EUROPÄISCHE
KOMMISSION

Brüssel, den 19.2.2020
COM(2020) 65 final

WEISSBUCH

Zur Künstlichen Intelligenz – ein europäisches Konzept für Exzellenz und Vertrauen

Weißbuch zur Künstlichen Intelligenz – Ein europäisches Konzept für Exzellenz und Vertrauen

Die Künstliche Intelligenz entwickelt sich schnell. Sie wird unser Leben verändern, indem sie die Gesundheitsfürsorge verbessert (z. B. durch präzisere Diagnostik und bessere Prävention von Krankheiten), die Effizienz der Landwirtschaft erhöht, zum Klimaschutz und zur Anpassung an den Klimawandel beiträgt, die Effizienz von Produktionsanlagen durch vorausschauende Wartung steigert, die Sicherheit der Europäerinnen und Europäer erhöht und noch auf viele andere Arten und Weisen, die derzeit gar nicht völlig absehbar sind. Gleichzeitig birgt die Künstliche Intelligenz (KI) eine Reihe potenzieller Gefahren z. B. wegen undurchsichtiger Entscheidungsprozesse oder wegen Diskriminierung aufgrund des Geschlechts oder anderer Faktoren, durch Eingriffe in unser Privatleben oder Missbrauch zu kriminellen Zwecken.

Vor dem Hintergrund des harten weltweiten Wettbewerbs brauchen wir ein solides europäisches Konzept, das auf der im April 2018 vorgelegten europäischen KI-Strategie[1] aufbaut. Um die mit KI einhergehenden Chancen und Herausforderungen anzunehmen, muss die EU geeint handeln und auf der Grundlage europäischer Werte ihren eigenen Weg zur Förderung der Entwicklung und Nutzung von KI festlegen.

Die Kommission ist entschlossen, wissenschaftliche Durchbrüche zu ermöglichen, die Technologieführerschaft der EU zu wahren und sicherzustellen, dass neue Technologien im Dienst aller Europäerinnen und Europäer stehen – sie sollen Verbesserungen im Alltag bewirken, und gleichzeitig die Rechte der Bürgerinnen und Bürger achten.

Kommissionspräsidentin Ursula von der Leyen kündigte in ihren politischen Leitlinien [2] ein koordiniertes europäisches Konzept für die menschlichen und ethischen Aspekte von KI sowie eine Reflexion über die bessere Nutzung von Big Data für Innovationen an.

Damit unterstützt die Kommission ein auf Regulierung und Finanzierung ausgerichtetes Konzept, das die Nutzung von KI fördert und gleichzeitig auf die mit dieser Technologie einhergehenden Gefahren eingeht. Dieses Weißbuch soll politische Optionen für die Verwirklichung dieser Ziele darlegen. Die Entwicklung und Nutzung von KI für militärische Zwecke werden in diesem Weißbuch nicht behandelt. Die Kommission lädt die Mitgliedstaaten, die anderen europäischen Organe wie auch alle Interessenträger, darunter die Industrie, Sozialpartner, Organisationen der Zivilgesellschaft, Forscherinnen und Forscher, die breite Öffentlichkeit und alle interessierten Kreise, ein, zu den nachstehenden Optionen Stellung zu nehmen und zur künftigen Entscheidungsfindung der Kommission in diesem Bereich beizutragen.

1. EINLEITUNG

Da digitale Technologien immer weiter in alle Bereiche des Alltags vordringen, sollten die Menschen ihnen auch vertrauen können. Vertrauenswürdigkeit ist eine Voraussetzung für ihre Akzeptanz. Dies ist eine Chance für ein Europa, das Werten und Rechtsstaatlichkeit große Bedeutung beimisst und nachweislich in der Lage ist, sichere, zuverlässige und Spitzenprodukte und -dienstleistungen anzubieten – von der Luftfahrt über den Energiesektor bis hin zur Automobilindustrie und Medizintechnik.

[1] KI für Europa, COM/2018/237 final.
[2] https://ec.europa.eu/commission/sites/beta-political/files/political-guidelines-next-commission_de.pdf.

Das nachhaltige Wirtschaftswachstum und das gesellschaftliche Wohlergehen in Europa stützen sich schon jetzt und auch in Zukunft zunehmend auf die Wertschöpfung durch Daten. KI ist eine der wichtigsten Anwendungen der Datenwirtschaft. Heutzutage beziehen sich die meisten Daten auf Verbraucher und werden auf zentralen Cloud-basierten Infrastrukturen gespeichert und verarbeitet. In Zukunft hingegen wird ein großer Teil der künftig sehr viel umfangreicheren Datenmengen aus der Industrie, der Wirtschaft und dem öffentlichen Sektor kommen und in verschiedensten Systemen gespeichert werden, insbesondere auf Rechnern, die am Rande des Netzes arbeiten. Dies eröffnet neue Chancen für Europa, dessen Position in den Bereichen digitalisierte Anwendungen für die Industrie und B2B-Anwendungen stark, im Bereich Verbraucherplattformen hingegen relativ schwach ist.

Einfach ausgedrückt ist KI ein Bestand an Technologien, die Daten, Algorithmen und Rechenleistung kombinieren. Fortschritte in der Informatik und die zunehmende Verfügbarkeit von Daten sind daher der Schlüsselfaktor für den derzeitigen Aufstieg der KI. Wie in der europäischen Datenstrategie[3] dargelegt, kann Europa seine technologischen und industriellen Stärken mit einer hochwertigen digitalen Infrastruktur und einem Rechtsrahmen kombinieren, der auf seinen Grundwerten beruht, um sich im Bereich der **Innovation in der Datenwirtschaft und ihren Anwendungen an die Weltspitze zu setzen**. Auf dieser Grundlage kann Europa ein KI-Ökosystem entwickeln, das der gesamten europäischen Gesellschaft und Wirtschaft die Vorteile der Technologie erschließt:

- **Bürgerinnen und Bürger** kommen in den Genuss neuer Vorteile wie z. B. bessere Gesundheitsversorgung, weniger Ausfälle von Haushaltsgeräten, sicherere und sauberere Verkehrssysteme, bessere öffentliche Dienste;
- **Unternehmen** können z. B. eine neue Generation von Produkten und Dienstleistungen entwickeln in Bereichen, in denen Europa besonders stark ist (Maschinenbau, Verkehr, Cybersicherheit, Landwirtschaft, grüne Wirtschaft und Kreislaufwirtschaft, Gesundheitswesen und Sektoren mit hoher Wertschöpfung wie Mode und Tourismus); und
- Dienste von **öffentlichem Interesse** profitieren z. B. durch niedrigere Kosten für die Erbringung von Dienstleistungen (Verkehr, Bildung, Energie und Abfallentsorgung), durch eine Verbesserung der Nachhaltigkeit von Produkten[4] und durch die Ausstattung von Strafverfolgungsbehörden mit geeigneten Instrumenten zum Schutz der Bürgerinnen und Bürger[5], mit angemessenen Garantien für die Achtung ihrer Rechte und Freiheiten.

Angesichts der erheblichen Auswirkungen, die KI auf unsere Gesellschaft und die notwendige Vertrauensbildung haben kann, ist es von entscheidender Bedeutung, dass die europäische KI auf unseren Werten und Grundrechten wie Menschenwürde und Schutz der Privatsphäre fußt.

Zudem sollten die Auswirkungen von KI-Systemen nicht nur aus dem Blickwinkel des Einzelnen betrachtet werden, sondern auch aus der Perspektive der gesamten Gesellschaft. KI-Systeme können bei der Verwirklichung der nachhaltigen Entwicklungsziele und der Förderung des demokratischen Prozesses und sozialer Rechte eine bedeutende Rolle spielen. Mit den unlängst vorgelegten

[3] COM(2020) 66 final.

[4] KI und die Digitalisierung allgemein sind maßgebliche Voraussetzungen für die Verwirklichung der Ziele des europäischen Grünen Deals. Der derzeitige ökologische Fußabdruck des IKT-Sektors entspricht Schätzungen zufolge jedoch mehr als 2 % aller Emissionen weltweit. In der zusammen mit diesem Weißbuch vorgelegten europäischen Digitalstrategie werden Maßnahmen für einen umweltverträglichen Wandel im digitalen Bereich vorgeschlagen.

[5] Mithilfe von KI-Tools können EU-Bürger u. U. besser vor Verbrechen und terroristischen Anschlägen geschützt werden. Mit solchen Tools könnten beispielsweise terroristische Propaganda im Internet erkannt, verdächtige Transaktionen beim Absatz gefährlicher Produkte aufgedeckt, gefährliche Gegenstände oder illegale Stoffe und Produkte identifiziert, Menschen in Notsituationen Hilfe geleistet und Ersthelfer angeleitet werden.

Vorschlägen für den Europäischen Grünen Deal[6] nimmt die EU bei der Bewältigung von Klima- und Umweltherausforderungen eine Vorreiterrolle ein. Digitale Technologien wie KI tragen entscheidend dazu bei, die Ziele des Grünen Deals zu erreichen. Angesichts der zunehmenden Bedeutung der KI muss den Umweltauswirkungen von KI-Systemen von Anfang bis Ende ihres Lebenszyklus und entlang der gesamten Lieferkette gebührend Rechnung getragen werden, beispielsweise hinsichtlich des Ressourcenverbrauchs beim Trainieren von Algorithmen und der Speicherung von Daten.

Nur mit einem gemeinsamen europäischen KI-Konzept können eine ausreichende Größenordnung erreicht und eine Fragmentierung des Binnenmarkts vermieden werden. Werden hier einzelne Initiativen auf nationaler Ebene ergriffen, könnte dies die Rechtssicherheit gefährden, das Vertrauen der Bürger untergraben und das Entstehen einer dynamischen europäischen Industrie verhindern.

In diesem Weißbuch werden politische Optionen vorgestellt mit dem Ziel, eine rasche und sichere Entwicklung der KI in Europa unter uneingeschränkter Achtung der Werte und Rechte der europäischen Bürgerinnen und Bürger zu ermöglichen. Die wichtigsten Bausteine dieses Weißbuchs sind:

- Der politische Rahmen mit Maßnahmen zur Abstimmung der Anstrengungen auf europäischer, nationaler und regionaler Ebene. Der Rahmen zielt darauf ab, in Partnerschaft zwischen öffentlichem und Privatsektor Ressourcen zu mobilisieren, um ein **„Ökosystem für Exzellenz“** aufzubauen, das bei Forschung und Innovation beginnt und sich über die gesamte Wertschöpfungskette erstreckt, und die richtigen Anreize zu schaffen, um die Akzeptanz von KI-Lösungen auch seitens kleiner und mittlerer Unternehmen (KMU) zu beschleunigen.

- Die Schlüsselelemente eines künftigen Rechtsrahmens für KI in Europa werden ein einzigartiges **„Ökosystem für Vertrauen“** schaffen. Um dieses Ziel zu erreichen, muss durch den Rahmen sichergestellt werden, dass die EU-Vorschriften eingehalten werden, einschließlich der Vorschriften zum Schutz der Grundrechte und der Verbraucherrechte, insbesondere im Falle von in der EU eingesetzten KI-Systemen mit hohen Risikopotenzial[7]. Ein Ökosystem für Vertrauen aufzubauen, ist schon an sich ein strategisches Ziel und sollte bei den Bürgerinnen und Bürgern das nötige Vertrauen schaffen, KI-Anwendungen zu nutzen, und Unternehmen und öffentlichen Stellen die Rechtssicherheit für KI-gestützte Innovationen. Die Kommission befürwortet nachdrücklich ein Konzept, bei dem der Mensch im Mittelpunkt steht, das auf der Mitteilung über die Schaffung von Vertrauen in eine auf den Menschen ausgerichtete KI[8] beruht und auch die während der Pilotphase eingegangenen Rückmeldungen zu den Ethik-Leitlinien der Hochrangigen Expertengruppe für Künstliche Intelligenz berücksichtigt.

Die europäische Datenstrategie, die zusammen mit diesem Weißbuch vorgelegt wird, soll Europa in die Lage versetzen, zur attraktivsten, sichersten und dynamischsten datenagilen Wirtschaft der Welt zu werden, indem Europa durch Daten befähigt wird, bessere Entscheidungen zu treffen und das Leben aller seiner Bürgerinnen und Bürger zu verändern. Die Strategie sieht eine Reihe politischer Maßnahmen vor, darunter die Mobilisierung privater und öffentlicher Investitionen, die zur Erreichung dieses Ziels erforderlich sind. Die Auswirkungen von KI, Internet der Dinge und anderen digitalen Technologien auf die Sicherheits- und Haftungsvorschriften werden in dem Bericht der Kommission analysiert, der ebenfalls zusammen mit diesem Weißbuch vorgelegt wird.

---

[6] COM(2019)640 final.

[7] Unter Umständen müssen weitere Vorkehrungen getroffen werden, um den Missbrauch von KI zu kriminellen Zwecken zu verhindern und zu bekämpfen, aber dies ist nicht Gegenstand dieses Weißbuchs.

[8] COM(2019)168.

2. DIE STÄRKEN IN INDUSTRIELLEN UND GEWERBLICHEN ABSATZMÄRKTEN NUTZEN

Europa verfügt über die Voraussetzungen zum Ausschöpfen des KI-Potenzials, und zwar nicht nur als Nutzer, sondern auch als Urheber und Hersteller dieser Technologie. Denn es gibt in Europa herausragende Forschungszentren und innovative Start-Ups, es ist weltweit führend in Robotik und hat wettbewerbsfähige Fertigungs- und Dienstleistungssektoren – von der Automobilindustrie bis zum Gesundheitswesen, von der Energieversorgung über Finanzdienstleistungen bis hin zur Landwirtschaft. Europa hat auch eine starke Recheninfrastruktur entwickelt (z. B. Hochleistungscomputer), die eine Voraussetzung für den Einsatz von KI ist. Ferner verfügt Europa über große Mengen öffentlicher und industrieller Daten, deren Potenzial nicht ausgeschöpft wird. Anerkannt sind auch seine industriellen Stärken im Bereich sichere digitale Systeme mit geringem Stromverbrauch, die für die Weiterentwicklung der KI von maßgeblicher Bedeutung sind.

Wenn die Kapazitäten der EU für Investitionen in Technologien und Infrastrukturen der nächsten Generation sowie in digitale Kompetenzen z. B. im Bereich Daten genutzt werden, stärkt dies die technologische Unabhängigkeit Europas bei den Schlüsseltechnologien und -infrastrukturen für die Datenwirtschaft. Die Infrastrukturen sollten die Schaffung europäischer Datenpools unterstützen, die eine vertrauenswürdige KI ermöglichen, d. h. eine KI auf der Grundlage europäischer Werte und Regeln.

Europa sollte seine Stärken nutzen, um seine Position in den Ökosystemen und entlang der Wertschöpfungskette auszubauen – von der Hardwareherstellung über Software bis hin zu Dienstleistungen. Bis zu einem gewissen Grad geschieht dies bereits. Europa produziert mehr als ein Viertel aller Industrie- und professionellen Serviceroboter (z. B. für Präzisionslandwirtschaft, Sicherheit, Gesundheitswesen und Logistik) und spielt eine wichtige Rolle bei der Entwicklung und Nutzung von Softwareanwendungen für Unternehmen und Organisationen (B2B-Anwendungen wie Software für Ressourcenplanung, Design- und Maschinenbau-Software) und von Anwendungen für elektronische Behördendienste und das „intelligente Unternehmen".

