DeutscherAnwaltVerein

Stellungnahme

des Deutschen Anwaltvereins durch den Ausschuss Informationsrecht

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)

Berlin/Brüssel, im Juli 2021

Mitglieder des Ausschusses Informationsrecht

- Rechtsanwalt Dr. Helmut Redeker (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-Geschäftsführung

- Rechtsanwältin Nicole Narewski, Berlin

Ansprechpartnerin in Brüssel

- Hannah Adzakpa, LL.M.

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
1000 Brüssel, Belgien
Tel.: +32 2 28028-12
Fax: +32 2 28028-13
E-Mail: bruessel@eu.anwaltverein.de
Transparenz-Registernummer:
87980341522-66

www.anwaltverein.de

Der Deutsche Anwaltverein (DAV) ist der freiwillige Zusammenschluss der deutschen Rechtsanwältinnen und Rechtsanwälte. Der DAV versammelt mehr als 62.000 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.

Diese Stellungnahme beschränkt sich auf einige Punkte aus Sicht des Informationsrechtsausschusses und geht u.a. nicht auf Fragen der Rechtsstaatlichkeit oder Auswirkungen auf die juristischen Berufe ein. Diesbezüglich wird auf die ausführliche DAV-Stellungnahme Nr. 40/2020 zum Weißbuch der EU-Kommission verwiesen.

1. Grundsätzlicher Ansatz der Regulierung

Der grundsätzliche Ansatz der Regulierung in Form einer horizontalen Regulierung ist zu begrüßen. Soweit Art. 2 Abs. 2 des Vorschlags der EU-Kommission für eine Verordnung zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz (im Folgenden abgekürzt KI-VO-E) allerdings unter Verweis auf entsprechende Verordnungen die Fahrzeug- und Luftfahrtindustrie von der Regulierung praktisch vollständig ausnimmt, ist dieses mit Blick auf diese besonders komplexen Bereiche zwar für einen gewissen Zeitraum tolerabel; es sollte jedoch, wie von der Kommission angedacht, auch in diesen Bereichen zeitnah eine entsprechende Regulierung erfolgen. Und dabei ergibt es Sinn, ein System zu schaffen, welches sowohl die im derzeitigen Entwurf erfassten KI-Systeme wie auch die in den besagten Industrien mehr oder minder gleichbehandelt. Denn eine Abgrenzung dürfte zum einen bei KI-Systemen, die in verschiedenen Industrien zum Einsatz kommen, zu zusätzlichem Problem- und Administrationsaufwand führen. Zum anderen wird es auch immer wieder Systeme geben, die im Grau- bzw. Grenzbereich dieser Ausnahme liegen. Man denke an Verkehrsinfrastruktursysteme, die mit Fahrzeugen kommunizieren.

Die Grundpfeiler des KI-VO-E für hochriskante KI-Systeme (dazu unter 3.) 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),
- 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 auch noch 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.

Allerdings ist kritisch zu hinterfragen, ob nicht die in Art. 29 Abs. 4 KI-VO-E geforderten Monitoring-, also Überwachungspflichten des Nutzers über ihr Ziel hinausschießen. Das Monitoring/die Überwachung von Systemen dürfte regelmäßig dem eigentlich innovativen autonomen Verhalten der Systeme entgegenstehen. Hier ist zum einen

über eine sachliche - aber auch möglicherweise über eine zeitliche - Beschränkung nachzudenken. Das gilt insbesondere, wenn KI-Systeme mutmaßlich nach einer bestimmten Zeit nicht weiter trainiert werden bzw. ggf. nicht mehr selbst lernen. Jedenfalls in diesen Fällen, tendenziell je nach Gefahr auch zuvor, sollte sodann eine Beobachtungspflicht ausreichend sein.

