DeutscherAnwaltVerein

Stellungnahme

des Deutschen Anwaltvereins durch die Ausschüsse Arbeitsrecht, Gefahrenabwehrrecht, Geistiges Eigentum, Europa, Informationsrecht und Migrationsrecht

zum Vorschlag der EU-Kommission für eine Verordnung zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz (Gesetz über Künstliche Intelligenz) vom 21.04.2021 (COM (2021) 206 final)

Stellungnahme Nr.: 57/2021 Brüssel, im November 2021

Mitglieder des Ausschusses Arbeitsrecht

- Rechtsanwältin Dr. Nathalie Oberthür, Köln (Vorsitzende und Berichterstatterin)
- Rechtsanwalt Dr. Christian Arnold, Stuttgart
- Rechtsanwältin Regina Bell, München
- Rechtsanwältin Dr. Susanne Clemenz, Gütersloh
- Rechtsanwalt Prof. Dr. Björn Gaul, Köln (Berichterstatter)
- Rechtsanwalt Roland Gross, Leipzig
- Rechtsanwalt Jürgen Markowski, Offenburg
- Rechtsanwalt Benja Mausner, Stuttgart
- Rechtsanwalt Dr. Thomas Müller-Bonanni, Düsseldorf
- Rechtsanwältin Dr. Barbara Reinhard, Frankfurt am Main
- Rechtsanwältin Dr. Ulrike Schweibert, Frankfurt
- Rechtsanwalt Dr. Uwe Silberberger, Düsseldorf

Zuständig in der DAV-Geschäftsstelle

- Rechtsanwalt Max Gröning

Deutscher Anwaltverein
Littenstraße 11, 10179 Berlin
Tel.: +49 30 726152-0
Fax: +49 30 726152-190
E-Mail: dav@anwaltverein.de

Büro Brüssel
Rue Joseph II 40, Boîte 7B
1000 Brüssel, Belgien
Tel.: +32 2 28028-12
Fax: +32 2 28028-13
E-Mail: bruessel@eu.anwaltverein.de
EU-Transparenz-Registernummer:
87980341522-66

www.anwaltverein.de

Mitglieder des Ausschusses Gefahrenabwehrrecht

- Rechtsanwältin Lea Voigt, Bremen (Vorsitzende)
- Rechtsanwalt Wilhelm Achelpöhler, Münster
- Rechtsanwalt Dr. David Albrecht, Berlin (Berichterstatter)
- Rechtsanwalt Dr. Eren Basar, Düsseldorf
- Prof. Dr. Annika Dießner, Berlin (ständiges Gastmitglied im Ausschuss)
- Rechtsanwalt Dr. Nikolas Gazeas, LL.M., Köln
- Rechtsanwalt Dr. Andreas Grözinger, Köln
- Rechtsanwalt Prof. Dr. Stefan König, Berlin
- Rechtsanwältin Dr. Regina Michalke, Frankfurt
- Prof. Dr. Mark A. Zöller, München (ständiges Gastmitglied im Ausschuss)

Zuständig in der DAV-Geschäftsstelle

- Rechtsanwalt Max Gröning

Mitglieder des Ausschusses Geistiges Eigentum

- Rechtsanwalt Prof. Dr. Jochen Bühling, Düsseldorf (Vorsitzender und Berichterstatter)
- Rechtsanwältin Jana Bogatz, München
- Rechtsanwalt Dr. Dirk Bruhn, Hamburg
- Rechtsanwalt Klaus Haft, Dipl.-Phys., Düsseldorf
- Rechtsanwältin Dr. Verena Hoene, Köln
- Rechtsanwalt Prof. Dr. Reinhard Ingerl, LL.M., München
- Rechtsanwältin Dr. Andrea Jaeger-Lenz, Hamburg
- Rechtsanwalt beim Bundesgerichtshof Dr. Matthias Koch LL.M., Karlsruhe
- Rechtsanwalt Prof. Dr. Johannes Kreile, München
- Rechtsanwalt Dr. Henrik Lehment, Düsseldorf
- Rechtsanwältin Dr. Birte Lorenzen, Hamburg

Zuständig in der DAV-Geschäftsstelle

- Hannah Adzakpa, LL.M.

Mitglieder des Ausschusses Europa

- Rechtsanwältin Dr. Claudia Seibel, Frankfurt (Vorsitzende)
- Rechtsanwältin Béatrice Deshayes, Paris
- Rechtsanwalt Prof. Dr. Christian Duve, Frankfurt am Main (Berichterstatter)
- Rechtsanwalt Prof. Dr. Thomas Gasteyer, LL.M., Frankfurt am Main
- Rechtsanwalt Prof. Dr. Hans-Jürgen Hellwig, Frankfurt am Main

- Rechtsanwalt Dr. Ulrich Karpenstein, Berlin
- Rechtsanwältin Gül Pinar, Hamburg
- Rechtsanwalt Prof. Dr. Dirk Uwer, Düsseldorf
- Rechtsanwalt Michael Jürgen Werner, Brüssel

Zuständig in der DAV-Geschäftsstelle

- Hannah Adzakpa, LL.M.

Mitglieder des Ausschusses Informationsrecht

- Rechtsanwalt Dr. Helmut Redeker, Bonn (Vorsitzender)
- Rechtsanwalt Dr. Simon Assion, Frankfurt am Main
- Rechtsanwältin Dr. Christiane Bierekoven, Düsseldorf
- Rechtsanwältin Isabell Conrad, München
- Rechtsanwalt Dr. Malte Grützmacher, LL.M., Hamburg (Berichterstatter)
- Rechtsanwalt Prof. Niko Härting, Berlin
- Rechtsanwalt Peter Huppertz, LL.M, Düsseldorf
- Rechtsanwältin Birgit Roth-Neuschild, Karlsruhe
- Rechtsanwalt Dr. Robert Selk, LL.M. (EU), München

Zuständig in der DAV-Geschäftsstelle

- Rechtsanwältin Nicole Narewski

Mitglieder des Ausschusses Migrationsrecht

- Rechtsanwältin Gisela Seidler, München (Vorsitzende)
- Rechtsanwalt Dr. Marco Bruns, Frankfurt am Main, stellvertretender Vorsitzender
- Rechtsanwalt Dr. Wolfgang Breidenbach, Halle/Saale
- Rechtsanwältin Maria Kalin, Ulm
- Rechtsanwalt Tim W. Kliebe, Frankfurt am Main
- Rechtsanwalt Dr. Jonathan Leuschner, Frankfurt am Main
- Rechtsanwältin Kerstin Müller, Köln
- Rechtsanwalt Berthold Münch, Heidelberg
- Rechtsanwalt Thomas Oberhäuser, Ulm
- Rechtsanwältin Simone Rapp, Berlin
- Rechtsanwalt Rolf Stahmann, Berlin (Berichterstatter)
- Rechtsanwältin Eva Steffen, Köln
- Rechtsanwalt Christoph Tometten, Berlin

Zuständig in der DAV-Geschäftsstelle

- Rechtsanwältin Bettina Bachmann

Verteiler

Deutschland

Bundesministerium der Justiz und für Verbraucherschutz
Bundesministerium für Wirtschaft und Energie
Ausschuss für Recht und Verbraucherschutz im Deutschen Bundestag
Ausschuss für Wirtschaft und Energie im Deutschen Bundestag
Ausschuss Digitale Agenda im Deutschen Bundestag
Ausschuss für die Angelegenheiten der Europäischen Union
Arbeitsgruppen Recht der im Deutschen Bundestag vertretenen Parteien
Justizministerien und -senatsverwaltungen der Länder
Rechtsausschüsse der Landtage
Europäische Kommission – Vertretung in Deutschland
Bundesrechtsanwaltskammer
Bundesnotarkammer
Bundesverband der Freien Berufe
Deutscher Richterbund
Deutscher Notarverein e.V.
Deutscher Steuerberaterverband
Bundesverband der Deutschen Industrie (BDI)
GRUR
BITKOM
DGRI
Gewerkschaft der Polizei (Bundesvorstand)
Deutsche Polizeigewerkschaft im DBB
Ver.di, Recht und Politik
Stiftung neue Verantwortung e.V.
DAV-Vorstand und Geschäftsführung
Vorsitzende der DAV-Gesetzgebungs- und Geschäftsführenden Ausschüsse des DAV
Vorsitzende der DAV-Landesverbände
Vorsitzende des FORUMs Junge Anwaltschaft

Europa

Europäische Kommission
- Generaldirektion Justiz und Verbraucher
- Generaldirektion Kommunikationsnetze, Inhalte und Technologien

Europäisches Parlament
- Ausschuss für Binnenmarkt und Verbraucherschutz
- Rechtsausschuss
- Sonderausschuss zu künstlicher Intelligenz im digitalen Zeitalter

Rat der Europäischen Union
Ständige Vertretung der Bundesrepublik Deutschland bei der EU
Justizreferenten der Landesvertretungen
Rat der Europäischen Anwaltschaften (CCBE)
Vertreter der Freien Berufe in Brüssel
DIHK Brüssel
BDI Brüssel

Presse

Frankfurter Allgemeine Zeitung
Süddeutsche Zeitung GmbH
Berliner Verlag GmbH
Redaktion NJW
Juve-Verlag
Redaktion Anwaltsblatt
Juris
Redaktion MultiMedia und Recht (MMR)
Redaktion heise online
JurPC

Der Deutsche Anwaltverein (DAV) ist der freiwillige Zusammenschluss der deutschen Rechtsanwältinnen und Rechtsanwälte. Der DAV versammelt mehr als 61.000 Rechtsanwältinnen und Rechtsanwälte sowie Anwaltsnotarinnen und Anwaltsnotare, die in 252 lokalen Anwaltvereinen im In- und Ausland organisiert sind. Er vertritt die Interessen der deutschen Anwaltschaft auf nationaler, europäischer und internationaler Ebene.

