Teil II
Künstliche Intelligenz, Profiling und Überwachung

https://doi.org/10.5771/9783748913344-103, am 22.09.2024, 11:20:46
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

https://doi.org/10.5771/9783748913344-103, am 22.09.2024, 11:20:46
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

Der KI-Verordnungsentwurf und biometrische Erkennung: Ein großer Wurf oder kompetenzwidrige Symbolpolitik?

Stephan Schindler und Sabrina Schomberg

Zusammenfassung

Mit dem Verordnungsentwurf zur Regulierung künstlicher Intelligenz v. 21.4.2021 soll nach dem Willen der Europäischen Kommission ein Rechtsrahmen für die Entwicklung, Vermarktung und Verwendung künstlicher Intelligenz im Einklang mit den Werten der Europäischen Union geschaffen werden.

Der Entwurf folgt einem risikobasierten Ansatz und enthält Vorgaben für Anbieter und Nutzer von KI-Systemen. Die biometrische Erkennung nimmt dabei eine herausgehobene Stellung ein. Vorgesehen ist zunächst ein Verbot der Verwendung biometrischer Echtzeit-Fernidentifizierungssysteme in öffentlich zugänglichen Räumen zu Strafverfolgungszwecken, das allerdings durch Ausnahmen abgemildert wird. Zudem werden KI-Systeme, die bestimmungsgemäß für die biometrische Echtzeit-Fernidentifizierung und die nachträgliche biometrische Fernidentifizierung natürlicher Personen verwendet werden sollen, als Hochrisiko-KI-Systeme eingeordnet und einer Reihe von Anforderungen unterworfen (z.B. Dokumentations- und Aufzeichnungspflichten, menschliche Aufsicht). Überdies gelten für Systeme zur biometrischen Kategorisierung spezifische Transparenzpflichten.

Auch wenn der Verordnungsentwurf insgesamt zu begrüßen ist, wirft er im Einzelnen doch zahlreiche Fragen auf. Einigen dieser Fragen wird in dem vorliegenden Beitrag nachgegangen. Ferner wird ein Blick darauf geworfen, ob die Europäische Union für den Erlass der vorgenannten Regelungen überhaupt zuständig ist. Dies betrifft insbesondere den Einsatz biometrischer Systeme durch staatliche Stellen zu Strafverfolgungszwecken.

https://doi.org/10.5771/9783748913344-103, am 22.09.2024, 11:20:46
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

Am 21.4.2021 hat die Europäische Kommission einen Verordnungsentwurf zur Regulierung künstlicher Intelligenz (KI) präsentiert. Der Entwurf folgt einem risikobasierten Ansatz und enthält zahlreiche, in erster Linie produktsicherheitsrechtliche Vorgaben für Anbieter und Nutzer von KI-Systemen. Die biometrische Erkennung nimmt dabei eine herausgehobene Stellung ein. Der folgende Beitrag gibt zunächst einen kurzen Überblick über KI (1.) und den Verordnungsentwurf (2.). Im Anschluss daran werden die spezifischen Vorschriften zur biometrischen Erkennung vorgestellt und bewertet (3.). Zudem werden Probleme bzgl. der Regelungskompetenz der Union angesprochen (4.). Der Beitrag schließt mit einem Fazit (5.).

1 Künstliche Intelligenz

Künstliche Intelligenz (KI) ist in den letzten Jahren in den Fokus der gesellschaftlichen, politischen und (rechts-)wissenschaftlichen Aufmerksamkeit geraten.

1.1 Begriff, Chancen und Risiken

Eine allgemein anerkannte Definition für KI gibt es derzeit nicht.[1] Die deutsche Bundesregierung versteht KI als „ein Teilgebiet der Informatik, welches sich mit der Erforschung von Mechanismen des intelligenten menschlichen Verhaltens befasst". Es gehe darum, „technische Systeme so zu konzipieren, dass sie Probleme eigenständig bearbeiten und sich dabei selbst auf veränderte Bedingungen einstellen können".[2] Die Europäische Kommission bezeichnet mit KI „Systeme mit einem ‚intelligenten' Verhalten, die ihre Umgebung analysieren und mit einem gewissen Grad an Autonomie handeln, um bestimmte Ziele zu erreichen".[3] Darauf aufbauend definiert die Hochrangige Expertengruppe der Europäischen Union für Künstliche Intelligenz KI-Systeme als „vom Menschen entwickelte Softwaresysteme […], die in Bezug auf ein komplexes Ziel auf physischer oder

1 Zur Terminologie *Herberger*, NJW 2018, 2825 (2825 ff.); ebenfalls *Geminn*, ZD 2021, 354 (354 f.).
2 BT-Drs. 19/1982, S. 2. Die Aussage stammt von der inzwischen abgelösten Bundesregierung.
3 COM(2018) 237 final, S. 1.

https://doi.org/10.5771/9783748913344-103, am 22.09.2024, 11:20:46
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

digitaler Ebene handeln, indem sie ihre Umgebung durch Datenerfassung wahrnehmen, die gesammelten strukturierten oder unstrukturierten Daten interpretieren, Schlussfolgerungen daraus ziehen oder die aus diesen Daten abgeleiteten Informationen verarbeiten, und über das bestmögliche Handeln zur Erreichung des vorgegebenen Ziels entscheiden".[4] KI zeichnet sich also durch eine gewisse Eigenständigkeit und Autonomie aus.[5]

Der KI wird – im Folgenden beispielhaft durch die Europäische Kommission – das Potenzial zugesprochen, die „Welt zum Besseren zu verändern: Sie kann die Gesundheitsversorgung verbessern, den Energieverbrauch senken, Autos sicherer machen und ermöglicht Landwirten eine effizientere Nutzung von Wasser und Naturressourcen. KI kann eingesetzt werden, um Umwelt- und Klimaveränderungen vorherzusagen, das Management finanzieller Risiken zu verbessern und die Werkzeuge zu schaffen, die wir brauchen, um genau auf unsere Bedürfnisse zugeschnittene Produkte mit weniger Abfällen herzustellen. Sie kann auch helfen, Betrug und Bedrohungen der Cybersicherheit zu erkennen, und versetzt die Strafverfolgungsbehörden in die Lage, Kriminalität wirksamer zu bekämpfen."[6]

Doch es gibt auch mahnende Stimmen. Etwa warnte der britische Physiker Stephen Hawking auf dem Web Summit 2017 davor, dass sich KI als schlimmstes Ereignis in der Geschichte unserer Zivilisation erweisen könnte.[7] Gefahren drohen u.a. der grundrechtlich geschützten Privatsphäre und der informationellen Selbstbestimmung (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG, Art. 7 und 8 GRCh, Art. 8 EMRK), der Meinungsfreiheit und dem Recht auf Gleichbehandlung,[8] denn KI schafft neue Möglichkeiten, das Verhalten von Menschen zu überwachen und auf menschliche Entscheidungen Einfluss zu nehmen (z.B. Algorithmen, die „Filterblasen" begünstigen).

---

4 *Hochrangige Expertengruppe für Künstliche Intelligenz* 2019, S. 6.

5 *Dettling/Krüger*, MMR 2019, 211 (212) bezeichnen „Autonomie" als „Kern von KI". Häufig wird zwischen „starker" (menschenähnlicher) und „schwacher" (stärker determinierter) KI unterschieden, z.B. *Plattform Industrie 4.0* 2019, S. 3 f.; dazu auch *Geminn*, ZD 2021, 354 (355); *Schindler*, ZD-Aktuell 2019, 06647.

6 COM(2019) 168 final, S. 1.

7 Im englischen Original: „worst event in the history of our civilization"; dazu auch *Geminn*, ZD 2021, 354 (354).

8 Z.B. *Ebers u.a.*, RDi 2021, 528 (528), die die Chancen und Risiken von KI inzwischen als „Gemeinplatz" bezeichnen. Speziell zu Diskriminierungsrisiken z.B. *Steege*, MMR 2019 (715).

https://doi.org/10.5771/9783748913344-103, am 22.09.2024, 11:20:46
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

1.2 Regulierungspflicht des Gesetzgebers

Die große Bedeutung und die erheblichen Risiken von KI werfen die Frage auf, ob die Europäische Union oder die Bundesrepublik Deutschland zur gesetzlichen Regulierung von KI verpflichtet sind.[9] Ein Ansatzpunkt hierfür sind die grundrechtlichen Schutzpflichten, die in Deutschland seit längerem anerkannt sind und von deren Existenz auch auf Ebene des Unionsrechts auszugehen ist.[10] Eine Diskussion über die Pflicht des Gesetzgebers, zur Abwehr von Gefahren tätig zu werden, ist in Deutschland insbesondere für den Bereich technischer Neuerungen nachweisbar,[11] etwa wenn durch neue Produkte Gefahren geschaffen werden, die außer Kontrolle geraten können, oder wenn schwerwiegende Machtasymmetrien zu entstehen drohen.[12]

Eine etwaige Pflicht zur Regulierung aufgrund von Schutzpflichten geht jedenfalls mit einem weiten Entscheidungsspielraum des Gesetzgebers einher.[13] Zudem ist zu berücksichtigen, dass KI weder in Deutschland noch in Europa gänzlich ungeregelt ist. So existieren beispielsweise im Datenschutzrecht (z.B. Art. 22 DSGVO zur automatisierten Entscheidungsfindung), im Straßenverkehrsrecht (z.B. §§ 1a ff. StVG zum automatisierten Fahren) oder im Verwaltungsverfahrensrecht (z.B. § 35a VwVfG zum automatisierten Erlass eines Verwaltungsaktes) Vorschriften, die insbesondere auch den Einsatz von KI erfassen. Völlige Untätigkeit kann dem Gesetzgeber daher bisher nicht vorgeworfen werden. Steht staatliches Eingriffshandeln in Frage, ist ferner zu berücksichtigen, dass der Einsatz von KI einer Rechtsgrundlage bedarf (Vorbehalt des Gesetzes), da er andernfalls rechtswidrig ist.[14] Mit der steigenden Verbreitung und Bedeutung von KI in immer mehr Lebensbereichen wächst allerdings der Druck auf den Gesetzge-

9 Z.B. *v. Westphalen*, ZIP 2020, 739 (742) bzgl. der Haftung für Fehlverhalten von KI.

10 Für Dtl. z.B. Merten/Papier/*Calliess*, § 44 Rn. 4 ff.; für die EU z.B. Calliess/Ruffert/*Kingreen*, Art. 51 GRCh Rn. 32 ff. Der EuGH hat aus den Grundfreiheiten Schutzpflichten abgeleitet, z.B. EuGH, NJW 1998, 1931 (1932). Schutzpflichten sind auch in Österreich, Frankreich und Irland sowie der EMRK bekannt, Merten/Papier/*Calliess*, § 44 Rn. 15 f.

11 Z.B. bzgl. Gentechnik *Damm/Hart*, KritV 1987, 183; bzgl. Kernenergie BVerfGE 49, 89 (keine Pflicht zur Regulierung, „die mit absoluter Sicherheit Grundrechtsgefährdungen ausschließt").

