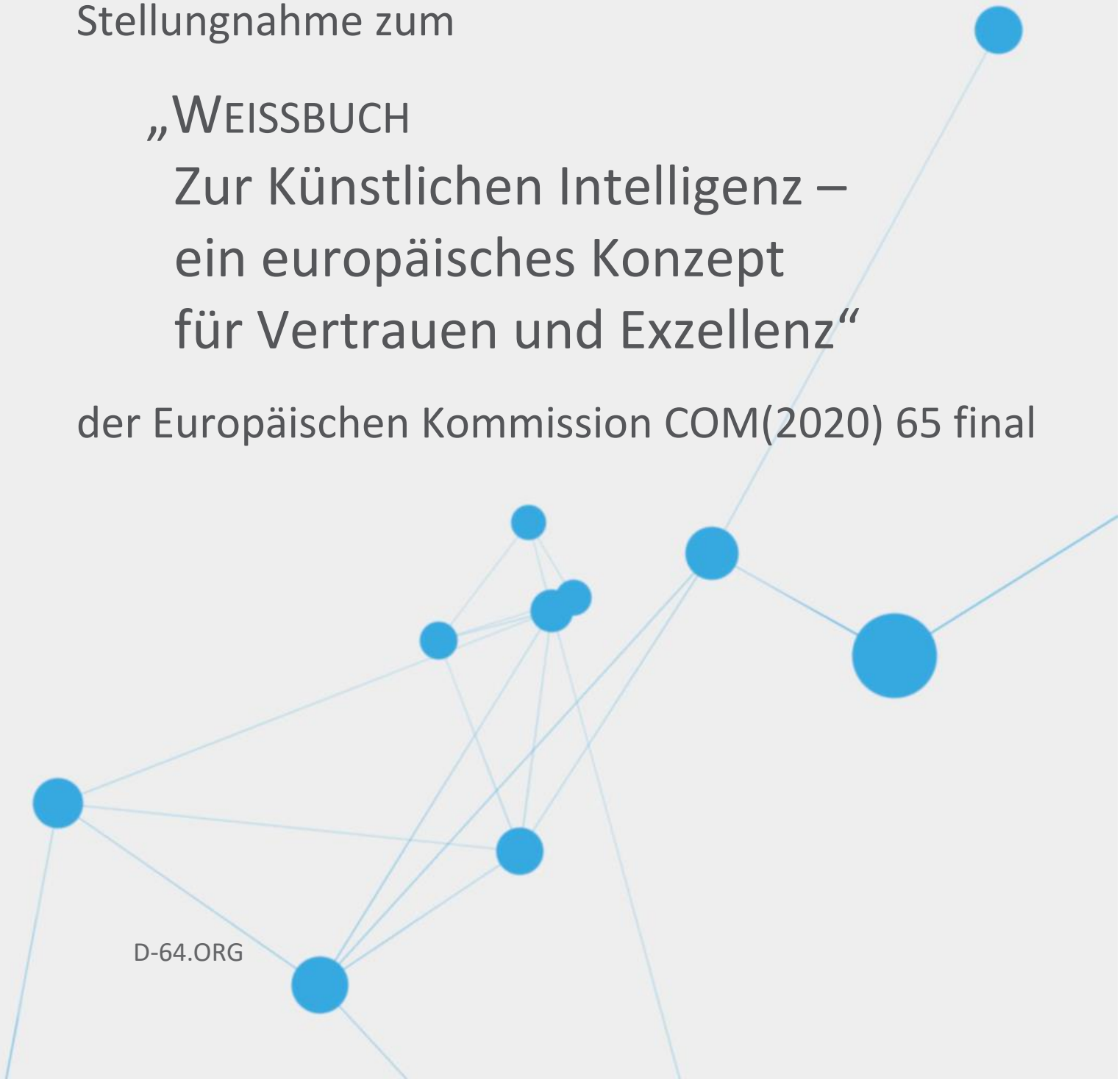
D64
Zentrum für
Digitalen Fortschritt

Die Regulierung Künstlicher Intelligenz und anderer algorithmischer Entscheidungssysteme

Stellungnahme zum

„Weissbuch
Zur Künstlichen Intelligenz –
ein europäisches Konzept
für Vertrauen und Exzellenz“

der Europäischen Kommission COM(2020) 65 final



D-64.ORG

Eine Arbeitsgruppe aus Mitgliedern der AG Künstliche Intelligenz von D64 sowie weiteren externen Mitarbeitenden hat sich intensiv mit dem von der EU-Kommission (im Folgenden KOM) vorgelegten Weißbuch „Zur Künstlichen Intelligenz – ein europäisches Konzept für Exzellenz und Vertrauen“ befasst und nimmt dazu im Folgenden detailliert Stellung.

Die Arbeitsgruppe hat es trotz Bemühungen nicht geschafft, das selbstgesetzte Ziel der Geschlechterparität innerhalb der Arbeitsgruppe zu erreichen. Eine Veröffentlichung der Stellungnahme wurde daraufhin ausführlich diskutiert. Die Arbeitsgruppe hat nach langer Diskussion beschlossen, die Stellungnahme der Öffentlichkeit zugänglich zu machen und den Mangel fehlender Parität dabei proaktiv zu thematisieren.

Die Veröffentlichung dieser Stellungnahme ist in diesem Sinne als „lebendes Dokument“ zu verstehen und soll als Grundlage für eine weitere öffentliche und vor allem inklusive Diskussion dienen. Ziel ist es, die Positionen aus dieser Stellungnahme und ggf. weitere Positionen zum Thema Künstliche Intelligenz aus unterschiedlichen Perspektiven zu beleuchten, die unsere heterogene Gesellschaft bestmöglich widerspiegeln. Diese Diskussion wird D64 zeitnah anstoßen.

INHALTSVERZEICHNIS

A. ABSTRACT

D64 begrüßt es, dass die EU-Kommission ein europäisches Konzept für Künstliche Intelligenz vorlegt, sieht jedoch auch Potenzial für Nachbesserungen. Diese regen wir in dieser Stellungnahme an. Unsere Stellungnahme ist von folgenden **Leitgedanken** getragen:

- **DIGITALISIERUNG IST KEIN SELBSTZWECK, SONDERN HEBEL ZUR STEIGERUNG UNSERES GESAMTGESELLSCHAFTLICHEN WOHLERGEHENS**

  D64 sieht sich insbesondere den europäischen **Grundwerten Freiheit, Gerechtigkeit und Solidarität** verpflichtet.[1] **Digitalisierung und Technologisierung sind kein Selbstzweck**. Aufgabe der Politik, Wirtschaft und Zivilgesellschaft ist es, Künstliche Intelligenz (KI) und andere algorithmische Systeme - wie jede andere Technologie auch - als Mittel zu begreifen, um diese Grundwerte zu stärken und das gesamtgesellschaftliche Wohlergehen zu vergrößern. Unter den richtigen Rahmenbedingungen können und sollten algorithmische Systeme aus Sicht von D64 zu einer gerechteren Entscheidungsfindung[2], zum Schutz unserer Gesundheit[3], zur Steigerung der Nachhaltigkeit[4] u.v.m. eingesetzt werden.

- **VERHÄLTNISMÄßIGE REGULIERUNG UND INNOVATIONSFÖRDERUNG SIND KEINE GEGENSPIELER, SONDERN GEHEN HAND IN HAND**

  Um die technologische Entwicklung in Richtung der erwünschten Zwecke zu steuern, ist aus Sicht von D64 neben dem Mittel der Förderung (*Ökosystem für Exzellenz*) gerade auch das Mittel der Regulierung (zum Schaffen eines *Ökosystems für Vertrauen*) erforderlich. Wir begreifen **verhältnismäßige Regulierung und Innovationsförderung als Zusammen- und nicht als Gegenspieler**: Regulierung schützt unsere Grundrechte und verhindert den gemeinwohlschädlichen Einsatz neuer Technologien. Damit baut sie Vorbehalte ab und trägt so wiederum zur verstärkten Nutzung neuer Technologien bei. Mit einer verstärkten Nutzung (Nachfrage) geht auch eine gesteigerte Entwicklung europäischer, digitaler Innovationen (Angebot) einher. Regulierung trägt somit letztlich zu unserer Wohlstandssicherung bei.

  Wir sind überzeugt, dass der Aufbau und die Stärkung einer eigenständigen europäischen Digitalwirtschaft möglich sind, die neben anderen 'digitalen Großmächten' wie den USA und China bestehen kann und gleichzeitig Produkte und Dienstleistungen anbietet, die unsere Grundwerte achten und stärken. Hierzu gilt es, die bestehende europäische Expertise mit einem ethischen Gebrauch von KI und anderen algorithmischen Systemen zu harmonisieren.

  Wir befürworten daher auch, dass die KOM nicht alleine auf das Mittel der Selbstregulierung oder des nachgelagerten Haftungsrechts setzt, sondern Vorgaben für die Entwicklung und den Einsatz von KI schaffen möchte. Den von der KOM gewählten **risikobasierten Ansatz** begrüßen wir grundsätzlich, regen jedoch eine Verbesserung der vorgeschlagenen Operationalisierung an. Der Ansatz fußt letztlich auf dem Gebot der Verhältnismäßigkeit staatlicher Eingriffe. Nur so ist ein angemessener Ausgleich zwischen dem Ziel, Vertrauen zu schaffen, und den Nachteilen unerwünschter Überregulierung möglich.

---

[1] Siehe insb. D64 – Zentrum für Digitalen Fortschritt, Grundwerte in der digitalisierten Gesellschaft, Der Einfluss Künstlicher Intelligenz auf Freiheit, Gerechtigkeit und Solidarität, November 2018, online: https://d-64.org/wp-content/uploads/2018/11/D64-Grundwerte-KI.pdf.

[2] Beispielsweise bei der Vergabe begrenzter Ressourcen wie Kita- oder Studienplätze, bei Einstellungsverfahren etc.

[3] Beispielsweise durch Krebs-Erkennungs-Software, sicherer Verkehr durch selbstfahrende Autos etc.

[4] Beispielsweise durch sparsameren Ressourceneinsatz in der industriellen Fertigung etc.

Die KOM sollte ihre guten Vorschläge aus Sicht von D64 daher insbesondere an folgenden Stellen **nachbessern**:

I. ORIENTIERUNG AM GESELLSCHAFTLICH ERWÜNSCHTEN, ANSTELLE EINER ORIENTIERUNG DES NORMATIVEN AM FAKTISCHEN

- Erstens teilen wir nicht die Prämisse, man müsse sich auf „eindeutig festgestellte Probleme beschränken, für die es praktikable Lösungen gibt“ (S. 12). Dies wird der europäischen Tradition der risikominimierenden Regulierung nicht gerecht. Ungewissheiten bezüglich der Auswirkungen neuer Technologien sind seit jeher kein pauschaler Ausschlussgrund für vorbeugende Risikominimierung (vgl. anstelle vieler: Gentechnikrecht). Zudem dürfen technische Gegebenheiten nicht den Gesetzgebungsprozess determinieren: Der Gesetzgeber gibt vor, was die Technik darf und nicht andersherum. In Ermangelung praktikabler Lösungen kommt als *ultima ratio* bei unvertretbar hohen Risiken für Individuen oder unsere Gesellschaft als Ganzes auch stets ein Verbot des Einsatzes bestimmter Anwendungen als praktikable Lösung in Betracht.
- Zweitens sollten technische Schwierigkeiten nicht *per se* über den normativen Anforderungskatalog bestimmen. Beim Einsatz von KI können sich zwar - insbesondere mit Blick auf tiefe neuronale Netze - neue technische Herausforderungen stellen, z.B. bezüglich der Herstellung von Transparenz und Nicht-Diskriminierung. Aufgrund der allgemeinen Handlungsfreiheit werden z.B. gerade bei nicht gewerblichen Tätigkeiten im Digitalen - ebenso wie im Analogen - weiterhin intransparente, qualitativ schlechte (z.B. auf veralteten Daten beruhende) und u.U. sogar diskriminierende Entscheidungen hinzunehmen sein. Im Zentrum sollte stets zuerst die Betrachtung des Risikos stehen, und sodann die Definition der gesellschaftlich erwünschten Anforderungen - unabhängig von der Frage, wie schwer oder einfach diese technisch zu erreichen sind.

II. ORIENTIERUNG AM KONKRETEN RISIKO, ANSTELLE VON EINZELNEN TECHNOLOGIEN UND SEKTOREN

- Wir raten davon ab, den antizipierten Regulierungsrahmen auf den Einsatz von **KI** in einzelnen **Sektoren** zu limitieren (Weißbuch, S. 19 ff.[5]).
- Zurzeit existiert keine allgemein anerkannte und erschöpfende Definition von KI. Zudem können algorithmische Systeme ohne KI-Komponente zu den exakt selben Zwecken mit den exakt selben Risiken eingesetzt werden wie „KI“.
- Ein algorithmisches Entscheidungssystem kann in mehreren Sektoren zum Einsatz kommen. Zwar lassen sich unter Umständen Sektoren ausmachen, in denen der Einsatz typischerweise besonders risikogeneigt ist. Diese typisierte Betrachtung darf aber nicht den Blick darauf verstellen, dass algorithmische Entscheidungssysteme auch jenseits dieser Sektoren im Einzelfall zu schwerwiegenden Grundrechtseingriffen führen können. Umgekehrt existieren in jedem Sektor auch gänzlich unriskante Anwendungen.
- Der regulatorische Anwendungsbereich sollte daher algorithmische Systeme umfassen, die aufgrund ihrer konkreten Verwendung zur **Entscheidung über Menschen** anhand von Daten zu hohen **Risiken** für grundrechtlich geschützte Güter führen.

[5] Alle im Folgenden genannten Seitenzahlen beziehen sich – sofern nicht gesondert gekennzeichnet – auf das Weißbuch KI der Europäischen Kommission.

