cepAdhoc

11.02.2020

Europäische Strategie zur künstlichen Intelligenz

Eine Bewertung des Entwurfs eines Weißbuchs der EU-Kommission zur KI

Alessandro Gasparotti und Lukas Harta, LL.M.

Mitte Januar wurde der Entwurf eines Weißbuchs der EU-Kommission zur Künstlichen Intelligenz (KI) öffentlich. Er umreißt die Schwächen der aktuellen Gesetzgebung und stellt drei Optionen für die zukünftige Regulierung von KI vor. Das cep bewertet diese Optionen wie folgt:

- **Option 1: Freiwilliges Kennzeichnungssystem (Label).** Diese Option würde die unternehmerische Freiheit respektieren, da Unternehmen selbst entscheiden können, ob sie das Label verwenden möchten. Sie könnte jedoch nicht ausreichen, um z.B. Sicherheits- und Haftungsfragen zu klären.
- **Option 2: Sektorale Anforderungen für Behörden.** Diese Option würde von Behörden verlangen, Informationen über die Effektivität der von ihnen verwendeten KI-Anwendungen zu veröffentlichen. Dies ist sachgerecht, da Behörden mehr Macht haben, in die Grundrechte der Menschen einzugreifen, als private Akteure.
- **Option 3: Obligatorische risikobasierte Anforderungen für risikoreiche KI-Anwendungen.** Diese Option würde nur risikoreiche KI-Anwendungen sowohl im privaten als auch im öffentlichen Sektor regulieren. Ohne eine genaue Definition des Begriffs "risikoreich" haben Unternehmen einen Anreiz, die möglichen Risiken ihrer KI-Anwendung herunterzuspielen, damit ihre Produkte nicht den Standards für risikoreiche KI-Anwendungen entsprechen müssen.

Alessandro Gasparotti und Lukas Harta sind wissenschaftliche Referenten im Fachbereich Binnenmarkt am cep | gasparotti@cep.eu
cep | Kaiser-Joseph-Straße 266 | 79098 Freiburg | Deutschland | Telefon +49 761 38693-107 | www.cep.eu

1 Politischer Kontext

Am 17. Januar 2020 wurde ein Dokumentenentwurf der Europäischen Kommission mit dem Titel „Struktur für das Weißbuch über künstliche Intelligenz – ein europäischer Ansatz“ öffentlich.[1] Die offizielle Veröffentlichung des Weißbuchs ist für den 19. Februar 2020 vorgesehen. Es ist Teil der umfassenderen Strategie der Kommission für künstliche Intelligenz (im Folgenden: „KI“). Sie umfasst die Mitteilung über KI für Europa,[2] den Koordinierten Plan für KI[3] und die Mitteilung über die Schaffung von Vertrauen in eine auf den Menschen ausgerichtete KI[4] (vgl. cep**Analysen** zu Investitionen,[5] zu Bildung und Sozialsystemen,[6] zu Rechtsvorschriften und ethischen Regeln[7] sowie zu den Ethikrichtlinien[8]). In diesem Zusammenhang hat die Präsidentin der Europäischen Kommission Ursula von der Leyen versprochen, in den ersten 100 Tagen ihrer Amtszeit „Rechtsvorschriften mit einem koordinierten europäischen Konzept für die menschlichen und ethischen Aspekte der künstlichen Intelligenz“[9] vorzuschlagen. Darüber hinaus verabschiedete der Ausschuss für Binnenmarkt und Verbraucherschutz des Europäischen Parlaments am 23. Januar 2020 eine Entschließung zu „Automatisierte[n] Entscheidungsfindungsprozesse[n]: Gewährleistung des Verbraucherschutzes und des freien Verkehrs von Waren und Dienstleistungen“.[10] Die Entschließung betont u.a. die Notwendigkeit eines risikobasierten Ansatzes bei der Regulierung von KI. Zudem fordert der Ausschuss die Kommission auf, ein Risikobewertungsschema für KI zu entwickeln, um einen kohärenten Ansatz für die Durchsetzung der Produktsicherheitsvorschriften im Binnenmarkt zu gewährleisten. Schließlich unterstrich Margrethe Vestager, Exekutiv-Vizepräsidentin der Europäischen Kommission für ein Europa für das digitale Zeitalter, in einem Meinungsaustausch mit dem Rechtsausschuss des Europäischen Parlaments am 27. Januar 2020 die Notwendigkeit, hohe Standards für KI in der EU festzulegen, insbesondere hohe Transparenz- und Rechenschaftsstandards für KI-Technologien, die im öffentlichen Sektor eingesetzt werden.[11]

