Vorschlag COM(2021) 206 vom 21. April 2021 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.

EUROPÄISCHES GESETZ ÜBER KÜNSTLICHE INTELLIGENZ

cep**Analyse** 27/2021

VOLLSTÄNDIGE ANALYSE [zur Kurzfassung]

Inhalt

A. Wesentliche Inhalte des Verordnungsvorschlags

1 Ziel- und Anwendungsbereich

- Die Verordnung enthält EU-weite Regeln für die Entwicklung, Vermarktung und Verwendung künstlicher Intelligenz („KI"). Dies soll [Erwägungsgründe 1, 5]
  - den Binnenmarkt stärken,

Autoren: Dr. Lukas Harta, LL.M. und Dr. Matthias Kullas | kullas@cep.eu
cep | Kaiser-Joseph-Straße 266 | 79098 Freiburg | Telefon 0761 38693-0 | www.cep.eu

  - die Gesundheit, die Sicherheit und die Grundrechte schützen.

- Ein KI-System ist eine Software,
  - die für von Menschen festgelegte Ziele Ergebnisse – wie Inhalte, Vorhersagen, Empfehlungen oder Entscheidungen – hervorbringen kann und damit ihr Umfeld beeinflusst, und
  - die zumindest mit einer der folgenden Techniken und Konzepte entwickelt wurde [Art. 3 (1), Anhang I]:
    - Konzepte maschinellen Lernens;
    - Logik- und wissensgestützte Konzepte, z.B. Wissensrepräsentation, induktive Programmierung, oder Inferenz- und Deduktionsmaschinen;
    - statistische Ansätze, Bayes'sche Schätz-, Such- und Optimierungsmethoden.

- Die Kommission kann die Liste von Techniken und Konzepten mittels delegierter Rechtsakte an Marktentwicklungen und technische Entwicklungen anpassen [Art. 4].

- Die Vorschriften der Verordnung gelten für [Art. 2(1)]
  - Anbieter von KI-Systemen aus der EU und Drittstaaten, die KI-Systeme in der EU in Verkehr bringen oder in Betrieb nehmen,
  - Gewerbliche und behördliche Nutzer („Nutzer") von KI-Systemen in der EU, und
  - Anbieter und Nutzer in einem Drittstaat, wenn die von KI-Systemen generierten Ergebnisse in der EU verwendet werden.

- Die Verordnung verfolgt einen risikobasierten Ansatz: Besonders gefährliche KI-Systeme werden verboten, während für andere KI-Systeme nach Risiko abgestufte Pflichten, freiwillige Verhaltenskodizes oder gar keine KI-spezifischen Pflichten gelten.

2 Verbotene KI-Systeme

- Die folgenden KI-Systeme dürfen nicht in Verkehr gebracht, in Betrieb genommen oder verwendet werden:
  - KI-Systeme, die Techniken der „unterschwelligen" Beeinflussung außerhalb des Bewusstseins einer Person einsetzen, um deren Verhalten zu beeinflussen, sodass sie sich selbst oder einer anderen Person einen „physischen oder psychischen Schaden" zufügen kann [Art. 5 (1) (a)];
  - KI-Systeme, die eine Schwäche oder Schutzbedürftigkeit einer Person aufgrund des Alters, einer körperlichen oder geistigen Behinderung ausnutzen, um sie zu beeinflussen, sodass sie sich selbst oder einer anderen Person einen „physischen oder psychischen Schaden" zufügen kann [Art. 5 (1) (b)].

- Behörden dürfen KI-Systeme nicht in Verkehr bringen, in Betrieb nehmen oder verwenden, die die Vertrauenswürdigkeit natürlicher Personen auf Grundlage ihres sozialen Verhaltens oder persönlicher Eigenschaften bewerten („social scoring"), wenn diese Bewertung für bestimmte Personen zu Benachteiligung führt [Art. 5 (1) (c)], nämlich
  - in sozialen Kontexten, die in keinem Zusammenhang stehen zu den Umständen, unter denen die Daten ursprünglich erzeugt oder erfasst wurden, oder
  - in einer Weise, die im Hinblick auf das soziale Verhalten der Person oder dessen Tragweite ungerechtfertigt oder unverhältnismäßig ist.