12 *Pieroth u.a.*, 2013 Rn. 110 bzgl. der Rspr. des BVerfG.

13 Merten/Papier/*Calliess*, § 44 Rn. 6 bzgl. der Rspr. des BVerfG.

14 S. z.B. die Diskussion um die automatisierte Kennzeichenerkennung, BVerfGE 120, 378; BVerfGE 150, 244; BVerfGE 150, 309.

https://doi.org/10.5771/9783748913344-103, am 22.09.2024, 11:20:46
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

ber, die Entwicklung, den Vertrieb und den Einsatz von KI umfassend zu regulieren.[15] In dieser Hinsicht hat die Europäische Kommission einen bedeutenden Schritt unternommen.

2 Der KI-Verordnungsentwurf der Kommission

Mit dem Entwurf einer Verordnung des Europäischen Parlaments und des Rates zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz[16] (im Folgenden: Verordnungsentwurf bzw. VO-E) vom 21.4.2021 möchte die Kommission sicherstellen, dass „ein einheitlicher Rechtsrahmen insbesondere für die Entwicklung, Vermarktung und Verwendung künstlicher Intelligenz im Einklang mit den Werten der Union" (EG 1 S. 1 VO-E) geschaffen wird. Ziel ist es, „die Entwicklung, Verwendung und Verbreitung künstlicher Intelligenz im Binnenmarkt zu fördern und gleichzeitig einen hohen Schutz öffentlicher Interessen wie Gesundheit und Sicherheit und den Schutz der […] Grundrechte zu gewährleisten" (EG 5 S. 1 VO-E).

Bei dem Verordnungsentwurf handelt es sich um den weltweit ersten Vorschlag für einen Rechtsrahmen für KI,[17] der dazu beitragen soll, „Europa zum globalen Zentrum für vertrauenswürdige künstliche Intelligenz (KI) [zu] machen".[18] Mit ihm knüpft die Kommission an den „Koordinierten Plan für künstliche Intelligenz" (2018), die Ausarbeitungen der Hochrangige Expertengruppe der Europäischen Union für Künstliche Intelligenz (2019) und das „Weißbuch zur künstlichen Intelligenz" (2020) an.[19]

2.1 KI-Systeme, Adressaten und Anwendungsbereich

Im Zentrum des Verordnungsentwurfs steht der Begriff des KI-Systems. Gem. Art. 3 Nr. 1 VO-E ist darunter eine Software zu verstehen, die mit

15 Zur Regulierungsnotwendigkeit auch *Hacker*, NJW 2020, 2142.
16 COM(2021) 206 final.
17 *Bomhard/Merkle*, RDi 2021, 276 (276).
18 *Europäische Kommission*, Pressemitteilung v. 21.4.2021.
19 S. COM(2018) 795 final; https://digital-strategy.ec.europa.eu/en/policies/expert-group-ai; COM(2020) 65 final.

https://doi.org/10.5771/9783748913344-103, am 22.09.2024, 11:20:46
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

einer oder mehreren der in Anhang I[20] aufgeführten Techniken und Konzepte (z.B. maschinelles Lernen, logik- und wissensgestützte Konzepte, statistische Ansätze) entwickelt worden ist und im Hinblick auf eine Reihe von Zielen, die vom Menschen[21] festgelegt werden, Ergebnisse wie Inhalte, Vorhersagen, Empfehlungen oder Entscheidungen hervorbringen kann, die das Umfeld beeinflussen, mit dem sie interagieren. Diese Definition wird als (zu) weit[22] und unscharf[23] empfunden und umfasst auch Software, die Informatiker nicht als KI bezeichnen würden.[24]

Der Verordnungsentwurf adressiert in erster Linie Anbieter, also Personen oder Stellen, die KI-Systeme entwickeln (lassen), um sie unter ihrem eigenen Namen oder ihrer eigenen Marke in Verkehr zu bringen oder in Betrieb zu nehmen (Art. 3 Nr. 2 VO-E), sowie Nutzer von KI-Systemen. Letztere sind Personen oder Stellen, die KI-Systeme in eigener Verantwortung zu nicht persönlichen[25] Tätigkeiten verwenden (Art. 3 Nr. 4 VO-E). In den Anwendungsbereich der vorgesehenen Verordnung fallen gem. Art. 2 Abs. 1 VO-E Anbieter, die KI-Systeme in der Union in Verkehr bringen oder in Betrieb nehmen (lit. a), Nutzer von KI-Systemen, die sich in der Union befinden (lit. b), sowie Anbieter und Nutzer von KI-Systemen, die in einem Drittland niedergelassen oder ansässig sind, wenn das vom System hervorgebrachte Ergebnis in der Union verwendet wird (lit. c). KI-Systeme, die ausschließlich für militärische Zwecke entwickelt oder verwendet werden, werden nicht erfasst (Art. 2 Abs. 3 VO-E).

20 Zur Befugnis der Kommission, delegierte Rechtsakte zur Änderung der Liste der Techniken und Konzepte in Anhang I zu erlassen, s. Art. 4 VO-E.

21 *Grützmacher/Füllsack*, ITRB 2021, 159 (160) werfen die Frage auf, „ob es nicht eines Tages gerade auch durch starke KI definierte Ziele geben wird".

22 *Bomhard/Merkle*, RDi 2021, 276 (277); *Ebers u.a.*, RDi 2021, 528 (529); *Kalbhenn*, ZUM 2021, 663 (664 f.).

23 *Roos/Weitz*, MMR 2021, 844 (845 und 850 f.).

24 *Ebert/Spiecker gen. Döhmann*, NVwZ 2021, 1188 (1189).

25 Wer ein KI-System im Rahmen einer persönlichen und nicht beruflichen Tätigkeit verwendet, ist kein Nutzer i.S.v. Art. 3 Nr. 4 VO-E; krit. *Geminn*, ZD 2021, 354 (356).

https://doi.org/10.5771/9783748913344-103, am 22.09.2024, 11:20:46
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

2.2 Risikobasierter und produktsicherheitsrechtlicher Ansatz

Der Verordnungsentwurf verfolgt einen risikobasierten Ansatz[26] (EG 14 VO-E) und unterteilt KI-Systeme in verschiedene Risikogruppen.[27] Der Begriff des Risikos wird, wie auch in der DSGVO,[28] nicht definiert, scheint jedoch v.a. auf die Bedrohung individueller Schutzgüter abzustellen.[29] KI-Praktiken, denen ein unannehmbares Risiko zugesprochen wird, werden gem. Art. 5 VO-E verboten (Titel II). Für Hochrisiko-KI-Systeme finden sich in Art. 6 ff. VO-E (Titel III) umfangreiche, insbesondere an Anbieter und Nutzer gerichtete Vorgaben. Bestimmte KI-Systeme unterliegen zudem (unabhängig von einer Einordnung als Hochrisiko-KI) den Transparenzpflichten des Art. 52 VO-E (Titel IV). Sonstige KI-Systeme werden der Selbstregulierung gem. Art. 69 VO-E (Titel IX) überlassen.[30]

Die Vorschriften sind in erster Linie produktsicherheitsrechtlicher Natur.[31] Sie enthalten – abgesehen von Art. 5 VO-E – keine Regelungen, die bestimmen, unter welchen Voraussetzungen und in welchen Situationen KI-Systeme zum Einsatz kommen dürfen. Dies gilt auch für die Vorschriften zu Hochrisiko-KI-Systemen, die als „Herzstück[32]" des Verordnungsentwurfs Anforderungen an die technische und organisatorische Ausgestaltung sowie die Sicherheit stellen, aber keine Rechtsgrundlagen[33] oder Ein-

---

26 Zu diesem Ansatz s.a. *Datenethikkommission der Bundesregierung* 2019, S. 173 ff. In der Unterrichtung der Enquete-Kommission „Künstliche Intelligenz" wird ebenfalls einem chancen- und risikobasierten Ansatz das Wort geredet, BT-Drs. 19/23700, S. 490.

27 Zum risikobasierten Ansatz z.B. *Valta/Vasel*, ZRP 2021, 142 (142 f.).

28 Zum Risikobegriff in der DSGVO z.B. *Schröder*, ZD 2019, 503.

29 Vgl. EG 27 S. 3 VO-E, wonach KI-Systeme hochriskant sind, wenn sie „erhebliche schädliche Auswirkungen auf die Gesundheit, die Sicherheit und die Grundrechte von Personen" haben.

30 In der Lit. wird häufig zwischen unannehmbarem, hohem, geringem und minimalem Risiko unterschieden, obwohl der verfügende Teil des VO-E ein geringes oder minimales Risiko nicht erwähnt, z.B. *Ebert/Spiecker gen. Döhmann*, NVwZ 2021, 1188 (1188); s. aber COM(2021) 206 final, S. 15.

31 *Roos/Weitz*, MMR 2021, 844 (845), die ein „spezifisches Produktsicherheitsrecht für Hochrisiko-KI-Systeme" erkennen; *Spindler*, CR 2021, 361 (364), wonach „der Vorschlag […] produktsicherheitsrechtlichen Ansätzen folgt"; *Grützmacher/Füllsack*, ITRB 2021, 159 (159) sehen „eine Art IT-bezogenes Sicherheitsrecht"; *Orssich*, EuZW 2022, 254 (256) spricht von einer „Anlehnung an Produktsicherheitsvorschriften".

32 *Roos/Weitz*, MMR 2021, 844 (844).

