daten
ethik
kommission

Datenethikkommission revisited – Update der Empfehlungen nötig?

Univ.-Prof. Dr. Christiane Wendehorst, LL.M., Universität Wien
Co-Vorsitzende der Datenethikkommission (DEK) 2018-2019

daten
ethik
kommission

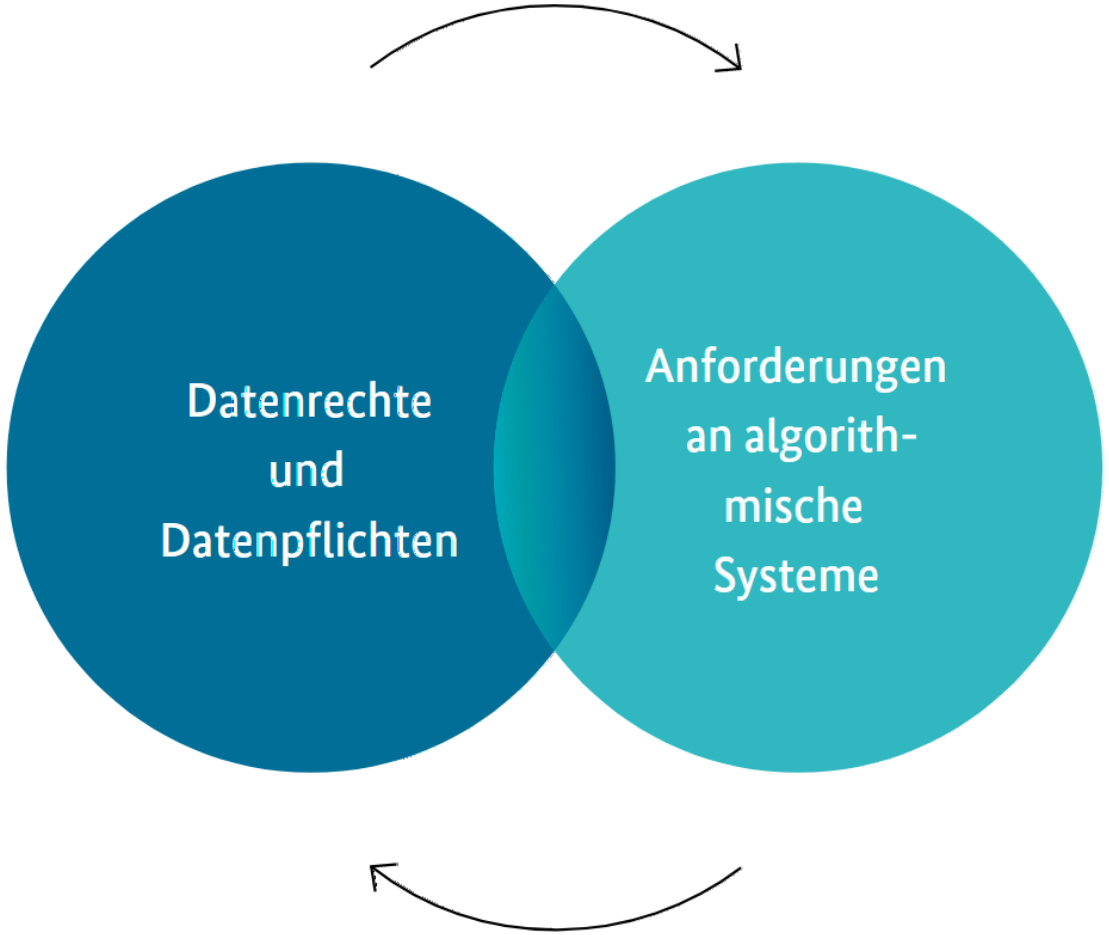
- DEK von der deutschen Bundesregierung im Sommer 2018 eingesetzt
- Entwicklung ethischer Leitlinien und konkreter Handlungsempfehlungen zu ADM, KI und Daten innerhalb eines Jahres
- 16 Mitglieder aus verschiedenen Disziplinen (Vorsitz: Christiane Wendehorst und Christiane Woopen)
- Gutachten mit 75 Handlungsempfehlungen am 23. Oktober 2019 in Berlin überreicht