Europa ist Spitzenreiter beim Einsatz von KI in der verarbeitenden Industrie. Mehr als die Hälfte der führenden Hersteller setzt in der Produktion an mindestens einer Station eine KI-Anwendung ein[9].

Ein Grund für die starke Stellung Europas in der Forschung ist das EU-Förderprogramm, das entscheidend dazu beigetragen hat, die Anstrengungen zu bündeln, Doppelarbeit zu vermeiden und öffentliche und private Investitionen in den Mitgliedstaaten zu mobilisieren. In den letzten drei Jahren wurden die europäischen FuI-Mittel für KI auf 1,5 Mrd. EUR und damit im Vergleich zum vorherigen Zeitraum um 70 % aufgestockt.

Allerdings wird in Europa nur ein Bruchteil dessen in Forschung und Innovation investiert, was in anderen Regionen der Welt an öffentlichen und privaten Investitionen fließt. 2016 wurden in Europa ca. 3,2 Mrd. EUR in KI investiert – gegenüber rund 12,1 Mrd. EUR in Nordamerika und 6,5 Mrd. EUR in Asien[10]. Deshalb muss Europa erheblich mehr investieren. Der „Koordinierte Plan für Künstliche Intelligenz"[11], der gemeinsam mit den Mitgliedstaaten erstellt wurde, erweist sich als gute Grundlage für den Aufbau einer engeren Zusammenarbeit im KI-Bereich in Europa und für die Schaffung von Synergien zur Maximierung der Investitionen in die KI-Wertschöpfungskette.

[9] Gefolgt von Japan (30 %) und den USA (28 %). Quelle: CapGemini (2019).
[10] „10 imperatives for Europe in the age of AI and automation" (Zehn zwingende Erfordernisse für Europa im Zeitalter von KI und Automatisierung), McKinsey, 2017.
[11] COM(2018)795.

3. NEUE CHANCEN NUTZEN: DIE NÄCHSTE DATENWELLE

Europas ist zwar derzeit in den Bereichen Verbraucheranwendungen und Online-Plattformen nicht so stark aufgestellt, was zu einem Wettbewerbsnachteil hinsichtlich des Zugangs zu Daten führt, aber es stehen bedeutende Veränderungen an hinsichtlich des Werts und der sektorübergreifenden Weiterverwendung von Daten. Die Menge der weltweit produzierten Daten nimmt rasch zu, von 33 Zettabyte im Jahr 2018 auf voraussichtlich 175 Zettabyte im Jahr 2025[12]. Jede neue Datenwelle bringt Europa Möglichkeiten, sich in der datenagilen Wirtschaft zu positionieren und an die Weltspitze zu setzen. Abgesehen davon wird sich die Art und Weise, wie Daten gespeichert und verarbeitet werden, in den kommenden fünf Jahren drastisch verändern. Gegenwärtig erfolgt die Verarbeitung und Analyse von Daten in der Cloud zu 80 % in Rechenzentren und zentralen Rechenanlagen und zu 20 % in intelligenten vernetzten Objekten wie Autos, Haushaltsgeräten oder Fertigungsrobotern und in Rechnern nahe beim Nutzer („Edge-Computing“, d. h. dezentrale Datenverarbeitung am Rand des Netzes). Bis zum Jahr 2025 dürften sich diese Anteile deutlich verschieben[13].

Europa ist weltweit führend in der Elektronik mit geringem Stromverbrauch, die für die nächste Generation spezialisierter KI-Prozessoren von zentraler Bedeutung ist. Auf diesem Markt dominieren derzeit Teilnehmer aus Drittländern. Ändern könnte sich dies durch Initiativen wie die Europäische Prozessorinitiative, die auf die Entwicklung von Rechensystemen mit geringem Stromverbrauch für Edge-Computing und Hochleistungsrechner der nächsten Generation abzielt, und die Arbeit des gemeinsamen Unternehmens für digitale Schlüsseltechnologien, das 2021 an den Start gehen soll. Darüber hinaus ist Europa führend in neuromorphen Lösungen[14], die sich hervorragend für die Automatisierung von industriellen Prozessen (Industrie 4.0) und Verkehrsträgern eignen. Sie können die Energieeffizienz um ein Mehrfaches steigern.

Die jüngsten Fortschritte in der Quanteninformatik werden zu exponentiellen Steigerungen der Verarbeitungskapazität führen[15]. Europa kann hier dank seiner akademischen Stärken im Bereich Quanteninformatik und der starken Position der europäischen Industrie im Bereich Quantensimulatoren und Programmierumgebungen für Quantencomputer eine Vorreiterrolle einnehmen. Europäische Initiativen, die die Zahl der Quantentest- und Quantenversuchseinrichtungen erhöhen sollen, werden dazu beitragen, dass diese neuen Quantenlösungen in einer ganzen Reihe von industriellen und akademischen Sektoren angewendet werden.

Parallel dazu wird Europa auf der Grundlage seiner eigenen wissenschaftlichen Exzellenz weiterhin eine Vorreiterrolle bei den algorithmischen Grundlagen der KI einnehmen. Zwischen Fachdisziplinen, die gegenwärtig separat voneinander arbeiten, wie maschinelles Lernen und „Deep Learning“ (dessen Merkmale begrenzte Interpretierbarkeit, Bedarf an großen Datenmengen für das Trainieren von Modellen und Lernen durch Korrelationen sind) und symbolischen Ansätzen (bei denen Regeln durch menschliche Eingriffe geschaffen werden) müssen Brücken geschlagen werden. Die Kombination von symbolischem Schlussfolgern und tiefen neuronalen Netzen kann u. U. helfen, die Erklärbarkeit von KI-Ergebnissen zu verbessern.

[12] IDC, 2019.
[13] Gartner, 2017.
[14] Neuromorphe Lösungen sind sehr große Systeme integrierter Schaltungen, die neurobiologische Architekturen des Nervensystems nachahmen.
[15] Quantencomputer werden in Bruchteilen von Sekunden sehr viel umfangreichere Datensätze verarbeiten können als heutige Höchstleistungsrechner, was die Entwicklung neuer KI-Anwendungen für alle Sektoren ermöglicht.

4. EIN ÖKOSYSTEM FÜR EXZELLENZ

Um ein Exzellenzökosystem aufzubauen, das die Entwicklung und Nutzung von KI in der gesamten Wirtschaft und öffentlichen Verwaltung der EU unterstützen kann, müssen auf mehreren Ebenen verstärkte Maßnahmen ergriffen werden.

A. ZUSAMMENARBEIT MIT DEN MITGLIEDSTAATEN

Im Rahmen ihrer KI-Strategie[16], die im April 2018 angenommen wurde, hat die Kommission im Dezember 2018 einen gemeinsam mit den Mitgliedstaaten erstellten Plan vorgelegt, um die Entwicklung und Nutzung von KI in Europa zu fördern[17].

In diesem Plan werden etwa 70 gemeinsame Maßnahmen für eine engere und effizientere Zusammenarbeit zwischen den Mitgliedstaaten und der Kommission in Schlüsselbereichen wie Forschung, Investitionen, Markteinführung, Kompetenzen und Begabungen, Daten und internationale Zusammenarbeit vorgeschlagen. Der Plan soll bis 2027 laufen, seine Durchführung wird regelmäßig überwacht, und er wird periodisch überarbeitet.

Ziel ist es, die Wirkung von Investitionen in Forschung, Innovation und Einführung zu maximieren, nationale KI-Strategien zu bewerten und mit den Mitgliedstaaten auf dem koordinierten Plan für KI aufzubauen und ihn auszuweiten:

- *Maßnahme 1: Die Kommission wird den Mitgliedstaaten unter Berücksichtigung der Ergebnisse der öffentlichen Konsultation zum Weißbuch eine Neufassung des koordinierten Plans unterbreiten, die bis Ende 2020 angenommen werden sollte*

EU-Mittel für KI sollen Investitionen in Bereichen mobilisieren und bündeln, in denen Mitgliedstaaten im Alleingang nicht genug erreichen können. Das Ziel ist, in der EU in den nächsten zehn Jahren insgesamt mehr als 20 Mrd. EUR[18] an KI-Investitionen pro Jahr zu mobilisieren. Um private und öffentliche Investitionen anzuziehen, wird die EU Mittel aus dem Programm „Digitales Europa“ und Horizont Europa bereitstellen sowie aus den Europäischen Struktur- und Investitionsfonds, um den Erfordernissen sowohl weniger entwickelter Regionen als auch ländlicher Gebiete gerecht zu werden.

Der Koordinierte Plan könnte auch das gesellschaftliche und ökologische Wohlergehen als einen wichtigen Grundsatz für KI herausstellen. KI-Systeme haben das Potenzial, zur Bewältigung der drängendsten Probleme wie Klimawandel und Umweltzerstörung beizutragen. Dies muss unbedingt in umweltverträglicher Weise geschehen. KI kann und sollte selbst kritisch prüfen, wie Ressourcen verwendet werden und wie hoch der Energieverbrauch ist, und so trainiert werden, dass Entscheidungen bevorzugt werden, die gut für die Umwelt sind. Die Kommission wird gemeinsam mit dem Mitgliedstaaten Optionen prüfen, die entsprechende KI-Lösungen fördern und Anreize dafür bieten.

B. DIE ARBEIT DER FORSCHUNGS- UND INNOVATIONSGEMEINSCHAFT FOKUSSIEREN

Europa kann es sich nicht leisten, an der aktuell fragmentierten Landschaft von Kompetenzzentren festzuhalten, in der keines der Zentren die Größenordnung erreicht, mit der es dem Wettbewerb mit den weltweit führenden Instituten gewachsen wäre. Es müssen unbedingt mehr Synergien zwischen

[16] Künstliche Intelligenz für Europa, COM(2018)237.
[17] Koordinierter Plan für künstliche Intelligenz, COM(2018)795.
[18] COM(2018)237.

den zahlreichen europäischen KI-Forschungszentren geschaffen und Netzwerke unter ihnen aufgebaut werden; außerdem müssen ihre Bemühungen um größere Exzellenz und darum, die besten Forscher anzuwerben und zu halten und die besten Technologien zu entwickeln, koordiniert werden. Europa braucht ein Leitzentrum für Forschung, Innovation und Expertise, das diese Bemühungen koordiniert und eine weltweite Bezugsgröße für Exzellenz im KI-Bereich wird, Investitionen mobilisieren kann und für die schlauesten Köpfe in diesem Bereich attraktiv ist.

Die Zentren und Netzwerke sollten sich auf Sektoren konzentrieren, in denen Europa das Zeug zum globalen Spitzenreiter hat, wie z. B. Industrie, Gesundheitswesen, Verkehr, Finanzwesen, Agrar- und Lebensmittelwertschöpfungsketten, Energie/Umwelt, Forstwirtschaft, Erdbeobachtung und Raumfahrt. In all diesen Bereichen ist der Wettlauf um die Führungsposition in der Welt in vollem Gange, und Europa verfügt über beträchtliches Potenzial, Know-how und Fachwissen[19]. Ebenso wichtig ist die Einrichtung von Test- und Versuchsanlagen, um die Entwicklung und anschließende Einführung neuer KI-Anwendungen zu unterstützen.

- *Maßnahme 2: Die Kommission wird die Einrichtung von Exzellenz- und Testzentren erleichtern, die europäische, nationale und private Investitionen bündeln können, möglicherweise einschließlich der Schaffung eines neuen Rechtsinstruments. Die Kommission hat vorgeschlagen, im Rahmen des Mehrjährigen Finanzrahmens 2021-2027 einen nicht unerheblichen Betrag aus dem Programm „Digitales Europa", ggf. ergänzt durch FuI-Mittel aus Horizont Europa, eigens für die Förderung europäischer Testzentren von Weltrang vorzusehen.*

C. KOMPETENZEN

Das europäische KI-Konzept muss dadurch untermauert werden, dass besonderes Gewicht auf Kompetenzen gelegt wird, um dem Fachkräftemangel abzuhelfen.[20] Die Kommission wird in Kürze eine aktualisierte Agenda für neue Kompetenzen vorlegen, mit der sichergestellt werden soll, dass alle Menschen in Europa vom Übergang zu einer grünen Wirtschaft und von der Digitalisierung der Wirtschaft in der EU profitieren können. Eine mögliche Initiative wäre auch, sektorale Regulierungsbehörden bei der Erweiterung ihrer KI-Kompetenzen zu unterstützen, damit sie einschlägige Vorschriften wirksam und effizient umsetzen können. Der überarbeitete Aktionsplan für digitale Bildung wird dazu beitragen, daten- und KI-gestützte Technologien wie Lernanalytik und prädiktive Analytik besser zu nutzen, um die allgemeine und berufliche Bildung zu verbessern und für das digitale Zeitalter tauglich zu machen. Mithilfe des Plans wird auch auf allen Ebenen des Bildungssystems stärker für KI sensibilisiert, damit Bürgerinnen und Bürger dann fundierte Entscheidungen treffen können, bei denen KI eine immer größere Rolle spielen wird.

Die Vermittlung der Kompetenzen, die für die Arbeit im KI-Bereich notwendig sind, und die Weiterqualifizierung der Arbeitskräfte, um sie für den durch die Entwicklungen im Bereich der KI angestoßenen Wandel zu rüsten, werden eine Priorität des zusammen mit den Mitgliedstaaten überarbeiteten Koordinierten KI-Plans sein. Dies könnte die Umwandlung der Bewertungsliste der Ethik-Leitlinien in einen indikativen „Lehrplan" für KI-Entwickler umfassen, der dann Ausbildungseinrichtungen zur Verfügung gestellt wird. Besonderes Augenmerk sollte darauf gelegt werden, mehr Frauen in diesem Bereich auszubilden und zu beschäftigen.

[19] Der geplante Europäische Verteidigungsfonds und die Ständige Strukturierte Zusammenarbeit (SSZ) werden ebenfalls Möglichkeiten für Forschung und Entwicklung im Bereich der KI bieten. Entsprechende Projekte sollten aber mit den zivilen KI-Programmen der EU abgestimmt werden.

[20] https://ec.europa.eu/jrc/en/publication/academic-offer-and-demand-advanced-profiles-eu

Abgesehen davon wäre ein Leitzentrum für KI-Forschung und Innovation in Europa aufgrund seiner Möglichkeiten für Talente aus der ganzen Welt attraktiv. Ein solches Zentrum würde auch Exzellenz in Kompetenzen entwickeln und verbreiten, die dann in ganz Europa Wurzeln schlagen und wachsen können.

- *Maßnahme 3: Aufbau und Unterstützung von Netzen führender Universitäten und Hochschuleinrichtungen im Rahmen des Programms „Digitales Europa"), um die besten Lehrkräfte und Wissenschaftler anwerben und weltweit führende KI-Masterstudiengänge anbieten zu können*

Neben dem Aspekt der Weiterqualifizierung haben die Entwicklung und der Einsatz von KI-Systemen auch unmittelbare Folgen für Arbeitnehmer und Arbeitgeber. Die Einbeziehung der Sozialpartner wird entscheidend zu einem menschenzentrierten KI-Konzept für den Arbeitsplatz beitragen.