3 Biometrische Echtzeit-Fernidentifizierungssysteme

- Ein biometrisches Echtzeit-Fernidentifizierungssystem ist ein KI-System, das Personen aus der Ferne anhand von biometrischen Daten ohne erhebliche Verzögerung identifizieren kann, ohne dass der Nutzer des KI-Systems vorher weiß, ob die Person im Anwendungsbereich des KI-Systems anwesend sein wird, z.B. die Echtzeit-Identifizierung von Personen auf videoüberwachten öffentlichen Plätzen [Art. 3 (33) (36), (37)].

- Die Verwendung biometrischer Echtzeit-Fernidentifizierungssysteme in öffentlich zugänglichen Räumen zu Strafverfolgungszwecken – für andere Zwecke gilt die Datenschutzgrundverordnung – ist nur zulässig, wenn sie unbedingt erforderlich ist [Art. (5) (1) (d)]
  - zur gezielten Suche nach bestimmten potenziellen Opfern von Straftaten oder nach vermissten Kindern,
  - zur Abwendung einer konkreten, erheblichen und unmittelbaren Gefahr für das Leben oder die körperliche Unversehrtheit von Personen oder eines Terroranschlags oder
  - zum Erkennen, Aufspüren, Identifizieren oder Verfolgen eines Täters oder Verdächtigen einer Straftat, wenn
    - für die Straftat ein Europäischer Haftbefehl, unabhängig von der Strafbarkeit der Tat im Vollstreckungsmitgliedstaat, ausgestellt werden kann – z.B. bei Vergewaltigung, Drogenhandel und Geldfälschung – und
    - die Höchstfreiheitsstrafe für die Straftat in dem Mitgliedstaat, der das biometrische Echtzeit-Feinidentifizierungssystem einsetzt, mindestens drei Jahre beträgt.

- Der Einsatz biometrischer Echtzeit-Fernidentifizierungssysteme muss
  - im nationalen Recht vorgesehen sein [Art. 5 (4)] und
  - von einer Justizbehörde oder unabhängigen Verwaltungsbehörde genehmigt werden, was in dringenden Fällen auch nachträglich möglich ist [Art. 5 (3)].

4 Hochrisiko KI-Systeme

4.1 Definition

- Als Hochrisiko-KI-System gilt ein KI-System, das
  - ein Produkt oder eine Sicherheitskomponente eines Produkts ist, das von bestehenden EU-Gesundheits- und Sicherheitsharmonisierungsregeln erfasst ist und nach diesen Regeln einer Konformitätsbewertung durch Dritte unterliegt, z.B. Medizinprodukte, Aufzüge und Spielzeuge [Art. 6 (1), Anhang II], oder
  - in einem der folgenden Bereiche eingesetzt wird [Art. 6 (2), Anhang III]:
    - biometrische Identifizierung und Kategorisierung von Personen: Anwendungsfeld ist die biometrische Fernidentifizierung;
    - Verwaltung und Betrieb kritischer Infrastrukturen: Anwendungsfeld ist die Verwendung als Sicherheitskomponenten im Straßenverkehr sowie in der Wasser-, Gas-, Wärme- und Stromversorgung;
    - Bildung: Anwendungsfeld ist insbesondere die Entscheidung über den Zugang oder die Zuweisung von Personen zu Bildungseinrichtungen sowie die Bewertung von Schülern und Teilnehmern an Zugangstests;
    - Beschäftigung, Personalmanagement und Zugang zur Selbstständigkeit: Anwendungsfeld ist insbesondere die Bewertung von Bewerbern in Vorstellungsgesprächen;
    - Zugänglichkeit und Inanspruchnahme grundlegender privater und öffentlicher Dienste und Leistungen: Anwendungsfeld ist insbesondere die Kreditwürdigkeitsprüfung;
    - Strafverfolgung: Anwendungsfeld ist insbesondere die Prognose, ob eine Person erneut Straftaten begehen wird;
    - Migration, Asyl und Grenzkontrolle: Anwendungsfeld ist insbesondere die Prüfung der Echtheit von Dokumenten;
    - Rechtspflege und demokratische Prozesse: Anwendungsfeld ist die Unterstützung von Justizbehörden bei der Ermittlung und Auslegung von Sachverhalten und Rechtsvorschriften sowie bei der Anwendung des Rechts.