2. Gegenstand und Reichweite der Regulatorik

Die KI-Systeme sind in Art. 3 Nr. 1 KI-VO-E legal definiert. Die Regelung erscheint einerseits 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 künftig kann nicht ausgeschlossen werden, dass auch die KI selbst Ziele definiert, zumindest dann, wenn sie sich einer sogenannten „starken“ KI annähert. Dieser Bereich muss erst recht reguliert werden. Während insofern eine Nachbesserung allerdings in Ansehung der Unsicherheit über den Durchbruch „starker“ KI nicht dringlich ist, besteht unmittelbarer Nachbesserungsbedarf mit Blick auf den Annex I des Entwurfs, welcher die regulierten Systeme sehr weit fasst und hierunter insbesondere auch normale Expertensysteme sowie Such- und Optimierungsmethoden fasst. Zu prüfen ist allgemein, ob als KI mittels des Annex I nur solche Systeme definiert werden, deren Entscheidungen bzw. deren Verhalten (als mit zumutbaren Mitteln) praktisch unvorhersehbar anzusehen sind.

Auf diesem Wege würden man im Zweifel ohne Not zahlreiche bereits bestehende IT-Systeme bzw. Softwarelösungen der umfangreichen, von der Kommission geplanten Regulierung für KI-Systeme unterwerfen. Dieser Mehraufwand erscheint in Ansehung der Tatsache, dass diese sich bisher nicht als besonders gefährlich erwiesen haben, problematisch, da administrativ überbürdend.

Soweit dann nach der KI-VO-E ein Fall künstlicher Intelligenz vorliegt, unterscheidet diese zwar zu Recht verschiedene Stufen der KI; die im Grundsatz vorgesehene Dreistufigkeit erscheint jedoch teils etwas willkürlich:

- So finden sich in Art. 5 KI-VO-E *intolerable und verbotene KI-Systeme*, 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 auch durchaus problematisch, so

dass gegen deren Auflistung im Grundsatz nichts einzuwenden ist. Was allerdings fehlt, ist eine Regelung, welche eine gewisse Guidance für oder gegen das Verbot entsprechender KI 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.

- Auch 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 dabei wirklich auf solche beschränkt werden sollten, bei denen eine Konformitätsprüfung durch Dritte erforderlich ist, sollte kritisch hinterfragt werden. Immerhin dürfte die insofern in Annex II aufgeführte EU-Gesetzgebung hier ein deutlicher Fingerzeig für ein höheres Gefahrenpotenzial sein.
- Vor diesem Hintergrund ist es allerdings auch verständlich, dass Abs. 2 des Art. 6 KI-VO-E die Möglichkeit zur Klassifizierung an das hochriskante KI-System und damit zu regulierende KI-System durch Annex III erweitert. Zwar ist auch hier ähnlich wie bei Art. 5 KI-VO-E ersichtlich, dass es der EU-Kommission vor allem um die Regulierung grund- bzw. menschenrechtsrelevanter KI-Systeme geht. Auch hier gilt aber, dass die Abgrenzung in Ansehung der Liste des Annex III teils willkürlich erscheint und damit auch mit Blick auf die Erweiterungsmöglichkeiten des Annex III nach Art. 7 KI-VO-E anfällig für politische Einflussnahmen durch Lobbyisten ist. 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.
- Schließlich findet sich in Art. 69 KI-VO-E eine Regelung für *sonstige* KI-Systeme, welche mit Ausnahme der Regelung in Art. 52 KI-VO-E unreguliert bzw. der Selbstregulierung überlassen bleiben sollen. Da es sich um ein junges Feld der Regulierung handelt, ist nachvollziehbar, dass nicht sämtliche Systeme ohne weiteres reguliert werden sollen. Auch spricht der bereits angesprochene starke Formalismus und der erhöhte Dokumentations- und Administrationsaufwand der Regulierung dafür, dass derartige Systeme zumindest vorerst unreguliert bleiben sollten. Andererseits sollte nicht verkannt werden, dass auch auf diese die Regulierung Auswirkungen hat (vgl. dazu unten unter 7.). Und schließlich fragt

sich auch, ob nicht die Gesamtregulierung auch auf diese Gruppen ausgedehnt werden sollte. Sie denkt ja stark in den Kategorien von Risiken und Nutzen und kommt daher bei dieser Gruppe von Systemen automatisch zu niedrigeren Anforderungen. Die Ausdehnung der Regulatorik hätte also keine dramatischen Folgen. Ermöglicht würden dann fließende Übergänge. – Das Datenschutzrecht etwa unterscheidet für seine Anwendbarkeit ja auch nicht zwischen datenschutzrechtlich unterschiedlich riskanten Verarbeitungen, reguliert also nicht nur hochriskante Verarbeitungen, sondern siehe allenfalls zusätzliche gesetzlichen Anforderungen vor. – Schließlich gilt im Übrigen auch hier wieder, dass KI-Systeme naturgemäß teils bei gleicher Technologie bzw. gleichen Systemen je nach Anwendungsgebiet sodann reguliert oder eben unreguliert wären. Abgrenzungsschwierigkeiten liegen dabei auf der Hand.