In dem Weißbuch heißt es, dass das Ziel des europäischen Ansatzes darin besteht, „die Entwicklung und Einführung künstlicher Intelligenz in ganz Europa zu fördern und gleichzeitig sicherzustellen, dass die Technologie in einer Art und Weise entwickelt und genutzt wird, die die europäischen Werte und Grundsätze respektiert.“[12] Nach Ansicht der Kommission sind drei Tätigkeitsbereiche von zentraler Bedeutung, um diese Ziele zu erreichen: Investitionen, Zugang zu Daten und KI-Regulierung. Um Investitionen in KI zu fördern, beabsichtigt die Kommission, EU-Mittel einzusetzen, um

- eine „weltweit führende Rechen- und Dateninfrastruktur für künstliche Intelligenz in Europa“ zu schaffen,[13]
- digitale Innovationszentren, die die Akzeptanz von KI verbessern werden, zu stärken und
- den Zugang zu Finanzmitteln für KI-Innovatoren sicherzustellen.

---

1 www.euractiv.com/wp-content/uploads/sites/2/2020/01/AI-white-paper-EURACTIV.pdf.
2 COM(2018) 237.
3 COM(2018) 795.
4 COM(2019) 168.
5 Centrum für Europäische Politik: cep**Analyse** Nr. 10/2019.
6 Centrum für Europäische Politik: cep**Analyse** Nr. 12/2019.
7 Centrum für Europäische Politik: cep**Analyse** Nr. 13/2019.
8 Centrum für Europäische Politik: cep**Analyse** Nr. 16/2019.
9 Von der Leyen: Politische Leitlinien für die künftige Europäische Kommission 2019-2024, verfügbar unter https://ec.europa.eu/commission/sites/beta-political/files/political-guidelines-next-commission_de.pdf S. 16.
10 2019/2915(RSP).
11 https://www.euractiv.com/section/digital/news/eus-vestager-calls-on-public-sector-to-establish-particularly-high-ai-standards/.
12 Europäische Kommission: Entwurf eines Weißbuchs über KI, verfügbar unter www.euractiv.com/wp-content/uploads/sites/2/2020/01/AI-white-paper-EURACTIV.pdf S. 1.
13 Ebd. S. 5.

Es ist zu erwarten, dass die Kommission zu diesem Zweck eine Überprüfung des Koordinierten Plans für KI[14] veröffentlichen wird.

Zudem strebt die Kommission die Entwicklung gemeinsamer europäischer Datenräume an und beabsichtigt, bis Anfang 2021 einen Durchführungsrechtsakt über hochwertige Datensätze des öffentlichen Sektors zu erlassen. Diese Datensätze sollten kostenlos und in maschinenlesbarem Format verfügbar sein. Der Hauptteil des Weißbuchs befasst sich mit dem dritten Tätigkeitsfeld: KI-Regulierung. Daher steht die KI-Regulierung im Mittelpunkt dieses cep**Adhocs**.

2 Der Entwurf des Weißbuchs über KI-Regulierung

2.1 Schwächen in der aktuellen KI-Gesetzgebung

KI bringt viele Möglichkeiten mit sich, z.B. die Durchführung komplexer Aufgaben in einem Bruchteil der Zeit, die ein Mensch benötigt. Aber sie birgt auch Herausforderungen für Sicherheits- und Haftungsanforderungen an Produkte, die mit einer solchen Technologie ausgestattet sind. Die Herausforderungen ergeben sich u.a. aus der Autonomie KI-fähiger Produkte – d.h. wenn KI-fähige Produkte ihre Aufgaben ohne menschliche Aufsicht ausführen – und der Undurchsichtigkeit von KI-Entscheidungen – d.h. wenn der Prozess, der zu einem bestimmten Ergebnis geführt hat, schwierig oder sogar unmöglich zu verstehen ist.