- Die Kommission kann mit delegierten Rechtsakten neue Anwendungsfelder innerhalb der aufgelisteten Bereiche hinzufügen, wenn diese ein Gesundheits-, Sicherheits- oder Grundrechtsrisiko darstellen, das in Schwere und Wahrscheinlichkeit des Schadens den Risiken in den bereits aufgelisteten Feldern entspricht. Dabei berücksichtigt die Kommission insbesondere die Zweckbestimmung des KI-Systems, die zu erwartenden Schäden sowie die Abhängigkeit der Nutzer vom KI-Systemen und deren Schutzbedürftigkeit. [Art. 7 (1) (2)].

4.2 Anforderungen an Hochrisiko-KI-Systeme

- Anbieter müssen gewährleisten, dass Hochrisiko-KI-Systeme die folgenden Anforderungen erfüllen: Sie müssen
  - mit repräsentativen, fehlerfreien und vollständigen Datensätzen entwickelt werden [Art. 10 (1), (3)];
  - hinreichend transparent sein, damit Nutzer die Ergebnisse des Hochrisiko-KIS angemessen interpretieren und verwenden können [Art. 13 (1);
  - im Hinblick auf ihre Zweckbestimmung hinreichend genau, robust und cybersicher sein [Art. 15 (1)];
  - während des Betriebs automatisch Vorgänge und Ereignisse protokollieren [Art. 12 (1)] und
  - von Personen beaufsichtigt werden können, sodass diese den Betrieb des Hochrisiko-KI-Systems überwachen und stoppen sowie dessen Ergebnis außer Kraft setzen können [Art. 14 (1), (4)].

4.3 Pflichten für Anbieter von Hochrisiko-KI-Systemen

4.3.1 Prüf- und Sorgfaltspflichten

- Vor Inverkehrbringen von Hochrisiko-KI-Systemen ist eine Konformitätsbewertung durchzuführen [Art. 16 (a) und Art. 19 (1)].
  - Bei einem KI-System zur biometrischen Fernidentifizierung kann der Anbieter die Konformitätsbewertung [Art. 43 (1)]
    - unter Beteiligung einer „notifizierten Stelle“ durchführen oder
    - selbst durchführen, sofern das KI-System einer im EU-Amtsblatt veröffentlichten harmonisierten Norm entspricht.
  - Bei einem KI-System, das ein Produkt oder Sicherheitskomponente eines Produkts ist, das von bestehenden EU-Gesundheits- und Sicherheitsharmonisierungsregeln erfasst ist und nach diesen Regeln einer

Konformitätsbewertung durch Dritte unterliegt, erfolgt die Konformitätsbewertung durch diese Dritten [Art. 43 (3)].
  - Bei allen anderen KI-Systemen erfolgt die Konformitätsbewertung durch den Anbieter selbst [Art. 43 (2)].

  Wenn ein KI-System einer im EU-Amtsblatt veröffentlichten harmonisierten Norm entspricht, wird die Konformität mit den Anforderungen an Hochrisiko-KI-Systeme vermutet [Art. 40].