daten
ethik
kommission

daten ethik kommission

daten
ethik
kommission

Datenperspektive und Algorithmenpersp



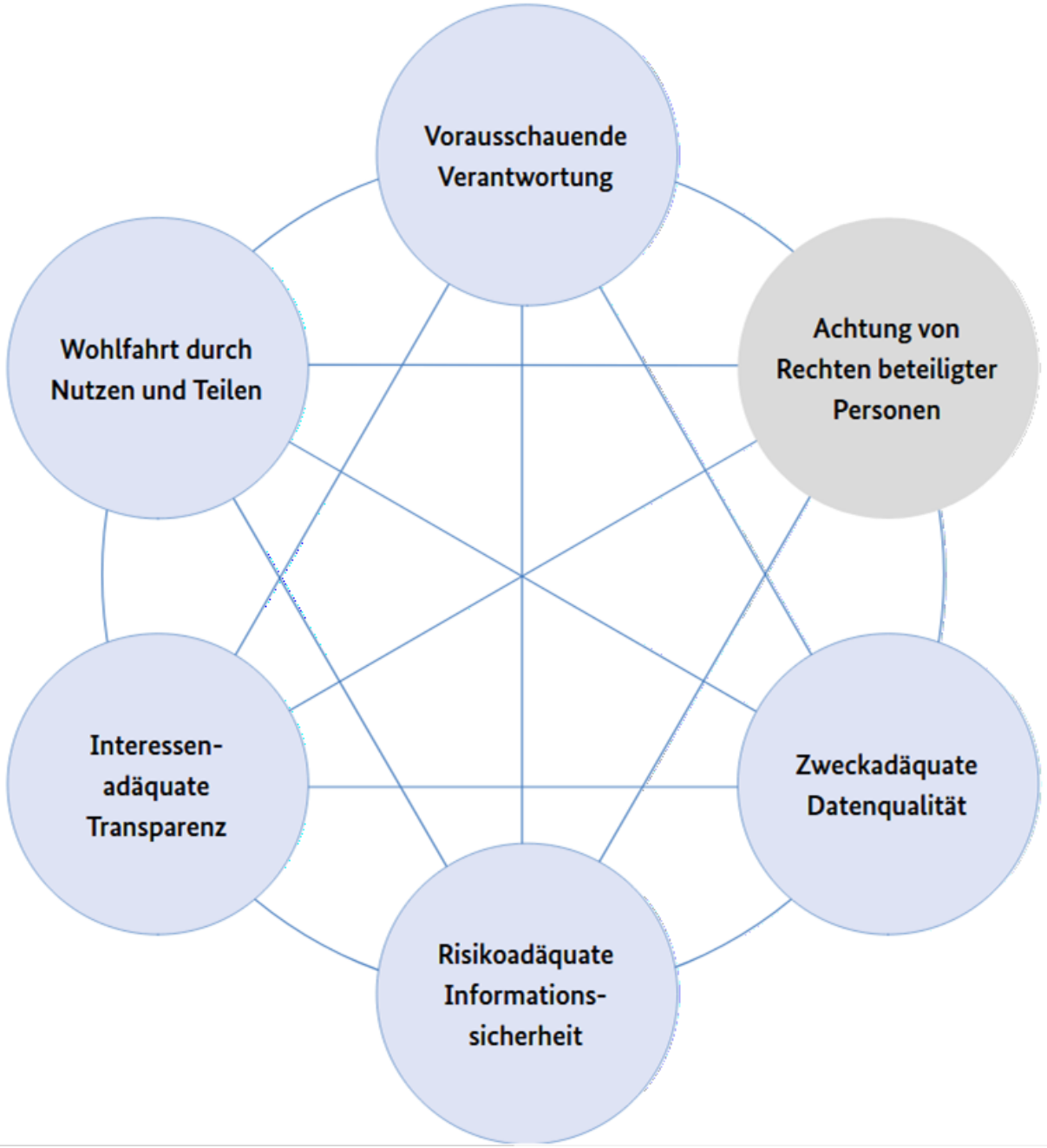
daten
ethik
kommission

Daten

daten ethik kommission

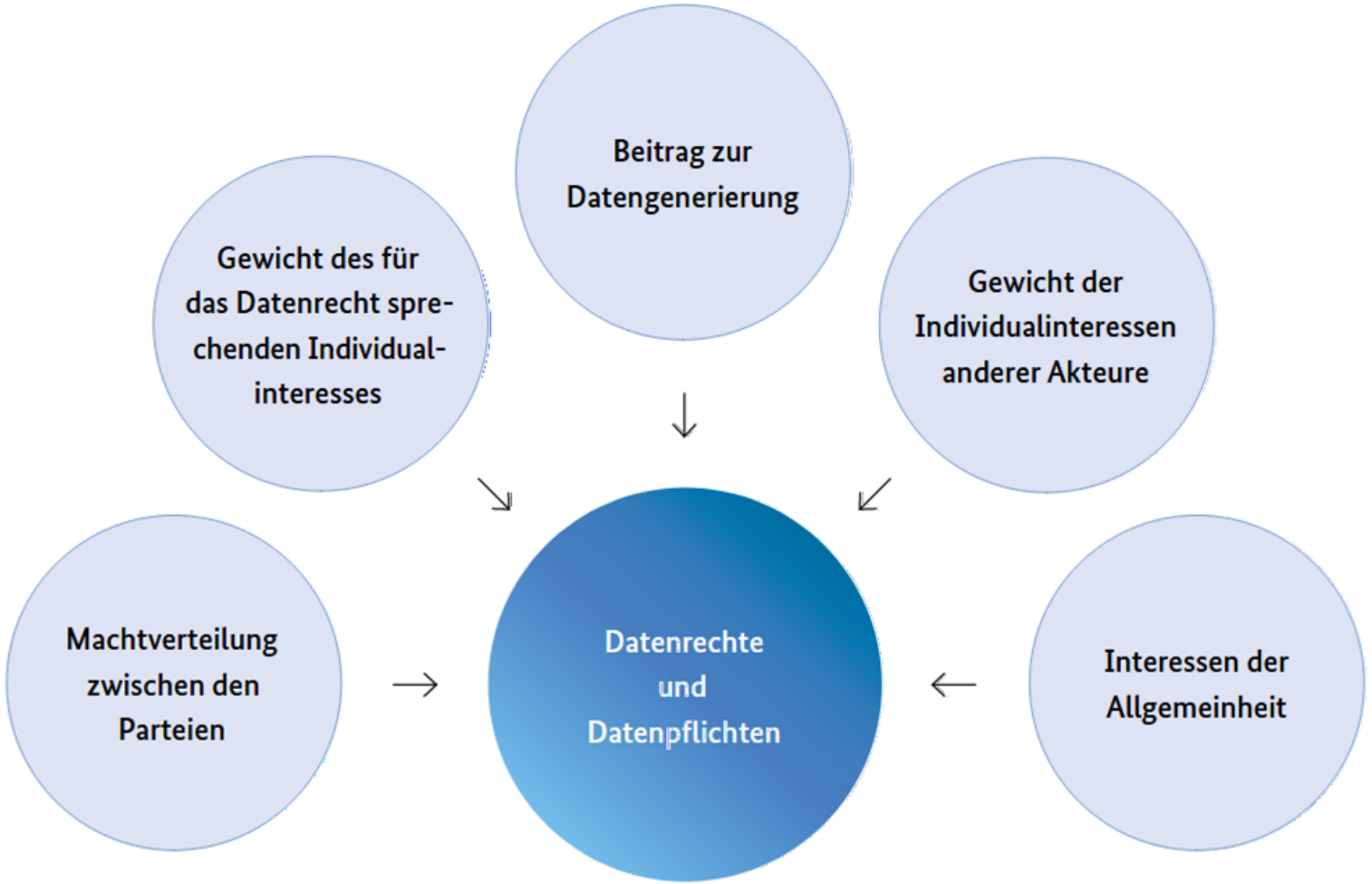
Anforderungen an den Umgang mit Daten

- Parallelen zu Grundsätzen der Datenverarbeitung nach der DSGVO
- **Potenziale von Datennutzung** für die allgemeine Wohlfahrt
- Es kann ein ethisches Gebot geben, Daten zu nutzen