Die Kommission weist im Weißbuch darauf hin, dass es bereits einen soliden Bestand an Rechtsvorschriften auf EU- und nationaler Ebene gibt, die auf KI anwendbar sind.[15] Die beiden wichtigsten EU-Rechtsvorschriften zur Regelung der Sicherheitsanforderungen und des Haftungsregimes für die Verwendung von KI sind die Richtlinie über die allgemeine Produktsicherheit[16] und die Produkthaftungsrichtlinie.[17] Allerdings weist die Kommission auch darauf hin, dass – aufgrund der raschen Entwicklung von KI – die bestehenden Vorschriften möglicherweise nicht alle spezifischen Risiken abdecken, die bei einer weit verbreiteten Nutzung von KI zu erwarten sind. Nach einer ersten Konsultation von Mitgliedstaaten, Unternehmen und anderen Interessengruppen hat die Kommission u.a. die folgenden drei Schwächen in den derzeitigen Rechtsvorschriften identifiziert:

(1) Verschärfung der Risiken aufgrund autonomer Entscheidungen durch KI-fähige Produkte

Die Kommission erwähnt u.a. persönliche Sicherheitsrisiken, Cyber-Bedrohungen und Risiken durch den Verlust der Konnektivität, d.h. eine Verbindungsunterbrechung. Letzteres gilt insbesondere, wenn ein KI-fähiges Produkt zum Funktionieren auf Cloud-Computing angewiesen ist. Wenn z.B. ein Autofahrer ein Navigationsgerät benutzt, verursacht eine Unterbrechung der Verbindung keine schwerwiegenden Sicherheitsrisiken; es ist immer noch der Autofahrer, der das Auto lenkt und nicht das Navigationsgerät. Verliert jedoch ein autonom fahrendes Auto die Verbindung, erhält das Auto keine Informationen mehr über seine aktuelle Position, den Straßenverlauf, den Straßenzustand oder die Verkehrsbedingungen. Dies kann zu unangepasster Geschwindigkeit führen. In vergleichbarer Weise mag ein „gehacktes" Navigationsgerät, das den Fahrer falsch führt, für den Benutzer zwar sehr unangenehm sein. Ein „gehacktes" autonomes Auto jedoch könnte dazu

[14] COM(2018) 795.
[15] Europäische Kommission: Entwurf eines Weißbuchs über KI, verfügbar unter www.euractiv.com/wp-content/uploads/sites/2/2020/01/AI-white-paper-EURACTIV.pdf S. 10.
[16] Richtlinie 2001/95/EG des Europäischen Parlaments und des Rates vom 3. Dezember 2001 über die allgemeine Produktsicherheit.
[17] Richtlinie 85/374/EWG zur Angleichung der Rechts- und Verwaltungsvorschriften der Mitgliedstaaten über die Haftung für fehlerhafte Produkte.

verwendet werden, schwere Unfälle oder sogar Terroranschläge herbeizuführen. Somit werden auch Cyber-Bedrohungen durch autonome Entscheidungen KI-fähiger Produkte verschärft.

(2) Veränderung der Eigenschaften von KI-fähigen Produkten während ihres Lebenszyklus

Wahrscheinlich verändern sich KI-fähige Produkte während ihres Lebenszyklus, insbesondere durch maschinelles Lernen – d.h. wenn eine KI-Anwendung eine bestimmte Aufgabe ausführt, ohne explizit darauf programmiert zu sein, sondern stattdessen Muster und Schlussfolgerungen verwendet – oder durch umfangreiche Aktualisierungen der Datenbank, die KI-fähige Produkte zum Lernen verwenden.

Ein KI-fähiges Produkt könnte die Sicherheitsnormen beim ersten Inverkehrbringen erfüllen, was sowohl nach der Produkthaftungsrichtlinie[18] als auch nach der Richtlinie über die allgemeine Produktsicherheit[19] der maßgebliche Zeitpunkt ist. Es könnte jedoch zu einem späteren Zeitpunkt diese Standards nicht mehr einhalten, da sich sein Verhalten geändert hat, z.B. wenn es aufgrund neuer Daten zu anderen Ergebnissen kommt. Wird etwa eine KI-fähige Fitness-Uhr in Verkehr gebracht, die mit ausgewogenen Daten kalibriert wurde, kann es passieren, dass sie mit der Zeit hauptsächlich Daten von aktiven und gesunden Menschen sammelt. Wenn die Uhr diese Daten dann dazu verwendet, den Benutzern ein Training vorzuschlagen, könnte die Uhr alte oder untrainierte Menschen dazu ermutigen, zu viel zu trainieren, was ein Risiko für deren Gesundheit darstellt. Wenn die Uhr zudem ein Gerät zur elektrischen Muskelstimulation autonom steuert, könnten Benutzer durch das Gerät direkt geschädigt werden, ohne die Kontrolle über die von der KI getroffene Entscheidung zu haben.