33 S. aber die Verarbeitungserlaubnis im Kontext der Beobachtung, Erkennung und Korrektur von Verzerrungen bei Hochrisiko-KI-Systemen gem. Art. 10 Abs. 5 VO-E (i.V.m. Art. 9 Abs. 2 lit. g DSGVO).

https://doi.org/10.5771/9783748913344-103, am 22.09.2024, 11:20:46
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

griffsschwellen formulieren. Auffällig ist zudem, dass der Verordnungsentwurf keine individuellen Rechte für die von dem Einsatz von KI-Systemen betroffenen (z.B. beurteilten oder gesteuerten[34]) Personen vorsieht.[35] Soweit eine Verarbeitung personenbezogener Daten stattfindet, gelten aber die Rechtsgrundlagen und Betroffenenrechte der Datenschutzgesetze (DSGVO, JI-RL).[36]

2.2.1 Verbotene Praktiken im Bereich der KI

Art. 5 Abs. 1 VO-E (Titel II) nennt „manipulative, ausbeuterische und soziale Kontrollpraktiken", die nach Ansicht der Kommission gegen die Werte der Union verstoßen und verboten werden sollen (EG 15 VO-E). Konkret betrifft dies das Inverkehrbringen, die Inbetriebnahme oder die Verwendung von KI-Systemen, die durch den Einsatz von Techniken der unterschwelligen Beeinflussung (lit. a) oder das Ausnutzen der Verletzlichkeit bestimmter Gruppen von Personen (lit. b) physische oder psychische Verletzungen hervorrufen können oder die von Behörden zur Bewertung oder Klassifizierung der Vertrauenswürdigkeit natürlicher Personen auf Grundlage ihres sozialen Verhaltens, persönlicher Eigenschaften oder Persönlichkeitsmerkmale verwendet werden und zu Schlechterstellung oder Benachteiligung führen können (lit. c; sog. „Social Scoring"). Auch soll die Verwendung biometrischer Echtzeit-Fernidentifizierungssysteme in öffentlich zugänglichen Räumen zu Strafverfolgungszwecken verboten werden (lit. d), wobei aber Ausnahmen vorgesehen sind.[37]

2.2.2 Hochrisiko-KI-Systeme

Die Art. 6 ff. VO-E (Titel III) enthalten Anforderungen an Hochrisiko-KI-Systeme. Gemeint sind KI-Systeme, die „erhebliche schädliche Auswirkungen auf die Gesundheit, die Sicherheit und die Grundrechte von Personen in der Union haben" (EG 27 S. 3 VO-E; s.a. Art. 7 Abs. 1 lit. b VO-E). Zu den Hochrisiko-KI-Systemen zählen zum einen KI-Systeme, die als Pro-

34 *Ebert/Spiecker gen. Döhmann*, NVwZ 2021, 1188 (1193).
35 Dazu *Ebers u.a.*, RDi 2021, 528 (537); *Bomhard/Merkle*, RDi 2021, 276 (283).
36 Zum Regelungsspielraum der EU-Mitgliedstaaten s. *Hornung*, DuD 2022 i.E.
37 Überblick z.B. bei *Ebert/Spiecker gen. Döhmann*, NVwZ 2021, 1188 (1189 f.); *Veale/Zuiderveen Borgesius*, CRi 2021, 97 (98 ff.).

https://doi.org/10.5771/9783748913344-103, am 22.09.2024, 11:20:46
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

dukt oder Sicherheitskomponente eines Produkts den Harmonisierungsvorschriften des Anhangs II unterfallen (z.B. Medizinprodukte oder Fahrzeuge) und einer Konformitätsbewertung durch Dritte unterzogen werden müssen (Art. 6 Abs. 1 VO-E). Zum anderen gelten die in Anhang III genannten KI-Systeme als hochriskant (Art. 6 Abs. 2 VO-E). Anhang III erfasst u.a. KI-Systeme in den Bereichen biometrische Identifizierung und Kategorisierung, Verwaltung und kritische Infrastrukturen, Bildung und Beschäftigung, Strafverfolgung, Migration und Grenzkontrolle sowie Rechtspflege. Gem. Art. 7 VO-E wird der Kommission die Befugnis übertragen, delegierte Rechtsakte zur Änderung der Liste in Anhang III zu erlassen, um Hochrisiko-KI-Systeme hinzuzufügen.

Hochrisiko-KI-Systeme müssen die Anforderungen der Art. 8 bis 15 VO-E erfüllen. Dies betrifft die Einrichtung eines Risikomanagementsystems (Art. 9 VO-E), Qualitätskriterien für Trainings-, Validierungs- und Testdatensätze (Art. 10 VO-E[38]), technische Dokumentationen (Art. 11 VO-E), automatische Aufzeichnungen bzw. Protokollierungen (Art. 12 VO-E), die Bereitstellung von Informationen für Nutzer einschließlich einer Gebrauchsanweisung (Art. 13 VO-E[39]), eine wirksame menschliche Aufsicht (Art. 14 VO-E[40]) sowie ein angemessenes Maß an Genauigkeit, Robustheit und Cybersicherheit (Art. 15 VO-E).[41] Die Erfüllung dieser Anforderungen ist durch die Anbieter (Art. 3 Nr. 2 VO-E) sicherzustellen (Art. 16 lit. a VO-E).

Als wahrscheinlich wichtigste Anforderung[42] müssen Anbieter von Hochrisiko-KI-Systemen gem. Art. 19 Abs. 1 i.V.m. Art. 16 lit. e VO-E sicherstellen, dass ihre Systeme vor dem Inverkehrbringen oder der Inbetriebnahme einer Konformitätsbewertung nach Art. 43 VO-E unterzogen werden.[43] Zudem trifft Anbieter u.a. die Pflicht, ein Qualitätsmanagement einzurichten (Art. 17 VO-E), die in Art. 11 VO-E genannte technische Do-

38 Krit. *Ebers u.a.*, RDi 2021, 528 (533) bzgl. der Anforderung, dass die Datensätze fehlerfrei sein müssen (Art. 10 Abs. 3 VO-E), was technisch unmöglich sei.

39 Krit. *Ebers u.a.*, RDi 2021, 528 (533 f.), die die Vorgaben für zu allgemein halten.

40 Krit. *Ebers u.a.*, RDi 2021, 528 (534) u.a. bzgl. der Anforderung, dass es Menschen ermöglicht werden muss, Fähigkeiten und Grenzen des Hochrisiko-KI-Systems vollständig zu verstehen, was unrealistisch sei; ebenfalls *Geminn*, ZD 2021, 354 (357).

41 Ausführlich z.B. *Spindler*, CR 2021, 361 (366 ff.); *Kalbhenn*, ZUM 2021, 663 (667 ff.).

42 *Ebert/Spiecker gen. Döhmann*, NVwZ 2021, 1188 (1191).

43 Krit. zur Ausgestaltung bei Hochrisiko-KI-Systemen nach Anhang III *Ebers u.a.*, RDi 2021, 528 (533); ausführlich zur Konformitätsbewertung *Spindler*, CR 2021, 361 (369 ff.).

https://doi.org/10.5771/9783748913344-103, am 22.09.2024, 11:20:46
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

kumentation zu erstellen (Art. 18 VO-E) und Korrekturmaßnahmen zu ergreifen, wenn das KI-System nicht der Verordnung entspricht (Art. 21 VO-E). Ferner müssen Anbieter gem. Art. 61 VO-E ein „Post-Market Monitoring“[44] vornehmen und schwerwiegende Vorfälle oder Fehlfunktionen melden (Art. 62 VO-E), was an die Meldepflicht gem. Art. 33 DSGVO erinnert.[45] Überdies sind Hochrisiko-KI-Systeme i.S.v. Art. 6 Abs. 2 VO-E gem. Art. 51 VO-E vor dem Inverkehrbringen oder der Inbetriebnahme vom Anbieter in einer EU-Datenbank (Art. 60 VO-E) zu registrieren.

Weit weniger Pflichten treffen die Nutzer. Sie müssen das Hochrisiko-KI-System entsprechend der beigefügten Gebrauchsanweisung verwenden (Art. 29 Abs. 1 i.V.m. Art. 13 Abs. 2 und 3 VO-E), dafür sorgen, dass die Eingabedaten mit Blick auf die Zweckbestimmung relevant sind (Art. 29 Abs. 3 VO-E), und den Betrieb anhand der Gebrauchsanweisung überwachen (Art. 29 Abs. 4 VO-E). Sie sind unter bestimmten Voraussetzungen verpflichtet, Anbieter und Händler über Risiken und Vorfälle sowie Fehlfunktionen zu informieren. Die gem. Art. 13 VO-E bereitgestellten Informationen haben sie ggf. für die Durchführung einer Datenschutz-Folgenabschätzung gem. Art. 35 DSGVO zu verwenden (Art. 29 Abs. 6 VO-E).

Pflichten treffen gem. Art. 24, 26 bis 28 ff. VO-E auch Hersteller, Einführer (Art. 3 Nr. 6 VO-E) sowie Händler (Art. 3 Nr. 7 VO-E). Für Hochrisiko-KI-Systeme im Anwendungsbereich bestimmter produktsicherheitsrechtlicher Rechtsakte (Kraftfahrzeuge, Eisenbahnen, Schiff- und Luftfahrt) gilt gem. Art. 2 Abs. 2 VO-E nur Art. 84 VO-E, der die Bewertung und Überarbeitung der vorgesehenen Verordnung regelt.[46]

2.2.3 Transparenzpflichten

Art. 52 VO-E (Titel IV) enthält Transparenzpflichten für KI-Systeme, die für die Interaktion mit natürlichen Personen bestimmt sind (Abs. 1), für Emotionserkennungssysteme und Systeme zur biometrischen Kategorisierung (Abs. 2) sowie für KI-Systeme, die „Deep-Fakes“ hervorbringen (Abs. 3). Dabei sind Ausnahmen im Kontext der Aufdeckung, Verhütung, Ermittlung und Verfolgung von Straftaten (Abs. 2 und 3) sowie der Meinungs-, Wissenschafts- und Kunstfreiheit (Abs. 3) vorgesehen.

---

44 *Geminn*, ZD 2021, 354 (357).

45 S. *Spindler*, CR 2021, 361 (372).

46 Zu den dahinterstehenden Konzepten des „New Legislative Framework“ und des „Old Approach“ *Spindler*, CR 2021, 361 (364); *Roos/Weitz*, MMR 2021, 844 (845).

https://doi.org/10.5771/9783748913344-103, am 22.09.2024, 11:20:46
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

Durch die Transparenzpflichten soll sichergestellt werden, dass Personen, die mit den genannten KI-Systemen interagieren bzw. mit „Deepfakes" in Berührung kommen, darüber informiert werden, damit sie bewusste Entscheidungen treffen und bestimmte Situationen vermeiden können.[47] Ein Recht auf menschliche Intervention (vgl. Art. 22 Abs. 3 DSGVO) oder einen Dienst ohne KI gewährt Art. 52 VO-E nicht.[48] Sollte eines der in Art. 52 VO-E aufgeführten Systeme gleichzeitig ein Hochrisiko-KI-System sein (z.B. ein System zur Emotionserkennung, das gleichzeitig Anhang III Nr. 6 lit. b oder Nr. 7 lit. a unterfällt[49]), greifen zudem die Vorschriften in Titel III (Art. 52 Abs. 4 VO-E).