daten ethik kommission

Datenrechte und ende Datenpflichten



- Rechte an „co-generierten Daten“
- **Kein (exklusives) „Dateneigentum“**
- Theoretisches Konzept von EU übernommen

daten
ethik
kommission

Anforderungen an den Umgang mit personenbezogenen Daten

daten ethik kommission

Anforderungen an die Nutzung personenbezogener Daten

1

Die DEK empfiehlt **Maßnahmen gegen ethisch nicht-vertretbare Datennutzungen**. Dazu gehören etwa Totalüberwachung, die Integrität der Persönlichkeit verletzende Profilbildung, gezielte Ausnutzung von Vulnerabilitäten, sog. Addictive Designs und Dark Patterns, [illegible]mokratieprinzip zuwiderlaufende Beeinflussung [illegible]Wahlen, Lock-in und systematische Schädi[illegible]rauchern sowie viele Formen des Handels [illegible]ezogenen Daten.

Diverse Regelungen und Maßnahmen in neueren EU-Rechtsakten

Sowohl das Datenschutzrecht als auch die übrige Rechtsordnung (u. a. Zivilrecht, Lauterkeitsrecht) enthalten bereits eine Fülle von Instrumenten, die gegen derartige Datennutzungen eingesetzt werden können. Gemessen an Breitenwirkung und Schädigungspotenzial werden diese Instrumente indessen bislang nicht in ausreichender Weise genutzt – insbesondere gegenüber marktmächtigen Unternehmen. Dieses **Vollzugsdefizit** hat verschiedene Ursachen, die es systematisch anzugehen gilt.

3

Neben der Schärfung des Bewusstseins bei handelnden Akteuren (z. B. Aufsichtsbehörden) für die bereits bestehenden Möglichkeiten ist dringend eine **Konkre[illegible]isierung und punktuelle Verschärfung des geltenden [illegible]rahmens** angezeigt. Dazu gehören etwa eine spezi[illegible]nierung von datenspezifischen Klauselverboten, [illegible]nd Treuepflichten, Deliktstatbeständen und [illegible]n Geschäftspraktiken sowie die Schaffung eines [illegible]s konkreteren Rechtsrahmens für Profilbildungen [illegible]d Scoring wie auch für den Datenhandel.

Nicht gelöst: Rechtsordnung allgemein „datenfit“ machen

4

Um die Wirkungskraft der Aufsichtsbehörden zu erhöhen, bedürfen diese einer weitaus besseren personellen und sachlichen Ausstattung. Sofern es nicht gelingt, die Abstimmung unter den deutschen Datenschutzaufsichtsbehörden zu verstärken und zu formalisieren und so die einheitliche und kohärente Anwendung des Datenschu[illegible]rechts zu gewährleisten, ist eine **Zentralisierung der Datenschutzaufsicht für den Markt** in einer – mit einem weiten Mandat ausgestatteten und eng mit anderen Fachaufsichtsbehörden kooperierenden – Behörde auf Bundesebene zu erwägen. Die Zuständigkeit der Landesdatenschutzbehörden für den öffentlichen Bereich soll hingegen unangetastet bleiben.

Datenstrategie BReg

5

Die Anerkennung von **„Dateneigentum“** im Sinne eines dem Sacheigentum oder dem geistigen Eigentum nachgebildeten Ausschließlichkeitsrechts an Daten würde nach Auffassung der DEK bestehende Probleme nicht lösen und stattdessen eine Reihe neuer Probleme schaffen. Sie wird daher **nicht empfohlen**. Die DEK empfiehlt auch nicht die Anerkennung gener[illegible] schaftlicher Verwertungsrechte an per[illegible] Daten, wie sie etwa durch Verwertu[illegible] geltend gemacht werden könnten.

Daten-VO

6

Wenngleich die plakative Bezeichnung zur allgemeinen Bewusstseinsbildung beigetragen hat, plädiert die DEK dafür, **von der Bezeichnung von Daten als „Gegenleistung“ abzusehen**. Unabhängig von der künftigen Auslegung des sog. Koppelungsverbots durch die Aufsichtsbehörden und den EuGH fordert die DEK, dass Verbrauchern jeweils **zumutbare Alternativen** gegenüber der Freigabe von Daten zur auch kommerziellen Nutzung angeboten werden müssen (z. B. entsprechend ausgestaltete **Bezahlmodelle**).

daten ethik kommission

Nicht gelöst: Personalisierte Risikoeinschätzung udgl

Nicht gelöst: Digitaler Nachlass

Ankündigung Beschäftigten-Datenschutz

ePA, Europäischer Gesundheits-datenraum u.a.

BIK+ und ähnliche Initiativen

Nicht gelöst: Datenschutzfreund-liches Design

Daten-Verordnung

7

Die Verwendung von Daten zur **personalisierten Risiko-einschätzung** (z. B. im Rahmen von Telematiktarifen bei bestimmten Versicherungen) sollte an **enge Voraussetzungen** geknüpft werden. So darf die Datenverarbeitung beispielsweise nicht den Kern privater Lebensführung betreffen, es muss ein klarer ursächlicher Zusammenhang zwischen Daten und Risiko vorliegen, und die Preis-zwischen personalisiertem und nicht persona-llte im Einzelnen noch festzulegende t überschreiten. Weitere Anforderun-parenz, Nichtdiskriminierung und den sonen.

