der Länder

Bundesrechtsanwaltskammer
The German Federal Bar
Barreau Fédéral Allemand
www.brak.de

Büro Berlin – Hans Litten Haus
Littenstraße 9
10179 Berlin
Deutschland
Tel. +49.30.28 49 39 - 0
Fax +49.30.28 49 39 -11
Mail zentrale@brak.de

Büro Brüssel
Avenue des Nerviens 85/9
1040 Brüssel
Belgien
Tel. +32.2.743 86 46
Fax +32.2.743 86 56
Mail brak.bxl@brak.eu

Die Bundesrechtsanwaltskammer ist die Dachorganisation der anwaltlichen Selbstverwaltung. Sie vertritt die Interessen der 28 Rechtsanwaltskammern und damit der gesamten Anwaltschaft der Bundesrepublik Deutschland mit rund 166.000 Rechtsanwältinnen und Rechtsanwälten gegenüber Behörden, Gerichten und Organisationen – auf nationaler, europäischer und internationaler Ebene.

Stellungnahme

Die Europäische Kommission hat am 21. April 2021 ihren Vorschlag für eine Verordnung zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz (Gesetz über künstliche Intelligenz und zur Änderung bestimmter Rechtsakte der Union (COM(2021) 206 final) (nachstehend: „KI-VO-E“) veröffentlicht. Der KI-VO-E berücksichtigt u.a. 1215 Beiträge zur Konsultation zum Weißbuch zur KI vom 19.02.2020,[1] die Schlussfolgerungen des Rates vom 21.10.2020[2], diverse Entschließungen des Europäischen Parlamentes zur KI[3] sowie solche der High Level Expert Group on AI.[4] Er setzt sich gleich in seiner Begründung nicht nur mit den Chancen des Einsatzes von KI sondern vielmehr mit den von KI ausgehenden Risiken auseinander und verweist insoweit u.a. auf die Forderung des Rates, insbesondere Probleme wie Undurchsichtigkeit, Komplexität, der sogenannte „Bias“, ein gewisses Maß an Unberechenbarkeit und teilweise autonomes Verhalten einiger KI-Systeme anzugehen, um deren Vereinbarkeit mit den Grundrechten sicherzustellen und die Durchsetzung der Rechtsvorschriften zu erleichtern.[5]

Folgende Ziele sind mit dem Verordnungsvorschlag verbunden[6]:

- Es muss gewährleistet sein, dass die auf dem Unionsmarkt in Verkehr gebrachten und verwendeten KI-Systeme sicher sind und die bestehenden Grundrechte und die Werte der Union wahren.
- Zur Förderung von Investitionen in KI und innovativen KI muss Rechtssicherheit gewährleistet sein.
- Die Governance und die wirksame Durchsetzung des geltenden Rechts zur Wahrung der Grundrechte sowie die Sicherheitsanforderungen an KI-Systeme müssen gestärkt werden.
- Die Entwicklung eines Binnenmarkts für rechtskonforme, sichere und vertrauenswürdige KI-Anwendungen muss erleichtert werden und es gilt, eine Marktfragmentierung zu verhindern.

Die Bundesrechtsanwaltskammer begrüßt den Regulierungsvorschlag der Kommission als weltweit ersten und mutigen Versuch, einen Rechtsrahmen für die Entwicklung, das Inverkehrbringen, den Betrieb und auch die im Rahmen beruflicher Tätigkeiten erfolgende Nutzung künstlicher Intelligenz durch Private ebenso wie durch staatliche Behörden zu schaffen und dabei den Schutz der von KI-Systemen Betroffenen in den Fokus zu nehmen.

---

[1] Weißbuch zur künstlichen Intelligenz – Ein europäisches Konzept für Exzellenz und Vertrauen, COM(2020) 65 final/2, 2020.
[2] Rat der Europäischen Union, Schlussfolgerungen des Vorsitzes – Die Charta der Grundrechte im Zusammenhang mit künstlicher Intelligenz und dem digitalen Wandel, 11481/20, 2020.
[3] Entschließungen des Europäischen Parlaments vom 20.10.2020 mit Empfehlungen an die Kommission zu dem Rahmen für ethische Aspekte von künstlicher Intelligenz, Robotik und damit zusammenhängenden Technologien, 2020/2012 (INL), für eine Regelung der zivilrechtlichen Haftung beim Einsatz künstlicher Intelligenz, 2020/2014 (INL), zu den Rechten des geistigen Eigentums bei der Entwicklung von KI-Technologien, 2020/2015 (INI), ferner Berichtsentwürfe über künstliche Intelligenz im Strafrecht und ihre Verwendung durch die Polizei und Justizbehörden in Strafsachen, 2020/2016(INI), und über künstliche Intelligenz in der Bildung, der Kultur und dem audiovisuellen Bereich, 2020/2017(INI).
[4] HLEG, Ethics Guidelines for Trustworthy AI, 2019; HLEG, Assessment List for Trustworthy Artificial Intelligence (ALTAI) for self-assessment, 2020.
[5] KI-VO-E, Seite 2.
[6] Begründung zum KI-VO-E, Ziff. 1.1, Seite 3.

Die Zukunft ist digital, das nimmt Anwaltschaft und Rechtsdienstleistungen nicht aus. Digitalisierung schafft Innovationen und Effizienzgewinne, was Unternehmen wie Verbrauchern gleichermaßen zugutekommt. Qualitätssteigerung und Effektivität liegen im Interesse der Mandanten und damit auch der Anwaltschaft. In diesem Digitalisierungsprozess ist indes sorgfältig zwischen weiterer Digitalisierung und Wahrung der Grundwerte des Rechtsstaats abzuwägen. Es ist nach Lösungen zu suchen, wie bewährte rechtsstaatliche Prinzipien mit den Vorteilen moderner Kommunikation im Interesse der Rechtsuchenden und eines funktionierenden Rechtsstaats in der digitalen Welt verbunden werden können. Dem trägt der KI-VO-E durchweg in begrüßenswerter Weise Rechnung. Insgesamt handelt es sich um einen großen Wurf der Kommission. Gleichwohl bedarf dieser an einzelnen Stellen der Nachschärfung.

Zum Einwurf im Einzelnen:

1. Allgemeines

Die Kommission gründet den Verordnungsvorschlag auf Art. 114 AEUV zur Binnenmarktintegration, zusätzlich kommt Art. 16 AEUV hinsichtlich der Verarbeitung personenbezogener Daten zur Anwendung. Die BRAK erinnert in diesem Zusammenhang daran, dass auch bei solchen Vorhaben, die nicht unmittelbar auf Grundlage der justiziellen Zusammenarbeit fußen, die rechtsstaatlichen Belange der Justiz und Rechtspflege beachtet werden müssen, wo diese berührt wird.