III. „GESTUFTE REGULIERUNG“, ANSTELLE EINER BINÄREN UNTERTEILUNG IN ANWENDUNGEN MIT UND OHNE HOHES RISIKO

- Die Kommission möchte in Anwendungen ohne Risiko und Anwendungen mit hohem Risiko unterteilen. Für letztere sollen stets alle Anforderungen (von menschlicher Aufsicht über Transparenz bis hin zu Qualität/Robustheit) gleichzeitig gelten (Weißbuch, S. 22 ff.).
- Wir halten diese binäre Unterteilung für zu undifferenziert. Erforderlich ist eine „gestufte Regulierung“, die je nach konkretem Risiko feingranularere Abstufungen vorsieht (siehe Abbildung unten). Je größer das Risiko der Anwendung ist, desto mehr Anforderungen müssen erfüllt werden. Dabei kommen je Stufe immer weitere Anforderungen hinzu. Wenn z.B. ein Algorithmus basierend auf den Ergebnissen des Online-Fragebogens auf Stufe 4 eingeordnet wird, muss dieser auch Anforderungen 2 und 3 erfüllen. Konkret dürfte diese Anwendung dann nur eingesetzt werden, wenn ein Mensch sie kontrolliert (Menschliche Aufsicht) sowie die betroffene Person darüber informiert wird, dass (Transparenz „Ob“) und in welcher Form (Transparenz „Wie“) ein Algorithmus für die Entscheidung zum Einsatz kommt. Mit „gestufter Regulierung“ wird sichergestellt, dass das Risiko einer Anwendung in einem verhältnismäßigen Maß zu ihrer Regulierung steht.

IV. „TASTENDE REGULIERUNG“, ANSTELLE EINES REGULATORISCHEN SCHNELLSCHUSSES

- „Tastend“ heißt, dass der Gesetzgeber nicht von Anfang an alle Stufen festlegt, sondern in **einem ersten Schritt nur die erste Stufe** verpflichtend macht. Das heißt, dass Akteure, die algorithmische Entscheidungssysteme einsetzen, einen **einfachen Online-Fragebogen** ausfüllen. Um dieses behördliche Wissen sodann in **gesamtgesellschaftliches Wissen** zu transferieren, sollten die Behörden Jahresberichte sowie die gesammelten statistischen Daten zur Verwendung von algorithmischen Entscheidungssystemen und den dabei entstehenden Risiken veröffentlichen.
- Basierend auf diesen Ergebnissen sollte der Gesetzgeber dann die Anwendungen auswählen, für **in weiteren Schritten die weitergehenden Anforderungen** wie z.B. im Hinblick auf Nicht-Diskriminierung, menschliche Aufsicht, Genauigkeit und Robustheit gelten. Der Gesetzgeber lernt also kontinuierlich hinzu und erhebt Daten für die weitere Regulierung.

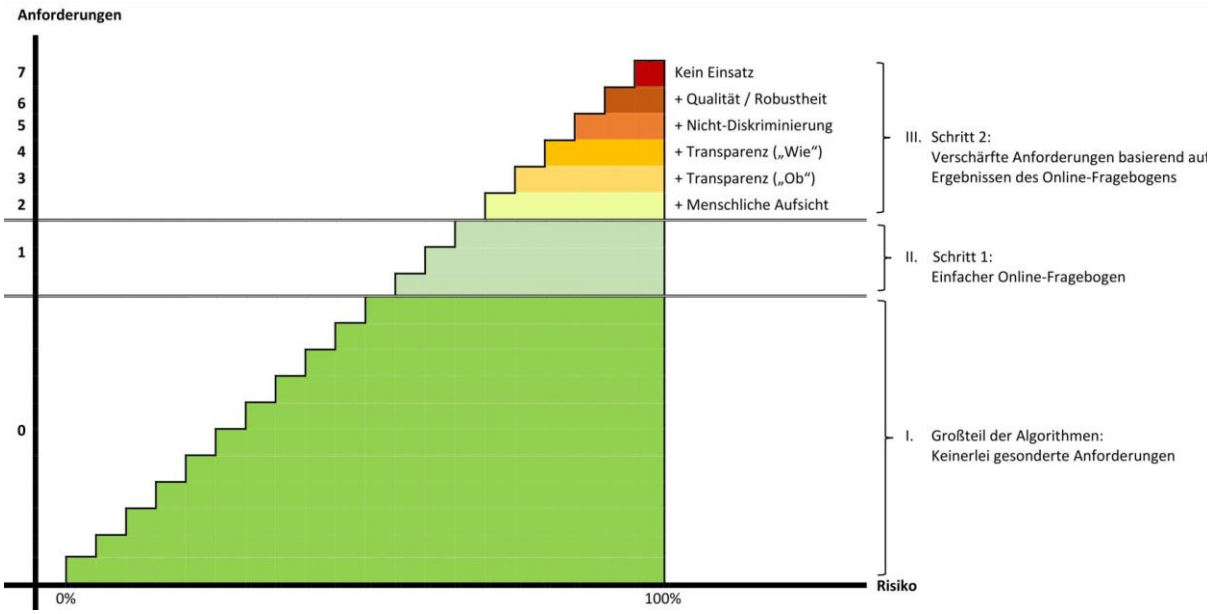


Abbildung 1: „Gestufte“ und „tastende“ Regulierung.

B. DETAILLIERTE POSITIONEN ZUM „ÖKOSYSTEM FÜR VERTRAUEN“

Wir begrüßen die im Kapitel zum ***„Ökosystem für Exzellenz“*** (S. 6 - 10) der KOM vorgeschlagenen Fördermaßnahmen nahezu vollumfänglich und sehen daher insoweit keinen Anlass für eine ausführliche Stellungnahme. Es gilt jedoch zu betonen, dass diese Maßnahmen in gleichem Maße wie das *Ökosystem für Vertrauen* (S. 10 - 31) der Förderung der oben geschilderten Zwecke dienen müssen. Dies muss z.B. bezüglich finanzieller Anreize durch entsprechende Vergabebedingungen sowie bezüglich (Fort-)Bildungsmaßnahmen durch alle Geschlechter, Alters- und Bevölkerungsgruppen gleichermaßen erreichende Angebote sichergestellt werden.

Bezüglich der Stellungnahme zum grundsätzlich **positiv zu bewertenden** Vorschlag eines ***„Ökosystems für Vertrauen“*** orientieren sich die nachfolgenden Verbesserungsvorschläge grds. an der Gliederung des Weißbuchs selbst.

I. PROBLEMSTELLUNG

KOM WEISSBUCH: Unter ‚Problemstellung‘ stellt die KOM der nachfolgenden Konzeption eines Regulierungskonzepts die Erörterung von Risiken und Gefahren bei der Anwendung von KI vorweg (S. 12 ff.). Die KOM hebt die Wahrung der Grundrechte hervor, insbesondere des Schutzes der personenbezogenen Daten, Privatsphäre und Nicht-Diskriminierung, sowie das Recht auf freie Meinungsäußerung, die Versammlungsfreiheit, die Achtung der Menschenwürde, das Recht auf einen wirksamen gerichtlichen Rechtsbehelf und ein faires Verfahren sowie den Verbraucherschutz. Damit orientiert sich die KOM an der Evaluation einer im Auftrag des Europarates erstellten Studie[6] über die Implikationen algorithmischer Entscheidungssysteme für die Menschenrechte.

Besondere Merkmale vieler (auf maschinellem Lernen basierenden) KI-Systeme wie Opazität, Komplexität, Unvorhersehbarkeit und teilautonomes Verhalten (S. 14) forderten die Wirksamkeit bestehender EU-Rechtsvorschriften heraus. Die KOM fürchtet diesbezüglich Risiken für die Betroffenen und potenziell marktschädliche Rechtsunsicherheiten für Unternehmen.

Position D64: Wir **begrüßen** ausdrücklich, dass die KOM den künftigen Rechtsrahmen auf den Schutz der Grundrechte ausrichten will. So sieht auch D64 grundsätzlich mögliche Risiken (siehe Box unten) für den **Nicht-Diskriminierungs-Grundsatz** (z.B. Job-Bewerbungen, Art. 3 GG), die **persönlichen Entfaltungsmöglichkeiten** (z.B. Kreditanträge, Art. 2 I GG), die **persönliche** (z.B. Gesichts- und Gangerkennung, Art. 2 I i.V.m. Art. 1 I GG) sowie **räumliche** (z.B. Sprachassistenten, Art. 13 GG) **Privatsphäre** oder die **Meinungs- und Versammlungsfreiheit** (z.B. Newsfeed-Sortierung, Art. 5 und 8 GG).

---

[6] Europarat, Algorithms and Human Rights - Study on the human rights dimensions of automated data processing techniques and possible regulator implications, Study DGI(2017)12, März 2018, online: https://rm.coe.int/algorithms-and-human-rights-en-rev/16807956b5.

Wir plädieren dafür, die Auflistung der Meinungsfreiheit (S.12) entsprechend der Formulierung in der Europäischen Charta der Grundrechte ausdrücklich um die Dimension der bisher nicht erwähnten **Informationsfreiheit** zu erweitern. So wohnt etwa algorithmenbasierten „*Gatekeepern*" im Rahmen der Meinungsbildung eine fundamentale Bedeutung und Herausforderung für die Demokratie inne. Die KOM sollte den Schutz der pluralistischen **Demokratie** daher ebenfalls als Dimension in der Problemstellung ausdrücklich einschließen. Dies entspräche auch der Leitidee des Weißbuchs, das Fundament europäischer Werte zu schützen.

RISIKO

D64 versteht unter „Risiko" die Kombination aus der **Eintrittswahrscheinlichkeit** eines schädigenden Ereignisses und der **Schwere** des möglichen Schadens (vgl. auch etwa die ähnliche Legaldefinition in § 2 Nr. 23 ProdSG).

Die **Eintrittswahrscheinlichkeit** hängt aus Sicht von D64 insbesondere ab von:

- **Skalierung**
  Algorithmische Systeme können, ohne dass sie physisch nachproduziert werden müssen, eine große Anzahl von Anwenderinnen und Anwendern und somit auch Betroffenen finden (sog. Skalierbarkeit). Sind mehr Personen einem System ausgesetzt, steigt auch die statistische Wahrscheinlichkeit des Eintritts eines Schadensfalles.
- **Ausweichmöglichkeit**
  Haben Betroffene eine echte Wahlmöglichkeit bei der Auswahl der Systeme, die Entscheidungen über sie treffen, können sie sich für jene mit dem geringsten Risiko entscheiden. Eine informierte Entscheidung können Betroffene aber nur treffen, wenn die Auswirkungen der Systeme für sie transparent sind. Bei privaten Monopolstellungen oder staatlichen Anwendenden ist die Ausweichmöglichkeit besonders gering.

Die **Schwere des möglichen Schadens** hängt aus Sicht von D64 insbesondere ab von:

- **Abstrakter Rang des geschützten Gutes**
  In der Grundrechtsdogmatik sind verfassungsrechtlich oder im Rahmen der Rechtsprechung entwickelte Hierarchien unterschiedlicher Grundrechtspositionen anerkannt (z.B. Unantastbarkeit der Menschenwürde; besonderes Gewicht der informationellen Selbstbestimmung aufgrund ihrer Nähe zur und normativen Anknüpfung an die Menschenwürde; besondere Bedeutung der Meinungsfreiheit für die demokratische Grundordnung etc.). Zudem gilt es stets auch die Folgewirkungen und Einschüchterungseffekte eines (drohenden) Schadens (sog. *chilling effects*) zu betrachten, die sich auf das geschützte Rechtsgut oder aber auf andere Güter ergeben können.
- **Konkrete Dauer und Umfang / Intensität der Anwendung**
  Nicht jede Beeinträchtigung eines geschützten Rechtsguts wiegt gleich schwer. Maßgeblich ist vielmehr, wie intensiv, wie lange andauernd / häufig und wie umfangreich die konkrete Beeinträchtigung ist.

D64 stimmt mit der KOM darin überein, dass spezifische Merkmale von KI den bestehenden Rechtsrahmen herausfordern. Elemente wie die hohe **Skalierbarkeit**, **Entwicklungsgeschwindigkeit und Opazität** stellen dabei jedoch keine ausschließlichen Charakteristika von KI-Anwendungen dar.

Algorithmische Systeme verarbeiten typischerweise die Daten von einer Vielzahl an Betroffenen und weisen bereits dadurch regelmäßig ein hohes Risiko für die Grundrechte aller Betroffenen auf. Diese Auswirkungen auf einen großen Anwenderkreis können sie schon kurz nach Markteintritt haben. In Bezug auf die Entwicklungsgeschwindigkeit liegen zwischen technischer Innovation und marktreifen Produkten häufig lediglich wenige Monate. Damit verdichtet sich der Zeitrahmen, in dem die Gesellschaft Debatten über die Fortentwicklung solcher Systeme führen und der Gesetzgeber den Rechtsrahmen anpassen kann. Im Fall von KI ist die Skalierbarkeit teilweise besonders kritisch, da das konkrete Verhalten von KI-Systemen in vielen Fällen nicht sicher vorhergesagt werden kann. Ohne die notwendigen Korrekturen kann dies zur Fortschreibung bestehender Diskriminierungen führen. Als Problem sehen wir es ebenfalls an, dass es für Betroffene in der Regel überaus schwierig ist, die Funktionsweise von Algorithmen nachzuvollziehen (sog. Opazität) und so z.B. Diskriminierungen bei algorithmengestützten Entscheidungen zu erkennen und geltend zu machen. Laien haben es ohne Erklärung gleichermaßen schwer, komplexe klassische Algorithmen oder KI-Anwendungen nachzuvollziehen.[7]

Wir raten davon ab, den antizipierten Regulierungsrahmen explizit auf KI zu limitieren, da auch **Technologien ohne KI-Komponente** mit **vergleichbaren Risiken** für die Grundrechte der Betroffenen verbunden sein können (siehe hierzu ausführlich unten *B.III.1.a.i*).

Noch weiterer Debatten bedarf aus Sicht von D64 die Frage, ob und inwiefern dieselben Regeln für den **staatlichen** und **privatwirtschaftlichen Einsatz** algorithmischer Entscheidungssysteme gelten sollen. Für eine Differenzierung sprechen aus unserer Sicht insbesondere drei Gesichtspunkte:

- Von staatlichen Stellen geht typischerweise ein erhöhtes Schadensrisiko aus. Sie haben umfangreiche exekutive Eingriffsbefugnisse und stellen öffentliche Güter und Dienstleistungen für eine Vielzahl an Personen bereit. Dabei haben sie regelmäßig eine Monopolstellung inne. Staatliche Stellen müssen daher auch bei der Automatisierung ihrer Entscheidungen besonders hohen Anforderungen (siehe unten *B.III.2.b*) unterliegen.
- Staatliche Stellen sind im Unterschied zu Privaten unmittelbar an die Grundrechte gebunden. Sie müssen daher Anforderungen wie Nicht-Diskriminierung jederzeit und uneingeschränkt erfüllen.[8]
- Staatliche Stellen sind keine Grundrechtsträger; sie können sich nicht auf den Schutz etwa von Berufs- und Geschäftsgeheimnissen berufen. Sie sind somit in besonderem Maße zur Transparenz ihrer Entscheidungen aufgerufen.