8

Die DEK empfiehlt der Bundesregierung, Fragen rund um den **„digitalen Nachlass"** mit dem Urteil des BGH von 2018 nicht als erledigt anzusehen. Die praktisch lückenlose Aufzeichnung von digital geführter Kommu-nikation, die in vielen Fällen an die Stelle des flüchtig gesprochenen Wortes tritt, und ihre Aushändigung an ben bedeutet eine neue Dimension von Gefährdung für ivatheit. Ihr sollte mit einer Reihe von Maßnahmen et werden, welche neue Pflichten von Dienste-ern, Qualitätssicherung bei Angeboten digitaler nlassplanung sowie nationale Regelungen zum post-mortalen Datenschutz umfassen.

9

Die DEK empfiehlt der Bundesregierung, die Sozialpartner einzuladen, ausgehend von den bereits in Tarifverträgen bestehenden Beispielen guter Übung eine gemeinsame e für gesetzliche Konkretisierungen des **Beschäftig-atenschutzes** zu entwickeln. Dabei sollten auch die ange von Personen in unüblichen Beschäftigungsfor-men berücksichtigt werden.

10

Mit Blick auf die Vorteile eines **digitalisierten Gesund-heitswesens** spricht sich die DEK für einen raschen Ausbau digitaler Infrastrukturen innerhalb des Ge-sundheitssektors aus. Der qualitative und quantitative Ausbau digitalisierter V die informationell Hierzu ge elektron wicklung gitaler Ge Gesundheitsi

11

Die DEK fordert, dem erheblichen Vollzugsdefizit des gel-tenden Rechts betreffend den **Schutz von Kindern und Jugendlichen** im digitalen Raum abzuhelfen. Insbeson-dere sollten Technologien – einschließlich eines effekti-ven Identitätenmanagements – sowie Standardoptionen entwickelt und verpflichtend vorgesehen werden, welche einen zuverlässigen Schutz der Kinder und Jugendlichen gewährleisten und zugleich familienadäquat sind, indem sie Erziehungsb noch eine übermä ög-liche

12

Was den Umgang mit Daten **pflege- und schutzbedürf-tiger Menschen** betrifft, sollte für professionelle Akteure im Pflegebereich durch Standards und Leitlinien mehr Rechtssicherheit geschaffen werden. Zugleich ist eine gesetzliche Klarstellung zu erwägen, dass – soweit eine Datenverarbeitung auf die Einwilligung des pflege- und schutzbedürftigen Menschen gestützt werden muss – in Patientenverfügungen auch bestimmte Dispositionen in Bezug auf die Datenverarbeitung (z. B. für den Fall der dauernden Einwilligungsunfähigkeit infolge von Demenz) getroffen werden können.

13

Die DEK empfiehlt, eine Reihe verbindlicher Vorgaben für **datenschutzfreundliches Design von Produkten und Dienstleistungen** einzuführen und damit die an Ver-antwortliche im Sinne der DSGVO gerichteten Vorgaben von Datenschutz „by design" und „by default" bereits auf der Ebene der Hersteller wie auch der Diensteanbieter wirksam werden zu lassen. Dies betrifft insbesondere Vorgaben für Verbraucherendgeräte. In diesem menhang sind auch einheitliche Bild me) einzuführen, die dem Verb Kaufentscheidung ermöglich

14

Ferner bedarf es einer Reihe weiter verschiedenen Ebenen, um für Hersteller ei **ze zur Implementierung eines datenschutzfreundlichen Designs** zu schaffen. Neben wirksamen Rechtsbehelfen entlang der Vertriebskette, mit deren Hilfe Hersteller mit in die Verantwortung für unzureichenden Datenschutz „by design" und „by default" genommen werden können, ist insbesondere an Vorgaben in Ausschreibungsbedin-gungen und Beschaffungsrichtlinien für die öffentliche Hand sowie an Bedingungen bei Förderprogrammen zu denken. Das Gleiche gilt für datenschutzfreundliche **Methoden der Produktentwicklung**, einschließlich des Trainierens algorithmischer Systeme.

15

Trotz des berechtigten Fokus auf Datenschutz natürlicher Personen darf der **Schutzbedarf von Unternehmen und juristischen Personen** nicht in den Hintergrund treten. Durch die umfassende Verknüpfbarkeit von Einzeldaten kann ein lückenloses Bild interner Betriebsabläufe hen und in die Hände von Konkurrenten, V partnern, Übernahmeinteressenten usw stellt aufgrund umfangreicher Datenflü u. a. eine Gefährdung der digitalen Souv lands und Europas dar. Viele Handlungsemp sind daher sinngemäß auch auf die Daten juristisch Personen zu übertragen. Die DEK fordert die Bundes-regierung auf, Schritte zu unternehmen, um den **daten-bezogenen Schutz von Unternehmen zu verbessern.**

daten
ethik
kommission

Verbesserung des kontrollierten Zugangs zu personenbezogenen Daten

daten ethik kommission

Verbesserung des kontrollierten Zugangs zu personenbezogenen Daten

16

Die DEK sieht in einer Datennutzung für gemeinwohlorientierte Forschungszwecke (z. B. zur Verbesserung [...]esundheitsfürsorge) enormes Potenzial, das es zum [...]inzelnen und der Allgemeinheit zu nutzen [...] Datenschutzrecht erkennt dieses Po[...]ihe weitreichender Privilegierungen [...]gs bestehen auch Unsicherheiten, [...]ck auf die Reichweite des sog. Wei[...]rivilegs sowie des Forschungsbegriffs [...]nhang mit der Entwicklung von Produkten. [...] muss aus Sicht der DEK durch entsprechende **gesetzliche Klarstellungen** begegnet werden.