2.2.4 Sonstige KI-Systeme

KI-Systeme, die den eben dargestellten Vorschriften in Ermangelung eines besonderen Risikos nicht unterfallen (z.B. KI-gestützte Videospiele sowie Spamfilter[50]), können auf freiwilliger Basis Verhaltenskodizes (sog. „Codes of Conduct") unterworfen werden (Art. 69 VO-E).[51]

2.3 Innovationsförderung, Aufsicht, Sanktionen

Die Art. 53 ff. VO-E (Titel V) enthalten Regelungen zur Innovationsförderung. Dies betrifft v.a. die Einrichtung von KI-Reallaboren, „um die Entwicklung und Erprobung innovativer KI-Systeme […] unter strenger Regulierungsaufsicht zu erleichtern" (EG 71 S. 2 VO-E). Zudem sind Aufsichts- und Überwachungsstrukturen vorgesehen (Titel VI). So soll – vergleichbar dem Europäischen Datenschutzausschuss (Art. 68 ff. DSGVO) – ein Europäischer Ausschuss für künstliche Intelligenz eingerichtet werden (Art. 56 ff. VO-E). Ferner sind nationale Aufsichtsbehörden zu benennen (Art. 59 VO-E).[52] Gem. Art. 60 VO-E (Titel VII) soll die Kommission in Zusammenarbeit mit den Mitgliedstaaten eine EU-Datenbank für Hochrisiko-KI-Systeme nach Art. 6 Abs. 2 VO-E errichten und pflegen. Verstöße ge-

47 COM(2021) 206 final, S. 17.
48 *Spindler*, CR 2021, 361 (368 und 374), der dem krit. gegenübersteht.
49 S. *Orssich*, EuZW 2022, 254 (260).
50 *Grützmacher/Füllsack*, ITRB 2021, 159 (161).
51 Dazu *Spindler*, CR 2021, 361 (371).
52 Dazu *Spindler*, CR 2021, 361 (372).

https://doi.org/10.5771/9783748913344-103, am 22.09.2024, 11:20:46
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

gen die vorgesehene Verordnung sollen u.a. mit Geldbußen geahndet werden (Art. 71 f. VO-E, Titel X).

3 Biometrische Erkennung im KI-Verordnungsentwurf

In dem Verordnungsentwurf nimmt die biometrische Erkennung eine herausgehobene Stellung ein, was sich in den zahlreichen Erwähnungen im Gesetzestext (z.B. Art. 3 Nrn. 33 bis 38, Art. 5 Abs. 1 lit. d, Art. 6 Abs. 2 i.V.m. Anhang III Nr. 1, Art. 52 Abs. 2 VO-E) und in den Erwägungsgründen (EG 7, 8, 18 bis 24, 33, 64, 65, 70 VO-E) zeigt.

3.1 Biometrische Erkennung und biometrische Daten

Biometrische Erkennung ist die automatisierte Erkennung von Menschen anhand biologischer oder verhaltensbezogener Merkmale.[53] Dafür werden bestimmte – idealerweise bei jedem Menschen einzigartige – biologische (bzw. körperliche) oder verhaltenstypische Merkmale eines Menschen erfasst (z.B. Struktur der Iris oder der Papillarleisten, spezifische Merkmale des Gesichts, Eigenarten des Gangs etc.) und automatisiert mit vorab hinterlegten Merkmalssätzen (Referenzdaten) verglichen. Wird eine hohe Übereinstimmung errechnet, spricht dies dafür, dass die verglichenen Merkmalssätze zur selben Person gehören.

Ein solches Verständnis zeigt sich auch in Art. 3 Nr. 33 VO-E.[54] Demnach sind biometrische Daten mit speziellen technischen Verfahren gewonnene personenbezogene Daten zu den physischen, physiologischen oder verhaltenstypischen Merkmalen einer natürlichen Person, die die eindeutige Identifizierung dieser Person ermöglichen oder bestätigen. Auch in dieser Definition kommt zum Ausdruck, dass auf den Körper oder das Verhalten eines Menschen bezogene Merkmale genutzt werden, um den Merkmalsträger zu erkennen bzw. zu identifizieren. Von dem erforderlichen Personenbezug (Art. 4 Nr. 1 DSGVO, Art. 3 Nr. 1 JI-RL) ist bei Informationen über Merkmale, die sich auf eine natürliche Person beziehen und diese identifizierbar machen, regelmäßig auszugehen.

---

53 ISO/IEC 2382-37:2017, S. 2: „automated recognition of individuals based on their biological and behavioural characteristics“, s. https://standards.iso.org/ittf/PubliclyAvailableStandards/index.html.

54 Die Vorschrift ist wortgleich mit Art. 4 Nr. 14 DSGVO, Art. 3 Nr. 13 JI-RL.

https://doi.org/10.5771/9783748913344-103, am 22.09.2024, 11:20:46
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

3.2 Biometrische Erkennung als verbotene Praktik

Art. 5 Abs. 1 lit. d VO-E verbietet die Verwendung biometrischer Echtzeit-Fernidentifizierungssysteme in öffentlich zugänglichen Räumen zu Strafverfolgungszwecken, nicht aber die Herstellung oder den Vertrieb solcher Systeme.

Fernidentifizierungssysteme sind KI-Systeme, die dem Zweck dienen, natürliche Personen aus der Ferne durch Abgleich biometrischer Daten mit den in einer Referenzdatenbank gespeicherten biometrischen Daten zu identifizieren, ohne dass der Nutzer des KI-Systems vorher weiß, ob die Person anwesend sein wird und identifiziert werden kann (Art. 3 Nr. 36 VO-E). Echtzeit bedeutet, dass die Erfassung biometrischer Daten, der Abgleich und die Identifizierung ohne erhebliche Verzögerung erfolgen (Art. 3 Nr. 37 VO-E). Dies umfasst „die Verwendung von ‚Live-Material' oder ‚Near-live-Material' wie Videoaufnahmen" (EG 8 S. 5 VO-E). Da die Identifizierung „aus der Ferne" möglich sein muss, werden Systeme, die einen unmittelbaren Kontakt der zu erkennenden Person zu den Sensoren des Systems erfordern (z.B. berührungsbasierende Fingerabdruckerkennungssysteme), nicht erfasst. Zu fordern ist ein gewisser Abstand. Entscheidend ist dabei aber nicht so sehr, wie viele Meter der Sensor des biometrischen Systems von der betroffenen Person entfernt ist, sondern dass die Erkennung ohne Mitwirkung – und damit ggf. auch ohne Wissen – der Person erfolgen kann, woraus sich eine besondere Belastung (z.B. die Ungewissheit, ob eine Erkennung stattgefunden hat) ergeben kann.[55]

Zu denken ist v.a. an Gesichtserkennungssysteme,[56] die es in Verbindung mit Videoüberwachung erlauben, in öffentlich zugänglichen Räumen (Art. 3 Nr. 39 VO-E) Personen auf Entfernungen von vielen Metern ohne deren Mitwirkung zu erfassen und durch einen unverzüglich stattfindenden Abgleich mit den Aufnahmen in einer Referenzdatenbank zu identifizieren. Der Einsatz solcher Systeme zu Strafverfolgungszwecken, also zur Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten durch die zuständigen Behörden (Art. 3 Nrn. 41 und 40 VO-E), wurde in Deutschland bereits in Pilotprojekten erprobt (z.B. „Sicherheitsbahnhof Berlin Südkreuz").[57] Er zielt darauf ab, Personen aufzuspüren, nach denen zur Verhinderung oder Verfolgung von Straftaten gefahndet wird.

---

55 S. *Schindler*, ZD-Aktuell 2021, 05221.

56 Ggf. auch Gangerkennung, die ebenfalls auf Entfernung möglich ist.

57 Z.B. *Salzmann/Schindler*, ZD-Aktuell 2018, 06344; *Schindler*, ZD-Aktuell 2017, 05799.

https://doi.org/10.5771/9783748913344-103, am 22.09.2024, 11:20:46
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

Der Verordnungsentwurf enthält kein ausnahmsloses Verbot, sondern erlaubt gem. Art. 5 Abs. 1 lit. d VO-E die Verwendung in öffentlich zugänglichen Räumen zu Strafverfolgungszwecken, wenn dies „unbedingt erforderlich" ist für die gezielte Suche nach Opfern von Straftaten oder vermissten Kindern (i), für die Abwehr konkreter, erheblicher und unmittelbarer Gefahren für das Leben oder die körperliche Unversehrtheit natürlicher Personen oder eines Terroranschlags (ii) oder für das Erkennen, Aufspüren, Identifizieren oder Verfolgen von Tätern oder Verdächtigen bestimmter schwerwiegender Straftaten (iii).

In Art. 5 Abs. 2 bis 4 VO-E finden sich weitere Anforderungen. Gem. Abs. 2 sind die der Verwendung zugrundeliegende Situation, insbesondere der drohende Schaden, wenn das System nicht eingesetzt würde, und die Folgen der Verwendung des Systems (Schwere, Wahrscheinlichkeit, Ausmaß) für die Rechte und Freiheiten betroffener Personen zu berücksichtigen. Dies läuft auf eine Verhältnismäßigkeitsprüfung hinaus.[58] Ferner werden notwendige und verhältnismäßige Schutzmaßnahmen und Bedingungen (zeitliche und räumliche Beschränkungen) gefordert. Abs. 3 verlangt zudem eine vorherige Genehmigung durch eine Justizbehörde oder eine unabhängige Verwaltungsbehörde des Mitgliedstaats, die nur erteilt werden darf, wenn der Einsatz des Systems unter Berücksichtigung von Abs. 2 für das Erreichen eines der in Abs. 1 lit. d genannten Ziele notwendig und verhältnismäßig ist. Über die Möglichkeit einer Genehmigung entscheiden die Mitgliedstaaten gem. Abs. 4 in „detaillierten nationalen Rechtsvorschriften" (EG 22 S. 1 VO-E), die die Beantragung, Erteilung und Ausübung der Genehmigung regeln. Mithin bedarf es spezifischer gesetzlicher Rechtsgrundlagen, die sich mit den Voraussetzungen der Verwendung biometrischer Echtzeit-Identifizierungssysteme in öffentlich zugänglichen Räumen zu Strafverfolgungszwecken auseinandersetzen.

Diese Anforderungen werden z.T. als unzureichend kritisiert.[59] Es würden „Tür und Tor für eine biometrische Erkennung eröffnet".[60] Auch dem Europäischen Datenschutzausschuss und dem Europäischen Datenschutzbeauftragten geht das Verbot nicht weit genug.[61] Dem ist zuzugeben, dass

58 S.a. EG 20 S. 1 VO-E, wonach sichergestellt werden soll, „dass diese Systeme verantwortungsvoll und verhältnismäßig genutzt werden".

59 Z.B. *Spindler*, CR 2021, 361 (374), der die zahlreichen Ausnahmetatbestände kritisiert; *Ebert/Spiecker gen. Döhmann*, NVwZ 2021, 1188 (1190); *Ebers u.a.*, RDi 2021, 528 (531).

60 *Spindler*, CR 2021, 361 (365).