Die Kommission verfolgt einen horizontalen (nicht sektorspezifischen) und risikobasierten Ansatz, ergänzt durch einen Verhaltenskodex für KI-Systeme, die kein hohes Risiko darstellen. Der Anwendungsbereich des KI-VO-E soll sich dabei auch auf Anbieter bzw. Betreiber außerhalb der EU erstrecken, sofern deren Systeme in der EU in den Verkehr gebracht oder in Betrieb genommen werden; außerhalb der EU ansässige KI-Nutzer sind erfasst, wenn das von dem System hervorgebrachte Ergebnis in der EU verwendet wird (Art. 2 Abs. 1 KI-VO-E). Das ist zu begrüßen; ausgesprochen bedenklich erscheint indessen, dass von diesem weiten Anwendungsbereich generell nach Art. 2 Abs. 4 KI-VO-E Behörden und internationale Organisationen ausgenommen sein sollen, soweit diese im Rahmen internationaler Übereinkünfte im Bereich der Strafverfolgung und justiziellen Zusammenarbeit mit der EU oder mit einem oder mehreren Mitgliedsstaaten KI-Systeme verwenden. Damit könnten von KI-Systemen erzeugte Ergebnisse, die von EU-Behörden bzw. Strafverfolgungsbehörden der EU-Mitgliedsstaaten nach den Vorgaben des KI-VO-E grundsätzlich nicht erzeugt und verwendet werden dürften, in deren Ermittlungsergebnisse über ausländische Behörden und Organisationen gleichwohl einfließen. Zudem ist nicht ausgeschlossen, dass die Behörden der EU und deren Mitgliedsstaaten im Rahmen der Zusammenarbeit mit entsprechenden Behörden und Organisationen in Drittstaaten letztlich an von diesen erzeugten KI-Ergebnissen mitwirken, selbst soweit diese Drittstaaten hiesige rechtsstaatliche Standards und die Anforderungen des KI-VO-E nicht erfüllen. Der vom KI-VO-E angestrebte Grundrechtsschutz gerade im Bereich der Strafverfolgung weist hier eine bedenkliche Lücke auf; offenbar ging der Kommission das Interesse an einer „ungestörten“ Zusammenarbeit mit Drittstaaten im Bereich der Strafverfolgung vor. Dies sollte dringend überdacht werden.

Hinsichtlich der Definition umfasster KI-Systeme in Art. 3 Nr. 1 KI-VO-E verfolgt die Kommission ebenfalls einen weiten Ansatz. Als KI umfasst ist danach eine Software (gleich ob in Produkte eingebettet oder als „stand alone“-Lösung), die mit einer der in Anhang I des KI-VO-E aufgeführten Techniken und Konzepte entwickelt worden ist und im Hinblick auf von Menschen festgelegte Ziele Ergebnisse wie Inhalte, Vorhersagen, Empfehlungen oder Entscheidungen hervorbringen kann, die das Umfeld beeinflussen, mit dem sie interagieren. Zu den entsprechenden Techniken und Konzepten des Anhanges I des KI-VO-E zählen Konzepte des maschinellen Lernens unter Verwendung einer breiten Palette von

Methoden, einschließlich des „deep learning“, logik- und wissensgestützte Konzepte inklusive Expertensysteme, sowie statistische Ansätze, Bayessche Schätz-, Such- und Optimierungsmethoden. Auch hinsichtlich der für die Entwicklung von KI-Systemen unentbehrlichen Daten weist Art. 3 Nrn. 29 – 33 KI-VO-E sehr weitreichende Definitionen für Trainingsdaten, Validierungsdaten, Testdaten, Eingabedaten und biometrische Daten auf.

2. Risikoeinteilung

Der risikobasierte Ansatz des KI-VO-E trennt zwischen KI-Systemen mit unannehmbarem, mit hohem, mit geringem und mit minimalem Risiko. Solche mit unannehmbarem Risiko sind im Grundsatz verboten (Art. 5 KI-VO-E).

Hochrisiko-KI-Systeme unterliegen einem Risikomanagementsystem (Art. 6 ff., 9 KI-VO-E), näher bestimmten Daten-Governance- und Datenverwaltungsverfahren für Trainings-, Validierungs- und Testdatensätzen (Art. 10 KI-VO-E), Dokumentations- und Aufzeichnungspflichten (Art. 11 und 12 KI-VO-E), Protokollierungsanforderungen (Art. 12 KI-VO-E), Transparenzanforderungen (Art. 13 KI-VO-E), müssen von Menschen wirksam beaufsichtigt werden können (Art. 14 KI-VO-E) und einem angemessenen Maß an Genauigkeit, Robustheit und Cybersicherheit entsprechen (Art. 15 KI-VO-E). Anbieter unterliegen einem strengen Pflichtenkatalog (Art. 16 KI-VO-E) müssen u.a. ein Qualitätsmanagementsystem einrichten, Dokumentationspflichten erfüllen und Konformitätsbewertungsverfahren durchführen (Art. 17 ff. KI-VO-E). Insgesamt sind diese und weitere Pflichten von Herstellern, Bevollmächtigten, Einführern, Händlern und Nutzern oder die Anbringung von CE-Kennzeichen den in weiten Teilen vereinheitlichen Produktvorschriften aus unterschiedlichsten Bereichen[7] angenähert.

Für andere als Hochrisiko-KI-Systeme gelten im Wesentlichen nur Transparenzpflichten, insbesondere, wenn sie der Interaktion mit Menschen, der Emotionserkennung oder biometrischen Kategorisierung dienen oder „Deepfakes“ ermöglichen (Art. 52 KI-VO-E).

a) Verbotene KI-Systeme und Ausnahmetatbestände

Zu den verbotenen KI-Systemen zählen insbesondere solche zum „social scoring“, die der Bewertung oder Klassifizierung der Vertrauenswürdigkeit natürlicher Personen über einen bestimmten Zeitraum auf der Grundlage ihres sozialen Verhaltens oder bekannter oder vorhergesagter persönlicher Eigenschaften oder Persönlichkeitsmerkmale dienen. Dieses Verbot wird indessen durch Art. 5 Abs. 1 lit. c) KI-VO-E zunächst dahingehend relativiert, dass es nur solche Systeme betrifft, die zu einer Schlechterstellung oder Benachteiligung natürlicher Personen führen, sei dies aufgrund von sozialen Zusammenhängen, die in keinem Kontext mit der ursprünglichen Datenerzeugung stehen oder in einer Weise, die sich im Hinblick auf ihr soziales Verhalten oder dessen Tragweise ungerechtfertigt oder unverhältnismäßig erweist. Bereits dies schränkt das Verbot erheblich ein. Vor allem jedoch teilt die BRAK die Kritik, dass sich das Verbot nur an öffentliche bzw. staatliche Stellen, nicht hingegen an private Betreiber richtet.[8]

[7] Hierzu vgl. auch die dem besseren Verständnis und der einheitlichen und kohärenteren Anwendung der Produktvorschriften der EU in den verschiedenen Bereichen und im gesamten Binnenmarkt dienende Bekanntmachung der Kommission „Leitfaden für die Umsetzung der Produktvorschriften der EU 2016“ („Blue Guide“)“ (2016/C 272/01).
[8] Vgl. Spindler, CR 6/2021, 361 ff., Rdn. 25 f.