17

Die Zersplitterung der Rechtslage, sowohl innerhalb Deutschlands als auch der EU Mitgliedstaaten untereinander, kann ein Hindernis für datengetriebene For[...]bung darstellen. Empfohlen wird daher eine **Harmoni[...]r forschungsspezifischen Regelungen** sowohl [...]nd Landesebene als auch der verschiede[...] Regelungen innerhalb der EU. Auch die [...]s Notifizierungsverfahrens für mitglied[...]elungen zum Forschungsdatenschutz [...]inrichtung einer europäischen Clearing-Stelle [...]grenzüberschreitende Forschungsprojekte könnte eine Erleichterung bringen.

18

Bei Forschung mit besonders sensiblen [...]sonenbezogener Daten (z. B. Gesund[...] Forschende durch **Handreichungen** [...]holung von Einwilligungen sowie d[...] gesetzliche **Anerkennung innovativ**[...] unterstützt werden. Zusätzlich zu den [...]gen zur Reichweite des sog. Weiterverarb[...] für die Forschung könnten dazu auch digitale Ein[...] assistenten oder ein sog. Meta Consent gehören.

[...]ie Entwicklung in Rich[...]**tssystems**", in dem [...]undheitsversorgung [...]tzt im Sinne der evidenz[...] werden, um die Versorgung [...]kontinuierlich zu verbessern. Allerdings sollte flankierend, beispielsweise durch **Verwertungsverbote**, mehr Schutz vor dem erheblichen Diskriminierungspotenzial sensibler Datenkategorien geschaffen werden.

20

Im Zentrum aller Bemühungen um eine Verbesserung des kontrollierten Zugangs zu (ursprünglich) personenbezogenen Daten steht die Entwicklung von Verfahren und Standards der **Anonymisierung** und **Pseudonymisierung**. Durch rechtliche Vermutungen, dass bei Einhaltung des Standards kein Personenbezug mehr gegeben ist bzw. dass „geeignete Garantien" für die Rechte betroffener Personen vorliegen, könnte die Rechtssicherheit deutlich verbessert werden. Diese Maßnahmen sollten flankiert werden durch strafbewehrte Verbote einer De-Anonymisierung (für den Fall, dass bei bisher anonymen Daten, etwa durch die Entwicklung der Technik, ein Personenbezug hergestellt werden kann) bzw. der Aufhebung der Pseudonymisierung jenseits eng definierter Rechtfertigungsgründe. Auch die Forschung im Bereich **synthetischer Daten** ist vielversprechend und sollte weiter gefördert werden.

21

Großes Potenzial sieht die DEK grundsätzlich auch [...]**n Datenmanagement- und Datentreu[...]**diese praxisgerecht, robust und [...]ltet sind. Solche Modelle [...]ashboards (**Privacy** [...]u umfassenden [...]inwilligungsver[...]**nagement Services,** [...]Einzelnen zur Kontrolle [...]en Daten sowie die Entlas[...]n Entscheidungen, die ihn über[...]. Die DEK empfiehlt, Forschung und Entwicklung im Bereich von Datenmanagement- und Datentr[...]handsystemen intensiv zu fördern, mahnt [...] dass eine die Rechte und Interessen [...] wahrende Entwicklung ohne eine **h[...]ische Regulierung** nicht zu erwar[...]rung müsste zentrale Funktionen [...] Betreiber solcher Systeme nur seh[...] werden können. Andererseits geht e[...] Einzelnen vor vermeintlichen Interessen[...] Wahrheit vorrangig wirtschaftliche Eigeninter[...] Interessen Dritter vertreten. Sofern dieser Schutz auch in der Praxis garantiert werden kann, kann Datentreuhandmodellen die Funktion einer wichtigen Schnittstelle zwischen Belangen des Datenschutzes und der Datenwirtschaft zukommen.

22

In Bezug auf das Recht auf **Datenportabilität** aus Art. 20 DSGVO empfiehlt die DEK die Erarbeitung bra[...] bezogener Verhaltensregeln und Stan[...] Datenformate. Soweit Art. 20 DS[...] terwechsel erleichtern, sond[...] für andere Anbieter verbes[...] eine sorgfältige Evaluieru[...] Portabilitätsrecht auf den[...] zunehmende Stärkung der [...] ter verhindert werden kann. B[...] solchen Evaluierung vorliegen, so[...] len Erweiterung des Portabilitätsrechts, [...] als bereitgestellte Daten oder auf Portierung in Ec[...] abgesehen werden.

23

Eine **Pflicht zur Interoperabilität bzw. Interkonnektivität** in bestimmten S[...]t[...]n bei Messenger-Diensten [...] beitragen, M[...]en. Für [...] d. h[...] len. D[...]nte Basisdiens[...]t in Europa neu aufzubau[...]

Europäischer Gesundheitsdatenraum

Europäischer Gesundheitsdaten-raum

Daten-Governance-Rechtsakt etabliert anderes Modell von Datentreuhand als DEK

Daten-Verordnung u.a. weichen von Empfehlung zu behutsamem Vorgehen ab

Datenstrategie der BReg

Daten-Governance-Rechtsakt u begleitende Entwicklungen

Gesetz Digitale Märkte

daten
ethik
kommission

Datenzugangsdebatten jenseits des Personenbezugs

Datenzugangsdebatten jenseits des Personenbezugs

24

Für die Entwicklung der europäischen Datenwirtschaft sieht die DEK einen zentralen Faktor im Zugang europäischer …hmen zu geeigneten nicht-personenbezogenen …neter Qualität. **Datenzugang** nutzt allerdings …e ein entsprechendes Bewusstsein für …on Daten haben und über entsprechende …z verfügen, und in ganz überproportionalem …enigen, bei denen bereits der größte Ausgangs… an Daten und die besten Dateninfrastrukturen vorhanden sind. Die DEK empfiehlt daher, bei der Diskussion um eine Verbesserung des Datenzugangs stets die genannten Faktoren gemäß dem **ASISA-Prinzip** *(Awareness – Skills – Infrastructures – Stocks – Access)* mit zu berücksichtigen.