---

1. Zusammenfassung

Der DAV begrüßt den Verordnungsvorschlag der EU-Kommission für eine Verordnung zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz (im Folgenden „KI-VO-E“). Durch die einheitliche, minimalinvasive Regulierung von KI soll Innovation gefördert und Rechtssicherheit geschaffen werden.

Der DAV hat sich bereits in der Stellungnahme Nr. 40/2020 zum Weißbuch der EU-Kommission dafür eingesetzt, dass die Grundrechte auch im Umgang mit KI vollumfänglich gewahrt bleiben und die Funktion der Anwaltschaft als persönliche und vertraulich agierende Vertreter des Bürgers geschützt wird. Der DAV hat sich auch dafür ausgesprochen, den besonders hohen Grundrechtsrisiken bei der Anwendung von KI in der Justiz durch besonders strenge Anforderungen Rechnung zu tragen. Gerichtliche und ähnlich verbindliche Entscheidungen staatlicher Akteure dürfen dementsprechend nicht automatisiert werden. Außerdem müssen wirksame Rechtsbehelfs- und Kontrollmechanismen für diejenigen geschaffen werden, die durch die KI in ihren Rechten berührt werden. Die Notwendigkeit, den Vorrang der menschlichen Entscheidung in Justiz und Behörden zu wahren, steht auch im Vordergrund der Stellungnahme des Rats der Europäischen Anwaltschaften (CCBE) zum KI-VO-E. Der DAV hat sich an der Ausarbeitung der Stellungnahme beteiligt und unterstützt die wesentlichen darin geäußerten Positionen.

In einer offiziellen Rückmeldung auf den KI-VO-E hat der DAV u.a. darauf verwiesen, dass die Komplexität, Länge und zahlreichen Rückverweisungen des KI-VO-E auf andere Verordnungen und Richtlinien zu praktischen Anwendungsschwierigkeiten und Rechtsunsicherheiten führen könnten.

Das Ziel dieser Stellungnahme besteht daher darin, die Verhandlungen im EU-Parlament und im Rat durch eine Zusammenfassung und Ergänzung wesentlicher Informationen zu unterstützen.

2. Definition, Anwendungsbereich und allgemeine Dogmatik

2.1 Definition von KI-Systemen

Angesichts der unterschiedlichen, teilweise weitreichenden Rechtsfolgen, ist die Definition von KI-Systemen von zentraler Bedeutung. Sie werden in Art. 3 Nr. 1 KI-VO-E legal definiert.

Die Regelung erscheint mit Blick auf zukünftige Entwicklungen insoweit zu eng zu sein, als Art. 3 Abs. 1 KI-VO-E auf von Menschen festgelegte Ziele abstellt. Denn es ist durchaus möglich, dass künftig auch die KI selbst Ziele definiert. Das gilt zumindest dann, wenn sie sich einer sogenannten „starken“ KI annähert. Insoweit bedarf es früher oder später einer Regulierung.

Aktuell besteht ein unmittelbarer Nachbesserungsbedarf mit Blick auf den Annex I des Entwurfs. Dieser fasst die Systeme, die unter den Anwendungsbereich der KI-VO fallen sollen, sehr weit. Aktuell könnten insbesondere auch normale Expertensysteme sowie Such- und Optimierungsmethoden in den Anwendungsbereich fallen.

Eine Möglichkeit der Beschränkung könnte darin bestehen, als KI mittels des Annex I nur solche Systeme zu definieren, deren Entscheidungen bzw. deren Verhalten (als mit zumutbaren Mitteln) praktisch unvorhersehbar anzusehen sind. Auf diesem Wege ließe sich vermeiden, dass ohne Not zahlreiche, bereits bestehende IT-Systeme bzw. Softwarelösungen der umfangreichen, von der Kommission geplanten Regulierung für KI-Systeme unterworfen werden.

2.2 Anwendungsbereich

Der DAV begrüßt den KI-VO-E in Form einer horizontalen Regulierung. Soweit Art. 2 Abs. 2 KI-VO-E unter Verweis auf entsprechende Verordnungen die Fahrzeug- und Luftfahrtindustrie von der Regulierung praktisch vollständig ausnimmt, sollte, wie von der Kommission angedacht, zeitnah eine entsprechende Regulierung erfolgen.

2.3 Regelungstechnik, Umfang und Aufbau

Der DAV begrüßt den risikobasierten Ansatz der KI-VO-E. Der DAV hatte sich für eine Differenzierung nach mindestens fünf Risikostufen eingesetzt, damit alle KI-Systeme je nach Eingriffsintensität bestimmte Transparenz-, Sicherheits- und Kontrollanforderungen erfüllen müssen. Die binäre Einteilung in Hochrisiko- / Nicht-Hochrisiko-KI-Systeme im KI-VO-E lässt dagegen weniger Raum für Differenzierungen. Sollte der KI-VO-E in dieser Hinsicht überarbeitet werden, wäre eine Weiterentwicklung denkbar.

Hilfreich könnte auch eine Reduzierung der in dem KI-VO-E angelegten Komplexität sein. Sie ergibt sich insbesondere aus zahlreichen Querverweisungen. Die Rückverweisungen auf andere Verordnungen (etwa Art. 42 Abs. 2 und Art. 47 Abs. 6 KI-VO-E) erschweren die Lesbarkeit und damit die Anwendung der KI-VO-E.

3. Verbotene KI-Systeme

In Art. 5 KI-VO-E werden *intolerable und verbotene KI-Systeme* aufgeführt, bei denen es ganz offenbar im Wesentlichen darum geht, besonders gravierende Grund- bzw. Menschenrechtseingriffe zu unterbinden.

Die in Art. 5 Abs. 1 KI-VO-E aufgeführten KI-Systeme sind in der Tat problematisch, so dass gegen deren Auflistung nichts einzuwenden ist. Was allerdings fehlt, ist eine Regelung, welche gewisse Leitlinien für oder gegen das Verbot entsprechender KI-Systeme schafft und auf diesem Wege die Grundlage für eine zukunftsbezogene Erweiterung eines entsprechenden Katalogs bietet. Auch dürfte im Sinne der Grundrechtsrelevanz noch deutlicher zwischen dem Einsatz von KI durch den Staat und durch Private zu differenzieren sein.

3.1 Social Scoring

In Art. 5 Nr. 1 lit. c) KI-VO-E werden bestimmte KI-Systeme „zur Bewertung oder Klassifizierung der Vertrauenswürdigkeit natürlicher Personen“ (sog. „Social Scoring“) durch Behörden oder in deren Auftrag verboten. Aufgrund der Eingriffsintensität und des besonderen Risikos von Social Scoring begrüßt der DAV dieses Verbot. Deswegen ist es bedauerlich, dass das Verbot durch die in (i) und (ii) genannten Bedingungen aufgeweicht wird, da durch den Wortlaut so viel Raum für eine weite Auslegung bleibt, dass das Verbot umgangen werden könnte. Insbesondere die Formulierung „in keinem

Zusammenhang zu den Umständen“ (i), sowie die Begriffe „ungerechtfertigt oder unverhältnismäßig“ (ii) könnten in diesem Wortlaut Raum für eine zu weite Auslegung lassen, die es ermöglichen könnte, das Verbot zu umgehen. Darüber hinaus sollte das Verbot auf das Inverkehrbringen, die Inbetriebnahme oder die Nutzung von KI-Systemen durch private Akteure ausgedehnt werden und nicht auf Behörden beschränkt sein. Der DAV weist in diesem Zusammenhang auf die Stellungnahme des CCBE hin, die im Zusammenhang mit Social Scoring auf die Gefahren für auf Demokratie und Rechtsstaatlichkeit hinweist. Beim Social Scoring werden nicht nur die Rechte auf Privatsphäre und Familienleben verletzt, sondern auch die Gefahr von Diskriminierung verschärft. Die Anonymität, einschließlich der Tatsache, dass man für bestimmte Verhaltensweisen nicht bewertet wird, ist oft der Grundstein dafür, dass man seine Grundrechte uneingeschränkt wahrnehmen kann. Dieses Recht auf Anonymität und die Privatsphäre wird durch Social Scoring ausgehöhlt oder sogar unmöglich gemacht. Im schlimmsten Fall könnte durch Social Scoring sogar die Unschuldsvermutung *de facto* außer Kraft gesetzt werden.