61 *EDSA/EDSB*, Gemeinsame Stellungnahme 5/2021; dazu auch *o.V.*, ZD-Aktuell 2021, 05266.

https://doi.org/10.5771/9783748913344-103, am 22.09.2024, 11:20:46
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

die Verwendung biometrischer Echtzeit-Fernidentifizierungssysteme (v.a. Gesichtserkennung) in öffentlich zugänglichen Räumen zu Strafverfolgungszwecken erhebliche Eingriffe in das Grundrecht auf informationelle Selbstbestimmung bzw. Schutz personenbezogener Daten (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG, Art. 7 und 8 GRCh,[62] Art. 8 EMRK[63])[64] hervorrufen kann, da regelmäßig zahlreiche Personen erfasst werden, die hierfür keinen Anlass gegeben haben, was Einschüchterungseffekte mit sich bringt.[65] Zudem wird mit dem Gesicht auf ein höchstpersönliches[66] Merkmal zurückgegriffen und die Erstellung von Bewegungsprofilen ermöglicht.[67] All dies kann, wie in EG 18 S. 1 VO-E dargelegt, „die Privatsphäre [besser: informationelle Selbstbestimmung] eines großen Teils der Bevölkerung" beeinträchtigen und „ein Gefühl der ständigen Überwachung" hervorrufen. Daran anknüpfend fordert eine Europäische Bürgerinitiative[68], ein Verbot „biometrischer Massenüberwachung".[69] Es ist anzunehmen, dass diese Forderung Einfluss auf den Verordnungsentwurf gehabt hat.[70]

---

62 Zum str. Verhältnis von Art. 7 zu Art. 8 GRCh z.B. Meyer/Hölscheidt/*Bernsdorff*, Art. 8 Rn. 13.

63 Zu Art. 8 EMRK als Datenschutzgrundrecht z.B. Karpenstein/Mayer/*Pätzold*, Art. 8 EMRK Rn. 28 ff.

64 Wird biometrische Erkennung durch staatliche deutsche Stellen eingesetzt, ist dies zunächst an den deutschen Grundrechten zu messen, Art. 1 Abs. 3 GG. Bei Durchführung des Rechts der Union sind gem. Art. 51 Abs. 1 S. 1 GRCh zudem europäische Grundrechte anwendbar. Da die Verarbeitung biometrischer Daten zur Bekämpfung von Straftaten in den Anwendungsbereich der JI-Richtlinie fällt (s.u.), ist von einer Durchführung des Unionsrechts auszugehen (str., z.B. Lisken/Denninger/*Müller/Schwabenbauer*, Kap. G Rn. 385 ff.). Dies würde v.a. mit Blick auf Art. 5 Abs. 1 lit. d, Abs. 2 bis 4 VO-E erst recht bei Inkrafttreten des Verordnungsentwurfs gelten. Zum schwierigen Verhältnis der deutschen und europäischen Grundrechte zueinander z.B. *Lehner*, JA 2022, 177; *Preßlein*, EuR 2021, 247. Hinzu tritt die EMRK, die bei Auslegung der deutschen und europäischen Grundrechte zu berücksichtigen ist, s. BVerfGE 111, 307 (315 ff.) u. Art. 52 Abs. 3, 53 GRCh. Der Verordnungsentwurf an sich ist als Rechtsakt der Organe der Union (grds. nur; s. aber die Solange-Rspr. des BVerfG) an der Grundrechtecharta zu messen, Art. 51 Abs. 1 S. 1 GRCh.

65 Z.B. BVerfGE 120, 378 (402) bzgl. automatisierter Kennzeichenerkennung.

66 BVerfGE 150, 244 (269) zählt das Gesicht zu den höchstpersönlichen Merkmalen.

67 Ausführlich zur rechtlichen Einordnung *Schindler* 2021.

68 *Zivilgesellschaftliche Initiative für ein Verbot biometrischer Massenüberwachung*, ABl. 2021/L 13/1.

69 S. die Website der Initiative unter https://reclaimyourface.eu/de/.

70 Politische Hintergründe vermuten auch *Ebert/Spiecker gen. Döhmann*, NVwZ 2021, 1188 (1190).

https://doi.org/10.5771/9783748913344-103, am 22.09.2024, 11:20:46
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

Allerdings ist auch die große Bedeutung einer effektiven Bekämpfung von Straftaten[71] zu berücksichtigen, die in bestimmten Situationen für die Verwendung biometrischer Echtzeit-Fernidentifizierungssysteme in öffentlich zugänglichen Räumen sprechen kann. Ein vollständiges Verbot ist daher nicht zielführend. Mit Blick auf die erheblichen Grundrechtseingriffe, die von biometrischen Echtzeit-Fernidentifizierungssystemen in öffentlich zugänglichen Räumen ausgehen können, müssen – unabhängig von dem Verordnungsentwurf – strenge Anforderungen erfüllt werden, um einen Einsatz zu rechtfertigen. Erforderlich ist sowohl nach deutschem als auch nach europäischem Recht eine gesetzliche Grundlage (Vorbehalt des Gesetzes),[72] die höchsten Bestimmtheit- und Verhältnismäßigkeitsanforderungen genügen muss. Dies umfasst spezifische Eingriffsschwellen, die ein angemessenes Verhältnis zwischen den verfolgten Zielen und der Schwere des Eingriffs herstellen, räumliche und zeitliche Begrenzungen, die einen flächendeckenden Einsatz verhindern, den Ausschluss oder zumindest die strenge Eingrenzung der Erstellung von Bewegungsprofilen, einen Richtervorbehalt sowie weitere technische und organisatorische Maßnahmen, um einen ausreichenden Grundrechtsschutz zu gewährleisten.[73] Dass durch Art. 5 Abs. 1 lit. d, Abs. 2 bis 4 VO-E strengere Anforderungen aufgestellt werden, ist nicht erkennbar.

Überdies sind, da bei Verwendung biometrischer Echtzeit-Fernidentifizierungssysteme personenbezogene (biometrische) Daten durch die zuständigen Behörden zum Zweck der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten verarbeitet werden, die (in nationales Recht umzusetzenden) Vorgaben der JI-Richtlinie zu beachten (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 JI-RL).[74] Die Regelungen in Art. 5 Abs. 1 lit. d, Abs. 2 bis 4 VO-E sollen dabei als lex specialis zu Art. 10 JI-RL, der neben Art. 8 JI-RL zusätzliche Anforderungen u.a. an die Verarbeitung biometrischer Daten (Art. 3 Nr. 13 JI-RL) stellt, verstanden werden (EG 23 VO-E). Hinsichtlich der Betroffenenrechte (zu denen der Verordnungsentwurf keine Regelungen enthält) sowie der sonstigen datenschutzrechtlichen Pflichten des Verantwortlichen gilt ebenfalls die JI-Richtlinie.

Insgesamt sind die Auswirkungen von Art. 5 Abs. 1 lit. d, Abs. 2 bis 4 VO-E auf die materiell-rechtliche Situation – zumindest in Deutschland – überschaubar. Aufgrund des Vorbehalts des Gesetzes ist die Verwendung

71 Z.B. betont BVerfGE 100, 313 (389) „die unabweisbaren Bedürfnisse einer wirksamen Strafverfolgung".
72 Auf europäischer Ebene s. Art. 52 Abs. 1 S. 1 GRCh („gesetzlich vorgesehen").
73 *Hornung/Schindler*, ZD 2017, 203 (207 f.).
74 Zum Anwendungsbereich s. *Hornung u.a.*, ZIS 2018, 566 (569 ff.).

https://doi.org/10.5771/9783748913344-103, am 22.09.2024, 11:20:46
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

biometrischer Echtzeit-Fernidentifizierungssysteme in öffentlich zugänglichen Räumen zu Strafverfolgungszwecken auch ohne Art. 5 Abs. 1 lit. d VO-E verboten, solange keine verfassungskonforme Rechtsgrundlage besteht, was für biometrische Gesichtserkennung in Deutschland derzeit nicht der Fall ist.[75] Die in Art. 5 Abs. 1 lit. d, Abs. 2 bis 4 VO-E aufgestellten Anforderungen gehen nicht über diejenigen hinaus, die auch nach bisher geltendem Recht zu stellen sind. Auffällig ist zudem, dass die Verwendung biometrischer Echtzeit-Fernidentifizierungssysteme in öffentlich zugänglichen Räumen nur zu Strafverfolgungszwecken verboten werden soll, nicht aber, wenn staatliche oder nichtstaatliche Stellen solche Systeme zu anderen Zwecken verwenden, obwohl dies nicht weniger stark in die Rechte betroffener Personen eingreifen kann (und eine Verwendung zu Strafverfolgungszwecken noch am ehesten zu rechtfertigen ist).[76]

3.3 Biometrische Erkennung als Hochrisiko-KI

Gem. Art. 6 Abs. 2 VO-E i.V.m. Anhang III Nr. 1 werden KI-Systeme, die bestimmungsgemäß für die biometrische Echtzeit-Fernidentifizierung (Art. 3 Nr. 37 VO-E) und die nachträgliche biometrische Fernidentifizierung (Art. 3 Nr. 38 VO-E) natürlicher Personen verwendet werden sollen, als Hochrisiko-KI-Systeme eingeordnet,[77] was v.a. mit möglicherweise „verzerrten Ergebnissen" aufgrund technischer Ungenauigkeiten, die eine „diskriminierende Wirkung" haben können, begründet wird (EG 33 VO-E).

Dies bedeutet zunächst, dass biometrische Echtzeit-Fernidentifizierungssysteme i.S.v. Art. 5 Abs. 1 lit. d VO-E gleichzeitig Hochrisiko-KI-Systeme sind. Anhang III Nr. 1 geht aber darüber hinaus, da keine Beschränkung auf die Verwendung in öffentlichen Räumen zu Strafverfolgungszwecken vorgesehen ist und sowohl staatliche als auch nichtstaatliche Akteure adressiert werden. Außerdem werden Systeme zur nachträglichen biometrischen Fernidentifizierung genannt. Dabei handelt es sich um Fernidentifizierungssysteme, die keine Echtzeit-Fernidentifizierungssysteme sind (Art. 3 Nr. 38 VO-E). Dies meint gem. EG 8 S. 6 und 7 VO-E Systeme, bei denen „die biometrischen Daten schon zuvor erfasst [wurden] und der Ab-

75 S. *Hornung/Schindler*, ZD 2017, 203 (207 f.).

76 Angesprochen auch bei *Veale/Zuiderveen Borgesius*, CRi 2021, 97 (101).

77 Ferner ist es denkbar, dass biometrische Erkennung als Sicherheitskomponente (Art. 3 Nr. 14 VO-E, z.B. zur Absicherung vor unbefugten Zugriffen) eines unter Anhang II fallenden Produkts zum Einsatz kommt und damit ebenfalls als Hochrisiko-KI einzuordnen ist.

https://doi.org/10.5771/9783748913344-103, am 22.09.2024, 11:20:46
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

gleich und die Identifizierung […] erst mit erheblicher Verzögerung [erfolgt]". Zu denken ist z.B. an „Bild- oder Videoaufnahmen, die von Video-Überwachungssystemen oder privaten Geräten vor der Anwendung des KI-Systems […] erzeugt wurden". In der Praxis betrifft dies u.a. Gesichtserkennungssysteme, bei denen „aus der Ferne" (Art. 3 Nr. 36 VO-E) erstellte Videoaufnahmen erst mit deutlicher zeitlicher Verzögerung (ggf. Tage oder Wochen nach der Anfertigung) ausgewertet werden. Da letztlich nahezu jedem Gesichtserkennungssystem Gesichtsbilder aus vorab angefertigten Videoaufnahmen zugeführt werden können, ist entscheidend, dass dies „bestimmungsgemäß" erfolgt (Anhang III Nr. 1). Erfasst werden etwa Gesichtserkennungssysteme, wie sie im Nachgang der Ausschreitungen während des G20-Gipfels in Hamburg zum Einsatz kamen. Zur Aufklärung begangener Straftaten hatte die Polizei in den Wochen und Monaten nach dem Gipfel mehrere Terabyte an Videodaten (polizeiliche und private Aufnahmen) in ein Gesichtserkennungssystem eingespielt und für die biometrische Suche aufbereitet. In der so geschaffenen Referenzdatenbank wurden Suchläufe mit Lichtbildaufnahmen tatverdächtiger Personen durchgeführt, um Erkenntnisse über das Vor- und Nachtatverhalten sowie weitere Straftaten dieser Personen zu gewinnen.[78]

Auf die Frage, ob und unter welchen Voraussetzungen ein Einsatz von Hochrisiko-KI-Systemen zulässig ist, geben die Art. 8 ff. VO-E keine Antwort. Sie enthalten weder Rechtsgrundlagen noch Eingriffsschwellen.[79] Maßgeblich sind somit die allgemeinen, v.a. auch datenschutzrechtlichen Vorschriften (z.B. Art. 6 und 9 DSGVO). Hinsichtlich der Anforderungen, die in dem Verordnungsentwurf an Hochrisiko-KI-Systeme gestellt werden, gelten für biometrische Fernidentifizierungssysteme einige Besonderheiten.