25

…tützt die DEK die bereits auf europäischer …n Maßnahmen zur Förderung von …**en** im weitesten Sinne (z. B. Platt… …r Programmierschnittstellen und …Modellverträge, EU-Unterstützungs… …empfiehlt der Bundesre… …durch entsprechende … Ebene zu flankieren. In d… sich die Einrichtung eine… an, welche bei Aushandlu… rungen und bei Streitigkeiten …

26

Die DEK sieht einen Schlüsselfaktor in einer holistisch gedach…igen und strategischen **Wirtschaftspolitik**, wel… …ng innovativer europäischer Unternehmen …durch Akteure aus Drittstaaten ebenso …kt wie der übermäßigen Abhängigkeit von …(z. B. Serverkapazitäten) in Drittstaaten. Dabei …chtige Balance zu finden zwischen gewollter inter… nationaler Kooperation und Vernetzung einerseits und ande… rerseits der entschlossenen Übernahme von Verantwortung für nachhaltige Sicherheit und Wohlfahrt in Europa vor dem Hintergrund sich wandelnder globaler Machtverhältnisse.

27

Die DEK sieht auch unter dem Blickwinkel einer Förde… rung der Datenwirtschaft keinen Bedarf nach der Einfüh… rung neuer Ausschließlichkeitsrechte („Dateneigentum", „Datenerzeugerrecht"), sondern empfiehlt stattdessen eine **beschränkte Drittwirkung vertraglicher Vereinbarungen** (z. B. betreffend Beschränk… …Weiter… gabe von Daten) p… Regimes zum … wäre es wün… würden, wie e… Einschaltung von … tellrechtlicher Belange bei d… …eren können („**Datenpartnerschaften**").

28

In bestehenden Wertschöpf… tions- und Vertrieb… innerhalb wie a… enormer wirts… den einzelnen … bestehenden Vertrag… keine bzw. eine unfaire und/oder … …ung des Datenzugangs, oder es fehlt ganz an einer vertraglichen Vereinbarung. Weit über die klassische „Datenwirtschaft" …aus ist daher **Bewusstseinsbildung bei Wirtschaftstrei…** …derlich, die durch praktische Hilfestellungen …äge) ergänzt werden sollte.

Darüber hinaus regt die DEK eine **behutsame Ergänzung des geltenden Rechtsrahmens** an. Dabei sollte ein erster Schritt darin liegen, die Sonderbeziehung zwischen einer Partei, welche zur Generierung von Daten in einem Wertschöpfungssystem beigetragen hat, und der Partei, welche die Daten faktisch kontrolliert, in § 311 BGB explizit anzuführen. Unter anderem sollte die Aufnahme von Ver… über ein faires und effizientes D… teil einer solchen allgemeine… sollte geprüft werden, ob da… forderlich sind, welche von pur… B2B-Geschäften über ein dispositives D… sektorspezifischen Datenzugangsrechten rangieren könnten.

30

Die DEK sieht großes Potenzial in **Konzepten offener Daten des öffentlichen Sektors** (Open Government Data, OGD) und empfiehlt, solche Konzepte auszubauen und zu fördern. Sie empfiehlt eine Reihe von Maßnahmen, die einen teilweise noch nicht ganz vollzogenen **Bewusstseinswandel öffentlicher Stellen** befördern und das T… len von Daten im Rahmen von OGD-Konzepten pr… erleichtern könnten. Dazu gehört neben der Eta… entsprechender **Infrastrukturen** (z. B. Plattfor… eine Harmonisierung und punktuelle Ergänzu… zeit zersplitterten und nicht in jeder Hinsicht k… ten **Rechtsrahmens**.

31

Allerdings sieht die DEK auch ein schwer zu lösendes Spannungsverhältnis zwischen der Diskussion um OGD …mit Prinzipien wie „offen by default" und „offen für …le Zwecke") einerseits und um besseren Schutz von Geschäftsgeheimnissen und personenbezogenen Daten (mit gesetzlichen Vorgaben wie „Datenschutz by default") andererseits. Sie plädiert dafür, in Zweifelsfällen zugunsten des staatlichen Schutzauftrags zu entscheiden, der in Bezug auf Daten, welche Einzelne oder Unternehmen dem Staat – oft nicht freiwillig – anvertraut haben (z. B. Steuerdaten), besteht. Di… …zauftrag ist durch eine … die auch t… gegen M…

32

In diesem Zusammenhang wird insbesondere empfohlen, für das Teilen von Daten durch den öffentlichen Sektor **Standardlizenzen und Modellkonditionen** zu entwickeln …– mindestens sektorspezifisch – deren Verwendung …zuschreiben. Diese sollten klar definierte …die Rechte betroffener Dritter enthalten. …ie Mechanismen vorsehen, die geeignet …einwohlschädigende Nutzung der Daten …zu verhindern wie eine wettbewerbsrechtlich unerwünschte Verstärkung bestehender Marktmacht oder eine Doppelbelastung des Steuerzahlers.

33

Betreffend **Konzepte offener Daten im privaten Sektor** sollte in erster Linie auf die **Ermutigung und Förderung eines freiwilligen Teilens** von Daten gesetzt werden. Dabei ist nicht … …rastrukturen (z. B. Plattformen) … mög… …

Insges… …gesetzlichen Datenzugangsrechten zu einem behutsamen Vorgehen, idealerweise **zunächst in ausgewählten Sektoren**. Beispielsweise könnte ein Bedarf im Nachrichten-, Mobilitäts- oder Energiesektor geprüft werden. Dabei sind jeweils alle möglichen Konsequenzen einer Zugangsgewährungs- oder gar Offenlegungspflicht sorgsam zu bedenken und gegeneinander abzuwägen, angefangen von möglichen Implikationen für den Datenschutz und Schutz von Geschäftsgeheimnissen, über Folgen für Investitionsentscheidungen und die Verteilung von Marktmacht bis hin zu den strategischen Interessen deutscher und europäischer Unternehmen im Verhältnis zu Unternehmen in Drittstaaten.