[7] Siehe z.B. das Beispiel des klassischen Algorithmus zur Vergabe von Studienplätzen in Frankreich, der ohne jegliche Erklärung veröffentlicht wurde und daher erst mithilfe der Zusammenarbeit mehrerer Freiwilliger auf GitHub aufgearbeitet werden konnte, https://www.bertelsmann-stiftung.de/fileadmin/files/BSt/Publikationen/GrauePublikationen/ADM_Fallstudien.pdf, S. 25.

[8] Für Private gilt diese Verpflichtung nur in den Ausnahmekonstellationen der mittelbaren Grundrechtsbindung oder wenn der Gesetzgeber ein Diskriminierungsverbot einfachgesetzlichen normiert hat (wie insb. durch das AGG).

II. BESTEHENDER RECHTSRAHMEN

KOM WEISSBUCH: Die KOM kommt 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“ (S. 18 f.).

Position D64: Auch wir sind der Auffassung, dass das bestehende Datenschutzrecht sowie das bestehende Produktsicherheitsrecht die Risiken, die durch die Entwicklung und den Einsatz algorithmischer Systeme theoretisch entstehen können, nicht adäquat abdecken. Sie sind auch nicht der richtige Ort zur Normierung risikominimierender Maßnahmen. Wir unterstützen daher die Überlegung, einen separaten Rechtsrahmen zu schaffen.

1. Produktsicherheitsrecht

Die primäre Ausrichtung des Produktsicherheitsrechts auf physische Produkte, sowie der darin primär bezweckte Schutz der Gesundheit - und nicht auch anderer Rechtsgüter - führt zu Schutzlücken.

a. Primäre Ausrichtung auf physische Produkte

Aufgrund der potenziell schädlichen Auswirkungen körperlicher technischer Produkte auf Sicherheit und Gesundheit bestehen bereits seit Jahrzehnten Produktsicherheitsvorschriften. Das CE-Kennzeichen, das Herstellende sich in der Regel selbst vergeben und mit dem sie die Einhaltung gesetzlicher Vorgaben zum Ausdruck bringen, sorgt für sichere Produkte wie etwa elektrische Niederspannungsgeräte, Arbeitsmittel oder Maschinen. Mit Ausnahme der Medizinprodukterichtlinie (bzw. künftig -verordnung) gelten diese Vorschriften jedoch typischerweise nur für in physische Produkte eingebettete Software (sog. *embedded software*). Hingegen finden sie keine Anwendung auf Software, die auf keinem dem jeweiligen Regelungsbereich unterfallenden Gerät, wie z.B. einem PC oder einem Handy, ausgeführt wird (sog. *stand-alone software*).

Die Feststellungen im „Bericht über die Auswirkungen von Künstlicher Intelligenz, des Internets der Dinge und der Robotik auf Sicherheits- und Haftungsfragen“, wonach die bestehenden Vorschriften diesbezüglich angepasst und präzisiert werden sollten (s. Zusammenfassung des Berichts im Weißbuch, S. 18), unterstützen wir. Die körperlichen Auswirkungen von KI auf Gesundheit und Sicherheit lassen sich hierdurch abdecken.

b. Kein adäquater Schutz anderer Rechtsgüter

Das Produktsicherheitsrecht anzupassen reicht jedoch nicht aus, um sämtliche Risiken, die von algorithmischen Systemen ausgehen, adäquat abzudecken. Denn sie bezwecken lediglich den Schutz der Gesundheit und nicht den anderer Rechtsgüter. Jedoch sind die von Algorithmen ausgehenden nicht-körperlichen Auswirkungen auf unsere Privatsphäre[9] und spätestens seit der Lehman Brothers-Pleite und der Finanzkrise ab 2008 auf unser Wirtschaftssystem[10] als hinreichende Gründe für eine risikominimierende Regulierung anerkannt.

---

[9] Siehe die DSGVO für die Verarbeitung personenbezogener Daten.

[10] Siehe z.B. die Capital Requirements Regulation i.V.m. zahlreichen Guidelines für sog. Risikomodelle für Kundenkredite oder die MiFIR und MiFID II für den Hochfrequenzhandel.

Darüber hinaus haben Algorithmen neben quantifizier- bzw. bezifferbaren Auswirkungen - z.B. auf die körperliche Unversehrtheit und auf unser Wirtschaftssystem - jedoch auch (potenzielle) Auswirkungen auf zahlreiche weitere grundrechtlich geschützte Güter (siehe oben *B.I.*). Diese werden weder durch die Produktsicherheitsvorschriften abgedeckt, noch ist das mit ihnen verbundene Modell der Co-Regulierung aus unserer Sicht das richtige Regulierungsmodell (siehe hierzu ausführlich unten, *B.III.2.d*), um diese Auswirkungen abzudecken.

2. Datenschutzrecht

Das Datenschutzrecht kennt mit Art. 22 (i.V.m. Art. 13-15) DSGVO, der Transparenz und menschliche Letztentscheidung anordnet, bereits eine dem Anliegen der KOM sowie dem von D64 nahekommende Vorschrift. Diese ist in ihrem Anwendungsbereich jedoch auf vollautomatisierte Entscheidungen mit rechtlicher Wirkung oder einer anderweitigen erheblichen Beeinträchtigung der Person beschränkt. Art. 22 DSGVO schützt daher nicht vor dem in der Praxis überwiegend vorkommenden Einsatz von Algorithmen zur Entscheidungsvorbereitung. Zudem erfasst Art. 22 nur Entscheidungen auf Grund der Verarbeitung personenbezogener und nicht etwa anonymisierter Daten.

Bereits wegen des begrenzten Anwendungsbereiches der DSGVO wird ihre Anpassung nicht genügen, um Gefahren für die Rechte und Freiheiten natürlicher Personen entgegenzutreten. In jedem Fall wäre die DSGVO gemessen an ihrer Schutzrichtung der falsche Ort zur Normierung von Qualitäts- und Nicht-Diskriminierungsanforderungen.

III. Tastender Regulierungsansatz

Um zu ermitteln, welche algorithmischen Entscheidungssysteme weiteren Regulierungsbedarf hervorrufen, sollte die KOM den Ansatz einer **„tastenden Regulierung“** wählen.

In einem **ersten Schritt** sollte sie Transparenz über den Einsatz solcher Systeme und die damit einhergehenden Risiken schaffen. Dies gelingt, wenn die Anwendenden algorithmischer Entscheidungssysteme, eine Risikofolgenabschätzung für solche Systeme vornehmen, die sie gegenüber einer Aufsichtsbehörde einreichen müssen.

Auf dieser fundierten, evidenzbasierten Grundlage sollte die KOM spezifische Regulierungsanforderungen für den zweiten und alle weiteren Schritte ableiten.

Die Erkenntnisse über den Einsatz solcher Systeme und ihre Regulierung korrelieren miteinander: Die KOM sollte die Anforderungen daher stets an Veränderungen anpassen, die mit der der technischen Fortentwicklung einhergehen.

1. Erster Schritt: Risikofolgenabschätzung für algorithmische Entscheidungssysteme

a. Anwendungsbereich: Algorithmische Entscheidungssysteme

KOM Weissbuch: Die KOM geht davon aus, dass der zu entwickelnde Rechtsrahmen „für Produkte und Dienstleistungen gelten soll, bei denen **KI** zum Einsatz kommt“ (S. 19). KI müsse daher „für die Zwecke dieses Weißbuchs sowie für alle weiteren künftigen politischen Initiativen klar definiert werden“ (je S. 19). Die KOM greift dazu die Definition der Hochrangigen Expertengruppe auf.[11] Die KOM verengt den Anwendungsbereich weiter

[11] „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

grundsätzlich[12] auf solche KI-Anwendungen, die sowohl einem vorab abschließend aufgelisteten **Risiko-Sektor** (genannt werden Gesundheit, Verkehr, Energie sowie Teile des öffentlichen Sektors) zuzuordnen sind (S. 20) *und* zusätzlich im konkreten Anwendungsfall „so eingesetzt werden, dass mit **erheblichen Risiken** zu rechnen ist“ (S. 21).

Position D64: Wir halten es für zentral, **Überregulierung zu vermeiden**, den **Bürokratieaufwand so gering wie nur zwingend nötig** zu halten und so **die internationale Konkurrenzfähigkeit der europäischen Digitalwirtschaft** (insbesondere gegenüber den USA und China) aufrecht zu erhalten. Daher begrüßen wir den Ansatz, lediglich Systeme zu erfassen, die so eingesetzt werden, dass mit regulierungsbedürftigen Risiken zu rechnen ist (risikobasierter Ansatz; S. 21). Dies gewährleistet ein ausgewogenes Verhältnis zwischen dem potentiellen Risiko für die Grundrechte der Betroffenen und den Eingriffen in die Grundrechte der Herstellenden, Anwendenden und anderen Akteuren im Ökosystem „algorithmischer Entscheidungssysteme“. Der risikobasierte Ansatz ist bereits durch das Gebot der Rechtsstaatlichkeit (Verhältnismäßigkeitsgrundsatz) verfassungsrechtlich vorgezeichnet.

Die zentrale Frage ist jedoch, wie die Bestimmung dieses Risikos vonstattengehen soll. Die von der KOM vorgenommenen Eingrenzungen des Anwendungsbereichs halten wir aus einer Reihe von Gründen für **ungeeignet**.

i. Keine Begrenzung auf KI

Der Ansatz der KOM, den Anwendungsbereich auf KI zu begrenzen, ist aus unserer Sicht ungeeignet:

- Zunächst **mangelt** es an einer konsensfähigen, **einheitlichen Definition** von „KI“. Der Begriff ist zu allgemein, als dass er eine sinnvolle Abgrenzung schaffen kann. Einerseits fehlt es an einer Definition des Begriffs der „Intelligenz“ bzw. einer Antwort auf die Frage, ab wann sich ein System intelligent verhält. Geht es darum, ob ein System menschliches Verhalten imitiert, kämen wir schnell zu dem Ergebnis, dass jedes Softwaresystem menschliches Verhalten imitiert, indem es Fragen beantwortet, die alternativ ein Mensch beantwortet hätte. Andere Ansätze unterscheiden hingegen zwischen regelbasierten Systemen und solchen, die lernfähig sind (Maschinelles Lernen), und grenzen teilweise noch weiter auf die Untergruppe derjenigen lernfähigen Systeme ein, die die Lernweise des menschlichen Gehirns imitieren (Neuronale Netze/*Deep Learning*). Doch auch bei einer Begrenzung auf das Element des „maschinellen Lernens“ stellen sich zahlreiche bis dato unbeantwortete Folgefragen: Reicht es bereits aus, wenn eine Teilkomponente Elemente des maschinellen Lernens nutzt? Muss das System im Einsatz weiter lernen oder sind auch austrainierte Systeme erfasst?
- Ferner existieren eine Vielzahl alltäglicher **KI-Anwendungen**, die aus Sicht von D64 (und in diesem Falle auch der KOM) **keinerlei spezifisches Regulierungsbedürfnis** auslösen (z.B. Foto-

---

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.", *High-Level Expert Group on Artificial Intelligence*, A Definition of AI: Main Capabilities and Disciplines, 08.04.2019, S. 8, online: https://ec.europa.eu/digital-single-market/en/news/definition-artificial-intelligence-main-capabilities-and-scientific-disciplines. Die deutsche Übersetzung ist dem Weißbuch, Fn. 47 auf S. 19 entnommen.

[12] Auf S. 22 wird dieser Grundsatz dann wiederum durchbrochen durch „Ausnahmefälle […], 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“.

Filter, Musik- und Produktvorschläge, Übersetzungsdienste, intelligente Warenflusssysteme u.v.m.). Umgekehrt können jedoch aus Sicht von D64 von algorithmischen Systemen, die **keine KI-Komponente** enthalten, ähnlich **hohe Risiken** ausgehen, die einen Regulierungsbedarf auslösen. Lediglich KI in den Anwendungsbereich aufzunehmen wäre daher nicht Ausfluss eines von der KOM grundsätzlich befürworteten (S. 20) verhältnismäßigen, risikobasierten (d.h. bereits definitorisch am Risiko einer jeweiligen Anwendung und nicht an ihrer technischen Konzeption orientierten) Regulierungsansatzes. Zudem würde eine solche technikbasierte Abgrenzung eine ungerechtfertigte Ungleichbehandlung unterschiedlicher Technologien zur Folge haben.

- Letztlich würde eine Beschränkung regulatorischer Anforderungen auf KI entgegen des eigentlichen Anliegens der KOM ungewollt **Anreize** schaffen, **Systeme ohne KI-Komponente zu entwickeln bzw. einzusetzen**.

D64 hält eine Begrenzung des Anwendungsbereichs auf KI daher nicht für adäquat.

ii. Keine Begrenzung auf einzelne Sektoren

Wir halten eine sektorale Verengung des Anwendungsbereichs nicht für zielführend:

- Es ist das erklärte Ziel der KOM, den Schutz der Grundrechte zu wahren. Vor diesem Hintergrund wäre es zunächst mit einem verhältnismäßigen, risikoadäquaten Ansatz nicht zu vereinbaren, lediglich hoch riskante Anwendungen bestimmter Sektoren zu regulieren, diejenigen in nicht erfassten Sektoren jedoch unberücksichtigt zu lassen.
- Zudem würde eine sektorenspezifische Regulierung ohnehin nicht davon entbinden, das jeweilige Risiko von Anwendungen innerhalb des regulierten Sektors zu bestimmen, da es anderenfalls innerhalb der regulierten Sektoren zu einer Überregulierung von nicht risikogeneigten Anwendungen käme. Dies lässt sich am Beispiel des Verkehrssektors illustrieren: Während eine KI, die ein Auto steuern soll, wegen der Unfallgefahr ein hohes Risiko darstellt, erscheint das Risiko eines KI-basierten intelligenten Verkehrsstromverteilers (der Verkehrsflüsse so regelt, dass die Straßen möglichst gleichmäßig ausgelastet sind und der Verkehr möglichst im Fluss bleibt) deutlich geringer, auch wenn beide Systeme demselben Sektor zuzuordnen sind. Wenn eine Risikoklassifizierung jedoch ohnehin erforderlich ist, spricht vieles dafür, von Anfang an regulatorische Anforderungen allein an das jeweilige Risiko zu knüpfen.
- Ein Vorteil sektoraler Eingrenzung ist eine vermeintliche Erhöhung der **Rechtssicherheit** für nicht erfasste Sektoren. Dem ist jedoch entgegen zu halten, dass sich einzelne **Sektoren teilweise schwer definieren** lassen. Mit einem sektorenspezifischen Regulierungsansatz gehen also Abgrenzungsschwierigkeiten einher. Die von der KOM angeführten Sektoren orientieren sich teilweise
  - am Einsatzgebiet („Gesundheit, Verkehr, Energie“, S. 20) und teilweise
  - am Einsetzenden selbst („Teile des öffentlichen Sektors“, S. 20).