(3) Schwierigkeiten im Zusammenhang mit der Rechtsdurchsetzung

KI-fähige Produkte basieren oft nicht mehr auf einem leicht lesbaren Code. Während das Ergebnis in den meisten Fällen präziser ist, ist es nicht immer möglich, die Kausalität oder den Prozess der Ergebnisfindung der KI zu verstehen. Wenn eine KI-fähige Software beispielsweise Bewerber zu einem Stellenangebot interviewt, können die Parameter, die zum Ergebnis führen, undurchsichtig sein. Wenn ein Bewerber glaubt, dass er diskriminiert wurde, könnten daher die Entdeckung und die mögliche Wiedergutmachung der Diskriminierung unmöglich sein.

2.2 Regulierungsoptionen für zukünftige Gesetzgebung

Um die Schwächen der derzeitigen Gesetzgebung zu beheben, stellt das Weißbuch drei mögliche Regulierungsoptionen vor:

Option 1: Freiwilliges Kennzeichnungssystem (Label)

KI-Entwickler, die bestimmte Vorgaben erfüllen, dürfen ein Label „ethische/vertrauenswürdige KI“ verwenden. Die Einhaltung der Vorgaben muss durchgesetzt werden. Darüber hinaus ist die Kommission der Ansicht, dass ein Label für „ethische/vertrauenswürdige KI“ Europa helfen würde, eine wichtige Rolle in den

[18] Art. 7 lit. b der Richtlinie 85/374/EWG.
[19] Art. 3 Abs. 1 der Richtlinie 2001/95/EG.

internationalen Diskussionen über ethische und vertrauenswürdige KI zu spielen.[20] Die Kommission stellt jedoch fest, dass ein freiwilliges Label möglicherweise nicht ausreicht, um z.B. Sicherheits- und Haftungsfragen zu klären.

cep**Bewertung**: Dieser Ansatz ist für Entwickler und Nutzer von KI am wenigsten belastend, da die Verwendung des Labels freiwillig ist. Daher respektiert Option 1 die unternehmerische Freiheit. Entwicklern von KI würden nur dann zusätzliche Kosten entstehen, wenn sie die die Labelvorgaben freiwillig erfüllen möchten. Wenn das Label jedoch von den Verbrauchern sehr geschätzt wird, werden Unternehmen dazu gedrängt, sich an die Labelvorgaben zu halten, um den Verbrauchern ihre "Vertrauenswürdigkeit" zu signalisieren. Doch auch in diesem Fall ist ein Label sachgerecht, da es dazu führt, dass Unternehmen die Wünsche der Verbraucher erfüllen und die Transparenz für Verbraucher erhöht.

Die Frage, welche Behörde für die Erteilung und Durchsetzung des Labels zuständig sein sollte, wird im Weißbuch nicht erörtert. Das durch die Datenschutzgrundverordnung (im Folgenden: „DSGVO“)* eingeführte Zertifizierungssystem, das nachweist, dass Unternehmen die DSGVO-Vorschriften einhalten, zeigt jedoch, dass dieser Aspekt sehr wichtig ist. Das DSGVO-Zertifizierungssystem wird nur selten verwendet, da es in der EU nicht einheitlich angewendet wird.** Denn die nationalen Behörden legen die DSGVO unterschiedlich aus und setzen unterschiedliche Standards für den Erhalt der Zertifizierung. Dies verzerrt den Wettbewerb innerhalb des Binnenmarkts und verringert die Rechtssicherheit für Unternehmen, die in einem Land zertifiziert sind, wenn sie in einem anderen Land tätig werden. Es ist daher von entscheidender Bedeutung, einheitliche und klare Vorgaben zu schaffen, die einzuhalten sind, um das EU-Label für vertrauenswürdige KI zu erhalten.

* Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr.