Grundsätzlich im Bereich der KI verboten ist nach Art. 5 Abs. 1 lit. d) 2 KI-VO-E die Verwendung biometrischer Echtzeit-Fernidentifizierungssysteme in öffentlich zugänglichen Räumen zu Strafverfolgungszwecken, was indes wiederum durch umfassende Ausnahmen stark relativiert wird. So soll der Einsatz nach Art. 5 Abs. 1 lit. d) i) – iii) KI-VO-E zulässig sein, wenn dies „unbedingt erforderlich" ist zur gezielten Suche nach potenziellen Opfern von Straftaten oder vermissten Kindern, zur Abwendung von konkreten, erheblichen und unmittelbaren Gefahren für Leib und Leben einschließlich der Terrorprävention, oder zur Strafverfolgung bei einer Straftat, die nach dem Recht des betreffenden Staates mit einer Freiheitsstrafe oder freiheitsentziehenden Sicherungsmaßregel von mindestens drei Jahren geahndet werden kann.

Auch in den EU-Mitgliedsstaaten findet schon heute eine weitreichende Videoüberwachung im öffentlichen Raum statt,[9] die Betroffene in einer Vielzahl von Grundrechten zu beeinträchtigen geeignet ist – einschließlich der anwaltlichen Berufsausübung, deren Schutz vor staatlicher Kontrolle und Bevormundung nicht allein den individuellen Belangen des Rechtsanwalts und seines Mandanten dient, sondern auch und vor allem dem öffentlichen Interesse an einer wirksamen und geordneten Rechtspflege Rechnung trägt und das Vertrauensverhältnis zwischen Anwalt und Mandant schützt. Maßnahmen, die geeignet sind, das Entstehen des Vertrauensverhältnisses zwischen Rechtsanwalt und Mandant auch nur im Ansatz zu stören oder gar auszuschließen, greifen nicht nur in die Subjektstellung des Mandanten, sondern auch in die Berufsausübungsfreiheit des Rechtsanwalts ein.[10] Die anwaltliche Verschwiegenheit ist Ausdruck der besonderen Stellung des Anwalts als Organ der Rechtspflege und dient folglich auch und insbesondere dem Interesse des Mandanten, sie wird durch Art. 6 i.V.m. Art. 8 EMRK geschützt.

Auch wenn Art. 5 Abs. 2 KI-VO-E vermeintlich strenge Anforderungen an die Verhältnismäßigkeit des Einsatzes entsprechender biometrischer Echtzeit-Fernidentifizierungssysteme stellt, so teilt die BRAK die gegen die vorgesehenen Ausnahmen sowie die in Art. 5 Abs. 4 KI-VO-E vorgesehene Öffnungsklausel, die es den Mitgliedstaaten ermöglicht, den Einsatz entsprechender Systeme unter den in Art. 5 Abs. 1 lit d), 2 – 4 KI-VO-E vorgesehenen Bedingungen grundsätzlich vollständig oder teilweise zu genehmigen, wonach im Ergebnis die Massenüberwachung im öffentlichen Raum nicht verhindert, sondern vielmehr ermöglicht wird.[11] Dies gilt umso mehr, als von dem generellen Verbot Überwachungstechnologien, welche entweder nicht in Echtzeit arbeiten oder von anderen als staatlichen Strafverfolgungsbehörden durchgeführt werden, überhaupt nicht umfasst sind.[12] Angesichts der Risiken dieser Technologien muss ein derartiger KI-Einsatz nach Auffassung der BRAK insbesondere durch Private erst recht vom Verbotstatbestand umfasst sein.

Ergänzend anzumerken sei schließlich, dass die in Art. 5 Abs. 1 lit. d) i) und ii) KI-VO-E normierten Ausnahmetatbestände Fälle der Gefahrenabwehr und nicht der Strafverfolgung betreffen und daher ohnehin nicht dem generellen, auf Strafverfolgungszwecke beschränkten Verbot des Art. 5 Abs. 1 KI-VO-E unterfallen dürften.

---

[9] Eine im Sommer 2019 am Berliner Bahnhof Südkreuz getestete intelligente Analysesoftware soll beispielsweise in der Lage gewesen sein, liegende Personen, das Betreten bestimmter Bereiche sowie Personenströme und Ansammlungen oder abgestellte Gegenstände und ihr Verhältnis zu Personen zu erkennen (s. ZD-Aktuell 2019, 06071). In einem niederländischen Testlauf führt die KI „ethnisches" Profiling zur Identifizierung von Dieben durch: https://t1p.de/f6te, aufgerufen am 25.06.2021.

[10] Vgl. BVerfG, NJW 2020, 1740 m.w.N.

[11] Auch hierzu vgl. Spindler, CR 6/2021, Rdn. 27 m.w.N.

[12] Der Einsatz der Anwendung des umstrittenen Unternehmens Clearview AI würde nicht als verbotene KI mit unannehmbarem Risiko im Sinne der Verordnung eingestuft werden.

b) Hochrisiko-KI-Systeme

Als Systeme mit hohem Risiko werden nach dem KI-VO-E insbesondere solche Systeme angesehen, die in Anbetracht ihres Verwendungszweckes ein hohes Risiko für die Gesundheit, Sicherheit oder die Grundrechte der Unionsbürger darstellen, wobei sowohl die Schwere des möglichen Schadens als auch die Wahrscheinlichkeit seines Eintretens zu berücksichtigen sind.[13] Konkret erfasst Art. 6 Abs. 1 KI-VO-E insoweit KI-Systeme, die als Sicherheitskomponente eines der in Anhang II aufgeführten produktsicherheitsrechtlichen Vorschriften unterfallenden Produktes verwendet werden oder selbst ein solches Produkt darstellen und entsprechende Produkte zudem einer Konformitätsbewertung nach den in Anhang II aufgeführten Vorschriften unterliegen. Angesprochen sind damit KI-Systeme in Produkten, die sicherheitsrelevanten Richtlinien und Verordnungen für Maschinen, Spielzeuge, Sportboote, Aufzüge, Funkanlagen, Medizinprodukte und dgl. mehr unterliegen.