  Zudem erkennt die KOM selbst an, dass sich **einzelne Anwendungen zwar keinem der in den Blick gefassten Sektor zuordnen** lassen, aber dennoch hohe Risiken mit sich bringen. Als zweite Kategorie erkennt sie daher **Ausnahmefälle** für bestimmte Einsatzzwecke bzw. Technologien an, für die „aufgrund der immanenten Risiken [...] unabhängig vom betreffenden Sektor [...] die nachstehenden Anforderungen dennoch gelten würden“ (S. 21). Wir erachten die erwähnten, potentiell regulierungsbedürftigen Beispiele der KI-Anwendungen i.R.d. Einstellungsverfahrens, sowie der biometrischen Fernidentifikation (insbesondere Gesichtserkennung) grundsätzlich als hoch riskant. Gleiches gilt für bestimmte Verfahren der personalisierten Risikoklassifizierung (z.B. *credit scoring*, personalisierte

Preissetzung etc.). Das Erfordernis, Ausnahmefälle für solche Beispiele zu schaffen, spricht jedoch von Grund auf gegen eine sektorale Verengung des Anwendungsbereichs aus Gründen der sodann nur vermeintlichen Rechtssicherheit.

- Des Weiteren sind auch die im Softwarebereich **kurzen Innovationszyklen** zu beachten, da zahlreiche Innovationen im Bereich automatisierter Entscheidungssystem bald auch in Sektoren zum Einsatz kommen könnten, die zum jetzigen Zeitpunkt noch nicht in den Blick genommen werden.
- Ein und dieselbe digitale Technologie kann auf verschiedenste Art und Weise mit jeweils stark divergierenden Risiken eingesetzt werden. Ein System der Gesichtserkennung zur Entsperrung des Handys ist beispielsweise deutlich weniger regulierungsbedürftig als ein System der Gesichtserkennung zum Zwecke des automatischen Vollzugs von Rechtsverstößen wie das Überqueren einer roten Fußgängerampel. Allerdings entscheiden zumeist nicht **die Entwickelnden bzw. die Herstellenden** als potentiell Verantwortliche/r (ausführlich hierzu unten, *B.III.2.c*) selbst, sondern vielmehr die Anwenderinnen und Anwender **über den Sektor,** indem das **algorithmische System zum Einsatz kommt**. Wir plädieren dahingehend dafür, jedenfalls Herstellerpflichten sektorunabhängig zu regulieren. Nur dies kann ausschließen, dass einerseits die Bestimmung (durch Wahl des Einsatz-Sektors) und andererseits die Einhaltung des Pflichtenkataloges (bei der Herstellung), auf unterschiedliche private Akteure verteilt werden. Die Alternative, alleine die Anwendenden in die Pflicht zu nehmen, wäre nicht mit dem sonst zu begrüßenden Ansatz der KOM vereinbar, den Akteur in die Pflicht zu nehmen, der am besten in der Lage ist, potenzielle Risiken zu bewältigen (S. 27).
- Letztlich lassen im Rahmen des europäischen Gesetzgebungsprozesses **nationale Interessen am Schutz eigener wirtschaftsstarker Sektoren** eine inadäquate Sektorenauswahl erwarten.

Insgesamt ist eine sektorale Verengung des Anwendungsbereichs nach Ansicht von D64 daher abzulehnen.

iii. Begrenzung auf staatliche oder geschäftsmäßig genutzte algorithmische Entscheidungssysteme

Im ersten Schritt der tastenden Regulierung sollte der Anwendungsbereich nicht auf den Einsatz von KI in ausgewählten Sektoren begrenzt werden. Allerdings ist es auch nicht angezeigt, für die Entwicklung bzw. den Einsatz eines jeglichen algorithmischen Systems eine Risikofolgenabschätzung zu verlangen.

Vielmehr gehen die geschilderten Risiken (siehe oben *B.1. Problemstellung*) nach Auffassung von D64 nahezu ausschließlich von **algorithmischen Entscheidungssystemen** aus:

> **ALGORITHMISCHE ENTSCHEIDUNGSSYSTEME**
>
> Im Sinne dieser Stellungnahme sind Algorithmische Entscheidungssysteme algorithmische Systeme, die anhand Daten Entscheidungen über Menschen mit potentiellen Auswirkungen auf grundrechtlich geschützte Güter treffen oder solche vorbereiten.

Um darüber hinaus nicht bereits private, hobbymäßige oder ausbildungs- bzw. studienbedingte Tätigkeiten zu erfassen, erscheint es angemessen, den Anwendungsbereich auf die **geschäftsmäßige**[13] Entwicklung oder Anwendung von algorithmischen Entscheidungssystemen zu

[13] Für eine solche Verengung des Anwendungsbereichs s. etwa § 5 TMG.

verengen. Erst hier kann berechtigterweise eine risikominimierende Entwicklung verlangt werden. Selbiges gilt für den Einsatz seitens **staatlicher** Stellen.

b. Anforderung: Risikofolgenabschätzung

Herzstück der tastenden Regulierung ist eine **Risikofolgenabschätzung** aktuell und zukünftig genutzter algorithmischer Entscheidungssysteme. Nach Ansicht von D64 sollten Anwendende das Risiko durch eine interne Risikofolgenabschätzung (sog. *algorithmic impact assessment*) bestimmen müssen. Im Interesse der Rechtssicherheit sollte der Gesetzgeber hierfür **exakte Kriterien** oder gar ein konkretes, **online zur Verfügung stehendes Prüfschema** vorgeben, in dem auch bereits Risikominimierungsmaßnahmen (z.B. die Gewährleistung menschlicher Aufsicht oder Anwendung bestimmter Fairnessmaße etc.) berücksichtigt werden können.[14] Bei der Zusammenstellung der einzuschätzenden potenziellen Auswirkungen ist eine Orientierung an den unter „Problemstellung“ diskutierten Effekten von KI denkbar.

Diese Einschätzungen dienen der Aufsichtsbehörde mittelfristig um Klarheit über tatsächlich bestehende Risiken zu erlangen. Um das so erlangte **Wissen zu sammeln und in die Gesellschaft zu tragen**, sollten die Behörden Jahresberichte sowie die gesammelten statistischen Daten zur Verwendung von algorithmischen Entscheidungssystemen und den damit verbundenen Risiken veröffentlichen. Dies würde den gesellschaftlichen Diskurs fördern und eine fundierte, evidenzbasierte Grundlage für die Ausgestaltung weitergehender regulatorischer Anforderungen wie z.B. im Hinblick auf Nicht-Diskriminierung, Genauigkeit und Robustheit etc. bieten.

Nach einer **Laufzeit von einem Jahr** sollte die KOM anhand der vorgenommenen Risikofolgenabschätzungen (z.B. mittels delegierter Rechtsakte) definieren, welche weitergehenden Anforderungen (siehe hierzu ausführlich unten, *B.III.2.b* Arten von Anforderungen) für welche – anhand ihres konkreten Risikos ausgewählten – algorithmischen Entscheidungssysteme gelten sollen (‚gestufte‘, ‚tastende‘ Regulierung).

> **WECHSELWIRKUNG ZW. WEITEM ANWENDUNGSBEREICH UND ENGEM PFLICHTENKREIS**
>
> Es besteht eine starke Wechselwirkung zwischen dem Anwendungsbereich und dem Katalog an Anforderungen an algorithmische Systeme.
>
> Die KOM schlägt vor, den **Anwendungsbereich von Anfang an eng** zu fassen und auf den sektoralen Einsatz von KI zu begrenzen und bringt einen **weitreichenden Pflichtenkatalog** (S. 22 ff.) ins Spiel.
>
> Wir sprechen uns im Gegensatz dazu dafür aus, in einem ersten Schritt mit einem **weiten Anwendungsbereich** umfassendes Wissen über die tatsächlichen von algorithmischen Entscheidungssystemen ausgehenden Risiken zu sammeln. Dieser sollte jedoch zunächst lediglich mit der **geringsten Verpflichtung** – der Vornahme einer Risikofolgenabschätzung gegenüber einer Aufsichtsbehörde – einher gehen. Erst in einem zweiten Schritt soll die KOM dann risikoadäquat weitergehende Anforderungen festlegen.

[14] Als Vorbild könnten das „Worksheet to Assess Algorithm Risk“ des Ethics and Algorithms Toolkit (Beta), online verfügbar unter: https://ethicstoolkit.ai/assets/part_1_worksheet.pdf sowie die Beta-Version (v0.8, Stand: 30.05.2020) des online ausfüllbaren „Algorithmic Impact Assessment“ der Kanadischen Regierung, online verfügbar unter: https://open.canada.ca/aia-eia-js/ dienen.

2. Weitere Schritte: Gestufte Anforderungen, je nach im ersten Schritt ermitteltem Risiko

a. Anwendungsbereich

Aus Sicht von D64 sollten die regulatorischen Anforderungen für algorithmische Entscheidungssysteme gelten, die zu hohen Risiken für grundrechtlich geschützte Güter führen. Welche Anwendungen besonders risikobehaftet sind, gilt es im ersten Schritt des tastenden Ansatzes zu ermitteln (siehe oben *B.III.1*).

D64 lehnt eine sektorale Verengung des Anwendungsbereichs der ersten Stufe ab (siehe oben *B.III.1.a*) Was allenfalls denkbar erscheint, ist eine sektorale Differenzierung der jeweiligen Anforderungen (sektorspezifische Risikoklassifizierungsregeln), sobald der horizontale Anwendungsbereich eröffnet ist.

b. Arten von Anforderungen

KOM WEISSBUCH: Die KOM sieht vor, für KI-Anwendungen mit hohem Risiko gewisse verbindliche rechtliche Anforderungen festzuschreiben. Für Anwendungen und Sektoren ohne hohes Risiko sollen diese hingegen nicht gelten.

Position D64: Wir begrüßen die Bestrebungen der KOM, mittels Anforderungen an die Systemgestaltung zu einer gemeinwohlorientierten Technologieentwicklung beizutragen. Dabei sehen wir die genannten Anforderungen auch grundsätzlich als geeignet an, die bestehenden Probleme zu adressieren. D64 begrüßt es dabei, dass die KOM einen risikobasierten Ansatz wählt. Dieser fußt letztlich in dem verfassungsrechtlich vorgegebenen Gebot der Verhältnismäßigkeit, wonach staatliche Eingriffe etwa in die Berufsfreiheit (durch Anforderungen an die Systemgestaltung) in einem angemessenen Verhältnis zu den potentiellen Bedrohungen für die geschützten Rechtsgüter stehen müssen. Nur so ist ein Mittelweg zwischen dem notwendigen Grundrechtsschutz und den Nachteilen einer unerwünschten Überregulierung möglich. Wir halten die vorgeschlagene **binäre Unterteilung**, gemäß welcher sämtliche Arten von Anforderungen an Künstliche Intelligenz stets für Anwendungen mit hohem Risiko und nie für Anwendungen darunter gelten sollen für **zu undifferenziert.** Wir plädieren vielmehr für eine **„gestufte Regulierung“**, die je nach konkretem Risiko **feingranulare Abstufungen** vorsieht (s. oben Abb. 1).

Bei dieser weiteren Ausgestaltung gilt es aus unserer Sicht insbesondere folgende Herausforderungen zu berücksichtigen:

i. Trainingsdaten

KOM WEISSBUCH: Die KOM fordert bezüglich der Daten, die als Trainingsdaten für KI-Systeme verwendet werden, Sicherheit und Robustheit[15], Nicht-Diskriminierung[16] und Privatheit[17] (S. 22 f.).

Position D64: Wir unterstützen diese Anforderungen angesichts der potentiellen Reproduktion und Fortschreibung bereits bestehender, menschlich verursachter Diskriminierungen beim Lernen aus statistischen Daten.

---

[15] Die KOM sieht diesbezüglich „Anforderungen die hinreichend gewährleisten, dass anschließende Nutzung der KI-gestützten Produkte oder Dienstleistungen sicher ist“ vor, S. 22.

[16] Nach dem Vorschlag der KOM hätten die Adressaten „angemessene Maßnahmen zu ergreifen, um sicherzustellen, dass eine solche spätere Nutzung von KI-Systemen nicht zu Ergebnissen führt, die eine verbotene Diskriminierung darstellen.“, S. 22.

[17] Die KOM fordert diesbezüglich „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“, S. 23.

REPRODUKTION VON DISKRIMINIERUNGEN BEIM LERNEN AUS DATEN

Ein algorithmisches Entscheidungssysteme kann nur Ausschnitte bestehender Strukturen abbilden. Wenn dort unerwünschte Muster - wie durch Menschen verursachte Diskriminierungen - existieren, sollte insb. eine KI so entwickelt werden, dass sie diese nicht fortschreibt.

So weisen z.B. bestimmte Bevölkerungsgruppen nach Straffälligkeit ein statistisch gesehen höheres Rückfallrisiko auf. Werden sie nun strengeren Bedingungen in der Resozialisierung unterworfen, schriebe das diese Tendenz u. U. fort. Dieses Beispiel zeigt jedoch zugleich, dass es eine komplexe politische Frage ist, welche Muster bei der Entscheidungsfindung herauszurechnen oder berechtigterweise zu berücksichtigen sind.