D. SCHWERPUNKT AUF KMU

Es muss sichergestellt werden, dass auch KMU Zugang zu KI haben und diese nutzen können. Die digitalen Innovationszentren[21] und die Plattform für KI auf Anforderung[22] sollten zu diesem Zweck weiter gestärkt werden und die Zusammenarbeit von KMU fördern. Das Programm „Digitales Europa" wird hierbei von entscheidender Bedeutung sein. Zwar sollten alle digitalen Innovationszentren KMU dabei unterstützen, sich mit KI vertraut zu machen und KI zu nutzen, aber es ist wichtig, dass in jedem Mitgliedstaat mindestens ein Innovationszentrum auf KI hochspezialisiert ist.

KMU und Start-ups müssen Zugang zu Finanzmitteln haben, um ihre Verfahren anpassen oder mit KI innovativ arbeiten zu können. Aufbauend auf dem geplanten, mit 100 Mio. EUR ausgestatteten Pilotinvestitionsfonds für KI und Blockchain will die Kommission den Zugang zu Finanzmitteln für KI im Rahmen des Programms „InvestEU" noch weiter ausbauen[23]. In der Liste der Bereiche, die für eine Inanspruchnahme der InvestEU-Garantie infrage kommen, ist KI ausdrücklich genannt.

- *Maßnahme 4: Die Kommission wird mit den Mitgliedstaaten zusammenarbeiten, damit mindestens ein digitales Innovationszentrum pro Mitgliedstaat auf KI hochspezialisiert ist. Digitale Innovationszentren können im Rahmen des Programms „Digitales Europa" unterstützt werden*.
- *Die Kommission und der Europäische Investitionsfonds werden im ersten Quartal 2020 ein Pilotprogramm mit einem Etat von 100 Mio. EUR starten, um Beteiligungskapital für innovative KI-Entwicklungen bereitzustellen. Vorbehaltlich der endgültigen Einigung über den MFR beabsichtigt die Kommission ab 2021 eine erhebliche Aufstockung über InvestEU.*

[21] ec.europe.eu/digital-single-market/en/news/digital-innovation-hubs-helping-companies-across-economy-make-most-digital-opportunities.
[22] www.Ai4eu.eu.
[23] Europe.eu/investeu.

E. PARTNERSCHAFT MIT DEM PRIVATEN SEKTOR

Der Privatsektor muss unbedingt in vollem Umfang an der Ausarbeitung der Forschungs- und Innovationsagenda beteiligt werden und die erforderliche Kofinanzierung bereitstellen. Hierzu müssen sowohl eine breit angelegte öffentlich-private Partnerschaft aufgebaut als auch die Führungsspitzen von Unternehmen mit ins Boot geholt werden.

- *Maßnahme 5: Im Kontext von Horizont Europa wird die Kommission eine neue öffentlich-private Partnerschaft für KI, Daten und Robotik gründen, um die Anstrengungen zu bündeln, die Koordinierung von KI-Forschung und Innovation zu gewährleisten, mit anderen öffentlich-privaten Partnerschaften im Rahmen von Horizont Europa zu kooperieren und mit den vorgenannten Testeinrichtungen und digitalen Innovationszentren zusammenzuarbeiten.*

F. DIE NUTZUNG VON KI IM ÖFFENTLICHEN SEKTOR FÖRDERN

Es ist äußerst wichtig, dass öffentliche Verwaltungen, Krankenhäuser, Versorgungsbetriebe und Verkehrsdienste, Finanzaufsichtsbehörden und andere Bereiche von öffentlichem Interesse rasch mit der Einführung KI-gestützter Produkte und Dienstleistungen beginnen. Ein besonderer Schwerpunkt wird auf den Bereichen Gesundheitsfürsorge und Verkehr liegen, in denen die Technologien so weit ausgereift sind, dass sie in großem Maßstab eingesetzt werden können.

- *Maßnahme 6: Die Kommission wird offene und transparente Dialoge auf Sektorebene initiieren und dabei dem Gesundheitssektor, Verwaltungen ländlicher Gebiete und den Betreibern öffentlicher Dienste Vorrang einräumen, damit ein Aktionsplan vorgelegt werden kann, der die Entwicklung, Erprobung und Einführung erleichtert. Im Zuge dieser Dialoge soll je Sektor ein Programm zur Einführung von KI erarbeitet werden, das die Beschaffung von KI-Systemen fördert und dazu beiträgt, die öffentlichen Vergabeverfahren anzupassen.*

G. DEN ZUGANG ZU DATEN UND RECHENINFRASTRUKTUREN SICHERN

Die in diesem Weißbuch dargelegten Aktionsbereiche ergänzen den parallel hierzu im Rahmen der europäischen Datenstrategie vorgelegten Plan. Die Verbesserung des Zugangs zu Daten und ihrer Verwaltung ist von grundlegender Bedeutung Ohne Daten ist die Entwicklung von KI- und anderen digitalen Anwendungen nicht möglich. Da die enormen Mengen neuer Daten erst noch erzeugt werden müssen, hat Europa die Chance, sich an die Spitze der Daten- und KI-Revolution zu setzen. Wenn verantwortungsvolle Datenverwaltungsmethoden gefördert und die FAIR-Grundsätze eingehalten werden, trägt dies zur Vertrauensbildung bei und gewährleistet, dass Daten weiterverwendet werden können[24]. Ebenso wichtig sind Investitionen in maßgebliche Rechentechnologien und -infrastrukturen.

Die Kommission schlägt vor, im Rahmen des Programms „Digitales Europa“ mehr als 4 Mrd. EUR zur Förderung von Hochleistungs- und Quantenrechnen, einschließlich Edge-Computing und KI-, Daten- und Cloud-Infrastruktur, bereitzustellen. In der europäischen Datenstrategie werden diese Prioritäten weiter ausgeführt.

[24] FAIR = Findable, Accessible, Interoperable and Reusable (auffindbar, zugänglich, interoperabel und wiederverwendbar), siehe Schlussbericht und Aktionsplan der Expertengruppe der Kommission zu FAIR-Daten, 2018, https://ec.europa.eu/info/sites/info/files/turning_fair_into_reality_1.pdf.

H. INTERNATIONALE ASPEKTE

Europa verfügt über gute Voraussetzungen für eine globale Führungsrolle beim Aufbau von Allianzen rund um gemeinsame Werte und bei der Förderung des ethischen Umgangs mit KI. Die KI-Arbeit der EU schlägt sich bereits in internationalen Diskussionen nieder. Bei der Ausarbeitung der Ethik-Leitlinien bezog die Hochrangige Expertengruppe eine Reihe von Organisationen aus Drittländern und verschiedene Regierungsbeobachter ein. Gleichzeitig war die EU eng an der Entwicklung der ethischen Grundsätze für KI der OECD beteiligt[25]. Diese Grundsätze wurden anschließend von den G20 in ihrer Ministererklärung zu Handel und digitaler Wirtschaft vom Juni 2019 gebilligt.

Gleichzeitig weiß die EU sehr wohl, dass auch in anderen multilateralen Foren wie dem Europarat, der Organisation der Vereinten Nationen für Erziehung, Wissenschaft und Kultur (UNESCO), der Organisation für wirtschaftliche Zusammenarbeit und Entwicklung (OECD), der Welthandelsorganisation (WTO) und der Internationalen Fernmeldeunion (ITU) wichtige Arbeit zum Thema KI geleistet wird. Auf der Ebene der Vereinten Nationen ist die EU am Follow-Up zum Bericht der Hochrangigen Gruppe für digitale Zusammenarbeit beteiligt, die auch eine Empfehlung zu KI umfasst.

Die EU wird auch künftig sowohl mit gleich gesinnten Ländern als auch mit globalen Akteuren im KI-Bereich zusammenarbeiten – auf der Grundlage eines Konzepts, das auf Regeln und Werten der EU basiert (z. B. regulatorische Aufwärtskonvergenz, Zugang zu grundlegenden Ressourcen einschließlich Daten und Schaffung gleicher Wettbewerbsbedingungen). Die Kommission wird die Politik von Drittländern, die Datenströme beschränken, aufmerksam verfolgen und in bilateralen Verhandlungen sowie auf WTO-Ebene gegen ungerechtfertigte Beschränkungen vorgehen. Die Kommission ist überzeugt davon, dass die internationale Zusammenarbeit im KI-Bereich auf einem Ansatz beruhen muss, der die Achtung von Grundrechten und Menschenwürde, Pluralismus, Inklusion, Diskriminierungsfreiheit und den Schutz der Privatsphäre und personenbezogener Daten fördert[26], und es wird ihr ein Anliegen sein, ihre Werte in der ganzen Welt zu vermitteln[27]. Selbstverständlich kann die verantwortungsvolle Entwicklung und Nutzung von KI sowohl die Verwirklichung der Ziele für nachhaltige Entwicklung als auch die Agenda 2030 maßgeblich voranbringen.

5. EIN ÖKOSYSTEM FÜR VERTRAUEN: KI-REGULIERUNGSRAHMEN

Wie jede neue Technologie bringt auch KI sowohl Chancen als auch Risiken mit sich. Angesichts der Informationsasymmetrien in algorithmischen Entscheidungsprozessen fürchten Bürgerinnen und Bürger, ihre Rechte und Sicherheit nicht mehr verteidigen zu können, und Unternehmen sind wegen mangelnder Rechtssicherheit beunruhigt. KI kann zwar dazu beitragen, die Sicherheit der Bürgerinnen und Bürger zu schützen, und es ihnen ermöglichen, ihre Grundrechte wahrzunehmen, aber es besteht auch die Sorge, dass KI unbeabsichtigte Auswirkungen haben oder sogar für kriminelle Zwecke missbraucht werden kann. Auf diese Sorgen muss eingegangen werden. Abgesehen von fehlenden Investitionen und Kenntnissen ist mangelndes Vertrauen ein Haupthinderungsgrund für eine breitere Akzeptanz von KI.

[25] https://www.oecd.org/going-digital/ai/principles/.

[26] Im Rahmen des Partnerschaftsinstruments wird die Kommission ein mit 2,5 Mio. EUR dotiertes Projekt finanzieren, das die Zusammenarbeit mit gleich gesinnten Partnern erleichtern wird, um die KI-Ethik-Leitlinien der EU zu fördern und gemeinsame Grundsätze und operative Schlussfolgerungen zu verabschieden.

[27] Präsidentin Von der Leyen, Eine Union, die mehr erreichen will – Meine Agenda für Europa, Seite 17.

Deshalb legte die Kommission am 25. April 2018 eine KI-Strategie[28] vor, die sowohl verstärkte Investitionen in Forschung, Innovation und KI-Kapazitäten in der gesamten EU vorsieht als auch gleichzeitig den sozioökonomischen Aspekten Rechnung trägt. Sie verständigte sich mit den Mitgliedstaaten auf einen koordinierten Plan[29], um die Strategien abzustimmen. Ferner setzte die Kommission eine Hochrangige Expertengruppe ein, die im April 2019 Leitlinien für eine vertrauenswürdige KI[30] vorlegte.

Die Kommission legte eine Mitteilung[31] vor, in der sie die sieben Kernanforderungen der Expertengruppe begrüßte:

- Vorrang menschlichen Handelns und menschlicher Aufsicht
- Technische Robustheit und Sicherheit
- Privatsphäre und Datenqualitätsmanagement
- Transparenz
- Vielfalt, Nichtdiskriminierung und Fairness
- Gesellschaftliches und ökologisches Wohlergehen und
- Rechenschaftspflicht

Darüber hinaus enthalten die Leitlinien eine Bewertungsliste als praktische Hilfestellung für Unternehmen. Im zweiten Halbjahr 2019 haben mehr als 350 Einrichtungen diese Bewertungsliste getestet und Rückmeldungen übermittelt. Die Hochrangige Gruppe überarbeitet zurzeit ihre Leitlinien unter Berücksichtigung dieser Rückmeldungen und wird ihre Arbeit bis Juni 2020 abschließen. Eine zentrale Erkenntnis aus diesen Rückmeldungen ist, dass einige der Anforderungen bereits Eingang in geltende Rechts- und Verwaltungsvorschriften gefunden haben. Die Anforderungen in Bezug auf Transparenz, Rückverfolgbarkeit und Kontrolle durch den Menschen sind hingegen in den Rechtsvorschriften in vielen Wirtschaftszweigen noch nicht ausdrücklich abgedeckt.

Neben diesen unverbindlichen Leitlinien der Hochrangigen Expertengruppe und im Einklang mit den politischen Leitlinien der Präsidentin würde ein klarer europäischer Regulierungsrahmen das Vertrauen von Verbraucherinnen und Verbrauchern und Unternehmen in künstliche Intelligenz stärken und damit die Einführung der Technologie beschleunigen. Ein solcher Regulierungsrahmen sollte mit anderen Maßnahmen zur Förderung der Innovationskapazität und Wettbewerbsfähigkeit Europas in diesem Bereich im Einklang stehen. Er muss zudem optimale Ergebnisse für Gesellschaft, Umwelt und Wirtschaft und die Vereinbarkeit mit den Rechtsvorschriften, Grundsätzen und Werten der EU gewährleisten. Dies ist insbesondere in solchen Bereichen relevant, in denen Bürgerrechte unmittelbar betroffen sein könnten, z. B. im Falle von KI-Anwendungen für die Bereiche Strafverfolgung und Justiz.

Entwickler und Nutzer von KI unterliegen bereits europäischen Rechtsvorschriften über Grundrechte (z. B. Datenschutz, Schutz der Privatsphäre und Nichtdiskriminierung), Verbraucherschutz sowie Produktsicherheit und -haftung. Die Verbraucher erwarten die gleiche Sicherheit und die gleiche Achtung ihrer Rechte, unabhängig davon, ob ein Produkt oder System KI-gestützt ist oder nicht. Allerdings können bestimmte Besonderheiten der KI (z. B. die Opazität) die Anwendung und Durchsetzung dieser Rechtsvorschriften erschweren. Deshalb muss geprüft werden, ob die geltenden

[28] COM(2018)237.
[29] COM(2018)795.
[30] https://ec.europa.eu/futurium/en/ai-alliance-consultation/guidelines#Top
[31] COM(2019)168.

Rechtsvorschriften den KI-Risiken gewachsen sind und wirksam durchgesetzt werden können oder ob sie angepasst werden müssen bzw. neue Rechtsvorschriften erforderlich sind.

Da sich die KI so rasant weiterentwickelt, muss der Regulierungsrahmen Raum für weitere Entwicklungen lassen. Etwaige Änderungen sollten sich auf eindeutig festgestellte Probleme beschränken, für die es praktikable Lösungen gibt.

Die Mitgliedstaaten verweisen darauf, dass es gegenwärtig keinen einheitlichen europäischen Rahmen gibt. Die Datenethikkommission in Deutschland plädiert für ein fünfstufiges risikobasiertes Regulierungssystem, das von keiner Regulierung für die KI-Systeme mit dem geringsten Risiko bis hin zu einem vollständigen Verbot für die Systeme mit dem höchsten Risiko reichen würde. Dänemark hat gerade den Prototyp eines Ethiksiegels für Daten vorgestellt, und Malta hat eine freiwillige KI-Zertifizierung eingeführt. Wenn es der EU nicht gelingt, ein EU-weites Konzept vorzustellen, besteht die reale Gefahr einer Fragmentierung des Binnenmarkts, was den Zielen Vertrauen, Rechtssicherheit und Markteinführung abträglich wäre.