Änderungsvorschlag zu Artikel 5

(1) Folgende Praktiken im Bereich der künstlichen Intelligenz sind verboten:
(….)

c) das Inverkehrbringen, die Inbetriebnahme oder die Verwendung von KI-Systemen ~~durch Behörden oder in deren Auftrag~~ zur Bewertung oder Klassifizierung der Vertrauenswürdigkeit natürlicher Personen über einen bestimmten Zeitraum auf der Grundlage ihres sozialen Verhaltens oder bekannter oder vorhergesagter persönlicher Eigenschaften oder Persönlichkeitsmerkmale, ~~wobei die soziale Bewertung zu einem oder beiden der folgenden Ergebnisse führt:~~

~~i) Schlechterstellung oder Benachteiligung bestimmter natürlicher Personen oder ganzer Gruppen natürlicher Personen in sozialen Zusammenhängen, die in keinem Zusammenhang zu den Umständen stehen, unter denen die Daten ursprünglich erzeugt oder erfasst wurden;~~

~~ii) Schlechterstellung oder Benachteiligung bestimmter natürlicher Personen oder ganzer Gruppen natürlicher Personen, in einer Weise, die im Hinblick auf ihr soziales Verhalten oder dessen Tragweite ungerechtfertigt oder unverhältnismäßig ist;~~

3.2 Biometrische Fernidentifizierung

Art. 5 Nr. 1 lit. d) KI-VO-E verbietet die Verwendung biometrischer Echtzeit-Fernidentifizierungssysteme in öffentlich zugänglichen Räumen zu Strafverfolgungszwecken. Allerdings wird dieses Verbot durch drei weitreichende Ausnahmen eingeschränkt. Es ist kritisch zu hinterfragen, warum biometrische Identifikationssysteme verboten sind, wenn sie in Realtime funktionieren, sonst aber nur

als Hochrisiko-KI-Systeme behandelt werden. Es ist nicht zu erkennen, dass die Gefahren solcher Systeme so unterschiedlich sind, dass diese unterschiedliche Behandlung gerechtfertigt wäre. Zudem ist unter Art. 5 ausschließlich die Nutzung zu Strafverfolgungszwecken untersagt - eine Nutzung durch private Akteure ist somit nicht verboten.

Viele Studien belegen die hohen Risiken biometrischer Identifizierungssysteme, da die Wahrscheinlichkeit schwerwiegender Verletzungen von Grundrechten wie der Privatsphäre und des Grundsatzes der Nichtdiskriminierung sehr hoch ist und weitreichende Folgen für die betroffene Person haben kann.[1] In vielen Situationen ist die Anonymität der wichtigste Schutz der Freiheit – und biometrische Identifizierungstechniken, die große Bereiche des öffentlichen Raums abdecken, gefährden diese Freiheit. Biometrische Identifizierungssysteme scheinen zudem zu hohen Fehlerquoten zu neigen und anfällig für Manipulationen zu sein.
Deswegen schließt sich der DAV der gemeinsamen Stellungnahme des Europäischen Datenschutzausschusses (EDPB) und des Europäische Datenschutzbeauftragten (EDPS) vom Juni 2021 an, die ein generelles Verbot von biometrischer Überwachung in öffentlichen Räumen fordert.[2] Ein neuer Initiativbericht des EU-Parlaments vom 6. Oktober 2021 liegt auf derselben Linie. Die Verwendung von biometrischen Fernidentifizierungssystemen in öffentlich zugänglichen Räumen sollte komplett verboten werden – unabhängig davon, ob die Überwachung durch private oder staatliche Akteure erfolgt und unabhängig davon, ob sie in Echtzeit oder mit Verzögerung stattfindet.

Änderungsvorschlag zu Artikel 5

(1) Folgende Praktiken im Bereich der künstlichen Intelligenz sind verboten:
(….)
d) die Verwendung biometrischer ~~Echtzeit-~~Fernidentifizierungssysteme in öffentlich zugänglichen Räumen, ~~außer wenn und insoweit dies im Hinblick auf eines der folgenden Ziele unbedingt erforderlich ist:~~

~~i) gezielte Suche nach bestimmten potenziellen Opfern von Straftaten oder nach vermissten Kindern;~~

~~ii) Abwenden einer konkreten, erheblichen und unmittelbaren Gefahr für das Leben oder die körperliche Unversehrtheit natürlicher Personen oder eines Terroranschlags;~~

[1] Christiane Wendehorst & Yannic Duller, Biometric Recognition and Behavioural Detection Assessing the ethical aspects of biometric recognition and behavioural detection techniques with a focus on their current and future use in public spaces, Study Requested by the JURI and PETI committees, August 2021; Studie Greens/EFA: current practices of biometric mass surveillance in the EU, 25 Oct 2021.
[2] EDPB-EDPS, Joint Opinion 5/2021 on the proposal for a Regulation of the European Parliament and the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act), 18 June 2021, RN 29-35.

~~iii) Erkennen, Aufspüren, Identifizieren oder Verfolgen eines Täters oder Verdächtigen einer Straftat im Sinne des Artikels 2 Absatz 2 des Rahmenbeschlusses 2002/584/JI des Rates62, der in dem betreffenden Mitgliedstaat nach dessen Recht mit einer Freiheitsstrafe oder einer freiheitsentziehenden Maßregel der Sicherung im Höchstmaß von mindestens drei Jahren bedroht ist.~~

3.3 Fehlendes Verbot von „Robo-Richtern“

Art. 5 KI-VO-E sieht momentan nicht vor KI-Systeme, die eigenständig gerichtliche Entscheidungen treffen, grundsätzlich zu verbieten. Wie bereits in SN 40/2020 ausführlich dargelegt (RN 22-31), dürfen gerichtliche und ähnlich eingriffsintensive verbindliche Entscheidungen staatlicher Instanzen jedoch nicht vollständig automatisiert werden.

Kein KI-System kann das Recht des Einzelnen erfüllen, von einem unparteiischen und unabhängigen Gericht gehört zu werden, wie es in Art. 47 Abs. (2) der EU-Grundrechtecharta (GRCh) festgelegt ist. Da es unmöglich ist festzustellen, auf welche Kriterien ein KI-System das Ergebnis stützt, und mit Hilfe welcher – möglicherweise unzureichenden oder voreingenommenen – Informationen zu Sachverhalt und Rechtsprechung dieses trainiert wurde, dürfte die Überprüfung der Unparteilichkeit des KI-Systems praktisch in vielen Konstellationen unmöglich sein. Darüber hinaus erfordert das Kriterium der Unparteilichkeit auch, dass die entscheidende Richterpersönlichkeit als Akteur identifiziert werden kann. KI-Systeme haben jedoch keine Rechtspersönlichkeit und können daher auch nicht für eine Entscheidung verantwortlich gemacht werden. Daher würde die Ersetzung einer gerichtlichen Entscheidung durch KI-Technologie eine Verletzung des Rechts auf rechtliches Gehör durch ein unabhängiges und unparteiisches Gericht darstellen.

Ergänzungsvorschlag zu Artikel 5

(1) Folgende Praktiken im Bereich der künstlichen Intelligenz sind verboten:
(….)
e) das Inverkehrbringen, die Inbetriebnahme oder die Verwendung von KI-Systemen, die den Zweck haben, gerichtliche und ähnlich eingriffsintensive verbindliche Entscheidungen staatlicher Instanzen zu automatisieren.

3.4 Fehlendes Verbot von Predictive Policing verletzt die Unschuldsvermutung

In Anhang III Ziff. 6 lit. a) KI-VO-E werden „KI-Systeme, die bestimmungsgemäß von Strafverfolgungsbehörden für individuelle Risikobewertungen natürlicher Personen“ eingesetzt werden, als Hochrisiko kategorisiert.

Der DAV fordert, dass jegliche Art der sog. „ vorhersagenden Polizeiarbeit“ (Predictive Policing) verboten werden muss und zwar sowohl im Bereich der Strafverfolgung, als auch im Bereich der Gefahrenabwehr. KI-Systeme, die zum Zwecke des Predictive Policing eingesetzt werden, können in Strafverfahren etwa zur Erstellung von Rückfallprognosen genutzt werden, um u.a. die Haftdauer eines Verurteilten zu bestimmen. Auf dem Gebiet des Gefahrenabwehrrechts greifen Polizeibehörden bereits jetzt auf KI-gestütztes Predictive Policing zurück, um ortsbezogene Gefahrprognosen zu erstellen. Eine Erstreckung solcher automatisierten Prognosen auf das Verhalten individueller Personen, um die Wahrscheinlichkeit zukünftiger Gefährdungshandlungen des/ der Betroffenen abzuschätzen, verbietet sich.