- Anbieter müssen vor Inverkehrbringen eines Hochrisiko-KI-Systems ein Risikomanagementsystem einrichten, das während dessen gesamten Lebenszyklus die Risiken ermittelt [Art. 9 (1)].
  - Die Risikoermittlung erfolgt durch Tests und ein System zur Beobachtung nach dem Inverkehrbringen [Art. 9 (4) und Art. 61 (1), (2)].
  - Ggf. müssen Risikomanagementmaßnahmen ergriffen werden, damit das Risiko des Systems „vertretbar" ist [Art. 9 (4)].
- Anbieter müssen eine technische Dokumentation erstellen und auf dem neuesten Stand halten, die belegt, dass ihre Systeme die Anforderungen an Hochrisiko-KI-Systeme erfüllen [Art. 11 (1) und Art. 18].
- Anbieter müssen Gebrauchsanweisungen bereitstellen, die insbesondere Informationen zu den Merkmalen, Fähigkeiten und Leistungsgrenzen ihrer Systeme beinhalten [Art. 13 (2), (3)].
- Anbieter müssen ein Qualitätsmanagementsystem einrichten, das die Einhaltung der KI-Verordnung gewährleistet [Art. 17 (1)].

4.3.2 Meldepflichten

- Anbieter müssen schwerwiegende Vorfälle oder Fehlfunktionen der Aufsichtsbehörde melden [Art. 3 (44) und Art. 62 (1)].
  - Schwerwiegende Vorfälle sind Vorkommnisse, die zur Folge haben können:
    - den Tod oder schwere gesundheitliche Schäden einer Person,
    - schwere Sach- oder Umweltschäden oder
    - eine schwere und unumkehrbare Störung kritischer Infrastruktur.
  - Fehlfunktionen sind Vorkommnisse, die einen Verstoß gegen EU-Recht zum Schutz der Grundrechte darstellen.

5 Risikounabhängige Transparenzpflichten

- Bei KI-Systemen, die für die Interaktion mit natürlichen Personen bestimmt sind, müssen die Anbieter sicherstellen, dass Personen, die mit dem KI-System interagieren, darüber informiert werden, sofern dies nicht offensichtlich ist [Art. 52 (1)].
- Bei KI-Systemen zur Emotionserkennung oder zur biometrischen Kategorisierung – dies sind Systeme, die Personen Kategorien wie Alter, Geschlecht, ethnische Herkunft, sexuelle oder politische Orientierung zuordnen – müssen die Nutzer die erfassten Personen über den Betrieb des Systems informieren [Art. 52 (2)].
- Nutzer von „Deepfake"-KI-Systemen, die Bild-, Ton- oder Videoinhalte so manipulieren, dass sie wirklichen Personen, Gegenständen und Orten merklich ähneln und fälschlicherweise als echt erscheinen, müssen angeben, dass die Inhalte künstlich erzeugt oder manipuliert wurden [Art. 52 (3)].

6 Verhaltenskodizes

- Kommission und Mitgliedstaaten fördern und erleichtern die Aufstellung von Verhaltenskodizes durch Anbieter von KI-Systemen und/oder deren Interessenvertretungen; die Kodizes sollen erreichen, dass [Art. 69]
  - die Anforderungen an Hochrisiko-KI-Systeme auch auf andere KI-Systeme angewandt werden oder
  - dass Anbieter von KI-Systemen freiwillig Anforderungen erfüllen, die über jene der Verordnung hinausgehen, z.B. an Nachhaltigkeit oder Barrierefreiheit.

7 Durchsetzung und Aufsicht

- Die Mitgliedstaaten benennen eine unabhängige Behörde („Marktüberwachungsbehörde"), die KI-Systeme gemäß der Marktüberwachungsverordnung [VO (EU) 2019/1020] überwacht [Art. 3 (26) und Art. 59 (2)].
  - Die Marktüberwachungsbehörden überwachen, ob KI-Systeme und ihre Verwendung den Anforderungen der Verordnung entsprechen.
  - Die Marktüberwachungsbehörden erhalten – auch aus der Distanz – uneingeschränkten Zugang
    - zu den von den Anbietern genutzten Trainings-, Validierungs- und Testdatensätzen [Art. 64 (1)] sowie
    - auf begründetes Verlangen zu Quellcodes [Art. 64 (2)].