Art. 12 Abs. 4 VO-E sieht vor, dass die Protokollierungsfunktion in der Lage sein muss, den Zeitraum der Verwendung, die Referenzdatenbank, bestimmte Eingabedaten und die Identität der menschlichen Aufsichtspersonen festzuhalten. Art. 14 Abs. 5 VO-E bestimmt, dass das System so gestaltet sein muss, dass der Nutzer keine Maßnahmen oder Entscheidungen allein aufgrund des vom System hervorgebrachten Identifizierungsergebnisses trifft, solange dies nicht von mindestens zwei natürlichen Personen überprüft und bestätigt wurde. Diese Anforderung kann bei Echtzeit-Fer-

78 S. *Salzmann/Schindler*, ZD-Aktuell 2018, 06344. Der HmbBfDI hat die Löschung der Referenzdatenbank angeordnet. Der Bescheid wurde vom VG Hamburg (Urt. v. 23.10.2019, 17 K 203/19) aufgehoben, krit. *Mysegades*, NVwZ 2020, 852.

79 Allerdings sieht Art. 29 Abs. 4 VO-E vor, dass die Nutzer die Verwendung in bestimmten Situationen aussetzen.

https://doi.org/10.5771/9783748913344-103, am 22.09.2024, 11:20:46
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

nidentifizierungssystemen zu Strafverfolgungszwecken problematisch sein, wenn auf eine Identifizierung eine sofortige Reaktion angezeigt ist (z.B. bei Identifizierung eines gesuchten Terrorverdächtigen an einem belebten Ort). Für derartige Situationen sollten Ausnahmen vorgesehen werden.

Bei den in Anhang III Nrn. 2 bis 8 aufgeführten Hochrisiko-KI-Systemen sieht Art. 43 Abs. 2 VO-E ein Konformitätsbewertungsverfahren auf Grundlage interner Kontrolle gem. Anhang VI vor. Für biometrische Systeme i.S.v. Anhang III Nr. 1 bestimmt Art. 43 Abs. 1 VO-E hingegen, dass, so keine harmonisierenden Normen oder gemeinsame Spezifikationen gem. Art. 40 und 41 VO-E vorliegen, das Verfahren mit einer Zertifizierungsstelle nach Anhang VII greift.[80]

Insgesamt sind die Anforderungen an Hochrisiko-KI-Systeme zu begrüßen, auch wenn sie häufig sehr allgemein gehalten sind[81] und teilweise, gerade auch bei biometrischen Systemen, schlicht unerfüllbar scheinen (z.B. Fehlerfreiheit von Trainingsdaten gem. Art. 10 Abs. 3 VO-E[82], vollständiges Verstehen der Fähigkeiten und Grenzen gem. Art. 14 Abs. 4 lit. a VO-E[83]). Zu bedenken ist ferner, dass die nachträgliche biometrische Fernidentifizierung (Anhang III Nr. 1) zu Strafverfolgungszwecken, wenn sie auf der systematischen Auswertung umfangreicher Videoaufnahmen beruht, ähnlich schwerwiegende Grundrechtseingriffe hervorrufen kann, wie die dem Verbot gem. Art. 5 Abs. 1 lit. d VO-E unterfallende Echtzeit-Fernidentifizierung (z.B. bei Erstellung umfassender Bewegungsprofile). Durch Verzögerung der Auswertung der Aufnahmen um ein paar Stunden, kann das Verbot dem Wortlaut nach umgangen werden.[84]

3.4 Emotionserkennung und biometrische Kategorisierung

Gem. Art. 52 Abs. 2 VO-E müssen Verwender[85] eines Emotionserkennungssystems oder eines Systems zur biometrischen Kategorisierung die davon betroffenen natürlichen Personen über den Betrieb des Systems informieren. In welcher Form zu informieren ist, wird nicht näher be-

80 Dazu *Spindler*, CR 2021, 361 (370).
81 Z.B. *Ebers*, RDi 2021, 588 (590).
82 *Ebers u.a.*, RDi 2021, 528 (533).
83 *Ebers u.a.*, RDi 2021, 528 (534).
84 Angerissen auch bei *Veale/Zuiderveen Borgesius*, CRi 2021, 97 (101).
85 Der Begriff wird nicht definiert und nur in Art. 52 Abs. 2 VO-E genutzt. Es ist anzunehmen, dass damit der Nutzer (Art. 3 Nr. 4 VO-E: „Stelle, die ein KI-System in eigener Verantwortung verwendet") gemeint ist.

https://doi.org/10.5771/9783748913344-103, am 22.09.2024, 11:20:46
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

stimmt. Hier bietet sich eine Anlehnung an Art. 12 Abs. 1 DSGVO an (klare und einfache Sprache etc.). Zu der Frage, unter welchen inhaltlichen Voraussetzungen eine Verwendung zulässig ist, verhält sich die Vorschrift ebenfalls nicht.

Emotionserkennungssysteme[86] sind KI-Systeme, die Emotionen oder Absichten natürlicher Personen auf der Grundlage ihrer biometrischen Daten feststellen oder daraus ableiten (Art. 3 Nr. 34 VO-E). Die Bezugnahme auf biometrische Daten gem. Art. 3 Nr. 33 VO-E ist unglücklich, da die Emotionserkennung nicht auf die eindeutige Identifizierung natürlicher Personen abzielt und auch nicht nachvollziehbar ist, warum bei Emotionserkennungssystemen, die nicht auf biometrische Daten zurückgreifen, keine Informationspflichten bestehen sollen, obwohl gleichfalls die Emotionen natürlicher Personen festgestellt werden.

Systeme zur biometrischen Kategorisierung sind gem. Art. 3 Nr. 35 VO-E KI-Systeme, die dem Zweck dienen, natürliche Personen auf der Grundlage ihrer biometrischen Daten bestimmten Kategorien (z.B. Geschlecht, Alter, Haarfarbe, Augenfarbe, Tätowierung, ethnische Herkunft, sexuelle oder politische Ausrichtung) zuzuordnen. Zu denken ist z.B. an eine videogestützte Alters- und Geschlechtserkennung, um Kunden auf Werbebildschirmen zielgruppengerechte Werbung vorzuspielen.[87] Unklar ist allerdings, wie anhand biometrischer Daten eine Kategorisierung nach politischer Ausrichtung erfolgen soll (s. Art. 3 Nr. 35 VO-E). Zudem stellt sich auch hier die Frage, warum nur Kategorisierungen auf Grundlage biometrischer Daten erfasst werden, zumal eine Kategorisierung z.B. nach Geschlecht, Alter sowie Haut- und Haarfarbe regelmäßig keiner Merkmale bedarf, die eine eindeutige Identifizierung i.S.v. Art. 3 Nr. 33 VO-E ermöglichen.

Bei Systemen, die für eine biometrische Kategorisierung zur Aufdeckung, Verhütung, Ermittlung und Verfolgung von Straftaten verwendet werden (etwa Alters- und Geschlechtserkennung als Hilfsmittel bei der polizeilichen Auswertung von Videoaufnahmen), besteht keine Informationspflicht (Art. 52 Abs. 2 S. 2 VO-E).

86 Aus technischer Sicht z.B. *Brand u.a.*, Informatik Spektrum 2012, 424.
87 S. *Wentland/Schindler*, ZD-Aktuell 2017, 05855.

https://doi.org/10.5771/9783748913344-103, am 22.09.2024, 11:20:46
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

4 Unzureichende Regelungskompetenz der Union

Fraglich ist, ob die Union für den Erlass der vorgenannten Regelungen überhaupt zuständig ist. In dem Bezugsvermerk und in EG 2 VO-E werden die Art. 114 und 16 AEUV als Rechtsgrundlagen angegeben. Dies ist in Teilen nicht überzeugend.

Gem. Art. 114 Abs. 1 S. 2 AEUV können Maßnahmen zur Angleichung der Rechts- und Verwaltungsvorschriften der Mitgliedstaaten getroffen werden, welche die Errichtung und das Funktionieren des Binnenmarkts zum Gegenstand haben (s. Art. 3 Abs. 3 UAbs. 1 S. 1 EUV). Der Binnenmarkt umfasst einen Raum ohne Binnengrenzen, in dem der freie Verkehr von Waren, Personen, Dienstleistungen und Kapital gewährleistet ist (Art. 26 Abs. 2 AEUV). Seine Verwirklichung erfordert die Beseitigung von Freiverkehrshindernissen und Wettbewerbsverfälschungen.[88] Ersteres erfolgt z.B. durch die Vereinheitlichung technischer Spezifikationen, um technische Handelshemmnisse abzubauen,[89] letzteres durch Angleichung nationaler Rechtsvorschriften über Produktionsbedingungen in bestimmten Wirtschaftssektoren.[90] Insgesamt stellt der Binnenmarkt „einen denkbar weiten Bezugspunkt für eine Rechtsetzungskompetenz der Union dar“,[91] der das Zivil- und Handelsrecht, das besondere Verwaltungsrecht und ggf. sogar das Straf(verfahrens-)recht umfasst.[92]

Mit Blick darauf, dass KI-Systeme „problemlos in verschiedenen Bereichen der Wirtschaft und Gesellschaft, auch grenzüberschreitend, eingesetzt werden und in der gesamten Union verkehren [können]“ (EG 2 S. 1 VO-E), ist es nachvollziehbar, auf Grundlage von Art. 114 AEUV eine europaweit einheitliche Regulierung von KI-Systemen anzustreben. Hierdurch können „Unterschiede, die den freien Verkehr von KI-Systemen […] im Binnenmarkt behindern, vermieden werden“ und Allgemeininteressen sowie Rechte von Personen im gesamten Binnenmarkt gleichermaßen geschützt werden (EG 2 S. 4 VO-E). Dies gilt jedenfalls insoweit, als in erster Linie technische und organisatorische Anforderungen produktsicherheitsrechtlicher Art an die Anbieter von KI-Systemen gestellt und Nutzer zur Einhaltung (Art. 29 Abs. 1 VO-E: Verwendung entsprechend der Gebrauchsanweisung) verpflichtet werden, wie dies v.a. bei der Hochrisiko-KI der Fall ist.