Der Einsatz von Predictive Policing-KI-Systemen im Bereich der Strafverfolgung verletzt das Recht auf ein faires Verfahren. Ein Einsatz zur Erstellung individueller Gefahrprognosen in der präventiven Polizeiarbeit würde das nicht hinnehmbare Risiko der Diskriminierung bestimmter Bevölkerungsgruppen begründen. KI-Systeme, die zur vorhersagenden Polizeiarbeit eingesetzt werden, spiegeln Verzerrungen in den Datensätzen wieder. Diese Verzerrungen rühren daher, dass herkömmliche Kriminalitätsstatistiken polizeiliche Aktivitäten widerspiegeln. Da polizeiliche Aktivitäten in Bezug auf einige soziale Gruppen häufiger stattfinden als in Bezug auf andere Gruppen, fließt dieses Ungleichgewicht in die Datensätze mit ein. Jegliche KI-Systeme der vorhersagenden Polizeiarbeit, die auf solchen Datensätzen aufbauen, können somit polizeiliche Voreingenommenheit widerspiegeln. Das bedeutet, dass KI-Systeme der vorhersagenden Polizeiarbeit auf dem Gebiet der Strafverfolgung die Unschuldsvermutung verletzen, indem sie Personen auf Grundlage von Rückschlüssen auf eine größere Gruppe als individuell verdächtig behandeln. Die Ergebnisse von Risikobewertungsinstrumenten im Strafrechtssystem und im vorgerichtlichen Kontext, wie z. B. Algorithmen zur Erstellung von Profilen von Personen in Gerichtsverfahren, stellen eine ernsthafte Bedrohung der Grundrechte dar. Entsprechendes gilt für individuelle Verhaltensprognosen auf dem Gebiet der polizeilichen Gefahrenabwehr.

Es ist stets zu berücksichtigen, dass die KI-Systeme sich auf rein mathematische Algorithmen gründen, denen ausschließlich statistische Berechnungen (Prognosen, Wahrscheinlichkeiten, Korrelationen) mit allen den damit verbundenen in der Statistik

bekannten Fehlerquellen zu Grunde liegen. Das System ist nur so gut wie die Datenqualität, die ihr zur Anlernung des „richtigen“ Wahrscheinlichkeits-Algorithmus zur Verfügung gestellt wird. Hinzu kommt, dass die Funktionsweise von Algorithmen weder transparent noch erklärbar ist. „*Wir wissen, welche Information eingespeist wird und was herauskommt, aber was dazwischen passiert, ist eine ‚Black Box‘*“ (vgl. hierzu Billis, Knust, Rui, FS für Sieber, S. 693 ff/707 m.w.N). Dies hat zur Konsequenz, dass Entscheidungen, die auf der Grundlage solcher von Maschinen berechneter „Erkenntnisse“ getroffen werden, für den in strafrechtlicher Hinsicht hiervon Betroffenen zu einer paradoxen „Beweislastumkehr“ führen. Es liegt an ihm, den (angesichts der „Black Box“) realistischer Weise nicht zu leistenden Nachweis zu erbringen, dass er von einem maschinellen Algorithmus zu Unrecht belastet wird.

Diese Instrumente stützen sich bei ihren Bewertungen auf eine umfassende Erhebung personenbezogener Daten, die nichts mit dem mutmaßlichen Fehlverhalten eines Betroffenen zu tun haben müssen. Darüber hinaus können einige KI-Systeme der vorhersagenden Polizeiarbeit auch die Anzahl der Fälle berücksichtigen, in denen eine Person einer Straftat verdächtigt wurde, unabhängig davon, ob diese Person anschließend verurteilt wurde oder nicht.

Diese Erhebung personenbezogener Daten zum Zweck der Vorhersage des Risikos einer erneuten Straftat kann nicht als notwendig oder verhältnismäßig im Hinblick auf das verfolgte Ziel angesehen werden, insbesondere im Hinblick auf die Auswirkungen auf das Recht auf Privatsphäre und die Unschuldsvermutung. Ein Bericht von Fair Trials belegt, dass die Einführung von KI-Systemen zur vorausschauenden Polizeiarbeit in vielen EU Mitgliedsstaaten zu diskriminierenden Ergebnissen geführt hat.[3]

Der Einsatz von KI-Systemen ist im Bereich der digitalen Forensik und der Bewertung des Rückfallrisikos mit Herausforderungen verbunden, da die spezifische Funktionsweise der Algorithmen den von den Ergebnissen ihrer Anwendung betroffenen Personen in der Regel nicht offengelegt wird. Dadurch kann der Betroffene die von den Algorithmen getroffenen Vorhersagen nicht in Frage stellen, was das Recht auf ein faires Verfahren gefährdet. Da der KI-VO-E nicht vorsieht, dass die Funktionsweise des algorithmischen Systems den Nutzern in zumutbarer Weise

[3] Fair Trials: “*Automating injustice: the use of Artificial intelligence & Automated decision-making systems in Criminal justice in Europe*”, 9 September 2021.

öffentlich zugänglich gemacht wird, gibt es keine Möglichkeit, eine auf diesen Daten basierende Entscheidung anzufechten.

Selbst wenn die hierfür erforderlichen Angaben frei zugänglich wären, müssten die betroffenen Parteien die kostspielige und zeitintensive Last der Datenanalyse selbst tragen. Eine solche Belastung würde ihre Situation im Verfahren erheblich verschlechtern und die Grundsätze eines fairen Verfahrens verletzen.

Ergänzungsvorschlag zu Artikel 5

(1) Folgende Praktiken im Bereich der künstlichen Intelligenz sind verboten:
(….)
f) KI-Systeme, die von Strafverfolgungs- und Sicherheitsbehörden für individuelle Risikobewertungen natürlicher Personen verwendet werden sollen, um das Risiko abzuschätzen, dass eine natürliche Person Straftaten begeht oder erneut begeht oder dass eine Person zum Opfer möglicher Straftaten wird.

3.5 Fehlendes Verbot von Lügendetektoren zur Strafverfolgung und im Migrationsrecht

Anhang III Ziff. 6 lit. b) KI-VO-E kategorisiert KI-Systeme, die „von Strafverfolgungsbehörden als Lügendetektoren“ eingesetzt werden sollen, als Hochrisiko. In Anhang III Ziff. 7 lit. a) werden unter der Überschrift „Migration, Asyl und Grenzkontrolle“ KI-Systeme, die „bestimmungsgemäß von zuständigen Behörden als Lügendetektoren (…) verwendet werden sollen“ als Hochrisiko kategorisiert. Da die Zuverlässigkeit von Lügendetektoren hochumstritten ist und große Risiken mit Blick auf die Unschuldsvermutung und allgemeine Verteidigungsrechte bestehen, setzt sich der DAV für ein vollständiges Verbot von Lügendetektoren, inklusive eines Verbots der Verwendung durch private Akteure, ein.

Ergänzungsvorschlag zu Artikel 5

(1) Folgende Praktiken im Bereich der künstlichen Intelligenz sind verboten:
(….)
g) KI-Systeme, die als Lügendetektoren und ähnliche Instrumente oder zur Ermittlung des emotionalen Zustands einer natürlichen Person verwendet werden sollen.

3.6 Fehlendes Verbot von KI-Systemen im Bereich Migration, Asyl und Grenzkontrollen

Der DAV fordert wie die CCBE-Stellungnahme ein Verbot von KI-Systemen im Bereich Migration, Asyl und Grenzkontrollen, bis diese von einer unabhängigen Stelle auf ihre Übereinstimmung mit internationalen Menschenrechtsstandards geprüft worden sind. Es gibt immer mehr Beispiele für den Einsatz von KI im Bereich der Migrationskontrolle, die eine wachsende Bedrohung für die Grundrechte von Migranten, das EU-Recht und die Menschenwürde darstellen.

Da die Migrationspolitik der EU zunehmend durch KI-Systeme wie Gesichtserkennung, Profilerstellung und Prognoseinstrumente unterstützt wird, die in Migrationssteuerungsprozessen, einschließlich der Zwangsrückführung, eingesetzt werden, besteht ein hohes Risiko, dass diese Anwendungsbereiche gegen das Recht auf Privatsphäre, das Recht auf Nichtdiskriminierung und verschiedene Grundsätze des internationalen Migrationsrechts, einschließlich des Rechts auf Asyl, verstoßen. Insbesondere besteht auch ein erhebliches Machtungleichgewicht, das durch den Einsatz von KI-Systemen im Bereich Migration, Asyl und Grenzkontrollen verschärft und ausgenutzt wird.