Ferner als Hochrisiko-KI-Systeme erfasst sind nach Art. 6 Abs. 2 KI-VO-E die in Anhang III KI-VO-E beschriebenen KI-Systeme. Zu diesen zählen neben Systemen zur biometrischen Identifizierung und Kategorisierung natürlicher Personen, Verwaltung und Betrieb kritischer Infrastrukturen, allgemeiner und beruflicher Bildung, Beschäftigung, Personalmanagement und Zugang zur Selbstständigkeit sowie der Zugänglichkeit und Inanspruchnahme grundlegender privater und öffentlicher Dienste und Leistungen auch und vor allem KI-Systeme im Bereich „Strafverfolgung“ (Anhang III, Ziff. 6), „Migration“, „Asyl und Grenzkontrolle“ (Anhang III, Ziff. 7) sowie „Rechtspflege und demokratische Prozesse“. Auf die drei letztgenannten Bereiche soll in abweichender Reihenfolge nachstehend näher eingegangen werden. Verkannt wird dabei nicht, dass sich der KI-VO-E in erster Linie auf Art. 114 AEUV stützt, der die Annahme von Maßnahmen für die Errichtung und das Funktionieren des Binnenmarktes vorsieht, und der Kommission im Übrigen im Hinblick auf die grundsätzliche Rechtssetzungskompetenz der Mitgliedsstaaten und den Subsidiaritätsgrundsatz im Bereich der Justiz enge Grenzen gesetzt sind. Gleichwohl darf dies kein grundsätzlicher Hinderungsgrund sein, KI-Systeme mit tatsächlich unannehmbar hohem Risiko lediglich als Hochrisiko-KI zu beurteilen und den Mitgliedstaaten insoweit – wenn auch unter Beachtung der künftigen Anforderungen des KI-VO-E – Einsatzmöglichkeiten zu eröffnen. Dies vorausgeschickt ist Folgendes anzumerken:

(1) KI-Systeme im Bereich „Rechtspflege und demokratische Prozesse“

Unter der Überschrift „Rechtspflege und demokratische Prozesse“ beschreibt Anhang III, Ziff. 8 KI-VO-E:

> *„KI-Systeme, die bestimmungsgemäß Justizbehörden bei der Ermittlung und Auslegung von Sachverhalten und Rechtsvorschriften und bei der Anwendung des Rechts auf konkrete Sachverhalte unterstützen sollen.“*

Der Verordnungsentwurf spricht an diversen Stellen von „Justizbehörden und unabhängigen Verwaltungsbehörden“ sowie von „Strafverfolgungsbehörden“. Als „Justizbehörden“ im Sinne des Anhanges III, Ziff. 8, werden daher in erster Line, wenn nicht ausschließlich, die Gerichte zu verstehen sein. Der Regelungsentwurf umfasst damit keineswegs weitgehende Bereiche von „Rechtspflege und demokratischen Prozessen“, wie dies die Überschrift andeutet. Da der Vorschlag die Sachverhaltsfeststellung, Rechtsanwendung und Subsumtion erfasst, die nicht nur Sache von Gerichten, sondern gerade im öffentlichen Recht vielmehr auch der Verwaltungsbehörden ist, deren Entscheidungen nicht minder gravierende Auswirkungen als ein Urteil haben können und die gerichtlichen Entscheidungen – so der

[13] Vgl. ErwGr. 32 KI-VO-E.

weitere Rechtsweg vom Betroffenen denn beschritten wird – durchweg vorgelagert sind, tritt die Bundesrechtsanwaltskammer für eine Erweiterung des Anhangs III Ziff. 8 auf solche Entscheidungen von Verwaltungsbehörden ein, die in gleicher Weise wie ein Urteil der Rechtskraft fähig sind.

Klarstellungsbedürftig erscheint auch, dass die Regelung keineswegs nur KI-Systeme betrifft, die bei Ermittlung und Auslegung von Sachverhalten und Rechtsvorschriften und Anwendung des Rechts unterstützen sollen, sondern auch bei der Ermittlung oder Auslegung von Sachverhalten oder Rechtsvorschriften oder der Rechtsanwendung.

Was nach dem Regelungsvorschlag gänzlich ausgeschlossen scheint, ist der Einsatz von KI-Systemen, die bei der Ermittlung/Auslegung von Sachverhalten und Rechtsvorschriften sowie der Rechtsanwendung nicht nur „unterstützen" sollen, sondern an Stelle einer „menschlichen" Entscheidung treten, die Ermittlung/Auslegung von Sachverhalten und Rechtsvorschriften und die Anwendung folglich selbsttätig vornehmen. Dann allerdings wäre es nur konsequent, entsprechende KI-Systeme als solche mit unannehmbar hohem Risiko zu qualifizieren und damit einem Verbot zu unterwerfen. Für ein solches Verbot spricht, dass die von der Justiz getroffenen Entscheidungen Menschen und deren weitere Schicksale prägen. Eine unabhängige und vertrauenswürdige Justiz stellt einen Grundpfeiler gleichermaßen eines Rechtsstaats und einer freiheitlich demokratischen Grundordnung dar. Der Einsatz von KI muss daher maßvoll erfolgen, um das gesellschaftliche Vertrauen in die Arbeit der Justiz nicht dauerhaft zu beschädigen. Mit dem KI-VO-E soll gerade sichergestellt werden, dass das Recht auf einen wirksamen Rechtsbehelf und ein unparteiisches Gericht und die Unschuldsvermutung gewahrt werden (Art. 47 und 48 EU-Grundrechtecharta) sowie der allgemeine Grundsatz guter Verwaltung gewahrt werden. Die Verpflichtungen zu Vorabtests, Risikomanagement und menschlicher Aufsicht sollen das Risiko, in kritischen Bereichen wie unter anderem der Strafverfolgung und Justiz mithilfe der KI falsche oder verzerrte Entscheidungen zu treffen, nach dem ausdrücklichen Willen der Kommission verringern.[14] Die Garantie des wirkungsvollen Rechtsschutzes ist ein wesentlicher Bestandteil des Rechtsstaats und umfasst auch den Zugang zu den Gerichten, die Prüfung des Streitbegehrens in einem förmlichen Verfahren sowie die verbindliche gerichtliche Entscheidung. Diese Rechtsschutzmöglichkeit wird in Deutschland aus dem Rechtsstaatsprinzip i.V.m. Art. 2 Abs. 1 GG als allgemeiner Justizgewährungsanspruch abgeleitet. Aus dem Wortlaut von Art. 92 i.V.m. Art. 97 GG ergibt sich, dass die rechtsprechende Gewalt dem Richter vorbehalten ist. Nach Art. 101 Abs. 1 S. 2 GG darf niemand seinem gesetzlichen Richter entzogen werden; dabei steht fest, dass der gesetzliche Richter im Sinne dieser Norm eine natürliche Person sein muss[15]. Auch nach §§ 1, 2, 5, 5 a ff., 25 f. DRiG und insbesondere § 27 Abs. 1 DRiG („Richter auf Lebenszeit") muss der Richter eine natürliche Person sein, ebenso wie nach einzelnen Verfahrensordnungen (so etwa § 348 Abs. 1 S. 1 ZPO, wonach im Grundsatz die Zivilkammer durch eines ihrer Mitglieder als Einzelrichter entscheidet).[16] Zudem dürfte auch das Recht auf ein öffentliches Verfahren aus Art. 6 EMRK die Leitung durch einen menschlichen Richter voraussetzen. Hinzu kommt schließlich, dass eine mit vorbestehenden Daten trainierte und entscheidungsersetzende KI in der Justiz kaum je in der Lage sein wird, noch unbestimmte Rechtsbegriffe auszufüllen, besondere Einzelfallgestaltungen oder gar gesellschaftliche Entwicklungen zu berücksichtigen und Rechtsfortbildung zu betreiben.