88 Streinz/*Schröder*, Art. 114 AEUV Rn. 18 ff.
89 Streinz/*Schröder*, Art. 114 AEUV Rn. 25.
90 Streinz/*Schröder*, Art. 114 AEUV Rn. 26.
91 Streinz/*Schröder*, Art. 114 AEUV Rn. 18.
92 Geiger u.a./*Khan*, Art. 114 AEUV Rn. 10.

https://doi.org/10.5771/9783748913344-103, am 22.09.2024, 11:20:46
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

An ihre Grenzen kommt die Binnenmarktkompetenz jedoch, wenn staatlichen Stellen detailliert vorgegeben wird, ob und unter welchen Voraussetzungen KI-Systeme eingesetzt werden dürfen. Besonders deutlich wird dies bei dem Verbot der Verwendung biometrischer Echtzeit-Fernidentifizierungssysteme in öffentlich zugänglichen Räumen zu Strafverfolgungszwecken (Art. 5 Abs. 1 lit. d, Abs. 2 bis 4 VO-E), das einen Binnenmarktbezug nicht erkennen lässt.[93] Insoweit besteht ein Unterschied zur Richtlinie 2006/24/EG über die Vorratsspeicherung, die, obwohl sie den Umgang mit Daten im Kontext der Ermittlung, Feststellung und Verfolgung von Straftaten betraf, auf die Binnenmarktkompetenz gestützt werden konnte, da sie im Wesentlichen die Pflicht (privater) Diensteanbieter zur Speicherung von Verkehrs- und Standortdaten regelte, nicht aber die Nutzung dieser Daten durch die zuständigen Behörden.[94]

Als Kompetenzgrundlage wird in EG 2 S. 5 VO-E ferner auf Art. 16 Abs. 2 AEUV abgestellt, soweit der Verordnungsentwurf „konkrete Vorschriften zum Schutz von Privatpersonen im Hinblick auf die Verarbeitung personenbezogener Daten enthält, mit denen v.a. die Verwendung von KI-Systemen zur biometrischen Echtzeit-Fernidentifizierung in öffentlich zugänglichen Räumen zu Strafverfolgungszwecken eingeschränkt wird". Gemeint ist erkennbar Art. 5 Abs. 1 lit. d, Abs. 2 bis 4 VO-E.

Art. 16 Abs. 2 AEUV erlaubt den Erlass von Vorschriften über den Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Mitgliedstaaten im Rahmen der Ausübung von Tätigkeiten, die in den Anwendungsbereich des Unionsrechts fallen, und über den freien Datenverkehr. KI-Systeme zur biometrischen Identifizierung und Kategorisierung i.S.d. Verordnungsentwurfs beruhen per Definition auf der Verarbeitung personenbezogener Daten (Art. 3 Nr. 33 i.V.m. Art. 3 Nrn. 35 bis 38 VO-E). Dass die Vorschriften im Verordnungsentwurf tatsächlich auf den Schutz natürlicher Personen bei Verarbeitung personenbezogener Daten abzielen, wie dies z.B. in der DSGVO oder der JI-Richtlinie der Fall ist, ist allerdings nicht ohne weiteres erkennbar. In Art. 5 Abs. 1 lit. d, Abs. 2 bis 4 VO-E finden personenbezogene Daten keine explizite Erwähnung. Die Regelungen zur Hochrisiko-KI enthalten ebenfalls so gut wie keine Vorschriften, die spezifisch auf den Umgang mit personenbezogenen Daten eingehen (s. aber Art. 10 Abs. 5 VO-E).

Vor allem aber ist fraglich, ob Art. 5 Abs. 1 lit. d, Abs. 2 bis 4 VO-E überhaupt eine Tätigkeit regelt, die in den Anwendungsbereich des Unions-

93 *Valta/Vasel*, ZRP 2021, 142 (143); krit. auch *Ebers u.a.*, RDi 2021, 528 (529).
94 Dazu EuGH, NJW 2009, 1801.

https://doi.org/10.5771/9783748913344-103, am 22.09.2024, 11:20:46
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

rechts i.S.v. Art. 16 Abs. 2 AEUV fällt.[95] Der Anwendungsbereich wäre jedenfalls gegeben, wenn für die geregelte Tätigkeit eine eigenständige Kompetenzgrundlage im Unionsrecht bestehen würde.[96] Eine solche ist, da es sich um Vorschriften handelt, die das innerstaatliche Polizei- und Strafverfahrensrecht betreffen,[97] nicht ersichtlich (s. Art. 2 bis 6 AEUV). Als Anknüpfungspunkt für den Anwendungsbereich des Unionsrechts kommt allenfalls der Raum der Freiheit, der Sicherheit und des Rechts in Betracht (Art. 3 Abs. 2 EUV, Art. 67 ff. i.V.m. Art. 4 Abs. 2 lit. j AEUV), der u.a. die grenzüberschreitende justizielle und polizeiliche Zusammenarbeit umfasst. Ein grenzüberschreitender Bezug ist bei Art. 5 Abs. 1 lit. d, Abs. 2 bis 4 VO-E allerdings nicht erkennbar. Vielmehr ist der rein innerstaatliche Einsatz biometrischer Echtzeit-Fernidentifizierungssysteme zu Strafverfolgungszwecken betroffen. Anders als bei der JI-Richtlinie lässt sich auch nicht argumentieren, dass in erster Linie datenschutzspezifische prozedurale und institutionelle Vorkehrungen (z.B. Betroffenenrechte, Datensicherheit etc.) geregelt sind, um bei (möglicherweise auftretenden) grenzüberschreitenden Sachverhalten ein einheitliches Datenschutzniveau zu gewährleisten, während die materiellen Vorgaben für den Einsatz auf Mindestvorgaben beschränkt sind (s. Art. 8 und 10 JI-RL).[98] Die bloße Berührung eines Zuständigkeitsbereichs der Union genügt nicht, damit Art. 5 Abs. 1 lit. d, Abs. 2 bis 4 VO-E in den Anwendungsbereich des Unionsrechts fällt.[99] Folglich fehlt es für Art. 5 Abs. 1 lit. d, Abs. 2 bis 4 VO-E an einer Regelungskompetenz der Union.[100]

5 Fazit

Der Kommission ist zuzugestehen, „dass sie einen mutigen Anlauf genommen hat, um weltweit eine der ersten Regulierungen von KI-Systemen vor-

95 Dass der freie Datenverkehr i.S.v. Art. 16 Abs. 2 AEUV betroffen ist, ist nicht erkennbar.

96 Lisken/Denninger/*Müller/Schwabenbauer*, Kap. G Rn. 422.

97 *Ebers u.a.*, RDi 2021, 528 (529), demnach es sich um Vorschriften handelt, „die in der Regel Teil des mitgliedstaatlichen Polizei- oder Straf(verfahrens)rechts sind".

98 S. *Bäcker*, BT-Ausschuss-Drs. 17(4)585 B; Lisken/Denninger/*Müller/Schwabenbauer*, Kap. G Rn. 420 f.

99 S. Lisken/Denninger/*Müller/Schwabenbauer*, Kap. G Rn. 417 ff.

100 Im Ergebnis auch *Valta/Vasel*, ZRP 2021, 142 (143 f.); krit. auch *Burri/v. Bothmer* 2021, S. 6 f.

https://doi.org/10.5771/9783748913344-103, am 22.09.2024, 11:20:46
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

zunehmen".[101] Bei dem Verbot der Verwendung biometrischer Echtzeit-Fernidentifizierungssysteme in öffentlich zugänglichen Räumen zu Strafverfolgungszwecken gem. Art. 5 Abs. 1 lit. d VO-E drängt sich allerdings der Verdacht auf, dass es sich eher um „gegenwartsgebundene Symbolpolitik"[102] handelt, die als Reaktion auf öffentlichkeitswirksam[103] geäußerte Ängste vor einer ausufernden Massenüberwachung zu verstehen ist. Damit soll nicht in Abrede gestellt werden, dass diese Form biometrischer Erkennung schwerwiegende Grundrechtseingriffe hervorrufen und daher – wenn überhaupt – nur äußerst zurückhaltend eingesetzt werden sollte. Jedoch fällt ihre Regulierung nicht in die Kompetenz der Union, sondern zählt zum „Wesenskern staatlicher Souveränität"[104]. Zudem stellen die Art. 5 Abs. 1 lit. d, Abs. 2 bis 4 VO-E keine Anforderungen, die nicht auch aus dem deutschen Verfassungsrecht abgeleitet werden können.

Soweit biometrische Erkennung als Hochrisiko-KI einzuordnen ist, gelten die Vorgaben in Art. 6 ff. VO-E. Diese sind größtenteils allgemein formuliert und bedürfen der Konkretisierung durch die Anbieter sowie Normungsorganisationen.[105] Für biometrische Systeme i.S.v. Anhang III Nr. 1 bestehen Besonderheiten hinsichtlich der Protokollierung (Art. 12 Abs. 4 VO-E), der menschlichen Aufsicht (Art. 14 Abs. 5 VO-E) und der Konformitätsbewertung. Rechtsgrundlagen oder Eingriffsschwellen sind nicht vorgesehen.

Systeme zur Emotionserkennung und zur biometrischen Kategorisierung unterliegen gem. Art. 52 Abs. 2 VO-E Transparenzpflichten, wobei nicht nachvollziehbar ist, warum dies nur für Systeme gelten soll, die auf Grundlage biometrischer Daten funktionieren. Etwa arbeiten Streamingdienste an der Emotionserkennung anhand von Hintergrundgeräuschen oder der Spracheingabe.[106] Die Bezugnahme auf biometrische Daten sollte daher gestrichen werden, damit die Transparenzpflichten für alle KI-Systeme gelten, die Emotionen erkennen.

Insgesamt ist es zu begrüßen, dass sich die Kommission der Regulierung von KI angenommen hat. Die vorgeschlagenen Regelungen bedürfen je-

---

101 *Spindler*, CR 2021, 361 (373); deutlich negativer *Valta/Vasel*, ZRP 2021, 142 (145): „Planbarkeits-Übermut".

102 *Valta/Vasel*, ZRP 2021, 142 (143).

103 S. https://reclaimyourface.eu/de/.

104 Lisken/Denninger/*Müller/Schwabenbauer*, Kap. G Rn. 399.

105 Krit. z.B. *Ebers*, RDi 2021, 588, 590 und 596 f.; von der Notwendigkeit, die abstrakten Anforderungen zu konkretisieren, sprechen auch *Bomhard/Merkle*, RDi 2021, 276, 283.