** Centrum für Europäische Politik: cep** Analyse** Nr. 01/2020.

Option 2: Sektorale Anforderungen an Behörden und für Gesichtserkennung

Dieser Ansatz stellt Anforderungen an Behörden, wenn diese KI-fähige Produkte benutzen. Die Anforderungen enthalten, wie die kanadische Richtlinie zur automatisierten Entscheidungsfindung, Regelungen für

- Folgenabschätzungen der verwendeten Algorithmen (d.h. Anforderungen, wie die Auswirkungen von Algorithmen auf Verwaltungsentscheidungen zu prüfen sind, wobei wichtigere Entscheidungen einer genaueren Prüfung unterzogen würden),
- Qualitätssicherung (d. h. Anforderungen, die sicherstellen, dass die von der KI-Anwendung verwendeten Daten auf unbeabsichtigte Datenverzerrungen und andere Faktoren, die die Ergebnisse verzerren können, geprüft werden),
- Rechtsschutzmechanismen und
- Berichtspflichten für die Behörde (z.B. Anforderungen an Behörden, Informationen über die Effektivität und Effizienz der KI-Anwendungen bei der Erfüllung der Ziele der Behörden auf einer Website zu veröffentlichen).

[20] Centrum für Europäische Politik: cep**Input** Nr. 07/2019.

Das Ziel von Option 2 wäre es, sicherzustellen, dass Behörden KI in einer Weise einsetzen, die das Risiko von Fehlentscheidungen verringert und zu effizienteren, genaueren, konsistenteren und verständlicheren Entscheidungen führt.

cep**Bewertung**: Der Vorteil dieser Option ist die sektorale und problemspezifische KI-Regulierung. Da Behörden wesentlich mehr Macht haben, in die Grundrechte der Menschen einzugreifen, als private Akteure, ist die Regulierung der Nutzung von KI durch Behörden dringender als zwischen privaten Akteuren. Außerdem würde die damit einhergehende klare Definition des Anwendungsbereichs der KI-Gesetzgebung den KI-Entwicklern und Nutzern helfen, zu bestimmen, ob eine solche Regelung (z.B. die Berichtspflicht) für sie gilt oder nicht. Die Behörden wüssten mit Sicherheit, dass dem so ist, private Nutzer wüssten mit Sicherheit, dass dem nicht so ist. Obwohl die Regulierung unter Option 2 nur die Verwendung von KI durch Behörden zum Gegenstand hat, könnte sie dennoch eine Signalwirkung für den privaten Sektor haben, indem sie Unternehmen dazu ermutigt, wesentliche Standards des öffentlichen Sektors einzuhalten, um gegenüber den Verbrauchern „Vertrauenswürdigkeit“ zu signalisieren. Einige Verbraucher könnten Produkte, die die Anforderungen für Behörden erfüllen, billigeren Produkten vorziehen, die dies nicht tun. Ein solcher Ansatz zur Regulierung könnte im privaten Sektor das Ergebnis erzielen, das ein freiwilliges Label (Option 1) vorsieht.

Unter Option 2 erörtert die Kommission zudem, ob spezifische Regeln für den Einsatz von Gesichtserkennungssystemen im öffentlichen Raum eingeführt werden sollten oder ob der Einsatz dieser Technologie im öffentlichen Raum für einen Zeitraum von z.B. drei bis fünf Jahren verboten werden sollte. In dieser Zeit sollte eine solide Methodik zur Bewertung der Auswirkungen dieser Technologie und möglicher Maßnahmen zum Risikomanagement identifiziert und entwickelt werden. Das Verbot von Gesichtserkennungssystemen würde für öffentliche und private Akteure gleichermaßen gelten. Ausnahmen sollten etwa für Forschung & Entwicklung und Sicherheitszwecke in Betracht gezogen werden.

cep**Bewertung**: Es stimmt zwar, dass die Gesichtserkennungstechnologie mehr Herausforderungen an Grundrechte stellt als viele andere KI-Anwendungen. Aber wie die Kommission selbst erkannt hat, könnte eine so weitreichende Maßnahme wie ein vollständiges Verbot der Gesichtserkennungstechnologie deren Entwicklung in der EU behindern. Dies gilt umso mehr, da dieser Markt bereits von Nicht-EU-Unternehmen dominiert wird. Außerdem würde die KI-Gesetzgebung, abgesehen vom Verbot der Gesichtserkennungstechnologie, private Akteure nicht erfassen.