Dies bedeutet, dass gerichtliche Entscheidungen im Grundsatz dem Menschen vorbehalten bleiben müssen – Urteile über Menschen sind von Menschen zu treffen. Den Richter vollständig durch KI-Systeme, die selbstständig Entscheidungen treffen, zu ersetzen, ist daher ausgeschlossen. Eine KI kann nicht die Entscheidungsgewalt haben. Nach der Rechtsprechung des BVerfG soll der Einzelne nicht bloßes Objekt des gerichtlichen Verfahrens sein, sondern vor einer Entscheidung, die seine Rechte

[14] Ziff. 3.5 der Begründung sowie ErwGr. 28 und des KI-VO-E.
[15] Vgl. Enders, Einsatz künstlicher Intelligenz bei juristischer Entscheidungsfindung, JA 2018, 721, 722 m.w.N.
[16] Enders, a.a.O. m.w.N.

betrifft, zu Worte kommen, um Einfluss auf das Verfahren und sein Ergebnis nehmen zu können.[17] Eine dem verfassungsrechtlichen Anspruch genügende Gewährung rechtlichen Gehörs setzt auch voraus, dass der Verfahrensbeteiligte bei Anwendung der von ihm zu verlangenden Sorgfalt zu erkennen vermag, auf welchen Tatsachenvortrag es für die Entscheidung ankommen kann. Dies ist bei einer von KI getroffenen Entscheidung nicht zu gewährleisten. Richterliche Entscheidungen allein basierend auf Vorgaben selbstständig entscheidender KI-Systeme wären letztendlich eine reine Formalität. Dies schließt letztlich auch solche Systeme aus, die zu einem „Übernahmeautomatismus" führen und in dem der Richter die Entscheidung nicht mehr fällt, sondern nur noch verkündet.[18] Gänzlich ausgeschlossen erscheint der BRAK der Einsatz von KI-Systemen damit insbesondere in Straf- und Strafvollstreckungsverfahren.

Was damit in Anbetracht der unbestreitbaren Effizienz- und Kostenvorteile des Einsatzes künstlicher Intelligenz gleichwohl nicht von vornherein ausgeschlossen sein sollte, ist Parteien in zivil- oder verwaltungsgerichtlichen Rechtsstreitigkeiten die Möglichkeit zu geben, sich freiwillig einer automatisierten Entscheidung zu unterwerfen, sofern diese anfechtbar ist und insoweit der Entscheidung durch einen menschlichen Richter unterzogen werden kann – nicht anders etwa, als Parteien die Möglichkeit haben, sich einer gerichtsinternen Mediation zu unterwerfen und deren Resultat als endgültige Regelung zu akzeptieren oder aber abzulehnen und auf einer Entscheidung durch menschliche Richter zu bestehen. Die Regelung des Art. 22 DS-GVO kann insoweit Leitlinie auch für gerichtliche Entscheidungen durch KI-Systeme sein. Wollte man den Einsatz entsprechender entscheidungsersetzender aber auf freiwilliger Inanspruchnahme beruhender und der Überprüfung durch menschliche Richter unterliegender KI-Systeme in der Justiz gänzlich ausschließen, so könnte dies eine Abwanderung in die Streiterledigung durch KI-Systeme privater Betreiber zur Folge haben, wie sie auch jetzt bereits vielfältig etwa bei Zahlungsdienstleistern oder Internet-Marktplätzen eingesetzt werden. Zweifellos mehr Vertrauen dürfte der Bürger jedoch in justiz-eigene KI-Systeme haben, deren Entwicklung nicht von vornherein unterbunden werden sollte. Entsprechendes Vertrauen wird allerdings auch nur dann entstehen, wenn die verwendete KI hinreichend „neutral" ist, nicht also etwa bei Einsatz eines streiterledigenden KI-Systems einer Verwaltungsbehörde in einem diese betreffenden Verfahren. Derartige Anwendungsmöglichkeiten müssen ausgeschlossen bleiben.

Lediglich entscheidungsunterstützende KI-Systeme sind nach dem KI-VO-E zwar grundsätzlich zulässig, sie werden aus gutem Grund jedoch als Hochrisiko-Systeme beurteilt und den diesbezüglichen Anforderungen unterworfen, insbesondere der menschlichen Aufsicht nach Art. 14 KI-VO-E, die es den aufsichtführenden Personen u.a. ermöglichen soll, die Fähigkeiten und Grenzen des Systems zu verstehen, Anzeichen von Anomalien und Fehlern zu erkennen und sich einer möglichen Neigung zu einem automatischen oder übermäßigen Vertrauen in das von einem Hochrisiko-KI-System hervorgebrachte Ergebnis („Automatisierungsbias") bewusst zu bleiben. Einem solchen Automatisierungsbias kann auch der Richter unterliegen und es insoweit unbewusst versäumen, den Parteien hinreichendes rechtliches Gehör zu gewähren. Jedenfalls im Bereich der Justiz hält die BRAK es daher für erforderlich, dass die Parteien hinreichend darüber aufgeklärt werden, welches KI-System zur Unterstützung richterlicher Entscheidungsfindung verwendet wurde. Da die Parteien mit dem KI-System selbst nicht interagieren und selbst nicht dessen Nutzer sind, nützen ihnen die Transparenzpflichten nach den Art. 13 und 52 KI-VO-E nicht. Die BRAK hält daher die Einführung einer Informationspflicht über den Einsatz entscheidungsunterstützender KI-Systeme in der Justiz für erforderlich.

[17] BVerfG, NJW 1984, 113; BVerfG, NJW 1984, 2403; BVerfG NJW, 2013, 1058, 1060 Rdn. 58.
[18] Vgl. auch Enders, a.a.O. (Fn. 15), S. 723.