Im Migrationsrecht spielen für behördliche Entscheidungen eine Vielzahl von komplexen tatsächlichen Umständen im konkreten Einzelfall eine Rolle. Es ist sehr häufig im Rahmen eine Bewertung und ausführliche Abwägung verschiedener Umstände erforderlich. Zudem hat das Gebot der Verhältnismäßigkeit einer Entscheidung außerordentlich hohes Gewicht. In vielen Fällen haben die Behörden zudem ein Ermessen. Allenfalls in Bereichen, in denen Bewertungen und Abwägungen auf Tatbestands- oder Rechtsfolgenseite keine Rolle spielen, wäre der Einsatz eines KI-Systems, allerdings als Hochrisikosystem denkbar.
Besonders kritisch wären insbesondere

- die Bewertung der Glaubhaftigkeit von Angaben oder der Glaubwürdigkeit von Antragstellern in Asylverfahren sowie die Bewertung von Verfolgungsgefahren im Herkunftsstaat durch KI-Systeme,
- die Bewertung der Schlüssigkeit eines beabsichtigten Aufenthaltszwecks einschließlich eventueller Missbrauchsgefahren in Visaverfahren durch KI-Systeme,

- die Bewertung des Bestandes einer schützenswerten familiären Lebensgemeinschaft bei Verfahren auf Familiennachzugs bzw. hinsichtlich des aufenthaltsrechtlichen des Schutzes von Ehe und Familie durch KI-Systeme,
- die Bewertung etwaiger erforderlicher Qualifikationen im Bereich der Zuwanderung in Ausbildung und Beruf durch KI-Systeme;
- die Bewertung der von einem Ausländer ausgehenden Gefahren für die öffentliche Sicherheit und Ordnung im Ausweisungsrecht durch KI-Systeme,
- die Bewertung von Fluchtgefahren bei einer Abschiebungshaft durch KI-Systeme.

Ergänzungsvorschlag zu Artikel 5

(1) Folgende Praktiken im Bereich der künstlichen Intelligenz sind verboten:
(….)
h) Im Bereich Migration, Asyl und Grenzkontrollen sind folgende Praktiken verboten, bis diese von einer unabhängigen Stelle auf ihre Übereinstimmung mit internationalen Menschenrechtsstandards geprüft worden sind:
i) KI-Systeme, die bestimmungsgemäß von zuständigen Behörden zur Bewertung eines Risikos verwendet werden sollen, einschließlich eines Sicherheitsrisikos, eines Risikos der irregulären Einwanderung oder eines Gesundheitsrisikos, das von einer natürlichen Person ausgeht, die in das Hoheitsgebiet eines Mitgliedstaats einzureisen beabsichtigt oder eingereist ist;
ii) KI-Systeme, die bestimmungsgemäß von zuständigen Behörden zur Überprüfung der Echtheit von Reisedokumenten und Nachweisunterlagen natürlicher Personen und zur Erkennung unechter Dokumente durch Prüfung ihrer Sicherheitsmerkmale verwendet werden sollen;
iii) KI-Systeme, die bestimmungsgemäß zuständige Behörden bei der Prüfung von Asyl- und Visumanträgen sowie in Verfahren auf Erteilung von Aufenthaltstiteln und damit verbundenen Beschwerden im Hinblick auf die Feststellung der Berechtigung der den Antrag stellenden natürlichen Personen unterstützen sollen.

4. Hochrisiko-KI-Systeme

Die in Art. 6 ff. KI-VO-E gelisteten *Hochrisiko-KI-Systeme* werden zunächst legal definiert.

Überzeugend ist diese Definition insoweit, als sie sicherheitsrelevante KI bzw. Produkte mit KI-Basis reguliert (Art. 6 Abs. 1 KI-VO-E). Ob die regulierten Systeme wirklich auf solche beschränkt werden sollten, bei denen eine Konformitätsprüfung durch Dritte erforderlich ist, sollte kritisch hinterfragt werden. Gleichzeitig sollte jedoch der Grundsatz der risikoangemessenen Regulierung von KI-Systemen beibehalten und sollten nur solche Systeme als Hochrisiko-KI-Systeme eingestuft werden, deren

Eigenschaften eine verstärkte Regulierung notwendig machen. Immerhin dürfte die insofern in Annex II aufgeführte EU-Gesetzgebung hier ein deutlicher Fingerzeig für ein höheres Gefahrenpotenzial sein. Vor diesem Hintergrund ist es verständlich, dass Art. 6 Abs. 2 KI-VO-E die Möglichkeit zur Klassifizierung als hochriskantes und damit zu regulierendes KI-System durch Annex III erweitert.

Allerdings sind die in Annex III genannten Kategorien von Hochrisiko-KI-Systemen zu weit gefasst. KI-Systeme bedürfen keiner Ex-Ante-Regulierung in Form von Transparenzpflichten oder Anforderungen an die Datenbasis, wenn bereits marktwirtschaftliche Prinzipien die Regulierungsziele verwirklichen. Beispielsweise erfasst Annex III derzeit Angebote wie die Internetsprachschule Duolingo. Das Unternehmen bietet einen KI-basierten Sprachtest an, den Hochschulbewerber als Nachweis für ihre Fremdsprachenkenntnisse verwenden können.[4] Ein kommerzielles Testsystem, das den Teilnehmern fehlerhaft bzw. ohne nachvollziehbaren Grund ein erfolgreiches Testergebnis vorenthält, wird sich im Marktvergleich gegen andere Testsysteme nicht durchsetzen. Die Anbieter solcher Anwendungen haben ein Eigeninteresse daran, nachvollziehbare und qualitativ hochwertige Tests anzubieten. Eine zusätzlich hierzu wirkende Ex-Ante-Regulierung ist überflüssig.

Zudem sind, auch wenn es der EU-Kommission vor allem um die Regulierung grund- bzw. menschenrechtsrelevanter KI-Systeme geht, die Kriterien für die Berücksichtigung in der Liste des Annex III nicht ohne weiteres ersichtlich und erschweren daher auch eine Einschätzung der Erweiterungsmöglichkeiten des Annex III nach Art. 7 KI-VO-E. Auch hier gilt, dass Art. 7 KI-VO-E in Abs. 2 noch klarere Leitlinien für eine Erfassung weiterer KI-Systeme in Annex III bieten sollte.

Die Grundpfeiler des KI-VO-E für hochriskante KI-Systeme sind ebenfalls positiv zu bewerten, nämlich namentlich:

- eine verstärkte Verpflichtung zum Qualitäts- und Risikomanagement (Art. 9 und 17 KI-VO-E) einschl. Post Market Monitoring (Art. 61 KI-VO-E),
- eine stärkere Regulierung von Trainings- und Testdaten (Art. 10 und 9 Abs. 5 – 7 KI-VO-E),

[4] https://www.ft.com/content/a5970b6c-e731-45a7-b75b-721e90e32e1c, 25. Juli 2021.

- eine Forderung nach den Möglichkeiten und der Durchführung eines Event Logging (Art. 12, 16 lit. a) und d) bzw. Art. 29 Abs. 5 KI-VO-E) sowie schließlich
- die Beobachtungspflichten nicht nur des Anbieters, sondern auch des Nutzers (Art. 29 Abs. 4 KI-VO-E).

Die besagten Anforderungen und Pflichten sollten dazu führen, den typischen Risiken zumindest der sog. schwachen KI – insbesondere solcher KI-Systeme, die zu einem gewissen Grad selbstlernend agieren – ein Stück weit entgegenwirken zu können.

So liegt die besondere Schwierigkeit der rechtlichen Behandlung der Gefahren der KI darin, dass KI-Systeme einerseits menschliches Verhalten und menschliche Entscheidungen substituieren bzw. übernehmen können, insofern also effizienzfördernd wirken, andererseits ihr Verhalten und ihre Entscheidung oftmals *unvorhersehbar* sind, so dass es eines erhöhten Qualitäts- und Risikomanagements bedarf. Hinzu kommt, dass Mängel von KI-Systemen nicht allein in der Konstruktion und Fabrikation begründet sein müssen, sondern insbesondere das Training der Systeme (etwa neuronaler Netze) von besonderer Bedeutung ist. Insofern wirken die Anforderungen an das Training und die Governance von Trainings- und anderen Daten (vgl. Art. 10, Art. 9 Abs. 5 - 7 KI-VO-E) mutmaßlich risikoreduzierend. Da Fehlentscheidungen und Fehlverhalten dieser Systeme aber nicht von vornherein ausgeschlossen werden können, ist es konsequent, (i) mit dem Event Logging eine spätere Nachverfolgbarkeit einzufordern und (ii) mit Hilfe der Anforderungen und Pflichten mit Blick auf Testdaten sowie Beobachtungspflichten eine erhöhte Aufmerksamkeit mit Blick auf die Systeme einzufordern.

