§ 4. Hochrisiko-KI-Systeme: Risikobasierter Ansatz*

A. Grundkonzept des risikobasierten Ansatzes

I. Allgemeine Risiken beim Einsatz von KI-Systemen

Die **Entscheidungspfade,** auf denen KI-Systeme wandeln, sind häufig **verschlungen.** 1
Wer solche Anwendungen nutzt, sieht sich deshalb oftmals mit einem Ergebnis konfrontiert, dessen Zustandekommen er nicht versteht. Betroffene beschleicht dann mitunter die Sorge, unbemerkt Opfer diskriminierender Entscheidungen zu werden oder „ex machina" unrechtmäßigen Maßnahmen ausgeliefert zu sein. Nicht zuletzt aus diesen Gründen ist vielen Menschen KI – allen Lobpreisungen in Politik und Digitalwirtschaft zum Trotz – unheimlich.

Diese **Ängste und Bedenken** sind nicht gänzlich unbegründet. Denn die Entschei- 2
dungsprozesse eines KI-Systems basieren auf **Wertentscheidungen,** welche die Programmierer ihm eingeschrieben haben. KI-Systeme übernehmen bestehende Stereotype und Alltagsdiskriminierungen, die in den ihnen eingefütterten Trainingsdaten stecken. Gleichzeitig besteht das Risiko, dass sie selbst neue **diskriminierende Muster** etablieren oder unterstützen.[1] Sie sind somit weder wertfrei noch neutral.

Eine opake Funktionsweise ist kein Alleinstellungsmerkmal Künstlicher Intelligenz. Die- 3
se Eigenart teilen KI-Produkte vielmehr mit anderen **Risikotechnologien**[2], etwa der Nanotechnologie[3], der Humangenetik oder der Arzneimittelentwicklung[4].[5] Auch ihr Einsatz baut auf **Hypothesen und Prognosen** auf, die dem Gesetzgeber besonderes Fingerspitzengefühl abverlangen. Und dennoch: Viele KI-Systeme zeichnen sich durch eine zusätzliche Besonderheit[6] aus: Sie entwickeln sich (dank der Techniken maschinellen Lernens) selbständig weiter. Ihre Ergebnisse lassen sich daher häufig nur bedingt vorhersagen und mögliche Entwicklungen nicht exakt antizipieren.

Diesen **emergenten Risiken** neuer Technologien sollte der Gesetzgeber einerseits durch 4
klare normative Rahmenbedingungen wirksam **Einhalt** gebieten. Andererseits ist er gehalten, die **(Weiter-)Entwicklung** Künstlicher Intelligenz nicht zu stark zu bremsen, sondern zu **fördern.** Denn nur wenn KI-Unternehmen hinreichend Handlungsfreiheit genießen, um innovative marktreife Produkte zu entwickeln, bleibt die Digitalwirtschaft der Union global wettbewerbsfähig. An welchen Stellschrauben der Normgeber mit Blick auf die damit verbundenen Risiken für das ökonomisch florierende KI-Ökosystem drehen sollte, gehört zu den schwierigen Fragen, die er bei der Regulierung lernender Systeme beantworten muss. Denn die Landschaft der Algorithmen ist vielfältig, dynamisch und nur schwer überschaubar.

---

* Der Beitrag ist unter Mitarbeit der wissenschaftlichen Mitarbeiterin Katja Neumann und der Forschungsreferentin Christine Wiesehöfer entstanden. Besonderer Dank gilt auch Levke Burfeind, Martin Feldhaus sowie Mert Dinçer für ihre sehr gute Unterstützung.

[1] Vgl. bspw. Müller EuZ 2022, A1 (A2).

[2] Zu Technik- und Risikoregulierung vgl. bspw. Steege NZV 2022, 257.

[3] Vgl. bspw. zum Stand vor der Aktualisierung der REACH-VO im Jahre 2020 Schulz/Föhl ZUR 2018, 155; zum risikobasierten Ansatz im Rahmen der neuen Chemikalienstrategie der EU vgl. Hussing/von der Heyden ZRP 2022, 231 (233 f.).

[4] Vgl. bspw. Schauer PharmR 2022, 482.

[5] Zum Recht der Risikoregulierung als Vergleichsfolie s. bspw. Martini, Blackbox Algorithmus, 2019, 114 ff.

[6] Zu den Besonderheiten und Herausforderungen bspw. Zech ZfPW 2019, 198.

II. Die Entwicklung des risikobasierten Ansatzes in der EU-Regulierung

5 Um einen sachgerechten Interessenausgleich zwischen Grundrechtsschutz und Innovationsoffenheit herzustellen, wählt die KI-VO einen **risikobasierten Ansatz:** Er passt die **Regulierungsintensität** an das Risiko an, das von der konkreten Anwendung ausgeht. Je größer und wahrscheinlicher ein drohender Schaden, desto enger ist das Normenkorsett, in das er sie presst.[7] Das Konzept des risikobasierten Ansatzes ist **keine Neuschöpfung der KI-VO.** Es findet sich – in unterschiedlicher Spielart bzw. als Ausprägung verschiedener Regulierungsmodelle – bereits an **zahlreichen Stellen der Rechtsordnung.** So sind bspw. dem Produktsicherheitsrecht risikogestufte Pflichten nicht unbekannt: Die Medizinprodukte-VO (VO (EU) 2017/745) stellt je nach Produktrisiko differenzierte Anforderungen bei der Konformitätsbewertung.[8] In der Marktüberwachungsverordnung (VO (EU) 2019/1020) steuert der risikobasierte Ansatz den Entscheidungsprozess der Marktüberwachungsbehörden, „welche Arten von Produkten in welchem Umfang welchen Überprüfungen" standhalten müssen (Art. 11 Abs. 3 UAbs. 2 VO (EU) 2019/1020). Das Konzept findet seinen Niederschlag aber auch in gänzlich anderen Rechtsgebieten, so ua etwa in den Vorschriften zur Bekämpfung von Geldwäsche und Terrorismusfinanzierung (vgl. in Deutschland § 3a GwG).[9]

1. Der risikobasierte Ansatz als neues Leitkonzept für das EU-Digital-Regulierungspaket und völkerrechtliche Regulierungsansätze

6 Der risikobasierte Ansatz prägt nicht nur überkommene Rechtsmaterien, sondern durchdringt auch das EU-Digital-Regulierungspaket insgesamt in nachhaltiger Weise. So kommt er nicht zuletzt im Entwurf des **Digital Services Act** (DSA-E)[10] zum Tragen. Einige Vorschriften gelten für alle Anbieter von Vermittlungsdiensten (Art. 10–13 DSA-E), andere nur für Hosting-Diensteanbieter (Art. 14 ff., 16 ff. DSA-E) und für sehr große Online-Plattformen (Art. 25 ff. DSA-E). Sehr große Unternehmen müssen mit Blick auf die erhöhten Risiken, die von ihrem Geschäftsbetrieb ausgehen, ein umfangreicheres Pflichtprogramm befolgen als kleinere (idS bspw. Erwgr. Nr. 43 DSA-E).[11] Die Union baut den risikobasierten Ansatz damit zu einem Grundpfeiler ihres Normgebäudes für neue digitale Technologien aus. Aber auch **völkerrechtlich** setzt sich das Konzept als Regulierungs-

---

[7] Gutachten der Datenethikkommission, 2019, 25, abrufbar unter: https://www.bmjv.de/SharedDocs/Downloads/DE/Themen/Fokusthemen/Gutachten_DEK_DE.html;jsessionid=FF71C19934371EB93FE4A14E4C67E962.1_cid334?nn=11678504 (zuletzt aufgerufen am 4.10.2022).

[8] Dauses/Ludwigs EU-WirtschaftsR-HdB/Langner/Klindt/Schucht C. VI. Rn. 140 ff.

[9] Der Ansatz basiert insoweit auf einer Empfehlung der Financial Action Task Force (FATF) in Recommendations, International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation, 2012–2022. Sie fand in die Richtlinie (EU) 2015/849 des Europäischen Parlaments und des Rates vom 20.5.2015 zur Verhinderung der Nutzung des Finanzsystems zum Zwecke der Geldwäsche und der Terrorismusfinanzierung, zur Änderung der Verordnung (EU) Nr. 648/2012 des Europäischen Parlaments und des Rates und zur Aufhebung der Richtlinie 2005/60/EG des Europäischen Parlaments und des Rates und der Richtlinie 2006/70/EG der Kommission Eingang, vgl. Erwgr. Nr. 22 RL (EU) 2015/849; ausführlich dazu BeckOK GwG/Müller GwG § 3a Rn. 1 ff. Die Intensität der Maßnahmen bzw. Sorgfaltspflichten, die die zuständigen Stellen ergreifen bzw. die Verpflichteten walten lassen müssen, um Geldwäsche und Terrorismusfinanzierung zu verhindern bzw. zu bekämpfen, richtet sich nach den Risiken des konkreten Lebenssachverhalts.

[10] COM(2020) 825 final.

[11] Sehr großen Online-Plattformen (Art. 25 DSA-E) trägt der DSA insbes. auf, ihre Tätigkeiten in Hinblick auf ihre systemischen Risiken auszuwerten und entsprechende Maßnahmen einzuleiten, um jene abzuschwächen, vgl. insbes. Abschnitt 4 DSA-E, Art. 25 ff. DSA-E, Erwgr. Nr. 46 ff. DSA-E. Die Anforderungen an die Risikoeinschätzungen in den Art. 26, 27 DSA-E ähneln dabei dem für Hochrisiko-KI-Systeme geforderten Risikomanagement des Art. 9 KI-VO-E. De Gregorio und Dunn stufen den risikobasierten Ansatz im DSA-E als einen „hybriden" Ansatz zwischen dem der VO (EU) 2016/679 („bottom-up") und dem des KI-VO-E („top-down") ein (vgl. Gregorio/Dunn Common Market Law Review 2022, 437 (488)).

modell für Künstliche Intelligenz (womöglich) durch: Das sog. **Ad Hoc Committee on Artificial Intelligence** (CAHAI) des Europarats schlägt als Schlüsselelement eines völkerrechtlich bindenden[12] „Rechtsrahmens für die Entwicklung, den Entwurf und die Anwendung künstlicher Intelligenz auf der Grundlage der Standards des Europarats zu Menschenrechten, Demokratie und Rechtsstaatlichkeit"[13] einen risikobasierten Ansatz (Nr. 18–21 CAHAI) vor, der in seiner (noch groben) Zielrichtung der Risikoeinteilung des KI-VO-E ähnelt.[14]

2. Lehren aus der Erfahrung mit der DS-GVO

Auch die DS-GVO **(VO (EU) 2016/679)**[15] als datenschutzrechtlicher Grundbaustein der KI-Regulierung hat den risikobasierten Ansatz zumindest **teilweise in ihre dogmatische Grundstruktur** eingeflochten.[16] Er zielt dort darauf, Instrumente des Risikomanagements zu nutzen, um sicherzustellen, dass die Vorschriften besser Beachtung finden.[17] Der Ansatz steuert die Intensität der Compliance-Maßnahmen[18], die Verantwortliche – je nach Risiko der Datenverarbeitung für Grundfreiheiten und Grundrechte natürlicher Personen, insbes. deren Recht auf Schutz personenbezogener Daten (vgl. Art. 1 Abs. 2 DS-GVO) – erfüllen müssen. Manche ihrer Pflichten bestehen nur bei **hohem Risiko,** etwa die Datenschutz-Folgenabschätzung des Art. 35 DS-GVO.[19] Andere Pflichten entfallen bei **geringem Risiko,** bspw. die Benachrichtigungspflicht aus Art. 34 DS-GVO oder die Verpflichtung, ein Verzeichnis der Verarbeitungstätigkeiten zu führen (Art. 30 Abs. 5 DS-GVO). Der regulatorische Grundgedanke des Ansatzes scheint auch in **Art. 24 Abs. 1 DS-GVO** und **Art. 25 Abs. 1 DS-GVO** sehr deutlich auf: Die Vorschriften zum Pflichtenkanon des Verantwortlichen und zu „Data Protection by Design" sowie „by Default" knüpfen ihr 7

[12] Breuer, The Council of Europe as an AI Standard Setter 2022, https://verfassungsblog.de/the-council-of-europe-as-an-ai-standard-setter/ (zuletzt aufgerufen am 4.10.2022).

[13] Ad hoc Committee on Artificial Intelligence (CAHAI), Possible elements of a legal framework on artificial intelligence, based on the Council of Europe's standards on human rights, democracy and the rule of law, CM(2021)173-add.

[14] Das CAHAI schlägt ebenfalls eine Risikoklassifizierung vor (bspw. anhand der Kategorien „niedriges Risiko", „hohes Risiko", „unannehmbares Risiko"), worauf ggf. ein „Human Rights, Democracy and Rule of Law Impact Assessment" (HUDERIA) folgen muss, vgl. CAHAI CM(2021)173-add, Ziff. 19. Ebenso zieht das CAHAI ein (Teil-)Verbot oder Moratorium für spezifische Systeme in Betracht, insoweit zählt es beispielhaft die biometrische Identifizierung und Kategorisierung sowie bestimmte Sozialkreditsysteme auf (vgl. CAHAI CM(2021)173-add, Ziff. 21). Ein detaillierter Vergleich zwischen dem CAHAI-Vorschlag und dem KI-VO-E findet sich bei Breuer, The Council of Europe as an AI Standard Setter 2022, abrufbar unter: https://verfassungsblog.de/the-council-of-europe-as-an-ai-standard-setter/ (zuletzt aufgerufen am 4.10.2022).

[15] Ausf. zu ihrem risikobasierten Ansatz bspw. Schröder ZD 2019, 503.

[16] Schon vor dem Inkrafttreten der DS-GVO hatte die Union eine erste Spielart eines „risikobasierten Ansatzes" im Datenschutzrecht in der vorangehenden Richtlinie zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (RL 95/46/EG [Datenschutz-RL]) etabliert – insbes. in den Vorschriften zur Sicherheit der Verarbeitung (Art. 17 Datenschutz-RL) und zur Vorabkontrolle (Art. 20 Datenschutz-RL), aber auch in der Norm zur Verarbeitung besonderer Kategorien personenbezogener Daten (Art. 8 Datenschutz-RL); s. Artikel-29-Datenschutzgruppe, Statement on the role of a risk-based approach in data protection legal frameworks (WP (218) 2014, 2). Dennoch war damals noch keine Rede von einem risikobasierten Ansatz als Konzept. Seine erste Erwähnung im Datenschutzrecht fand er erst zu einem deutlich späteren Zeitpunkt, insbes. in einer Stellungnahme des Information and Privacy Commissioners Ontario, Canada im Jahre 2010 (auf die die Union allerdings nie verwies); Schröder ZD 2019, 503 (503).

[17] Gellert Journal of Ethics and Legal Technologies 2021, 15 (27).

[18] „So, contrary to the GDPR where the risk-based approach serves mainly to determine the intensity of compliance measures, the risk-based approach in the AIA has a much more substantive scope since it determines what gets regulated in the first place, with the risk that some AI systems are unduly categorised as non-high risk", Gellert Journal of Ethics and Legal Technologies 2021, 15 (21).

[19] Zur Datenschutz-Folgenabschätzung beim Einsatz Künstlicher Intelligenz vgl. bspw. Schürmann ZD 2022, 316.

Pflichtenniveau ausdrücklich an die Eintrittswahrscheinlichkeit und die Schwere der Risiken an.[20]

8 Der risikobasierte Ansatz der DS-GVO stieß allerdings auch auf **Skepsis.** Insbes. beschwor er die Befürchtung herauf, einem „‚US-amerikanischen', schadensbasierten Schutz" den Boden zu bereiten, der dem auf den EU-Grundrechten basierenden Charakter des Datenschutzes direkt zuwiderlaufe und ein niedrigeres Schutzniveau etabliere.[21] Diese Einschätzung überzeugt in dieser apodiktischen Strenge nicht. Denn es ist nicht nur regulatorisch sachgerecht, sondern auch mit Blick auf die Berufsfreiheit und die unternehmerische Freiheit der Betreiber (Art. 15, 16 GRCh) geboten, das Maß der Pflichten an der (potenziellen) Schadenshöhe auszurichten. Berechtigt ist aber ein anderer Kritikpunkt: Der risikobasierte Ansatz, wie ihn die DS-GVO ausgeformt hat, geht für die Rechtsunterworfenen mit nicht unerheblichen **Rechtsunsicherheiten** einher. Der Verantwortliche muss die risikorelevanten Umstände auf der Grundlage des gesetzlich vorgegebenen Kategorienrasters selbst einschätzen, um herauszufinden, welche (sanktionsbewehrten) Pflichten er erfüllen muss. Das Konzept knüpft damit an den Umfang des Risikos Rechtsfolgen, die nicht vollumfänglich in voraussehbarer Weise gesetzlich ausdifferenziert sind. So muss der Verantwortliche insbes. zentrale, aus Art. 24, 25 DS-GVO erwachsende Pflichten zur Technikgestaltung und zu datenschutzfreundlichen Voreinstellungen zumindest in Teilen aus einer – notwendig **wertungsbehafteten – Risikoanalyse** selbst ableiten.

9 In der Gesamtschau präsentiert sich der risikobasierte Ansatz der DS-GVO mehr als **zartes Pflänzchen** denn als ein ausgewachsenes Konzept: Statt das Pflichtenniveau durchgängig – etwa im Hinblick auf den Verarbeitungskontext – nach unterschiedlichen Risikogruppen abzustufen, unterwirft die Verordnung den Bäcker, den Metzger und das kleine Softwareunternehmen genauso wie Google, Facebook und Co. im Grundsatz dem gleichen normativen Pflichtenheft. Insbes. unterliegen sämtliche Verantwortliche dem **Erlaubnisvorbehalt** (Art. 6 Abs. 1 DS-GVO) und haben weitgehend die gleichen, anbieterunabhängigen **Betroffenenrechte** zu gewährleisten.

10 Diese Weichenstellung des Unionsgesetzgebers, Verarbeitungen im Grundsatz gleich zu behandeln, kann im Ergebnis eine **Ungleichbehandlung der Pflichtunterworfenen** nach sich ziehen. **Kleinere Unternehmen** treffen die Vorgaben in einem **„One-Size-Fits-All-Konzept"** nämlich proportional **wirtschaftlich spürbarer** als große Unternehmen. Für kleine Unternehmen ist es bspw. ungleich aufwendiger, Datenschutzerklärungen anzupassen, und ihren Geschäftsbetrieb auf neue Vorgaben auszurichten. Große Unternehmen, die auf die Expertise einer eigenen Rechtsabteilung zurückgreifen können, können diesen – im Verhältnis zu ihrem Gesamtumsatz geringen – Aufwand leichter stemmen. Die wirtschaftlichen Auswirkungen der DS-GVO nehmen mit der Größe des jeweiligen IT-Unternehmens mithin tendenziell ab. Die Anpassungsprozesse, welche ihr Datenschutzregime Verantwortlichen abverlangt, spielen etablierten Unternehmen mit gefestigter Marktposition dadurch im Grundsatz in die Hände. Ökonomen der Universität Oxford haben das (jedenfalls für die IT-Branche) in einer Untersuchung empirisch untermauert: Kleine IT-Unternehmen büßten im Gefolge der DS-GVO schätzungsweise rund 2,1 % ihrer Umsätze und 12,1 % ihrer Gewinne ein. Bei großen IT-Konzernen konn-

[20] Ob die Datenverarbeitung ein normales oder ein hohes Risiko auslöst, bemisst sich dabei nach einer objektiven Betrachtung (Erwgr. Nr. 76 S. 2 DS-GVO). Die DS-GVO definiert den Terminus „Risiko" zwar nicht legal. In der Sache unterfallen ihm aber nicht nur materielle Nachteile, sondern – wie Erwgr. Nr. 75 S. 1 DS-GVO (und mittelbar auch Art. 82 Abs. 1 DS-GVO) zu entnehmen ist – jegliche Schadensformen (physische, materielle oder immaterielle Schäden). Vgl. auch Ehmann/Selmayr/Heberlein DS-GVO Art. 5 Rn. 30. Die sich daran orientierenden Pflichten des Verantwortlichen dürfen zugleich nicht unverhältnismäßig sein (Art. 52 Abs. 1 S. 2 GRCh). Auch Art. 24 Abs. 2 DS-GVO fordert aus gutem Grund eine Abwägung zwischen dem „Gefährdungsgrad der Risiken" und der „mit [den] Schutzmaßnahmen verbundene[n] Belastung", Paal/Pauly/Martini DS-GVO/BDSG Art. 24 Rn. 11.

[21] „The main fears and arguments against it argued that it would lead to a ‚US' harms-based type of protection, which goes directly counter the EU fundamental rights-based nature of data protection", Gellert, The Risk-Based Approach to Data Protection 2020, 2.

ten die Forscher nicht in gleichem Maße negative Auswirkungen nachweisen: Sie büßten im Schnitt nur 0,7% ihrer Umsätze und 4,6% ihrer Gewinne ein.[22] Faktisch verteilt der Unionsgesetzgeber die **Last, das Datenschutzrecht anzuwenden und umzusetzen, asymmetrisch.** Die DS-GVO trifft die Akteure, die sie erreichen sollte, um die Rechte und Freiheiten natürlicher Personen effektiv zu schützen, dadurch gerade **nicht zielgenau.** Einem stringent durchgehaltenen risikobasierten Ansatz entspräche es, die **regulatorischen Anforderungen** stärker an die jeweiligen Adressaten und das **kontextspezifische Gefährdungspotenzial** einer Verarbeitung anzupassen.[23] Der KI-VO-E will das besser machen. Er versucht, aus den Optimierungsbedarfen der DS-GVO zu lernen, und den risikobasierten Ansatz konsequenter umzusetzen.[24]

B. Die Risikopyramide des KI-VO-E

I. Grundkonzept

Bereits in ihrem Weißbuch zur Künstlichen Intelligenz (2020) hat die Kommission ein klares **Bekenntnis** zu einem stringenten risikobasierten Ansatz abgegeben: „[D]er Gesetzgeber schreitet nur in solchen konkreten Situationen ein, in denen ein berechtigter Anlass für Bedenken besteht oder in denen vernünftigerweise davon ausgegangen werden kann, dass solche Bedenken in naher Zukunft auftreten werden."[25] Die Normen der neuen Verordnung sollen sich mithin an die Intensität und den Umfang der jeweiligen Risiken der entsprechenden KI-Systeme anpassen.[26] Mit dieser Konzeption stuft die Kommission den risikobasierten Ansatz als geeignet ein, „um zu vermeiden, dass [der neue Rechtsrahmen] insbesondere für KMU einen unverhältnismäßigen Aufwand verursacht."[27] 11

Während die DS-GVO den risikobasierten Ansatz vor allem als Instrument versteht, um abstrakte horizontale Regelungen auf die Risikosituation des Einzelfalls anzupassen und auf dieser Grundlage die Verantwortlichen konkrete Handlungspflichten ableiten zu lassen,[28] nutzt der KI-VO-E die Risikoeinstufung, um das **Pflichtenniveau** schon auf **normativer Ebene** auszudifferenzieren.[29] Das Regulierungskonzept für Künstliche Intelligenz knüpft sein Pflichtenregime unmittelbar an die eingesetzte Technologie an. Das wirkt sich auch auf die Regelungstechnik aus: Während der Ansatz der DS-GVO in der Tendenz prozedural, also auf die Art und Weise der Verarbeitung, ausgerichtet ist, um das Risiko zu bestimmen, folgt der KI-VO-E stärker der **produktsicherheitsrechtlichen Regulierungsphilosophie.** 12

Ein Steuerungsansatz, der unmittelbar an technische Grundlagen eines Produkts anknüpft, um die regulativen Maßnahmen **zielgenauer** auf die einzelnen KI-Systeme auszurichten, muss hinreichend detailliert bestimmen, welche Systeme in welche Kategorie des Regulierungsregimes fallen. Diskretionäre Entscheidungsspielräume (wie im Rahmen der DS-GVO) wären insoweit wenig sinnstiftend. Vielmehr muss gesetzlich klar umrissen sein, welche Anwendungen der Sekundärrechtsakt tatbestandlich erfasst und welche Anforde- 13

[22] Chen/Frey/Presidente, Privacy Regulation and Firm Performance: Estimating the GDPR Effect Globally 2022, 25, abrufbar unter: https://www.oxfordmartin.ox.ac.uk/downloads/Privacy-Regulation-and-Firm-Performance-Giorgio-WP-Upload-2022-1.pdf (zuletzt aufgerufen am 4.10.2022).

[23] Vgl. auch Martini, Grundlinien eines Kontrollsystems für algorithmenbasierte Entscheidungsprozesse, 2019, 41 ff., abrufbar unter: https://www.vzbv.de/sites/default/files/downloads/2019/07/17/martini_-_adm-kontrollsystem_2.pdf (zuletzt aufgerufen am 4.10.2022); Martini/Hohmann NJW 2020, 3573 (3578).

[24] Vgl. insbes. Erwgr. Nr. 14 S. 1 KI-VO-E.

[25] Begr. Nr. 1.1 KI-VO-E.

[26] Erwgr. Nr. 14 S. 2 KI-VO-E; die Art. 53 ff. KI-VO-E treffen besondere Vorgaben für KMU.

[27] COM(2020) 65 final, 20.

[28] Vgl. Artikel-29-Datenschutzgruppe, Statement on the role of a risk-based approach in data protection legal frameworks (WP (218) 2014, 2); Gellert Journal of Ethics and Legal Technologies 2021, 15 (20).

[29] Gellert Journal of Ethics and Legal Technologies 2021, 15 (26).

rungen diejenigen konkret erfüllen müssen, die ein solches System anbieten, herstellen oder nutzen. **Unterschiedliche Risikoklassen** – wie sie der KI-VO-E vorgibt – können diese Stufungen im Grundsatz detailscharf herausarbeiten und bestimmen.