35

Die DEK empfiehlt, Zugangsgewährungspflichten privater Unternehmen **zugunsten gemeinwohlorientierter Zwecke und des öffentlichen Sektors** (Business-to-Government, B2G) in Erwägung zu ziehen. Auch diesbezüglich dürfte indessen ein behutsames … …anzuraten sein.

Europäische u nationale Datenstrategien

Europäische u nationale Datenräume

Gaia-X usw.

Nicht erfolgt: Anpassung Zivilrecht

Daten-Verordnung

Daten-Governance-Rechtsakt

Nicht erfolgt: Anpassung Zivilrecht

Daten-Verordnung u.a. weichen von Empfehlung zu behutsamem Vorgehen ab

Daten-Governance-Rechtsakt

Daten-Verordnung

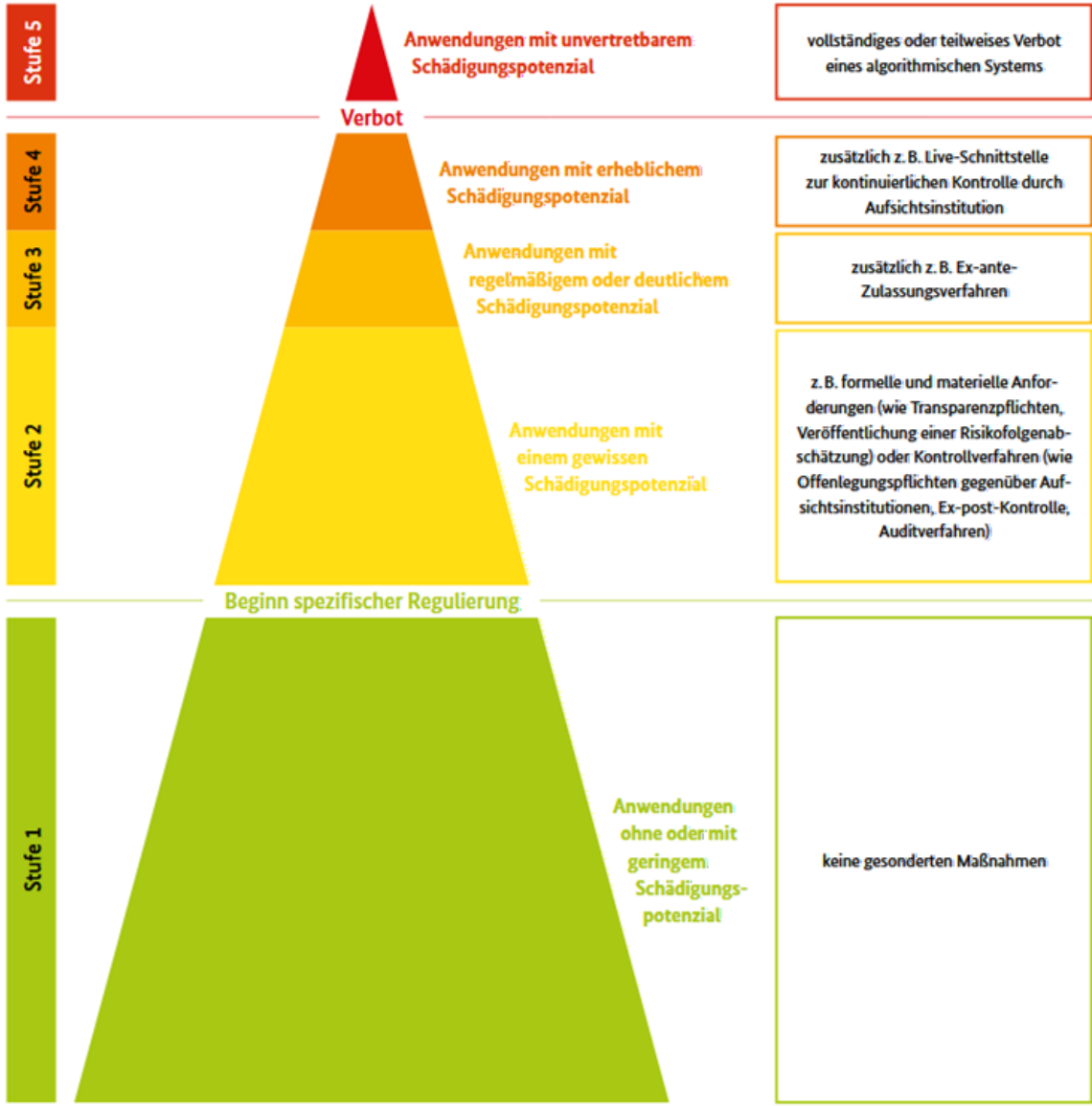
daten
ethik
kommission

Algorithmische Systeme

daten ethik kommission

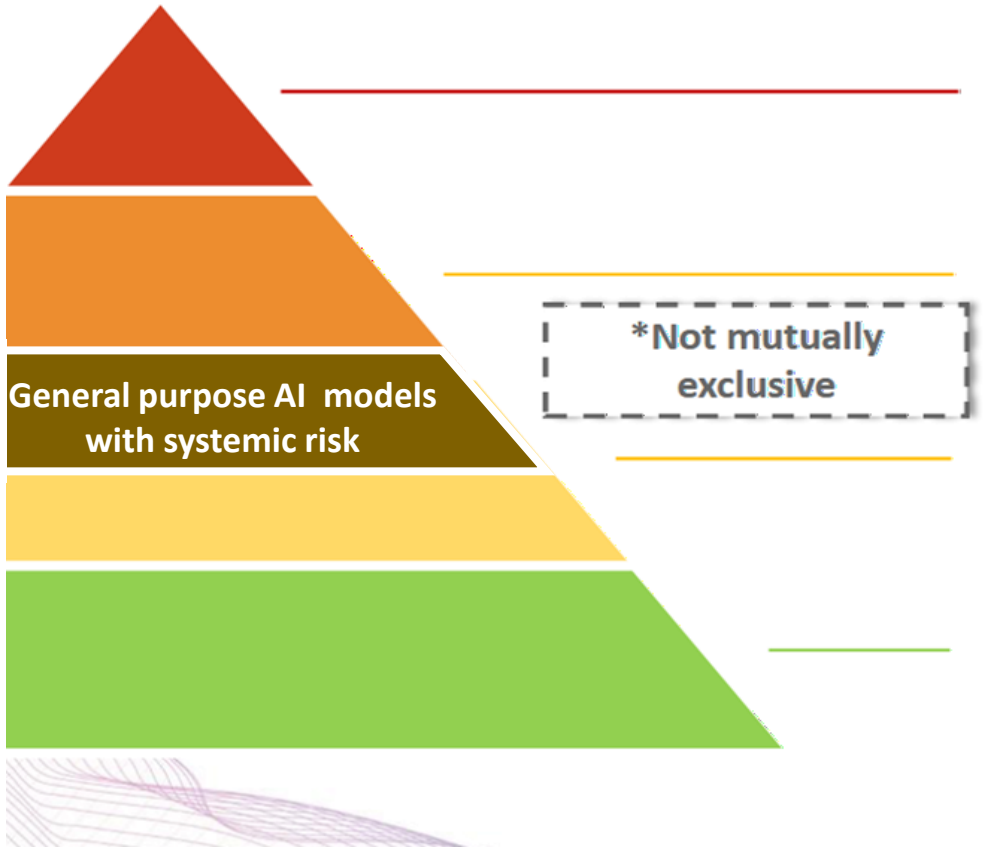
Empfehlung eines risikoadaptierten Regulierungsansatzes

- „Kritikalitätspyramide“: Bestimmung der **Systemkritikalität** aufgrund des Schädigungspotenzials
- Großer **„grüner Bereich“**
- (Überprüfbare) **Einordnung** in eine Kritikalitätsstufe anhand eines Kriterienkatalogs



daten ethik kommission

Risikobasierter Regulierungsansatz der KI-VO Und Visualisierung durch die Europäische Kommission



daten ethik kommission

Empfehlung eines risiko-adaptierten Regulierungsansatzes

36

Die DEK empfiehlt einen **risikoadaptierten Regulierungsansatz** für algorithmische Systeme. Er sollte auf dem Grundsatz aufbauen, dass ein steigendes Schädigungspotenzial mit wachsenden Anforderungen und Eingriffstiefen der regulatorischen Instrumente einhergeht. Für die Beurteilung kommt es jeweils auf das **gesamte sozio-technische System** an, also alle Komponenten einer algorithmischen Anwendung einschließlich aller menschlichen Akteure, von der Entwicklungsphase (z. B. hinsichtlich der verwendeten Trainingsdaten) bis hin zur Implementierung in einer Anwendungsumgebung und zur Phase von Bewertung und Korrektur.

37

Die DEK empfiehlt, die Bestimmung des Schädigungspotenzials algorithmischer Systeme für Einzelne und/oder die Gesellschaft anhand eines **übergreifenden Modells** einheitlich vorzunehmen. Dafür sollte
mit Hilfe von **Kriterien** ein Prüfschem