Ein solider europäischer Regulierungsrahmen für eine vertrauenswürdige KI wird alle europäischen Bürgerinnen und Bürger schützen und zur Schaffung eines reibungslos funktionierenden Binnenmarkts beitragen, im Interesse der Weiterentwicklung und Verbreitung von KI sowie der Stärkung der industriellen Basis Europas im Bereich KI.

A. PROBLEMSTELLUNG

KI kann viel Gutes bewirken, da sie z. B. Produkte und Verfahren sicherer macht, sie kann aber auch Schäden verursachen. Diese Schäden können sowohl materiell (Sicherheit und Gesundheit des Einzelnen, einschließlich Verlust von Menschenleben, Sachschäden) als auch immateriell (Verlust der Privatsphäre, Einschränkung des Rechts auf freie Meinungsäußerung, Menschenwürde, Diskriminierung z. B. beim Zugang zu Beschäftigung) sein und sich in einer Vielzahl von Risiken manifestieren. Der Schwerpunkt eines Regulierungsrahmens sollte auf der Frage liegen, wie die Gefahr potenzieller und vor allem der schwersten Schäden minimiert werden kann.

Die größten Risiken in Verbindung mit der Nutzung von KI betreffen die Anwendung von Vorschriften zum Schutz von Grundrechten (einschließlich Datenschutz und Schutz der Privatsphäre und Nichtdiskriminierung) sowie Fragen der Sicherheit[32] und Haftung.

Risiken für die Grundrechte, einschließlich des Schutzes personenbezogener Daten und der Privatsphäre und Nichtdiskriminierung

Infolge der Nutzung von KI können die Werte, auf denen die EU gründet, beeinträchtigt und Grundrechte[33] verletzt werden. Dies gilt auch für das Recht auf freie Meinungsäußerung, die Versammlungsfreiheit, die Achtung der Menschenwürde, die Nichtdiskriminierung ungeachtet des Geschlechts, der Rasse oder der ethnischen Herkunft, der religiösen Überzeugung oder Weltanschauung, einer Behinderung, des Alters oder der sexuellen Ausrichtung, den Schutz personenbezogener Daten und des Privatlebens[34], das Recht auf einen wirksamen gerichtlichen

[32] Dazu zählen auch Cybersicherheitsaspekte, Fragen in Verbindung mit KI-Anwendungen in kritischen Infrastrukturen oder mit dem Missbrauch von KI.

[33] Eine Studie im Auftrag des Europarates zeigt, dass eine große Zahl von Grundrechten durch den Einsatz von KI beeinträchtigt werden könnte, https://rm.coe.int/algorithms-and-human-rights-en-rev/16807956b5.

[34] Die Datenschutz-Grundverordnung und die e-Datenschutzrichtlinie (neue e-Datenschutzverordnung im Annahmeverfahren) gehen zwar auf diese Risiken ein, doch u. U. müsste untersucht werden, ob KI-Systeme zusätzliche

Rechtsbehelf und ein faires Verfahren sowie den Verbraucherschutz. Diese Risiken können das Ergebnis von Fehlern in der Gestaltung der KI-Systeme sein (auch hinsichtlich der Kontrolle durch den Menschen) oder von Fehlern bei der Verwendung von Daten, wenn etwaige Verzerrungen nicht korrigiert wurden (z. B. wenn das System nur mit Daten von Männern trainiert wird, was zu suboptimalen Ergebnissen für Frauen führt).

KI kann viele Funktionen übernehmen, die zuvor nur vom Menschen wahrgenommen werden konnten. Infolgedessen werden Bürgerinnen und Bürger und juristische Personen zunehmend von Maßnahmen und Entscheidungen betroffen, die von oder mithilfe von KI-Systemen gefällt werden und zuweilen schwer nachvollziehbar sind oder kaum wirksam angefochten werden könnten. Darüber hinaus bietet KI immer mehr Möglichkeiten, die täglichen Gewohnheiten von Menschen zu erfassen und zu analysieren. So besteht z. B. potenziell die Gefahr, dass KI – unter Verstoß gegen die Datenschutz- und andere Vorschriften der EU – von staatlichen Behörden oder anderen Stellen zur Massenüberwachung oder von Arbeitgebern zur Überwachung des Verhaltens ihrer Angestellten genutzt werden. Durch die Analyse großer Datenmengen und die Feststellung von Verbindungen zwischen ihnen kann KI auch dazu genutzt werden, Daten von Personen gezielt zurückzuverfolgen und zu de-anonymisieren, wodurch neue Risiken für den Schutz personenbezogener Daten entstehen, selbst wenn die Datensätze an sich keine personenbezogenen Daten enthalten. KI wird auch von Online-Mittlern genutzt, um Informationen für ihre Nutzer zu priorisieren und Inhalte zu moderieren. Dabei können die verarbeiteten Daten, die Art und Weise, in der die Anwendungen ausgelegt wurden, und beschränkte Möglichkeiten für ein Eingreifen des Menschen auf Kosten des Rechts auf freie Meinungsäußerung, des Schutzes personenbezogener Daten, der Privatsphäre und politischer Freiheiten gehen.

Bestimmte KI-Algorithmen können, wenn sie zur Vorhersage der Rückfälligkeit von Straftätern genutzt werden, aufgrund von Geschlecht oder Rasse diskriminieren; sie weisen unterschiedliche Rückfälligkeitswahrscheinlichkeiten für Männer und Frauen oder für In- und Ausländer aus. *Quelle: Tolan S., Miron M., Gomez E. und Castillo C. „Why Machine Learning May Lead to Unfairness: Evidence from Risk Assessment for Juvenile Justice in Catalonia", Preis für die beste Arbeit, Internationale Konferenz über KI und Recht, 2019.*

Bestimmte KI-Programme für die Gesichtserkennung diskriminieren aufgrund von Geschlecht oder Rasse, weil ihre Fehlerquote bei der Bestimmung des Geschlechts im Falle von hellhäutigen Männern gering, im Falle von dunkelhäutigen Frauen hingegen hoch ist. Quelle: *Joy Buolamwini, Timnit Gebru; Proceedings of the 1st Conference on Fairness, Accountability and Transparency, PMLR 81:77-91, 2018.*

Vorurteile und Diskriminierung können in allen gesellschaftlichen und wirtschaftlichen Tätigkeitsfeldern auftreten. Die Entscheidungsfindung des Menschen ist nicht immun gegen Fehler und Voreingenommenheiten. Aber in KI-Systemen könnten die gleichen Voreingenommenheiten eine viel größere Wirkung entfalten und ohne die sozialen Kontrollmechanismen, die das menschliche Verhalten regeln, viele Menschen beeinträchtigen und diskriminieren[35]. Dies kann auch geschehen,

Risiken bergen. Die Kommission wird die Anwendung der Datenschutz-Grundverordnung kontinuierlich überwachen und bewerten.

[35] Der Beratende Ausschuss der Kommission für die Chancengleichheit von Frauen und Männern erarbeitet zurzeit eine „Stellungnahme zur Künstlichen Intelligenz", in der unter anderem die Auswirkungen der KI auf die Gleichstellung der Geschlechter analysiert werden und die voraussichtlich Anfang 2020 angenommen wird. In der Strategie der EU für die

wenn das KI-System „lernt“, während es angewendet wird. In solchen Fällen resultieren die Risiken, wenn dies in der Entwurfsphase nicht hätte verhindert oder vorhergesehen werden können, nicht aus Fehlern in der ursprünglichen Auslegung des Systems, sondern aus den praktischen Folgen der Korrelationen oder Muster, die das System in großen Datensätzen identifiziert.

Die besonderen Merkmale vieler KI-Technologien wie Opazität („Blackbox-Effekt“), Komplexität, Unvorhersehbarkeit und teilautonomes Verhalten können die Prüfung der Vereinbarkeit und die wirksame Durchsetzung von EU-Rechtsvorschriften zum Schutz der Grundrechte erschweren. Strafverfolgungsbehörden und Betroffene können u. U. nicht nachvollziehen, wie eine bestimmte unter Einsatz von KI getroffene Entscheidung gefällt wurde, und somit auch nicht verifizieren, ob die einschlägigen Vorschriften eingehalten wurden. Natürliche wie juristische Personen könnten in Fällen, in denen sich solche Entscheidungen nachteilig auf sie auswirken, beim effektiven Zugang zur Justiz auf Schwierigkeiten stoßen.

Risiken für die Sicherheit und das wirksame Funktionieren der Haftungsregelung

KI-Technologien können neue Sicherheitsrisiken für die Nutzer mit sich bringen, wenn sie in Produkte und Dienstleistungen eingebettet sind. So ist beispielsweise denkbar, dass ein autonomes Fahrzeug aufgrund eines Fehlers in der Objekterkennungstechnik einen Gegenstand auf der Straße falsch identifiziert und einen Unfall mit Verletzungen und Sachschäden verursacht. Wie bei den Risiken im Bereich der Grundrechte können diese Risiken durch Fehler in der Gestaltung der KI-Technologie bedingt sein oder durch Probleme bei der Verfügbarkeit und der Qualität von Daten bzw. anderen Problemen, die sich aus dem Maschinellen Lernen ergeben. Einige dieser Risiken sind zwar nicht auf KI-gestützte Produkte und Dienstleistungen beschränkt, allerdings kann der Einsatz von KI die Risiken erhöhen oder verschärfen.

Wenn es keine klaren Sicherheitsvorschriften in Bezug auf diese Risiken gibt, kann dies neben den Risiken für die betroffenen Personen auch zu Rechtsunsicherheit für Unternehmen führen, die KI-gestützte Produkte in der EU vermarkten. Marktüberwachungs- und Strafvollzugsbehörden können in eine Situation kommen, in der sie nicht wissen, ob sie tätig werden können, weil ihnen keine entsprechenden Befugnisse erteilt wurden bzw. weil sie nicht über die geeigneten technischen Kapazitäten zur Inspektion dieser Systeme verfügen[36]. Mangelnde Rechtssicherheit kann somit zu einer Senkung des Sicherheitsniveaus führen und die Wettbewerbsfähigkeit europäischer Unternehmen beinträchtigen.

Treten Sicherheitsrisiken tatsächlich auf, ist es aufgrund des Fehlens klarer Anforderungen und der oben genannten Merkmale der KI-Technologien schwierig, potenziell problematische Entscheidungen, die unter Einbeziehung von KI-Systemen getroffen wurden, zurückzuverfolgen. Dadurch kann es für

Gleichstellung der Geschlechter (2020-2024) wird der Zusammenhang zwischen KI und der Gleichstellung der

Nach der Produkthaftungsrichtlinie haften Hersteller für Schäden, die durch fehlerhafte Produkte verursacht werden. Im Falle KI-gestützter Systeme wie z. B. bei autonomen Fahrzeugen kann es jedoch schwierig sein, einen Produktfehler, den entstandenen Schaden und den Kausalzusammenhang zwischen diesen beiden nachzuweisen. Darüber hinaus besteht eine gewisse Unsicherheit darüber, wie und in welchem Umfang die Produkthaftungsrichtlinie auf bestimmte Arten von Mängeln Anwendung findet, z. B. wenn diese auf Schwächen bei der Cybersicherheit des Produkts zurückzuführen sind.

denen das Risiko nicht mit dem Produkt als solchem zusammenhängt.

Personen, die einen Schaden erlitten haben, schwer werden, eine Entschädigung nach dem geltenden EU- und nationalen Haftungsrecht zu erhalten[37].

Daher ist die bereits in Bezug auf die Grundrechte erwähnte Schwierigkeit, potenziell problematische Entscheidungen von KI-Systemen zurückzuverfolgen, auch bei Sicherheits- und Haftungsfragen gegeben. So könnten möglicherweise Geschädigte z. B. keinen Zugang zu Nachweisen haben, die zur Beweisführung in einem Gerichtsverfahren erforderlich sind, und ihnen stehen u. U. weniger Rechtsbehelfe zur Verfügung als in Fällen, in denen der Schaden durch herkömmliche Technologien verursacht wird. Diese Risiken werden mit zunehmender Verbreitung von KI weiter zunehmen.

B. MÖGLICHE ANPASSUNGEN DES BESTEHENDEN EU-RECHTSRAHMENS UNTER BERÜCKSICHTIGUNG VON KI

Ein umfangreicher Bestand an EU-Produktsicherheits- und Produkthaftungsvorschriften [38], einschließlich sektorspezifischer Bestimmungen, die ferner durch nationale Rechtsvorschriften und einschlägige Normen ergänzt werden, ist für eine Reihe neuer KI-Anwendungen relevant und potenziell auf diese anwendbar.

Was den Schutz der Grundrechte und der Verbraucherrechte angeht, so umfasst der EU-Rechtsrahmen Vorschriften wie die Richtlinie zur Anwendung des Gleichbehandlungsgrundsatzes ohne Unterschied der Rasse oder der ethnischen Herkunft[39], die Richtlinie über die Gleichbehandlung in Beschäftigung und Beruf [40], die Richtlinien zur Gleichbehandlung von Männern und Frauen in Arbeits- und Beschäftigungsfragen und beim Zugang zu Gütern und Dienstleistungen [41], eine Reihe von Verbraucherschutzvorschriften[42] sowie Vorschriften zum Schutz personenbezogener Daten und der Privatsphäre, insbesondere die Datenschutz-Grundverordnung und andere sektorspezifische Rechtsvorschriften mit Bestimmungen zum Schutz personenbezogener Daten, wie die Richtlinie zum Datenschutz bei der Strafverfolgung [43]. Darüber hinaus werden ab 2025 die Vorschriften zur Barrierefreiheit von Produkten und Dienstleistungen gelten, die in dem europäischen Rechtsakt zur Barrierefreiheit festgelegt wurden[44]. Darüber hinaus müssen die Grundrechte bei der Umsetzung anderer EU-Rechtsvorschriften, u. a. in den Bereichen Finanzdienstleistungen, Migration und Verantwortung von Online-Vermittlern, geachtet werden.

Auch wenn die EU-Rechtsvorschriften unbeschadet des Einsatzes von KI grundsätzlich weiterhin in vollem Umfang anwendbar sind, ist es wichtig zu bewerten, ob sie angemessen durchgesetzt werden können, um den von KI-Systemen ausgehenden Risiken zu begegnen, oder ob manche Rechtsinstrumente angepasst werden müssen.

---

[37] Die Auswirkungen von KI, dem Internet der Dinge und anderen digitalen Technologien auf die Sicherheits- und Haftungsvorschriften werden in dem Bericht der Kommission, der ebenfalls zusammen mit diesem Weißbuch vorgelegt wird, analysiert.

[38] Der EU-Rechtsrahmen für die Produktsicherheit umfasst als Sicherheitsnetz die Richtlinie über die allgemeine Produktsicherheit (Richtlinie 2001/95/EG) sowie ferner eine Reihe sektorspezifischer Vorschriften für verschiedene Produktkategorien – von Maschinen, Flugzeugen und Autos bis hin zu Spielzeug und Medizinprodukten –, um ein hohes Maß an Gesundheit und Sicherheit zu gewährleisten. Die Produkthaftungsbestimmungen werden durch verschiedene Systeme der zivilrechtlichen Haftung für Schäden, die durch Produkte oder Dienstleistungen verursacht werden, ergänzt.

[39] Richtlinie 2000/43/EG.

[40] Richtlinie 2000/78/EG.

[41] Richtlinie 2004/113/EG. Richtlinie 2006/54/EG.