II. Das Stufensystem des KI-VO-E im Überblick

14 Der KI-VO-E unterscheidet zwischen **vier verschiedenen Risikostufen.** Diese steigern sich von Anwendungen, die kein bzw. nur ein geringes Risiko bergen, über sog. Hochrisiko-KI-Systeme, bis hin zu Systemen, von denen ein nicht hinnehmbares Risiko ausgeht. Zusammen formen sie eine **Regulierungspyramide.**

15 Eine **Legaldefinition** des Begriffs „Risiko" kennt der KI-VO-E – ebenso wie auch schon die DS-GVO – nicht. Eine solche könnte ergänzend dazu beitragen, die Stufenzuordnung zu vereinfachen.[30] Der Ausschuss für Binnenmarkt und Verbraucherschutz („IMCO"-Ausschuss) sowie der Ausschuss für bürgerliche Freiheiten, Justiz und Inneres („LIBE"-Ausschuss) des Europäischen Parlaments schlagen daher in einem Berichtsentwurf vor, eine Begriffsdefinition in den Verordnungstext zu integrieren. „Risiko" soll – entsprechend dem tradierten Begriffsverständnis[31] – „die Kombination aus der Wahrscheinlichkeit des Auftretens einer Gefahr, die einen Schaden verursacht, und dem Schweregrad dieses Schadens" bezeichnen.[32]

16 Auf der höchsten Risikostufe der Regulierungspyramide stehen solche Systeme, von denen a priori ein nicht tragbares Risiko für natürliche Personen ausgeht **(Art. 5 KI-VO-E).** Für sie gilt als Ultima Ratio ein **Verbot** (→ Rn. 21 ff.).

17 Weniger intensiv reguliert, dafür mit umso mehr Vorschriften normativ eingehegt sind – auf der **zweithöchsten Stufe** der Risikopyramide – die sog. **Hochrisiko-KI-Systeme (Titel III, Art. 6 ff. KI-VO-E).** Was genau ein Hochrisiko-System auszeichnet, definiert der Unionsgesetzgeber nicht abstrakt. Er konkretisiert dies vielmehr im Wege von Listen. Ihre Grobsortierung knüpft an Einsatzgebiete der Systeme an. **Zwei Kategorien** von Hochrisiko-KI-Systemen (Art. 6 KI-VO-E) etabliert der Gesetzgeber: Die erste Kategorie bilden Anwendungen, die ein Produkt oder eine Sicherheitskomponente eines Produkts[33] repräsentieren, das bereits unter die existierenden EU-**Harmonisierungsvorschriften** fällt, die Anhang II KI-VO-E auflistet und bereits einer rechtlich geforderten **Konformitätsbewertung** durch Dritte unterliegt (Art. 6 Abs. 1 KI-VO-E; → Rn. 41 ff.). Die zweite Kategorie erfasst **eigenständige Systeme,** die aufgrund der Art ihres Einsatzgebietes nach der Wertung des KI-VO-E ebenfalls ein hohes Risiko bergen (Art. 6 Abs. 2 KI-VO-E; → Rn. 50 ff.).

18 In die **dritte Stufe** der Risikopyramide ordnet der KI-VO-E KI-Systeme mit **geringen Risiken** ein, insbes. Chatbots sowie Anwendungen, die Bild-, Ton- bzw. Videoinhalte erzeugen und manipulieren (sog. „Deepfakes") – Art. 52 KI-VO-E. Sie müssen besondere **Transparenz- bzw. Offenlegungsanforderungen**[34] erfüllen: Für die Anwender muss insbes. erkennbar sein, dass sie mit solchen Systemen konfrontiert sind.[35]

---

[30] Begr. Nr. 3.1 KI-VO-E.

[31] Zum Begriff des Risikos in der DS-GVO vgl. bspw. Paal/Pauly/Martini DS-GVO/BDSG Art. 35 Rn. 15a ff.

[32] „'[R]isk' means the combination of the probability of an occurrence of a hazard causing harm and the degree of severity of that harm", Draft Report on the proposal for a regulation of the European Parliament and of the Council on harmonised rules on Artificial Intelligence (Artificial Intelligence Act), PE731.563, 2021/0106(COD), 2022, Änderungsantrag Nr. 73.

[33] „Sicherheitskomponente eines Produkts oder Systems" sind Bestandteile, die eine Sicherheitsfunktion für das Produkt oder das System erfüllen oder deren Ausfall bzw. Störung die Gesundheit und Sicherheit von Personen oder Sachen gefährdet (Art. 3 Nr. 14 KI-VO-E).

[34] → Rn. 128 ff.

[35] Für Deepfakes, die unter die Meinungs-, Kunst- und Wissenschaftsfreiheit fallen, formuliert der KI-VO-E eine Ausnahme (vgl. Art. 52 Abs. 3 UAbs. 2 KI-VO-E) – ebenso für alle sensiblen Systeme des Art. 52 KI-VO-E sub specie solcher Anwendungen, die für die Strafverfolgung zugelassen sind (Art. 52 Abs. 1 S. 2, Abs. 2 S. 2, Abs. 3 UAbs. 2 KI-VO-E).

Den „großflächigen" Boden der Pyramide formen Anwendungen aus, die ein **Risiko im Einzelfall** bergen (→ Rn. 135 ff.). Die **unterste Risikostufe** erfasst somit im Grundsatz alle KI-Systeme. Sie spannt dadurch gleichsam ein **Auffangnetz** für Anwendungen auf, von denen grds. nur minimale Risiken ausgehen. Der Verordnungsentwurf hält für sie in **Art. 69 KI-VO-E** eine (etwas kryptische) Sonderregelung vor: Er möchte **Verhaltenskodizes** auf freiwilliger Basis fördern. 19

Den **Mitgliedstaaten** kommt nicht die Befugnis zu, die hierarchischen Einordnungen neu zu justieren bzw. anders zu bewerten: Sie sind an die Risikostufen gebunden, welche der Unionsgesetzgeber festlegt. Der Verordnungsentwurf belässt den Mitgliedstaaten bislang mithin nur sehr enge Regelungsspielräume.[36] Ordnet der KI-VO-E ein System in eine Risikostufe ein, heißt das jedoch nicht, dass auf es nur die Regelungen des jeweiligen Abschnitts des KI-VO-E zur Anwendung kommen. Rechtmäßigkeitsanforderungen können sich auch aus **anderen Rechtsakten** der Union oder der Mitgliedstaaten (zB der DS-GVO) ergeben (Erwgr. Nr. 41 KI-VO-E). Der KI-VO-E spart insbes. **Haftungsfragen** aus. Die Union möchte dafür in einem neuen Rechtsakt eine gesonderte Regelung treffen. Im Oktober 2022 hat die Kommission einen Richtlinienvorschlag vorgelegt.[37] Er soll denjenigen, der mit potenziell fehlerhaften Ergebnissen einer KI konfrontiert ist, vor der Beweisnot schützen, die ihre opake Entscheidungsstruktur mit sich bringt. Als legistisches Instrument greift der Rechtsakt auf eine Umkehr der Beweislast zurück. 20

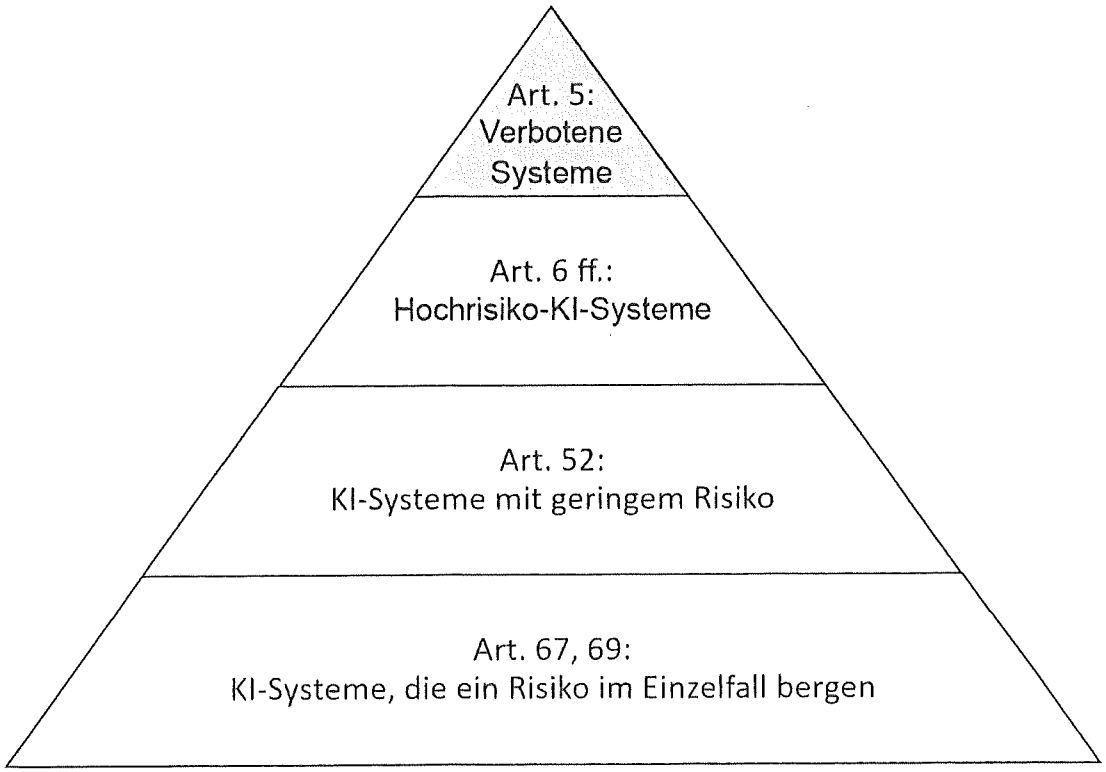

Abb. 1: Risikostufen für KI-Systeme (eigene Darstellung)

[36] Ausf. zu den Spielräumen vgl. bspw. Hornung DuD 2022, 561 (561 ff.).

[37] Vorschlag der Kommission für eine Richtlinie zur Anpassung der Vorschriften über außervertragliche zivilrechtliche Haftung an künstliche Intelligenz (Richtlinie über KI-Haftung), COM(2022) 496 final.

C. Verbotene KI-Systeme (Art. 5 KI-VO-E)

21 Systeme, die verboten sind, weil von ihnen ein untragbares Risiko ausgeht, bündelt der KI-VO-E in seinem **Art. 5.** Dessen kritische Schwelle überschreiten Anwendungen, wenn sie zentrale Leitideen und Grundwerte der Union, insbes. die Grundrechte, verletzen.[38]

22 Art. 5 KI-VO-E listet **vier verschiedene Kategorien** verbotener Praktiken auf: Systeme, die natürliche Personen durch **unterschwellige Beeinflussung** manipulieren bzw. ihre **Schwächen ausnutzen** und sie (psychisch oder physisch) **schädigen,** stuft die Kommission als mit der Werteordnung der Union prinzipiell unvereinbar ein (Art. 5 Abs. 1 Buchst. a–b KI-VO-E; → I., Rn. 23 ff.). Auch behördliche Systeme, die das Verhalten natürlicher Personen **bewerten** und auf dieser Grundlage Entscheidungen fällen (Sozialkredit-System[39]), untersagt der KI-VO-E grds. (Art. 5 Abs. 1 Buchst. c KI-VO-E; → II., Rn. 29 ff.). Der Unionsgesetzgeber bekennt sich überdies dazu, **biometrische Echtzeit-Fernidentifizierungssysteme,** die Strafverfolgung betreiben sollen, nicht in öffentlich zugänglichen Räumen (Erwgr. Nr. 8 f. KI-VO-E)[40] zuzulassen (Art. 5 Abs. 1 Buchst. d KI-VO-E; III.; → Rn. 32 ff.). In den ersten drei Fällen (Buchst. a bis c) unterbindet der KI-VO-E das Inverkehrbringen, die Inbetriebnahme *und* die Verwendung entsprechender Systeme, in der vierten Kategorie (Buchst. d) hingegen nur die Verwendung. Solche KI-Anwendungen zu *entwickeln,* ist demgegenüber nicht verboten. KI-Systeme, die richterliche Urteile automatisiert treffen (sog. **Robo-Richter**), erfasst Art. 5 KI-VO-E gar nicht. Insoweit entpuppt sich die Vorschrift als lückenhaft und sollte eine Ergänzung erfahren.[41]

I. Unterschwellige Beeinflussung (Art. 5 Abs. 1 Buchst. a KI-VO-E)

23 Art. 5 Abs. 1 Buchst. a KI-VO-E nimmt KI-Systeme in das regulatorische Fadenkreuz, die „Techniken der unterschwelligen Beeinflussung" einsetzen. Zielen die Anwendungen darauf, das **menschliche Verhalten** zu **manipulieren,** gehen davon Gefahren für die Entscheidungsautonomie des Einzelnen aus, denen der KI-VO-E mit der scharfen Maßnahme eines Verbots entgegentritt – allerdings nicht generell, sondern nur, wenn das System einer Person einen physischen oder psychischen Schaden zufügt oder zufügen kann.[42]

24 **„Unterschwellig"** beeinflussen Techniken dann, wenn für die betroffene Person die Manipulation nicht erkennbar ist und sie ihr Verhalten in eine Richtung lenken, die mit ihren Präferenzen an sich nicht übereinstimmt. Der Tatbestand ist damit **sehr weit** gefasst.

25 Aber nicht jegliche Form verbraucherschädigender Verhaltenssteuerung fällt unter das Verbot. Erforderlich ist eine **wesentliche Manipulation.** An welchen Kriterien sich die Wesentlichkeit festmacht, lässt der Wortlaut indes offen.

26 Der Tatbestand greift auch nicht schon immer dann, wenn eine Person das Verhalten einer anderen im Ergebnis steuert. Die Manipulation muss vielmehr zielgerichtet erfolgen. An die **Manipulationsabsicht**[43] („um das Verhalten [...] zu beeinflussen") legt der KI-VO-E keine strengen Maßstäbe an. Erforderlich ist aber eine klare Zurechenbarkeit. Wenn die Einflussnahme auf Umständen basiert, die nicht Bestandteil des Systems sind und die der Anbieter oder Nutzer nicht beeinflussen kann, greift das Verbot bspw. nicht

[38] Begr. Nr. 5.2.2 KI-VO-E.
[39] Zur Frage, ob ein Social-Scoring-System öffentlicher Stellen unter bestimmten Voraussetzungen weiterhin zulässig sein könnte, vgl. bspw. Bomhard/Merkle RDi 2021, 276 (279).
[40] Erwgr. Nr. 8 f. KI-VO-E.
[41] IdS auch die Stellungnahme des Deutschen Anwaltvereins Nr. 57/2021, 11.
[42] Vgl. den eindeutigen Wortlaut des Art. 5 Abs. 1 Buchst. a KI-VO-E.
[43] Die französische Ratspräsidentschaft hat in ihrem Kompromisstext im Juni 2022 empfohlen, dass es keinesfalls mehr einer Absicht bedarf, den Schaden hervorzurufen, vielmehr solle es ausreichen, dass ein solcher auf den „manipulativen oder ausbeuterischen" Praktiken basiert; vgl. Erwgr. Nr. 16, 14 Ratsdok. 10069/22.

(Erwgr. Nr. 16 S. 4 KI-VO-E). Der KI-VO-E setzt voraus, dass die Einflussnahme in der Kontrollmacht des Anbieters liegt.

Es genügt auch nicht jeglicher Schaden, um die Verbotsschwelle auszulösen; erforderlich ist vielmehr ein **physischer oder psychischer Schaden.** Bloße Vermögensschäden, insbes. nachteilige Vertragsabschlüsse, genügen mithin nicht. Ebenso wenig schützt der Tatbestand die reine Entscheidungsautonomie, also die Freiheit, Entscheidungen unbeeinflusst von äußeren Lenkungsfaktoren zu treffen.[44] Aus diesen Gründen erfasst Art. 5 Abs. 1 Buchst. a KI-VO-E verbraucherschädigende Phänomene, wie bspw. **Dark Patterns** und Verhaltensbeeinflussung im Gefolge **personalisierter Werbung,** regelmäßig nicht.[45] 27

II. Ausnutzen der Schwäche oder Schutzbedürftigkeit (Art. 5 Abs. 1 Buchst. b KI-VO-E)

Ebenso wie Art. 5 Abs. 1 Buchst. a KI-VO-E soll der Verbotstatbestand des Art. 5 Abs. 1 Buchst. b KI-VO-E das „Selbstbestimmungsrecht der EU-Bürger als Fundament unserer Werteordnung [...] schützen."[46] Er ist (noch) weiter gefasst als Buchst. a. Denn er knüpft nicht daran an, dass ein System eine Person unterschwellig beeinflusst. Er lässt vielmehr genügen, eine **Schwäche oder Schutzbedürftigkeit** auszunutzen, die aus dem **Alter** oder der **körperlichen oder geistigen Behinderung** von Personen erwächst.[47] Wie Buchst. a greift auch Art. 5 Abs. 1 Buchst. b KI-VO-E ausschließlich bei **physischen und psychischen Schäden.** Reine **Vermögensschäden** lässt er nicht ausreichen. Obgleich die ersten beiden Kategorien des Art. 5 KI-VO-E typische Manipulationspraktiken erfassen und dadurch auch die Bestimmungen der UGP-Richtlinie effektiv ergänzen könnten (die anders als Art. 5 Abs. 1 und 2 des KI-VO-E eine „Geschäftspraxis" voraussetzen), bleiben die Verbotstatbestände wegen der Anknüpfung an einen Schaden, der über einen Vermögensschaden hinausgeht,[48] in ihren Auswirkungen de facto stark limitiert. 28

III. Social Scoring (Art. 5 Abs. 1 Buchst. c KI-VO-E)

Auch „Social Scoring" via KI stellt sich der KI-VO-E mit einem Verbot entgegen (Art. 5 Abs. 1 Buchst. c KI-VO-E). Er nimmt damit solche Systeme ins Visier, die Behörden oder Dritte als Teil eines öffentlichen Auftrags einsetzen, um die **Vertrauenswürdigkeit** natürlicher Personen auf der Grundlage ihres **sozialen Verhaltens,** persönlicher Eigenschaften oder ihrer Persönlichkeitsmerkmale zu bewerten oder zu klassifizieren. Wenn die soziale Bewertung im Ergebnis dazu führt, die Person(en) schlechter zu stellen und/oder zu benachteiligen, sind solche Systeme unzulässig. Wie sich die Verknüpfung zwischen dem KI-System und der **Benachteiligung** oder **Schlechterstellung** im Detail darstellt, ist dabei nicht belanglos: Die Nachteile müssen entweder in einem **sozialen Zusammenhang** eintreten, der in keinem Kontext zu der ursprünglichen Datenerhebung steht (Art. 5 Abs. 1 Buchst. c lit. i KI-VO-E), oder sie müssen im Hinblick auf das soziale Verhalten ungerechtfertigt oder unverhältnismäßig sein (Art. 5 Abs. 1 Buchst. c lit. ii KI-VO-E)[49], damit der Verbotstatbestand das System erfasst. 29

---

[44] Krit. dazu Linardatos GPR 2022, 58 (60f.).

[45] AA wohl Ebert/Spiecker NVwZ 2021, 1188 (1189).

[46] Veale/Zuiderveen-Borgesius CRi 2021, 97 Rn. 15; nähere Darstellung bei Hacker European Law Journal 2021, 1 (27); Rostalski/Weiss ZfDR 2021, 329 (338).

[47] Auch in Buchst. b möchte die französische Ratspräsidentschaft Änderungen vornehmen und als mögliche Tatbestandsalternative noch hinzufügen, eine wirtschaftliche oder soziale Situation auszunutzen; vgl. Art. 5 Abs. 1 Buchst. b Ratsdok. 10069/22.

[48] Veale/Zuiderveen-Borgesius CRi 2021, 97 Rn. 15.

[49] Der DAV kritisiert insbes. die Begriffe dieser letzten Ausnahme. Er sieht die Gefahr, dass sie ein Einfallstor öffnen, das Verbot zu umgehen, Stellungnahme des Deutschen Anwaltvereins Nr. 57/2021, 9.

30 Das Verbot des Art. 5 Abs. 1 Buchst. c KI-VO-E adressiert bewusst nur **Behörden** und ihre Dienstleister, nicht aber private Wirtschaftsakteure, die Scoring-Systeme für ihre Zwecke einsetzen. Wirtschaftsauskunfteien dürfen diese Systeme daher weiterhin auf den Markt bringen bzw. verwenden. Wenn Private Social-Credit-Anwendungen einsetzen, sind allerdings auch Grundrechtsverletzungen durch **mittelbare Drittwirkungen** denkbar.[50] Auch aus diesem Grund votiert die slowenische Ratspräsidentschaft dafür, diese Eingrenzung des Tatbestandes aufzuweichen.[51]

31 Der KI-VO-E untersagt nur den Einsatz „über einen bestimmten Zeitraum" („over a certain period of time"). Er soll prima facie also grds. nicht den einmaligen[52], sondern lediglich den **wiederholten Einsatz** erfassen, der darauf gerichtet ist, Erkenntnisse über eine Beobachtungsperiode zu sammeln. Eindeutig ist dies aber nicht; auch eine einmalige Verwendung kann sich über einen bestimmten Zeitraum erstrecken – allerdings beträfe sie letztlich eher einen Zeitpunkt als einen Zeitraum. Um möglichen Unklarheiten und daraus erwachsenden Rechtsunsicherheiten vorzubeugen, sollte der Gesetzgeber den Tatbestand präzisieren.

IV. Systeme biometrischer Echtzeit-Fernidentifizierung (Art. 5 Abs. 1 Buchst. d KI-VO-E)

32 Die hohe gesellschaftliche Sensibilität, die biometrischen **Echtzeit-Fernidentifizierungssystemen** immanent ist,[53] sucht Art. 5 Abs. 1 Buchst. d KI-VO-E normativ einzufangen. Solche Systeme zeichnen sich dadurch aus, dass sie natürliche Personen ohne erhebliche zeitliche Verzögerung (Art. 3 Nr. 37 KI-VO-E) unter Rückgriff auf biometrische Daten durch einen Abgleich mit einer Referenzdatenbank eindeutig identifizieren (Art. 3 Nr. 36 KI-VO-E).[54] Da sie tief in die Grundrechte, insbes. das Grundrecht auf Schutz personenbezogener Daten und das Recht auf Achtung des Privatlebens (Art. 8 und 9 GRCh), hineinwirken, verbietet der Entwurf es, sie in **öffentlich zugänglichen Räumen** zu **Strafverfolgungszwecken** zu verwenden.

33 Dies gilt jedoch nicht absolut. Vielmehr lässt Art. 5 Abs. 1 Buchst. d KI-VO-E ihren Einsatz für spezifische Zielsetzungen zu. Die **Ausnahmetatbestände** sind aber an hohe Voraussetzungen geknüpft: Zulässig sind biometrische Fernidentifizierungssysteme bei der Suche nach vermissten Opfern (insbes. Kindern), um konkrete Gefahren für Leib und Leben oder einen Terroranschlag abzuwenden oder um die Verfolgung bestimmter Straftaten zu ermöglichen. Der Einsatz des Systems ist dann darüber hinaus durch **besondere Schutzmaßnahmen** zu flankieren und ua **zeitlich und räumlich zu begrenzen** (Art. 5 Abs. 2, Erwgr. Nr. 20 S. 2 KI-VO-E). Er unterliegt ferner einem **Genehmigungsvorbe-**

---

[50] Vgl. etwa Ebers/Hoch/Rosenkranz/Ruschemeier/Steinrötter RDi 2021, 528 (530). Einschlägig können dann aber die Regelungen für Hochrisiko-KI-Systeme aus Art. 6 Abs. 2 iVm Anhang III Nr. 5 Buchst. b sein.

[51] Die slowenische Ratspräsidentschaft will auch die Nutzung durch private Akteure umfasst sehen; Art. 5 Abs. 1 Buchst. c Ratsdok. 14278/21, Erwgr. Nr. 17 Ratsdok. 14278/21.

[52] Vgl. auch Linardatos GPR 2022, 58 (61).

[53] Zu dieser Sensibilität vgl. bspw. Hornung/Schindler DuD 2021, 515; Martini NVwZ-Extra 2/2022, 1; Schindler ZD-Aktuell 2021, 5221.

[54] Von dieser Definition möchte die französische Ratspräsidentschaft solche Systeme ausnehmen, „[...] deren einziger Zweck darin besteht, zu bestätigen, dass eine bestimmte natürliche Person die Person ist, die sie vorgibt zu sein, und Systeme, die dazu dienen, die Identität einer natürlichen Person ausschließlich zum Zwecke des Zugangs zu einem Dienst, einem Gerät oder einer Räumlichkeit zu bestätigen" („excluding verification/authentication systems whose sole purpose is to confirm that a specific natural person is the person he or she claims to be, and systems that are used to confirm the identity of a natural person for the sole purpose of having access to a service, a device or premises"), Erwgr. Nr. 8 Ratsdok. 10069/22, Art. 3 Nr. 36 Ratsdok. 10069/22.

halt: Die zuständige Justiz- oder unabhängige Verwaltungsbehörde des jeweiligen Mitgliedstaates muss den Einsatz gestatten (Art. 5 Abs. 3, Erwgr. Nr. 21 KI-VO-E).[55]

Soweit Fernidentifizierungssysteme nicht in Echtzeit, sondern **zeitlich asynchron** operieren, unterfallen sie zwar nicht dem Verbot des Art. 5 KI-VO-E. Regulatorische Freiheit genießen sie gleichwohl nicht. Vielmehr greifen dann die Bestimmungen für Hochrisiko-KI-Systeme (Art. 6 Abs. 2 ff., Anhang III Nr. 1 Buchst. a KI-VO-E; → Rn. 55). 34

Der rechtliche Rahmen für biometrische Identifizierungssysteme ist vielen **Nichtregierungsorganisationen** sowie dem **Europäischen Parlament** nicht eng genug: Sie wünschen sich ein **vorläufiges Moratorium bzw. generelles Verbot** der Technik.[56] Die jetzige Begrenzung auf „Echtzeit"-Systeme ermögliche es den Behörden, umstrittene und problematische Software wie bspw. PimEyes[57] und Clearview AI[58] zur Anwendung zu bringen.[59] Auch die Tatsache, dass der Entwurf es **privaten Stellen** nicht verbietet, die Systeme zu verwenden, ruft Kritiker auf den Plan.[60] Denn gerade in privater Hand geht von Systemen, die die Anonymität des Alltäglichen faktisch aufheben, eine besondere, nur schwer kontrollierbare Gefahr aus. Inwieweit die Union über die notwendige Gesetzgebungskompetenz verfügt, den Einsatz von Fernidentifizierungssystemen zu Strafverfolgungszwecken anstelle der Mitgliedstaaten zu regulieren, lässt sich ebenfalls hinterfragen.[61] 35

D. Hochrisiko-KI-Systeme (Art. 6 ff. KI-VO-E)

Anders als die **verbotenen Praktiken des Art. 5 KI-VO-E** verbannt der Verordnungsentwurf **Hochrisiko-KI-Systeme** nicht von vornherein aus dem gesellschaftlichen Alltag. 36

[55] Die slowenische und französische Ratspräsidentschaft schlagen insoweit vor, es ausreichen zu lassen, wenn die Verantwortlichen die Genehmigung noch während des Einsatzes („without undue delay") einholen und die Verwendung einstellen, falls die Zulassungsinstanz diese versagt; Art. 5 Abs. 3 Ratsdok. 14278/21; Art. 5 Abs. 3 Ratsdok. 10069/22.