(2) Hochrisiko-KI-Systeme im Bereich der Strafverfolgung

Im Bereich der Strafverfolgung sieht Anhang III, Ziff. 6. des KI-VO-E detaillierte Definitionen von Hochrisiko-KI-Systemen vor, nämlich in nachfolgender Gliederung solche, die von Strafverfolgungsbehörden

a) für individuelle Risikobewertungen natürlicher Personen verwendet werden sollen, um das Risiko abzuschätzen, dass eine natürliche Person Straftaten begeht oder erneut begeht oder dass eine Person zum Opfer möglicher Straftaten wird;
b) als Lügendetektoren und ähnliche Instrumente oder zur Ermittlung des emotionalen Zustands einer natürlichen Person verwendet werden sollen;
c) zur Aufdeckung von Deepfakes gemäß Artikel 52 Absatz 3 verwendet werden sollen;
d) zur Bewertung der Verlässlichkeit von Beweismitteln im Zuge der Ermittlung oder Verfolgung von Straftaten verwendet werden sollen;
e) zur Vorhersage des Auftretens oder erneuten Auftretens einer tatsächlichen oder potenziellen Straftat auf der Grundlage des Profils natürlicher Personen gemäß Artikel 3 Absatz 4 der Richtlinie (EU) 2016/680 oder zur Bewertung von Persönlichkeitsmerkmalen und Eigenschaften oder vergangenen kriminellen Verhaltens natürlicher Personen oder von Gruppen verwendet werden sollen;
f) zur Erstellung von Profilen natürlicher Personen gemäß Artikel 3 Absatz 4 der Richtlinie (EU) 2016/680 im Zuge der Aufdeckung, Ermittlung oder Verfolgung von Straftaten verwendet werden sollen;

sowie schließlich generell KI-Systeme,

g) die bestimmungsgemäß zur Kriminalanalyse natürlicher Personen eingesetzt werden sollen und es den Strafverfolgungsbehörden ermöglichen, große komplexe verknüpfte und unverknüpfte Datensätze aus verschiedenen Datenquellen oder in verschiedenen Datenformaten zu durchsuchen, um unbekannte Muster zu erkennen oder verdeckte Beziehungen in den Daten aufzudecken.

In Erwägungsgrund 38 KI-VO-E wird zutreffend darauf hingewiesen, dass Maßnahmen von Strafverfolgungsbehörden im Zusammenhang mit bestimmten Verwendungen von KI-Systemen durch ein erhebliches Machtungleichgewicht gekennzeichnet sind und zur Überwachung, Festnahme oder zum Entzug der Freiheit einer natürlichen Person sowie zu anderen nachteiligen Auswirkungen auf die in der Grundrechtecharta verankerten Grundrechte führen können. Dies gelte insbesondere dann, wenn das KI-System nicht mit hochwertigen Daten trainiert werde, die Anforderungen an seine Genauigkeit oder Robustheit nicht erfülle oder das System nicht ordnungsgemäß konzipiert und getestet werde, bevor es in Verkehr gebracht oder in anderer Weise in Betrieb genommen werde. Denn in diesen Fällen könne es Personen in diskriminierender oder anderweitig falscher oder ungerechter Weise ausgrenzen. Wie in Erwägungsgrund 38 KI-VO-E ferner zutreffend ausgeführt wird, könnte die Ausübung wichtiger verfahrensrechtlicher Grundrechte wie des Rechts auf einen wirksamen Rechtsbehelf und ein unparteiisches Gericht sowie die Unschuldsvermutung und Verteidigungsrechte behindert werden. Dies gelte insbesondere, wenn solche KI-Systeme nicht hinreichend transparent, erklärbar und dokumentiert sind, weshalb es angezeigt sei, eine Reihe von KI-Systemen, die im Rahmen der Strafverfolgung eingesetzt werden sollen und bei denen Genauigkeit, Zuverlässigkeit und Transparenz besonders wichtig sind, als hochriskant einzustufen, um nachteilige Auswirkungen zu vermeiden, das Vertrauen der Öffentlichkeit zu erhalten und die Rechenschaftspflicht und einen wirksamen Rechtsschutz zu gewährleisten. Angesichts der Art der betreffenden Tätigkeiten und der damit verbundenen Risiken sollten diese Hochrisiko-KI-Systeme nach Erwägungsgrund 38 KI-VO-E insbesondere KI-Systeme umfassen, die von Strafverfolgungsbehörden für individuelle Risikobewertungen, als Lügendetektoren und ähnliche Instrumente oder zur Ermittlung des emotionalen Zustands natürlicher Personen, zur Aufdeckung von „Deepfakes“, zur Bewertung der Zuverlässigkeit von Beweismitteln in Strafverfahren, zur Vorhersage des Auftretens oder erneuten Auftretens einer tatsächlichen oder potenziellen Straftat auf der Grundlage des Profils

natürlicher Personen oder zur Bewertung von Persönlichkeitsmerkmalen und Eigenschaften oder vergangenen kriminellen Verhaltens von natürlichen Personen oder Gruppen, zur Erstellung eines Profils während der Aufdeckung, Untersuchung oder strafrechtlichen Verfolgung einer Straftat sowie zur Kriminalanalyse in Bezug auf natürliche Personen eingesetzt werden.

So richtig die entsprechenden Erwägungen sind, so sehr überrascht, dass nicht wenigstens einzelne der angeführten Anwendungen nicht als KI mit unannehmbar hohem Risiko bewertet und einem entsprechenden Verbot unterworfen werden. Ein Verbot fordert die BRAK aus den von der Kommission selbst angeführten Gründen jedenfalls für KI-Systeme zur Abschätzung des Risikos, dass eine natürliche Person Straftaten begeht oder erneut begeht und KI-Systemen zum Einsatz als Lügendetektoren und ähnliche Instrumente oder zur Ermittlung des emotionalen Zustands einer natürlichen Person im Sinne des Anhanges III, Ziff. 6 lit. a) und b) KI-VO-E.

(3) Hochrisiko-KI-Systeme im Bereich Migration, Asyl und Grenzkontrolle

Nach Anhang III Ziff. 7 gelten im Bereich Migration, Asyl und Grenzkontrolle als Hochrisiko-KI-Systeme solche, die bestimmungsgemäß von den zuständigen Behörden

a) als Lügendetektoren und ähnliche Instrumente oder zur Ermittlung des emotionalen Zustands einer natürlichen Person verwendet werden sollen;
b) zur Bewertung eines Risikos verwendet werden sollen, einschließlich eines Sicherheitsrisikos, eines Risikos der irregulären Einwanderung oder eines Gesundheitsrisikos, das von einer natürlichen Person ausgeht, die in das Hoheitsgebiet eines Mitgliedstaats einzureisen beabsichtigt oder eingereist ist;
c) zur Überprüfung der Echtheit von Reisedokumenten und Nachweisunterlagen natürlicher Personen und zur Erkennung unechter Dokumente durch Prüfung ihrer Sicherheitsmerkmale verwendet werden sollen;
d) bei der Prüfung von Asyl- und Visumanträgen sowie Aufenthaltstiteln und damit verbundenen Beschwerden im Hinblick auf die Feststellung der Berechtigung der den Antrag stellenden natürlichen Personen unterstützen sollen.