[42] Beispielsweise die Richtlinie über unlautere Geschäftspraktiken (Richtlinie 2005/29/EG) und die Richtlinie über die Verbraucherrechte (Richtlinie 2011/83/EG).

[43] Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr.

[44] Richtlinie (EU) 2019/882 über die Barrierefreiheitsanforderungen für Produkte und Dienstleistungen.

Beispielsweise sind die Wirtschaftsakteure nach wie vor uneingeschränkt dafür verantwortlich, dafür zu sorgen, dass die bestehenden Verbraucherschutzvorschriften beim Einsatz von KI eingehalten werden; algorithmenbasierte Auswertungen des Verbraucherverhaltens, bei denen gegen bestehende Vorschriften verstoßen wird, sind nicht zulässig und Verstöße werden entsprechend geahndet.

Die Kommission ist der Auffassung, dass der Rechtsrahmen verbessert werden könnte, um den folgenden Risiken und Situationen zu begegnen:

- *Wirksame Anwendung und Durchsetzung bestehender Rechtsvorschriften der EU und der Mitgliedstaaten:* Die wesentlichen Merkmale der KI bringen Herausforderungen für die ordnungsgemäße Anwendung und Durchsetzung der Rechtsvorschriften der EU und der Mitgliedstaaten mit sich. Der Mangel an Transparenz (Opazität der KI) macht es schwer, etwaige Verstöße gegen Rechtsvorschriften zu aufzudecken und nachzuweisen, dies betrifft auch Bestimmungen zum Schutz der Grundrechte, zur Lösung von Haftungsfragen und über die Voraussetzungen für die Geltendmachung von Schadenersatz. Um eine wirksame Anwendung und Durchsetzung zu gewährleisten, kann es daher erforderlich sein, die bestehenden Rechtsvorschriften in manchen Bereichen, z. B. in Bezug auf Haftungsfragen, anzupassen oder zu präzisieren, wie in dem Bericht, der diesem Weißbuch beigefügt ist, näher ausgeführt wird.

- *Einschränkung des Anwendungsbereichs bestehender EU-Rechtsvorschriften:* Bei den EU-Produktsicherheitsvorschriften liegt ein wesentlicher Schwerpunkt auf dem Inverkehrbringen von Produkten. Nach den EU-Produktsicherheitsvorschriften muss Software, wenn sie Teil des Endprodukts ist, den einschlägigen Produktsicherheitsvorschriften entsprechen, hingegen ist die Frage, ob eigenständige Software von den EU-Produktsicherheitsvorschriften erfasst wird – abgesehen von einigen Sektoren, für die es explizite Vorschriften gibt[45] – noch zu klären. Die derzeit geltenden allgemeinen Sicherheitsvorschriften sind auf Produkte anwendbar und gelten nicht für Dienstleistungen, und somit grundsätzlich auch nicht für Dienstleistungen, die auf KI-Technologien basieren (z. B. Gesundheitsdienstleistungen, Finanzdienstleistungen und Verkehrsdienstleistungen).

- *Veränderliche Funktionen der KI-Systeme:* Wenn Software, einschließlich KI, in Produkte eingebunden wird, kann dies die Funktionsweise dieser Produkte und Systeme im weiteren Verlauf ihres Lebenszyklus verändern. Dies gilt insbesondere für Systeme, die häufige Software-Updates erfordern oder auf Maschinellem Lernen beruhen. Dies kann zum Entstehen neuen Risiken führen, die zum Zeitpunkt des Inverkehrbringens des Systems nicht bestanden. Diese Risiken werden in den geltenden Rechtsvorschriften, die sich in erster Linie auf Sicherheitsrisiken konzentrieren, die zum Zeitpunkt des Inverkehrbringens bestehen, nicht angemessen berücksichtigt.

- *Unsicherheit hinsichtlich der Aufteilung der Zuständigkeiten zwischen den verschiedenen Wirtschaftsteilnehmern in der Lieferkette:* Generell trägt nach den EU-Produktsicherheitsvorschriften der Hersteller des in Verkehr gebrachten Produkts die Verantwortung für Produktsicherheit, einschließlich aller Komponenten, die z. B. auch KI-Systeme umfassen können. Unklarheiten können bei den Vorschriften jedoch beispielsweise

[45] So gilt beispielsweise Software, die vom Hersteller für medizinische Zwecke bestimmt ist, als Medizinprodukt im Sinne der Verordnung über Medizinprodukte (Verordnung (EU) 2017/745).

dann aufkommen, wenn KI integriert wird, nachdem das Produkt von einer Partei in Verkehr gebracht wurde, die nicht der Hersteller ist. Darüber hinaus wird im EU-Produkthaftungsrecht die Haftung der Hersteller geregelt, während die Haftung anderer in der Lieferkette in den nationalen Haftungsregeln geregelt wird.

- *Änderungen des Sicherheitskonzepts:* Der Einsatz von KI in Produkten und Dienstleistungen kann zu Risiken führen, die derzeit in den EU-Rechtsvorschriften nicht explizit erfasst sind. Diese Risiken können beispielsweise mit Cyberbedrohungen, Gefährdungen der persönlichen Sicherheit (z. B. im Zusammenhang mit neuen Anwendungen von KI z. B. für Haushaltsgeräte) oder mit Risiken verbunden sein, die sich aus dem Verlust der Konnektivität ergeben. Diese Risiken können zum Zeitpunkt des Inverkehrbringens der Produkte bestehen oder infolge von Software-Updates oder eigenständigem Lernen bei der Verwendung des Produkts entstehen. Die EU sollte die ihr zur Verfügung stehenden Instrumente umfassend nutzen, um die verfügbare Faktengrundlage zu potenziellen Risiken im Zusammenhang mit KI-Anwendungen zu verbessern, und dabei auch auf die Erfahrungen der EU-Cybersicherheitsagentur (ENISA) bei der Bewertung Bedrohungslandschaft im Bereich der KI zurückgreifen.

Wie bereits erwähnt, prüfen mehrere Mitgliedstaaten bereits Optionen, wie die durch KI geschaffenen Herausforderungen in nationalen Rechtsvorschriften angegangen werden können. Dies birgt die Gefahr einer Fragmentierung des Binnenmarkts. Das Bestehen unterschiedlicher nationaler Vorschriften dürfte Hemmnisse für Unternehmen schaffen, die KI-Systeme im Binnenmarkt verkaufen und betreiben wollen. Ein gemeinsames Konzept auf EU-Ebene würde es europäischen Unternehmen ermöglichen, von einem reibungslosen Zugang zum Binnenmarkt zu profitieren, und ihre Wettbewerbsfähigkeit auf den globalen Märkten stärken.

Bericht über die Auswirkungen von Künstlicher Intelligenz, des Internets der Dinge und der Robotik auf Sicherheits- und Haftungsfragen

In dem zusammen mit diesem Weißbuch vorgelegten Bericht wird der einschlägige Rechtsrahmen analysiert. Dabei wird der Frage nachgegangen, wo es Unsicherheiten hinsichtlich der Anwendung dieses Rechtsrahmens wegen der spezifischen Risiken gibt, die von KI-Systemen und anderen digitalen Technologien ausgehen.

Der Bericht kommt zu dem Schluss, dass die geltenden Produktsicherheitsvorschriften bereits ein erweitertes Konzept des Schutzes vor allen Arten von Risiken, die von dem Produkt je nach seiner Verwendung ausgehen, unterstützen. Um größere Rechtssicherheit zu schaffen, könnten jedoch Bestimmungen aufgenommen werden, die sich ausdrücklich auf neue Risiken im Zusammenhang mit den neuen digitalen Technologien beziehen.

- Das autonome Verhalten bestimmter KI-Systeme während ihres Lebenszyklus kann zu erheblichen sicherheitsrelevanten Änderungen der Produkte führen, die eine neue Risikobewertung erforderlich machen können. Darüber hinaus kann es nötig sein, als Schutzmaßnahme die Kontrolle durch den Menschen ab der Phase der Auslegung und während des gesamten Lebenszyklus der KI-Produkte und -Systeme vorzusehen.
- Explizite Verpflichtungen für Hersteller könnten ggf. auch in Bezug auf psychische Sicherheitsrisiken für Anwender in Erwägung gezogen werden (z. B. bei Zusammenarbeit mit humanoiden Robotern).
- Die Produktsicherheitsvorschriften der Union könnten sowohl spezifische Anforderungen vorsehen, um die Sicherheitsrisiken auszuräumen, die von fehlerhaften Daten in der Phase der Auslegung ausgehen, als auch Mechanismen, mit denen sichergestellt wird, dass die Qualität der Daten während der gesamten Nutzung der KI-Produkte und -Systeme aufrechterhalten wird.
- Die Frage der Opazität von auf Algorithmen basierenden Systemen könnte durch die Festlegung von Transparenzanforderungen angegangen werden.
- Im Falle eigenständiger Software, die als solche in Verkehr gebracht wird oder nach dem Inverkehrbringen in ein Produkt heruntergeladen wird, müssen die bestehenden Vorschriften möglicherweise angepasst und präzisiert werden, wenn die Software sicherheitsrelevante Auswirkungen hat.
- Angesichts der zunehmenden Komplexität der Lieferketten bei neuen Technologien könnten auch Bestimmungen, die eine Zusammenarbeit zwischen den Wirtschaftsteilnehmern in der Lieferkette und den Nutzern verbindlich vorschreiben, zur Rechtssicherheit beitragen.

Die Merkmale neuer digitaler Technologien wie KI, Internet der Dinge und Robotik können bestimmte Aspekte der bestehenden Haftungsrahmen infrage stellen und deren Wirksamkeit verringern. Aufgrund mancher dieser Eigenschaften könnte es schwierig werden, den Schaden zu einer Person zurückzuverfolgen, was nach den meisten nationalen Vorschriften erforderlich wäre, um verschuldensabhängige Ansprüche geltend zu machen. Dies könnte die Kosten für die Geschädigten erheblich erhöhen und dazu führen, dass Haftungsansprüche gegenüber anderen Akteuren als den Herstellern schwer geltend zu machen oder zu belegen sind.

- Personen, die infolge der Nutzung von KI-Systemen einen Schaden erlitten haben, müssen das gleiche Schutzniveau genießen wie Personen, die durch andere Technologien geschädigt wurden. Gleichzeitig muss genug Raum für die Weiterentwicklung technologischer Innovationen bleiben.
- Alle Optionen, die zur Erreichung dieses Ziels ins Auge gefasst werden – einschließlich möglicher Änderungen der Produkthaftungsrichtlinie und einer etwaigen weiteren gezielten Harmonisierung der nationalen Haftungsvorschriften - sollten sorgfältig geprüft werden. So bittet die Kommission beispielsweise um Stellungnahmen zu der Frage, ob und in welchem Umfang es erforderlich sein könnte, die Folgen der Komplexität abzumildern, indem für Schäden, die durch den Betrieb von KI-Anwendungen verursacht werden, die in den nationalen Haftungsvorschriften vorgesehenen Beweislastregeln geändert werden.

Angesichts der vorstehenden Ausführungen kommt die Kommission zu dem Schluss, dass – zusätzlich

zu den möglichen Anpassungen der bestehenden Rechtsvorschriften — möglicherweise neue, speziell auf KI ausgerichtete Rechtsvorschriften erforderlich sind, um den Rechtsrahmen der EU an die derzeitigen und erwarteten technologischen und kommerziellen Entwicklungen anzupassen.

C. ANWENDUNGSBEREICH EINES KÜNFTIGEN EU-RECHTSRAHMENS

Eine zentrale Frage für den künftigen spezifischen Rechtsrahmen für KI ist die Festlegung des Anwendungsbereichs. Die Arbeitshypothese lautet, dass der Rechtsrahmen für Produkte und Dienstleistungen gelten soll, bei denen KI zum Einsatz kommt. KI sollte daher für die Zwecke dieses Weißbuchs sowie für alle weiteren künftigen politische Initiativen klar definiert werden.

In ihrer Mitteilung über KI für Europa legte die Kommission eine erste Definition von KI vor[46]. Diese Definition wurde von der Hochrangigen Expertengruppe weiter präzisiert[47].

In jedem neuen Rechtsinstrument muss die KI-Definition einerseits flexibel genug sein, damit dem technischen Fortschrift Rechnung getragen werden kann, und andererseits präzise, um die erforderliche Rechtssicherheit zu gewährleisten.

Für die Zwecke dieses Weißbuchs sowie etwaiger künftiger Diskussionen über politische Initiativen erscheint es wichtig, Klarheit in Bezug auf die wichtigsten Elemente, aus denen sich KI zusammensetzt, d. h. „Daten“ und „Algorithmen“, zu schaffen. KI kann in Hardware integriert sein. Bei Techniken des Maschinellen Lernens, einer Untergruppe der KI, werden Algorithmen so trainiert, dass sie auf der Grundlage eines Datensatzes bestimmte Muster ableiten können, um zu ermitteln, welche Handlungsschritte zur Erreichung eines bestimmten Ziels erforderlich sind. Algorithmen können auch weiterlernen, während sie im Einsatz sind. Während KI-basierte Produkte eigenständig handeln können, indem sie ihre Umgebung wahrnehmen und ohne dass sie vorab festgelegte Anweisungen befolgen, wird ihr Verhalten von den Produktentwicklern in breiten Zügen festgelegt und auch eingeschränkt. Der Mensch bestimmt und programmiert die Ziele, die ein KI-System erreichen soll.

> Beim autonomen Fahren beispielsweise verwendet der Algorithmus in Echtzeit die Fahrzeugdaten (Geschwindigkeit, Motorverbrauch, Stoßdämpfer usw.) und die Daten der Sensoren, die die gesamte Umgebung des Fahrzeugs (Straße, Schilder, andere Fahrzeuge, Fußgänger usw.) abtasten, um abzuleiten, welche Richtung, Beschleunigung und Geschwindigkeit das Fahrzeug wählen sollte, um einen bestimmten Zielort zu erreichen. Anhand der Beobachtungsdaten nimmt der Algorithmus Anpassungen an die Straßensituation und an die äußeren Bedingungen, einschließlich des Verhaltens anderer Fahrer, vor und leitet daraus das angenehmste und sicherste Fahrverhalten ab.