3. Umfang und Aufbau des Verordnungsentwurfs / Regelungstechnik

Die Gesamtverordnung erscheint auf den ersten Blick sehr lang und in ihrer Struktur durchaus komplex. Dieses dürfte zu gewissen Anwendungsschwierigkeiten und u.U. auch zu Rechtsunsicherheiten führen:

- So ist etwa für den Leser nicht ohne weiteres ersichtlich, welche Anforderungen des Kapitel 2 den Anbieter in welcher Form treffen, bzw. warum dieses eigentlich separat von den Anbieterpflichten in Kapitel 3 geregelt ist, der sodann zum einen pauschal (Art. 16 lit. a KI-VO-E) und zum anderen wiederholt konkret (so etwa in Art. 17 Abs. 1 lit. e und f KI-VO-E) auf das Kapitel 2 zurückverweist.
- Problematisch erscheinen auch die vielen redundanten Regelungen, die zu Normwidersprüchen führen könnten (z. B. Art. 16 lit. g und Art. 21 KI-VO-E).
- Auch 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.

Abschließend ist zu monieren, dass die Regelungen von äußerst unterschiedlicher Regelungstiefe sind. Teils werden echte Details, teils nur grobe Linien vorgegeben. Hier sollten die allgemeinen Prinzipien deutlicher herausgearbeitet und mit anderen Prinzipien des europäischen Produktsicherheits-, aber auch des Produkthaftungsrechts abgeglichen werden. Damit würde auch die Rechtssicherheit erhöht.

4. Einzelregelungen und Aspekte

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) KI-VO-E). Der Unterschied überzeugt nicht.
- Weiter kritisch zu hinterfragen ist, dass die biometrischen Identifikationssysteme weitgehend nur verboten sind, wenn sie in Realtime funktionieren (Art. 5 Nr. 1 lit. d) KI-VO-E), sonst aber nur als Hochriskante KI-Systeme zu behandeln sind. Es ist nicht zu erkennen, dass die Gefahren solcher Systeme so unterschiedlich sind, dass sie diese unterschiedliche Behandlung rechtfertigen.
- Auffällig ist, dass in Art. 9 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 (vgl. § 1 Abs. 2 Nr. 5 ProdHaftG; *Hofmann*, CR 2020, 282, 284 f.). Hier sollte in Ansehung der Hoch-Risiko-Systeme einerseits und Bußgelder sowie zur Innovationsförderung anderseits zumindest der Kompromiss gesucht werden, auf den neuesten Stand der Technik abzustellen.
- Nicht realistisch erscheint 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. Gerade mit Blick auf die Vollständigkeit und Fehlerfreiheit scheint dieses unmöglich. Ergänzt werden sollte ein "bestmöglich" oder "im zumutbaren Rahmen". Auch ist zu bedenken, dass mitunter je nach Zweckbestimmung auch schlechte Daten gut sein können. 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 fehlt zu Art.

10 Abs. 3 S. 1 KI-VO-E eine Rückausnahme, die es erlaubt, von diesen Qualitätsanforderungen an Trainings-, Validierungs- und Testdatensätze abzurücken, *soweit* der Schutz anderer Rechtgüter (insb. der Datenschutz) dieses zwingend erfordert.

- Art. 14 Nr. 5 KI-VO-E sieht die Bestätigung einer durch lernende Systeme getroffenen Identifikation von Personen durch zwei Menschen vor, was zumindest dann nicht überzeugt, wenn auch ohne KI nur ein Mensch entscheidet. Oder ist hier intendiert, KI-Vorschläge, die sonst aus Bequemlichkeit übernommen werden könnten, einem Vieraugen-Prinzip zu unterwerfen?
- 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 nationaler 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 müssen Eine Klarstellung wäre sinnvoll.