Es gilt jedoch zu berücksichtigen, dass

- die konkrete Ausgestaltung bzw. Operationalisierung der Nicht-Diskriminierungsanforderungen keine Frage des „Standes der Technik“ ist, sondern **politischer Wertentscheidungen** bedarf;
- für die Operationalisierung der Nicht-Diskriminierungsanforderungen zahlreiche sogenannte **Fairness-Maße** (wie etwa *individual* oder *group fairness*) entwickelt wurden, die sich jedoch teilweise gegenseitig ausschließen;[18]
- aufgrund des politischen Charakters der demokratisch legitimierte Gesetzgeber selbst und nicht Normungsgremien solche Wertentscheidungen treffen sollten (siehe hierzu ausführlich unten *B.III.2.d.* Governance);
- teilweise ein **Zielkonflikt** zwischen unterschiedlichen Anforderungen (wie Nicht-Diskriminierung und Genauigkeit[19] oder zwischen Nicht-Diskriminierung und Privatheit[20]) ausgemacht wird.

Die von D64 im Zuge der tastenden Regulierung geforderte Risikofolgenabschätzung sollte sich nicht nur darauf begrenzen, etwaige Risiken zu benennen und zu kategorisieren, sondern auch grundlegende Angaben der implementierten Maßnahmen zur Risikominimierung (wie z.B. der Anwendung von Fairnessmaßen bzgl. der Trainingsdaten) enthalten.

In Bezug auf algorithmische Entscheidungssysteme ohne KI-Komponente gilt, dass diskriminierende Muster nicht nur über Trainingsdaten, sondern auch über die Personen, die die Entscheidungsregeln des Systems festlegen, auf gleiche Weise diskriminierende Auswirkungen haben können[21], die es ebenfalls zu verhindern gilt.

---

[18] Binns, On the Apparent Conflict Between Individual and Group Fairness, arXiv:1912.06883, 14.12.2019, online: https://arxiv.org/abs/1912.06883v1. Für eine beispielhafte Auflistung von 19 unterschiedlichen Fairness-Maßen siehe: Barocas / Hardt / Narayana, Fairness in Machine Learning - Limitations and Opportunities, [incomplete working draft 21 Feb. 2020], S. 75 m.w.N., online: https://fairmlbook.org/pdf/fairmlbook.pdf.

[19] Zliobaite, On the relation between accuracy and fairness in binary classification, arXiv:1505.05723, 21.05.2015, online: https://arxiv.org/pdf/1505.05723.pdf; Friedler et al., A comparative study of fairness-enhancing interventions in machine learning, arXiv:1802.04422, 13.02.2018, online: https://arxiv.org/abs/1802.04422.

[20] Vale / Binns, Fairer machine learning in the realworld: Mitigating discrimination without collecting sensitive data, Big Data & Society, July–December 2017: 1–17, online: https://journals.sagepub.com/doi/pdf/10.1177/2053951717743530.

[21] So z.B. der Algorithmus zur Studienplatzvergabe in Frankreich, oben Fn. 9.

ii. Aufbewahrung von Daten und Aufzeichnungen

KOM WEISSBUCH: Die KOM fordert aufgrund der mit der Opazität mancher KI-Systeme einhergehenden „Schwierigkeiten, die Einhaltung der geltenden Vorschriften wirksam zu überprüfen und durchzusetzen“ spezifische Regelungen, 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 sollen (S. 23).

Position D64: Wir begrüßen diese Anforderungen grundsätzlich. Schwierigkeiten bezüglich der Überprüfung der Einhaltung der geltenden Vorschriften beschränken sich jedoch nicht auf KI-Systeme, sondern betreffen nahezu jegliche algorithmischen Entscheidungssysteme gleichermaßen (siehe oben *B.1. Problemstellung*).

D64 weist kritisch darauf hin, dass mit dieser Anforderung jedoch - je nach Ausgestaltung - ein erheblicher **bürokratischer Mehraufwand** einhergehen kann (wenn z.B. jedweder Zugriff und jede noch so kleine Veränderung der Trainingsdaten dokumentiert werden muss), der **so weit wie möglich vermieden** werden sollte. Die für manche Tätigkeiten sehr umfassenden und zeitaufwändigen fortlaufenden Dokumentationspflichten der DSGVO sollten hier nicht zum Vorbild genommen werden. Eine Aufzeichnung über die Programmierung des Algorithmus (z.B. durch Modelle, Kommentierungen im Code, Versionsverwaltung, Anforderungs- oder Workflowmanagement) gehört jedoch ohnehin zum guten Stil einer jeden Programmiertätigkeit.

iii. Bereitstellung von Informationen

KOM WEISSBUCH: Nach Ansicht der KOM sollten „proaktiv angemessene Informationen über den Einsatz von KI-Systemen mit hohem Risiko bereitgestellt werden“ (S. 23 f.).

Position D64: Wir unterstützen diese Anforderung nachdrücklich.

- **Transparenz gegenüber Behörden**
  Wir plädieren zuvorderst für Transparenzpflichten gegenüber staatlichen Aufsichtsbehörden. So können Eingriffe in die Geschäfts- und Betriebsgeheimnisse von Software-Herstellenden möglichst gering gehalten werden (Amtsgeheimnis). Der Ansatz erlaubt dadurch gleichzeitig detailliertere Einsichtsbefugnisse als diese zugunsten der allgemeinen Öffentlichkeit möglich wären. Neben dem **„Ob“** des Einsatzes („Kennzeichnungspflicht“) kommen daher auch Informationen über das **„Wie“** (weitergehende „Informationspflichten“) des Einsatzes in Betracht.
  Im Zentrum unserer Forderung stehen daher gegenüber Behörden einzureichende und von dieser - zum Zwecke der gesamtgesellschaftlichen Transparenz - zu einem Jahresbericht zusammenzufassende Risikofolgenabschätzungen (siehe oben *B.III.1.b*).

- Transparenz gegenüber der Öffentlichkeit
  D64 hält Transparenzgebote gegenüber der breiten Öffentlichkeit grds. für wichtig, um Aufmerksamkeit für und Wissen über die Implikationen des Einsatzes von algorithmischen Systemen zu schaffen. Allerdings nehmen einzelne Privatpersonen wegen des schon bestehenden *information overloads* von allgemein gefassten Informationen regelmäßig maximal oberflächlich Kenntnis. Entscheidend ist jedoch nicht, dass jeder die Informationen tatsächlich wahrnimmt, sondern dass diejenigen die dies wollen es auch können. Gerade zivilgesellschaftliche Vereinigungen können das so erhaltene Wissen analysieren und für eine breite Öffentlichkeit einfach verständlich aufarbeiten.
  Allerdings kommen Transparenzgebote nach unserer Auffassung aufgrund der damit verbundenen tiefgreifenden Eingriffe in die Geschäfts- und Betriebsgeheimnisse von Software-Herstellenden vornehmlich in Form von Hinweisen bezüglich des „Ob“ der

Verwendung algorithmischer Entscheidungssysteme („Kennzeichnungspflichten“) und nur in begründeten Ausnahmefällen bezüglich weitergehender Informationen zum „Wie“ des Einsatzes infrage.

- Transparenz gegenüber den Betroffenen einzelner Entscheidungen
  Sofern Einzelne von automatisierten Entscheidungen betroffen sind, kann es zur Wahrung bestehender Rechte (z.B. der Nichtdiskriminierung von Beschäftigten) aus unserer Sicht notwendig sein, diese mit zusätzlichen Rechten bezüglich des „Wie“ einer Entscheidungsfindung auszustatten. Die betrifft vor allem Informations- sowie Begründungspflichten. In Frage kommen insbesondere allgemeine Angaben bezüglich der für die Entscheidungsfindung maßgeblichen Kriterien (*Right to Explanation*).
- Besondere Transparenzverpflichtung staatlicher Stellen
  Aufgrund der dargestellten Unterschiede zwischen dem Einsatz algorithmischer Entscheidungssysteme durch private und **staatliche Stellen** (siehe oben *B.1. Problemstellung*) fordert D64 für letztere zusätzlich:
  - Ein **öffentliches Register** staatlicher algorithmischer Entscheidungssysteme, in dem zumindest das „Ob“ des jeweiligen Einsatzes einsehbar ist.
  - Die verstärkte Entwicklung, Anschaffung und Verwendung **nicht-proprietärer open-source Software**, um diese einerseits selbst anpassen und andererseits gegebenenfalls veröffentlichen zu können („public money, public code“).
  - In besonders kritischen Bereichen, wie z.B. dem Sicherheitsbereich, die parallele Entwicklung klassischer und intelligenter Systeme, und bei wesentlich gleicher Eignung beider Systeme die **Verwendung des transparenteren / erklärbareren Systems**.[22]

iv. Robustheit und Genauigkeit

KOM WEISSBUCH: Die KOM fordert, dass KI-Anwendungen technisch solide (Robustheit) und präzise (Genauigkeit) sein sollten (S. 24).

Position D64: Wir begrüßen dies grundsätzlich. Die angedachten Anforderungen sind jedoch noch unterspezifiziert. Eine konstruktive Debatte zu diesem Thema bedarf konkreterer Vorschläge. Dabei sollte auch berücksichtigt werden, dass die Genauigkeit eines (KI-basierten) Vorhersagesystems *ex ante* zwar provisorisch mithilfe von Testdatensätzen evaluiert werden kann, in der Anwendungspraxis jedoch nur *ex post* erfolgen kann. Überdies gilt, dass solche Systeme auch Realitäten schaffen können, das heißt dass sie - gleichsam einer sich selbst erfüllenden Prophezeiung - mit ihrer Entscheidung zum Eintreten des vorhergesagten Ereignisses/Zustandes selbst beitragen.

Es ist ferner erneut nicht ersichtlich, weshalb sich die Forderung, dass sich Systeme zuverlässig gemäß ihrem beabsichtigten Verwendungszweck verhalten, auf KI-Systeme beschränken sollte.

---

[22] Als durchaus positives Beispiel kann diesbezüglich die parallele Testung und der Vergleich unterschiedlicher Prognosemodelle i.R.d. des *predictive policing* Projekts des LKA NRW herangezogen werden, im Rahmen dessen sich letztlich „Insbesondere im Hinblick auf die Transparenz, die leichte Nachvollziehbarkeit und die weiteren oben beschriebenen Vorteile […] bei der (technisch) methodischen Umsetzung für die Verwendung von Entscheidungsbäumen entschieden“ wurde: Landeskriminalamt NRW, Abschlussbericht Projekt SKALA, 2018, S. 54, online: https://lka.polizei.nrw/sites/default/files/2018-06/180208_Abschlussbericht_SKALA.pdf.

v. Menschliche Aufsicht

> **KOM WEISSBUCH:** Die KOM fordert einen dem jeweiligen Risiko angemessenen - insbesondere von der beabsichtigten Nutzung der Systeme und den Auswirkungen abhängenden - Grad an menschlicher Aufsicht (S. 25).

Position D64: Wir begrüßen diese Anforderung grundsätzlich. Es gehört zum unveräußerlichen Kern der Menschenwürde (Art. 1 Abs. 1 GG), dass Betroffene durch umfassende oder einschneidende vollautomatisierte Prozesse nicht zum bloßen Objekt fremden Handelns verkommen dürfen. Um zu effizienteren und effektiveren Entscheidungen zu gelangen, kann **die Automatisierung mancher (Entscheidungs-)Prozesse** jedoch auch **ausdrücklich erwünscht** sein. Menschliche Aufsicht muss daher **nicht für alle Fälle zwingend nötig** sein, sie sollte aber **stets möglich** sein.

Es gilt zu beachten, dass menschliche **Aufsicht und Transparenz Hand in Hand** gehen. Die den Aufsehenden zur Verfügung stehenden Informationen bestimmen Qualität, Umfang und Nutzen menschlicher Aufsicht. Menschliche Aufsicht sollte daher grundsätzlichen dieselben Informationen und Richtlinien zur Entscheidungsfindung erhalten wie die Entscheidungssysteme selbst.

Wer effektive menschliche Aufsicht fordert, muss auch ein **kritisches Abwägen des Sachverhalts** - bzw. der maschinengenerierten Empfehlung oder Entscheidung - ermöglichen. Dies erfordert, dass menschliche Aufsicht an Standards zur Erklärbarkeit der Outputs von KI-Systemen geknüpft wird. Ansonsten sind Aufsichtspflichten ein zahnloses Instrument.

Zudem gilt es das **Problem des standardmäßigen Übernehmens** von Entscheidungsempfehlungen, insbesondere um sich keiner eigenen Haftung auszusetzen (sog. *automation bias*), anzugehen. In diesem Zusammenhang ist es wichtig, Abweichungen von maschinellen Entscheidungsempfehlungen nicht *per se* als sorgfaltswidrig und umgekehrt die Befolgung maschineller Entscheidungsempfehlungen nicht *per se* als sorgfaltsgetreu anzusehen.

vi. Besondere Anforderungen an ausgewählte Technologien

Position D64: Die oben dargestellten Anforderungen sind vorwiegend auf Entscheidungssoftware zugeschnitten und nach unserer Auffassung sind damit auch deren zentrale Risiken abgedeckt. Der Vorteil dieser Anforderungen liegt gerade in ihrer **Technologieneutralität**, sodass auch zukünftige, sich rasch entwickelnde neue Technologien umfasst wären.

Allerdings halten wir es für erforderlich, darüber hinaus die nachfolgenden **spezifischen Technologien** in den Blick zu nehmen. Die obenstehenden Anforderungen decken ihre besonderen Risiken nicht ab.

- **Biometrische Fernidentifikation**
  D64 unterstützt es nachdrücklich, der biometrischen Fernidentifikation aufgrund der potenziellen tiefgreifenden Auswirkungen auf die Freiheitsrechte besondere Aufmerksamkeit zukommen zu lassen. Wir sehen das Hauptproblem jedoch **nicht** in der **mangelnden Funktion bezüglich einzelner Bevölkerungsgruppen** (vgl. S. 13). Vielmehr liegt dieses gerade in **einer unausweichlichen und höchst präzisen, flächendeckenden Funktion und Verwendung** (vgl. sog. „zweite Welle“ der Debatte um KI-Regulierung).[23] Neben biometrischen Verfahren kommen (insbesondere mit der Gangerkennung) auch weitere, kritische Verfahren der Fernidentifikation in Betracht.

[23] Siehe dazu bspw. die aktuelle Diskussion um das in Polen entwickelte System PimEyes.