[46] COM(2018) 237 final, S. 1: „Künstliche Intelligenz (KI) bezeichnet Systeme mit einem „intelligenten“ Verhalten, die ihre Umgebung analysieren und mit einem gewissen Grad an Autonomie handeln, um bestimmte Ziele zu erreichen.
KI-basierte Systeme können rein softwaregestützt in einer virtuellen Umgebung arbeiten (z. B. Sprachassistenten, Bildanalysesoftware, Suchmaschinen, Sprach- und Gesichtserkennungssysteme), aber auch in Hardware-Systeme eingebettet sein (z. B. moderne Roboter, autonome Pkw, Drohnen oder Anwendungen des ‚Internet der Dinge‘).“

[47] Hochrangige Expertengruppe, Eine Definition der KI, S. 8: „Künstliche-Intelligenz-(KI)-Systeme sind vom Menschen entwickelte Software- (und möglicherweise auch Hardware-) Systeme, die in Bezug auf ein komplexes Ziel auf physischer oder digitaler Ebene agieren, indem sie ihre Umgebung durch Datenerfassung wahrnehmen, die gesammelten strukturierten oder unstrukturierten Daten interpretieren, Schlussfolgerungen daraus ziehen oder die aus diesen Daten abgeleiteten Informationen verarbeiten und über die geeignete(n) Maßnahme(n) zur Erreichung des vorgegebenen Ziels entscheiden. KI-Systeme können entweder symbolische Regeln verwenden oder ein numerisches Modell erlernen, und sind auch in der Lage, die Auswirkungen ihrer früheren Handlungen auf die Umgebung zu analysieren und ihr Verhalten entsprechend anzupassen.“

Die EU verfügt über einen strengen Rechtsrahmen, um unter anderem den Verbraucherschutz zu gewährleisten, gegen unlautere Geschäftspraktiken vorzugehen und die personenbezogenen Daten und die Privatsphäre der Bürgerinnen und Bürger zu schützen. Darüber hinaus enthält der Besitzstand spezifische Vorschriften für einzelne Sektoren (z. B. Gesundheitswesen und Verkehr). Diese bestehenden EU-Rechtsvorschriften werden auch weiterhin für KI gelten, allerdings sind möglicherweise bestimmte Aktualisierungen erforderlich, um dem digitalen Wandel und dem Einsatz von KI Rechnung zu tragen (siehe Abschnitt B). Folglich werden die Aspekte, die bereits durch bestehende horizontale oder sektorspezifische Rechtsvorschriften abgedeckt sind(z. B. in den Rechtsvorschriften über Medizinprodukte [48] oder Verkehrssysteme), weiterhin durch diese Rechtsvorschriften geregelt.

Grundsätzlich sollte der neue Rechtsrahmen für KI zielführend und nicht übermäßig präskriptiv sein, um zu vermeiden, dass er insbesondere für KMU einen unverhältnismäßigen Aufwand verursacht. Um dieses Gleichgewicht zu erreichen, sollte nach Ansicht der Kommission ein risikobasierter Ansatz verfolgt werden.

Ein risikobasierter Ansatz ist wichtig, um die Verhältnismäßigkeit des regulatorischen Eingreifens zu gewährleisten. Allerdings bedarf es hier klarer Kriterien, um zwischen den verschiedenen KI-Anwendungen differenzieren zu können, insbesondere in Bezug auf die Frage, ob sie ein „hohes Risiko“ darstellen oder nicht[49]. Es sollte für alle Beteiligten klar und leicht verständlich sein, was unter einer unter einer KI-Anwendung mit hohem Risiko zu verstehen ist. Allerdings gelten auch für KI-Anwendungen, die nicht als Anwendung mit hohem Risiko eingestuft werden, uneingeschränkt die bereits bestehenden EU-Vorschriften.

Die Kommission ist der Auffassung, dass bei der Einstufung einer KI-Anwendung als Anwendung mit hohem Risiko generell berücksichtigt werden sollte, was auf dem Spiel steht, wobei zu prüfen ist, ob sowohl der Sektor als auch die beabsichtigte Verwendung erhebliche Risiken bergen, insbesondere unter den Gesichtspunkten Sicherheit, Verbraucherrechte und Grundrechte. Eine KI-Anwendung sollte insbesondere dann als Anwendung mit hohem Risiko angesehen werden, wenn sie die beiden folgenden Kriterien erfüllt:

- Erstens wird die KI-Anwendung in einem Sektor eingesetzt, in dem aufgrund der Art der typischen Tätigkeiten mit erheblichen Risiken zu rechnen ist. Mit diesem ersten Kriterium wird sichergestellt, dass die regulatorischen Eingriffe auf diejenigen Bereiche ausgerichtet sind, in denen das Eintreten von Risiken generell am wahrscheinlichsten ist. Die betreffenden Sektoren sollten in dem neuen Rechtsrahmen ausdrücklich genannt und erschöpfend aufgelistet werden. Beispiele wären hier die Sektoren Gesundheitswesen, Verkehr, Energie sowie Teile des öffentlichen Sektors [50] . Die Liste sollte regelmäßig überprüft und erforderlichenfalls entsprechend den einschlägigen Entwicklungen in der Praxis geändert werden;

[48] So gibt es beispielsweise bei KI-Systemen unterschiedliche Sicherheitserwägungen und rechtliche Auswirkungen je nachdem, ob es sich um Systeme handelt, die fachspezifische medizinische Informationen für Ärzte bereitstellen, Systeme, die medizinische Informationen direkt für Patienten bereitstellen, oder um Systeme, die selbst medizinische Aufgaben direkt am Patienten ausführen. Die Kommission untersucht zurzeit diese besonderen Herausforderungen, die sich speziell im Gesundheitswesen in Bezug auf Sicherheits- und Haftungsfragen stellen.

[49] In den EU-Rechtsvorschriften können „Risiken“ je nach dem betreffenden Bereich, z. B. Produktsicherheit, anders eingestuft werden als hier beschrieben.

[50] Der öffentliche Sektor könnte Bereiche wie Asyl, Migration, Grenzkontrollen und Justizwesen, soziale Sicherheit und Arbeitsverwaltungen umfassen.

- Zweites Kriterium ist, ob die KI-Anwendung in dem betreffenden Sektor so eingesetzt wird, dass mit erheblichen Risiken zu rechnen ist. Dieses zweite Kriterium spiegelt die Erkenntnis wider, dass nicht jede Nutzung von KI in den ausgewählten Sektoren notwendigerweise mit erheblichen Risiken verbunden ist. Hier kann das Gesundheitswesen im Allgemeinen zwar tatsächlich ein relevanter Sektor sein, jedoch dürfte ein Fehler in einem Terminvereinbarungssystem eines Krankenhauses in der Regel keine so erheblichen Risiken mit sich bringen, dass ein gesetzgeberisches Eingreifen gerechtfertigt wäre. Zur Bewertung des Risikos einer bestimmten Verwendung könnten die Auswirkungen auf die betroffenen Parteien betrachtet werden. So könnte zum Beispiel unterschieden werden zwischen KI-Anwendungen, die rechtliche oder ähnlich erhebliche Auswirkungen auf die Rechte einer natürlichen Person oder eines Unternehmens haben können, Anwendungen, von denen Verletzungs- oder Lebensgefahr oder die Gefahr eines erheblichen materiellen oder immateriellen Schadens ausgeht, und Anwendungen, deren Auswirkungen von natürlichen oder juristischen Personen realistischerweise nicht vermieden werden können.

Mit diesen beiden kumulativen Kriterien würde sichergestellt, dass der Anwendungsbereich des Rechtsrahmens zielgerichtet ist und Rechtssicherheit bietet. Die verbindlichen Anforderungen des neuen Rechtsrahmens für KI (s. u. Abschnitt D) würden grundsätzlich nur für diejenigen Anwendungen gelten, die nach diesen beiden kumulativen Kriterien als Anwendungen mit hohem Risiko eingestuft wurden.

Ungeachtet der vorstehenden Ausführungen kann es auch Ausnahmefälle geben, in denen aufgrund der immanenten Risiken der Einsatz von KI-Anwendungen für bestimmte Zwecke grundsätzlich – d. h. unabhängig von dem betreffenden Sektor – als hochriskant einzustufen ist, und in denen die nachstehenden Anforderungen dennoch gelten würden [51] . Zur Veranschaulichung könnten insbesondere folgende Überlegungen angestellt werden:

- Angesichts ihrer Bedeutung für den Einzelnen und unter Berücksichtigung des EU-Besitzstands zur Gleichbehandlung im Beschäftigungsbereich würden KI-Anwendungen, die bei Einstellungsverfahren sowie in Situationen eingesetzt werden, die sich auf die Rechte von Arbeitnehmern auswirken, ausnahmslos als Anwendungen mit hohem Risiko eingestuft, sodass die nachstehenden Anforderungen stets gelten würden. Ferner könnten hier spezifische Anwendungen in Betracht gezogen werden, die Auswirkungen auf die Verbraucherrechte haben.

- Der Einsatz von KI-Anwendungen für die Zwecke der biometrischen Fernidentifikation[52] und anderer in die Privatsphäre eingreifender Überwachungstechnologien würde ausnahmslos als mit hohem Risiko behaftet angesehen, sodass die nachstehenden Anforderungen stets gelten würden.

[51] Es sei darauf hingewiesen, dass auch andere EU-Rechtsvorschriften Anwendung finden können. Beispielsweise kann in Fällen, in denen KI in ein Verbraucherprodukt integriert ist, die Richtlinie über die allgemeine Produktsicherheit gelten.

[52] Die biometrische Fernidentifikation ist von der biometrischen Authentifizierung zu unterscheiden (bei letzterer handelt es sich um einen Sicherheitsprozess, der sich auf die einzigartigen biologischen Merkmale einer Person stützt, um deren Angaben zu ihrer Identität zu überprüfen). Bei der biometrischen Fernidentifikation handelt es sich um ein Verfahren, bei dem die Identität vieler Personen mithilfe biometrischer Identifikatoren (Fingerabdrücke, Gesicht, Iris, Gefäßmuster usw.) aus der Ferne im öffentlichen Raum permanent durch Abgleich mit in einer Datenbank gespeicherten Daten ermittelt werden.

D. ARTEN VON ANFORDERUNGEN

Bei der Ausgestaltung des künftigen Rechtsrahmens für KI wird zu entscheiden sein, welche Arten verbindlicher rechtlicher Anforderungen den einschlägigen Akteuren auferlegt werden sollen. Diese Anforderungen können durch Standards weiter spezifiziert werden. Wie in Abschnitt C ausgeführt, und zusätzlich zu bereits bestehenden Rechtsvorschriften, würden diese Anforderungen nur für KI-Anwendungen mit hohem Risiko gelten, wodurch sichergestellt würde, dass regulatorische Eingriffe zielgerichtet und verhältnismäßig sind.

Unter Berücksichtigung der Leitlinien der Hochrangigen Expertengruppe und der vorstehenden Ausführungen könnten sich die Anforderungen an KI-Anwendungen mit hohem Risiko auf die folgenden Schlüsselmerkmale beziehen, die in den nachstehenden Unterabschnitten eingehender erörtert werden:

- Trainingsdaten
- Aufbewahrung von Daten und Aufzeichnungen
- Vorzulegende Informationen
- Robustheit und Genauigkeit
- Menschliche Aufsicht
- besondere Anforderungen an bestimmte KI-Anwendungen, z. B. Anwendungen für die biometrische Fernidentifikation.

Zur Gewährleistung der Rechtssicherheit werden diese Anforderungen weiter zu spezifizieren sein, um klare Maßstäbe für alle Akteure festzulegen, die sie erfüllen müssen.

a) Trainingsdaten

Es ist wichtiger denn je, die Werte und Regeln der EU und insbesondere die Rechte, die den Bürgerinnen und Bürgern aus dem EU-Recht erwachsen, zu fördern, zu stärken und zu verteidigen. Diese Bemühungen betreffen zweifellos auch die in der EU vermarkteten und verwendeten KI-Anwendungen mit hohem Risiko, die hier betrachtet werden.

Wie bereits erwähnt, gibt es ohne Daten keine KI. In vielen Fällen hängen die Funktionsweise vieler KI-Systeme und die Handlungsschritte und Entscheidungen, zu denen sie führen können, stark von den Daten ab, mit dem die Systeme trainiert wurden. Daher sollten geeignete Maßnahmen ergriffen werden, damit bei den Daten, die als Trainingsdaten für KI-Systeme verwendet werden, die Werte und die Regeln der EU eingehalten werden, insbesondere was Sicherheitsfragen und die bestehenden Rechtsvorschriften zum Schutz der Grundrechte angeht. So könnten für die Trainingsdaten von KI-Systemen folgende Anforderungen in Betracht gezogen werden:

- Anforderungen, die hinreichend gewährleisten, dass die anschließende Nutzung der KI-gestützten Produkte oder Dienstleistungen sicher ist, weil sie den Standards entspricht, die in den geltenden (bereits bestehenden und etwaigen ergänzenden) EU-Sicherheitsvorschriften festgelegt sind. Dies kann beispielsweise Anforderungen umfassen, durch die gewährleistet wird, dass KI-Systeme anhand von Datensätzen trainiert werden, die alle Szenarien abdecken, die für die Vermeidung gefährlicher Situationen relevant sind.

- Ferner die Auflage, angemessene Maßnahmen zu ergreifen, um sicherzustellen, dass eine solche spätere Nutzung von KI-Systemen nicht zu Ergebnissen führt, die eine verbotene Diskriminierung darstellen. Diese Auflagen könnten insbesondere die Verpflichtung umfassen, Datensätze zu verwenden, die ausreichend repräsentativ sind. Damit soll vor allem sichergestellt werden, dass alle relevanten Aspekte wie Geschlecht, ethnische Zugehörigkeit

und andere mögliche Gründe für verbotene Diskriminierung in diesen Datensätzen angemessen berücksichtigt werden;

- Auflagen, durch die sichergestellt werden soll, dass die Privatsphäre und die personenbezogenen Daten bei der Nutzung von KI-gestützten Produkten und Diensten angemessen geschützt werden. Die Aspekte, die in den Anwendungsbereich der Datenschutz-Grundverordnung bzw. der Richtlinie über den Datenschutz bei der Strafverfolgung fallen, werden durch die genannten Rechtsakte geregelt.

b) Aufbewahrung von Daten und Aufzeichnungen

Unter Berücksichtigung von Aspekten wie der Komplexität und der Opazität vieler KI-Systeme und der möglicherweise damit verbundenen Schwierigkeiten, die Einhaltung der geltenden Vorschriften wirksam zu überprüfen und durchzusetzen, müssen Anforderungen formuliert werden, die für die Aufbewahrung von Aufzeichnungen über die Programmierung des Algorithmus und die für KI-Systeme mit hohem Risiko verwendeten Trainingsdaten sowie in bestimmten Fällen die Aufbewahrung der Daten selbst gelten. Entsprechende Anforderungen ermöglichen es in erster Linie, potenziell problematische Handlungen oder Entscheidungen von KI-Systemen zurückzuverfolgen und zu überprüfen. Dies dürfte nicht nur die Überwachung und Durchsetzung erleichtern, sondern auch stärkere Anreize für die betreffenden Wirtschaftsteilnehmer bieten, zu einem frühen Zeitpunkt zu berücksichtigen, dass diese Vorschriften eingehalten werden müssen.

Zu diesem Zweck könnte in dem Rechtsrahmen die Pflicht vorgesehen werden, Folgendes aufzubewahren:

- genaue Aufzeichnungen zu den für das Training und die Erprobung der KI-Systeme verwendeten Datensätze, einschließlich einer Beschreibung der wichtigsten Merkmale und der Art und Weise, wie die Datensätze ausgewählt wurden;

- in bestimmten begründeten Fällen die Datensätze selbst;

- Dokumentation der für Programmierung[53] und Training verwendeten Methoden, der für Aufbau, Erprobung und Validierung der KI-Systeme eingesetzten Verfahren und Techniken, ggf. unter Beachtung von Sicherheitsanforderungen und unter Vermeidung von Verzerrungen, die zu verbotenen Diskriminierungen führen könnten.