5. 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. Die dortigen Erlaubnisse (einschl. der Einwilligung) greifen regelmäßig zu kurz; ob die Ergänzung in der DSGVO oder in der KI-VO-E erfolgt, kann dahinstehen. Hintergrund ist, dass Art. 6 Abs. 1 lit. c DSGVO für Daten i.S.v. Art. 9 Abs. 1 DSGVO nicht greift.

Auch die Kollision mit dem Geheimnisschutz sollte nicht nur mit Blick auf Behörden (Art. 70 KI-VO-E) geregelt werden. Zwar werden primär mit diesen Informationen zur Dokumentation und über Störungen ausgetauscht. Es besteht aber gleichwohl die Möglichkeit, dass Dritte diese Informationen einsehen könnten. Hier fragt sich, ob Art. 70 KI-VO-E klar genug vermittelt, ob auch Eventlogs und Trainingsdaten (etwa im

Rahmen zivilrechtlicher Auseinandersetzungen) zur Verfügung gestellt werden dürfen oder ob es sich um nach Abs. 1 lit. a schutzwürdige Daten handelt.

6. Regulatorik und KMUs

Kritisch zu hinterfragen ist, ob die KI-Reallabore (Sandboxes), wie sie in Art. 53 f. KI-VO-E geregelt sind, im Rahmen des verfassungsrechtlich Zulässigen (Gleichberechtigung) ausgeweitet werden sollten, um KMUs die Entwicklung innovativer KI-Systeme und auch deren Erprobung in der Praxis zu ermöglichen. Die umfassende Regulatorik, insbesondere die zahlreichen Dokumentations- und Meldepflichten könnten ein Hemmnis für KMUs, insb. Startups, darstellen, selbst wenn die Pflicht zum Qualitätsmanagement durch Art. 17 Abs. 2 KI-VO-E – wenn auch kaum prognostizierbar – relativiert wird und auch andere Erleichterungen vorgesehen sind (vgl. Art. 3 Nr. 3, Art. 55, 59 Abs. 7, 69 Abs. 4, 71 KI-VO-E). Unklar ist bei Art. 17 Abs. 2 KI-VO-E übrigens, ob es richtig ist, auf den Anbieter bzw. dessen Größe abzustellen oder ob nicht eher der Konzern des Anbieters entscheidend sein sollte. Zu erwägen ist, auch für den Umfang der Regulatorik noch stärker auf die Gefahren der KI-Systeme (auch in quantitativer Hinsicht) abzustellen.

Hier ist zu empfehlen, den Dialog mit entsprechenden Wirtschaftsverbänden zu suchen.

7. Sonstige Konsequenzen

Die KI-VO wird, wenn sie in Kraft tritt direkte Auswirkungen auf das nationale Recht haben. In Deutschland wird sie als Schutzgesetz i.S.v. § 823 Abs. 2 BGB u.a. eine deliktische Haftung begründen können. Auch wird sie im Rahmen des § 823 Abs. 1 BGB Verkehrs(sicherungs)pflichten begründen. Insofern fragt sich, ob nicht einige der Regelungen der KI-VO-E den Akteuren zu weit reichende Pflichten und damit Haftungsrisiken auferlegten. Das gilt insb. für die Pflicht der Nutzer zur Befolgung der Instruktionen nach Art. 29 Abs. 1 KI-VO-E und die Informations- und Überwachungspflichten der Nutzer nach Art 29 Abs. 4 KI-VO-E. Besonders kritisch könnte diese auch mit Blick auf strafrechtliche Fahrlässigkeitsnormen (insb. die fahrlässige Körperverletzung und Tötung) sein, für die die KI-VO-E möglicherweise im Sinne der Konkordanz der Rechtsordnung Sorgfaltsmaßstäbe statuieren würde.

Unbenommen dessen ist es richtig, davon auszugehen, dass die Regelungen die zivilrechtliche Haftung zumindest der Anbieter mit prägen sollten; andernfalls müssten sie sich auf zwei Haftungsmaßstäbe einstellen: einerseits auf einen Maßstab des öffentlichen Sicherheitsrechts und anderseits auf einen zivilrechtlichen Haftungsmaßstab. Dies dürfte unzumutbar sein.