- **Deep Fakes**
  Von künstlich generierten Inhalten zu vermeintlich echten Personen und Sachverhalten (sog. *deep fakes*; mittels *Generative Adversarial Networks*) können erhebliche Risiken für die Persönlichkeitsrechte der betroffenen Personen sowie für die öffentliche Meinungsbildung ausgehen.
- **Sprachassistenten und -bots**
  Sprachassistenten und -bots (z.B. im Rahmen einer Telefonberatung) können die Integrität und Vertraulichkeit zwischenmenschlicher Kommunikation gefährden. Um diese aufrecht zu erhalten, halten wir es für erforderlich, in speziellen Anwendungsfällen[24] Kennzeichnungspflichten vorzusehen.

c. Adressaten

KOM WEISSBUCH: Die KOM definiert die Anforderungen an algorithmische Systeme zunächst abstrakt, ohne konkret diejenigen zu benennen, die ihnen nachkommen müssen. Stattdessen entwickelt sie eine Formel, anhand derer sie die Adressaten der Anforderungen in Zukunft bestimmen will: Diejenigen Akteure, die am besten in der Lage sind, das potentielle Risiko einzuhegen, sind Adressaten der Anforderungen an algorithmische Systeme.[25] Der Ansatz trage der Gewissheit Rechnung, dass nicht jeder Akteur auf alle Phasen im Lebenszyklus eines algorithmischen Systems gleichermaßen Einfluss nimmt. So gäben Entwicklerinnen und Entwickler die grundlegenden Funktionsweisen algorithmischer Systeme zwar zunächst vor, sie hätten aber bspw. regelmäßig keine Entscheidungsmacht darüber, wie die Anwendenden solche Systeme einsetzen.

Position D64: Wir halten den an einer effektiven Risikominimierung sowie an den tatsächlichen Möglichkeiten orientierten Ansatz für grundsätzlich sinnvoll. Eine ausgewogene konkrete Ausgestaltung könnte sich an den nachfolgenden Aspekten orientieren.

i. Grundsätze für die Zuweisung

Die Zuweisung der Anforderungen an einzelne Akteure sollte nach Ansicht von D64 zu einem möglichst hohen Maß an **Rechtssicherheit**, Effektivität bzw. **Einfachheit der Rechtsdurchsetzung** (aus Sicht der Betroffenen) sowie **Effektivität der Rechtsgewährung** (aus gesamtökonomischer Perspektive) führen.

(1) Rechtssicherheit

Das rechtsstaatliche Gebot der Bestimmtheit gibt vor, dass klar erkennbar sein muss, **wer wann Adressat** einer Verpflichtung ist.

(2) Effektivität der Rechtsdurchsetzung

Betroffene Personen sollten ihre Rechte stets einfach **gegenüber einer verantwortlichen Person geltend machen** können. Die Anwendenden entscheiden, ob und welches KI-System sie einsetzen,

---

[24] Ausnahme: Die maschinelle Generierung der Kommunikationsinhalte ergibt sich bereits zweifelsfrei aus den Umständen oder es besteht bereits offensichtlich kein Vertrauenstatbestand (z.B. Ansagen an Bahnhöfen etc.).

[25] Die KOM nennt neben Entwicklerinnen und Entwicklern und Anwenderinnen und Anwendern auch Herstellerinnen und Hersteller, Händlerinnen oder Händler sowie Importeure, Dienstleister, professionelle oder private Nutzerinnen und Nutzer.

um von ihnen festgelegte Verarbeitungszwecke zu erreichen.[26] Indem sie das System gegenüber den Betroffenen einsetzen, nehmen sie den entscheidenden Schritt vor, der die Betroffenen den entsprechenden Risiken aussetzt. Sie sind es zudem, die unmittelbar gegenüber den Betroffenen in Erscheinung treten. Für die Betroffenen ist dabei typischerweise weder ersichtlich, noch von Bedeutung, wer das algorithmische Entscheidungssystem auf wessen Weisung hin hergestellt hat. Dies spricht in der Tendenz für eine stetige **Verpflichtung der Anwendenden** algorithmischer Entscheidungssysteme.

(3) Effektivität der Rechtsgewährung

Niemand sollte über sein eigenes Können hinaus verpflichtet werden. Das Können hängt in einem ersten Schritt davon ab, welche **Anforderung** in welcher **Phase** des Lebenszyklus eines algorithmischen Entscheidungssystems[27] gewährleistet werden muss (Abbildung 2 unten) und in einem zweiten Schritt davon, welcher **Akteur** für diese **Phase** verantwortlich ist (Abbildung 3 unten).

Anforderungsanayse und -definiton	Entwicklung (Entwurf, Implementierung, Tests, Feedback)	Inbetriebnahme und Personalisierung	Einsatz
			Menschliche Aufsicht
			Transparenz „Ob“
Grundvoraussetzungen schaffen; Problem: Neuronale Netze			Transparenz „Wie“
	Aufbewahrung von Daten und Aufzeichnungen	Aufbewahrung von Daten und Aufzeichnungen	
Grund-voraussetzungen schaffen	Nicht-Diskriminierung	Nicht-Diskriminierung	
	Robustheit und Genauigkeit		

Abbildung 2: Zuordnung der Anforderungen zu einzelnen Phasen des Lebenszyklus eines algorithmischen Entscheidungssystems

Es sind stets die Anwendenden, die algorithmische Systeme einsetzen. Wer hingegen für die anderen Phasen verantwortlich ist hängt stark vom Einzelfall ab. Nachfolgende Konstellationen können als typisierte Beispiele verstanden werden:

Szenario	Anforderungsanayse und -definiton	Entwicklung	Inbetriebnahme und Personalisierung	Einsatz
In-House-Entwicklung	Anwendende	Anwendende	Anwendende	Anwendende
Auftragsentwicklung	Anwendende	Anwendende durch Herstellende	Anwendende durch Herstellende	Anwendende
Einkauf von Modulen, z.B. neuronale Netze zur Gesichtserkennung	Herstellende	Herstellende	Anwendende	Anwendende
Einkauf von Modulen, die bereits Voreinstellungen für die Daten, z.B. durch Fairnessmaße, treffen	Herstellende	Herstellende	Herstellende / Anwendende	Anwendende
Fertige Standardprodukte	Herstellende	Herstellende	Herstellende	Anwendende
System bleibt beim Hersteller (z.B. Schufa)	Herstellende	Herstellende	Herstellende	Herstellende / Anwendende

Abbildung 3: Verantwortliche für einzelne Phasen des Lebenszyklus eines algorithmischen Entscheidungssystems

[26] Anwendende gleichen insoweit den Verantwortlichen i.R.d. europäischen Datenschutzrechts. Dieses nimmt primär die „Verantwortlichen“ – also diejenigen, die über die Zwecke und Mittel der Verarbeitung personenbezogener Daten entscheiden – in die Pflicht die Anforderungen der DSGVO zu erfüllen.

[27] Auch wenn die unterschiedlichen Phasen der Softwareentwicklung aufgrund ‚agiler‘ Entwicklungsprozesse immer weniger linear verlaufen lassen sich weiterhin drei übergeordnete Phasen voneinander trennen.

Die Möglichkeiten der Einflussnahme auf die Systemgestaltung sind dabei fließend:

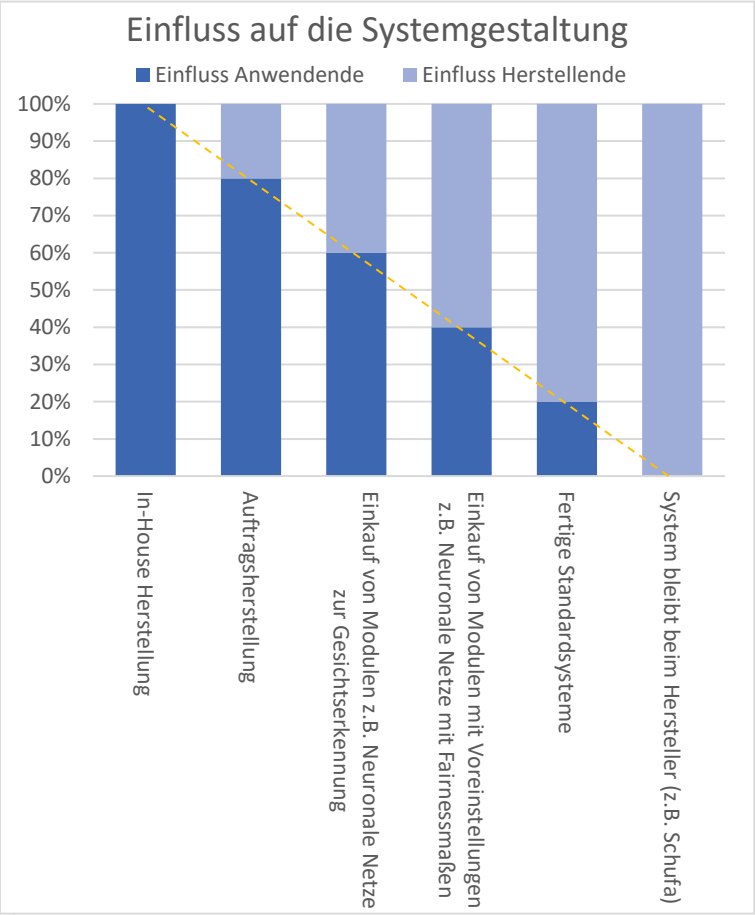


Abbildung 4: Fließender Übergang des Einflusses der Akteure auf die Systemgestaltung

Gerade kleine Anwendende werden sich regelmäßig proprietärer Standardsoftware oder gar der Entscheidungssysteme externer Dienstleister bedienen, auf die sie nahezu kaum einwirken können.

Auch in diesen Fällen könnte von ihnen jedoch verlangt werden, lediglich Systeme einzukaufen, die den gesetzlichen Anforderungen entsprechen. Verpflichtungen, die **rein die Anwendenden adressieren**, würden somit über die Nachfrage rechtskonformer Produkte am Markt **mittelbar ebenfalls gegenüber den Herstellenden** wirken. Gerade bei kleinen Nachfragenden ohne das notwendige Know-How um die Systeme zu überprüfen sowie bei monopolistischen, ausländischen Anbietenden kommt diese mittelbare Wirkung jedoch an ihre Grenzen.

Die **Herstellenden** sind zur Überprüfung und Gewährleistung der der Entwicklungsphase zuzuordnenden Anforderungen aufgrund ihrer spezifischen Fachkenntnisse hingegen regelmäßig besonders kostengünstig in der Lage. Aus gesamtökonomischer Perspektive ist es daher grundsätzlich sinnvoll sie zu den diesbezüglichen Anforderungen zu verpflichten. Sie werden die Kosten hierfür dann ohnehin an ihre jeweiligen Abnehmer weiterleiten.

Dies spricht in der Tendenz dafür (zumindest auch) **Herstellende in die Pflicht zu nehmen**.

ii. Stete Verantwortlichkeit der Anwendenden plus punktuelle Verantwortlichkeit der Herstellenden

Die Anwendenden sollten nach Ansicht von D64 stets verantwortlich zeichnen müssen, Herstellende ggf. zusätzlich für die in die Entwicklungsphase fallenden Anforderungen Nicht-Diskriminierung (ggf. inkl. Aufzeichnung der Trainingsdaten) sowie Qualität und Robustheit.

(1) Keine pauschale Verantwortlichkeit der Herstellenden

Dabei sollten die Herstellenden nicht pauschal für sämtliche Verpflichtungen eintreten müssen.

In der bestehenden Rechtsordnung nimmt zwar insbesondere das Produktsicherheitsrecht zentral die Herstellenden in die regulatorische Pflicht. Sein Regime gilt jedoch für **größtenteils statische physische Produkte**. Diese zeichnen sich dadurch aus, dass sie einmalig in den Verkehr gebracht und anschließend i.d.R. weder durch die Herstellenden selbst noch durch die Anwenderinnen und Anwender modifiziert werden.

Diese Prämisse gilt jedenfalls nicht für alle algorithmischen Systeme. Machine Learning-Systeme können z.B. auch nach dem Inverkehrbringen weiterlernen – auch wenn dies in der Praxis eher die Ausnahme sein dürfte. Regelmäßig optimieren Herstellende die Systeme jedoch durch **Updates**. Auch im Rahmen des Weiterlernens erreichte Verbesserungen des Systems werden in der Praxis in der Regel erst nach eingehender Prüfung und Überwachung des Lernprozesses und daher ebenso wie sonstige Updates punktuell übertragen.

Eine weitere Herausforderung birgt zudem das Prinzip der **agilen Produktentwicklung.** Bei dieser werden unterschiedliche Module zusammengesetzt und unterschiedliche Akteure können beteiligt sein. Allerdings wird es **stets einen letztverantwortlichen Hersteller** geben, der für die Zusammensetzung verantwortlich ist und die Interaktion zwischen den Modulen gewährleistet.

Viele **Systeme** können zu unterschiedlichen **Zwecken eingesetzt werden**. So können Anwendende ein neuronales Netz zur Gesichtserkennung bspw. einsetzen, um Mobiltelefone zu entsperren, oder um Personen im Rahmen einer Überwachung zu identifizieren. Den Herstellenden muss nicht zwingend bekannt sein, zu welchem Zweck die Anwendenden ihr algorithmisches System einsetzen werden und sie können dies auch nicht zwangsläufig überprüfen. Es sind also Szenarien denkbar, in denen die Herstellenden allenfalls abstrakt einschätzen können, welche Risiken es hervorruft, wenn sie ein KI-System auf den Markt bringen. Als Faustformel kann aber gelten, dass sie umso höhere Anforderungen erfüllen müssen, je konkreter abzusehen ist, dass Anwendende ihr System zu riskanten Zwecken einsetzen. So ist etwa bei einer Recruiting-Software der Zweck ihres Einsatzes von den Herstellenden vorgegeben und die Anwendenden können diesen Zweck auch nicht ändern, ohne in den Programmcode der Software einzugreifen. Sie können allerdings den sektoralen Einsatzbereich - *i.e.* die Job-Branche - bestimmen.

(2) Stete Verantwortlichkeit der Anwendenden

Die Anwendenden entscheiden über den konkreten Einsatzbereich, treten gegenüber den Betroffenen in Erscheinung und tragen die Früchte des mit der Entscheidungsautomatisierung einhergehenden Rationalisierungsprozesses. Im Interesse der Rechtssicherheit und der Effektivität der Durchsetzung der Betroffenenrechte sollten sie **stets** für die Anforderungen **verantwortlich** sein.

iii. Stufenweise Verantwortungszuweisung

Ein weiteres Argument für die „tastende“ Ausgestaltung des Rechtsrahmens ist, dass Beteiligte unterschiedliche Möglichkeiten haben unterschiedliche Anforderungen zu erfüllen. Der Adressatenkreis sollte daher stufenweise für verschiedene Anforderungen erschlossen werden.