Option 3: Obligatorische risikobasierte Anforderungen für risikoreiche KI-Anwendungen

Die neue KI-Gesetzgebung würde nur für risikoreiche KI-Anwendungen gelten, während die bestehende Gesetzgebung – z.B. die DSGVO – weiterhin für alle Anwendungen gelten würde. Eine Möglichkeit, risikoreiche KI-Anwendungen zu definieren, wäre es, zu beurteilen, ob eine Anwendung kumulativ

- in einen der besonders sensiblen Bereiche fällt, die klar spezifiziert werden würden (z.B. Gesundheitswesen, Transport, Polizei und Justiz) und

- eine abstraktere Definition von „risikoreicher“ Anwendung erfüllt; diese Definition könnte wie folgt lauten: „Risikoreiche Anwendungen sind KI-Anwendungen, die für ein Individuum oder eine juristische Person rechtliche Auswirkungen haben können oder ein Risiko von Verletzung, Tod oder erheblichen materiellen Schäden für ein Individuum oder eine juristische Person darstellen können.”[21]

cep**Bewertung**: Der Hauptvorteil dieser Option besteht darin, dass sie auf dynamische und flexible Weise alle risikoreichen KI-Anwendungen – auch im privaten Sektor – abdecken könnte. Die Interpretation des Begriffs „risikoreich“ lässt jedoch einen Ermessensspielraum und gibt, wenn nicht genau definiert, Unternehmen einen Anreiz, die möglichen Risiken ihres Produkts herunterzuspielen, damit ihre KI-Anwendungen nicht den Standards für risikoreiche Anwendungen* entsprechen müssen. Das Weißbuch lässt zudem offen, was der Inhalt der risikobasierten Regulierung sein könnte, und stellt lediglich fest, dass ein solches Instrument Anforderungen an Transparenz und Rechenschaftspflicht festlegen könnte.

* Centrum für Europäische Politik: cep**Analyse** Nr. Nr. 01/2020.

2.3 Zusätzliche regulatorische Optionen

Darüber hinaus erwägt die Kommission zwei weitere Regulierungsoptionen, die mit jeder der drei oben genannten Optionen kombiniert werden können:

(1) Sicherheits- und Haftungsvorschriften

Die Kommission erwägt, die bestehenden Sicherheits- und Haftungsvorschriften – namentlich die Richtlinie über die allgemeine Produktsicherheit, die Maschinenrichtlinie,[22] die Richtlinie über Funkanlagen[23] und die Produkthaftungsrichtlinie – zu ändern, um den spezifischen Risiken von KI-fähigen Produkten Rechnung zu tragen.

cep**Bewertung**: Der Vorteil dieses Ansatzes besteht darin, dass er die von der Kommission festgestellten Schwächen in der aktuellen Gesetzgebung angeht, ohne dass KI-spezifische Rechtsakte eingeführt werden. Dadurch werden spezifische Verpflichtungen für verschiedene Sektoren, Akteure oder Kategorien von KI-Anwendungen vermieden.

(2) Aufsicht

Die Mitgliedstaaten sollten bestehende oder neu einzurichtende Behörden damit beauftragen, die Anwendung und die Durchsetzung des künftigen Regulierungsrahmens für KI zu überwachen.

[21] Europäische Kommission: Entwurf eines Weißbuchs über KI, verfügbar unter www.euractiv.com/wp-content/uploads/sites/2/2020/01/AI-white-paper-EURACTIV.pdf S. 16.

[22] Richtlinie 2006/42/EG des Europäischen Parlaments und des Rates vom 17. Mai 2006 über Maschinen.

[23] Richtlinie 2014/53/EU des Europäischen Parlaments und des Rates vom 16. April 2014 zur Harmonisierung der Rechtsvorschriften der Mitgliedstaaten über die Bereitstellung von Funkanlagen auf dem Markt.

cep**Bewertung**: Wie die Anwendung der DSGVO gezeigt hat, ist es von entscheidender Bedeutung, dass die nationalen Behörden ausreichend finanziert sind und über die Instrumente zur Zusammenarbeit mit anderen Behörden in der EU verfügen. Darüber hinaus sollten bestimmte Vorgehensweisen der nationalen Behörden harmonisiert werden, da sonst eine rechtliche Zersplitterung den Wettbewerb im Binnenmarkt verzerren könnte, z.B. bei der Verhängung von Sanktionen.*

* Centrum für Europäische Politik: cep**Analyse** Nr. 01/2020.

2.4 Schlussbemerkungen

Die Kommission scheint einen risikobasierten Ansatz zu befürworten (Option drei). Ein solcher Ansatz könnte von den nationalen Behörden durchgesetzt und mit einer Aktualisierung der Sicherheits- und Haftungsgesetzgebung gekoppelt werden. Interessanterweise rät die Kommission von einem Verbot von Gesichtserkennungstechnologien ab und bevorzugt stattdessen deren Regulierung durch die vollständige Umsetzung der einschlägigen DSGVO-Bestimmungen.