106 *Korz u.a.* 2021, Gefühle im Patent: Emotionserkennung beim Musikstreaming.

https://doi.org/10.5771/9783748913344-103, am 22.09.2024, 11:20:46
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

doch an verschiedenen Stellen der Nachbesserung, die im weiteren Gesetzgebungsverfahren geleistet werden sollte.

Literatur

Internetquellen wurden am 15.08.2022 zuletzt abgerufen.

Bäcker, M., Stellungnahme zur öffentlichen Anhörung des Innenausschusses des Deutschen Bundestages am 22. Oktober 2012, 14.00 Uhr über den Entwurf einer EU-Richtlinie über die Datenverarbeitung bei Polizei und Strafjustiz vom 25. Januar 2012 [KOM(2012) 10 endg.], BT-Ausschuss-Drs. 17(4)585 B.

Bomhard, D. / Merkle, M., Europäische KI-Verordnung. Der aktuelle Kommissionsentwurf und praktische Auswirkungen, RDi 2021, 276.

Brand, M. / Klompmaker, F. / Schleining, P. / Weiß, F., Automatische Emotionserkennung. Technologien, Deutung und Anwendungen, Informatik Spektrum 2012, 424.

Burri, T. / Bothmer, F. v., The New EU Legislation on Artificial Intelligence: A Primer, 2021, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3831424.

Calliess, C. / Ruffert, M. (Hrsg.), EUV/AEUV, Das Verfassungsrecht der Europäischen Union mit Europäischer Grundrechtecharta, 6. Aufl., München 2022 (zitiert als Calliess/Ruffert/*Bearbeiter*).

Damm, R. / Hart, D., Rechtliche Regulierung riskanter Technologien. Am Beispiel der Gentechnologie nach Vorlage des Berichts der Enquete-Kommission „Chancen und Risiken der Gentechnologie", KritV 1987, 183.

Datenethikkommission der Bundesregierung, Gutachten, Berlin 2019, https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/it-digitalpolitik/gutachten-datenethikkommission.pdf?__blob=publicationFile&v=6.

Dettling, H.-U. / Krüger, S., Erste Schritte im Recht der Künstlichen Intelligenz. Entwurf der „Ethik-Leitlinien für eine vertrauenswürdige KI", MMR 2019, 211.

Ebers, M., Standardisierung Künstlicher Intelligenz und KI-Verordnungsvorschlag, RDi 2021, 588.

Ebers, M. / Hoch, V. R. S. / Rosenkranz, F. / Ruschemeier, H. / Steinrötter, B., Der Entwurf für eine EU-KI-Verordnung: Richtige Richtung mit Optimierungsbedarf. Eine kritische Bewertung durch Mitglieder der Robotics & AI Law Society (RAILS), RDi 2021, 528.

Ebert, A. / Spiecker gen. Döhmann, I., Der Kommissionsentwurf für eine KI-Verordnung der EU. Die EU als Trendsetter weltweiter KI-Regulierung, NVwZ 2021, 1188.

Europäische Kommission, Pressemitteilung v. 21.04.2021. Ein Europa für das digitale Zeitalter: Kommission schlägt neue Vorschriften und Maßnahmen für Exzellenz und Vertrauen im Bereich der künstlichen Intelligenz vor, https://ec.europa.eu/commission/presscorner/detail/de/ip_21_1682.

https://doi.org/10.5771/9783748913344-103, am 22.09.2024, 11:20:46
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

Europäischer Datenschutzausschuss / Europäischer Datenschutzbeauftragter, Gemeinsame Stellungnahme 5/2021 zum Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz (Gesetz über künstliche Intelligenz) und zur Änderung bestimmter Rechtsakte der Union v. 18. Juni 2021, Brüssel 2021.

Geiger, R. / Khan, D.-E. / Kotzur, M., (Hrsg.), EUV/AEUV, 6. Aufl., München 2017 (zitiert als Geiger u.a./*Bearbeiter*).

Geminn, C., Die Regulierung Künstlicher Intelligenz. Anmerkungen zum Entwurf eines Artificial Intelligence Act, ZD 2021, 354.

Grützmacher, M. / Füllsack, A. L., Der Entwurf einer EU-KI-Verordnung. Ein erster Überblick über den Vorschlag der Kommission v. 21.4.2021, ITRB 2021, 159.

Hacker, P., Europäische und nationale Regulierung von Künstlicher Intelligenz, NJW 2020, 2142.

Herberger, M., „Künstliche Intelligenz" und Recht. Ein Orientierungsversuch, NJW 2018, 2825.

Hochrangige Expertengruppe für Künstliche Intelligenz, Eine Definition der KI: Wichtigste Fähigkeiten und Wissenschaftsgebiete, Brüssel 2019.

Hornung, G., KI-Regulierung im Mehrebensystem. KI-Verordnungsentwurf und nationale Ergänzungen, DuD 2022 i.E.

Hornung, G. / Schindler, S., Das biometrische Auge der Polizei. Rechtsfragen des Einsatzes von Videoüberwachung mit biometrischer Gesichtserkennung, ZD 2017, 203.

Hornung, G. / Schindler, S. / Schneider, J., Die Europäisierung des strafverfahrensrechtlichen Datenschutzes. Zum Anwendungsbereich der neuen Datenschutz-Richtlinie für Polizei und Justiz, ZIS 2018, 566.

Korz, J. / Cezanne, L. / Noyan, A. / van den Heuvel, E., Gefühle im Patent: Emotionserkennung beim Musikstreaming, Themen-Blog der GI v. 21.05.2021, https://gi.de/themen/beitrag/gefuehle-im-patent-emotionserkennung-beim-musikstreaming.

Kalbhenn, J. C., Designvorgaben für Chatbots, Deepfakes und Emotionserkennungssysteme: Der Vorschlag der Europäischen Kommission zu einer KI-VO als Erweiterung der medienrechtlichen Plattformregulierung, ZUM 2021, 663.

Karpenstein, U. / Mayer, F. C. (Hrsg.), Konvention zum Schutz der Menschenrechte und Grundfreiheiten, 3. Aufl., München 2022 (zitiert als Karpenstein/Mayer/*Bearbeiter*).

Lehner, R., Deutscher und europäischer Grundrechtsschutz nach den Entscheidungen zum „Recht auf Vergessen". Von der Alternativität zur Komplementarität?, JA 2022, 177.

Lisken, H. / Denninger, E. (Begr.), Handbuch des Polizeirechts. Gefahrenabwehr, Strafverfolgung, Rechtsschutz, hrsg. v. Bäcker, M. / Denninger, E. / Graulich, K., 7. Aufl., München 2021 (zitiert als Lisken/Denninger/*Bearbeiter*).

Merten, D. / Papier, H-J. (Hrsg.), Handbuch der Grundrechte in Deutschland und Europa, Band II, München 2006 (zitiert als Merten/Papier/*Bearbeiter*).

https://doi.org/10.5771/9783748913344-103, am 22.09.2024, 11:20:46
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

Meyer, J. / Hölscheidt, S. (Hrsg.), Charta der Grundrechte der Europäischen Union, 5. Aufl., Baden-Baden 2019 (zitiert als Meyer/Hölscheidt/*Bearbeiter*).

Mysegades, J., Keine staatliche Gesichtserkennung ohne Spezial-Rechtsgrundlage, NVwZ 2020, 852.

Orssich, I., Das europäische Konzept für vertrauenswürdige Künstliche Intelligenz, EuZW 2022, 254.

o.V., EDSA/EDSB: Forderung nach Verbot biometrischer Gesichtserkennung, ZD-Aktuell 2021, 05266.

Pieroth, B. / Schlink, B. / Kingreen, T. / Poscher, R., Grundrechte Staatsrecht II, 29. Aufl., Heidelberg 2013.

Plattform Industrie 4.0, Künstliche Intelligenz und Recht im Kontext von Industrie 4.0, Berlin 2019.

Preßlein, D., Grundgesetz vs. Grundrechtecharta? Zur „europäisierten Grundrechtsprüfung" des BVerfG nach den Beschlüssen zum „Recht auf Vergessen" und „Europäischer Haftbefehl III", EuR 2021, 247.

Roos, P. / Weitz, C. A., Hochrisiko-KI-Systeme im Kommissionsentwurf für eine KI-Verordnung. IT- und produktsicherheitsrechtliche Pflichten von Anbietern, Einführern, Händlern und Nutzern, MMR 2021, 844.

Salzmann, M. / Schindler, S., Polizeiliche Gesichtserkennung in Deutschland, ZD-Aktuell 2018, 06344.

Schindler, S., Biometrische Videoüberwachung. Zur Zulässigkeit biometrischer Gesichtserkennung in Verbindung mit Videoüberwachung zur Bekämpfung von Straftaten, Baden-Baden 2021.

Schindler, S., EU-Kommission: Verordnungsentwurf zur Regulierung von KI - Das Ende polizeilicher Gesichtserkennung im öffentlichen Raum?, ZD-Aktuell 2021, 05221.

Schindler, S., Künstliche Intelligenz und (Datenschutz-)Recht, ZD-Aktuell 2019, 06647.

Schindler, S., Noch einmal: Pilotprojekt zur intelligenten Videoüberwachung am Bahnhof Berlin Südkreuz, ZD-Aktuell 2017, 05799.

Schröder, M., Der risikobasierte Ansatz in der DS-GVO. Risiko oder Chance für den Datenschutz?, ZD 2019, 503.

Spindler, G., Der Vorschlag der EU-Kommission für eine Verordnung zur Regulierung der Künstlichen Intelligenz (KI-VO-E). Ansatz, Instrumente, Qualität und Kontext, CR 2021, 361.

Steege, H., Algorithmenbasierte Diskriminierung durch Einsatz von Künstlicher Intelligenz. Rechtsvergleichende Überlegungen und relevante Einsatzgebiete, MMR 2019, 715.

Streinz, R. (Hrsg.), EUV/AEUV, 3. Aufl., München 2018 (zitiert als Streinz/*Bearbeiter*).

Valta, M. / Vasel, J., Kommissionsvorschlag für eine Verordnung über Künstliche Intelligenz – Mit viel Bürokratie und wenig Risiko zum KI-Standort?, ZRP 2021, 142.

https://doi.org/10.5771/9783748913344-103, am 22.09.2024, 11:20:46
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

Veale, M. / Zuiderveen Borgesius, F., Demystifying the Draft EU Artificial Intelligence Act. Analysing the good, the bad, and the unclear elements of the proposed approach, Cri 2021, 97.

Wentland, K. / Schindler, S., Videogestützte Kundenanalyse zu Werbezwecken, ZD-Aktuell 2017, 05855.

Westphalen, F. v., Künstliche Intelligenz (KI) – Dateneigentum, Haftung, Bilanzierung, ZIP 2020, 737.

https://doi.org/10.5771/9783748913344-103, am 22.09.2024, 11:20:46
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb