**„Fundamentalkritik“ des White Papers und des Datenstrategiepapiers der EU-Kommission vom 19. Februar 2020**

Stand: 17. März 2020

von *Yannik Borutta, Ass. jur. Matthias Haag, Ass. jur. Hanna Hoffmann, Johannes Kevekordes, Verena Vogt*[1]

Am 19. Februar 2020 hat die EU-Kommission neben dem lang erwarteten und im Voraus angekündigten Weißbuch zur künstlichen Intelligenz[2], ein Dokument zur Gestaltung der digitalen Zukunft Europas[3], eines zur europäischen Datenstrategie[4] und einen Bericht über die Auswirkungen künstlicher Intelligenz, des Internets der Dinge und der Robotik in Hinblick auf Sicherheit und Haftung[5] veröffentlicht.

Kommissionspräsidentin Ursula von der Leyen erklärte in ihrer Präsentation der neuen EU-Digitalstrategie, dass die „Ziele für die Gestaltung der digitalen Zukunft Europas [alles abdecken,] von der Cybersicherheit über kritische Infrastrukturen, digitale Bildung und Kompetenzen bis hin zu Demokratie und Medien“[6]. Ob man diesem Versprechen gerecht geworden ist und inwieweit dabei inhaltliche Akzente gesetzt werden konnten, soll im Folgenden untersucht werden. Dazu sollen zunächst einzelne Vorschläge von ausgewählten Dokumenten erörtert werden und es soll auf neu aufkommende Haftungsfragen, die sich im Zusammenhang mit dem Einsatz von KI stellen, eingegangen werden.

# A. Weißbuch zur künstlichen Intelligenz

## I. Definition von Künstlicher Intelligenz

Es ist wichtig, zunächst den Anwendungsbereich eines künftigen EU-Rechtsrahmens festzulegen. Im Rahmen des Weißbuches sollen Produkte und Dienstleistungen umfasst werden, bei denen künstliche

---

[1] Die VerfasserInnen sind wissenschaftliche MitarbeiterInnen am Institut für Informations-, Telekommunikations- und Medienrecht (ITM) – zivilrechtliche Abteilung – unter Leitung von Herrn Prof. Dr. Thomas Hoeren an der Westfälischen Wilhelms-Universität Münster im vom BMBF geförderten Drittmittelprojekt GOAL (Fkz.: 01|S19020 A). Weitere Informationen finden sich unter: https://goal-projekt.de.

[2] EU-Kommission, Weißbuch, COM (2020) 65 vom 19.2.2020, abrufbar unter https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_de.pdf, zuletzt aufgerufen am 16.03.2020.

[3] EU-Kommission, Gestaltung der digitalen Zukunft Europas, COM (2020) 67 vom 19.2.2020, abrufbar unter https://ec.europa.eu/info/sites/info/files/communication-shaping-europes-digital-future-feb2020_de_0.pdf, zuletzt aufgerufen am 16.03.2020.

[4] EU-Kommission, Eine europäische Datenstrategie, COM (2020) 66 vom 19.2.2020, abrufbar unter https://ec.europa.eu/info/sites/info/files/communication-european-strategy-data-19feb2020_de.pdf, zuletzt aufgerufen am 16.03.2020.

[5] EU-Kommission, Bericht über die Auswirkungen künstlicher Intelligenz, des Internets der Dinge und der Robotik in Hinblick auf Sicherheit und Haftung, COM (2020) 64 vom 19.2.2020, abrufbar unter https://ec.europa.eu/info/sites/info/files/report-safety-liability-artificial-intelligence-feb2020_de.pdf, zuletzt aufgerufen am 16.03.2020.

[6] Pressemitteilung „Gestaltung der digitalen Zukunft Europas“, https://ec.europa.eu/commission/presscorner/detail/de/ip_20_273, zuletzt aufgerufen am 16.03.2020.

Intelligenz (KI) zum Einsatz kommt. Zu diesem Zwecke muss der Begriff der KI definiert werden. Die EU-Kommission scheint von der Definition der hochrangigen Expertengruppe zu KI, die diese auf Basis eines Vorschlags der Kommission entwickelt hat, überzeugt.[7] Diese kommt zu folgender Definition: „Künstliche Intelligenz--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 das bestmögliche Handeln 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."[8] Auffallend ist zunächst die schiere Merkmalsfülle des Definitionsversuchs. Zehn Merkmale müssen gleichzeitig erfüllt sein, damit es sich um KI handelt. Die Freude von KI-Entwicklern ob dieser Prüfung fällt allen Erwarten nach eher gering aus, die von Großkanzleien umso größer. Jedoch ist nicht von der Hand zu weisen, dass eine ernstzunehmende Definition von KI komplex ausfallen muss.