- Wenn ein KI-System den Anforderungen der Verordnung entspricht, aber dennoch ein Risiko für die Gesundheit oder Sicherheit von Personen oder andere Aspekte des öffentlichen Interesses darstellt, fordert die Marktüberwachungsbehörde den Anbieter des KI-Systems oder einen anderen beteiligten Akteur auf, alle geeigneten Maßnahmen zu treffen, um das Risiko zu beseitigen oder das KI-System vom Markt zu nehmen oder es zurückzurufen [Art. 67 (1)].
- Die Marktüberwachungsbehörde berichtet der Kommission regelmäßig über die Ergebnisse ihrer Marktüberwachungstätigkeiten [Art. 63 (2)].
- Ein „Europäischer Ausschuss für künstliche Intelligenz" – bestehend aus den nationalen Marktüberwachungsbehörden und dem Europäischen Datenschutzbeauftragten [Art. 57 (1)] – wird eingerichtet. Er unterstützt die Kommission und die nationalen Marktüberwachungsbehörden insbesondere bei [Art. 56]:
  - der Zusammenarbeit miteinander,
  - der einheitlichen Anwendung der Verordnung in der EU und
  - Analysen zu neu auftretenden Fragen im Anwendungsbereich der Verordnung.
- Die Kommission hat den Vorsitz im Ausschuss, beruft dessen Sitzungen ein und bereitet die Tagesordnung vor [Art. 57 (3)].

8 Sanktionen

- Geldbußen bis zu 30 Mio. Euro oder bis zu 6 % des weltweiten Jahresumsatzes – bei Organen, Einrichtungen und sonstigen Stellen der EU bis zu 500.000 Euro – drohen [Art. 71 (3), Art. 72 (2)]
  - beim Einsatz von verbotenen KI-Systemen,
  - beim unzulässigen Einsatz von biometrischen Echtzeit-Fernidentifizierungssystemen und
  - beim Einsatz eines Hochrisiko-KI-Systems, das mit Datensätzen entwickelt wurde, die nicht den Anforderungen der Verordnung entsprechen.
- Geldbußen bis zu 10 Mio. Euro oder bis zu 2 % des weltweiten Jahresumsatzes drohen bei falschen, unvollständigen oder irreführenden Angaben gegenüber notifizierten Stellen oder zuständigen nationalen Behörden [Art. 71 (5)].
- Geldbußen bis zu 20 Mio. Euro oder bis zu 4 % des weltweiten Jahresumsatzes – bei Organen, Einrichtungen und sonstigen Stellen der Union bis zu 250.000 Euro – drohen bei sonstigen Verstößen gegen die Verordnung [Art. 71 (4), Art. 72 (3)].

B. Juristischer und politischer Kontext

1 Stand der Gesetzgebung

21.4.21	Annahme durch Kommission
22.9.21	Stellungnahme Europäischer Wirtschafts- und Sozialausschuss
Offen	Annahme durch Europäisches Parlament und Rat, Veröffentlichung im Amtsblatt, Inkrafttreten

2 Politische Einflussmöglichkeiten

Generaldirektionen:	GD Kommunikationsnetze, Inhalte und Technologien
Ausschüsse des Europäischen Parlaments:	Binnenmarkt und LIBE, Berichterstatter Binnenmarkt: Brando Benifei (S&D-Fraktion, IT); Berichterstatter LIBE: Dragoș Tudorache (Renew, RO)
Bundesministerien:	Wirtschaft (federführend)
Ausschüsse des Deutschen Bundestags:	Wirtschaft (federführend)
Entscheidungsmodus im Rat:	Qualifizierte Mehrheit (Annahme durch 55% der Mitgliedstaaten, die 65% der EU-Bevölkerung ausmachen)

3 Formalien

Kompetenznorm:	Art. 16 AEUV (Datenschutz), Art. 114 AEUV (Binnenmarkt)
Art der Gesetzgebungszuständigkeit:	Geteilte Zuständigkeit (Art. 4 Abs. 2 AEUV)
Verfahrensart:	Art. 294 AEUV (ordentliches Gesetzgebungsverfahren)