Um eine wirksame Durchsetzung der einschlägigen Rechtsvorschriften zu gewährleisten, müssten die Aufzeichnungen, die Dokumentation und gegebenenfalls die Datensätze während eines begrenzten, angemessenen Zeitraums aufbewahrt werden. Es sollten Maßnahmen getroffen werden, um sicherzustellen, dass sie auf Anfrage zur Verfügung gestellt werden, insbesondere für Prüfungen oder Inspektionen durch zuständige Behörden. Erforderlichenfalls sollten Vorkehrungen getroffen werden, um sicherzustellen, dass vertrauliche Informationen wie Geschäftsgeheimnisse geschützt werden.

c) Bereitstellung von Informationen

Transparenz ist auch über die unter Buchstabe c genannten Aufzeichnungspflichten hinaus erforderlich. Um die angestrebten Ziele zu erreichen – insbesondere die Förderung eines verantwortungsvollen Einsatzes von KI, die Schaffung von Vertrauen und die Gewährleistung eines

[53] Beispielsweise Dokumentation zum Algorithmus, einschließlich Angaben dazu, wofür das Modell optimiert werden soll, welche Gewichtung zu Beginn bestimmten Parametern zugemessen wurde usw.

geeigneten Rechtsschutzes –, ist es wichtig, dass proaktiv angemessene Informationen über den Einsatz von KI-Systemen mit hohem Risiko bereitgestellt werden.

Daher könnten folgende Anforderungen in Betracht gezogen werden:

- Vorlage eindeutiger Angaben über die Fähigkeiten und Grenzen des KI-Systems, insbesondere über den Zweck, für den die Systeme bestimmt sind, die Bedingungen, unter denen davon ausgegangen werden kann, dass sie bestimmungsgemäß funktionieren, und über das erwartete Maß an Genauigkeit bei der Erreichung des angegebenen Zwecks. Diese Angaben sind insbesondere für die Betreiber der Systeme wichtig, können aber auch für die zuständigen Behörden und die betroffenen Parteien relevant sein.

- Abgesehen davon sollten Bürgerinnen und Bürger klar und deutlich darauf hingewiesen werden, wenn sie mit einem KI-System interagieren, und nicht mit einem Menschen. Die Datenschutzvorschriften der EU enthalten zwar bereits eine Reihe entsprechender Regeln[54], doch können zusätzliche Anforderungen erforderlich sein, um die oben genannten Ziele zu erreichen. Dabei sollte unnötiger Aufwand vermieden werden. Daher ist müssen solche Angaben beispielsweise dann nicht bereitgestellt werden, wenn für die Bürgerinnen und Bürger unmittelbar ersichtlich ist, dass sie mit KI-Systemen interagieren. Darüber hinaus ist es wichtig, dass die bereitgestellten Informationen objektiv, kurzgefasst und leicht verständlich sind. Wie diese Informationen bereitzustellen sind, sollte sich nach dem jeweiligen Kontext richten.

d) Robustheit und Genauigkeit

KI-Systeme – und dies gilt in besonderem Maße für KI-Anwendungen mit hohem Risiko – müssen technisch solide und präzise sein, um vertrauenswürdig zu sein. Dies bedeutet, dass solche Systeme verantwortungsvoll und nach gebührender Vorabbewertung der von ihnen möglicherweise ausgehenden Risiken entwickelt werden müssen. Bei ihrer Entwicklung und Funktionsweise muss gewährleistet werden, dass KI-Systeme sich zuverlässig gemäß ihrem beabsichtigten Verwendungszweck verhalten. Dabei sollten alle zumutbaren Maßnahmen ergriffen werden, um das Risiko etwaiger Schäden so gering wie möglich zu halten.

Daher könnten folgende Aspekte in Betracht gezogen werden:

- Anforderungen, die gewährleisten, dass die KI-Systeme in allen Phasen ihres Lebenszyklus robust und genau sind oder zumindest ihren Genauigkeitsgrad korrekt wiedergeben;

- Anforderungen, die gewährleisten, dass die Ergebnisse reproduzierbar sind;

- Anforderungen, die gewährleisten, dass KI-Systeme in allen Phasen ihre Lebenszyklus Fehler und Unstimmigkeiten angemessen bewältigen können.

[54] Insbesondere müssen nach Artikel 13 Absatz 2 Buchstabe f DSGVO die für die Verarbeitung Verantwortlichen zum Zeitpunkt der Erhebung der personenbezogenen Daten den betroffenen Personen weitere Informationen über das Bestehen einer automatisierten Entscheidungsfindung sowie bestimmte zusätzliche Informationen zur Verfügung stellen, die notwendig sind, um eine faire und transparente Verarbeitung zu gewährleisten.

- Anforderungen, die gewährleisten, dass KI-Systeme sowohl gegen offene Angriffe als auch gegen subtilere Versuche, Daten oder die Algorithmen selbst zu manipulieren, widerstandsfähig sind und dass in solchen Fällen Abhilfemaßnahmen ergriffen werden.

e) Menschliche Aufsicht

Die menschliche Aufsicht hilft, dafür zu sorgen, dass ein KI-System die menschliche Autonomie nicht untergräbt oder sich sonst nachteilig auswirkt. Das Ziel einer vertrauenswürdigen, ethischen und auf den Menschen ausgerichteten KI kann nur erreicht werden, wenn dafür gesorgt wird, dass Menschen bei KI-Anwendungen mit hohem Risiko gebührend mitwirken.

Zwar werden die KI-Anwendungen, für die in diesem Weißbuch spezifische rechtliche Regelungen in Betracht gezogen werden, ausnahmslos als Anwendungen mit hohem Risiko angesehen, die jeweils geeignete Art und der angemessene Grad der menschlichen Aufsicht können jedoch von Fall zu Fall variieren. Dies wird insbesondere von der beabsichtigten Nutzung der Systeme und den Auswirkungen abhängen, die die Nutzung auf die betroffenen Bürgerinnen und Bürger und juristischen Personen haben könnte. Ferner berührt dies auch nicht die in der DSGVO festgelegten Rechte, die greifen, wenn das KI-System personenbezogene Daten verarbeitet. Beispielsweise könnte die menschliche Aufsicht u. a. auf folgendem Wege ausgeübt werden:

- die Ergebnisse des KI-Systems werden erst dann wirksam, wenn sie zuvor von einem Menschen überprüft und validiert wurden (z. B. kann die Ablehnung eines Antrags auf Sozialleistungen nur durch einen Menschen erfolgen);

- die Ergebnisse des KI-Systems werden sofort wirksam, aber menschliches Eingreifen wird in einem späteren Schritt sichergestellt (z. B. kann die Ablehnung eines Antrags auf eine Kreditkarte von einem KI-System bearbeitet werden, doch muss später eine Überprüfung durch den Menschen möglich sein);

- Überwachung des KI-Systems während seines Betriebs und Möglichkeit, in Echtzeit einzugreifen und das System ggf. zu deaktivieren (z. B. verfügt ein fahrerloses Fahrzeug über eine Stopptaste oder einen Mechanismus, der aktiviert werden kann, wenn ein Mensch feststellt, dass der Fahrbetrieb nicht sicher ist);

- in der Entwurfsphase, indem Einschränkungen für den Betrieb des KI-Systems auferlegt werden (z. B. muss ein fahrerloses Fahrzeug unter bestimmten Bedingungen bei geringer Sicht den Betrieb einstellen, da in diesem Fall die Sensoren möglicherweise weniger zuverlässig sind, oder es muss unter allen Umständen einen vorgegebenen Abstand vom vorausfahrenden Fahrzeug einhalten).

f) Besondere Anforderungen an Systeme für biometrische Fernidentifikation

Die Erfassung und Auswertung biometrischer Daten [55] zum Zweck der Fernidentifikation [56], beispielsweise durch Einsatz von Gesichtserkennungstechnik im öffentlichen Raum birgt besondere

[55] Biometrische Daten werden definiert als „mit speziellen technischen Verfahren gewonnene personenbezogene Daten zu den physischen, physiologischen oder verhaltenstypischen Merkmalen einer natürlichen Person, die die eindeutige Authentifizierung oder Identifizierung dieser natürlichen Person ermöglichen oder bestätigen, wie Gesichtsbilder oder daktyloskopische [Fingerabdruck-] Daten“. (Richtlinie zum Datenschutz bei der Strafverfolgung, Artikel 3 Absatz 13; DSGVO, Artikel 4 Absatz 14; Verordnung (EU) 2018/1725, Artikel 3 Absatz 18).

Risiken in Bezug auf die Achtung der Grundrechte[57]. Im Hinblick auf das Ausmaß, in dem sich der Einsatz biometrischer Fernidentifikationssysteme auf die Grundrechte auswirkt, gibt es je nach Zweck, Kontext und Umfang des Einsatzes große Unterschiede.

Die Verarbeitung biometrischer Daten zum Zwecke der eindeutigen Identifizierung natürlicher Personen ist nach den Datenschutzvorschriften der EU außer unter bestimmten Bedingungen grundsätzlich verboten[58]. Insbesondere darf eine solche Verarbeitung nach der DSGVO nur auf Basis einer begrenzten Zahl von Gründen erfolgen, typischerweise aus Gründen eines wichtigen öffentlichen Interesses. In diesem Fall muss die Verarbeitung auf der Grundlage der Rechtsvorschriften der EU oder nationaler Rechtsvorschriften erfolgen, wobei die Anforderungen an die Verhältnismäßigkeit, die Achtung des Wesensgehalts des Rechts auf Datenschutz und geeignete Garantien einzuhalten sind. Gemäß der Richtlinie zum Datenschutz bei der Strafverfolgung muss für eine solche Verarbeitung eine unbedingte Erforderlichkeit vorliegen, sowie ferner im Prinzip eine Genehmigung nach EU-Recht oder nationalem Recht sowie geeignete Garantien. Da jegliche Verarbeitung biometrischer Daten zum Zwecke der eindeutigen Identifizierung einer natürlichen Person eine Ausnahme von einem im EU-Recht verankerten Verbot erfordern würde, würde sie der Charta der Grundrechte der EU unterliegen.

Daraus folgt, dass nach den geltenden Datenschutzvorschriften der EU und der Charta der Grundrechte KI nur dann für die Zwecke der biometrischen Fernidentifikation eingesetzt werden darf, wenn der betreffende Einsatz hinreichend begründet und verhältnismäßig ist und geeignete Garantien gewährleistet sind.

Um möglichen gesellschaftlichen Bedenken im Zusammenhang mit der Nutzung von KI zu solchen Zwecken im öffentlichen Raum Rechnung zu tragen und eine Fragmentierung des Binnenmarkts zu vermeiden, wird die Kommission eine breit angelegte europäische Debatte über die besonderen Umstände, die eine solche Nutzung rechtfertigen könnten, sowie über gemeinsame Sicherheitsvorkehrungen einleiten.

E. ADRESSATEN

In Bezug auf die Adressaten der rechtlichen Auflagen, die für die oben genannten KI-Anwendungen mit hohem Risiko gelten würden, sind im Wesentlichen zwei Fragen zu prüfen.

Erstens stellt sich die Frage, wie die Verpflichtungen auf die beteiligten Wirtschaftsteilnehmer aufgeteilt werden sollten. Im Lebenszyklus eines KI-Systems sind viele Akteure beteiligt. Hierzu gehören der Entwickler, der Betreiber (die Person, die ein KI-gestütztes Produkt oder eine KI-gestützte

[56] Im Zusammenhang mit der Gesichtserkennung bedeutet Identifizierung, dass das Muster des Gesichtsbilds einer Person mit vielen anderen in einer Datenbank gespeicherten Mustern verglichen wird, um herauszufinden, ob ihr Bild dort gespeichert ist. Authentifizierung (oder Verifizierung) wiederum wird häufig als 1:1-Vergleich bezeichnet. Es ermöglicht den Vergleich zweier biometrischer Templates, von denen in der Regel angenommen wird, dass sie derselben Person zuzuordnen sind. Es werden zwei biometrische Templates miteinander verglichen, um festzustellen, ob es sich bei den Personen auf den beiden Bildern um dieselbe Person handelt. Ein solches Verfahren wird beispielsweise an den für Grenzübertrittskontrollen an Flughäfen verwendeten Sicherheitsschleusen des automatischen Grenzkontrollsystems (ABC) angewandt.

[57] Zum Beispiel in Bezug auf die Würde der Menschen. Bei der Nutzung von Gesichtserkennungstechnik wiederum geht es in Bezug auf Grundrechtefragen vor allem um das Recht auf Achtung des Privatlebens und den Schutz personenbezogener Daten. Ferner gibt es auch potenzielle Auswirkungen im Bereich der Nichtdiskriminierung und der Rechte bestimmter Gruppen wie Kinder, ältere Menschen und Menschen mit Behinderungen. Darüber hinaus darf die Meinungs-, Vereinigungs- und Versammlungsfreiheit nicht durch den Einsatz der Technologie untergraben werden. Siehe: Facial recognition technology: fundamental rights considerations in the context of law enforcement (Gesichtserkennungstechnik: Überlegungen zu den Grundrechten im Kontext der Strafverfolgung). https://fra.europa.eu/en/publication/2019/facial-recognition.

[58] Artikel 9 DSGVO, Artikel 10 der Richtlinie zum Datenschutz bei der Strafverfolgung. Siehe auch Artikel 10 der Verordnung (EU) Nr. 2018/1725 (gilt für die Organe und Einrichtungen der EU).

Dienstleistung nutzt) und möglicherweise weitere Akteure (Hersteller, Händler oder Importeur, Dienstleister, professioneller oder privater Nutzer).

Nach Auffassung der Kommission sollten in einem künftigen Rechtsrahmen die einzelnen Verpflichtungen jeweils dem Akteur/den Akteuren obliegen, der/die am besten in der Lage ist/sind, potenzielle Risiken zu bewältigen. So wären möglicherweise die Entwickler von KI am besten in der Lage, den Risiken zu begegnen, die sich aus der Entwicklungsphase ergeben, während ihre Fähigkeit, die Risiken in der Nutzungsphase zu kontrollieren, eher eingeschränkt wäre. In diesem Fall sollte die entsprechende Verpflichtung dem Betreiber auferlegt werden. Dies gilt unbeschadet der Frage, welche Partei im Hinblick auf die Haftung gegenüber Endnutzern oder anderen Geschädigten und zur Gewährleistung eines wirksamen Zugangs zu den Gerichten für Schäden haftbar gemacht werden sollte. Nach dem EU-Produkthaftungsrecht obliegt die Haftung für fehlerhafte Produkte dem Hersteller, unbeschadet nationaler Rechtsvorschriften, die auch die Geltendmachung von Schadensersatzansprüchen gegenüber anderen Parteien zulassen können.

Zweitens stellt sich die Frage nach dem geografischen Anwendungsbereich der Rechtsvorschriften. Nach Ansicht der Kommission ist es von entscheidender Bedeutung, dass die Auflagen für alle einschlägigen Wirtschaftsteilnehmer gelten, die KI-gestützte Produkte oder Dienstleistungen in der EU anbieten, unabhängig davon, ob sie in der EU niedergelassen sind oder nicht. Andernfalls könnten die oben genannten Ziele der gesetzgeberischen Maßnahmen nicht vollständig erreicht werden.

F. EINHALTUNG UND DURCHSETZUNG

Um sicherzustellen, dass KI vertrauenswürdig und sicher ist und dass dabei die Achtung der europäischen Werte und Vorschriften gewährleistet ist, müssen die geltenden rechtlichen Anforderungen in der Praxis eingehalten und sowohl von den zuständigen nationalen und europäischen Behörden als auch von den betroffenen Parteien wirksam durchgesetzt werden. Die zuständigen Behörden sollten in der Lage sein, Einzelfälle zu untersuchen, aber auch die Auswirkungen auf die Gesellschaft zu bewerten.