(1) Transparenz und menschliche Aufsicht: Subjektive Rechte gegenüber den Anwendenden

Die Anforderungen ‚Menschliche Aufsicht‘ (bzw. Letztentscheidung) und ‚Transparenz‘ bezüglich des „Ob“ des Einsatzes algorithmischer Systeme (Kennzeichnungspflicht) setzen bei der konkreten Letztentscheidung durch den Anwendenden (und nicht der Systementwicklung) an. Ihre Gewährleistung ist jenen in aller Regel auch **ohne ein Mitwirken der Herstellenden** möglich.

Auch die Anforderung ‚Transparenz‘ bezüglich des „Wie“ - sprich bezüglich der abstrakten oder konkreten Funktionsweise / Logik eines Systems - setzt bei der Letztentscheidung an. Hierfür müssen dem Anwendenden jedoch selbst die nötigen Informationen (vom Hersteller) zur Verfügung stehen. Da eine solche Anforderung nur für verhältnismäßig riskante Anwendungen in Betracht kommt, kann von dem Anwendenden auch verlangt werden in diesen Bereichen nur Systeme einzusetzen, von denen er / sie zumindest die grundlegende Funktionsweise kennt und den Betroffenen entsprechend erklären kann.

Konformitätsbewertungsverfahren (die nicht bei der Letztentscheidung, sondern der Systemgestaltung ansetzen und daher klassischerweise die Herstellenden in die Pflicht nehmen) sind für diese Anforderungen daher nicht zielführend. Stattdessen sollten **subjektive Rechte der Betroffenen gegenüber den Anwendenden** geschaffen werden. Da diese Anforderungen zudem die geringste Eingriffstiefe in die Rechte der Anwendenden darstellen, könnte dies der **nächste Schritt einer tastenden Regulierung** sein.

(2) Nicht-Diskriminierung, Qualität und Robustheit: Weiterer Forschungsbedarf

Die Anforderungen Nicht-Diskriminierung sowie Qualität und Robustheit setzen hingegen nicht bei der Letztentscheidung, sondern bereits früher bei der Gestaltung der Systeme an. Ob diese Anforderungen durch die Anwendenden alleine gewährleistet werden können hängt stark von dem jeweiligen Zusammenwirken der an der Systemgestaltung beteiligten Akteure ab (s. Abb. 3 oben).

Der Gesetzgeber sollte diese Anforderungen sollte daher als letzten Schritt der tastenden Regulierung angehen. Dafür spricht auch, dass diese Anforderungen verhältnismäßig intensiv in die Gestaltungsfreiheit der Entwickelnden eingreifen.

Denkbar erscheinen nach derzeitigem Stand der Forschung zumindest drei Modelle:

- **Gemeinsame Verantwortlichkeit**
  Unter dem Aspekt der Einheitlichkeit der Rechtsordnung wäre es denkbar, die Regelungssystematik des Art. 26 DSGVO zu übernehmen und je nach Weisungsgebundenheit bzw. Entscheidungsfreiraum des Herstellenden gegenüber dem Anwendenden eine **alleinige Verantwortung des Anwendenden** oder eine **gemeinsame Verantwortung** anzunehmen. Dies würde unter dem Gesichtspunkt der Effektivität der Rechtsgewährung (siehe oben *B.III.2.c.iii.(3)*) diejenigen Anwendenden als alleinige Verantwortliche einstufen, die aufgrund ihrer Weisungsbefugnis gegenüber dem Hersteller selbst für die Einhaltung der Anforderungen sorgen können. Sobald der Herstellende hingegen eine gewisse Grenze an eigener Entscheidungsfreiheit überschreitet wäre er ebenfalls verantwortlich. Die Beteiligten könnten eine Vereinbarung darüber treffen, wer von ihnen welche Verpflichtung erfüllt und die betroffenen Personen über das Wesentliche dieser Vereinbarung informieren (vgl. Art. 26 Abs. 1 S. 2, Abs 2 S. 2 DSGVO). Ob eine gemeinsame Verantwortlichkeit besteht, sollte in jedem Fall anhand objektiver Umstände bestimmt werden. Der Vereinbarung sollte dabei maximal Indizwirkung zukommen,[28] um staatliche Eingriffsbefugnisse nicht von privatrechtlichen Vereinbarungen abhängig zu machen. Gegen ein solches, an der tatsächlichen Einflussmöglichkeit orientiertes Modell spricht insb., dass eine Abgrenzung bei den fließenden Übergängen der Formen der Zusammenarbeit in der Praxis oft schwierig sein dürfte.
- **Verantwortlichkeit der Anwendenden aber Vermutungswirkung der Rechtskonformität beim Einsatz (freiwillig) zertifizierter Produkte**
  Anwendende sowie Behörden dürften regelmäßig gleichermaßen vor der Herausforderung stehen, einschätzen zu müssen, ob komplexe algorithmische Systeme den jeweiligen Anforderungen entsprechen. Die **freiwillige** Einbindung der Expertise benannter Stellen im Rahmen von **Konformitätsbewertungsverfahren (Zertifizierung)** bzw. die Selbst-Zertifizierung der Hersteller, um in entsprechend regulierte Nischenmärkte einzudringen, könnte hier Abhilfe schaffen. Aus Gründen der Wirtschaftlichkeit wäre es auch sinnvoller, wenn die Herstellenden das Konformitätsbewertungsverfahren einmalig und zentral

[28] So anstelle vieler auch die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder zu Art. 26 DSGVO (Kurzpapier Nr. 16, S. 3) und bereits die Art. 29-Gruppe zur alten Datenschutzrichtlinie (WP 169, S. 14).

durchlaufen und die Anwendenden nicht jeweils Einzelnachweise erbringen müssten. Dies gilt zumindest für breite Standard-Anwendungen.

- **Verantwortlichkeit der Anwendenden plus Verpflichtung der Herstellenden zur Zertifizierung** Die Frage, wer für die Einhaltung einzelner Anforderungen verantwortlich sein soll (Adressaten), ist also unweigerlich mit der Frage verknüpft, wann und durch wen die Einhaltung überprüft werden soll (siehe hierzu unten *B.III.2.d*). Ein staatliches Regulierungsmodell, das den Anwendenden (und den Zeitpunkt nach dem Inverkehrbringen) in den Blick nimmt, könnte auch zusätzlich mit einem **verpflichtenden** Modell der Ko-Regulierung kombiniert werden, das Herstellende zur Vornahme von **Konformitätsbewertungsverfahren (Zertifizierung)** zum Zeitpunkt vor dem Inverkehrbringen verpflichtet. So sind Kfz-Herstellende beispielsweise im Rahmen der Kfz-Typengenehmigung ebenso für Sicherheit verantwortlich wie Autofahrende (Anwendende) durch das Straßenverkehrsrecht zum sicheren Fahren verpflichtet werden.

d. Governance

i. Freiwillige Kennzeichnungssysteme / Selbstregulierung

KOM WEISSBUCH: Die KOM erwägt es für Anwendungen, „die nicht als Anwendungen ‚mit hohem Risiko' eingestuft werden (...) ein freiwilliges Kennzeichnungssystem einzuführen" (S. 29).

Position D64: Wir halten dieses Vorhaben nur sehr bedingt für zielführend.

Im Lebensmittelbereich sind Verbraucherinnen und Verbraucher bereits mit einer solchen Vielzahl von Umwelt/Öko-, Nachhaltigkeits-, Nutri-Score-, Gentechnik-, Ursprungs-/Herkunfts-/Regional-Zeichen u.v.m. konfrontiert, dass dies gar ein Bedürfnis nach eigenen Gütesiegel-Bewertungsstellen[29] auslöst. Diese **Überforderung** muss im Bereich von Software vermieden werden. Kein Betroffener und keine Betroffene hat die Zeit, sich mit den hinter einem Siegel stehenden Kriterien auseinanderzusetzen. Sie müssen den Siegeln blind vertrauen können.

Zudem muss die Einhaltung der dahinterstehenden Anforderungen (zumindest durch staatlich Beliehene oder benannte Stellen) **überprüfbar** und **Verletzungen sanktionierbar** sein. Die Abwesenheit solcher Mechanismen im Rahmen der Selbstregulierung der Finanzbranche vor 2008 hat beispielsweise die Schwächen eines solchen Systems deutlich vor Augen geführt.

Darüber hinaus würde ein Label, wie es die KOM hier angedacht hat, nur Wirkung zeigen, wenn Anwender oder Betroffene tatsächlich eine Auswahl zwischen Diensten hätten. Bei Systemen, die im öffentlichen Sektor - bspw. im Jobcenter - eingesetzt werden, ist das z.B. nicht der Fall.

ii. Ko-Regulierung

KOM WEISSBUCH: Die KOM fordert mit der vorab vorzunehmenden Konformitätsbewertung am Maßstab der von Interessenträgern und europäischen Normungsorganisationen vorgegebenen technischen Normen (S. 27) ein System der Ko-Regulierung.

Position D64: Wir plädieren insbesondere auf der ersten Stufe der tastenden Regulierung für die Einführung **staatlicher Regulierung,** um Transparenz zu schaffen und Wissen zu erlangen. Hierfür ist keine (über dieses Konsultationsverfahrende) Einbeziehung Privater in Normgebung oder -aufsicht erforderlich. Gleichzeitig halten wir langfristig grundsätzlich auch den **punktuellen Einbezug** von Elementen der **Ko-Regulierung** für denkbar.

Sinnvoll könnte z.B. die Schaffung eines **„TES-Kennzeichens" (Trusted European Software)** sein, das die Einhaltung der durch den demokratisch legitimierten Gesetzgeber selbst grob

[29] Z.B. https://label-online.de

vorgegebenen (und durch Normierungsorganisationen konkretisierten) grundlegenden Anforderungen zum Ausdruck bringt.

Technische Normung hat eine Reihe von **Vorteilen** gegenüber rein staatlicher Regulierung, wie z.B.

- die schnellere Anpassungsfähigkeit,
- die erhöhte Akzeptanz der am Normgebungsprozess Beteiligten sowie
- die hohe technische Expertise der Beteiligten.

Sie eignet sich daher besonders für rein technische Vorgaben, die schnellen Änderungen unterliegen - wie z.B. Anforderungen an die Cybersicherheit.

Technische Normung weist jedoch im Verhältnis zu staatlicher Normung bedeutende **Nachteile** auf. Hierzu zählt insbesondere

- die mangelnde demokratische Legitimation. Diese ist umso größer, je allgemeiner die „grundlegenden Anforderungen" sind, welche der Staat den Normungsgremien zur konkretisierenden Ausgestaltung vorgibt. Dies erscheint besonders problematisch in Bereichen, die nicht lediglich ein Zusammentragen des „Standes der Technik", sondern politische Wertentscheidungen - wie z.B. die Vorgabe konkreter Fairnessmaße - erfordern;
- die mangelnde kostenfreie Verfügbarkeit. Technische Normen sind in der Regel nicht öffentlich und kostenfrei für jede und jeden, sondern nur gegen Entgelt auf den Seiten der Normungsorganisation erhältlich;
- die in der Praxis vorherrschende starke Interessengeleitetheit und Dominanz der Normierungsprozesse durch einige wenige marktmächtige Akteure.

Zentral für D64 wäre daher in jedem Fall, dass der Gesetzgeber durch entsprechende finanzielle Unterstützungen sicherstellt, dass die einschlägigen Normungsgremien **ausgeglichen besetzt** sind. Neben Vertreterinnen und Vertretern großer Konzerne sollten auch solche von KMUs/Start-Ups sowie der organisierten Zivilgesellschaft am Tisch Platz haben. Neben Programmierinnen und Programmierern bzw. Data Scientists müssen insbesondere auch Geisteswissenschaftlerinnen und Geisteswissenschaftler vertreten sein, da stets auch gesellschaftspolitisch relevante Fragen zu beantworten sein werden.

Zu bedenken gilt überdies, dass die geforderten **Konformitätsbewertungsverfahren** sich als nicht unerhebliche **Marktzugangsbarrieren** – insbesondere für Start-Ups und KMUs – entpuppen könnten. Diese wären im Unterschied zu großen Digitalkonzernen voraussichtlich weder unmittelbar selbst am Normungsprozess beteiligt, noch verfügen sie über eigene Rechtsabteilungen. Die Einbeziehung benannter Stellen ist zudem i.d.R. mit nicht unerheblichen finanziellen Aufwendungen verbunden. In jedem Fall würde sich so voraussichtlich die *‚time to market'* europäischer Anwendungen erheblich verlängern, wodurch etwaige *‚first mover advantages'* genommen werden.

Im Unterschied zum durch statische, physische Produkte gekennzeichneten Produktsicherheitsrecht verändern sich algorithmische Systeme in der Regel häufig durch **Updates/Patches** bzw. durch (in aller Regel ebenfalls punktuell und nicht kontinuierlich übertragene) Änderungen aufgrund des Weiterlernens. Dies würde häufige und **zahlreiche Neubewertungen** erforderlich machen. Die hiervon ausgehende Belastung könnte jedoch dadurch erheblich abgemildert werden, dass eine Zulassung lediglich für Systeme, deren Risiko eine gewisse Schwelle überschreitet, erforderlich wäre (vgl. oben Anwendungsbereich). Zudem könnte in Risikostufe I die Konformitätserklärung selbst und ohne Einbeziehung einer benannten Stelle vorgenommen werden. Das Erfordernis einer Neubewertung könnte auf die Vornahme „wesentlicher Änderungen" begrenzt werden.

Die Forderung, dass die Konformitätsbewertungen Teil der Konformitätsbewertungsmechanismen sein sollten, die es bereits für eine große Zahl von Produkten gibt (S. 27) ist hingegen nicht tragfähig. Die bestehenden Verfahren nehmen alleine die Hersteller in die Pflicht. Eine Reihe der gegenständlichen Anforderungen adressieren hingegen gerade auch die Anwenderinnen und Anwender (siehe oben *B.III.2.c.*).

iii. Staatliche Regulierung

In den vergangenen Jahren wurden eine Reihe **innovativer Instrumente zur Einbeziehung Privater** in den letztlich jedoch staatlichen Normgebungsprozess entwickelt,[30] die die Vorzüge der Ko-Regulierung in ein System staatlichen Normerlasses integrieren. Staatliche Regulierung ist vollkommen ausreichend um die, im ersten Schritt der tastenden Regulierung geforderte Risikofolgenabschätzung umzusetzen. Selbiges gilt für die Anforderungen Transparenz und menschliche Aufsicht.

e. Einhaltung der Durchsetzung (Aufsicht)

> **KOM WEISSBUCH:** Nach Ansicht der KOM sollten die zuständigen Behörden in der Lage sein, Einzelfälle zu untersuchen, aber auch die Auswirkungen auf die Gesellschaft zu bewerten (S. 27).