C. Bewertung

1 Ökonomische Folgenabschätzung

Die Verordnung benachteiligt KI-Systeme gegenüber anderen Technologien, insbesondere bereits etablierten Technologien, regulatorisch. Regulierung sollte jedoch technologieneutral sein. Statt KI-Systeme zu regulieren, sollte die Kommission ihre Regulierung auf die gewünschten Regulierungsziele ausrichten. So ist nicht nachvollziehbar, weshalb social scoring nur dann verboten werden sollte, wenn ein KI-System verwendet wird. Vielmehr sollte verboten werden, dass Maschinen Entscheidungen treffen, die erhebliche Auswirkungen auf die Rechte einer Person oder eines Unternehmens haben, wenn die Entscheidung nicht von einem Menschen korrigiert werden kann, etwa weil die Entscheidungslogik aufgrund ihrer Komplexität nicht durch einen Menschen überprüft werden kann (vgl. cep**Analyse** 4/2020).

Die Definition von KI-Systemen der Verordnung ist zu weit: Sie erfasst zahlreiche Softwareanwendungen, die seit vielen Jahren genutzt werden und nicht „intelligent", sondern logik-basiert sind. Die Definition sollte vielmehr berücksichtigen, ob ein System autonom lernt und Entscheidungen fällt.

Die Verordnung schafft gleiche Wettbewerbsbedingungen zwischen EU- und Nicht-EU-Anbietern, weil sie auch für nicht in der EU ansässige Anbieter von KI-Systemen gilt. Zudem verhindert sie, dass die Regelungen der Verordnung umgangen werden, indem KI-Systeme in Drittstaaten eingesetzt und die Ergebnisse anschließend in der EU genutzt werden.

Spezifiziert werden muss, was unter „unterschwelliger" Beeinflussung zu verstehen ist. Ferner muss definiert werden, wann ein „physischer oder psychischer Schaden" vorliegt. In der vorliegenden Formulierung könnte etwa jede Art von KI-gestützten Werbeanzeigen erfasst sein, sofern sie eine Person beeinflusst, etwas zu tun, das sie später vielleicht bereut.

Die besonders strengen Vorgaben für Hochrisiko-KI-Systeme sind sachgerecht, da von diesen KI-Systemen eine höhere Gefahr ausgeht. Die Beschränkung auf konkrete Anwendungsfelder in acht besonders riskanten Bereichen verringert die Kosten für die Nutzung von KI-Systemen in den restlichen Bereichen. Denn viele KI-Systeme werden sowohl in besonders riskanten als auch in weniger riskanten Bereichen eingesetzt.

Die Verpflichtung für Anbieter, Fehlerfreiheit und Vollständigkeit der Datensätze für die Entwicklung von KI zu garantieren, ist nicht erfüllbar. Wenn etwa ein KI-System mit den Angestelltendaten eines Unternehmens trainiert wird, werden diese Datensätze nie vollständig sein, da immer neues Personal eingestellt wird. Die Entscheidungen des KI-Systems werden daher mit der Zeit immer besser werden.

Zudem muss geklärt werden, wie Anbieter Transparenz schaffen können, damit die Nutzer die Ergebnisse ihrer KI-Systeme interpretieren können. So sind die logischen Schlüsse, die KI-Systeme nutzen, um Ergebnisse zu erzielen, selbst den Anbietern oft nicht bekannt. Gleiches gilt für die Anforderung, genau und robust zu sein. Diese Vorgaben müssen, etwa durch Standards, spezifiziert werden.

Konformitätsprüfungen von Hochrisiko-KI-Systemen durch die Anbieter selbst sind verfehlt. Vielmehr sollten solche Prüfungen immer durch unabhängige Dritte erfolgen, um die Gefahr oberflächlicher Prüfungen zu minimieren.