Angesichts des hohen Risikos, das bestimmte KI-Anwendungen für die Bürgerinnen und Bürger und für unsere Gesellschaft insgesamt darstellen (siehe Abschnitt A), ist die Kommission zum gegenwärtigen Zeitpunkt der Auffassung, dass eine objektive, vorab vorzunehmende Konformitätsbewertung erforderlich wäre, um zu überprüfen und sicherzustellen, dass bestimmte der oben genannten obligatorischen Auflagen für Anwendungen mit hohem Risiko (siehe Abschnitt D) erfüllt sind. Eine vorab vorzunehmende Konformitätsbewertung könnte Verfahren für die Prüfung, Inspektion oder Zertifizierung umfassen[59]. Dies könnte eine Überprüfung der Algorithmen und der in der Entwicklungsphase verwendeten Datensätze beinhalten.

Die Konformitätsbewertungen für KI-Anwendungen mit hohem Risiko sollten Teil der Konformitätsbewertungsmechanismen sein, die es bereits für eine große Zahl von Produkten gibt, die auf dem EU-Binnenmarkt in Verkehr gebracht werden. Kann nicht auf solche bestehenden Mechanismen zurückgegriffen werden, müssen unter Umständen ähnliche Mechanismen eingerichtet werden, die sich auf bewährte Verfahren und mögliche Beiträge von Interessenträgern und europäischen Normungsorganisationen stützen. Etwaige neue Mechanismen sollten verhältnismäßig

[59] Das System würde sich auf die bestehenden Konformitätsbewertungsverfahren in der EU (vgl. Beschluss 768/2008/EG) oder auf die Verordnung (EU) 2019/881 (Rechtsakt zur Cybersicherheit) stützen und den Besonderheiten der KI Rechnung tragen. Siehe den Leitfaden für die Umsetzung der Produktvorschriften der EU 2014 („Blue Guide“).

sein, nicht diskriminieren und transparente und objektive Kriterien zugrunde legen, die im Einklang mit internationalen Verpflichtungen stehen.

Bei der Konzeption und Umsetzung eines Systems, das sich auf vorab vorzunehmende Konformitätsbewertungen stützt, sollte insbesondere Folgendes berücksichtigt werden:

- Möglicherweise sind nicht alle oben genannten Anforderungen für eine Überprüfung im Rahmen einer vorab vorzunehmenden Konformitätsbewertung geeignet. So ist beispielsweise die Anforderung zu den vorzulegenden Informationen im Allgemeinen nicht für eine Überprüfung im Rahmen einer solchen Bewertung geeignet.

- Besonders zu berücksichtigen ist die Möglichkeit, dass sich bestimmte KI-Systeme weiterentwickeln und lernfähig sind, was möglicherweise wiederholte Bewertungen während der Lebensdauer der betreffenden KI-Systeme erforderlich macht.

- Die Notwendigkeit, die Trainingsdaten und die für Programmierung und Training verwendeten Methoden, Prozesse und Techniken, welche für Aufbau, Erprobung und Validierung der KI-Systeme eingesetzt wurden, zu überprüfen.

- Ergibt die Konformitätsbewertung, dass ein KI-System die Anforderungen nicht erfüllt, z. B. in Bezug auf die verwendeten Trainingsdaten, müssen die festgestellten Mängel behoben werden, indem beispielsweise das System in der EU so nachtrainiert wird, dass alle geltenden Anforderungen erfüllt werden.

Die Konformitätsbewertung wäre für alle Wirtschaftsteilnehmer, für die die Anforderungen gelten, unabhängig vom Ort ihrer Niederlassung obligatorisch[60]. Um den Verwaltungsaufwand für KMU zu begrenzen, könnten Unterstützungsstrukturen unter anderem im Rahmen von digitalen Innovationszentren in Betracht gezogen werden. Darüber hinaus könnten Standards und spezielle Online-Instrumente die Einhaltung der Vorschriften erleichtern.

Die vorab vorzunehmenden Konformitätsbewertungen sollten die Überwachung der Einhaltung der Vorschriften und die nachträgliche Durchsetzung durch die zuständigen nationalen Behörden nicht berühren. Dies gilt für KI-Anwendungen mit hohem Risiko, aber auch für andere KI-Anwendungen, die rechtlichen Anforderungen unterliegen; allerdings kann die Tatsache, dass eine Anwendung mit einem hohem Risiko behaftet ist, für die zuständigen nationalen Behörden Anlass sein, dieser besondere Aufmerksamkeit zu schenken. Ex-post-Kontrollen sollten durch eine angemessene Dokumentation der entsprechenden AI-Anwendung ermöglicht werden (siehe Abschnitt E) sowie gegebenenfalls durch die Möglichkeit für Dritte, z. B. zuständige Behörden, solche Anwendungen zu testen. Dies kann besonders wichtig sein, wenn Risiken für die Grundrechte entstehen, da diese kontextabhängig sind. Eine solche Überwachung der Einhaltung der Vorschriften sollte Teil eines kontinuierlichen Marktüberwachungssystems sein. Aspekte im Zusammenhang mit der Governance werden in Abschnitt H weiter unten erörtert.

Darüber hinaus sollten sowohl für KI-Anwendungen mit hohem Risiko als auch für andere KI-Anwendungen wirksame Rechtsbehelfe für Parteien vorgesehen werden, die von negativen Auswirkungen von KI-Systemen betroffen sind. Fragen, die sich auf haftungsrelevante Aspekte

[60] Zu der einschlägigen Governance-Struktur, einschließlich der für die Durchführung der Konformitätsbewertungen benannten Stellen, siehe Abschnitt H.

beziehen, werden im Bericht über den Sicherheits- und Haftungsrahmen, der zusammen mit diesem Weißbuch vorgelegt wird, weiter erörtert.

G. FREIWILLIGE KENNZEICHNUNG FÜR KI-ANWENDUNGEN OHNE HOHES RISIKO

Für KI-Anwendungen, die nicht als Anwendungen „mit hohem Risiko“ eingestuft werden (siehe Abschnitt C) und für die daher nicht die oben erörterten obligatorischen Anforderungen gelten (siehe Abschnitte D, E und F), wäre eine Option, neben den geltenden Rechtsvorschriften ein freiwilliges Kennzeichnungssystem einzuführen.

Im Rahmen des Systems könnten interessierte Wirtschaftsteilnehmer, die nicht den obligatorischen Auflagen unterliegen, sich freiwillig für die Einhaltung dieser Auflagen oder eine Reihe ähnlicher Anforderungen, die speziell für die Zwecke des freiwilligen Systems festgelegt wurden, entscheiden. Die KI-Anwendungen der betreffenden Wirtschaftsteilnehmer würden dann ein Gütesiegel erhalten.

Mit dem freiwilligen Gütesiegel könnten diese Wirtschaftsakteuren signalisieren, dass ihre KI-gestützten Produkte und Dienstleistungen vertrauenswürdig sind. So könnten Nutzer leicht erkennen, dass die betreffenden Produkte und Dienstleistungen bestimmte objektive und standardisierte EU-weite Vorgaben erfüllen, die über die normalerweise geltenden rechtlichen Verpflichtungen hinausgehen. Dies würde dazu beitragen, das Vertrauen der Nutzer in KI-Systeme zu stärken und die allgemeine Akzeptanz dieser Technologie zu fördern.

Diese Option würde die Schaffung eines neuen Rechtsinstruments erfordern, in dem ein Rahmen für die freiwillige Kennzeichnung für Entwickler und/oder Betreiber von KI-Systemen festgelegt wird, die nicht als Anwendungen mit hohem Risiko eingestuft sind. Die Teilnahme am Kennzeichnungssystem wäre freiwillig, hat sich ein Entwickler oder Betreiber aber einmal für die Verwendung des Labels entschieden, wären die Anforderungen jedoch verbindlich. Durch die Kombination von Ex-ante-Maßnahmen und Ex-Post-Durchsetzung müsste sichergestellt werden, dass alle Anforderungen erfüllt werden.

H. GOVERNANCE

Eine europäische Governance-Struktur für KI in Form eines Rahmens für die Zusammenarbeit der zuständigen nationalen Behörden ist notwendig, um eine Aufsplitterung der Zuständigkeiten zu vermeiden, die Kapazitäten in den Mitgliedstaaten auszubauen und sicherzustellen, dass Europa sich schrittweise mit der für die Prüfung und Zertifizierung von KI-gestützten Produkten und Dienstleistungen erforderlichen Kapazitäten ausstattet. In diesem Zusammenhang wäre es von Vorteil, die zuständigen nationalen Behörden dabei zu unterstützen, ihren Auftrag in Bezug auf die Nutzung von KI zu erfüllen.

Eine europäische Governance-Struktur könnte als Forum für einen regelmäßigen Austausch von Informationen und bewährten Verfahren mit einer Vielzahl von Aufgaben betraut werden, einschließlich der Ermittlung neuer Trends und der Beratung in den Bereichen Normung und Zertifizierung. Sie sollte auch eine Schlüsselrolle spielen, wenn es darum geht, die Umsetzung des Rechtsrahmens zu fördern, beispielsweise durch die Herausgabe von Leitlinien, Stellungnahmen und die Bereitstellung von Fachwissen. Zu diesem Zweck sollte sie sich auf ein Netz nationaler Behörden stützen sowie auf sektorspezifische Netze und Regulierungsbehörden auf nationaler und EU-Ebene. Darüber hinaus könnte ein Sachverständigenausschuss die Kommission unterstützen.

Die Governance-Struktur sollte eine größtmögliche Beteiligung der Interessenträger gewährleisten. Die Interessenträger – Verbraucherorganisationen und Sozialpartner, Unternehmen, Forscher und

Organisationen der Zivilgesellschaft – sollten zur Umsetzung und Weiterentwicklung des Rahmens konsultiert werden.

Angesichts der bereits bestehenden Strukturen beispielsweise in den Bereichen Finanzen, Arzneimittel, Luftfahrt, Medizinprodukte, Verbraucherschutz und Datenschutz ist darauf zu achten, dass es bei der vorgeschlagenen Governance-Struktur keine Überschneidungen mit bestehenden Funktionen gibt. Stattdessen sollten enge Beziehungen zu anderen zuständigen Behörden der EU und der Mitgliedstaaten in den verschiedenen Sektoren geknüpft werden, um das vorhandene Fachwissen zu ergänzen und die bestehenden Behörden bei der Überwachung und Beaufsichtigung der Tätigkeiten der Wirtschaftsteilnehmer, die KI-Systeme und KI-gestützte Produkte und Dienstleistungen einsetzen, zu unterstützen.

Wird diese Option tatsächlich weiterverfolgt, könnte die Durchführung von Konformitätsbewertungen den von den Mitgliedstaaten benannten benannten Stellen übertragen werden. Testzentren sollten die unabhängige Prüfung und Bewertung von KI-Systemen gemäß den oben genannten Anforderungen ermöglichen. Eine unabhängige Bewertung wird das Vertrauen stärken und sorgt für Objektivität. Dies könnte auch die Arbeit der jeweils zuständigen Behörden erleichtern.

Die EU verfügt über hervorragende Test- und Bewertungszentren und sollte ihre Kapazitäten auch im Bereich der KI ausbauen. Wirtschaftsteilnehmer mit Sitz in Drittländern, die in den Binnenmarkt eintreten wollen, könnten sich entweder an benannte Stellen mit Sitz in der EU wenden oder – vorbehaltlich der Abkommen über die gegenseitige Anerkennung mit Drittländern – Stellen aus Drittländern in Anspruch nehmen, die für die Durchführung einer solchen Bewertung benannt wurden.

Die Governance-Struktur für den Bereich KI und die hier erörterten etwaigen Konformitätsbewertungen würden die nach geltendem EU-Recht vorgesehenen Befugnisse und Zuständigkeiten der jeweils zuständigen Behörden in einzelnen Sektoren oder bestimmten Bereichen (Finanzen, Arzneimittel, Luftfahrt, Medizinprodukte, Verbraucherschutz, Datenschutz usw.) unberührt lassen.

6. FAZIT

KI ist eine strategische Technologie, die viele Vorteile für Bürgerinnen und Bürger, für Unternehmen und die Gesellschaft insgesamt bietet, sofern sie auf den Menschen ausgerichtet, ethisch und nachhaltig ist und die Grundrechte und -werte achtet. KI bietet wichtige Effizienz- und Produktivitätsgewinne, die die Wettbewerbsfähigkeit der europäischen Industrie stärken und das Wohlergehen der Bürger verbessern können. Sie kann auch dazu beitragen, Lösungen für einige der drängendsten gesellschaftlichen Herausforderungen zu finden, darunter die Bekämpfung des Klimawandels und der Umweltzerstörung, die Herausforderungen im Zusammenhang mit der Nachhaltigkeit und dem demografischen Wandel, der Schutz unserer Demokratien und, soweit erforderlich und verhältnismäßig, die Kriminalitätsbekämpfung.

Damit Europa die Chancen, die die KI bietet, in vollem Umfang nutzen kann, muss es die erforderlichen industriellen und technologischen Kapazitäten entwickeln und stärken. Wie in der begleitenden europäischen Datenstrategie dargelegt, erfordert dies auch Maßnahmen, die es der EU ermöglichen, zu einem globalen Kotenpunkt für Daten zu werden.

Der europäische Ansatz für KI zielt darauf ab, die Innovationsfähigkeit Europas im Bereich der KI zu fördern und gleichzeitig die Entwicklung und Einführung ethischer und vertrauenswürdiger KI in der gesamten EU-Wirtschaft zu unterstützen. KI sollte im Dienste der Menschen stehen und eine positive Kraft für die Gesellschaft sein.

Mit diesem Weißbuch und dem begleitenden Bericht über den Sicherheits- und Haftungsrahmen leitet die Kommission eine breit angelegte Konsultation der Zivilgesellschaft, der Industrie und der Wissenschaftskreise in den Mitgliedstaaten zu konkreten Vorschlägen für ein europäisches KI-Konzept ein. Dazu gehören sowohl politische Mittel zur Ankurbelung von Investitionen in Forschung und Innovation, zur Förderung der Entwicklung von Kompetenzen und der Akzeptanz von KI durch KMU als auch Vorschläge für Schlüsselelemente eines künftigen Rechtsrahmens. Diese Konsultation wird einen umfassenden Dialog mit allen betroffenen Parteien ermöglichen, der in die Gestaltung der nächsten Schritte der Kommission einfließen wird.

Die Kommission bittet um Stellungnahmen zu den im Weißbuch enthaltenen Vorschlägen im Wege einer öffentlichen Konsultation, die in englischer Sprache verfügbar ist unter: https://ec.europa.eu/info/consultations_en. Stellungnahmen können bis zum 19. Mai 2020 übermittelt werden..

Die Beiträge, die die Kommission im Rahmen einer öffentlichen Konsultation erhält, werden in der Regel veröffentlicht. Allerdings kann beantragt werden, dass Beiträge oder Teile davon vertraulich behandelt werden. Geben Sie bitte gegebenenfalls auf dem Deckblatt Ihrer Stellungnahme klar und deutlich an, dass sie nicht veröffentlicht werden soll. In diesem Fall übermitteln Sie bitte der Kommission gleichzeitig eine nichtvertrauliche Fassung der Stellungnahme zur Veröffentlichung.