Position D64: Wir unterstützen dies vollumfänglich. Zum Zwecke der Bewertung von Auswirkungen auf die Gesellschaft erscheint insbesondere die Pflicht zur Durchführung und Übermittlung einer Risikofolgenabschätzung durch die Anwenderinnen und Anwender (siehe oben *B.III.1.b*) von Bedeutung.

Dabei sollte das Befugnis- und Sanktionsregime der DSGVO langfristig als Vorbild für die Kompetenzen der Aufsichtsbehörden dienen. Insbesondere das **am unternehmerischen Umsatz orientierte Sanktionsmodell** der DSGVO stellt einen wirksamen Durchsetzungsmechanismus dar. Hinzutreten sollten Auskunftsrechte sowie auch Möglichkeiten der Überprüfung von Systemen durch die zuständigen Behörden.

Um die Anforderungen (siehe oben *B.III.2.b*) nicht zum bloßen Papiertiger verkommen zu lassen und nicht zuletzt auch um das Vertrauen der Bürgerinnen und Bürger in einen handlungsfähigen Staat aufrecht zu erhalten, bedarf es **hinreichend ausgestatteter** und durchsetzungsstarker Aufsichtsbehörden. Die im Rahmen der Datenschutzaufsicht teils gravierenden personellen Unterbesetzungen[31] gilt es zu vermeiden.

Um eine **Fragmentierung der Aufsicht** - wie insbesondere im Bereich des Datenschutzes - zu vermeiden, ist aus Sicht von D64 mehr denn je ein **koordiniertes, europäisches Vorgehen** gefragt. Der Nationalstaat allein steht hier angesichts der fortwährenden Internationalisierung von Datenflüssen und -märkten vor stetig wachsenden Herausforderungen. Dies darf jedoch weder zu Nationalisierungstendenzen noch zur Kapitulation des Staates vor digitalen Großkonzernen führen. Nach der Datenschutz-Grundverordnung wird die Regulierung algorithmischer Entscheidungssysteme die zweite zentrale Technologie-Regulierung im 21. Jh. sein. Gemeinsam mit dem *Digital Services Act* werden diese drei Bausteine die Sicherstellung der Einhaltung unserer Grundwerte in der digitalen Welt sicherstellen können und müssen.

---

[30] Im Bereich der legislativen Normgebung zählen dazu insbesondere die im Rahmen der „better regulation"-Reform vorgesehenen Konformitätsbewertungsverfahren (wovon eines auch Anlass der vorliegenden Stellungnahme ist). Auch im Bereich der exekutiven Normkonkretisierung brachte die Debatte um eine „neue Verwaltungswissenschaft" zahlreiche neue Kooperationsinstrumente hervor.

[31] Siehe z. B. die für zahlreiche digitale Marktführer gleichzeitig zuständige irische nationale Datenschutzbehörde.

C. DIE ZUKUNFT IM BLICK

Der verstärkte Einsatz von KI und anderen algorithmischen Systemen kann zu tiefgreifenden Umwälzungen unserer Gesellschaft als Ganzes führen - sie sind Chance und Herausforderung zugleich. Technologiebezogene Regulierung allein kann nicht alle sozialen, ethischen, ökonomischen, ökologischen Auswirkungen in Bahnen lenken, die mit unserer europäischen Werteordnung übereinstimmen. Insofern begrüßen wir die im Kapitel zum *Ökosystem für Exzellenz* der KOM vorgeschlagenen Fördermaßnahmen, rufen jedoch zur weitergehenden gesellschaftlichen Debatte über Aspekte auf, die das Weißbuch nicht oder nicht hinreichend adressiert:

- **Autonome Waffensysteme**
  Im Hinblick auf autonome Waffensysteme bedarf es internationaler Einigungsbestrebungen, vergleichbar zu internationalen Abkommen zu anderen Waffentypen.
- **Wettbewerb**
  In einem idealisierten Wettbewerbssystem treibt die Konkurrenz am Markt die Herstellenden dazu an, technisch und ethisch hochwertige Produkte auf den Markt zu bringen. Echte Wahlmöglichkeiten der Verbraucherinnen und Verbraucher mildern Schwächen und potentiell negative Auswirkungen einzelner KI-Anwendungen ab. Eine zentrale Rolle wird daher auch die Debatte um die Generierung eines breiten Feldes an Anbieterinnen und Anbietern - bestehend nicht nur aus wenigen großen Playern, sondern einer Vielzahl auch kleinerer Herstellender - einnehmen. Die KOM sollte das europäische Wettbewerbsrecht daher gerade im KI-Kontext konsequent zur Durchsetzung bringen und Monopolbildungen vermeiden.
- **Arbeitsmarkt und Chancen- bzw. Bildungsgerechtigkeit**[32]
  Setzt die Wirtschaft künftig vermehrt auf den Einsatz von KI-Systemen, führt dies zu mehr Automatisierung. Es ist absehbar, dass KI-Systeme menschliche Arbeitskraft in einigen Wirtschaftssektoren weitgehend verdrängen werden. Wenngleich die Entwicklung und der Betrieb von KI-Systemen auch neue Arbeitsplätze schaffen, wird der Bedarf nach menschlicher Arbeitskraft insbesondere für einfache, repetitive Aufgaben sinken. Die neuen Arbeitsplätze werden den Mitarbeiterinnen und Mitarbeitern neue und tendenzielle höhere Qualifikationen abverlangen. Die wachsenden Qualifikationsanforderungen machen umfassende Maßnahmen erforderlich, um Bildungsgerechtigkeit - auch mit Blick auf lebenslanges Lernen - zu verwirklichen. Im Fokus der Debatte muss auch die Sicherstellung eines gleichen Zugangs aller Teilnehmer des Bildungssystems zu digitalen Ressourcen stehen. Selbst bei großen Anstrengungen der EU und der Nationalstaaten werden aber nicht alle Teilnehmer am Wirtschaftsverkehr gleich von dem Einsatz von KI-Technologien profitieren. Union und Mitgliedstaaten müssen mit der Zivilgesellschaft in einen offenen Dialog über Fragen der Verteilungsgerechtigkeit eintreten.

[32] Siehe dazu in ersten Ansätzen Weißbuch, S. 7 f.

- **Kompetenz der Zivilbevölkerung**
  Neben rein wirtschaftlich orientierten Aspekten sollte auch die allgemeine Kompetenz der Zivilbevölkerung stets mitgedacht werden. Eine kompetente Zivilbevölkerung ist sowohl in der Lage, algorithmische Systeme verantwortungsbewusst einzusetzen, als auch ihre Auswirkungen aus Betroffenenperspektive zu reflektieren.
- **Umwelt und Nachhaltigkeit**[33]
  Komplexe Rechenprozesse wie z.B. das Training tiefer neuronaler Netze können einen erheblichen Bedarf an Ressourcen haben. Die EU strebt eine nachhaltige Wirtschaft (*Green Deal*) an. Die Debatte sollte daher auch stets die Umweltbilanz, insbesondere den CO_2-Verbrauch von KI-Systemen, berücksichtigen.
- **Inklusion & Diversität**
  Auch unabhängig von der Betroffenenperspektive algorithmischer Systeme können bestehende Diskriminierungen und Ungleichheit wie z.B. Rassismus, Gehaltsbenachteiligung von Frauen oder überproportionale Vertretung von Männern in technischen Berufen sich reproduzieren, sodass die Punkte Inklusion und Diversität auch über den vorliegenden Regulierungsrahmen hinaus Berücksichtigung finden sollten.

D64 wird sich weiterhin aktiv an der Diskussion und Gestaltung dieser Themenfelder beteiligen.

[33] Siehe dazu in ersten Ansätzen Weißbuch, S. 2 f.

AUTORINNEN UND AUTOREN

KOORDINATION UND WISSENSCHAFTLICHE LEITUNG

MICHAEL B. STRECKER ist ausgebildeter Jurist (LMU) und Politikwissenschaftler (HfP, München). Nach knapp zwei Jahren im Grundsatzreferat Digitalisierung des BMJV und in der Geschäftsstelle der Datenethikkommission promoviert er nun am Lehrstuhl für Öffentliches Recht und Recht der Digitalisierung der Uni Bielefeld (Prof. Dr. Thomas Wischmeyer) zum Thema „Regulierungsmodelle für algorithmische Systeme“. Seit 10/2020 ist er zusätzlich Referent Themenentwicklung Digitalisierung beim SPD-Parteivorstand.

WEITERE AUTORINNEN UND AUTOREN

DAVID WAGNER ist ausgebildeter Jurist (JLU) und arbeitet als Forschungsreferent am Forschungsinstitut für öffentliche Verwaltung (Speyer) im Programmbereich „Transformation des Staates in Zeiten der Digitalisierung“. Er promoviert bei Prof. Dr. Mario Martini zu datenschutzrechtlichen Aspekten von Open Data.

MAXIMILIAN GAHNTZ hat Public Policy und Politik- und Verwaltungswissenschaft (Columbia University, Sciences Po Paris und Universität Konstanz) studiert. Derzeit ist er Fellow des Mercator Kollegs für Internationale Aufgaben und beschäftigt sich in diesem Kontext mit digitalpolitischen Fragen, insbesondere mit Künstlicher Intelligenz. Zuvor arbeitete er als Berater für Organisationen des öffentlichen Sektors.

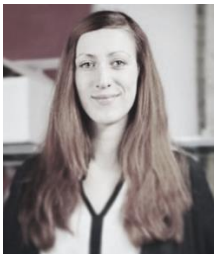
QUIRIN WEINZIERL ist ausgebildeter Jurist (LMU, Yale Law School). Er arbeitet als Forschungsreferent am Forschungsinstitut für öffentliche Verwaltung (Speyer), wo er ein vom BMJV gefördertes Forschungsprojekt zu „Dark Patterns“ leitet. Er promoviert bei Prof. Dr. Mario Martini zu Fragen von Verhaltenssteuerung und Recht.

KATJA NEUMANN ist ausgebildete Juristin (BLS) und studiert derzeit zusätzlich Informatik an der Universität Hamburg. Zudem arbeitet sie als Wissenschaftliche Mitarbeiterin an der Deutschen Universität für Verwaltungswissenschaften (Speyer) am Lehrstuhl für Verwaltungswissenschaft, Staatsrecht, Verwaltungsrecht und Europarecht (Prof. Dr. Mario Martini).

PHILIPP C. OTTE ist Politikwissenschafter (Freie Universität Berlin, Universidad Complutense de Madrid) und arbeitete als Senior Product Manager Digital Strategy bei N24 und WELT, wo er sich mit der digitalen Transformation der Medienbranche beschäftigte.

JAN KUHLEN ist studierter Jurist und Soziologe (Eberhard-Karls-Universität Tübingen) und mittlerweile Rechtsanwalt in eigener Kanzlei. Er war von 2018 - 2020 Sachverständiger der Enquete Kommission Künstliche Intelligenz des Deutschen Bundestages. Gemeinsam mit D64 klagt er gegen die Vorratsdaten-speicherung.

HENRIKE SCHLOTTMANN hält einen MSci in Mathematik (University College London). Sie war mehrere Jahre bei einer internationalen Managementberatung tätig und hat dort Projekte im Bereich Digitalisierung und Innovation begleitet. Heute ist sie Managing Director beim ProjectTogether und organisierte dort unter anderem mit 28.361 Teilnehmenden einen der größten Hackathons der Welt (#WirVsVirus).



SIMONE ORGEL studierte Kommunikation in sozialen und wirtschaftlichen Kontexten (Universität der Künste Berlin, University of Toronto) und hat als Kommunikationsexpertin für verschiedene öffentliche und private Institutionen gearbeitet. Heute ist sie Digitalstrategin, strategische Kommunikationsberaterin und Künstlerin, die sich auf Beteiligungsprozesse und Gemeinschaftsbildung im digitalen Raum konzentriert.

.

IMPRESSUM

ÜBER D64

D64 ist die Denkfabrik des digitalen Wandels. Unsere Mitglieder sind von der gesamtgesellschaftlichen Auswirkung der digitalen Transformation auf sämtliche Bereiche des öffentlichen und privaten Lebens überzeugt und wollen diese progressiv und inklusiv gestalten. Dabei liefern wir Impulse um die digitale Transformation zum positiven Gelingen zu bringen. Wir sind uns einig, dass man eine Politik der Zukunft nicht mit Konzepten von gestern machen kann. D64 – Zentrum für digitalen Fortschritt e.V. wurde 2011gegründet und ist gemeinnützig, überparteilich und unabhängig. Wir haben über 500 Mitglieder bundesweit, die sich allesamt ehrenamtlich engagieren und über das vereinseigene „digitale Vereinsheim“ organisieren. D64 bringt Expertinnen und Expertise aus Wissenschaft, Wirtschaft, Kultur, Zivilgesellschaft, Bildung und Politik zusammen und bringt diese Expertise in die politische Debatte ein. Jetzt Mitglied werden!

d-64.org/mitglied-werden

TICKER

Melde dich beim D64-Ticker an, um über aktuelle Ereignisse aus der Digitalszene und dem politischen Umfeld auf dem Laufenden zu bleiben! Du erhältst dann werktags jeden Morgen einen Newsletter mit entsprechenden Meldungen.

ticker.d-64.org

ADRESSE

D64 – Zentrum für Digitalen Fortschritt e.V.
Vorsitzender: Henning Tillmann
Vorsitzende: Laura-Kristine Krause
Gipsstr. 3
10119 Berlin

KONTAKT

D64 Vorstand
vorstand@d-64.org

EMPFOHLENE ZITIERWEISE

D64, Die Regulierung Künstlicher Intelligenz und anderer algorithmischer Entscheidungssysteme, Stellungnahme zum KI-Weißbuch, Oktober 2020

BERLIN, OKTOBER 2020