[56] Entschließung des Europäischen Parlaments 2020/2016(INI), P9_TA(2021)0405; bspw. Algorithmwatch, AlgorithmWatch's response to the European Commission's proposed regulation on Artificial Intelligence – a major step with major gaps 2021. Die europaweite Initiative „Reclaim Your Face" (https://reclaimyourface.eu/de/) sowie die deutsche Bewegung „Gesichtserkennung stoppen" (https://gesichtserkennung-stoppen.de/) stehen ebenfalls paradigmatisch für ein breites Engagement gegen den Einsatz. Ihr Unterstützerkreis setzt sich aus Nichtregierungsorganisationen, Politikern sowie Privatpersonen zusammen.

[57] PimEyes ist eine Suchmaschine, die biometrische Gesichtserkennung ausführt. Sie speichert in einer Datenbank die biometrischen Informationsgehalte öffentlich zugänglicher Internetbilder, um so Personen, deren Bilder Nutzer in die Datenbank hochladen, zu identifizieren. Der Landesbeauftragte für Datenschutz und Informationsfreiheit in Baden-Württemberg hat im Mai 2021 ein Verfahren gegen PimEyes eingeleitet, vgl. LfDI, Pressemitteilung Gesichtserkennung: LfDI eröffnet Verfahren gegen Unternehmen PimEyes, Mai 2021, abrufbar unter: https://www.baden-wuerttemberg.datenschutz.de/gesichtserkennung-lfdi-eroeffnet-verfahren-gegen-unternehmen-pimeyes/ (zuletzt aufgerufen am 4.10.2022).

[58] Clearview AI ist ein amerikanisches Unternehmen, das eine zentrale Biometriedatenbank führt, in die es Bilder und Videos einstellt, die es aus öffentlich zugänglichen Quellen, bspw. Social-Media-Kanälen, kopiert und mit seinem Datenbestand abgleicht. Mehrere Datenschutzbehörden – zuletzt auch Italiens und Großbritanniens – haben bereits Bußgelder in Millionenhöhe verhängt, vgl. dazu bspw. Information Commissioner's Office, Pressemitteilung, ICO fines facial recognition database company Clearview AI Inc more than £7.5 m and orders UK data to be deleted, May 2022, abrufbar unter: https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2022/05/ico-fines-facial-recognition-database-company-clearview-ai-inc/ (zuletzt aufgerufen am 4.10.2022); Qasim ZD-Aktuell 2022, 01144; siehe ausführlich zum Unternehmen auch Hill, The Secretive Company That Might End Privacy as We Know It, New York Times, Januar 2020, abrufbar unter: https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html (zuletzt aufgerufen am 4.10.2022).

[59] Krit. dazu Electronic Privacy Information Center, Feedback to the European Commission Regarding the Proposal for Harmonized Rules on Artificial Intelligence, 2021, 4, abrufbar unter: https://epic.org/apa/comments/EPIC-EC-Aug2021-AIA-Comments.pdf (zuletzt aufgerufen am 4.10.2022).

[60] Bspw. Electronic Privacy Information Center, Feedback to the European Commission Regarding the Proposal for Harmonized Rules on Artificial Intelligence, 2021, 5, abrufbar unter: https://epic.org/apa/comments/EPIC-EC-Aug2021-AIA-Comments.pdf (zuletzt aufgerufen am 4.10.2022).

[61] → Rn. 94 ff.

Er presst sie vielmehr in ein **enges Korsett** von Regulierungsmaßnahmen, die Art. 6 ff. KI-VO-E im Einzelnen auffächern. Die Vorschriften verfolgen das Ziel, in besonders hohem Maße gefahrträchtige KI-Systeme regulatorisch so einzuhegen, dass ihre Risiken mit den gemeinsamen Grundwerten der EU sowie den rechtlich verbürgten Individualrechten im Einklang stehen und dadurch verantwortbar sind.

37 Die **Vielfalt der Pflichten,** die der EU-Gesetzgeber aus der Taufe hebt, ist groß. Betreiber[62] von Hochrisiko-KI-Systemen müssen etwa ein Risikomanagementsystem einführen (Art. 9 KI-VO-E), menschliche Kontrolle sicherstellen (Art. 14 KI-VO-E) sowie Genauigkeit, Robustheit und Cybersicherheit des Systems gewährleisten (Art. 15 KI-VO-E). Das System muss auch aufzeigen, welche Fehlerquote bei seinen Berechnungen zu erwarten ist (Art. 15 Abs. 2 KI-VO-E). V. a. aber müssen Hochrisiko-KI-Systeme zwingend ein Konformitätsbewertungsverfahren durchlaufen, bevor sie (markiert mit einem CE-Kennzeichen) zum Einsatz kommen dürfen (Art. 19 KI-VO-E).[63] Das Pflichtenprogramm erstreckt sich im Grundsatz über den **gesamten Lebenszyklus** des Systems hinweg (vgl. insbes. Art. 15 Abs. 1 KI-VO-E).

38 Für solche Systeme, die bereits vor dem Datum, an welchem die Verordnung Geltung erlangt, in Verkehr gebracht oder in Betrieb genommen wurden, sieht der Entwurf aus **Bestandsschutzgründen** eine Privilegierung vor: Auf sie finden die Vorschriften der Art. 6 ff. KI-VO-E nur Anwendung, wenn sich ihre „Konzeption oder Zweckbestimmung **wesentlich geändert**[64]" hat (Art. 83 Abs. 2 KI-VO-E).

39 Verstößt der Anbieter gegen die Sorgfaltspflichten der Art. 8 ff. KI-VO-E, trägt der Geschädigte nach allgemeinen Haftungsprinzipien grds. die **Beweislast.** Die Kommission möchte das in ihrem Vorschlag für ein **KI-Haftungsgesetz**[65] ändern: Betreibt der Anbieter kein hinreichendes Risikomanagement oder verwendet unzureichende Trainingsdaten bzw. stellt die menschliche Aufsicht nicht sicher, kehrt sich die Beweislast um. Gleiches gilt, wenn der Anbieter die Informationen, die der Betroffene benötigt, um seine Schädigung durch eine KI nachzuweisen, nicht oder nicht in hinreichendem Maße zur Verfügung stellt. Strafrechtliche Verantwortlichkeit und Fragen des straßenverkehrsrechtlichen Haftungsrechts lässt der Vorschlag jedoch unberührt.

I. Klassifizierung der Hochrisiko-KI-Systeme

40 Der KI-VO-E kennt **zwei Wege,** auf denen eine KI-Anwendung die sensible Stufe eines Hochrisiko-KI-Systems erklimmen kann: Entweder es handelt sich um **Produkte** bzw. **Sicherheitskomponenten** dieser Produkte, die unter die Harmonisierungsvorschriften des unionalen Produktsicherheitsrechts fallen (1., → Rn. 41 ff.). Oder das System unterfällt einem **Positivkatalog** sensibler Anwendungsbereiche risikogeneigter KI (2., → Rn. 50 ff.). Da die Definition von KI-Systemen in Art. 3 Nr. 1 KI-VO-E sehr weit gefasst ist,[66] stem-

[62] Der KI-VO-E formuliert die Anforderungen an Hochrisiko-KI-Systeme in Titel III Kapitel 2 KI-VO-E häufig passiv ohne ausdrücklichen Adressaten. Für eigenständige Systeme treffen die Pflichten primär den Anbieter (Art. 16 KI-VO-E) bzw. den Produkthersteller (Art. 24 KI-VO-E), wenn das KI-System Teil eines Produktes ist. Weitere mögliche Adressaten für Teile der Regeln können insbes. Bevollmächtigte (Art. 25 KI-VO-E), Einführer (Art. 26 KI-VO-E), Händler (Art. 27 KI-VO-E) sowie Nutzer (Art. 29 KI-VO-E) sein.

[63] Innerhalb der Bereiche des Anhangs III Nr. 2–8 KI-VO-E muss der Anbieter des Systems aufgrund Art. 43 Abs. 2 S. 1 KI-VO-E eine eigene Konformitätsbewertung erstellen. Anders hingegen im Bereich des Anhangs III Nr. 1 KI-VO-E (biometrische Identifizierung): Hier richten sich die Anforderungen für das Konformitätsbewertungsverfahren nach Art. 43 Abs. 1 KI-VO-E. In diesem Fall bedarf es einer Bewertung durch Dritte.

[64] Hervorhebung d. Verf.

[65] Vorschlag der Kommission für eine Richtlinie zur Anpassung der Vorschriften über außervertragliche zivilrechtliche Haftung an künstliche Intelligenz (Richtlinie über KI-Haftung), COM(2022) 496 final.

[66] Unter den Begriff fällt jegliche „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

men die Vorgaben des Art. 6 KI-VO-E nahezu allein die wichtige Aufgabe, den Anwendungsbereich der strengen Regeln für Hochrisiko-KI-Systeme auf ein verträgliches Maß zu begrenzen.

1. Hochrisiko-KI-Systeme nach dem Produktsicherheitsrecht (Art. 6 Abs. 1 KI-VO-E)

Anwendungen, die einer im Unionsrecht **bereits an anderer Stelle regulatorisch eingehegten Produktgruppe** unterfallen (zB Medizinprodukte wie Software, die Diagnosen stellen kann) oder die als **Sicherheitskomponente**[67] eines solchen Produkts Verwendung finden (etwa eine Software in einem Auto), lösen in den Augen der Kommission ein gesteigertes Kontrollbedürfnis aus, das ihre Einordnung als Hochrisiko-KI-Systeme rechtfertigt. Die betroffenen Produktarten adressiert der KI-VO-E im Wege einer Liste von **Harmonisierungsvorschriften,** also Richtlinien und Verordnungen, die konkrete Schutzmaßnahmen für bestimmte Produktgruppen unionsweit einheitlich spezifizieren.[68] Regelt die Union darin bereits umfassend die Sicherheit eines bestimmten Produkttyps, sollen die Vorkehrungen künftig auch solche Gefahren berücksichtigen, die aus dem Einsatz von KI in diesen Produkten erwachsen können. 41

Art. 6 Abs. 1 KI-VO-E adressiert eine Vielzahl an Produkten, die zu großen Teilen im **Transportbereich** angesiedelt sind. Kommt bspw. ein KI-System in einem Auto zum Einsatz, um dort für den Fahrer die Fahrspur zu halten, gilt es als hochriskant. Außerdem erfasst er ua **Maschinen, Spielzeug** und **Medizinprodukte** (Anhang II Abschnitt A, B KI-VO-E). Allerdings bezieht der KI-VO-E nicht alle diese Produkte gleichermaßen in seinen normativen Radius ein. Denn die meisten Regeln der Art. 8 ff. KI-VO-E sind nur auf denjenigen Teil der Produkte direkt anwendbar, die dem sog. Neueren Produktsicherheitskonzept der Union (New Approach und New Legislative Framework)[69] unterfallen (b, → Rn. 46 ff.). Manche Produkte unterliegen hingegen den älteren Ansätzen der sog. Detailharmonisierung, die sich nicht ohne Weiteres mit dem Konzept des KI-VO-E synchronisieren lassen. Für sie gelten daher gesonderte Regeln (a, → Rn. 43 ff.). 42

Menschen festgelegt werden, Ergebnisse wie Inhalte, Vorhersagen, Empfehlungen oder Entscheidungen hervorbringen kann, die das Umfeld beeinflussen, mit dem sie interagieren" (Art. 3 Nr. 1 KI-VO-E). Die angesprochenen Techniken und Konzepte sind insbes. Deep Learning, logik- und wissensgestützte Konzepte oder statistische Ansätze (Anhang I KI-VO-E).

[67] Darunter versteht der Entwurf „einen Bestandteil eines Produkts oder Systems, der eine Sicherheitsfunktion für dieses Produkt oder System erfüllt oder [...] die Gesundheit und Sicherheit von Personen oder Sachen gefährdet", wenn er ausfällt oder gestört ist (Art. 3 Nr. 14 KI-VO-E).

[68] Die Harmonisierungsvorschriften betreffen zurzeit vornehmlich körperliche Objekte. Die Spielzeugrichtlinie nimmt bspw. Computerspiele explizit aus (Art. 2 Abs. 1 UAbs. 2 RL 2009/48/EG iVm Anhang I Nr. 15 RL 2009/48/EG). Dass ein KI-System selbst das Produkt im Sinne einer Harmonisierungsvorschrift darstellt, tritt nach der aktuellen Konzeption nur selten ein (Wiebe BB 2022, 899 (900)). Ein relevanter Anwendungsfall sind Medizinprodukte; zu ihnen zählt ausweislich der Medizinprodukteverordnung auch Software (Art. 2 Nr. 1 VO (EU) 2017/745). Die Funkanlagen-Richtlinie (RL 2014/53/EU) adressiert zwar primär körperliche Funkanlagen, trifft jedoch auch Anweisungen für den Fall, dass Nutzer eine Funkanlage im Nachhinein mit einer anderen Software bespielen. Vgl. zB Art. 3 Abs. 3 UAbs. 1 Buchst. i, Art. 4 RL sowie Erwgr. Nr. 16, 19 RL 2014/53/EU. Die Richtlinie formuliert daher einen weiteren Ausnahmefall einer Harmonisierungsvorschrift, die auch eigenständige Softwareprodukte adressiert.

[69] Der New Approach ist insbes. durch eine Kombination aus vier Prinzipien charakterisiert: Die Verordnungen oder Richtlinien der Union formulieren nur grundlegende Sicherheitsstandards, die Details überlassen sie den privaten Normungsorganisationen CEN, CENELEC oder ETSI. Die Produktverantwortlichen sind nicht verpflichtet, die privaten Standards einzuhalten, gelangen jedoch in den Genuss einer Konformitätsvermutung für Produkte, die sie nach den Standards herstellen; s. dazu bspw. Dauses/Ludwigs EU-WirtschaftsR-HdB/Langner/Klindt/Schucht C. VI. Rn. 9. Das New Legislative Framework überarbeitete diesen Ansatz vor allem im Hinblick auf die behördliche Marktüberwachung, die Zuordnung der Produktverantwortlichkeit auf die einzelnen Akteure sowie eine Standardisierung des Konformitätsbewertungsverfahrens, vgl. Dauses/Ludwigs EU-WirtschaftsR-HdB/Langner/Klindt/Schucht C. VI. Rn. 18 f.

a) Produktregulierung nach dem alten Regulierungskonzept

43 Für KI-Systeme, die dem Anwendungsbereich der in Anhang II Abschnitt B KI-VO-E bestimmten Harmonisierungsvorschriften unterfallen, greift ein **Sonderkonzept,** um konzeptuelle Friktionen zwischen den Regelungstechniken der Detailharmonisierung und denen des KI-VO-E zu verhindern. Zu den adressierten Produktbereichen gehören va Kraftfahrzeuge (VO (EU) 168/2013, VO (EU) 167/2013, VO (EU) 2018/858) sowie die Zivilluftfahrt (VO (EG) 300/2008, VO (EU) 2018/1139).

44 Diese Systeme stuft der KI-VO-E zwar **stets als Hochrisiko-Anwendungen** ein.[70] Allerdings wendet der Verordnungsentwurf die meisten seiner Vorschriften auf sie nicht an (Art. 2 Abs. 2 KI-VO-E). Vielmehr gilt dann lediglich Art. 84 KI-VO-E.[71] Produkte, die unter das „Alte Konzept" fallen, müssen somit die Anforderungen des KI-VO-E an Hochrisiko-KI-Systeme **nicht unmittelbar** erfüllen.[72] Der Grund hierfür liegt in einem Zusammentreffen zweier **grundlegend verschiedener regulatorischer Produktsicherheitsansätze.** So setzt das alte Regulierungskonzept bspw. allein auf staatliche Normen; auch nimmt die Prüfung der Anforderungen durch **staatliche Stellen** eine zentrale Rolle ein.[73] Damit lassen sich die Vorgaben für Hochrisiko-KI-Systeme nicht ohne Weiteres synchronisieren. Denn im KI-VO-E sind ebenso harmonisierte Normen der privaten Normungsorganisationen grundlegend verankert wie ein grds. rein internes Konformitätsbewertungsverfahren des Herstellers oder mithilfe einer privaten notifizierten Stelle. Deshalb plant die Kommission, dass die Union stattdessen die Harmonisierungsgrundlagen selbst **erneuert** und die darauf beruhenden Durchführungsrechtsakte oder delegierten Rechtsakte **ergänzt** (Erwgr. Nr. 29 KI-VO-E). In diesem Zuge will sie die Regeln für Hochrisiko-KI-Systeme dort inkludieren.[74]

45 Bisher sind jedoch für Harmonisierungsrechtsvorschriften des alten Konzepts keine konkreten Erneuerungen in Planung.[75] Immerhin gilt seit dem Sommer 2022 eine Durchführungsverordnung der Kommission zu technischen Spezifikationen vollautomatisiert fahrender Fahrzeuge.[76] Die KI-Systeme in solchen Autos unterfallen dadurch gemeinsam mit

---

[70] Alle Produkte, die unter diese Normen fallen, müssen eine Vorab-Konformitätsbewertung durch Dritte durchlaufen, SWD(2021) 84 final Part 2/2 (Impact Assessment – Annexes), 39. Damit ist die Voraussetzung des Art. 6 Abs. 1 Buchst. b KI-VO-E stets erfüllt.

[71] Diese Norm regelt den Umfang, in dem die Kommission die Umsetzung und mögliche Änderungsbedarfe der KI-VO begleitet.

[72] Die KI-VO wird allerdings auf die Normen aus Anhang II Abschnitt B mittelbar einwirken: Erlässt die Kommission Durchführungsrechtsakte oder delegierte Rechtsakte, die auf den Normen des Anhangs II Abschnitt B beruhen, muss sie dabei die Anforderungen für Hochrisiko-KI-Systeme aus Titel III Kapitel 2 beachten (Art. 75–82 KI-VO-E). Dadurch entfalten die Vorgaben für ua Risikomanagement, Daten-Governance und menschliche Aufsicht auch auf diese Produkte ihre Wirkung, wenn sie KI-Systeme inkludieren, vgl. Begr. Nr. 1.2 KI-VO-E.

[73] SWD(2021) 84 final Part 2/2 (Impact Assessment – Annexes).

[74] SWD(2021) 84 final Part 2/2 (Impact Assessment – Annexes), 40. Die Harmonisierungsvorschriften sollen jedoch ihren Charakter als Produktsicherheitsvorschriften beibehalten, auch wenn der Gesetzgeber Qualitätsanforderungen an KI in die bestehenden Produktgesetze integriert: Sofern diese Vorschriften zukünftig auch Sicherheitsanforderungen an KI formulieren, geschieht dies letztlich zu dem Zweck, dass die adressierten Produkte als Gegenstände der Harmonisierungsvorschriften selbst sicher sind; SWD(2021) 84 final Part 1/2 (Impact Assessment), 7. Primäres Ziel der Normen ist es also auch weiterhin nicht, KI zu regulieren.

[75] SWD(2021) 84 final Part 1/2 (Impact Assessment), 7.

[76] Durchführungsverordnung (EU) 2022/1426 der Kommission vom 5.8.2022 mit detaillierten Regelungen zur Durchführung der Verordnung (EU) 2019/2144 des Europäischen Parlaments und des Rates im Hinblick auf die einheitlichen Verfahren und technischen Spezifikationen für die Typgenehmigung des automatisierten Fahrsystems (ADS) vollautomatisierter Fahrzeuge (ABl. L 221, 1), mit detaillierten Regelungen zur Durchführung der Verordnung (EU) 2019/2144 des Europäischen Parlaments und des Rates vom 27.11.2019 über die Typgenehmigung von Kraftfahrzeugen und Kraftfahrzeuganhängern sowie von Systemen, Bauteilen und selbstständigen technischen Einheiten für diese Fahrzeuge im Hinblick auf ihre allgemeine Sicherheit und den Schutz der Fahrzeuginsassen und von ungeschützten Verkehrsteilnehmern, zur Änderung der Verordnung (EU) 2018/858 des Europäischen Parlaments und des Rates und zur Aufhebung der Verordnungen (EG) Nr. 78/2009, (EG) Nr. 79/2009 und (EG) Nr. 661/2009 des Europäischen Parlaments und des Rates

dem Auto den Sicherheitsvorschriften für das Fahrzeug (wobei die Vorschriften nun Qualitätsanforderungen an KI-Systeme inkludieren). Da sich jedoch keine weiteren Anpassungsvorhaben abzeichnen und auch eine direkte Anwendung der Regeln im KI-VO-E ausgeschlossen sein soll, bleibt für die meisten dem alten Regulierungskonzept unterfallenden Hochrisiko-KI-Systeme auf absehbare Zeit eine Sonderrolle bestehen. Insofern lässt sich auch kritisch fragen, weshalb diese Kategorie überhaupt Teil des KI-VO-E sein sollte oder ob sie lediglich den Begriff der Hochrisiko-KI-Systeme verwässert.

b) Produktregulierung nach dem neuen Rechtsrahmen

Für Produkte, die bereits Sicherheitsvorkehrungen des **neuen Rechtsrahmens** (New Approach und New Legislative Framework) unterworfen sind, ordnet Anhang II Abschnitt A KI-VO-E die Einstufung als Hochrisiko-KI-System an. Darunter fallen etwa Maschinen (RL 2006/42/EG), Medizinprodukte (VO (EU) 2017/745), Funkanlagen (RL 2014/53/EU) oder Spielzeug (RL 2009/48/EG). Nicht jedes der Produkte, das diesen Sektoren zugehört, muss aber die Pflichten für Hochrisiko-KI-Systeme einhalten. Erforderlich ist vielmehr zusätzlich, dass die Produkte aufgrund von Harmonisierungsvorschriften der Union einer **Vorab-Konformitätsbewertung durch Dritte** unterliegen (Art. 6 Abs. 1 Buchst. b KI-VO-E). Damit vollzieht der KI-VO-E eine Risikoklassifizierung nach, die der neue Rechtsrahmen für diese Produkte aufstellt. 46

Die **Medizinprodukte-VO** (VO (EU) 2017/745) als wichtiges Referenzfeld kennt bspw. vier Risikoklassen, für die sie teilweise eine externe, teilweise eine interne Konformitätsprüfung vorsieht. Produkte mit dem geringsten Risiko (wie bspw. Verbandmaterial) unterliegen lediglich einer Konformitätsbewertung durch den Hersteller, nicht aber durch Dritte (Art. 51 Abs. 1, Art. 52 Abs. 7 VO (EU) 2017/745; Erwgr. Nr. 60 VO (EU) 2017/745).[77] Die Regeln für Hochrisiko-KI-Systeme werden daher nur für die Medizinprodukte, denen ein **mittleres oder hohes Risiko** anhaftet, gelten.[78] Für medizinische Software ist **keine pauschale Risikogruppe** vorgesehen: Die Kategorisierung einer Software, die ein *Medizinprodukt* steuert, ist vielmehr von der Klasse des Produkts abhängig (Ziff. 3.3. Anhang VIII VO (EU) 2017/745). Sie ist derselben Klasse wie das Produkt zuzurechnen. Liefert eine selbstständige KI-Software zB Informationen für Entscheidungen über Diagnosen und Therapien und hat sie damit mind. Einfluss auf eine mögliche schwerwiegende Verschlechterung des Gesundheitszustandes, muss der Hersteller eine externe Stelle für die Konformitätsbewertung einschalten. Die Software gilt daher dann als Hochrisiko-KI-System (Art. 52 Abs. 3, 4 VO (EU) 2017/745 iVm Ziff. 6.3. Anhang VIII VO (EU) 2017/745).[79] 47

Die Konzeption des KI-VO-E zielt darauf, möglichst viele der neuen Anforderungen für Hochrisiko-KI-Systeme in die bestehenden Produktsicherheitsverfahren zu **integrieren.** Zurzeit sind bspw. Aktualisierungen der Maschinen-RL (RL 2006/42/EG) sowie der Richtlinie über die allgemeine Produktsicherheit (RL 2001/95/EG) in Arbeit, die auch auf die Entwicklungen der KI-Technologien reagieren sollen.[80] Die Normen behalten dadurch ihren Charakter als Produktsicherheitsvorschriften; ihr oberstes Ziel bleibt die Sicherheit des jeweiligen Produktes. Für die Produkte, die dem neuen Rechtsrahmen unterfallen, gelten zukünftig **daneben** die Vorschriften des KI-VO-E.[81] 48

sowie der Verordnungen (EG) Nr. 631/2009, (EU) Nr. 406/2010, (EU) Nr. 672/2010, (EU) Nr. 1003/2010, (EU) Nr. 1005/2010, (EU) Nr. 1008/2010, (EU) Nr. 1009/2010, (EU) Nr. 19/2011, (EU) Nr. 109/2011, (EU) Nr. 458/2011, (EU) Nr. 65/2012, (EU) Nr. 130/2012, (EU) Nr. 347/2012, (EU) Nr. 351/2012, (EU) Nr. 1230/2012 und (EU) 2015/166 der Kommission im Hinblick auf die einheitlichen Verfahren und technischen Spezifikationen für die Typgenehmigung des automatisierten Fahrsystems (ADS) vollautomatisierter Fahrzeuge.

[77] Erwgr. Nr. 60 VO (EU) 2017/745.

[78] Erwgr. Nr. 31 S. 2 KI-VO-E.

[79] Ausführlich dazu bspw. Heil PharmR 2022, 473.

[80] SWD(2021) 84 final Part 1/2 (Impact Assessment), 6f.