4.1 KI Systeme im Bereich Beschäftigung (Annex III Ziff. 4)

Die extensive Definition der Künstlichen Intelligenz in Annex I in Verbindung mit der Definition der high-risk-Systeme in Annex III, die alle Entscheidungen zur Auswahl, die Arbeitszuweisung und die Überwachung von Verhalten und Leistung von Mitarbeitenden umfasst, führt im Arbeitsverhältnis zu einer nahezu umfassenden Unterwerfung aller informationstechnologischer Systeme unter den Anwendungsbereich der Verordnung. Dabei besteht ein Widerspruch der Definition von KI in Annex I gegenüber der Definition von KI in Art. 3 lit. a) der Entschließung des Europäischen Parlaments vom 20.10.2020 mit Empfehlungen an die Kommission für eine Regelung

der zivilrechtlichen Haftung beim Einsatz künstlicher Intelligenz (2020/2014(INL)). Danach ist ein „KI-System“ ein softwaregestütztes oder in Hardware-Geräte eingebettetes System, das ein Intelligenz simulierendes Verhalten zeigt, indem es unter anderem Daten sammelt und verarbeitet, seine Umgebung analysiert und interpretiert und mit einem gewissen Maß an Autonomie Maßnahmen ergreift, um bestimmte Ziele zu erreichen.

Es ist unbedingt erforderlich, dass alle Initiativen zu Regelungen in Bezug auf das Einführen und Anwenden von KI mit parallelen Initiativen zur Haftung abgestimmt werden. Dabei liegt es aus Sicht des DAV nahe, nicht jede Software als KI zu definieren, wie dies durch den hier in Rede stehenden KI-VO-E der Fall ist. Der damit verbundene Eingriff, der Hersteller, Anbieter und Nutzer gleichermaßen betrifft, dürfte nicht nur mit Blick auf die vorgeschaltete Frage der Subsidiarität, sondern auch mit Blick auf die inhaltliche Frage der Verhältnismäßigkeit des damit verbundenen Eingriffs in die unternehmerische Freiheit auch unter Berücksichtigung des Grundrechts auf informationelle Selbstbestimmung sowie den Schutz vor Diskriminierung zweifelhaft sein.

Deutlich wird die Problematik der Erfüllbarkeit der im aktuellen Vorschlag enthaltenen Regelungen auch in Bezug auf den Arbeitgeber, der als Nutzer ein solches System anwendet. Er kann bei vorhandener CE-Zertifizierung lediglich darauf vertrauen, dass das System die Vorgaben der Verordnung erfüllt. Die Dokumentationen, die der Anbieter bereitzustellen hat, mag dabei dem Arbeitgeber die Aufgabe erleichtern, die Wahrung anderweitiger Schutzvorschriften einschließlich des Datenschutzes zu gewährleisten. Sobald der Arbeitgeber allerdings ein entsprechendes System an seine eigenen unternehmerischen Bedürfnisse anpasst oder ein vorhandenes System durch eine bloße Zweckänderung zum high-risk-System macht, wird er gemäß Art. 28 VO-E zum Anbieter des Systems mit allen damit verbundenen Dokumentations- und Informationspflichten.

Darüber hinaus ist zu bedenken, dass der Schutz der Menschenrechte bei Einsatz von technischen Systemen nicht nur durch den Datenschutz, sondern in Deutschland auch durch die betriebliche Mitbestimmung gewährleistet wird, die insoweit umfassende Überprüfungs- und Mitbestimmungsrechte besitzt. Gerade kleine und mittlere

Unternehmen können durch die zusätzlichen bürokratischen Anforderungen schnell überfordert werden und erhebliche Wettbewerbsnachteile erleiden. Gleichzeitig besteht die Gefahr, dass technische Anforderungen jedenfalls durch den Nutzer nicht selbst überprüft werden können. Das gilt insbesondere dort, wo durch Zweckänderungen die Schwelle zwischen Nutzer und Anbieter überschritten wird.

Der DAV regt deshalb an, jedenfalls im Beschäftigungskontext lediglich solche Systeme in Annex III aufzunehmen, die Ansätze des maschinellen Lernens i.S.v. Annex I lit. (a) des Verordnungsentwurfs beinhalten und damit den Überlegungen in der Entschließung des Europäischen Parlaments vom 20.10.2020 nahekommen.

4.2 KI-Systeme im Bereich der öffentlichen Verwaltung (Annex III Ziff. 5)

Der Anwaltschaft kommt die besondere Aufgabe zu, sich für die Wahrung der Rechtsstaatlichkeit beim Einsatz von KI-Systemen durch die öffentliche Verwaltung einzusetzen.

KI-Systeme werden bei der Zuteilung von sozialen und wirtschaftlichen Rechten und Leistungen, bei der Überprüfung der Identität und bei der Berechnung der Zugangsberechtigung zu Sozialleistungen eingesetzt.

Die Intransparenz von KI-Systemen hat zur Folge, dass diskriminierende oder anderweitig verzerrte Ergebnisse rechtsstaatliche Verfahren gefährden, da sie schwer zu erkennen und vor einem Richter anzufechten sind.

Ein besonders kritisches Beispiel sind das Profiling und Punktevergabesysteme, die erhebliche Risiken für die Privatsphäre und den Datenschutz darstellen. All dies kann weitreichende Auswirkungen auf den Zugang der Menschen zu lebenswichtigen öffentlichen Dienstleistungen und damit auf das Grundrecht der Bürger auf soziale Sicherheit und soziale Unterstützung haben.

Das Risiko einer diskriminierenden Profilerstellung oder falscher Ergebnisse geht Hand in Hand mit den Risiken, die sich aus der Verarbeitung sensibler biometrischer Daten ergeben. Deswegen fordert der DAV, dass der Einsatz und die Anwendung von KI-Systemen, die den Zugang zu sozialen Rechten und Leistungen verletzen, eingeschränkt werden muss.

4.3 KI-Systeme im Bereich Strafverfolgung (Annex III Ziff. 6)

In Anhang III Ziff. 6 lit KI-VO-E lit. a) bis g) werden bestimmte KI-Systeme im Bereich Strafverfolgung als Hochrisiko definiert. Jeglicher Einsatz von KI-Systemen im Strafrecht geht mit beträchtlichen Risiken einher, die die Ausübung verfahrensrechtlicher Grundrechte behindern könnten. Insbesondere betrifft dies das Recht auf einen wirksamen Rechtsbehelf und ein unparteiisches Gericht sowie die Unschuldsvermutung und allgemeine Verteidigungsrechte.

Der DAV setzt sich für eine vollständige Wahrung der Grundsätze von Transparenz und Erklärbarkeit in der Strafverfolgung ein. In Fällen, in denen Entscheidungen auf Daten oder Ergebnissen beruhen, die von einem KI-System erstellt wurden, müssen die Parteien und/oder ihre Anwälte die Möglichkeit haben, Zugang zu diesem KI-System zu erhalten und dessen Merkmale, die verwendeten Daten und die Relevanz der von ihm gelieferten Ergebnisse bewerten können. Folglich sollte sog. „starke KI“ nur in dem Maße eingesetzt werden, in dem es noch möglich ist, zu überprüfen, wie die Maschine das vorgeschlagene Ergebnis erzielt hat, und die Elemente, die sich aus dem Einsatz von KI ergeben, von den persönlichen Überlegungen des Richters zu unterscheiden.

Deswegen setzt sich der DAV dafür ein, dass Art. 13 dahingehend ergänzt wird, dass KI-Systeme, wenn sie in der Justiz eingesetzt werden, das Recht auf ein faires Verfahren nicht beeinträchtigen und die Rechte der Verteidigung nicht verletzen dürfen. In Anbetracht der Tatsache, dass die Art und Weise, in der einige KI-Systeme ihre Ergebnisse produzieren, möglicherweise nicht hinreichend erklärt werden kann (das sog. „Blackbox-Problem“), und der Tatsache, dass das Transparenzerfordernis möglicherweise aus unterschiedlichen Gründen nicht immer erfüllt werden kann, muss der KI-VO-E andere Schutzmaßnahmen vorsehen. Beispielsweise könnte eine Regelung eingeführt werden, nach der das von einem KI-System gelieferte Ergebnis im Zweifelsfall oder wenn die Anforderungen an Transparenz oder Erklärbarkeit nicht erfüllt sind, nicht berücksichtigt werden darf.

Insbesondere setzt sich der DAV auch dafür ein, dass die Ausnahme der Transparenzverpflichtungen unter Art. 52 Abs. 1 im Bereich der Strafverfolgung aufgehoben wird. Diese Ausnahme ist zu weitreichend und gefährdet das Recht auf ein faires Verfahren. Deswegen schließt sich der DAV der gemeinsamen Stellungnahme

des EDPB und EDPS an. Diese fordert eine Unterscheidung zwischen KI-Systemen, die zur Aufdeckung oder Verhütung von Straftaten eingesetzt werden, und KI-Systemen, die zur Ermittlung oder Verfolgung von Straftaten beitragen sollen. Aufgrund der Unschuldsvermutung müssen die Sicherheitsvorkehrungen für Prävention und Aufdeckung stärker sein.[5] Deswegen ist der DAV der Ansicht, dass die vorgeschlagene Ausnahme vom Grundsatz der Transparenz gestrichen werden sollte.

Änderungsvorschlag zu Artikel 52

(1) Die Anbieter stellen sicher, dass KI-Systeme, die für die Interaktion mit natürlichen Personen bestimmt sind, so konzipiert und entwickelt werden, dass natürlichen Personen mitgeteilt wird, dass sie es mit einem KI-System zu tun haben, es sei denn, dies ist aufgrund der Umstände und des Kontexts der Nutzung offensichtlich. ~~Diese Vorgabe gilt nicht für gesetzlich zur Aufdeckung, Verhütung, Ermittlung und Verfolgung von Straftaten zugelassene KI-Systeme, es sei denn, diese Systeme stehen der Öffentlichkeit zur Anzeige einer Straftat zur Verfügung.~~

4.4 KI-Systeme im Bereich Migration, Asyl und Grenzkontrolle (Annex III Ziff. 7)

Gemäß Anhang III, Ziffer 7 werden bestimmte KI-Systeme im Berich Migration, Asyl und Grenzkontrolle als Hochrisikosysteme qualifiziert. Der DAV empfiehlt aus den bereits unter Ziffer 3.6 genannten Gründen, die Verwendung von KI-Systemen in diesem Bereich zu verbieten.

4.5 KI-Systeme in der Justiz (Annex III Ziff. 8)

KI-Systeme in der Justiz werden in Anhang III, Ziff. 8 KI-VO-E unter der Überschrift „Rechtspflege und demokratische Prozesse“ als Hochrisiko-KI-Systeme kategorisiert. Der Einsatz von KI-Systemen wirft insbesondere mit Blick auf die Grundrechte und die Rechtsstaatlichkeit viele Fragen auf, die nicht allein durch die Einstufung als Hochrisiko beantwortet werden können. Stattdessen empfiehlt der DAV, detaillierte Prinzipien und Grundsätze für den Einsatz von KI-Systemen im Justizbereich festzulegen. Jegliche unterstützenden KI-Systeme in der Justiz nur dann eingeführt werden, wenn ausreichende Garantien gegen Diskriminierung und Voreingenommenheit gegeben sind.

[5] EDPB-EDPS, Joint Opinion 5/2021 on the proposal for a Regulation of the European Parliament and the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act), 18 June 2021, RN 70.

Die Formulierung in Anhang III, Ziff. 8 KI-VO-E sollte so formuliert werden, dass es einem Richter nicht gestattet sein darf, seine Entscheidungsbefugnis ganz oder teilweise an ein KI-System zu delegieren. Insbesondere im Bereich der Justiz sollte nicht nur die automatisierte Entscheidungsfindung durch KI-Systeme verboten werden, sondern auch der Einsatz von KI-Systemen, die „Entscheidungen“ produzieren, die einen menschlichen Richter dazu verleiten könnten, diese unkritisch zu übernehmen - und damit faktisch eine automatisierte Entscheidungsfindung abzustempeln.

Der gesamte Entscheidungsfindungsprozess muss menschenzentriert bleiben. Richter müssen die volle Verantwortung für alle Entscheidungen übernehmen. Das Recht auf einen menschlichen Richter sollte in allen Phasen des Verfahrens gewährleistet sein. In Anhang III.8 und Erwägungsgrund 40 sollte klargestellt werden, dass in Fällen, in denen ein KI-System zur „Unterstützung“ von Justizbehörden eingesetzt werden kann, die Möglichkeit ausgeschlossen ist, dass dieses System tatsächlich Entscheidungen trifft oder den Wortlaut solcher Entscheidungen formuliert.

Wenn die Verwendung von unterstützenden KI-Systemen in der Justiz zu einer automatischen Übernahme von Entscheidungen führt, würden Richter Gefahr laufen, nichts weiter als ein Vehikel für maschinengenerierte Entscheidungen zu sein. Die Grenze zwischen einer Einstufung als Hochrisiko auf der einen Seite und verbotenen KI-Systemen auf der anderen Seite sollte danach definiert werden, ob den betroffenen Richtern ein ausreichender Ermessensspielraum überlassen wird, eine autonome, unparteiische und unvoreingenommene Entscheidung zu treffen.

Folglich sollte die Entscheidung eines Richters auf einer Begründung beruhen, die von der Vorhersage des KI-Instruments hinreichend unabhängig ist, so dass eine klare Unterscheidung zwischen beiden gewährleistet wird. Jeder Richter sollte seine eigene Argumentation so klar darlegen können, dass nachprüfbare Gründe für die Befolgung (oder Ablehnung) der durch KI-Systeme generierten Entscheidung angegeben werden können.[6] Wenn die letztendliche Entscheidung zu einer reinen Formalität verkommen würde, würde das Recht auf rechtliches Gehör unangemessen eingeschränkt.

[6] Enders, Peter, Einsatz künstlicher Intelligenz bei juristischer Entscheidungsfindung, JA 2018, 721 (723).

Der DAV fordert, dass der der KI-VO-E konkrete Bestimmungen enthält, die auf spezifische Risiken abzielen, wie z.B. das Risiko eines unfairen Verfahrens. Ein unfaires Verfahren wäre u.a. dann gegeben, wenn die Parteien nicht die Möglichkeit haben, die Ergebnisse eines KI-Systems, das in einem gerichtlichen Entscheidungsprozess eingesetzt wurde, zu bewerten, zu diskutieren und Einwände dagegen zu erheben.
Um die Achtung der Grundrechte und des Rechts auf ein faires Verfahren zu gewährleisten, sollte klar und deutlich zum Ausdruck gebracht werden, dass der KI-VO-E die Festlegung zusätzlicher allgemeiner Regeln nicht ausschließt, die den Einsatz von KI in den Bereichen der Justiz, einschließlich strafrechtlicher Ermittlungen durch die Strafverfolgungsbehörden, weiter einschränken oder verbieten. Der Einsatz von KI-Systemen in der Justiz muss mit den Grundwerten der Anwaltschaft und der Gewährleistung eines fairen Verfahrens in Einklang gebracht werden, insbesondere mit der Waffengleichheit und der Unparteilichkeit des Gerichts. Diese Grundrechte müssen für alle Rechtssuchenden gewährleistet bleiben.

5. Anforderungen für Hochrisiko-KI-Systeme

Ohne den Anspruch auf Vollständigkeit sei im Detail auf Folgendes hingewiesen:

- Inhaltlich zu hinterfragen ist, warum Nutzer im Sinne der geplanten Verordnung nur professionelle Nutzer sind (Art. 3 Abs. 4 KI-VO-E). Auch wenn das wahrscheinlich praktisch nur in wenigen Fällen von Bedeutung ist, fragt sich, was für nichtprofessionelle Anbieter und Anwender (etwa bei Idealvereinen und NGOS) heißt. Die DSGVO etwa kennt eine Ausnahme nur für natürliche Personen zur Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten (Art. 2 Abs. 2 lit. c) DSGVO). Der Unterschied überzeugt nicht.
- Auffällig ist, dass in Art. 9 Abs. 3 KI-VO-E für Sicherheitsmaßnahmen lediglich der *anerkannte Stand der Technik* gefordert wird. Dieses ist gerade für Hochrisiko-KI-Systeme überraschend, zumal etwa das Produkthaftungsrecht und auch die deutsche Rechtsprechung sogar die Einhaltung des Stands der Wissenschaft und Technik fordern.[7] Hier sollte in Ansehung der Hoch-Risiko-Systeme einerseits und Bußgelder sowie zur Innovationsförderung anderseits

[7] vgl. § 1 Abs. 2 Nr. 5 ProdHaftG; *Hofmann*, CR 2020, 282, 284 f.

zumindest der Kompromiss gesucht werden, auf den neuesten Stand der Technik abzustellen.

- Die Anforderung in Art. 10 Abs. 3 S. 1 KI-VO-E, nach der Trainings-, Validierungs- und Testdatensätze relevant, repräsentativ, fehlerfrei und vollständig sein müssen, ist darauf angelegt, durch harmonisierte Standards (Art. 40 KI-VO-E) oder Durchführungsrechtsakte der EU-Kommission (Art. 41 KI-VO-E) konkretisiert zu werden. Wenn die Industrie bzw. die Kommission diese konkretisierenden Maßnahmen definieren, sollten sie praxistaugliche Anforderungen an die Datensätze stellen. In Art. 10 Abs. 3 S. 1 KI-VO-E sollte daher ein „bestmöglich“ oder „im zumutbaren Rahmen“ ergänzt werden. Außerdem lassen sich die Relevanz, Repräsentanz, Vollständigkeit und Fehlerfreiheit der Daten nur vor dem Hintergrund des bestimmungsgemäßen Verwendungszwecks definieren. Dieser Bezug in Art. 10 Abs. 3 S. 1 KI-VO-E durch die Ergänzung „… *müssen mit Blick auf die Zweckbestimmung des Hochrisiko-KI-Systems relevant* …“ klargestellt werden. Schließlich sollte Art. 10 Abs. 3 S. 1 KI-VO-E so ausgebaut werden, dass diese Regelung begrenzte Verarbeitungen personenbezogener Daten rechtfertigen kann, ggf. in hinreichend pseudonymisierter Form. Daher sollte klargestellt werden, dass das Interesse am Erhalt eines repräsentativen, vollständigen und fehlerfreien Datensatzes ein berechtigtes Interesse im Sinne von Art. 6 Abs. 1 S. 1 lit. f DSGVO ist. Dennoch ist für einen gerechten Ausgleich der betroffenen Grundrechte in Einzelfällen eine Rückausnahme nötig, die es erlaubt, von diesen Qualitätsanforderungen an Trainings-, Validierungs- und Testdatensätze abzurücken, *soweit* der Schutz anderer Rechtgüter (insb. der Datenschutz) dieses zwingend erfordert.
- Art. 28 Abs. 1 KI-VO-E fordert vom Nutzer, die Anbieterpflichten einzuhalten, wenn er die Zweckbestimmung eines bereits im Verkehr befindlichen oder in Betrieb genommenen Hochrisiko-KI-Systems verändert oder wenn er eine wesentliche Änderung an dem Hochrisiko-KI-System vornimmt. Es ist zu bezweifeln, dass er hierzu in der Lage sein wird, ohne sich hierüber mit dem Original-Anbieter zu verständigen. Bei der Veredelung von IT-Diensten könnte dieses zu einer Abhängigkeit von der Wissenshoheit des Original-Anbieters auf abgeleiteten Märkten führen, der entweder durch "Zugangsrechte" zu diesem

Wissen gegen angemessene Vergütung entgegnet werden sollte oder aber zumindest durch eine Relativierung dieser Pflichten (z.B. "soweit" statt "wenn").

- Widersprüchlich ist es, wenn in Art. 28 Abs. 2 KI-VO-E der Anbieter teils aus der Verantwortlichkeit entlassen wird, wenn die KI-Systeme stark verändert bzw. entgegen ihrem Verwendungszweck genutzt werden. Dieses widerspricht dem grundsätzlichen Ansatz sowohl des Produkthaftungsrechts als auch des KI-VO-E (vgl. etwa Art. 9 Abs. 2 lit. b), 4 lit. c), 13 Abs. 3 lit. b) (iii) und 14 Abs. 2 KI-VO-E), nachdem auch immer der zu erwartende Missbrauch eines Systems vom Anbieter mitberücksichtigt und im optimalen Fall (Konstruktion vor Instruktion) mit verhindert werden sollte.
- Die Regelungen zu harmonisierten Normen nach Art. 40 KI-VO-E tragen das Risiko in sich, in einem sehr innovativen Geschäftsfeld nicht ausreichend schnell agieren zu können (sprich: die Vermutung könnte sich nach kurzer Zeit als überholt erweisen), die Regelung nach Art. 41 KI-VO-E beinhaltet das Risiko, Durchführungsakte in besonders sensiblen und grundrechtsrelevanten Bereichen auf die Kommission (also die Verwaltung) zu verlagern.
- Art. 63 Abs. 2 KI-VO-E sieht die Information nur von *"einschlägigen nationalen Wettbewerbsbehörden"* vor. Unklar ist, ob das heißt, dass nur Behörden aus einzelnen Mitgliedsstaaten unterrichtet werden müssen, oder ob in jedem Mitgliedsstaat die zuständige Wettbewerbsbehörde informiert werden muss. Eine Klarstellung wäre sinnvoll.

6. Daten- und Geheimnisschutz

Die aus Sicht des öffentlichen Sicherheits- und des Zivilrechts zu begrüßende, umfassende Datenaufzeichnung (insb. von Eventlogs) und Dokumentation, wie sie von der KI-VO-E gefordert werden, kollidieren mit dem Daten- und Geheimnisschutz.

Die KI-VO-E versucht, den widerstreitenden Schutz vor Gefahren mit dem Datenschutz an einigen Stellen in Einklang zu bringen (Art. 10 Abs. 5, Art. 29 Abs. 6 KI-VO-E). Es ist zu bezweifeln, dass diese Regelungen ausreichen, um KI-Systeme, die oftmals auf Big Data aufsetzen, ausreichend zu regulieren. Die Thematik und das Verhältnis zur DSGVO sind weiter zu klären. So stellt sich u.a. die Frage, ob Eventlogs fortlaufend mitgeschrieben und aufgezeichnet werden dürfen bzw. müssen. Sinnvoll könnte es u.U. sein, die Archivierung zeitlich zu begrenzen ("Ringspeicherung") und nur im Störfall

oder bei Rechtsgutverletzungen / Unfällen die Daten längerfristig zu speichern. Überdies sollte – gerade mit Blick auf KI-Systeme im medizinischen Bereich – mit Blick auf sensitive Daten i.S.v. Art. 9 Abs. 1 DSGVO eine zusätzliche Erlaubnisnorm geschaffen werden, die über die dort in Abs. 2 geregelten Tatbestände hinausgeht.

Art. 70 KI-VO-E betrifft die Wahrung der Vertraulichkeit der Informationen und Daten durch die dort im Einzelnen bezeichneten nationalen Behörden und notifizierten Stellen. Hier ist dringend eine Ausweitung der Verpflichtung zur Vertraulichkeit auf alle Behörden und Stellen einschließlich der Kommission geboten. Soweit Informationen und Daten geschützt sind, muss dieser Schutz auch bei der Ausübung der Aufgaben und Tätigkeiten durch sämtliche Behörden und Stellen gewahrt bleiben, die mit den Informationen und Daten in Berührung kommen.

Das Gleiche gilt für Private, soweit diese ebenfalls als Normadressaten in der Verordnung genannt und angesprochen sind. Auch hier ist für die umfassende Sicherung von Daten und Geschäftsgeheimnissen Sorge zu tragen. Dies betrifft zum einen diejenigen Anbieter (vgl. die Definition in Art. 3 Nr. 2), die selbst KI-Systeme entwickeln oder entwickeln lassen und in Verkehr bringen oder in Betrieb nehmen, und die Nutzer (vgl. die Definition in Art. 3 Nr. 3), die KI-Systeme verwenden. Im Rahmen dieser Tätigkeiten können sowohl Anbieter als auch Nutzer mit der Erstellung, Sammlung und Speicherung von Daten und Geschäftsgeheimnissen befasst sein. Darüber hinaus bestehen weitreichende Pflichten, etwa zur technischen Dokumentation (Art. 11) oder Aufzeichnungspflichten (Art. 12). Art. 13 verlangt darüber hinaus die Bereitstellung von Informationen für Nutzer. Für Hochrisiko-Systeme bestehen Informationspflichten nach Art. 22. Auch dabei können Geschäftsgeheimnisse betroffen sein, für deren Wahrung Sorge zu tragen ist. Art. 70 KI-VO-E muss auch diese Fallgestaltungen mit einbeziehen. Unabhängig davon, ob nach anderen gesetzlichen Vorschriften der Geheimnisschutz eingreift, wäre es unzureichend, wenn Art. 70 KI-VO-E nur einzelne Behörden und Stellen anspricht.

Soweit zum anderen Behörden in ihrer Tätigkeit betroffen sind, schließt dies nicht aus, dass auch Private dabei mit Geschäftsgeheimnissen in Berührung kommen. Ein Beispiel ist die Einsichtnahme in Akten im Rahmen der Wahrnehmung von

Informationsrechten. Auch dies spricht dafür, Private in die Verpflichtungen nach Art. 70 KI-VO-E einzubeziehen.

Hinsichtlich des Umfangs der Daten und Informationen darf es keine Beschränkung hinsichtlich des Geheimnisschutzes geben. Soweit es sich um Geschäftsgeheimnisse handelt, muss für den Schutz dieser Geheimnisse Sorge getragen werden. Die Richtlinie über den Schutz von Geschäftsgeheimnissen enthält ausreichende Ausnahmen in Einzelfällen (z.B. zum Schutz überragender Rechtsgüter). Darüber hinaus darf es keine weiteren Einschränkungen oder Ausnahmen des Geheimnisschutzes geben.

Für den Geheimnisschutz kann es keinen Unterschied machen, ob Daten durch KI-Systeme selbst generiert und gesammelt werden oder durch natürliche Personen mit Hilfe von KI-Systemen. Für diese Daten und Informationen muss unterschiedslos der Geheimnisschutz gewahrt bleiben.

Mit dem Geheimnisschutz müssen die Sanktionen korrespondieren, die in den Artt. 71 und 72 formuliert sind. Diese Vorschriften nehmen nicht ausdrücklich Bezug auf die Wahrung der Vertraulichkeit nach Art. 70. Die konkrete Nennung der Verpflichtungen nach Art. 5 und 10 lässt es zumindest offen, ob der Schutz der Geschäftsgeheimnisse davon ebenfalls erfasst sein soll. Hier wäre eine Klarstellung wünschenswert, die Verstöße gegen Art. 70 ausdrücklich einbezieht.