Zutreffend wird in Erwägungsgrund 39 des KI-VO-E ausgeführt, dass KI-Systeme, die in den Bereichen Migration, Asyl und Grenzkontrolle eingesetzt werden, Menschen betreffen, die sich häufig in einer besonders prekären Lage befinden und vom Ergebnis der Maßnahmen der zuständigen Behörden abhängig sind. Die Genauigkeit, der nichtdiskriminierende Charakter und die Transparenz der KI-Systeme, die in solchen Zusammenhängen eingesetzt würden, seien daher besonders wichtig, um die Achtung der Grundrechte der betroffenen Personen, insbesondere ihrer Rechte auf Freizügigkeit, Nichtdiskriminierung, den Schutz des Privatlebens und personenbezogener Daten, den internationalen Schutz und die gute Verwaltung, zu gewährleisten.

In Anbetracht der Erwägungen der Kommission überrascht – wiederum – die Einordnung insbesondere der in Anhang III Ziff. 7 lit. a) und b) aufgezählten Systeme „nur“ als Hochrisiko-KI. Personen, welche vor Verfolgung oder ernsthaftem Schaden in ihren Herkunftsstaaten geflohen sind, haben das Recht, einen Antrag auf internationalen Schutz zu stellen. Das Grundrecht auf Asyl ist auf EU-Ebene in Art 18 GRC verankert. Zudem sind die EU-Mitgliedstaaten Vertragsparteien der Genfer Flüchtlingskonvention und haben entsprechende nationale Regelungen. Um seinen Schutzanspruch in der EU praktisch geltend machen zu können, muss der Schutzsuchende seinen Antrag effektiv an den EU-Außengrenzen oder innerhalb der Mitgliedstaaten stellen können. Auch hier weist die BRAK folglich auf die besonderen Gefahren des Einsatzes von Lügendetektoren vor Stellung eines Asylantrages, sowie von Anwendun-

gen, welche in diesem Zusammenhang auf ein Gefährdungspotential schließen lassen, hin und bekräftigt ihre Verbotsforderung für solche Technologien.[19] Dies gilt umso mehr, als fraglich ist, wie die betroffenen Personen gegen entsprechende KI-Entscheidungen in prekären Situationen denn tatsächlich vorgehen könnten. Es bestehen erhebliche Zweifel daran, dass Asylsuchende bei Einsatz derartiger Technologien ihren Anspruch auf Asyl wirksam geltend machen können. Asylsuchende haben zwar aus Art. 22 Asylverfahrens-RL einen Anspruch auf Rechtsberatung und -Vertretung im gesamten Asylverfahren und aus Art. 46 Verfahrens-RL ergibt sich das Recht auf einen wirksamen Rechtsbehelf. Beides jedoch erscheint bei Einsatz entsprechender KI-Systeme in besonderem Maße gefährdet. Auch vor dem Hintergrund der derzeit das EU-Gesetzgebungsverfahren durchlaufenden Vorhaben über ein Vorab-Screening mit beschleunigtem Asylverfahren erscheint der Einsatz von entsprechenden KI-Technologien an den Grenzen angesichts des Rechts auf ein faires Verfahren nicht nur als hoch riskant, sondern als unannehmbar und wird von der BRAK abgelehnt.

c) Ergänzend: Transparenzverpflichtungen für Hochrisiko- und bestimmte andere KI-Systeme

Aus Sicht der BRAK sind die unter Art. 13 KI-VO-E für Hochrisiko-KI-Systeme und Art. 52 KI-VO-E für zur Interaktion mit natürlichen Personen bestimmte sonstige KI-Systeme festgelegten Transparenzpflichten unerlässlicher Bestandteil der sicheren und nachvollziehbaren Anwendung von KI. Die entsprechenden Regelungen gelten nach ihrem jeweiligen Absatz 1 allerdings nur für solche KI-Systeme, die von vornherein für den jeweiligen Anwendungszweck entwickelt sind. Da sich der ursprüngliche Anwendungszweck von KI durch fortschreitendende technische Entwicklung ändern kann, sollten die entsprechenden Transparenzanforderungen jedenfalls klarstellend erweitert werden, indem in deren jeweiligem Absatz 1 jeweils folgender neuer Satz 2 eingefügt wird:

> „Dies gilt auch für entsprechende KI-Systeme, deren Anwendungszweck sich im Laufe des Einsatzes ändert. […]“

Kritisch erscheint der BRAK ferner, dass Betroffenen beim Einsatz der von Art. 52 KI-VO-E erfassten bestimmten KI-Systeme allein die dort normierten Informationspflichten zur Seite stehen, ohne dass sie den Einsatz entsprechender KI-Systeme beim Bezug von Waren oder der Inanspruchnahme von Leistungen ablehnen können.[20] Die BRAK fordert daher, Betroffenen die Möglichkeit einzuräumen, den Einsatz entsprechender KI-Systeme beim Bezug von Waren oder der Inanspruchnahme von Leistungen ablehnen zu können.

3. Aufsicht

Mit dem in Art. 56 ff. KI-VO-E vorgesehenen Aufsichtssystem ähnelt der Entwurf sehr den korrespondierenden Bestimmungen der DS-GVO, was im Übrigen auch für die vorgesehenen Sanktionen (Art. 71

[19] Derzeit wird das im Rahmen des EU-Projekts Horizon 2020 finanzierte Programm iBorderCtrl erprobt. Es arbeitet u.a. mit künstlicher Intelligenz und soll an den Grenzen derart eingesetzt werden, dass Migranten vor ihrer eigentlichen Antragsstellung mit einem Avatar in Kontakt treten und diesem Fragen beantworten. Das Programm sondert anhand von Mimik und Körpersprache mutmaßlich falsche Antworten aus. Es beinhaltet auch eine Gesichtserkennungstechnologie. Wird ein verdächtiger Fall gemeldet, werden Menschen zugeschaltet. Journalisten, welche das Programm getestet haben, berichten von einer Treffunsicherheit von ca. 25%. Zudem sollen hier Anwendungen zur Risikobeurteilung einzelner Personen zum Einsatz kommen. Gegen den Einsatz dieser Anwendung läuft derzeit ein Verfahren vor dem EuGH.

[20] Kritisch insoweit auch Spindler, CR 6/2021, 361, 368, Rdn. 46, der darauf hinweist, dass ein echtes opt-out-Recht, verbunden mit einem Anspruch auf Kontakt mit einem Menschen, dem Betroffenen mit der Regelung des Art. 52 (noch) nicht gewährt wird.

und 72 KI-VO-E) gilt. Auf europäischer Ebene soll mit einem „Europäischen Ausschuss für künstliche Intelligenz“ eine Einrichtung zur Beratung der EU-Kommission zum Zwecke der Koordinierung der Zusammenarbeit der nationalen Aufsichtsbehörden, der Koordinierung und Mitwirkung und an Leitlinien und Analysen der Kommission und nationaler Behörden sowie der Unterstützung der nationalen Aufsichtsbehörden und der Kommission bei der Gewährleistung einer einheitlichen Anwendung der Verordnung geschaffen werden. Anders als die nationale Datenschutzaufsicht soll die KI-Aufsicht durch nationale Behörden wahrgenommen werden, die als notifizierende Behörde und als Marktüberwachungsbehörde fungieren, wobei es den Mitgliedsstaaten freigestellt ist, mehr als eine Behörde zu benennen. Die entsprechenden Behörden sollten bei der Ausübung ihrer Tätigkeiten und der Wahrnehmung ihrer Aufgaben zwar Objektivität und Unparteilichkeit wahren, vollständige Unabhängigkeit wird von ihnen jedoch nicht verlangt.

In ihrem Weißbuch KI hatte die EU-Kommission vorgeschlagen, auf sektorspezifische Regulierungsbehörden zurückzugreifen und diese bei der Erweiterung ihrer KI-Kompetenzen zu unterstützen, damit sie einschlägige Vorschriften wirksam und effizient umsetzen können.[21] Dem trägt der Verordnungsentwurf Rechnung. So werden KI-Systeme zunächst der Marktüberwachungsverordnung[22] unterworfen (Art. 63 Abs. 1 KI-VO-E). Sodann ist vorgesehen, dass die Marktaufsichtsbehörden für harmonisierten Rechtsvorschriften unterliegende Produkte zugleich als zuständige Marktüberwachungsbehörden auch für die mit entsprechenden Produkten zusammenhängenden Hochrisiko-KI-Systeme gelten (Art. 63 Abs. 3 KI-VO-E). Entsprechendes gilt bei KI-Systemen, die von regulierten Finanzinstituten in den Verkehr gebracht, in Betrieb genommen oder eingesetzt werden; hier soll die jeweils zuständige Finanzaufsicht zugleich als zuständige KI-Marktüberwachungsbehörde gelten (Art. 63 Abs. 4 KI-VO-E). Für in den Bereichen Strafverfolgung, Migration, Asyl und Grenzkontrolle eingesetzte KI-Systeme haben die Mitgliedsstaaten wiederum jene Aufsichtsbehörden als zuständig zu benennen, die in diesen Bereichen nach der DS-GVO, der Datenschutz-RL für Polizei und Strafjustiz[23] oder aufgrund nationaler Bestimmungen bereits die Aufsicht führen (Art. 63 Abs. 5 KI-VO-E). Und soweit Organe, Einrichtungen und sonstige Stellen der EU in den Anwendungsbereich der Verordnung fallen, soll der Europäische Datenschutzbeauftragte die Funktion der für sie zuständigen Marktüberwachungsbehörde übernehmen (Art. 63 Abs. 6 KI-VO-E), der in Art. 59 Abs. 8 KI-VO-E ohnehin bereits als zuständige Aufsichtsbehörde vorgesehen ist.

In ihrer Stellungnahme 27/2020 hatte die BRAK darauf hingewiesen, dass die Aufsicht über den Einsatz von KI, soweit diese die Verarbeitung mandatsbezogener Daten umfasst, im anwaltlichen Bereich aus zwingenden rechtsstaatlichen wie primär- und verfassungsrechtlichen Gründen der anwaltlichen Selbstverwaltung vorbehalten bleiben muss und insoweit – zum wiederholten Male – die Einführung eines selbstverwalteten und unabhängigen Datenschutzbeauftragten aus der und für die Rechtsanwaltschaft gefordert, und dies insbesondere mit Blick auf den Einsatz von KI-Anwendungen in bzw. durch Anwaltskanzleien. Eine über entsprechende KI-Systeme auszuübende Aufsicht setzt nicht allein profunde Kenntnisse des anwaltlichen Berufsrechts und anwaltlicher Arbeitsabläufe zwingend voraus, sondern vielmehr ein grundlegendes Verständnis anwaltlicher Unabhängigkeit als Ausdruck rechtsstaatlich zwingender Staatsferne. Die Aufsicht über und Marktüberwachung von KI-Systemen im Bereich der Anwaltschaft sollte folglich dem von der BRAK geforderten unabhängigen Datenschutzbeauftragten für die Anwaltschaft zugewiesen werden. Dies gilt insbesondere dann, wenn sich die EU-Kommission, wozu sie unter den Voraussetzungen des Art. 7 KI-VO-E berechtigt wäre, entschließen sollte, Anhang III Nr. 8 KI-VO-E nicht allein auf Justizbehörden zu beschränken, sondern – wie die Überschrift der Nr. 8

[21] Weißbuch zur Künstlichen Intelligenz – ein europäisches Konzept für Exzellenz und Vertrauen, COM(2020) 65 final/2, Seiten 7 und 29.
[22] VO (EU) 2019/1020 über Marktüberwachung und die Konformität von Produkten.
[23] RL (EU) 2016/680.

„Rechtspflege und demokratische Prozesse“ bereits nahelegt – auf KI-Systeme aller an der Rechtspflege Beteiligten und damit auch die Anwaltschaft auszudehnen.[24] Eine entsprechende Einordnung besonders „gefahrgeneigter“ LegalTech-KI-Systeme als Hochrisiko-Systeme läge dabei insbesondere dann nahe, wenn diese von Anbietern eingesetzt werden, denen es an der Qualifikation zur Erbringung von Rechtsdienstleistungen mangelt.

4. Regulatory Sandboxes („KI-Reallabore“)

Zum Schutz des Mandatsgeheimnisses sollte in Artikel 53 Abs. 2 KI-VO-E schließlich vorgesehen werden, dass bei der Einrichtung von Reallaboren, die eine Verarbeitung von Mandatsinhalten zum Gegenstand haben, die anwaltliche Selbstverwaltung einzubeziehen ist. Gegenwärtig knüpft die in Artikel 53 Abs. 2 KI-VO-E vorgesehene Verpflichtung zur Einbindung weiterer Behörden an deren Aufsichtsbefugnis über die KI-Systeme an. Damit wäre, bliebe der Selbstverwaltung die Aufsicht verwehrt, die rechtsstaatlich gebotene Einbindung der anwaltlichen Selbstverwaltung in Fällen der Verwendung von mandatsbezogenen Daten in KI-Systemen nicht gewährleistet.

* * *

[24] Hierzu vgl. auch Kau, Der Aufstieg von Artificial Intelligence (AI) und seine Auswirkungen auf die Rechtsanwaltschaft, CR 7/2021, S. 498 ff., 503.