[81] SWD(2021) 84 final Part 2/2 (Impact Assessment – Annexes), 37.

c) Zwischenfazit

49 Für die Hochrisiko-KI-Systeme, die Bestandteil eines Produkts oder selbst ein Produkt sind, das den Produktsicherheitsvorschriften der Union unterfällt, sind auch künftig grds. allein die produktsicherheitsrechtlichen Harmonisierungsvorschriften maßstabsbildend. Nur für die nach dem neuen Produktsicherheitskonzept regulierten Systeme sollen auch die Regeln des KI-VO-E unmittelbar gelten. Damit bilden die produktbezogenen Systeme iSd Art. 6 Abs. 1 KI-VO-E zwar gemeinsam mit den eigenständigen Systemen iSd Art. 6 Abs. 2 KI-VO-E die Kategorie der Hochrisiko-KI-Systeme, unterfallen jedoch **nur teilweise denselben Rechtsfolgen.** Von besonderer Bedeutung wird insofern sein, wie die Union die Anforderungen der einzelnen Produktsicherheitsvorschriften konkret ausgestaltet und ob **Abweichungen** zu den Regeln des KI-VO-E entstehen. Davon wird auch abhängen, inwiefern dadurch ein (Abgrenzungs-)Problem entstehen kann, dass eigenständige Software, die Gegenstand der produktsicherheitsrechtlichen Harmonisierungsvorschriften ist,[82] den Produktsicherheitsvorschriften mit möglicherweise eigenen Anforderungen unterfällt, während jegliche weiteren eigenständigen KI-Softwaresysteme ausschließlich den Anforderungen des KI-VO-E unterfallen.

2. Eigenständige Hochrisiko-KI-Systeme (Art. 6 Abs. 2 KI-VO-E)

50 Ohne Rücksicht auf ihre produktsicherheitsrechtliche Klassifizierung stuft Art. 6 Abs. 2 iVm Anhang III KI-VO-E solche Systeme als hochriskant ein, von denen kraft ihres **sensiblen Anwendungsfeldes** besondere Gefahren für natürliche Personen ausgehen können.

51 Die Systeme iSd Art. 6 Abs. 2 KI-VO-E bergen absehbare Risiken,[83] die auf die **grundrechtliche Entfaltung** oder die **Gesundheit** und **Sicherheit** nachhaltig ausstrahlen können (vgl. Erwgr. Nr. 32 S. 1 KI-VO-E). Tragende Gründe für ihre Einordnung als Hochrisiko-KI-Systeme sind jeweils die „Schwere des möglichen Schadens" sowie die „Wahrscheinlichkeit seines Auftretens" (vgl. Erwgr. Nr. 32 S. 1 KI-VO-E),[84] also letztlich das **Risiko,** das von ihnen prognostisch ausgeht. Auch die Zweckbestimmung des KI-Systems, das Ausmaß seiner (zukünftigen) Verwendung, Umfang und Irreversibilität potenzieller Schäden sowie andere Rechtsvorschriften der Union, die bereits in Kraft getreten sind und den entsprechenden Risiken des Systems begegnen (können), waren für die Kommission maßgebliche Faktoren, um den Einsatzbereich des KI-Systems in die Liste des Anhangs III KI-VO-E aufzunehmen.[85]

52 Ist eine Systemgruppe Teil dieser Auflistung, ist es grds. irrelevant, ob **kleine, mittlere oder große Unternehmen** das KI-System einsetzen, ebenso wie die **Größe des potenziellen Betroffenenkreises** oder der **Umfang möglicher wirtschaftlicher Schäden.**[86] Auch ob eine Anwendung Entscheidungen vollständig automatisiert trifft oder ein **Mensch involviert** ist, spielt grds. keine Rolle.

53 So feinsäuberlich der Anhang III KI-VO-E die unterschiedlichen Kategorien auch auffächert, so wenig darf dies darüber hinwegtäuschen, welch **heterogene Sammlung** er erfasst. Er führt eine bunte Schar an Systemen unterschiedlicher Zielsetzungen, Einsatzgebiete und Gefährdungspotenziale zusammen. Die Bandbreite reicht von der Kreditwürdigkeitsprüfung (Anhang III Nr. 5 Buchst. b KI-VO-E) über Priorisierungen bei Not- und Rettungsdiensten (Anhang III Nr. 5 Buchst. c KI-VO-E) bis hin zur Kriminalanalyse (An-

---

[82] Das wird im Regelfall nur Software im Anwendungsbereich der Medizinprodukte-VO sein, s. dazu schon → Fn. 68.

[83] Begr. Nr. 5.2.3 KI-VO-E.

[84] Erwgr. Nr. 32 S. 1 KI-VO-E.

[85] Vgl. Art. 7 Abs. 2 KI-VO-E sowie die Ausführungen dieses Beitrags unter → Rn. 109 ff.

[86] Ausnahmen gibt es nur selten, so gelten Systeme zur Prüfung der Kreditwürdigkeit dann nicht als hochriskant, wenn Kleinanbieter sie für den Eigengebrauch in Betrieb nehmen (Anhang III Nr. 5 Buchst. b KI-VO-E).

hang III Nr. 6 Buchst. g KI-VO-E) sowie der Prüfung von Asyl- und Visumanträgen (Anhang III Nr. 7 Buchst. d KI-VO-E).

Bei aller Heterogenität lassen sich dennoch einige **Verbindungslinien** zwischen den Bereichen, die Anhang III KI-VO-E auflistet, erkennen: Bei den meisten der betroffenen KI-Systeme handelt es sich um Anwendungen des **öffentlichen Sektors.** Viele zielen darauf, die **gesellschaftliche Teilhabe** und die **Lebensgrundlagen** sowie die öffentliche **Infrastruktur** zu sichern (Anhang III Nrn. 2–5 KI-VO-E). Die Sektoren „Strafverfolgung" (Anhang III Nr. 6 KI-VO-E) sowie „Migration, Asyl und Grenzkontrolle" (Anhang III Nr. 7 KI-VO-E) erfassen Kernbereiche der **öffentlichen Sicherheit.** Auch Systeme der biometrischen Identifizierung (Anhang III Nr. 1 KI-VO-E) stehen in einem engen thematischen Bezug zur Aufgabe „Sicherheit".[87] In seinem konkreten Zuschnitt noch am wenigsten konturiert ist der Bereich **„Rechtspflege und demokratische Prozesse"** (Anhang III Nr. 8 KI-VO-E). 54

a) Biometrische Identifizierung und Kategorisierung natürlicher Personen (Anhang III Nr. 1 Buchst. a KI-VO-E)

Von einer Fernidentifizierung mit Daten „zu den physischen, physiologischen oder verhaltenstypischen Merkmalen einer natürlichen Person" (vgl. Art. 4 Nr. 14 DS-GVO) geht nicht nur die Gefahr aus, **besonders tief** in die **Freiheitsrechte Betroffener** (insbes. ihr Recht auf Schutz personenbezogener Daten [Art. 8 GRCh]), einzuwirken.[88] Sie birgt auch das Risiko, dass das System im Gefolge technischer Unzulänglichkeiten die Personen aufgrund ihres äußeren Erscheinungsbildes, das bspw. Rückschlüsse auf Geschlecht und Alter geben kann, **diskriminiert** (Erwgr. Nr. 33 S. 1 f. KI-VO-E). 55

Soweit biometrische Fernidentifizierung natürlicher Personen nicht bereits dem Verbot des **Art. 5 Abs. 1 Buchst. d KI-VO-E** unterfällt (→ Rn. 32), stuft der KI-VO-E sie daher als hochriskant ein. Das betrifft namentlich **asynchrone** Fernidentifizierungssysteme (also solche, die den erforderlichen Datenabgleich zeitlich verzögert vornehmen und damit nicht als **Echtzeit**-Fernidentifizierungssysteme Verwendung finden [vgl. Art. 3 Nr. 37 KI-VO-E]) sowie (unabhängig vom Einsatzmodus) solche Anwendungen, die **nicht zu Zwecken der Strafverfolgung,** sondern für andere Ziele zum Einsatz kommen. 56

Diese Fernidentifizierungssysteme unterwirft der KI-VO-E nicht nur den allgemeinen Anforderungen des Kap. 2 für Hochrisiko-KI-Systeme (Art. 8 ff. KI-VO-E). Mit Blick auf ihre hohe Grundrechtsrelevanz formuliert er für sie zusätzlich auch ein **normatives Sonderregime:** Sie unterliegen besonderen Protokollierungspflichten (vgl. Art. 12 Abs. 4 KI-VO-E) sowie spezifischen Vorgaben zur menschlichen Aufsicht (vgl. Art. 14 Abs. 5 KI-VO-E). Anders als andere Hochrisiko-KI-Systeme müssen sie sich darüber hinaus einer **Konformitätsbewertung durch eine unabhängige Instanz** stellen (Art. 19 Abs. 1 iVm Art. 43 KI-VO-E). Damit weist die Kommission dieser Unterkategorie eine auf sie zugeschnittene besondere Risikoeinstufung innerhalb der Hochrisiko-KI-Systeme zu und unterstreicht die **herausgehobene Kritikalität,** die sie dem Einsatz von „Smart Cams" beimisst. 57

b) Verwaltung und Betrieb kritischer Infrastrukturen (Anhang III Nr. 2 Buchst. a KI-VO-E)

Systeme, die als **Sicherheitskomponenten** in der Verwaltung oder beim **Betrieb kritischer Infrastruktur** (insbes. in der Wasser-, Gas-, Wärme- und Stromversorgung oder dem Straßenverkehr) zum Einsatz kommen, stuft der Unionsgesetzgeber aus gutem Grund als hochriskant ein. Sie kontrollieren nämlich nicht nur die Versorgung ganzer Städte und 58

[87] Ob in Hinblick auf die Kategorien, die (auch) den Bereich der nationalen Sicherheit umfassen, die Gesetzgebungskompetenz der EU besteht, ist unklar; → Rn. 95 ff.

[88] Vgl. bspw. Hornung/Schindler DuD 2021, 515 (517); Martini NVwZ-Extra 2/2022, 1 (5).

Gemeinden; wenn sie ausfallen, kann das auch gravierende Schäden sowohl für das **Leben** und die **Gesundheit** einer Vielzahl natürlicher Personen als auch für das **soziale und wirtschaftliche Leben** nach sich ziehen (Erwgr. Nr. 34 KI-VO-E).[89]

59 Sicherheitskomponenten des **Internets** bzw. der globalen digitalen Infrastruktur erfasst Anhang III Nr. 2 Buchst. a KI-VO-E hingegen nicht. Das reißt eine Schutzlücke. Je stärker wichtige Bestandteile der gesellschaftlichen Infrastruktur digital gesteuert und vernetzt sind, desto mehr entpuppt sich eine zuverlässige, sichere Anbindung an das Breitband- und Mobilfunknetz gleichsam als Lebensader der modernen Gesellschaft. Wenn die Systeme ausfallen, kann das ähnliche Wirkungen zeitigen wie das Versagen der Wärme- und Stromversorgung.[90] Auch Sicherheitskomponenten, die Emissionen und **Umweltverschmutzungen** kontrollieren sollen, erfasst der Katalog zu Unrecht nicht. Ihre Störung kann schwerwiegende Auswirkungen auf die Umwelt und Gesundheit der Bürger entfalten.[91]

60 Was Anhang III Nr. 2 Buchst. a KI-VO-E unter **„Sicherheitskomponenten"** versteht, konkretisiert der KI-VO-E nicht unmittelbar. Immerhin definiert Art. 3 Nr. 14 KI-VO-E aber den Begriff **„Sicherheitskomponente eines Produkts oder Systems"**[92]. Der Entwurf versteht darunter Bestandteile, die eine Sicherheitsfunktion für das Produkt oder das System erfüllen oder die Gesundheit und Sicherheit von Personen oder Sachen gefährden, wenn sie ausfallen oder eine Störung erfahren. Die Formulierung erhellt, dass Sicherheitskomponenten nicht allein solche Bestandteile eines Systems sind, welche die **Sicherheit des Systems** gewährleisten, sondern auch solche, die die Gesundheit und Sicherheit von Personen oder Sachen gefährden, wenn sie nicht mehr ordnungsgemäß funktionieren. Der Begriff adressiert mithin alle Gefahren für die **Gesundheit und Sicherheit** von Personen oder Sachen, nicht aber bspw. rein finanzielle Risiken.

61 Anhang III Nr. 2 Buchst. a KI-VO-E weicht in einem wichtigen Aspekt von den anderen Sachbereichen des Anhangs III KI-VO-E ab: Das Risiko der adressierten Systeme rührt weniger aus ihrem regelkonformen Einsatz her als daraus, dass sie **ausfallen.** Damit erweist sich diese Kategorie als **Solitär** unter den eigenständigen Systemen des Anhangs III. Sie steht den Systemen näher, welche das Sicherheitsrisiken adressierende Produktsicherheitskonzept aus Art. 6 Abs. 1 KI-VO-E erfasst.

c) Grundlagen der Lebensgestaltung (Anhang III Nrn. 3–5 KI-VO-E)

62 Als Hochrisiko-KI-Systeme klassifiziert der KI-VO-E neben sicherheitsrelevanten KI-Systemen eine Vielzahl von KI-Anwendungen aus Bereichen, die für die **Lebensgestaltung der Bevölkerung** eine zentrale Bedeutung entfalten.

63 Zu dieser Gruppe gehören insbes. Systeme, die über die **finanziellen Lebensgrundlagen** der Menschen bei öffentlichen Unterstützungsleistungen (Anhang III Nr. 5 Buchst. a KI-VO-E) sowie der Kreditvergabe (Anhang III Nr. 5 Buchst. b KI-VO-E) entscheiden, bspw. Anwendungen zur „Vorhersage von Sozialbetrug [und] Risikoanalyse"[93]. Auch Systeme, die Akteure im **Bildungsbereich** als Zugangskontrolle oder Bewertungsinstrument einsetzen (Anhang III Nr. 3 KI-VO-E; → Rn. 66 ff.), etwa um die Bewerbungsunterlagen für einen Studienplatz an einer Universität zu prüfen, fallen in diese Kategorie – auch solche, die in der **Arbeitswelt** für Auswahl- und Leistungsbewertungsprozesse zur Anwendung kommen (Anhang III Nr. 4 KI-VO-E; → Rn. 68 f.), bspw. um Mitarbeiter zu

[89] Erwgr. Nr. 34 KI-VO-E.

[90] So auch Draft Report on the proposal for a regulation of the European Parliament and of the Council on harmonised rules on Artificial Intelligence (Artificial Intelligence Act), PE731.563, 2021/0106(COD), 2022. Änderungsantrag Nr. 287 sowie Erwgr. Nr. 34, 99 (Anhang III) Ratsdok. 14278/21.

[91] Erwgr. Nr. 34 Ratsdok. 14278/21.

[92] Er rekurriert auf die produktsicherheitsrechtlichen Kategorisierung des Art. 6 Abs. 1 Buchst. a KI-VO-E.

[93] Muller/Schöppl/Avramidou/Talvitie/Férnandez-Peñalver, AIA in-depth, 2020, 9, abrufbar unter: https://allai.nl/wp-content/uploads/2022/04/AIA-in-depth-3a-High-Risk-AI-Classification.pdf (zuletzt aufgerufen am 4.10.2022).

kontrollieren und ihre Arbeitseffizienz zu überprüfen. Auch bei KI-Systemen, die bei **Not- oder Rettungsdiensten** Verwendung finden, ist es dem Verordnungsentwurf ein besonderes Anliegen, die Gefahren, die von ihnen ausgehen können, durch besondere Maßnahmen des Hochrisikoschutzes regulatorisch einzuhegen (Anhang III Nr. 5 Buchst. c KI-VO-E; → Rn. 70 ff.).

Denn in all diesen Einsatzkontexten stellen die Systeme Weichen für die Teilhabe des 64
Einzelnen an der Gesellschaft und an wesentlichen Dienstleistungen (wie Wohnraum oder Elektrizität) sowie die Freiheit, die eigenen Lebensumstände zu gestalten (Erwgr. Nr. 37 S. 1 KI-VO-E). Sie eint das Risiko, dass der KI-Einsatz besonders tiefgreifende und oft auch **längerfristige Einflüsse** auf die Lebensgrundlagen der betroffenen Personen zeitigen kann.

Alle Systeme des Anhangs III Nrn. 3–5 KI-VO-E zeichnen sich nicht nur durch die 65
Folgewirksamkeit ihrer Entscheidungen, sondern zudem durch ein besonders hohes **Diskriminierungsrisiko** aus. Nicht ohne Grund weist der Katalog daher starke Parallelen zum Anwendungsbereich der **Antidiskriminierungsrichtlinien** (Art. 3 Abs. 1 RL 2000/43/EG, Art. 3 Abs. 1 RL 2000/78/EG, Art. 3 Abs. 1 RL 2004/113/EG) auf. Auch sie spannen für Entscheidungen im Arbeits- und Bildungsbereich sowie die Versorgung mit der Öffentlichkeit zur Verfügung stehenden Gütern einen rechtlichen Rahmen auf, der Benachteiligungen aufgrund bestimmter Gruppenmerkmale verbietet.[94]

aa) Allgemeine und berufliche Bildung (Anhang III Nr. 3 KI-VO-E)

Mit Blick auf die fundamentale Bedeutung, welche der Bildung zukommt, um Lebens- 66
chancen zur Entfaltung zu bringen, stuft der KI-VO-E Anwendungen, die diesen Bereich steuern, als hochriskant ein. Das gilt insbes. für solche Systeme, die im Rahmen des **Zugangs** oder der Zuweisung natürlicher Personen zu allgemeinen und beruflichen **Bildungseinrichtungen** zum Einsatz kommen oder die Teilnehmer iRv Zulassungstests bewerten. Auch Systeme, deren Aufgabe es ist, die Schüler innerhalb ihrer Einrichtungen zu **beurteilen,** fallen in diese Kategorie. Dahinter steht der Gedanke, dass in diesen Einsatzgebieten nicht nur ein hohes Diskriminierungspotenzial (Erwgr. Nr. 35 S. 2 KI-VO-E) besteht, sondern dass die Anwendungen zusätzlich tief in die Lebensgestaltung und -planung der betroffenen Personen einwirken. Darüber hinaus können sie auch entscheidenden Einfluss auf die Möglichkeiten der Betroffenen nehmen, ihren Lebensunterhalt zu sichern (Erwgr. Nr. 35 S. 1 KI-VO-E).

In dem Berichtsentwurf des „IMCO"-Ausschusses sowie des „LIBE"-Ausschusses des 67
Europäischen Parlaments fordern die Abgeordneten, dass Kinder einen besseren Schutz vor KI-Systemen genießen sollten, die ihre Entwicklung nachhaltig beeinträchtigen bzw. beeinflussen können – und dass dieser Aspekt explizit Eingang in diese Schutznormen finden sollte.[95] Weitere Anwendungsfälle in Anhang III Nr. 3 KI-VO-E zu integrieren, zB Schul-Systeme, die Schüler **überwachen** und dadurch für mehr Sicherheit sorgen sollen,[96]

---

[94] Vertieft zum AGG und algorithmenbasierter Diskriminierung vgl. etwa Steege MMR 2019, 715; Sesing/Tschech MMR 2022, 24; Freyler NZA 2020, 284 (285 ff.); Dzida/Groh NJW 2018, 1917.

[95] Draft Report on the proposal for a regulation of the European Parliament and of the Council on harmonised rules on Artificial Intelligence (Artificial Intelligence Act), PE731.563, 2021/0106(COD), 2022, Änderungsanträge Nr. 23, 28.

[96] Schulen in Frankreich setzten bspw. Gesichtserkennungssysteme ein. Die nationale Datenschutzbehörde hat diese Praxis jedoch gestoppt, CNIL, Expérimentation de la reconnaissance faciale dans deux lycées: la CNIL précise sa position, abrufbar unter: https://www.cnil.fr/fr/experimentation-de-la-reconnaissance-faciale-dans-deux-lycees-la-cnil-precise-sa-position (zuletzt aufgerufen am 4.10.2022) sowie Algorithmwatch/Bertelsmann-Stiftung, Automating Society Report, 2020, 9, abrufbar unter: https://automatingsociety.algorithmwatch.org/wp-content/uploads/2021/01/Automating_Society_Report_2020_-_Deutsche_Ausgabe.pdf (zuletzt aufgerufen am 4.10.2022). Das Landesschulamt Sachsen-Anhalt setzt das System DyRiAS-Schule ein, um Schüler auf ihr Gewaltpotenzial hin zu analysieren, Algorithmwatch/Bertelsmann-Stiftung, Automating Society Report, 2020, 45, abrufbar unter: https://automatingsociety.algorithmwatch.org/wp-content/uploads/2021/01/Automating_Society_Report_2020_-_Deutsche_Ausgabe.pdf (zuletzt aufgerufen am 4.10.2022).

Proctoring[97] sowie Systeme, die den **Lernvorgang** optimieren sollen, ist in der Tat sachgerecht.[98] Denn die persönliche Entwicklung von Kindern ist mit Blick auf ihre Unerfahrenheit und die langfristigen Wirkungen, die KI-Systeme für ihre gesellschaftliche Teilhabe entfalten können, auf besondere Schutzregeln angewiesen, welche die technologischen Möglichkeiten regulatorisch einhegen.

bb) Beschäftigung, Personalmanagement und Zugang zur Selbstständigkeit (Anhang III Nr. 4 KI-VO-E)

68 KI-Systeme, die bei der Einstellung und Auswahl natürlicher Personen sowie im Rahmen des jeweiligen **Bewerbungsverfahrens** Einsatz finden, können bei der beruflichen Lebensplanung der betroffenen Personen eine zentrale Rolle einnehmen (Erwgr. Nr. 36 S. 1 KI-VO-E) und über Lebensperspektiven entscheiden. Der KI-VO-E stuft sie deshalb zu Recht als hochriskant ein. Aus ähnlichen Gründen unterfallen der Kategorie auch Systeme, die in Arbeitsverhältnissen über eine **Beförderung** oder **Kündigung** entscheiden und die Arbeitnehmer **kontrollieren** oder **bewerten.** Nicht zuletzt wirken sich Systeme, die das Verhalten oder die Leistung Beschäftigter überwachen, in grundlegender Weise auf deren Recht auf Privatsphäre aus (Erwgr. Nr. 36 S. 5 KI-VO-E).

69 Kritiker mahnen an, dass die Vorschriften des KI-VO-E weit gröber seien als diejenigen mancher **nationaler Arbeitsrechtssysteme:** Es stehe zu befürchten, dass ausgefeilte Errungenschaften einzelner Mitgliedstaaten auf den Gebieten des Arbeitsrechts und Beschäftigtendatenschutzes ihre Geltung einbüßen.[99] Der Deutsche Gewerkschaftsbund sieht den unionalen Schutzschirm überdies insgesamt noch nicht umfassend genug aufgespannt. Er fordert, dass Anhang III Nr. 4 KI-VO-E „sämtliche KI-Systeme [erfassen sollte], die bestimmungsgemäß für Entscheidungen [verwendet werden sollen], die die Anbahnung, Begründung, Durchführung und Abwicklung des Arbeitsverhältnisses betreffen".[100]

cc) Zugänglichkeit und Inanspruchnahme grundlegender privater und öffentlicher Dienste und Leistungen (Anhang III Nr. 5 KI-VO-E)

70 Ebenso wie in den Bereichen „Bildung" und „Arbeit" treffen Systeme, die Künstliche Intelligenz im Zusammenhang mit grundlegenden **privaten und öffentlichen Diensten und Leistungen** einsetzen, richtungsweisende Entscheidungen, die unmittelbar auf die **Lebensentfaltungschancen** des Einzelnen ausstrahlen können. Auf diesem Feld bergen KI-Anwendungen – insbes. mit Blick auf die gebotene Gleichbehandlung Betroffener, fehlende Nachvollziehbarkeit der Entscheidungen und Automatisierungsfehler – besondere Risiken für die grundrechtliche Entfaltung. Der KI-VO-E unterwirft sie deshalb zu Recht den Vorschriften für Hochrisiko-KI-Systeme.

71 Das gilt insbes. für Systeme, die beurteilen, ob Individuen **öffentliche Unterstützungsleistungen und -dienste** oder **Kredite** erhalten (Anhang III Nr. 5 Buchst. a, b KI-VO-E). Diese Entscheidungen entfalten nachhaltige Auswirkungen auf die **Teilhabe** natürlicher Personen an der Gesellschaft sowie den Zugang zu **lebenswichtigen Angeboten** wie Wohnraum und weitere Maßnahmen, um die eigenen Lebensumstände gestalten zu können (Erwgr. Nr. 37 S. 1 KI-VO-E). KI-gestützte Entscheidungen wirken bei natürlichen Personen, die von staatlichen Unterstützungsleistungen bzw. -diensten abhängig sind, tief in die Existenzgrundlagen hinein (Erwgr. Nr. 37 S. 5 f. KI-VO-E). Manche

---

[97] Damit ist die Online-Überwachung von Studierenden während einer zu Hause abzulegenden Prüfung bspw. mithilfe von Kamera- und Mikrofonaufnahmen gemeint. Eine KI könnte zB prüfen, ob der Blick der Prüflinge stets auf den Monitor gerichtet ist, sodass eine Zuhilfenahme eines aufgeschlagenen Lehrbuchs nicht möglich ist.

[98] Muller/Schöppl/Avramidou/Talvitie/Férnandez Peñalver, AIA in-depth, 2020, 8, abrufbar unter: https://allai.nl/wp-content/uploads/2022/04/AIA-in-depth-3a-High-Risk-AI-Classification.pdf (zuletzt aufgerufen am 4.10.2022).

[99] Stefano, The EU Proposed Regulation on AI: a threat to labour protection?, abrufbar unter: http://global-workplace-law-and-policy.kluwerlawonline.com/2021/04/16/the-eu-proposed-regulation-on-ai-a-threat-to-labour-protection/ (zuletzt aufgerufen am 4.10.2022).

[100] Anhörung des Ausschusses für Digitales des Deutschen Bundestages, Ausschussdrs. 20(23)78, 4.

Nichtregierungsorganisationen gehen sogar so weit, diesen Bereich in die **Nähe zum Social Scoring** des Art. 5 Abs. 1 Buchst. c KI-VO-E zu rücken, da dort ebenfalls eine umfassende Bewertung einer Person auf der Grundlage einer Vielzahl von Kriterien erfolgt.[101]

KI-Systeme zur **Kreditwürdigkeitsprüfung** und **Kreditpunktebewertung** kleiner Anbieter für den **Eigenbedarf** erfasst Nr. 5 Buchst. a, b und c KI-VO-E nicht. Die Kommission fürchtet bei einem solchen KI-Einsatz keine schwerwiegenden Konsequenzen (Erwgr. Nr. 37 S. 4 KI-VO-E).[102] Der „IMCO"-Ausschuss sowie der „LIBE"-Ausschuss des Europäischen Parlaments bewerten dies anders: Sie möchten solche Systeme in den Anwendungsbereich der Regeln für Hochrisiko-KI-Systeme einbeziehen.[103] 72

Nicht nur die Beurteilung der Kreditwürdigkeit ist mit hohen Risiken behaftet, sondern ebenso Vorgänge, die **Betrugsrisiken** erfassen oder die die **Berechnung der Beiträge** übernehmen, die Kunden zu zahlen haben. Es wäre daher sachgerecht, sie ebenfalls in den Katalog aufzunehmen.[104] Zudem nennt Erwgr. Nr. 37 S. 2 KI-VO-E lediglich Wohnraum, Elektrizität und Telekommunikationsdienstleistungen als betroffene Bereiche, nicht jedoch bspw. **Versicherungen**[105] oder die Versorgung mit anderen **Energieträgern,** wie Fernwärme oder Gas. Es ist angezeigt, diese Bereiche gleichermaßen in die KI-VO zu integrieren.[106] 73

Besondere Aufmerksamkeit lässt der KI-VO-E demgegenüber bereits jetzt solchen Systemen zuteilwerden, die die Auswahl vornehmen, welche Einsätze (ggf. in welcher Reihenfolge) **Not- und Rettungsdienste** erledigen sollen (Anhang III Nr. 5 Buchst. c KI-VO-E). Denn sie treffen in äußerst kritischen Situationen Entscheidungen über Leib, Leben und Eigentum natürlicher Personen (Erwgr. Nr. 37 S. 9 KI-VO-E). Der Katalog ist aber bislang lückenhaft. Systeme, die im Gesundheitswesen im Rahmen einer **Triage**-Situation Anwendung finden, erfasst er nicht.[107] Diese Lücke sollte die KI-VO schließen. So schlagen es (nicht zuletzt als Lehre aus der Covid-19-Pandemie) auch der „IMCO"-Ausschuss sowie der „LIBE"-Ausschuss des Europäischen Parlaments zu Recht ergänzend vor.[108] 74

d) Strafverfolgung (Anhang III Nr. 6 KI-VO-E)

KI-Systeme, die für Zwecke der Strafverfolgung zum Einsatz kommen, sind von einem besonderen **strukturellen Machtungleichgewicht** zwischen Anwendern und Betroffenen gekennzeichnet (Erwgr. Nr. 38 S. 1 KI-VO-E). Die Folgen, die sie für Betroffene auslösen, sind häufig schwerwiegend und die Auswirkungen auf Grundrechte, insbes. auf die verfahrensrechtlichen Grundrechte – bspw. die Unparteilichkeit der Gerichte, die Unschuldsvermutung oder Verteidigungsrechte (Erwgr. Nr. 38 S. 3 KI-VO-E) – sind erheb- 75

[101] Muller/Schöppl/Avramidou/Talvitie/Férnandez Peñalver, AIA in-depth 20.4.2020, 10, abrufbar unter: https://allai.nl/wp-content/uploads/2022/04/AIA-in-depth-3a-High-Risk-AI-Classification.pdf (zuletzt aufgerufen am 4.10.2022). Vgl. auch den Vorschlag der slowenischen Ratspräsidentschaft (→ Rn. 30 mit Fn. 51).

[102] Erwgr. Nr. 37 S. 4 KI-VO-E.

[103] Draft Report on the proposal for a regulation of the European Parliament and of the Council on harmonised rules on Artificial Intelligence (Artificial Intelligence Act), PE731.563, 2021/0106(COD), 2022, Änderungsanträge Nr. 24, 290.

[104] Muller/Schöppl/Avramidou/Talvitie/Férnandez Peñalver, AIA in-depth, 2020, 10, abrufbar unter: https://allai.nl/wp-content/uploads/2022/04/AIA-in-depth-3a-High-Risk-AI-Classification.pdf (zuletzt aufgerufen am 4.10.2022).

[105] Vgl. auch Draft Report on the proposal for a regulation of the European Parliament and of the Council on harmonised rules on Artificial Intelligence (Artificial Intelligence Act), PE731.563, 2021/0106(COD), 2022, Änderungsanträge Nr. 291; Erwgr. Nr. 37 Ratsdok. 14278/21.

[106] Muller/Schöppl/Avramidou/Talvitie/Férnandez Peñalver, AIA in-depth, 2020, 10, abrufbar unter: https://allai.nl/wp-content/uploads/2022/04/AIA-in-depth-3a-High-Risk-AI-Classification.pdf (zuletzt aufgerufen am 4.10.2022).

[107] Draft Report on the proposal for a regulation of the European Parliament and of the Council on harmonised rules on Artificial Intelligence (Artificial Intelligence Act), PE731.563, 2021/0106(COD), 2022, Änderungsantrag Nr. 292.

[108] Draft Report on the proposal for a regulation of the European Parliament and of the Council on harmonised rules on Artificial Intelligence (Artificial Intelligence Act), PE731.563, 2021/0106(COD), 2022, Änderungsantrag Nr. 292.

lich. Auch deshalb wählt der KI-VO-E für den Bereich der Strafverfolgung einen enumerativen Ansatz. Er benennt gezielt alle Einsatzgebiete, die ein hohes Risiko bergen.

76 Was der Verordnungsentwurf unter „Strafverfolgung" versteht, **definiert** Art. 3 Nr. 41 KI-VO-E legal: Der Topos beschreibt „Tätigkeiten der Strafverfolgungsbehörden", die Straftaten verhüten, ermitteln, aufdecken oder verfolgen sollen oder der Strafvollstreckung dienen. Auch Maßnahmen, die Gefahren für die öffentliche Sicherheit abwehren oder vor ihnen schützen sollen, zählt der KI-VO-E dazu – dies aber nicht generell, sondern (ebenso wie im Falle der JI-RL [RL (EU) 2016/680], welche sich der gleichen Terminologie bedient, Art. 1 Abs. 1 RL (EU) 2016/680) nur insoweit, als ein Bezug zur Aufklärung oder Verfolgung von Straftaten besteht, also die **kriminalpräventive Gefahrenabwehr** betroffen ist.[109] Die klassische Dichotomie zwischen Polizeirecht und Strafrecht ist dem Unionsrecht ohnedies nicht in gleicher Weise wie dem deutschen Recht vertraut.

77 Zu den Hochrisiko-Anwendungen zählt der KI-VO-E insbes. Systeme, die **Vorhersagen** über künftiges strafbares Verhalten treffen (Anhang III Nr. 6 Buchst. a KI-VO-E). Als hochriskant stuft er zudem Systeme ein, welche eine **Profilbildung** im Hinblick auf potenzielle künftige Straftäter und Straftaten vornehmen (Anhang III Nr. 6 Buchst. e KI-VO-E) oder dazu beitragen sollen, bereits begangene Straftaten aufzudecken, zu ermitteln oder zu verfolgen (Anhang III Nr. 6 Buchst. f KI-VO-E). Gleiches gilt für Systeme, die Datensätze durchsuchen, um **Muster** zu erkennen und damit die Kriminalanalyse natürlicher Personen zu unterstützen (Anhang III Nr. 6 Buchst. g KI-VO-E). Ein Beispiel dafür ist die Software „hessenDATA" des US-Konzerns „Palantir Technologies Inc.", die bei den Polizeibehörden und dem LKA des Landes Hessen im Einsatz ist. Sie wertet große Mengen bereits – rechtmäßig – erhobener personenbezogener Daten verschiedener Quellen zentral und automatisiert aus, um Gefahren für höchstrangige Gemeinschaftsgüter, insbes. den Bestand des Staates sowie das Leben und die Gesundheit natürlicher Personen, abzuwehren (§ 26 Abs. 1 S. 1 HSOG).

78 Auch **Lügendetektoren** sowie **Emotionserkennungssysteme** (Anhang III Nr. 6 Buchst. b KI-VO-E), also Anwendungen, die emotionale Zustände oder Absichten natürlicher Personen auf der Grundlage ihrer biometrischen Daten feststellen oder daraus ableiten sollen (Art. 3 Nr. 34 KI-VO-E), stuft der KI-VO-E zu Recht als hochriskant ein. Der Katalog des Anhangs III Nr. 6 Buchst. b KI-VO-E erfasst darüber hinaus solche Systeme, die **Deepfakes** aufdecken (Anhang III Nr. 6 Buchst. c KI-VO-E) oder die **Verlässlichkeit von Beweismitteln** bewerten (Anhang III Nr. 6 Buchst. d KI-VO-E). Ihnen ist gemein, dass sie die Echtheit von Artefakten klären sollen. Ebenso wie Lügendetektoren und Emotionserkennungssysteme beeinflussen sie bspw. die Beweisaufnahme in gerichtlichen Verfahren.

79 Ob Anhang III Nr. 6 KI-VO-E auch das sog. **„Predictive Policing"** den Art. 8 ff. KI-VO-E unterwirft, ist nicht ganz eindeutig. Der Wortlaut („um das Risiko abzuschätzen, dass eine *natürliche Person*[110] Straftaten begeht") lässt darauf schließen, dass zumindest **Anhang III Nr. 6 Buchst. a KI-VO-E** nur die **individuelle Risikobewertung** und Profilbildung einer natürlichen Person umfasst – nicht hingegen bestimmter Gruppen.[111] Das deutet womöglich darauf hin, dass Systeme, die bestimmte geographische Orte oder Gruppen betreffen, insgesamt nicht dem Anhang III Nr. 6 KI-VO-E unterliegen.[112]

80 Der Wortlaut des **Anhangs III Nr. 6 Buchst. e KI-VO-E** erfasst jedoch zumindest auch das kriminelle Verhalten von Gruppen („vergangenen kriminellen Verhaltens natürlicher Personen oder von Gruppen"). **Erwgr. Nr. 38 S. 5 KI-VO-E** schlägt in die gleiche

---

[109] Vgl. dazu insbes. Martini DÖV 2019, 732 (734 f.).

[110] Hervorhebung d. Verf.

[111] Ebers/Hoch/Rosenkranz/Ruschemeier/Steinrötter RDi 2021, 528 (532).

[112] Ebers/Hoch/Rosenkranz/Ruschemeier/Steinrötter RDi 2021, 528 (532); anders: Draft Report on the proposal for a regulation of the European Parliament and of the Council on harmonised rules on Artificial Intelligence (Artificial Intelligence Act), PE731.563, 2021/0106(COD), 2022, Änderungsanträge Nr. 293, 294; Spindler CR 2021, 361 Rn. 31.

Kerbe: Anwendungen, die kriminelles Verhalten „von natürlichen Personen oder Gruppen" bewerten sollen, gelten als Hochrisiko-KI-System.[113] Indem der Entwurf auch Gruppen und damit auch davon ausgehende raumbezogene Gefahren in seinen Schutzradius einbezieht, unterscheidet er insgesamt nicht strikt zwischen **personenbezogenem** und **raumbezogenem** „Predictive Policing".[114] Mit Blick auf die Risiken dieser Praktiken für die Grundrechte Betroffener sollten jedenfalls de lege ferenda auch solche Systeme das Pflichtenregime der Art. 8 ff. KI-VO-E beachten müssen, die raumbezogen Daten verarbeiten und auf dieser Grundlage Risiken in bestimmten Gegenden konstatieren. Denn „Predictive Policing" kann **strukturelle** und **systematische Diskriminierungen** benachteiligter Bevölkerungsgruppen nach sich ziehen,[115] ggf. sogar gegen die Unschuldsvermutung und die Menschenwürde verstoßen.[116] Obgleich diese Risiken in besonderem Maße personenbezogenem „Predictive Policing" inhärent sind, besteht doch auch beim Einsatz ortsbezogener Systeme die signifikante Gefahr, dass sich Stereotype der Kriminalitätswahrnehmung in Analysesystemen spiegeln und verfestigen[117]. In jedem Falle sollte der Gesetzgeber mit Blick auf das Gebot der Normenklarheit und Bestimmtheit den Verordnungstext noch nachschärfen, um klar abzugrenzen, welche Systeme er den Regeln der Art. 8 ff. KI-VO-E unterwerfen will und damit potenzielle **Rechtsunsicherheiten** beseitigen.

Anhang III Nr. 6 KI-VO-E adressiert ausschließlich Systeme, die zu Zwecken der **Strafverfolgung** zum Einsatz kommen. KI-Systeme, die bspw. als Instrument des **Marketings** oder der **Markterkundung** Anwendung finden, unterliegen (jenseits der Kreditwürdigkeitsprüfung und Kreditpunktebewertung [Anhang III Nr. 5 Buchst. b KI-VO-E]; → Rn. 72) den besonderen Anforderungen der Art. 8 ff. KI-VO-E daher grds. nicht. 81

e) Migration, Asyl und Grenzkontrolle (Anhang III Nr. 7 KI-VO-E)

Ebenso wie bei der Strafverfolgung ist der Einsatz von KI-Systemen im Bereich Migration, Asyl und Grenzkontrolle durch besonders tiefgehende **Abhängigkeitsverhältnisse** zwischen Behörden und Menschen in äußerst prekären Lebenslagen geprägt (Erwgr. Nr. 39 S. 1 KI-VO-E). Schon deshalb berühren sie zahlreiche sensible Grundrechtspositionen, insbes. das Recht auf Asyl aus Art. 18 GRCh. Dass der Entwurf sie als besonders risikobehaftet einstuft, ist daher folgerichtig. Der Anwendungsbereich des Anhangs III Nr. 7 KI-VO-E erstreckt sich auf Anwendungen wie **Lügendetektoren** (bspw. iBorderCtrl[118]) und **Emotionserkennungssysteme** (Anhang III Nr. 7 Buchst. a KI-VO-E) – aber auch auf Systeme, die der **Berechnung des Risikos** („einschließlich eines Sicherheitsrisikos, 82

[113] Auch der „IMCO"-Ausschuss und der „LIBE"-Ausschuss" des Europäischen Parlaments gehen davon aus, dass Anhang III Nr. 6 Buchst. a und Buchst. e KI-VO-E in der aktuellen Entwurfsfassung auf „Predictive Policing" abzielen, die Kommission solche Anwendungen folglich derzeit als Hochrisiko-KI-Systeme einstuft, Draft Report on the proposal for a regulation of the European Parliament and of the Council on harmonised rules on Artificial Intelligence (Artificial Intelligence Act), PE731.563, 2021/0106(COD), 2022, Änderungsanträge Nr. 16, 293, 294. Die Ausschüsse möchten solche Systeme am liebsten via Art. 5 KI-VO-E verboten sehen; Draft Report on the proposal for a regulation of the European Parliament and of the Council on harmonised rules on Artificial Intelligence (Artificial Intelligence Act), PE731.563, 2021/0106(COD), 2022, Änderungsantrag Nr. 76; ebenso Stellungnahme des Deutschen Anwaltvereins Nr. 57/2021, 11.

[114] Vgl. zu dieser Unterscheidung bspw. Singelnstein NStZ 2018, 1.

[115] Diese Systeme dienen gerade dazu, Orte statistischer Häufung von Straftaten zu erkunden, um so die Polizei- und Ordnungsbehörden an kriminalitätsgefährdeten Plätzen zielgenauer einzusetzen. Dies führt dazu, dass Personen, die sich dort aufhalten, leben oder arbeiten, häufiger polizeilichen Kontrollen und dem Einsatz technischer Systeme ausgesetzt sind als Personen, die sich vornehmlich in vermeintlich „sichereren" Gebieten befinden.

[116] Draft Report on the proposal for a regulation of the European Parliament and of the Council on harmonised rules on Artificial Intelligence (Artificial Intelligence Act), PE731.563, 2021/0106(COD), 2022, Änderungsantrag Nr. 16.

[117] Singelnstein NStZ 2018, 1 (4).

[118] Nähere Informationen zum Pilotprojekt finden sich bspw. bei Kolb, EU testet Lügendetektor an den Grenzen, Süddeutsche Zeitung, November 2018, abrufbar unter: https://www.sueddeutsche.de/digital/grenze-kuenstliche-intelligenz-software-iborderctrl-1.4196243 (zuletzt aufgerufen am 4.10.2022).

eines Risikos der irregulären Einwanderung oder eines Gesundheitsrisikos") dienen, das mit der (beabsichtigten) Reise einer natürlichen Person in die Union korreliert (Anhang III Nr. 7 Buchst. b KI-VO-E). Der Bereich umfasst auch Systeme, die Dokumente und Urkunden auf ihre **Echtheit überprüfen** können (Anhang III Nr. 7 Buchst. c KI-VO-E) sowie Anwendungen, die die zuständigen Behörden bei der Bearbeitung von **Anträgen** auf Asyl, Aufenthalt oder Visa unterstützen sollen (Anhang III Nr. 7 Buchst. d KI-VO-E).[119]

83 Nichtregierungsorganisationen bzw. Stiftungen treibt die Sorge um, dass die normativen Sicherungsmechanismen der Kommission für diese Anwendungen nicht streng genug sind, um Immigranten und Schutzsuchende ausreichend gegen Risiken zu immunisieren. Sie appellieren an den Gesetzgeber, spezifischen KI-Systemen bzw. ihrem konkreten Einsatz im Bereich „Migration" gänzlich einen Riegel vorzuschieben und Art. 5 KI-VO-E entsprechend zu erweitern, bspw. um die „individuelle Risikobewertung und Systeme zur Profilerstellung, die auf persönliche und sensible Daten zurückgreifen",[120] und den Katalog der Hochrisiko-KI-Systeme in Anhang III Nr. 7 KI-VO-E um weitere Systemkategorien zu ergänzen[121] – bspw. um Anwendungen, welche der **Überwachung der EU-Grenzen** dienen (bspw. mögliche zukünftige Systeme wie RoBorder[122], Foldout Solution Technology[123], Border UAS[124]).[125] In der Kritik steht insbes., dass der Bereich bisher keine Systeme umfasst, die **Vorhersagen** (zB von Flüchtlingsströmen) treffen sollen oder die zu **Identifizierungszwecken** natürlicher Personen an den Grenzen zur Anwendung kommen.[126] Anhang III Nr. 7 Buchst. b KI-VO-E („Bewertung eines Risikos") sowie Buchst. c KI-VO-E („Überprüfung der Echtheit von Reisedokumenten und Nachweisunterlagen natürlicher Personen") und Buchst. d KI-VO-E („Prüfung von Asyl- und Visumanträgen") erfassen allerdings Risikoermittlungssysteme und Mechanismen zur Identitätsüber-

---

[119] Vgl. Erwgr. Nr. 39 S. 3 KI-VO-E.

[120] Bertelsmann-Stiftung/GMF/Bosch-Stiftung, The EU's AI Act and its Human Rights Impacts on People Crossing Borders, Dialogue on Tech and Migration, A project of the Migration Strategy Group on International Cooperation and Development, June 2022, 7, abrufbar unter: https://www.bosch-stiftung.de/sites/default/files/publications/pdf/2022-06/The%20EUs%20AI%20Act%20and%20Its%20Human%20Rights%20Impacts.pdf (zuletzt aufgerufen am 4.10.2022); der DAV möchte viele der von der Kommission als besonders risikoreich eingestuften Systeme mit einem generellen Verbot belegt sehen: Stellungnahme des Deutschen Anwaltvereins Nr. 57/2021, 16.

[121] Bertelsmann-Stiftung/GMF/Bosch-Stiftung, The EU's AI Act and its Human Rights Impacts on People Crossing Borders, Dialogue on Tech and Migration, A project of the Migration Strategy Group on International Cooperation and Development, June 2022, 7 abrufbar unter: https://www.bosch-stiftung.de/sites/default/files/publications/pdf/2022-06/The%20EUs%20AI%20Act%20and%20Its%20Human%20Rights%20Impacts.pdf (zuletzt aufgerufen am 4.10.2022).

[122] Dabei handelt es sich um ein Projekt, das auf ein Grenzschutzsystem abzielt, welches ua unbemannte Roboter an Land, im Wasser und in der Luft einsetzt, vgl. https://roborder.eu/ (zuletzt aufgerufen am 4.10.2022); vgl. auch EU-Projektbeschreibung iRv Horizon 2020, abrufbar unter: https://cordis.europa.eu/project/id/740593 (zuletzt aufgerufen am 4.10.2022).

[123] Vgl. auch https://foldout.eu/ (zuletzt aufgerufen am 4.10.2022); Bolakis et al. in Akhgar/Kavallieros/Sdongos, Technology Development for Security Practitioners. Security Informatics and Law Enforcement, 2021, abrufbar unter: https://doi.org/10.1007/978-3-030-69460-9_16 (zuletzt aufgerufen am 4.10.2022); vgl. auch EU-Projektbeschreibung iRv Horizon 2020, abrufbar unter: https://cordis.europa.eu/project/id/787021/de (zuletzt aufgerufen am 4.10.2022).

[124] Dabei handelt es sich um ein Projekt, welches ein „unbemanntes Mehrzweckluftfahrzeug (leichter als Luft) [entwickelt], das über eine ultrahochauflösende Mehrfachsensor-Überwachungsnutzlast verfügt", EU-Projektbeschreibung iRv Horizon 2020, abrufbar unter: https://cordis.europa.eu/project/id/883272/de (zuletzt aufgerufen am 4.10.2022); vgl. https://borderuas.eu (zuletzt aufgerufen am 4.10.2022).

[125] Access Now/European Digital Rights (EDRi), Migration and Technology Monitor, the Platform for International Cooperation on Undocumented Migrants (PICUM) and Statewatch, Paper on Uses of AI in migration and border control: A fundamental rights approach to the Artificial Intelligence Act, abrufbar unter: https://edri.org/wp-content/uploads/2022/05/Migration_2-pager-02052022-for-online.pdf (zuletzt aufgerufen am 4.10.2022).

[126] S. bspw. European Digital Rights, Regulating Migration Tech: How the EU's AI Act can better protect people on the move, May 2022, abrufbar unter: https://edri.org/our-work/regulating-migration-tech-how-the-eus-ai-act-can-better-protect-people-on-the-move/ (zuletzt aufgerufen am 4.10.2022).

prüfung zumindest teilweise. **Emotionserkennungssysteme** muss der Unionsgesetzgeber auch nicht pauschal verbieten. Mit Blick auf ihre hohe Fehlerquote und die Sensibilität der Entscheidung, die sie treffen, sollten die Regelungen für Hochrisiko-KI-Systeme jedoch jedenfalls um besondere Anforderungen ergänzt werden. Insbes. sollten solche Systeme grds. nur zum Einsatz kommen, wenn Betroffene dem Einsatz zustimmen.

f) Rechtspflege und demokratische Prozesse (Anhang III Nr. 8 KI-VO-E)

KI-Systeme machen auch vor der Justiz nicht Halt. Ihr Einsatz kann rechtsstaatliche und demokratische Prozesse gefährden. Neben den individuellen Freiheiten natürlicher Personen kann Rechtspflege-KI die **Justizgrundrechte,** bspw. das Recht auf einen wirksamen Rechtsbehelf und ein unparteiisches Gericht (Art. 47 GRCh), verletzen (Erwgr. Nr. 40 S. 1 KI-VO-E). Der KI-VO-E stuft solche Systeme daher als hochriskant ein, soweit sie dabei unterstützen sollen, Sachverhalte und Rechtsvorschriften zu ermitteln und das Recht auf konkrete Lebenssachverhalte herunterzubrechen (Erwgr. Nr. 40 S. 2 KI-VO-E). 84

Die Überschrift des Anhangs III Nr. 8 KI-VO-E spricht allgemein von der „Rechtspflege" und adressiert somit nicht nur Gerichte iSd Art. 47 GRCh, sondern auch **Justizbehörden** („judicial authority"), insbes. Staatsanwaltschaften und Rechtspfleger.[127] In Deutschland treibt den Bundesrat deshalb die Sorge um, dass in Zukunft nahezu jeder Einsatz von KI in Justizbehörden in den Anwendungsbereich der VO fallen könnte (bspw. auch eine „bloße Unterstützungshandlung").[128] Er fürchtet eine inkonsistente „Unterbetonung des Gefährdungsvektors bei einer Überbetonung des Einsatzbereiches, da [die Definition] ohne Differenzierung den größten Teil des gesamten Tätigkeitsbereichs der Justiz erfasst".[129] 85

Ganz so weit und diffus, wie der Anwendungsbereich auf den ersten Blick wirkt, ist er bei näherer Betrachtung jedoch nicht. Er erstreckt sich **nicht allgemein** auf jegliche Tätigkeit in einer Justizbehörde. Voraussetzung ist vielmehr, dass die KI-Anwendung dabei unterstützt, „Sachverhalte und Rechtsvorschriften zu ermitteln und auszulegen"[130] bzw. dass das System in die **konkrete Subsumtion** eines zu entscheidenden Sachverhalts eingebunden ist (Erwgr. Nr. 40 S. 2 KI-VO-E). KI-Systeme, die lediglich in der allgemeinen Justizverwaltung, zB beim Geschäftsverteilungsplan oder der Zuteilung von Haushaltsressourcen oder für begleitende Verwaltungstätigkeiten zur Anwendung kommen, klassifiziert der Entwurf bewusst nicht als hochriskant. Paradigmatisch hierfür nennt er etwa die „Anonymisierung oder Pseudonymisierung gerichtlicher Urteile" oder „die Kommunikation zwischen dem Personal" (Erwgr. Nr. 40 S. 3 KI-VO-E). Der Entwurf sollte aber auch nicht jegliche Unterstützungsfunktionen einer KI bei der Subsumtion unter einen konkreten Sachverhalt als Hochrisiko-KI-System erfassen, sondern für den Graubereich klare Grenzlinien der Kritikalität definieren. 86

Indem Anhang III Nr. 8 Buchst. a KI-VO-E lediglich auf den Einsatz von KI-Systemen in Justizbehörden rekurriert, erfasst er auch den immer wichtiger werdenden Bereich der Automatisierung juristischer Tätigkeiten in der Rechtspflege durch Private **(„Legal Tech")**[131] nicht. Mit Blick auf die hohen Risiken, die sich mit dem Einsatz automatisierter Instrumente der Rechtsdurchsetzung verknüpfen (insbes. nachhaltige Schäden für die Rechtsdurchsetzung, die fehlerhafte Anwendungen hervorrufen können), ist das nicht sachgerecht. Es wäre vielmehr angezeigt, diese grds. in den Anwendungsbereich des Anhangs III Nr. 8 KI-VO-E einzubeziehen. 87

---

[127] Dazu auch (die Frage offen lassend) Conrad/Pickens/Baron/Henseler/Linna/Vinjumur/Schwemer/Tomada/Pasini, Automated Semantic Analysis of Information in Legal Text & AI and Intelligent Assistance for Legal Professionals in the Digital Workplace 2021 2021, Legal AI Systems in the EU's proposed Artificial Intelligence Act, 53 f.

[128] BR-Drs. 488/1/21, 21 f.

[129] BR-Drs. 488/1/21, 21 f.

[130] Erwgr. Nr. 40 S. 2 KI-VO-E.

[131] Ausf. zu Legal Tech und KI-VO-E (nicht nur in Hinblick auf den Einsatz durch Private) vgl. bspw. Engelmann/Brunotte/Lütkens RDi 2021, 317.

88 So sehr die Überschrift „Rechtspflege und demokratische Prozesse" raumgreifend weit formuliert ist, so wenig löst sie diesen Anspruch im Ergebnis ein; obgleich Anhang III Nr. 8 KI-VO-E nicht nur von der Rechtspflege, sondern auch von „demokratische[n] Prozesse[n]" spricht, benennt er keine KI-Systeme außerhalb von Justizbehörden. Sachgerecht wäre es, in dem Katalog auch KI-Anwendungen zu rubrizieren, welche die **demokratische Meinungsbildung** steuern – insbes. Systeme, die iRv Wahlen eingesetzt werden, um zB Wähler bei ihrer Stimmabgabe zu beeinflussen.[132]

3. Zwischenergebnis und Kritik

a) Heterogene Sammlung

89 Die Anhänge II, III KI-VO-E bündeln in ihren Katalogen einen bunten Strauß teils sehr verschiedenartiger KI-Anwendungen. Den **eigenständigen Systemen,** die Anhang III KI-VO-E auflistet, ist überwiegend das hohe Risiko ihrem **Zweck** eingeschrieben: Sie sollen in sensiblen Entscheidungskontexten über die Verwirklichung von Lebenschancen entscheiden, bspw. über den Zugang zu Bildung, Arbeitsplätzen oder öffentlichen Unterstützungsleistungen. Auch bei **planmäßigem, korrektem Gebrauch** sind die Auswirkungen der Systeme bzw. ihres konkreten Einsatzes gravierend.

90 Andere Anwendungen – vor allem diejenigen im Kontext des Produktsicherheitskonzepts, aber auch bspw. diejenigen des Anhangs III Nr. 2 Buchst. a KI-VO-E (Verwaltung und Betrieb kritischer Infrastrukturen) – bergen primär ein hohes Risiko im Hinblick auf mögliche **Fehlfunktionen.**[133] Darin offenbaren sich zwei unterschiedliche Zielsetzungen der Hochrisiko-Regeln: Gegen Systeme, die schon nach ihrer Zweckbestimmung riskant sind, können andere Abwehrmechanismen („Resistenz") erforderlich sein als gegen Systeme, die (nur) im Störungsfall besondere Risiken bergen („Resilienz").[134] Das machen bspw. die **Transparenzanforderungen** des Art. 13 Abs. 1 KI-VO-E deutlich, die Nutzer eines KI-Systems in die Lage versetzen sollen, dessen Ergebnisse angemessen zu interpretieren und zu verwenden. Bei einem KI-System, das routinemäßig primär eine Sicherheitsfunktion erfüllen soll, ist der Nutzen der Transparenzregelungen für die Zielsetzung, einen sicheren Betrieb zu ermöglichen, sehr begrenzt, für andere Systeme demgegenüber hoch. Womöglich ist das regulatorische Dach, das der KI-VO-E über die **disparaten Systeme** spannt, insoweit noch etwas zu weit.

91 Dass die Gruppe der Hochrisiko-KI-Systeme sehr breitgefächert ist und eine Vielzahl unterschiedlicher Systeme adressiert, war auch der Kommission bewusst. Das zeigt sich ua daran, dass der KI-VO-E für biometrische Identifizierungssysteme innerhalb seiner Hochrisiko-Vorschriften **Sonderregeln** statuiert (→ Rn. 57) oder Sondervorschriften für Systeme vorhält, die ihre Lernfähigkeit auch nach dem Inverkehrbringen noch aufrechterhalten (Art. 15 Abs. 3 UAbs. 3 KI-VO-E). Manche Vorschriften für weniger risikobehaftete Systeme sollen wiederum neben denjenigen für Hochrisiko-KI-Systeme anwendbar sein (Art. 52 Abs. 4 KI-VO-E).[135] Insofern schlägt der KI-VO-E jedenfalls innerhalb der Risikostufe nicht alle Systeme pauschal über einen Leisten, sondern nimmt bereits **Binnendifferenzierungen** vor. Das hat zwar seinen Preis: Die Rechtsanwender können nicht auf den ersten Blick erkennen, welche konkreten normativen Vorgaben für ein bestimmtes KI-System im Einzelnen gelten. Allerdings justieren diese Abstufungen – im Einklang mit

---

[132] IdS der „IMCO"-Ausschuss sowie der „LIBE"-Ausschuss des Europäischen Parlaments, Draft Report on the proposal for a regulation of the European Parliament and of the Council on harmonised rules on Artificial Intelligence (Artificial Intelligence Act), PE731.563, 2021/0106(COD), 2022, Änderungsantrag Nr. 26, Erwgr. Nr. 40: „[...] to influence the votes of natural persons in local, national or European Parliament elections or for the purpose of vote counting and processing in such elections [...]".

[133] Vgl. Floridi Philosophy & Technology 2021, 215 (219).

[134] Floridi Philosophy & Technology 2021, 215 (219).

[135] → Rn. 134.

dem Konzept des risikobasierten Ansatzes – das Regelungsprogramm des KI-VO-E präziser an die betroffenen Systeme aus.

Der Kompromissvorschlag der tschechischen Ratspräsidentschaft trägt noch zusätzliche **Einschränkungen** des Anwendungsbereichs der Hochrisiko-KI-Systeme in die Diskussion.[136] Eine weitere Ebene („another horizontal layer") in der Definition der Hochrisiko-KI-Systeme soll bereichsübergreifend diejenigen Systeme aussortieren, deren verminderte Kritikalität die Anwendung der Hochrisiko-Regeln nur in eingeschränktem Maße zu rechtfertigen vermag. Die eigenständigen Systeme des Art. 6 Abs. 2 KI-VO-E sollen nur dann als hochriskant gelten, wenn eine von zwei **zusätzlichen Voraussetzungen** erfüllt ist: Entweder muss die Entscheidung des KI-Systems **unmittelbar** ihre Wirksamkeit entfalten, ohne dass ein Mensch dieses Ergebnis überprüft. Oder aber der Output des Systems bildet die einzige Entscheidungsbasis bzw. steuert die Entscheidung in mehr als nur untergeordneter Weise („not purely accessory"), sodass zusätzlich ein **erhebliches** („significant") Risiko für Gesundheit, Sicherheit oder Grundrechte entsteht. Diese Änderungsinitiative verkleinert die Gruppe der Hochrisiko-KI-Systeme substanziell: Nur diejenigen Systeme, die tatsächlich über Entscheidungsmacht verfügen, sollen den strengen normativen Vorgaben für Qualitätsanforderungen unterfallen. Diese zusätzliche Voraussetzungsebene kann im Idealfall dafür sorgen, die Anwendungsbereiche der einzelnen Kategorien des Anhangs III flexibel und punktgenau nachzuschärfen. Allerdings geht die normative Wirkkraft der KI-VO dann in vielen Bereichen nicht hinreichend über die bereits bestehende datenschutzrechtliche Regelung des Art. 22 DS-GVO für vollautomatisierte Systeme hinaus. 92

b) Regelungslücken

Gravierende Schutzlücken lässt die Liste der erfassten Systeme nicht zurück. Dennoch gibt es einige sensible Anwendungsfelder von KI-Systemen, welche Anhang III KI-VO-E vermissen lässt.[137] Eine wichtige Kategorie, die Art. 6 KI-VO-E iVm Anhang III KI-VO-E bspw. bisher nicht als solche erfasst, sind Emotionserkennungssysteme im Marketing sowie im Gesundheitssektor ebenso Systeme, die **Deepfakes** generieren, also eigens erzeugte oder manipulierte Video- und Audioaufnahmen von existierenden Personen, die echt erscheinen und die Realität verzerren.[138] Diese Anwendungen unterfallen derzeit grds. lediglich den Transparenzanforderungen für KI-Systeme mit geringen Risiken (Art. 52 Abs. 3 KI-VO-E; → Rn. 128 ff.). Auch **Legal Tech-Systeme,** die Rechtsdienstleistungen automatisieren, sowie Systeme, die auf die **demokratische Willensbildung,** insbes. Wahlen, erheblichen Einfluss nehmen, nimmt die KI-Verordnung in ihrer bisherigen Fassung nicht hinreichend unter ihren regulatorischen Schutzschirm. 93

c) Abgrenzung zwischen den Risikogruppen

Aller Mühe des KI-VO-E um Detailtreue zum Trotz: Eine trennscharfe Abgrenzung zwischen den Risikogruppen des Stufensystems der KI-VO wird nicht immer bruchfrei möglich sein. Die Verordnung läuft dadurch Gefahr, dass Anbieter eines KI-Systems, das sich nicht eindeutig zuordnen lässt, **Anforderungen unterlaufen.** Der Rechtsausschuss des Europäischen Parlaments hat daher aus gutem Grund vorgeschlagen, bereits an prominenter Stelle (jedenfalls in den Erwägungsgründen) klarzustellen, dass KI-Systeme, die aufge- 94

[136] Ratsdok. 11124/22.

[137] Diese lassen sich auch nicht nachträglich durch Änderungen der Kommission (Art. 7 KI-VO-E) dem Schutz der Verordnung unterstellen. Denn die Kommission darf die betroffenen Lebensbereiche nicht erweitern; → Rn. 106 ff.

[138] Vgl. auch Draft Report on the proposal for a regulation of the European Parliament and of the Council on harmonised rules on Artificial Intelligence (Artificial Intelligence Act), PE731.563, 2021/0106(COD), 2022, Änderungsanträge 27, 297. Systeme, die Strafverfolgungsbehörden helfen sollen, Deepfakes aufzudecken, erfasst der Entwurf demgegenüber sehr wohl (s. Anhang III Nr. 6 Buchst. c KI-VO-E).

listete Zwecke mit hohem Risiko und nicht aufgelistete Zwecke mit geringem Risiko in sich vereinen, „vollständig unter Titel III dieser Verordnung fallen sollte[n], wenn diese Zwecke untrennbar miteinander verbunden sind."[139] Ebenso adressiert der KI-VO-E derzeit noch nicht hinreichend klar den Fall, in dem **zwei oder mehrere KI-Systeme,** die einzeln bzw. unabhängig voneinander zwar nur gering risikobehaftet sind, bei gemeinsamer Verwendung bzw. im Falle einer Verknüpfung aber hohe Risiken bergen.[140] Sachgerecht sind auch Regeln für ein Negativattestverfahren, mit dessen Hilfe Anwender für Zweifelsfälle eine behördliche Bescheinigung über die Risikoklassenzuordnung ihres KI-Systems erhalten können, die Rechtssicherheit schafft (vgl. etwa die Blaupause des § 54 Abs. 1 S. 2 MStV).

d) EU-Regelungskompetenz für den Einsatz von KI durch staatliche Stellen

95 Anhang III KI-VO-E richtet sein regulatorisches Fadenkreuz in erheblichem Umfang auf sicherheitssensitive Anwendungen des öffentlichen Sektors aus. Er trifft insbes. Vorgaben für die Strafverfolgung (Anhang III Nr. 6 KI-VO-E) sowie für die polizeiliche Gesichtserkennung (Anhang III Nr. 1 KI-VO-E).[141] Damit wirkt die Union im Wege unmittelbar geltender Normen nachhaltig in den Kernbereich **nationaler Sicherheitsstrategien** und damit in die Regelungskompetenz der Mitgliedstaaten hinein.

96 Das Sicherheitsrecht konstituiert als nationale Kernkompetenz die **Eigenstaatlichkeit der Mitgliedstaaten.**[142] Aus diesem Grund begrenzen die Verträge die unionale Kompetenz auf diesem Feld ausdrücklich (vgl. insbes. Art. 4 Abs. 2, 3 EUV („achtet [...] den Schutz der nationalen Sicherheit"); Art. 67 ff. AEUV). Für die Polizei verfügt die Union bspw. nur über die Befugnis, die **grenzüberschreitende polizeiliche Zusammenarbeit** zu regeln (Art. 87 ff. AEUV). Auch im Bereich der **justiziellen Zusammenarbeit** in Strafsachen zeigt der Grundsatz der gegenseitigen Anerkennung gerichtlicher Urteile und Entscheidungen implizit die Grenzen der unionalen Kompetenz auf (vgl. Art. 82 ff. AEUV). Als Ausfluss des **Subsidiaritätsprinzips** (Art. 5 Abs. 1 S. 2 EUV, Art. 69 EUV) betonen die Verträge im Bereich des Titels „Raum der Freiheit, der Sicherheit und des Rechts" explizit, dass die Mitgliedstaaten dafür zuständig bleiben, die öffentliche Ordnung und den Schutz der inneren Sicherheit aufrechtzuerhalten (vgl. Art. 72 AEUV).

97 Der KI-VO-E basiert nicht auf den spezifischen Normen des Titels V des AEUV. Vielmehr stützt er sich auf die **Binnenmarktkompetenz** aus Art. 114 Abs. 1 AEUV (vgl. Erwgr. Nr. 2 S. 3 f. KI-VO-E) sowie – hinsichtlich der konkreten Vorschriften, die bspw. bei der biometrischen Echtzeit-Fernidentifizierung, dem Schutz von Privatpersonen im Hinblick auf die Verarbeitung personenbezogener Daten dienen – ergänzend die **Datenschutzkompetenz** aus Art. 16 Abs. 2 AEUV[143].[144]

98 Eine tragfähige Grundlage liefert Art. 114 Abs. 1 AEUV für die Regeln des KI-VO-E, die in den Bereich der nationalen Sicherheit hineinwirken, seinem Wesen nach nur dann,

---

[139] Draft Opinion of the Committee on Legal Affairs, PE719.827, 2021/0106(COD), 2022, Erwgr. Nr. 6a.

[140] ALLAI, Hearing on the EU regulation on artificial intelligence, Anhörung des Ausschusses für Digitales des Deutschen Bundestages 26.9.2022, Deutscher Bundestag Ausschussdrucksache 20(23)84, 2, abrufbar unter: https://www.bundestag.de/resource/blob/912074/cac065ca1cd3c71cff76d17c90e1efa2/Stellungnahme-Muller-data.pdf (zuletzt aufgerufen am 4.10.2022).

[141] In Teilen gilt das darüber hinaus ua ebenfalls für die Vorgaben zur Rechtspflege (Anhang III Nr. 8 KI-VO-E) und im Bildungsbereich (Anhang III Nr. 3 KI-VO-E), dort ist jedoch nicht die nationale Sicherheit betroffen.

[142] S. dazu etwa Martini NVwZ-Extra 2/2022, 1 (16); vgl. auch BVerfGE 123, 267 (359) Rn. 252.

[143] Albers vertritt die Auffassung, dass Art. 16 Abs. 2 AEUV im „systematischen Zusammenhang [...] (nur) eine moderate Erweiterung dahin [schafft], dass er Regelungen insoweit zulässt, als sie im Sinne eines Mindeststandards die Bedingungen der Möglichkeit dafür gewährleisten, dass die justizielle und polizeiliche Zusammenarbeit in der Union und der Daten- und Informationsaustausch entsprechend den dafür geltenden normativen Maßstäben und sachgerecht laufen und laufen können." BeckOK DatenschutzR/Albers Grundlagen und bereichsspezifischer Datenschutz Syst. L Rn. 37 mwN.

[144] Begr. Nr. 2.1 KI-VO-E.

wenn sie darauf gerichtet sind, die Funktionsfähigkeit des Binnenmarkts zu unterstützen (vgl. Art. 114 Abs. 1 AEUV). Der **Markt** für KI-Systeme ist, auch in Bereichen, die die nationale Sicherheit betreffen, **europäisch** – dies schon deshalb, weil Nutzer – auch staatliche Akteure – KI-Systeme als Produkte und digitale Dienste in verschiedenen Ländern erwerben und einsetzen können (vgl. Erwgr. Nr. 2 S. 1 KI-VO-E). Für Unternehmen, die entsprechende Systeme entwickeln und verschiedenen nationalen Behörden anbieten möchten, sind daher unionsweit **einheitliche Anforderungen** von besonderem Interesse. Nur so können sie auch die Skaleneffekte, die digitale Produkte in sich bergen, wirksam nutzen. Divergierende rechtliche Rahmenbedingungen zwängen Unternehmen dazu, für jedes Land ein individuelles KI-System zu konzipieren. Schließlich greifen die Regulierungen zumeist tief in die Grundstrukturen und den gesamten Entwicklungsprozess der Systeme ein.

Der KI-VO-E möchte die Interessen der Mitgliedstaaten auf supranationaler Ebene **bündeln,** um ihnen den Anreiz zu nationalen Alleingängen bei der Gesetzgebung für KI-Systeme zu nehmen. So verhindert die Union auf diesem potenzialträchtigen Feld eine „Fragmentierung des Binnenmarkts".[145] Der Kommissionsentwurf schreibt damit aber auch eine Entwicklung fort, die sich bereits im Rahmen und bei Erlass der RL (EU) 2016/680[146] abzeichnete: ein „Paradigmenwechsel [...] hin zu einer Harmonisierung"[147] und damit zu einer „Europäisierung"[148] des Sicherheitsrechts. 99

Weder die Datenschutzkompetenz der Union aus Art. 16 Abs. 2 AEUV noch ihre Binnenmarktkompetenz aus Art. 114 Abs. 1 AEUV ändern jedoch etwas daran, dass Kernfragen der nationalen Sicherheit den Mitgliedstaaten vorbehalten bleiben.[149] Die Kompetenznormen stehen vielmehr unter dem Vorbehalt, die **Kompetenz der Mitgliedstaaten für die nationale Sicherheit** nicht anzutasten. Auch die Erklärung Nr. 20 zum Vertrag von Lissabon bekräftigt ausdrücklich, dass „immer dann, wenn Bestimmungen über den Schutz personenbezogener Daten, die auf der Grundlage von Artikel 16 zu erlassen sind, direkte Auswirkungen auf die nationale Sicherheit haben könnten, dieser Umstand gebührend zu berücksichtigen ist."[150] 100

Eine anerkannte trennscharfe Definition nationaler Sicherheit, die den Kompetenzrahmen für die Mitgliedstaaten bzw. die Union klar absteckt, besteht allerdings nicht. Der **EuGH** legt dem Topos der nationalen Sicherheit ein enges Verständnis zugrunde. Sein 101

---

[145] Begr. Nr. 2.1 KI-VO-E; Linardatos stellt insgesamt in Frage, ob – da die meisten Mitgliedstaaten noch keine KI-Regulierung getroffen haben – überhaupt eine Zersplitterung durch unterschiedliche Regelungen in den Mitgliedstaaten vorliegt, „andernfalls fände keine Rechtsangleichung iSd. Art. 114 Abs. 1 AEUV statt, sondern die Setzung von Einheitsrecht. [...]", vgl. Linardatos GPR 2022, 58; anders Hofmeister DVBl 2022, 625 (626), der eine baldige Regulierung als wichtig erachtet, um die Fragmentierung des Binnenmarktes abzuwenden; Spindler betont, dass diese Vorgehensweise derjenigen des Produktsicherheitsrechts gleichsteht (Spindler CR 2021, 361 Rn. 5).

[146] Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27.4.2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates.

[147] Pfeffer NVwZ 2022, 294 (295).

[148] BeckOK DatenschutzR/Albers Grundlagen und bereichsspezifischer Datenschutz Syst. L Rn. 22.

[149] Eine ähnl. geartete Diskussion fand bereits iRd RL (EU) 2016/680 zum Datenschutz in Strafsachen statt. Auch hier gingen die Meinungen auseinander, inwieweit sich die Richtlinie auf Art. 16 Abs. 2 AEUV stützen ließ. Kritiker betonten, dass der „Anwendungsbereich des Unionsrechts" gerade nicht eröffnet sei, die Richtlinie vielmehr über die Kompetenzgrenzen der Art. 82 ff. AEUV hinweggehe (bspw. Schantz/Wolff Neues DatenschutzR Rn. 235 f. mit Verweis auf den Bundesrat, BR-Drs. 51/12). Der Bundesrat argumentierte im Rahmen einer Subsidiaritätsrüge nach Art. 69 AEUV im Jahre 2012 gegen den Entwurf der RL (EU) 2016/680 zum Datenschutz in Strafsachen (RL (EU) 2016/680) zusätzlich mit einem systematischen Argument (vgl. BR-Drs. 51/12, 2). Im Hinblick auf die Polizei sei Art. 16 Abs. 2 AEUV in Zusammenhang mit Art. 87 AEUV zu deuten, der insoweit eine Konkretisierung darstelle. Es bedürfe somit immer einer Form der Zusammenarbeit. An dieser mangele es bei rein innerstaatlichen Sachverhalten (BR-Drs. 51/12, 3 (4)). Auch bestehe keine Kompetenz für nicht straftatbezogenes Gefahrenabwehrrecht (BR-Drs. 51/12, 4 (5)).

[150] Erklärung Nr. 20 zum Vertrag von Lissabon.

Kerngehalt erschöpfe sich darin, „die wesentlichen Funktionen des Staates und die grundlegenden Interessen der Gesellschaft [...] zu schützen".[151] In Deutschland hat das Bundesverfassungsgericht demgegenüber ua für das Straf- und Polizeirecht als Kern der grundgesetzlichen Identität zu Recht eine „verfassungsfeste Integrationsschranke"[152] erkannt, die der Kompetenz der Union unverrückbare Grenzen zieht:[153] In ihrem Urteil zum Lissabon-Vertrag postulieren die Richter, dass die Union in Bereichen wie dem Strafrecht sowie dem polizeilichen und militärischen Gewaltmonopol nur agieren dürfe, um einen gehaltvollen nationalen Grundrechtsschutz zu wahren, wenn eine grenzüberschreitende Koordinierung „sachlich notwendig" sei.[154]

102 Der KI-VO-E trifft zwar nicht direkt Entscheidungen über strafwürdiges Verhalten oder das Maß der Strafandrohung. Er begrenzt aber die **Mittel,** derer sich die Mitgliedstaaten bedienen können, um die Strafdrohung auszusprechen. Insoweit schiebt die Souveränität der Mitgliedstaaten der Unionskompetenz für den Bereich der nationalen Sicherheit einen Riegel vor, soweit der Gegenstand nicht notwendig unionsweiter Regelung bedarf, um die gemeinsamen Vertragsziele zu erreichen. Dessen eingedenk hat die **slowenische Ratspräsidentschaft** in ihrem Fortschrittsbericht im November 2021 vorgeschlagen, in Erwgr. Nr. 12 KI-VO-E sowie in Art. 2 KI-VO-E deutlich hervorzuheben, dass die Verordnung nicht für Systeme im Bereich der nationalen Sicherheit iSd Art. 4 Abs. 2 EUV Anwendung findet.[155] Auffällig ist jedoch, dass sie gleichwohl keine Änderungen im Katalog des Anhangs III KI-VO-E bzw. in Art. 5 KI-VO-E vorschlägt. Das deutet darauf hin, dass sie die entsprechenden Systeme nicht (ausschließlich) in dem mitgliedstaatlichen Kompetenzreservat der nationalen Sicherheit verortet.

103 Um die Grenzen, die das Subsidiaritätsprinzip der EU-Gesetzgebung zieht, nicht zu überschreiten, müsste der KI-VO-E den Mitgliedstaaten zumindest **Regelungsspielräume** zugestehen.[156] Solche nationalen Entscheidungskorridore kennt der Entwurf jedoch nicht in ausreichendem Maße.[157] Lediglich *eine* Bereichsausnahme zieht er explizit: Art. 2 Abs. 3 KI-VO-E nimmt solche KI-Systeme aus dem Anwendungsbereich der Verordnung heraus, die ausschließlich für **militärische Zwecke** entwickelt oder verwendet werden. Die Union müsste den Mitgliedstaaten in den sicherheitsrelevanten Bereichen die Möglichkeit eröffnen, in begrenztem Umfang von den „materiellen Anforderungen abweichen zu dürfen.[158] In welchem Ausmaß sich nationaler Protest regen wird, ist offen. Die Erfahrungen mit der Diskussion rund um die EU-Befugnisse in der RL (EU) 2016/680 im Bereich der Gefahrenabwehr und Strafverfolgung zeigen aber, dass jeder Griff in das Hausgut nationaler Sicherheit – ggf. auch in einer späten Phase des Gesetzgebungsverfahrens – nicht ohne Reaktionen bleiben wird.[159]

---

[151] Vgl. bspw. EuGH BeckRS 2022, 24116 Rn. 92. Die Rechtsprechung des EuGH befasst sich zwar mit der Auslegung einer sekundärrechtlichen Norm, legt diese jedoch „im Licht von Art. 4 Abs. 2 EUV" aus, EuGH EuZW 2021, 209 (215 Rn. 136).

[152] Pfeffer NVwZ 2022, 294 (295); Lisken/Denninger PolR-HdB/Müller/Schwabenbauer G. Informationsverarbeitung im Polizei- und Strafverfahrensrecht Rn. 399.

[153] BVerfGE 123, 267 (358).

[154] Die Union dürfe nur bei sachlicher Notwendigkeit und damit nur in grenzüberschreitenden Sachverhalten im Bereich des Strafrechts regulativ tätig werden. Vgl. dazu und insg. zur Europäisierung des Polizeirechts ausf. BVerfG NJW 2009, 2267 (2274 Rn. 251 f.); Pfeffer NVwZ 2022, 294 (295); Terhechte/Schöndorf-Haubold, Verwaltungsrecht der Europäischen Union, 2. Aufl. 2022, 1461 ff.

[155] Art. 2 Abs. 3, Erwgr. Nr. 12 Ratsdok. 14278/21. Ebenso Art. 2 Abs. 3 Ratsdok. 10069/22.

[156] Anders wohl ALLAI, Hearing on the EU regulation on artificial intelligence, Anhörung des Ausschusses für Digitales des Deutschen Bundestages, 2022, Deutscher Bundestag Ausschussdrucksache 20(23)84, 7.

[157] Martini NVwZ-Extra 2/2022, 1 (16).

[158] S. auch Ebers/Hoch/Rosenkranz/Ruschemeier/Steinrötter RDi 2021, 528 (590): „The AIA does not clearly state as to what extent the Member States may deviate from the substantive requirements contained therein, i.e., whether it establishes a framework of full harmonization or whether it is one of minimum harmonization [...]."

[159] Abgeschwächt auch Pfeffer NVwZ 2022, 294 (298). Der Bundesrat weist in seinen Empfehlungen bereits darauf hin, dass die Union „angesichts der äußerst begrenzten Gesetzgebungskompetenz der EU [...] von

II. Erweiterung des Hochrisiko-Katalogs (Art. 7 KI-VO-E)

Die Liste der eigenständigen Hochrisiko-KI-Systeme aus Anhang III KI-VO-E ist **nicht statisch.** Vielmehr kann die Kommission sie auf der Grundlage des Art. 7 KI-VO-E iVm Art. 73 KI-VO-E durch delegierte Verordnung erweitern. 104

Der Grundgedanke, von dem die Vorschrift beseelt ist, überzeugt: KI-Technologien bringen ihrem Wesen nach unvorhergesehene Entwicklungen mit sich. Das Bedürfnis, dem sich dynamisch fortschreibenden Entwicklungsprozess lernfähiger Systeme eine rasche normative Reaktion entgegenzusetzen, ist daher förmlich mit Händen zu greifen. Es der flexibleren **Normsetzung der Kommission** zu überlassen, den Katalog der Hochrisiko-KI-Systeme nachzujustieren, eröffnet die Möglichkeit zeitnaher regulatorischer Anpassung und Feinsteuerung. 105

1. Inhaltliche Grenzen der Änderungsbefugnis

Allem Bemühen um Flexibilität zum Trotz erteilt Art. 7 KI-VO-E der Kommission keine Carte Blanche. Er gibt vielmehr einen Korridor vor, innerhalb dessen die Kommission die Grenzen der abgestuften Kategorien aktualisieren, nachschärfen und verändern kann, um hinreichend dynamisch auf unvorhersehbare und schnelle Weiterentwicklungen Künstlicher Intelligenz reagieren zu können.[160] **Zwei Schutzmechanismen** sind es, welche der Verordnungsentwurf in sein System einzieht, um die Erweiterungen des Hochrisiko-Katalogs an das normative Steuerungsprogramm rückzubinden. 106

Das **Risiko** der neuen Systeme muss zum einen mit Blick auf ihr Potenzial, die **Gesundheit** zu schädigen, die **Sicherheit** zu beeinträchtigen oder sich auf die **Grundrechte** auszuwirken, demjenigen der KI-Systeme des Anhangs III KI-VO-E zumindest **äquivalent** sein. 107

Zum anderen müssen die nachträglich als solche klassifizierten Hochrisiko-KI-Systeme einem der **Bereiche** des Anhangs III Nr. 1–8 KI-VO-E zugehören. Der Kommission ist es also nicht gestattet, weitere Lebensbereiche in den Anwendungsradius der Verordnung aufzunehmen.[161] 108

Die **Kriterien,** die die Kommission heranzuziehen hat, um weitere eigenständige KI-Systeme zu ergänzen, entsprechen denen, die sie bereits bei der Auflistung in Anhang III KI-VO-E geprüft hat (Erwgr. Nr. 32 S. 2 KI-VO-E),[162] insbes. die Zweckbestimmung des Systems, das Ausmaß, in dem es Verwendung findet, sein Einsatzgebiet, die Anzahl der möglichen betroffenen Personen – aber auch die Irreversibilität möglicher Schäden sowie, ob bereits EU-weite Rechtsvorschriften bestehen, welche die fraglichen Risiken des Systems eindämmen (Art. 7 Abs. 2 KI-VO-E). 109

Das Kriterium „Risiko einer erheblichen wirtschaftlichen Schädigung einer Vielzahl von Verbraucherinnen und Verbrauchern"[163] findet sich in dem Katalog der Parameter des Art. 7 Abs. 1 Buchst. b, Abs. 2 KI-VO-E nicht ausdrücklich. Der Bundesrat kritisiert das.[164] Ob die **Regelungslücke** tatsächlich so groß ist, lässt sich allerdings bezweifeln. Immerhin ist bereits bei dem Schädigungsrisiko zu berücksichtigen, inwiefern KI-Systeme geeignet sind, „eine Vielzahl von Personen zu beeinträchtigen" (Art. 7 Abs. 2 Buchst. d KI-VO-E). Auch die Frage, in welchem Maß zwischen Nutzern und Betroffenen eines KI-Systems ein „Ungleichgewicht", bspw. im Hinblick auf eine Machtposition, besteht, ist als Bewertungskriterium heranzuziehen (Art. 7 Abs. 2 Buchst. f KI-VO-E). Eine Lücke 110

einer Regelung {des Einsatzes zu Gefahrenabwehrzwecken und} des strafverfolgungsbehördlichen Einsatzes" absehen solle; vgl. BR-Drs. 488/1/21, 25 Nr. 83 ff.

[160] Martini, Blackbox Algorithmus 2019, 116.

[161] Zu möglichen bisher nicht erfassten Lebensbereichen s. bspw. schon oben, → Rn. 93.

[162] Erwgr. Nr. 32 S. 2 KI-VO-E.

[163] BR-Drs. 488/1/21, 13 Nr. 44.

[164] BR-Drs. 488/1/21, 13 Nr. 44.

weist der Katalog des Art. 7 Abs. 2 KI-VO-E jedoch in Bezug auf die unversehrte **demokratische** Willensbildung sowie die **rechtsstaatlichen** Verfahren und Institutionen auf.[165] Diese sollte der Unionsgesetzgeber schließen.

111 Da sich KI-Systeme dynamisch entwickeln[166] und in alle Lebensbereiche vordringen, lässt sich kaum vorhersagen, worauf sich der Blick der Digitalwirtschaft künftig richten wird. Manche schlagen daher vor, der Kommission auch die Befugnis zuzugestehen, die **Bereiche** des Anhangs III KI-VO-E zu **erweitern** oder **neue hinzuzufügen,** sofern die Gefahren der Systeme einander äquivalent sind.[167] Will man der Kommission – auch mit Rücksicht auf ihre schwache demokratische Legitimation – so viel Rechtsmacht nicht anvertrauen, kann eine Alternative darin bestehen, die Zugehörigkeit eines KI-Systems zu einem der Sektoren lediglich als **Kriterium,** nicht hingegen als zwingende Voraussetzung zu begreifen.[168] Mit den Vorgaben des unionsrechtlichen Primärrechts ließe sich dieses Konzept durchaus vereinbaren. Denn das Unionsrecht zieht den Rahmen dessen, welche Regelungsbefugnisse auf die Kommission übertragen werden dürfen, weiter als bspw. die deutsche Wesentlichkeitslehre aus Art. 80 GG. Es hat bei seinen normativen Delegationsgrenzen weniger den Grundrechtsschutz als politische Kompetenzschranken vor Augen.

112 Der KI-VO-E gesteht der Kommission auch nicht die Kompetenz zu, den Katalog der eigenständigen Hochrisiko-KI-Systeme nachträglich wieder **einzudämmen.** Sofern sich einzelne Regeln als (zB für **kleinere Unternehmen**) nicht hinreichend passgenau erweisen, verbleibt folglich nur das schwerfällige Gesetzgebungsverfahren der Union, um die sich als zu belastend erweisenden Pflichten der Art. 8 ff. KI-VO-E wieder von den Schultern betroffener Beteiligter zu nehmen.

2. Verfahren zur Änderung

113 Der KI-VO-E trägt der Kommission auf, die Liste des Anhangs III KI-VO-E **jährlich** zu **überprüfen** (Art. 84 Abs. 1 KI-VO-E): Sie soll neue technologische Entwicklungen im Blick behalten und diese bei Bedarf den hohen Anforderungen für Hochrisiko-KI-Systeme unterwerfen, sofern sie in einen der acht Bereiche des Anhangs III KI-VO-E fallen.

114 Das **Verfahren,** das zur Anwendung kommt, um die Hochrisiko-Liste zu erweitern, regelt der KI-VO-E jedoch nur **rudimentär:** Er zurrt lediglich fest, dass der Rat oder das Europäische Parlament innerhalb von drei Monaten, nachdem die Kommission den delegierten Rechtsakt übermittelt hat, **Einwände** erheben können, um das Inkrafttreten zu verhindern (Art. 73 Abs. 5 KI-VO-E).

115 Bei Einwänden steht ein geregeltes Verfahren bereit, den Durchführungsrechtsakt mit Änderungen erneut vorzuschlagen oder den Berufungsausschuss mit einer Einigung zu beauftragen (Art. 5 VO (EU) 182/2011). In diesem Rahmen ist eine ernsthafte Beteiligung **anderer Interessengruppen** jedoch nicht vorgesehen.

116 Manche halten es auch deshalb für angemessen, ausdrücklich ein **strenges Prüfverfahren** zu verankern und die Vorschläge der Kommission als Durchführungsrechtsakte dem Prozedere aus Art. 5 VO (EU) 182/2011 zu unterziehen.[169] Das hätte zur Folge, dass sich standardmäßig ein Ausschuss mit Mitgliedern aller Mitgliedstaaten mit den Vorschlägen der Kommission befasste.

---

[165] Hinderks ZUM 2022, 110 (117): Dies sei insbes. notwendig, um – anders als der KI-VO-E es derzeit handhabt – entsprechend risikobehaftete Deepfakes als eigenständige HR-Systeme einzuordnen.

[166] Vgl. bspw. Ebert/Spiecker NVwZ 2021, 1188 (1190).

[167] Ebers/Hoch/Rosenkranz/Ruschemeier/Steinrötter RDi 2021, 528 (531 f.); wohl auch Mesarčík/Soláro-vá/Podroužek/Bielikova, Stance on The Proposal for a Regulation Laying Down Harmonised Rules on Artificial Intelligence – Artificial Intelligence Act 2021, 4.

[168] EDSB, Stellungnahme zum Weißbuch der Europäischen Kommission „Zur Künstlichen Intelligenz – ein europäisches Konzept für Exzellenz und Vertrauen", 4/2020, 12, Rn. 29 aE.

[169] Mesarčík/Solárová/Podroužek/Bielikova, Stance on The Proposal for a Regulation Laying Down Harmonised Rules on Artificial Intelligence – Artificial Intelligence Act 2021, 4.

Rechtspolitisch wünschenswert wäre es, wenn die Kommission nicht nur **Anhang III** KI-VO-E ergänzen, sondern auch die Harmonisierungsvorschriften des **Anhangs II** KI-VO-E durch delegierten Rechtsakt abändern könnte. Erwgr. Nr. 85 S. 1 KI-VO-E deutet dies an. Ein solches Recht spiegelt sich in den Artikeln des KI-VO-E jedoch nicht wider. 117

III. Datenbank (Art. 60 KI-VO-E)

Um hinreichende Transparenz über KI-Systeme herzustellen, hebt Art. 60 KI-VO-E (iVm Art. 51 KI-VO-E) eine **Datenbank** aus der Taufe. In diese müssen die Anbieter bzw. ihre Bevollmächtigten selbstständige Hochrisiko-KI-Systeme[170] eintragen, bevor sie die Anwendungen in den **Verkehr bringen** bzw. in **Betrieb nehmen.** Als regulatorisches Vorbild stand eine vergleichbare Einrichtung der VO (EU) 2017/745 Pate.[171] 118

Die Pflicht, die Systeme in die Datenbank einzutragen, löst **keinen allgemeinen Genehmigungsvorbehalt** aus. Die Liste soll es vielmehr sowohl den Behörden als auch der Wissenschaft sowie der Zivilgesellschaft ermöglichen, sich über die am Markt vorhandenen Lösungen einen **Überblick** zu verschaffen. Auf diese Weise soll sie unterstützend dazu beitragen, Hochrisiko-KI-Systeme zu **beaufsichtigen** und im laufenden Betrieb zu **überwachen.**[172] 119

Die Datenbank speichert die Daten, die die Anbieter bereitstellen müssen, in einer **öffentlich zugänglichen** Weise (Art. 60 Abs. 3 KI-VO-E). Die Kommission soll „funktionale[.] Spezifikationen [ausarbeiten]", damit die Datenbank ihren Sinn und Zweck erfüllen kann (Erwgr. Nr. 69 S. 3 KI-VO-E).[173] Das Verfahren, welches zur Anwendung kommt, um die Datenbank zu errichten, soll ferner „einen unabhängigen Prüfbericht umfassen" (Erwgr. Nr. 69 S. 3 KI-VO-E).[174] 120

Welche **Daten** die Datenbank sammelt, spezifiziert **Anhang VIII** KI-VO-E. Er listet insbes. die Kontaktdaten des Anbieters bzw. Bevollmächtigten, den Namen, die Zweckbestimmung und den Status des Systems, Angaben der notifizierten Stelle, die EU-Konformitätserklärung sowie elektronische Gebrauchsanweisungen[175] auf. 121

Die Registrierungspflicht trifft den **Anbieter,** also denjenigen, der ein KI-System entwickelt oder entwickeln lässt, um es unter eigenem Namen oder eigener Marke in Verkehr zu bringen oder in Betrieb zu nehmen (Art. 3 Nr. 2 KI-VO-E)[176] – nicht demgegenüber Händler,[177] Einführer,[178] Nutzer[179] oder sonstige Dritte. Der Anbieter muss auch nicht angeben, wer das System zu welchem tatsächlichen Zweck nutzt. 122

---

[170] Dazu schon → Rn. 50 ff.

[171] In der Datenbank „Eudamed" können verschiedene elektronische Systeme registriert werden. Sie enthält – ua ebenfalls um die Transparenz zu erhöhen – Informationen zu den Produkten und Wirtschaftsakteuren auf dem Markt, Details der Konformitätsbewertung, Benannten Stellen, Bescheinigungen und klinischen Prüfungen (Erwgr. Nr. 44 VO, Art. 28 VO (EU) 2017/745); vgl. Veale/Zuiderveen-Borgesius CRI 2021, 97 (111).

[172] Vgl. Begr. Nr. 5.2.3 aE.

[173] Erwgr. Nr. 69 S. 3 KI-VO-E.

[174] Erwgr. Nr. 69 S. 3 KI-VO-E.

[175] Anbieter von Hochrisiko-KI-Systemen in den Bereichen Strafverfolgung und Migration, Asyl und Grenzkontrolle gem. Anhang III Nr. 1, 6 und 7 KI-VO-E registrieren keine elektronischen Gebrauchsanweisungen, vgl. Anhang VIII Nr. 11 KI-VO-E.

[176] Den Anbieter konzipiert der KI-VO-E (neben dem Nutzer) als Hauptzielfigur seiner Regulierungsansätze; vgl. Begr. Nr. 3.4.

[177] Händler ist „eine natürliche oder juristische Person in der Lieferkette, die ein KI-System ohne Änderung seiner Merkmale auf dem Unionsmarkt bereitstellt, mit Ausnahme des Herstellers oder des Einführers" (Art. 3 Nr. 7 KI-VO-E).

[178] Darunter versteht der KI-VO-E „eine in der Union ansässige oder niedergelassene natürliche oder juristische Person, die ein KI-System, das den Namen oder die Marke einer außerhalb der Union ansässigen oder niedergelassenen natürlichen oder juristischen Person trägt, in der Union in Verkehr bringt oder in Betrieb nimmt" (Art. 3 Nr. 6 KI-VO-E).

123 Wenn hingegen ein Händler, Einführer, Nutzer oder sonstiger Dritter die **Zweckbestimmung** eines KI-Systems ändert oder die Anwendung **wesentlich verändert,** gilt auch er als Anbieter (vgl. Art. 28 Abs. 1 Buchst. b, c KI-VO-E)[180] und unterliegt in der Folge der **Registrierungspflicht** (Art. 16 Buchst. f KI-VO-E iVm Art. 51 iVm Art. 60 KI-VO-E).[181]

124 Die **Wirkkraft** der Datenbank ist in ihrer **Reichweite beschränkt** – dies schon deshalb, weil sie lediglich die eigenständigen Hochrisiko-KI-Systeme iSd Art. 6 **Abs. 2** KI-VO-E erfasst – nicht aber Systeme, die dem Regime des Art. 6 **Abs. 1** KI-VO-E unterfallen. Diese speichert sie „[a]us Gründen der Kohärenz mit den bestehenden Produktsicherheitsvorschriften"[182] nicht.

125 Auch aus anderen Gründen steht zumindest in Frage, inwieweit die Datenbank tatsächlich dazu beitragen kann, KI-Systeme wirksam zu kontrollieren: Soll sie nicht nur Transparenz fördern, sondern auch eine Kontrolle „von unten nach oben" ermöglichen, wären **Beschwerderechte** erforderlich.[183] Selbst wenn bspw. Zivilpersonen auch mithilfe der Datenbank bzw. der dort hinterlegten elektronischen Gebrauchsanweisungen auf rechtswidrig operierende KI-Systeme stießen, bräuchte es korrespondierende **Durchsetzungsrechte,** damit sie dieses Wissen nutzen könnten, um eine wirksame Kontrolle auszuüben.[184]

126 Eine weitere Sollbruchstelle der Datenbank ist die **Reichweite der Pflichtangaben.** Sie beschränkt sich auf **Elementardaten,** bspw. die Kontaktdaten der Anbieter und Verarbeitungszwecke. Damit lässt sich keine **wirksame Kontrolle** algorithmenbasierter Systeme herstellen – und folglich die innere Mission der Registrierungspflicht nur bedingt erfüllen. Um diese sicherzustellen, wäre es geboten, **technische Spezifikationen,** etwa das verwendete Grundmodell sowie Programmabläufe und Entscheidungsparameter, zu erfassen. Besondere Bedeutung hat das für Systeme, die sich für **verschiedene Zwecke** einsetzen lassen (im Exportrecht ist diese Konstellation unter dem Begriff Dual-Use-Güter bekannt: Eine Anwendung ist sensibel, eine andere nicht); an dieser Stelle sollte der Unionsgesetzgeber den Entwurf nachschärfen.

---

[179] Einen Nutzer definiert der Verordnungsentwurf als „eine natürliche oder juristische Person, Behörde, Einrichtung oder sonstige Stelle, die ein KI-System in eigener Verantwortung verwendet, es sei denn, das KI-System wird im Rahmen einer persönlichen und nicht beruflichen Tätigkeit verwendet" (Art. 3 Nr. 4 KI-VO-E).

[180] Für den konkreten Anwendungsfall des Art. 28 Abs. 1 Buchst. c KI-VO-E ist damit die Auslegung des Terminus „wesentliche Änderung" entscheidend. Die Definition, die der KI-VO-E bietet, hilft nur bedingt weiter: Er erklärt eine Änderung für wesentlich, wenn sie „sich auf die Konformität des KI-Systems mit den Anforderungen in Titel III Kapitel 2 dieser Verordnung auswirkt oder zu einer Änderung der Zweckbestimmung führt, für die das KI-System geprüft wurde" (vgl. Art. 3 Nr. 23 KI-VO-E). Entsprechend legt Erwgr. Nr. 66 S. 1 KI-VO-E fest, dass es einer neuen Konformitätsbewertung in zwei Konstellationen bedarf: wenn sich die Zweckbestimmung des Systems ändert oder wenn die Änderung „die Einhaltung [der] Verordnung durch das System beeinträchtigen könnte" (Erwgr. Nr. 66 S. 1 KI-VO-E). Die Zweckbestimmung für die Verwendung des Systems legt der Anbieter fest (vgl. Art. 3 Nr. 12 KI-VO-E). Erwgr. Nr. 66 S. 2 KI-VO-E sowie Art. 43 Abs. 4 UAbs. 2 KI-VO-E ordnen ferner an, dass für automatisiert lernende KI-Systeme besondere Bestimmungen gelten: Sofern sich die Änderungen innerhalb des vorab vom Anbieter festgelegten Rahmens bewegen und zum Zeitpunkt der Ex-ante-Konformitätsbewertung beurteilt wurden, liegt keine solche „wesentliche Änderung" vor (und bedarf es keiner neuen Konformitätsbewertung). Allerdings legt diese Auslegung es dem Anbieter in die Hand, vorab selbst festzulegen, ob ein KI-System, das maschinell weiterlernt, trotz seines hohen Risikos in der Datenbank registriert werden muss. Wenn der ursprüngliche Anbieter hingegen nur sehr enge Bestimmungen trifft, die den weiteren Lebenszyklus des Systems (auch wenn es zur Weiterentwicklung geeignet oder bestimmt ist) zum Gegenstand haben, führen bereits kleinste Änderungen zu (ua) der Registrierungspflicht.

[181] In dieser Konstellation ist die Datenbank ein wichtiger Baustein der Rechenschaftspflicht; Veale/Zuiderveen-Borgesius CRi 2021, 97 Rn. 105.

[182] Begr. Nr. 5.2.3 aE KI-VO-E.

[183] „These [electronic] instructions state what users must follow to avoid liability under the Draft AI Act. Yet without clear complaint rights, bottom-up enforcement on the basis of this database will be significantly hampered." Veale/Zuiderveen-Borgesius CRi 2021, 97 Rn. 104.

[184] Veale/Zuiderveen-Borgesius CRi 2021, 97 Rn. 104.

Allerdings ist auch insoweit Augenmaß geboten. Gerade bei **vernetzten Systemen** 127
können technische Dokumentationslasten extrem aufwändig sein; eine entsprechende Pflicht wüchse sich dann unversehens zu einer **unverhältnismäßigen Belastung** aus. Es drohte – ähnlich wie bereits im Rahmen des risikobasierten Ansatzes der DS-GVO – eine **Lastenasymmetrie,** die insbes. kleinere und mittlere Unternehmen überproportional schwer träfe.[185]

E. KI-Systeme mit geringem Risiko (Art. 52 KI-VO-E)

KI-Systeme, von denen nur geringe Risiken ausgehen, entlässt die Union weitgehend in 128
die regulatorische Freiheit. Lediglich für einige konkrete Anwendungen gibt **Art. 52** KI-VO-E spezifische **Transparenz- und Offenlegungspflichten** vor. Eine Auffangklausel für weitere KI-Systeme mit geringen Risiken kennt der Verordnungsentwurf nicht.

I. Tatbestandliche Voraussetzungen der Kennzeichnungspflicht

Die Transparenzverpflichtung trifft insbes. die **Anbieter interaktiver Systeme,** bspw. 129
Chatbots (Art. 52 Abs. 1 KI-VO-E). Sie müssen die Nutzer grds. darüber informieren, dass sie mit einem KI-System kommunizieren (es sei denn, dies ist offensichtlich).[186] Verwender von **Emotionserkennungssoftware**[187] oder von Systemen, die biometrische Kategorisierungen vornehmen, müssen den Einsatz dieser Anwendungen ebenfalls den Personen mitteilen, die das System erfasst (Art. 52 Abs. 2 KI-VO-E).

Der **Mehrwert** dieser gesetzlichen Verpflichtung erschließt sich nicht auf den ersten 130
Blick. Denn bereits die DS-GVO statuiert in **Art. 13 DS-GVO**[188] und **Art. 14 DS-GVO** Informationspflichten. Diese schließen jedoch keine Kennzeichnungspflicht ein. Eine solche begründet die DS-GVO vielmehr alleine für **vollständig automatisierte Entscheidungen** iSd Art. 22 DS-GVO (Art. 13 Abs. 2 Buchst. f DS-GVO). Für teilautomatisierte Entscheidungen – und damit für das Gros der heute im Einsatz befindlichen KI-Systeme – etabliert sie e contrario keine Hinweispflicht.[189]

Neben Emotionserkennungssystemen müssen auch Anwendungen, die sog. **„Deep-** 131
fakes" erstellen, offenlegen, dass sie Bild-, Ton- oder Videoinhalte manipuliert haben (vgl. Art. 52 Abs. 3 KI-VO-E).[190] Das hat auch einen guten Grund: Die Technik kann durch ihr hohes **Täuschungspotenzial** nicht nur gesellschaftliche Verwerfungen auslösen, sondern auch nicht unerhebliche **Auswirkungen auf demokratische Prozesse im Rechtsstaat** zeitigen.[191] Dass der KI-Verordnungsentwurf „Deepfake-Generatoren" insge-

---

[185] S. dazu bereits → Rn. 10; die Kommission möchte KMUs durch unterschiedliche Regelungen, bspw. durch die Errichtung von „KI-Reallaboren", unterstützen; vgl. Titel V des KI-VO-E (→ § 9 Rn. 24 ff.); ausführlich zu KI-Reallaboren: Truby/Brown/Ibrahim/Parellada European Journal of Risk Regulation 2022, 270.

[186] Der KI-VO-E räumt den Betroffenen nicht das Recht ein, ein System ablehnen zu dürfen, um stattdessen mit einem Menschen zu kommunizieren. Ein solches Recht, mit einem Menschen kommunizieren zu können, ist jedoch in solchen Konstellationen geboten, in denen der Nutzer auf das elektronische Angebot angewiesen ist, um hinreichende soziale Teilhabe zu erhalten oder sonst (zB im Verhältnis zur Verwaltung) keine Leistungsalternative für eine unverzichtbare Leistung zur Verfügung hat.

[187] Art. 3 Nr. 34 KI-VO-E definiert „Emotionserkennungssystem" als „ein KI-System, das dem Zweck dient, Emotionen oder Absichten natürlicher Personen auf der Grundlage ihrer biometrischen Daten festzustellen oder daraus abzuleiten." Solche Systeme können auch ein Hochrisiko-KI-System darstellen (vgl. Anhang III Nr. 6 Buchst. b und Nr. 7 Buchst. a KI-VO-E).

[188] Ausf. dazu bspw. Veale/Zuiderveen-Borgesius CRi 2021, 97 Rn. 73.