Für Anbieter eines Hochrisiko-KI-Systems wird es nicht immer möglich sein, ein Risikomanagementsystem einzurichten, mit dem sich die Risiken ihrer KI-Systeme über den gesamten Lebenszyklus umfassend ermitteln lassen, da sie hierfür auf Informationen, insbesondere Daten, der Nutzer angewiesen sind. Zudem ist das für Hochrisiko-KI-Systeme, die sich nach dem Inverkehrbringen nicht mehr verändern, auch nicht notwendig. Die Verordnung sollte daher unterscheiden zwischen Hochrisiko-KI-Systemen, die sich nach dem Inverkehrbringen nicht mehr verändern, und solchen, die im Einsatz stetig weiter lernen, etwa durch Daten, die sie generieren. Letztere benötigen eine strengere Regulierung als erstere. Auch zur Erfüllung der Pflicht, eine technische Dokumentation auf dem aktuellsten Stand zu halten, sind die Anbieter auf Informationen der Nutzer angewiesen.

Die vorgeschlagenen risikounabhängigen Transparenzpflichten erhöhen die Akzeptanz der Bevölkerung für KI. Allerdings sollte ergänzt werden, dass natürliche Personen *vor* – und nicht erst bei oder nach – der Interaktion mit KI-Systemen darüber informiert werden müssen. Gleiches gilt für durch Deepfake-Systeme bearbeitete Inhalte.

Dass die Marktüberwachungsbehörden uneingeschränkten Zugang zu Datensätzen bekommen, erleichtert einerseits die Marktüberwachung. Für Anbieter von KI-Systemen ist diese Pflicht jedoch nicht immer erfüllbar, da Datensätze häufig nicht oder nur kurz gespeichert werden, etwa wenn es sich um personenbezogene Daten handelt. Daher muss geklärt werden, wie die Pflicht, Zugang zu Daten zu gewähren, mit den Anforderungen der Datenschutzgrundverordnung in Einklang gebracht werden kann. Quellcodes sind in der Regel ein wesentliches Geschäftsgeheimnis von Unternehmen. Behörden sollten Zugriff auf Quellcodes daher nur als ultima ratio erhalten. Die Pflicht, Zugang auch aus der Distanz zu gewähren, birgt ein hohes Sicherheitsrisiko.

2 Juristische Bewertung

2.1 Kompetenz

Die Verordnung wird zu Recht auf eine doppelte Rechtsgrundlage gestützt: Für den Großteil der Vorschriften ist die Binnenmarktharmonisierungskompetenz [Art. 114 AEUV] die richtige Rechtsgrundlage. Die Vorschriften zum Einsatz biometrischer Echtzeit-Fernidentifizierungssysteme zu Strafverfolgungszwecken lassen sich hingegen nicht auf diese Kompetenz stützen. Hierfür ist die Datenschutzkompetenz [Art. 16 AEUV] die richtige Rechtsgrundlage.

2.2 Subsidiarität

Unproblematisch.

2.3 Verhältnismäßigkeit gegenüber den Mitgliedstaaten

Der Europäische Ausschuss für künstliche Intelligenz sollte aufgewertet und dadurch die Rolle der nationalen Aufsichtsbehörden in der Durchsetzung der Verordnung gegenüber der Kommission gestärkt werden. Der Ausschuss sollte nicht nur Hilfsorgan der Kommission sein, sondern aus eigener Initiative tätig werden können. Zudem sollte er analog zum „unabhängigen Europäischen Gremium für digitale Dienste" im Vorschlag für den Digital Services Act (s. cep**Analyse** 24/2021) gestaltet werden. Dann könnte er Empfehlungen erlassen, denen die nationalen Behörden entweder folgen oder die Abweichung von der Empfehlung erklären müssen.

2.4 Sonstige Vereinbarkeit mit EU-Recht

Die Befugnisse der Kommission, die Liste der unter die Verordnungen fallenden KI-Techniken und -Konzepte sowie die Anwendungsfelder von Hochrisiko-KI-System mit delegierten Rechtsakten zu ändern, sind zwar weitreichend, halten sich aber im Rahmen der Vorschriften für delegierte Rechtsakte [Art. 290 AEUV], denn sie sind hinreichend determiniert. Insbesondere gibt die Verordnung nicht nur vor, dass das Risiko neuer Anwendungsfelder dem der bereits enthaltenen Anwendungsfelder entsprechen muss. Vielmehr regelt sie auch, nach welchen Kriterien der Risikovergleich vorzunehmen ist. Außerdem bestünde angesichts der raschen technischen Entwicklung der KI die Gefahr, dass Änderungen der Verordnung im normalen Gesetzgebungsverfahren zu lange dauern.
Die Verwendung biometrischer Fernidentifizierungssysteme zu Strafverfolgungszwecken greift in das Recht auf Datenschutz [Art. 8 GRC] ein. Die Verordnung schränkt deren Nutzung daher zu Recht ein. Sie schützt das Recht auf Datenschutz jedoch nicht hinreichend. So macht es für die erfassten Personen keinen wesentlichen Unterschied, ob sie in Echtzeit oder mit zeitlichem Abstand von z. B. 24 Stunden identifiziert werden. Die Verordnung greift daher zu kurz. Sie sollte auf die Zeitdauer und den Grund der Erfassung abstellen und untersagen, dass der Einsatz kontinuierlich oder über einen längeren Zeitraum und ohne Beschränkung auf ein bestimmtes Ereignis in der Vergangenheit – z. B. ein von einer Videokamera aufgezeichnetes Verbrechen – erfolgt.
Die Verwendung von KI-Systemen zur Emotionserkennung oder biometrischen Kategorisierung stellt einen gravierenden Eingriff in das Recht auf Achtung des Privatlebens [Art. 7 GRC] und das Recht auf Datenschutz [Art. 8 GRC] dar und muss daher strengeren Anforderungen als einer bloßen Informationspflicht unterliegen. Vergleichbar mit den Regeln für KI-Systeme zur biometrischen Fernidentifizierung und den Vorschriften der DSGVO zur Verarbeitung biometrischer Daten zum Zweck der Identifizierung sollte die Verordnung abschließend aufzählen, zu welchen Zwecken die Verwendung von KI-Systemen zur Emotionserkennung oder biometrischen Kategorisierung zulässig ist. Bei solchen KI-Systemen ist außerdem besonders rigoros zu prüfen, ob sie zuverlässig zutreffende Ergebnisse hervorbringen. Denn grundsätzlich ist fraglich, wie gut sich z. B. die politische oder sexuelle Orientierung anhand äußerer Merkmale erkennen lassen. Nur wenn dies zu bejahen ist, sollten solche KI-Systeme zu den abschließend genannten Zwecken eingesetzt werden dürfen.
Die Regeln zu „social scoring"-Systemen dürfen nicht nur für Behörden, sondern müssen auch für private Anbieter gelten. Denn auch diese – z. B. soziale Medien und Anbieter von Cloud-Diensten – können große Mengen von personenbezogenen Daten sammeln und darauf basierend ein social scoring durchführen. Dies sollte nur zugelassen werden, wenn die Betroffenen darüber transparent – also nicht mit in AGB versteckten Hinweisen – informiert wurden und wirksam zugestimmt haben. Außerdem muss sichergestellt sein, dass niemand auf die Ergebnisse eines von Dritten ermittelten social scoring zugreifen und dadurch das Nutzungsverbot umgehen können.
Die vorgesehenen Geldbußen von bis zu 30 Mio. Euro oder 6% des weltweiten Jahresumsatzes sind unangemessen hoch. Zwar sind Strafdrohungen notwendig, die auch gegenüber Großkonzernen abschreckende Wirkung entfalten. Die Strafdrohungen der KI-Verordnung übersteigen aber die in anderen EU-Rechtsakten üblichen Sätze. Sie sind z. B. um 50% höher als die Strafdrohungen der DSGVO. Ein Grund hierfür ist nicht ersichtlich. Angesichts der unbestimmten Rechtsbegriffe, die erst noch gerichtlich bestimmt werden müssen, besteht die Gefahr, dass die drohenden Strafen vor allem kleine Unternehmen von der Entwicklung von KI-Systemen abhalten. Dies gilt umso mehr, als die KI-Technologie sich rasant weiterentwickelt, sodass kontinuierlich neue Rechtsfragen entstehen werden.