Es ist jedoch bedenklich, dass im Rahmen des White-Papers nicht differenziert wird, zwischen einem KI-Begriff, welcher u.a. im Rahmen von politischen oder ethischen Diskursen eingesetzt wird, sowie dem KI-Begriff, unter den tatsächlich juristisch subsumiert werden kann und welcher im Rahmen von Sekundärrecht verwendet werden kann. Für die Definition des letztere Begriffs sind die Merkmale „reasoning"[9] und „perception"[10] in der englischen Sprachfassung der Definition, welche auf originärem menschlichem Verhalten[11] aufbauen, überaus problematisch.

Der Gesetzgeber muss sich entscheiden: Entweder er definiert KI im Rahmen der schwelenden Auseinandersetzung mit den Grenzen von Intelligenz, Bewusstsein und Vernunft oder er betrachtet schlicht die jetzigen Modelle, die üblicherweise als „KI" bezeichnet werden und versucht für diese eine generalisierende Definition zu finden. Ein Spagat aus beidem muss misslingen.

## II. Anwendungsbereich

Die EU-Kommission schlägt vor, einen risikobasierten Regulierungsansatz zu wählen.[12] Es soll anhand klarer Kriterien zu bestimmen sein, ob ein „hohes Risiko" vorliege oder nicht. Dies sei zur Wahrung des Verhältnismäßigkeitsgrundsatzes wichtig. Allen Beteiligten müsse „klar und leicht verständlich sein, was unter einer KI-Anwendung mit hohem Risiko zu verstehen ist"[13]. Dies sei anhand zweier Kriterien zu untersuchen: des Sektors und der beabsichtigten Verwendung. Dabei sollen insbesondere die Aspekte Sicherheit, Verbraucherrechte und Grundrechte berücksichtigt werden. Zunächst müsse demnach geprüft werden, ob die KI in einem Sektor eingesetzt wird, in dem aufgrund der typischen Tätigkeiten mit erheblichen Risiken zu rechnen sei. Dadurch erfolge eine Eingrenzung auf Bereiche, in denen das Eintreten von Risiken generell am wahrscheinlichsten ist. Dafür solle der neue Rechtsrahmen diese Sektoren ausdrücklich und abschließend auflisten, wobei diese Liste regelmäßig

[7] Weißbuch, a.a.O. Fn. 2, S. 19, dort insb. auch Fn. 47.
[8] Hochrangige Expertengruppe, Eine Definition der KI: Wichtigste Fähigkeiten und Wissenschaftsgebiete, S. 6, abrufbar unter https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=60664 zuletzt aufgerufen am 16.03.2020; Weißbuch, a.a.O. (Fn. 2), S. 19, dort insb. Fn. 47.
[9] In der deutschen Sprachfassung: „Schlussfolgerung".
[10] In der deutschen Sprachfassung: „Wahrnehmung".
[11] bzw. von biologischen Lebewesen.
[12] Weißbuch, a.a.O. (Fn. 2), S. 20 f.
[13] Weißbuch, a.a.O. (Fn. 2), S. 20.

zu aktualisieren sei. In einem weiteren Schritt sei dann zu schauen, ob die KI so eingesetzt werde, dass mit erheblichen Risiken zu rechnen ist. Grundsätzlich sollten beide Kriterien kumulativ vorliegen, wobei es Ausnahmefälle geben könne, wie etwa bei der Erhebung biometrischer Daten.

Es ist zu begrüßen, dass die EU nun endlich eine Richtung vorgegeben hat, nachdem nicht nur große Unternehmen wie Microsoft, Google und IBM dies gefordert haben[14], sondern auch die Datenethikkommission in ihrem Gutachten dazu konkrete Vorschläge gemacht hat[15]. Letztere hat ein zu dem von der EU-Kommission vorgeschlagenen Modell vergleichbares Abstufungsmodell mit mehreren Risikokategorien für KI-Anwendungen vorgeschlagen.[16] Inwiefern eine erschöpfende Auflistung von Sektoren den beabsichtigten Schutzzweck erfüllt, erscheint fraglich. Es besteht das Risiko, durch eine abschließende Sektorenbenennung riskante Anwendungsfälle von KI in nicht erfassten Sektoren nicht zu berücksichtigen. Dieses Risiko kann jedoch durch eine sektorenunabhängige Ausnahmeregelung für hochriskante KI-Anwendungen, die die EU-Kommission ausdrücklich vorsehen will, gemindert werden. Erheblicher erscheint dagegen das Problem, diese Sektoren mit der generell höchsten Wahrscheinlichkeit zu bestimmen. Gerade aufgrund der erheblichen Bandbreite von KI-Anwendungen ist potentiell jeder Sektor geeignet, Risiken für Einzelne oder die Allgemeinheit zu verursachen. Insofern könnte die versprochene Rechtssicherheit für Betreiber vielmehr in einen Wettbewerb um das beste Lobbying vor der Verabschiedung der Regelung umschlagen. Daher ist die Alternative vorstellbar, aus der Sektoreneinstufung kein Ausschlusskriterium abzuleiten, sondern diese vielmehr als Bewertungsmaßstab zu berücksichtigen. Im Gesundheitsbereich muss unter Umständen eine strengere Prüfung als in der Forstwirtschaft erfolgen. Ein flexibler Bewertungsmaßstab würde mehr Spielraum für die Einstufung der Technologie bieten und so den unterschiedlichsten Anwendungsbeispielen gerecht werden. In juristisch-dogmatischer Hinsicht ist diesbezüglich im Rahmen der Regulierung von KI-Anwendungen die Bildung von Fallgruppen einer enumerativen Aufzählung von Anwendungsfällen vorzuziehen. Zudem könnten einzelne Sektoren weiterhin durch sektorbezogene Regelungen besonders behandelt werden.

## III. Regelungsvorschläge

### 1. Feststellung eines riskanten Anwendungsfalls

Ein weiteres Problem stellt die Feststellung eines riskanten Anwendungsfalls von KI dar. Laut EU-Kommission sollen dabei die Aspekte Sicherheit, Verbraucherrecht und Grundrechte besonders berücksichtigt werden. Sinnvoll ist es dabei sicherlich, neben den Interessen des einzelnen Betroffenen auch gesamtgesellschaftliche Risiken im Rahmen einer sozioinformatischen Gesamtanalyse[17] in die Bewertung miteinzubeziehen. Konkret nennt die Kommission als potentiell betroffene Rechte das Recht auf freie Meinungsäußerung, die Versammlungsfreiheit, die Achtung der Menschenwürde, die Nichtdiskriminierung aufgrund eines Katalogs von Eigenschaften, den Datenschutz, das Recht auf einen wirksamen gerichtlichen Rechtsbehelf und ein faires Verfahren sowie den Verbraucherschutz. Dieser

[14] *Torres*, At Davos, tech leaders call for AI regulation, https://www.ciodive.com/news/at-davos-tech-leaders-call-for-ai-regulation/570768/, zuletzt aufgerufen am 16.03.2020.
[15] Gutachten der Datenethikkommission, S. 173 ff., https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/it-digitalpolitik/gutachten-datenethikkommission.pdf?__blob=publicationFile&v=6, zuletzt aufgerufen am 16.03.2020.
[16] Dies entspricht im Wesentlichen dem von Prof. Dr. Zweig entwickelten Kritikalitätsmodell, siehe *Krafft/Zweig*, Transparenz und Nachvollziehbarkeit algorithmenbasierter Entscheidungsprozesse, Studie im Auftrag des Verbraucherzentrale Bundesverband e.V., 2019, S. 18 ff., https://www.vzbv.de/sites/default/files/downloads/2019/05/02/19-01-22_zweig_krafft_transparenz_adm-neu.pdf, zuletzt aufgerufen am 16.03.2020 (zu sog. Algorithmic Decision Making Systems (ADM-Systeme)).
[17] *Krafft/Zweig, ebd.*, S. 10 ff.

bunt gemischte Strauß an Rechten, der einem schon im Datenschutzrecht begegnet, zeigt die völlige Konturlosigkeit einer vorgestellten Risikobewertung. Ebenso wie im Datenschutzrecht bleibt völlig unklar, wie das Risiko für einen Betroffenen eigentlich aussieht. Es droht ein neues Metarecht, das sich über die gesamte Rechtsordnung erstreckt. Die durch die DSGVO für die Datenverarbeitung geschaffene Rechtsunsicherheit könnte durch zusätzliche horizontale Regeln für KI noch verstärkt werden, deren Vereinbarkeit mit der DSGVO zudem völlig unklar bleibt. Darüber hinaus würde die fast unbegrenzte Zwecksetzung der Regelung einer Aufsichtsbehörde weitreichende Befugnisse verschaffen, ähnlich wie es jetzt schon bei Datenschutzbehörden kritisiert wird. Selbst eine Abgrenzung von Befugnissen zwischen Datenschutz- und „Algorithmusbehörden" lässt das Weißbuch offen.

Zuletzt sehnt man sich vergeblich nach einer Aussage darüber, wer die folgenschwere Entscheidung, ob ein Risiko vorliegt eigentlich vornehmen soll. Der Staat, eine staatlich regulierte Zertifizierungsstelle oder gar der Betreiber selbst? Im Rahmen des White Papers wäre es notwendig gewesen, den genauen Adressaten der Prüfungspflicht zu benennen. Die vorgestellten Maßnahmen stellen sich sonst ohne hinreichende Kontur dar.

## 2. Anforderungen an algorithmische Hochrisikosysteme

Im Anschluss werden in dem Papier konkrete Anforderungen formuliert, welche an die zuvor beschriebenen Hochrisikosysteme zu stellen sein könnten. Dabei wird nach verschiedenen Schlüsselmerkmalen beziehungsweise Risikofaktoren differenziert, an die man regulatorisch anknüpfen könnte.

### *a. Trainingsdaten*

Begonnen wird zunächst mit den Trainingsdaten, welche die Funktionsweise und Entscheidungen der trainierten KI maßgeblich beeinflussen. Die Kommission schlägt die Formulierung von Vorschriften vor, die sicherstellen sollen, dass die Trainingsdatensätze vollständig und repräsentativ sind. So sollen Diskriminierung und die Entstehung anderer gefährlicher Situationen durch den Einsatz von KI vermieden werden.[18] Richtig an diesem Ansatz ist die Erkenntnis, dass die verwendeten Trainingsdatensätze eine entscheidende Rolle beim Risikomanagement von KI spielen. Die simpel gehaltene Vorgabe, dass die verwendeten Datensätze ausreichend repräsentativ sein müssen, übersieht aber das praktische Problem, dass im Vorhinein nicht immer erkennbar ist, ob ein Datensatz diesen Anforderungen wirklich entspricht. So ist beispielsweise an die Möglichkeit der sogenannten Proxy Discrimination[19] zu denken, bei der eine Diskriminierung aufgrund eines verbotenen Merkmals (i.S.d. AGG oder der GR-Charta) anhand eines anderen Indikators stattfindet, sodass das Fehlen des verbotenen Merkmals in den benutzten Daten dennoch keine Sicherheit vor entsprechender Diskriminierung bietet. Die praktische Umsetzung dieser scheinbar naheliegenden Lösung dürfte daher erhebliche Schwierigkeiten bereiten.

### *b. Aufbewahrung von Daten und Aufzeichnungen*

Anschließend geht die Kommission auf eine mögliche Pflicht zur Aufbewahrung von Daten und Aufzeichnungen beziehungsweise von Informationen über diese ein, die Aufschluss über Programmierung und Training des jeweiligen KI-Systems geben könnten.[20] Dies soll das Problem der

[18] Weißbuch, a.a.O. (Fn. 2), S. 22 f.
[19] Vgl. ausführlich zum Problem der „Proxy Discrimination" *Prince/Schwarcz,* Iowa Law Review, Forthcoming, verfügbar auf https://ssrn.com/abstract=3347959, zuletzt aufgerufen am 11.03.2020.
[20] Weißbuch, a.a.O. (Fn. 2), S. 23.

Komplexität und Intransparenz vieler KI-Anwendungen adressieren, welches häufig die Rückverfolgbarkeit von KI-Entscheidungen und die Überprüfung der Einhaltung der geltenden Vorschriften durch den Einsatz von KI erschwert. Es ist aber zu beachten, dass hier unter Umständen erhebliche Konflikte mit dem Datenschutzrecht drohen. Wenn Trainingsdatensätze selbst gespeichert werden sollen, nimmt dies den Charakter einer vorrätigen Speicherung personenbezogener Daten an, die mit dem Grundsatz der Datenminimierung des Art. 5 Abs. 1 lit. c DSGVO in einem Spannungsverhältnis stehen dürfte. Deshalb stellt sich die Frage, inwieweit eine gleichrangige horizontale Regelung diesen Grundsatz verdrängen könnte. Das Prinzip der Datenminimierung ist essentieller Ausdruck des Zweckbindungsgrundsatzes, welcher in Art. 8 Abs. 2 S. 1 EU-GR Charta primärrechtlich verankert ist. Daher könnte eine Einschränkung des Datenminimierungsgrundsatzes nur im Wege der praktischen Konkordanz erfolgen. Die Kollision des Datenminimierungsgrundsatz mit einer Aufzeichnungspflicht kann möglicherweise durch die Methode der „differential privacy“[21] aufgelöst werden, die Behörden nachträglich die Überprüfung von KI-Entscheidungen ermöglichen könnten.

### *c. Bereitstellung von Informationen über die KI*

Ein weiterer Regulierungsvorschlag betrifft die Bereitstellung von Informationen über die KI. So sollen den Betreibern von KI-Systemen unter anderem Informationen über Fähigkeiten und Grenzen des Systems zur Verfügung gestellt werden.[22] Dies scheint ein grundsätzlicher sinnvoller Ansatz zu sein, um sicherzustellen, dass die Systeme nur bestimmungsgemäß eingesetzt werden und das Training auch im Hinblick auf die entsprechenden Situationen erfolgt ist. Insbesondere lobenswert an diesem Vorschlag ist, dass dieser eine geringe Eingriffsintensität aufweist und dennoch geeignet erscheint, grobe Fehlerquellen beim Einsatz von KI zu vermeiden.

### *d. Robustheit und Genauigkeit*

Im Übrigen betont die EU-Kommission die Relevanz der Robustheit und Genauigkeit von KI-Systemen. Mag diese Feststellung auch richtig sein, folgen im Papier keine konkreten Vorschläge, wie deren Gewährleistung sichergestellt werden könnte.

### *e. Menschliche Mitwirkung*

Zuletzt stellt die Kommission klar, dass das Ziel einer vertrauenswürdigen, ethischen und menschenzentrierten KI aus ihrer Sicht nur erreicht werden könne, wenn die Mitwirkung von Menschen bei KI-Entscheidungen sichergestellt sei. Dazu werden verschiedene Möglichkeiten in den Raum gestellt, wie die Abhängigkeit des Wirksamwerdens einer KI-Entscheidung von einer vorherigen menschlichen Überprüfung, eine nachträgliche Kontrolle der Ergebnisse oder eine begleitende Überwachung des Systems durch einen Menschen. Solche Formen der Kontrolle, gerade in Form der Vorab-Kontrolle sind zugegebenermaßen recht effektiv, um evidente Fehler der KI noch vor einer realen Auswirkung zu erkennen. Kommt es auf eine detailliertere Prüfung an, könnte ein kontrollierender Mensch aber aufgrund des sogenannten automation bias dazu geneigt sein, nur zurückhaltend einzuschreiten, weil er letztlich (unterbewusst) auf die Richtigkeit der maschinellen Entscheidung vertraut. Außerdem ist zu bedenken, dass jede menschliche Beteiligung die Vorteile einer Implementierung von KI-Systemen teilweise einschränkt, teilweise sogar ganz zu Nichte macht, wenn es gerade auf die völlige Automatisierung von Handlungsabläufen ankommt. Vorstellbar ist eine solche Vorab-Kontrolle daher vor allem bei schwerwiegenden Entscheidungen einer KI über einen Menschen mit unmittelbarer Rechtsfolge (Einstellung, Kündigung, Verwaltungsakt). Grundsätzlich

[21] Siehe dazu *Kearns/Roth*, The Ethical Algorithm: The Science of Socially Aware Algorithm Design, New York 2019, S. 22 ff.
[22] Weißbuch, a.a.O. (Fn. 2), , S. 23 f.

sollte vor Einführung von Mitwirkungsverpflichtungen sorgsam geprüft werden, ob der konkrete Einsatz der KI die Schaffung solcher Pflichten vor dem Hintergrund eines potentiellen Innovationshemmnis für Unternehmen rechtfertigt.

## IV. Regelungsadressaten

Im Anschluss wird in dem White Paper das Problem des richtigen Adressaten der Neuregelungen aufgeworfen. So kommen mit Entwicklern, Händlern, Betreibern etc. viele verschiedene Akteure in Betracht. Die Kommission spricht sich dafür aus, dass die zu statuierenden Pflichten jeweils dem Akteur zugewiesen werden, der am ehesten in der Lage ist, die potentiellen Risiken zu bewältigen. Hinsichtlich der räumlichen Anwendbarkeit der Reformen soll das Marktortprinzip gelten. Konkreter werden die Forderungen im Übrigen nicht.

## V. Rechtsdurchsetzung

Zuletzt trifft die Kommission Aussagen zur Einhaltung und Durchsetzung der Regeln. Favorisiert wird dabei eine vorab vorzunehmende Konformitätsbewertung, die im Hinblick auf die Auflagen für Hochrisikosysteme durchgeführt werden soll. Orientiert werden soll sich dabei an in der EU bereits bestehenden Konformitätsbewertungsmechanismen beispielsweise im Bereich der Cybersicherheitszertifizierungen[23]. Es ist zu beachten, dass es sich bei den bestehenden Bewertungsmechanismen häufig um Formen der Selbstzertifizierung handelt, das heißt der Unternehmer prüft die Einhaltung der geltenden Sicherheitsvorschriften durch sein Produkt selbst. Zwar mag auf den ersten Blick zweifelhaft erscheinen, dass diese Form der Selbstkontrolle genauso effektiv ist wie eine externe Kontrolle durch den Staat. Jedenfalls kann aber davon ausgegangen werden, dass die Selbstzertifizierung dazu führt, dass den betroffenen Akteuren die Relevanz der Einhaltung der Vorschriften deutlich gemacht wird und sich damit zwingend auseinandergesetzt werden muss. Im Übrigen scheint eine flächendeckende ex-ante-Kontrolle sämtlicher KI-Systeme schon wegen ihrer schieren Menge kaum praktikabel und wäre auch deutlich zu eingriffsintensiv. Zudem können Marktaufsichtsbehörden die vorgebebenen Anforderungen ex post überprüfen und durchsetzen. Die Unternehmen handeln damit bei der Selbstzertifizierung im ständigen Bewusstsein einer nachträglich möglichen staatlichen Kontrolle.

## VI. Bedenkliche KI-Anwendungen

In dem Weißbuch werden die Werte der EU in den Vordergrund gerückt. Es hat sich bereits im April 2019 die hochrangige Expertengruppe für KI in ihren Ethik-Leitlinien mit – für die EU-Werte – bedenklichen KI-Anwendungen auseinandergesetzt.[24] Allerdings greift die EU-Kommission von den dort als bedenklich eingestuften KI-Anwendungen lediglich Systeme für eine biometrische Fernidentifikation auf. Weitere laut der Ethik-Leitlinien als bedenklich einzustufende KI-Anwendungen werden in dem Weißbuch unberücksichtigt gelassen. Dies ist u.a. der verdeckte Einsatz von KI-Systemen. Es scheint fraglich, inwieweit ein „Vertrauen“ gegenüber KI-Anwendungen aufgebaut werden soll, wenn diese verdeckt eingesetzt werden dürfen. Die fehlende Berücksichtigung der Möglichkeit eines Totalverbots von KI lässt befürchten, dass aufgrund wirtschaftlicher Interessen stark bedenkliche Systeme dennoch marktfähig gemacht werden.[25] Dies gilt insbesondere für letale

[23] Vgl. dazu EU-VO 2019/881.

[24] Hochrangige Expertengruppe für künstliche Intelligenz, Ethik-Leitlinien für eine vertrauenswürdige KI, S. 44 f, abrufbar unter https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=60425, zuletzt aufgerufen am 16.03.2020.

[25] Siehe auch *Metzinger*, Nehmt der Industrie die Ethik weg!, https://www.tagesspiegel.de/politik/eu-ethikrichtlinien-fuer-kuenstliche-intelligenz-nehmt-der-industrie-die-ethik-weg/24195388.html, zuletzt

autonome Waffensysteme, die eine dramatische Steigerung von Konfliktpotenzialen auch unter den Bedingungen symmetrischer Kriegsführung bedeuten könnten.[26]

### VII. Einsatz von KI durch Behörden

Die Kommission hat keine Differenzierung vorgenommen zwischen KI-Systemen, welche durch Behörden eingesetzt werden und solchen die durch Privatunternehmen verwendet werden. Das erinnert an die DSGVO, die ebenso private und staatliche Verantwortliche gleichbehandelt.

Es wird wie in der DSGVO wieder keine Differenzierung zwischen der Anwendung im Rahmen des Öffentlichen Rechts und des Zivilrechts gemacht. Diese traditionelle Unterscheidung ist jedoch notwendig, um Rechtsgüterabwägungen sinnvoll durchzuführen und Grundrechte im Rahmen ihrer gegenüber dem Staat abwehrrechtlichen Dimension und gegenüber Privatpersonen im Rahmen ihrer Schutzpflichten zu betrachten. Privatpersonen werden mit Pflichten belegt, denen eigentlich nur der Staat unterliegt und umgekehrt nimmt der Staat für sich trotz seiner unmittelbaren Grundrechtsbindung keine weitergehenden Pflichten an. Eine mangelnde Differenzierung zwischen öffentlichem Recht und Privatrecht zeigt somit einerseits den nicht zu verkennenden wachsenden Einfluss von transnationalen Big-Tech-Unternehmen, andererseits aber genauso den mangelnden hoheitlichen Blickwinkel im Rechtssetzungsprozess, in welchem nicht mehr unterschieden wird, ob „durch" Staaten „Macht" ausgeübt wird oder „durch" Privatpersonen. Grundsätzlich greifen für Privatpersonen nicht dieselben Einschränkungen wie für Staaten. Staaten müssen sich an den Verhältnismäßigkeitsgrundsatz halten, wobei bei eingriffsintensiven Maßnahmen lediglich die erforderlichen und angemessenen Eingriffe rechtfertigbar sind.

### VIII. Fazit

Im Rahmen eines europäischen Konzeptes für Exzellenz und Vertrauen hätte man sich gewünscht, dass die EU-Kommission weitere Regelungsinstrumente wie beispielsweise eine strengere ex-ante Kontrolle von KI-Systemen in den Blick nimmt. Gleichzeitig werden Werte und Grundrechte, sowie ausdrücklich das Vertrauen in KI (Stichwort „trustworthy AI") in den Vordergrund gerückt, eine Auseinandersetzung mit diesen findet durch die Kommission jedoch – soweit die EU überhaupt eine Regelungskompetenz dazu besitzt – nicht statt.

## B. Datenstrategie

In Anerkennung der Wichtigkeit von Daten, die gewissermaßen als Rohstoff für die Entwicklung von KI fungieren, hat die EU-Kommission neben dem Weißbuch zu KI auch ein Datentrategiepapier veröffentlicht, in dem sie erklärt, wie sie zukünftig innerhalb der EU einen erfolgreichen europäischen Datenbinnenmarkt schaffen will.[27] Die Datenstrategie der EU setzt deutliche Schwerpunkte auf der

aufgerufen am 16.03.2020 zur Kritik an der Besetzung der hochrangigen Expertengruppe zu künstlicher Intelligenz.

[26] Siehe zur Kritik an autonomen letalen Waffensystemen *Sauer*, Stopping 'Killer Robots': Why Now Is the Time to Ban Autonomous Weapons Systems, https://www.armscontrol.org/act/2016-09/features/stopping-%E2%80%98killer-robots%E2%80%99-why-now-time-ban-autonomous-weapons-systems, zuletzt aufgerufen am 16.03.2020.

[27] EU-Kommission, Eine europäische Datenstrategie, COM (2020) 66 vom 19.2.2020, abrufbar unter https://ec.europa.eu/info/sites/info/files/communication-european-strategy-data-19feb2020_de.pdf, zuletzt aufgerufen am 16.03.2020.

Förderung von Datenzugang und -nutzung, der Schaffung größerer Cloudinfrastrukturen sowie der Vereinheitlichung von Standards in einem gemeinsamen digitalen Datenbinnenmarkt. Die enorme Bedeutung von Daten für die europäische Wirtschaft und die besondere Dringlichkeit der Förderung von Datenräumen und der Data Economy wird dabei ausdrücklich von der EU-Kommission erkannt. Im Rahmen dessen schlägt sie zahlreiche Governance-Optionen angefangen von selbstregulierenden Kodizes und Absprachen, über Leitlinien und Empfehlungen bis hin zu echten gesetzlichen Regulierungen vor.

Zunächst ist festzuhalten, dass zahlreiche Vorschläge der EU-Kommission absolut sinnvoll erscheinen. Eine größere Unabhängigkeit von amerikanischen und chinesischen Cloud-Dienstleistern ist unbedingt wünschenswert, um einen echten europäischen Datenraum, der auf europäischen Rechtestandards basiert, zu schaffen. Datenzugangsrechte sind insb. für kleinere und mittlere Unternehmen (KMUs), wie die EU-Kommission selber betont, von großer Bedeutung, um innovative Ideen in der Data Economy zu verwirklichen. Sie sind zudem geeignet, die marktbeherrschenden Stellungen von digitalen Plattformen, die die EU-Kommission zutreffend beschreibt (insbesondere auch die Macht solcher Unternehmen, erhobene Daten marktübergreifend zu verwenden), eindämmen. Richtig wird auch die Problematik mangelnder Interoperabilität von Daten erkannt, die die Weitergabe von Daten und deren übergreifende Nutzung erheblich erschwert.

Letztlich bleibt das Strategiepapier aber absolut vage in seinen Vorschlägen. Es werden kaum echte Vorschläge gemacht. Stattdessen wird hauptsächlich auf zukünftige Projekte, Initiativen, Kodizes, Empfehlungen und Gesetze verwiesen. Insbesondere deren zeitliche Planung überrascht. Ein erster Vorschlag für einen Data Act, in dem u.a. Nutzungsrechte an nicht personenbezogenen Daten festgelegt werden sollen, soll schon im vierten Quartal 2021 veröffentlicht werden. Eine vorsichtig formuliert mutige Ansage, bedenkt man die komplexe Abgrenzung von personen- und nicht personenbezogenen Daten, sowie die damit einhergehende Konkurrenz zur DSGVO, die erforderliche genaue Analyse der ökonomischen Auswirkungen gesetzlicher Nutzungsrechte je nach deren Ausgestaltung und die vielen weiteren Problematiken. Gerade die Rede von gesetzlichen Nutzungsrechten ist dabei äußerst kritisch zu betrachten. In der Rechtswissenschaft wurde immer wieder das Risiko der Schaffung subjektiver Rechte an Daten diskutiert, nicht nur bei personen-, sondern auch bei nicht personenbezogener Daten.[28] Es ist völlig unklar, ob solche dinglichen Nutzungsrechte an Daten ökonomisch sinnvoll sind oder nicht. Noch viel unklarer ist darüber hinaus, wem die Einräumung solcher Rechte zustehen soll. Dazu findet man im Strategiepapier allerdings nichts. Es ist schlicht die Rede vom Dateninhaber und Datennutzer – ohne weitere Definition. Diese Definition, die entscheidende Bedeutung für die gesamte Diskussion um ein Recht an Daten hat, ist also völlig ungeklärt und soll nun bis zum vierten Quartal 2021, also in weniger als zwei Jahren wesentlich geklärt sein. Es kann sich hier nur um blinden Aktionismus handeln, vor dem nur eindrücklich gewarnt werden kann angesichts der großen Folgen, die die Verdinglichung von Daten für die gesamte Datenwirtschaft haben würde.

Wenn die EU-Kommission insofern auch Datenzugangsrechte in Betracht zieht, diese vornehmlich durch Selbstregulierung schaffen möchte und ansonsten sektorbezogene gesetzliche Zugangsansprüche schaffen möchte, ist dies überaus sinnvoll. Allein: die Aussage, dass bei der

[28] Siehe dazu insb. den Bericht der Arbeitsgruppe Digitaler Neustart der Konferenz der Justizministerinnen und Justizminister Digitaler Neustart, 2017, S. 29 ff., abrufbar unter https://www.justiz.nrw.de/JM/schwerpunkte/digitaler_neustart/zt_bericht_arbeitsgruppe/bericht_ag_dig_neustart.pdf, zuletzt aufgerufen am 16.03.2020, der keine Rechte an Daten de lege lata annimmt und die Schaffung neuer Rechte an Daten de lege ferenda ablehnt.

Regulierung solcher Zugangsrechte die Interessen des Dateninhabers abgewogen werden müssen, zeigt erneut, wie sehr das Strategiepapier eine aktionistische Maßnahme darstellt, ohne dass irgendwelche für das Zivilrecht zentrale Fragen geklärt sind. Insofern muss das Strategiepapier als das gesehen werden, was es ist: Eine Ankündigung für die Zukunft, ein Aufruf zum Handeln im Bereich der Data Economy, mehr nicht, weniger aber auch nicht. Der Wettbewerb um die Vorherrschaft im Datenuniversum wurde spätestens jetzt von der EU voll angenommen.