[189] Dazu bereits Martini, Blackbox Algorithmus, 2019, 177 f.

[190] Ausführlich und kritisch zu der Regulierung von Deepfakes im KI-VO-E vgl. Hinderks ZUM 2022, 110.

[191] Ausführlich dazu bspw. Linardatos GPR 2022, 58 (68 ff.): „entschieden abzulehnen"; vgl. auch Rostalski/Weiss ZfDR 2021, 329 (352).

samt als nur in geringem Umfang risikoträchtig einstuft, überrascht daher und ist kritikwürdig.[192]

II. Rechtsfolgen

132 Soweit die Kennzeichnungspflicht greift, muss der Verwender nicht nur über das **„Ob"**, sondern auch über das **„Wie"**, also über die **Entscheidungsparameter,** unterrichten. Das ergibt sich mittelbar aus der Formulierung „über den Betrieb des Systems informieren" in Art. 52 Abs. 2 KI-VO-E. Welche weitergehenden Informationen (die über die bloße Mitteilung hinausgehen, dass ein KI-System zur Anwendung kam) der Betroffene noch erhalten soll, lassen allerdings weder Art. 52 KI-VO-E noch Erwgr. Nr. 70 KI-VO-E erkennen. Bislang konkretisiert Erwgr. Nr. 70 KI-VO-E die Vorgaben des verfügenden Teils nur mit dem Hinweis, die Informationen auch barrierefrei zur Verfügung zu stellen (Erwgr. Nr. 70 S. 5 KI-VO-E). Wie die Systeme den Transparenzpflichten im Detail nachkommen müssen, sollte die Verordnung normativ präzisieren. Die Informationen sollten Betroffene zumindest in die Lage versetzen, nachvollziehen zu können, welche **Entscheidungsgrundlagen** das System genutzt hat, welche **Schlussfolgerungen** es aus den Eingabedaten gezogen hat und wie sich der Einsatz auf ihre **konkrete Situation** auswirkt bzw. ausgewirkt hat. Nur unter diesen Prämissen können sie bspw. Diskriminierungen aufdecken.

133 Die Transparenz- und Offenlegungspflichten des Art. 52 KI-VO-E gelten nicht pauschal. Für den Bereich der **Strafverfolgung** (Art. 52 Abs. 1 S. 2, Abs. 2 S. 2, Abs. 3 S. 2 KI-VO-E) formuliert der KI-VO-E vielmehr eine **Ausnahme,** um sicherzustellen, dass die Maßnahmen ihr Ziel im Ergebnis nicht verfehlen. Die Pflicht des Art. 52 Abs. 3 KI-VO-E greift auch dann nicht, wenn „Deepfakes" erforderlich sind, um die Meinungs- bzw. Kunst- und Wissenschaftsfreiheit auszuüben, und hinreichende Schutzvorkehrungen bestehen (Art. 52 Abs. 3 UAbs. 2 KI-VO-E).

134 Art. 52 KI-VO-E ist nicht die einzige Vorschrift des Gesetzespakets, die Transparenzpflichten formuliert. Auch **Art. 13 KI-VO-E** verschreibt sich dem Ziel, KI-Systemen **Transparenz** einzuhauchen. Beide Vorschriften unterscheiden sich aber fundamental. Art. 13 KI-VO-E adressiert die Konzeption und Entwicklung der Systeme (vgl. Erwgr. Nr. 47 KI-VO-E), Art. 52 KI-VO-E demgegenüber Anbieter, Verwender und Nutzer. Beide Vorschriften schließen sich zugleich nicht kategorisch aus. Der Verordnungsgeber trifft für ihr Verhältnis in **Art. 52 Abs. 4 KI-VO-E** eine **Kollisionsregel:** Die Vorgaben des Art. 52 KI-VO-E können neben den Pflichten des Titels III KI-VO-E zur Anwendung kommen. Die Risikozuordnung des KI-VO-E zieht mithin keine ganz strikte Stufentrennung nach sich. Im Einzelfall können Systeme (bspw. Emotionserkennungssysteme iSd Anhang III Nr. 6 Buchst. b, Nr. 7 Buchst. a KI-VO-E) vielmehr auch gleichzeitig den Regeln zweier Stufen unterliegen.[193]

---

[192] S. dazu auch schon → Rn. 93.

[193] AA wohl Draft Report on the proposal for a regulation of the European Parliament and of the Council on harmonised rules on Artificial Intelligence (Artificial Intelligence Act), PE731.563, 2021/0106(COD), 2022, Änderungsantrag Nr. 27. Das Parlament möchte in einem zusätzlichen Erwgr. Nr. 40a klarstellen, dass manche KI-Systeme den Hochrisiko-Anforderungen ebenso wie den Transparenzanforderungen unterfallen sollen. Das soll für Systeme gelten, die Deepfakes oder komplexere Schriftstücke generieren. Für diese Systeme soll der Gesetzgeber in Anhang III einen weiteren Lebensbereich ergänzen, vgl. Draft Report, aaO, Änderungsantrag Nr. 297, Anhang III Nr. 8a Buchst. a und b.

F. KI-Systeme, die ein Risiko im Einzelfall bergen (Art. 67, 69 KI-VO-E)

KI-Systeme, die **kein oder nur ein minimales Risiko im Einzelfall** bergen (bspw. Spam-Filter), unterfallen zwar der Legaldefinition des KI-Systems aus Art. 3 Nr. 1 KI-VO-E und damit dem Anwendungsbereich des KI-VO-E. Für sie hält er aber **keine besonderen Vorschriften** vor. 135

Immerhin kann die **Marktüberwachungsbehörde** auf der Grundlage des Art. 67 KI-VO-E im Einzelfall für alle KI-Systeme Maßnahmen treffen – dies jedoch nicht generell, sondern nur, wenn die Rechtsordnung an anderer Stelle eine konkrete Pflicht begründet, welche die Behörde einfordern kann. 136

Die Kommission möchte darüber hinaus für alle KI-Systeme sog. **Verhaltenskodizes** fördern (vgl. Art. 69 KI-VO-E). Das soll im Idealfall dazu beitragen, dass möglichst auch risikoarme KI-Systeme den Anforderungen des Titel III Kapitel 2 genügen (vgl. Art. 69 Abs. 1 KI-VO-E). Die Verhaltenskodizes sollen die Anbieter zudem ermutigen, sich **freiwillig** weiteren Anforderungen zu unterwerfen, die bspw. dem Ziel verschrieben sind, die **ökologische Nachhaltigkeit** zu fördern und Inhalte für Menschen mit Behinderungen barrierefrei zugänglich zu machen (vgl. Art. 69 Abs. 2 KI-VO-E). 137

Dass die Vorschrift in praxi durchgreifende Ergebnisse erzielt, ist jedoch **unwahrscheinlich.** Denn anders als im Rahmen der VO (EU) 2016/679 verspricht der KI-VO-E den Betreibern keine anderweitigen „Erleichterungen", um einen solchen Code of Conduct aufzustellen bzw. sich ihm zu unterwerfen.[194] 138

G. Zweckoffene KI-Systeme als ergänzende Kategorie?

Die slowenische Ratspräsidentschaft bringt eine weitere Kategorie von KI-Systemen ins Spiel, die der KI-VO-E perspektivisch **separat** behandeln könnte: Systeme, die **zweckoffen** sind, also keine Zweckbestimmung iSd Art. 3 Nr. 12 KI-VO-E aufweisen[195] **(„general purpose"),** sondern allgemein anwendbare Funktionen erfüllen können („able to perform generally applicable functions"). Zu ihnen sollen bspw. Bild- und Spracherkennung, Generierung von Audio- und Videodateien, Mustererkennung, Beantwortung von Fragen oder Übersetzungen zählen.[196] Die Kategorisierung baut auf dem Grundgedanken auf, dass solche Systeme einer Vielzahl von Verwendungen offenstehen, auf denen weitere Trainingsvorgänge und Softwareentwicklungen aufsetzen. Daher ist es sachgerecht, auch ihren Pflichtenkatalog offen zu gestalten. Nach der Vorstellung der slowenischen Ratspräsidentschaft soll das Pflichtenkorsett der KI-VO erst dann greifen, wenn jemand ein KI-System mit allgemeinem Verwendungszweck in den Verkehr bringt oder in Betrieb nimmt oder ein solches System nutzt und für das System eine konkrete Verwendung im Sinne der KI-VO bestimmt (Zweckbestimmung, vgl. auch Art. 3 Nr. 12 KI-VO-E).[197] 139

Die grundsätzliche Idee, diese Gruppe von KI-Systemen gleichsam neben die Risikopyramide zu stellen, scheint zu verfangen: Auch die französische und tschechische Ratspräsidentschaft behalten die Kategorie bei ihren Fortentwicklungen des Entwurfs bei. Frankreich schlägt jedoch eine **andere Richtung** ein:[198] Die Systeme sollen nicht explizit von den Regeln des KI-VO-E ausgenommen, sondern vielmehr ausdrücklich **inklu-** 140

[194] Spindler CR 2021, 361 Rn. 71.
[195] Art. 3 Nr. 12 Hs. 2 Ratsdok. 14278/21.
[196] Erwgr. Nr. 70a Ratsdok. 14278/21.
[197] Art. 52a Abs. 2, Erwgr. Nr. 70a Ratsdok. 14278/21.
[198] Darüber hinaus präzisiert der Vorschlag die Definition dahin, dass es sich um Systeme handeln soll, die in einer Vielzahl von Kontexten einsetzbar und in eine Vielzahl anderer KI-Systeme integrierbar sind; Art. 3 Nr. 1 Buchst. b Ratsdok. 10069/22, Erwgr. Nr. 12 Buchst. aa Ratsdok. 10069/22.

diert sein.[199] Da Akteure sie später als Bestandteil von Hochrisiko-KI-Anwendungen oder als solche selbst einsetzen könnten, sollen die Systeme auch schon vorher die meisten **Regeln für Hochrisiko-KI-Systeme** befolgen müssen.[200] Bislang sind nur wenige Ausnahmen vorgesehen, bspw. für die Aufzeichnungspflichten des Art. 12 KI-VO-E.[201] Zudem sollen die Transparenzpflichten weniger umfassend ausfallen. Eine Gebrauchsanweisung (Art. 13 Abs. 2 KI-VO-E) bleibt zwar verpflichtend, nicht aber zusätzliche Informationen, die dabei helfen könnten, die Ergebnisse des Systems zu interpretieren (Art. 13 Abs. 1 KI-VO-E). Auch auf das Erfordernis, menschliche Aufsicht herzustellen (Art. 14 KI-VO-E), verzichtet der Kompromissvorschlag.

141 Ob ein System **allgemein verwendbar** ist, macht er von der **Verwendungsabsicht** des Anbieters abhängig.[202] Ein Ausnahmetatbestand soll es ihm insbes. ermöglichen, in den Begleitinformationen zu einem System jegliche Hochrisiko-Anwendungen auszuschließen.[203] Diese Entscheidung muss nach Treu und Glauben („in good faith") erfolgen. Dabei ist besonders von Belang, ob die Anbieter einen späteren Missbrauch zuvor bereits absehen konnten. Die Einschätzung, ob ein allgemein verwendbares System die Hochrisiko-Regeln befolgen muss – und damit auch das Risiko, eine Fehleinschätzung abzugeben –, obliegt damit allein den Anbietern. Das Vorhaben begegnet auch deshalb insbes. im Hinblick auf **Open-Source-Systeme** (die ausdrücklich der Definition des französischen Vorschlags unterfallen[204]) Kritik: Solche Systeme entwickeln meist eine Vielzahl von Akteuren gemeinsam; komplexe rechtliche Verantwortungsstrukturen wirken sich auf deren Mitwirkungsbereitschaft typischerweise abschreckend aus.[205]

142 Während der Gedanke, KI-Systeme mit allgemeinem Verwendungszweck als solche gesondert adressieren zu müssen, überzeugt, scheinen die Konsequenzen, die daraus folgen sollen, noch nicht ausgereift zu sein. Eine **ausgewogene Verteilung der Pflichten und Risiken** erzielen die Vorschläge in ihrer gegenwärtigen Fassung noch nicht. Die zusätzliche Nebenkategorie wird damit noch einiger Überarbeitung bedürfen, um alle beteiligten Parteien angemessen in den Pflichtenkatalog einzubeziehen.

H. Fazit

143 Der risikobasierte Ansatz des KI-VO-E präsentiert sich als **vierstufige Pyramide:** Eine kleine Gruppe generell verbotener Praktiken formt ihre Spitze aus (Art. 5 KI-VO-E), eine große Gruppe hochriskanter Systeme unterwirft der KI-VO-E auf der nächsten Stufe einer Vielzahl zielgerichteter, intensiv regulierender Maßnahmen (Art. 6 ff. KI-VO-E). Die verbleibende breite Masse der KI-Systeme unterhalb der Hochrisiko-Schwelle hat lediglich Transparenzpflichten (Art. 52 KI-VO-E) oder nur freiwillige bzw. im Einzelfall zwingende Anforderungen (Art. 67, 69 KI-VO-E) zu erfüllen.

144 Der klare **Fokus** des Regelungssystems liegt zu Recht auf **Hochrisiko-KI-Systemen.** Der Gesetzgeber fächert sie in zwei **Unterklassen** auf: Systeme nach dem Produktsicherheitsgesetz (Art. 6 Abs. 1 KI-VO-E) und eigenständige Hochrisiko-KI-Systeme (Art. 6 Abs. 2 KI-VO-E).

---

[199] Die beschriebenen Änderungen des französischen Vorschlags übernimmt die Kompromissversion der tschechischen Ratspräsidentschaft unverändert, Ratsdok. 11124/22.
[200] Art. 4b Abs. 1 Ratsdok. 10069/22.
[201] Art. 4b Abs. 1 Ratsdok. 10069/22.
[202] Erwgr. Nr. 12 Buchst. aa Ratsdok. 10069/22.
[203] Art. 4c Ratsdok. 10069/22.
[204] Art. 3 Nr. 1b Ratsdok. 10069/22.
[205] Engler, Warum es eine schlechte Idee ist, quelloffene KI zu regulieren, abrufbar unter: https://background.tagesspiegel.de/digitalisierung/warum-es-eine-schlechte-idee-ist-quelloffene-ki-zu-regulieren (zuletzt aufgerufen am 4.10.2022).

Systeme, die Teil eines Produkts nach den **Produktsicherheitsgesetzen** der Union sind, unterfallen Regeln, die in das bisherige Produktsicherheitskonzept eingeflochten sind. Je nach Herangehensweise des einschlägigen Produktsicherheitsgesetzes – ob nach altem Ansatz oder New Approach und New Legislative Framework – muss entweder der Unionsgesetzgeber selbst KI-bezogene Vorgaben in die bestehenden Produktsicherheitsnormen integrieren oder die Normungsinstitute müssen die Anforderungen in ihren privaten Regularien ergänzen. Wirtschaftsakteure sind dann verpflichtet, die Regeln im Kontext der bereits bestehenden Verfahren, welche die Produktsicherheit garantieren sollen, anzuwenden. Für die praktische Wirksamkeit des KI-Regulierungsansatzes könnte sich als Pferdefuß erweisen, dass der Gesetzgeber die Produktsicherheitsregeln ursprünglich nicht für Systeme konzipiert hat, die sich – wie lernfähige KI-Anwendungen – in ihren Lebenszyklen **selbständig weiterentwickeln.** Uneingeschränkt gelten die Vorschriften des Titels III KI-VO-E im Ergebnis nur für diejenigen **eigenständigen** Hochrisiko-KI-Systeme, die unabhängig von einem bestimmten Produkt funktionieren und einem von acht als hochriskant identifizierten Lebensbereichen unterfallen. Inwiefern daraus unterschiedliche Konsequenzen für die beiden Kategorien von Hochrisiko-KI-Systemen erwachsen werden, ist bislang noch offen. 145

Eine klare **Abgrenzung** zwischen den **Risikogruppen** ist im Rahmen des Stufensystems nicht gänzlich bruchfrei möglich. Dadurch läuft die Verordnung Gefahr, dass KI-Systeme, die ihre Hersteller nicht eindeutig einer Stufe zuordnen können, gesetzliche **Anforderungen unterlaufen.** Ebenso können KI-Systeme im Laufe ihres **Lebenszyklus** in unterschiedliche Risikokategorien fallen. Dies gilt bereits dann, wenn ein KI-System zeitgleich in unterschiedlichen Kontexten Anwendung findet.[206] Darauf versuchen nunmehr die Regelungsvorschläge des Rates zu **General-Purpose-Systemen**[207] zu reagieren. Für marktfähige Systeme, deren konkrete Risikozuordnung für Anbieter und Hersteller ungewiss ist, verbleibt aber auch dann eine Rechtsunsicherheit. Viele Entwickler werden daher im Zweifel vorsorglich die Konformität für Hochrisikoanwendungen sicherstellen wollen; das erhöht die Markteintrittshürden für kleine Unternehmen spürbar.[208] Eine Regelung, nach der KI-Systeme, die zumindest teilweise ein hohes Risiko bergen, grds. den Vorgaben der Art. 8 ff. KI-VO-E unterliegen sollten, fehlt im derzeitigen Entwurf.[209] Eine solche Regelung aufzunehmen, schüfe Klarheit und Rechtssicherheit für die Anbieter, aber auch für Nutzer und Betroffene der Systeme. 146

Auch der Katalog des **Anhangs III KI-VO-E** wird im Laufe des Gesetzgebungsprozesses noch weiterer Überarbeitung bedürfen. Er birgt derzeit noch einige **Regelungslücken,** die es zu schließen gilt, um einen ausreichenden Schutz der Grundrechte Betroffener und der Werte der Union zu gewährleisten. Insbes. ein stärkerer **Schutz von Kindern** im Bereich „Allgemeine und berufliche Bildung" (Anhang III Nr. 3 Buchst. a und b KI-VO-E) ist angezeigt; jedenfalls wünschenswert wäre es, dass die Kommission sowohl das Breitband- und Mobilfunknetz als auch die Gas- und Fernwärmeversorgung ausdrücklich als **schützenswerte kritische Infrastruktur** iSd Anhang III Nr. 2 KI-VO-E gesondert herausstellte. Bei KI-Systemen, die im **arbeitsrechtlichen Kontext** (Anhang III Nr. 4 Buchst. a und b KI-VO-E) zum Einsatz kommen sollen, sind die Regeln einiger nationaler Rechtsrahmen bereits detaillierter als die im KI-VO-E. Dort läuft der Verordnungsentwurf Gefahr, den bereits bestehenden Schutz im Ergebnis zu verwässern. Unter den demokratischen Prozessen (Anhang III Nr. 8 KI-VO-E) ist der Einsatz von KI-Systemen im Bereich von Wahlen zwar besonders riskant (vgl. auch Anhang III Nr. 8: „demokratische Prozesse"), aber nicht legislativ konkret umhegt. Der Unionsgesetzgeber sollte hier nachsteuern. 147

[206] Valta/Vasel ZRP 2021, 142 (142).
[207] → Rn. 139 ff.
[208] Valta/Vasel ZRP 2021, 142 (142).
[209] Vgl. auch Erwgr. Nr. 6a, Draft Opinion of the Committee on Legal Affairs, PE719.827, 2021/0106(COD), 2022.

148 Auch das **„Predictive Policing"** im Bereich Strafverfolgung (Anhang III Nr. 6 KI-VO-E) erweist sich als offene Flanke des Entwurfs: Inwieweit Anhang III KI-VO-E diese KI-Technologie erfasst bzw. ob der Gesetzgeber – wie teilweise gefordert – sie gar nach Art. 5 KI-VO-E vollständig verbieten sollte, ist unklar. Jedenfalls ist der Unionsgesetzgeber aufgerufen, den offenen Wortlaut insgesamt nachzuschärfen, um Rechtsunsicherheiten vorzubeugen. Sowohl auf dem Feld der Strafverfolgung (Anhang III Nr. 6 KI-VO-E) als auch im Bereich des Gefahrenabwehrrechts gilt es allerdings noch abzustecken, inwieweit die Union sehr detailreiche Vorgaben treffen darf, ohne zu weit in die **Kernkompetenz** der Nationalstaaten im Bereich der **nationalen Sicherheit** vorzustoßen. Die Verordnung muss insoweit den Mitgliedstaaten zumindest ausreichende **Regelungsspielräume** eröffnen, die es ihnen ermöglichen, die Vorgaben der EU mit ihren nationalen Gesetzen sowie sicherheitsrelevanten nationalen Besonderheiten im Bereich der Sicherheit und öffentlichen Ordnung in Einklang zu bringen.

149 Für eigenständige Hochrisiko-KI-Systeme erhält die Kommission die Befugnis, den Anwendungsbereich der Regeln bei Bedarf auszuweiten, um den vielfältigen **dynamischen Entwicklungen** im KI-Sektor gerecht zu werden (Art. 7 KI-VO-E). Diese Ermächtigung ist nach der aktuellen Konzeption aber eng umgrenzt: Die Kommission darf nur innerhalb der bereits als hochriskant eingeschätzten Lebensbereiche zusätzliche Systemkategorien hinzufügen, nicht aber davon unabhängige, neue Lebensbereiche aufnehmen. Nachträgliche Streichungen sind nicht gestattet.

150 Die **Datenbank,** in welche die Anbieter von Hochrisiko-KI-Systemen Eckdaten eintragen müssen (vgl. Art. 60 KI-VO-E), folgt einer schlüssigen Grundidee: **Öffentlichkeit** kann für ausreichende Transparenz im Bereich des Einsatzes Künstlicher Intelligenz Sorge tragen. Um dieses Ziel zu erreichen, bedarf es jedoch einer weitläufigen Eintragungspflicht. Die Datenbank erfasst im derzeitigen Verordnungsentwurf lediglich eigenständige KI-Systeme und speichert zudem nur ihre Elementardaten. Da es darüber hinaus an effektiven Durchsetzungsrechten für Betroffene mangelt, könnte sich die Datenbank für die **Förderung von Transparenz** im Ergebnis als **zahnloser Tiger** erweisen. Um dies zu vermeiden, ist es angezeigt, die Registrierungspflichten auszuweiten und weiter normativ aufzufächern.

151 Die grundsätzliche Philosophie des risikobasierten Ansatzes, die **Regulierungsintensität** der KI-VO an der Schadenswahrscheinlichkeit und Schadenshöhe auszurichten, die vom Einsatz oder möglichen Fehlfunktionen bestimmter KI-Systeme ausgehen, überzeugt. Die Kommission hat insbes. aus den Erfahrungen mit der **DS-GVO** gelernt: Anders als im datenschutzrechtlichen Kontext gesteht der risikobasierte Ansatz des KI-VO-E den Rechtsanwendern deutlich weniger Flexibilität zu. Während es unter der der DS-GVO weitgehend den Akteuren obliegt, die mit persönlichen Daten umgehen, dem Risiko angemessene Vorkehrungen abzuschätzen, schneidet der KI-VO-E die gesetzlichen Pflichten klarer und passgenauer zu. Der regulatorische Grundansatz des einheitlichen unionalen Rechtsrahmens für KI-Systeme sorgt so für mehr **Rechtssicherheit** und **Ergebniswirksamkeit.** Die Divergenzen zwischen beiden Sekundärrechtsakten speisen sich allerdings auch aus ihren unterschiedlichen Anknüpfungspunkten: Datenschutz ist technologieübergreifend angelegt, die KI-Regulierung geht demgegenüber **technologiespezifisch** vor. Konkrete Regeln sind daher im fraglichen Kontext deutlich sinnvoller.

152 Die Kombination des risikobasierten Ansatzes mit der technischen Normierung „harmonisierter Standards" ist jedenfalls dazu in der Lage, die absehbaren Risiken digitaler Geschäftsmodelle zielgenau einzuhegen. Im Gegensatz zur Plattformgesetzgebung oder zum Datenschutzrecht könnte es dem Unionsgesetzgeber mit der KI-VO gelingen, dem **„Pacing Problem"** zu entkommen – und eine Risikotechnologie zu einem Zeitpunkt mit normativen Leitplanken zu flankieren, in der das Recht die Technikentwicklung noch rechtzeitig in gemeinwohlorientierte Bahnen lenken kann. Vermag es die EU, einen **regulierten Markt für vertrauenswürdige KI-Systeme** zu schaffen, könnte dank des **„Brüssel-Effekts"** ein globaler Goldstandard entstehen, der den Menschen und seine in-

dividuellen wie kollektiven Freiheiten und Bedürfnisse „by Design" in den Mittelpunkt stellt. Das entspricht durchaus auch dem Bedürfnis vieler Softwareentwickler. Denn nur wer Werte und Normen klar genug vor Augen hat, kann digitale Systeme entwickeln, die ihnen entsprechen.

Die neue Verordnung der EU zur Künstlichen Intelligenz

Herausgegeben von

Prof. Dr. Dr. Eric Hilgendorf
Julius-Maximilians-Universität Würzburg

und

Prof. Dr. David Roth-Isigkeit
Deutsche Universität für Verwaltungswissenschaften
Speyer

Bearbeitet von

Prof. Dr. Sabine Gless; Prof. Dr. Dr. Eric Hilgendorf; Prof. Dr. Ruth Janal LL.M.; JProf. Dr. Lea Katharina Kumkar; PD Dr. Dimitrios Linardatos; Prof. Dr. Mario Martini; Prof. Dr. Dr. Frauke Rostalski; Prof. Dr. David Roth-Isigkeit; Prof. Dr. Gerald Spindler; Prof. Dr. Wiebke Voß, LL.M. (Cambridge); Dr. Erik Weiss; PD Dr. Martin Zwickel

2023

C.H.BECK

Zitiervorschlag:
Hilgendorf/Roth-Isigkeit KI-VO/Bearbeiter

Deutsche Univ.
für Verwalt. Wiss.
Speyer

www.beck.de

ISBN 978 3 406 79682 1

© 2023 Verlag C.H. Beck oHG
Wilhelmstraße 9, 80801 München

Druck und Bindung: Beltz Grafische Betriebe GmbH
Am Fliegerhorst 8, 99947 Bad Langensalza
Satz: 3w+p GmbH, Rimpar
Umschlaggestaltung: Martina Busch, Grafikdesign, Homburg Saar

CO_2 neutral
chbeck.de/nachhaltig

Gedruckt auf säurefreiem, alterungsbeständigem Papier
(hergestellt aus chlorfrei gebleichtem Zellstoff)