welchem die Kritikalität algorithmisch
Grundlage der von der DEK vorgestell
ethischen und rechtlichen Grundsätze
bestimmen ist.

38

Regulatorische Instrumente und **Ant**
algorithmische Systeme sollten u. a. K
Kontrollinstrumente, Vorgaben für die
Erklärbarkeit und die Nachvollziehbark
sowie Regelungen zur Zuordnung von V
und Haftung für den Einsatz umfassen

39

Die DEK erachtet es als sinnvoll, mit B
gungspotenzial algorithmischer Syste
Schritt **fünf Kritikalitäts-Stufen** zu un
der untersten Stufe (Stufe 1) von Anw
oder mit geringem Schädigungspoten
Notwendigkeit einer besonderen Kon
Anforderungen, die über die allgemein
derungen, welche auch für Produkte ol
Elemente gelten, hinausgehen.

40

Bei Anwendungen mit einem **gewisse**
potenzial (Stufe 2) kann und soll bed
Regulierung einsetzen, wie etwa Ex-p
die Pflicht zur Erstellung und Veröffen
angemessenen Risikofolgenabschätzu
pflichten gegenüber Aufsichtsinstituti
gesteigerte Transparenzpflichten sowie
für Betroffene.

41

Bei Anwendungen mit **regelmäßigem** oder **deutlichem Schädigungspotenzial** (Stufe 3) können zusätzlich Zulassungsverfahren gerechtfertigt sein. Bei Anwendungen mit

algorithmischer Systeme für den Einzelnen und für Gruppen auch dann manifestieren können, wenn keine personenbezogenen Daten verarbeitet werden, und dass die Risiken nicht unbedingt solche des Datenschutzes sind, wenn sie etwa das Vermögen, E
Integrität oder Diskriminierung bet
ist zu bedenken, dass für eine künft
lierung algorithmischer Systeme ei
risikoadaptiertes Regulierungsregim
schutz in Betracht gezogen werden

Instrumente

45

Die DEK empfiehlt bei algorithmisc
ter Systemkritikalität (ab Stufe 2) ei
pflicht: Eine solche Pflicht trägt Be
zu machen, wann und in wel
sche Systeme
das „Ob
gi

47

In bestimmten Bereichen kann es
dem Betreiber algorithmischer Syst
allgemeinen Erläuterung der Logik

und Tragweite des Systems eine **individuelle Erklärung** der getroffenen Entscheidung abzuverlangen. Wesentlich ist dabei, dass betroffene Personen verständlich, relevant und konkret informiert werden. Die DEK begrüßt

50

Die Anforderungen an **Dokumentation und Protokollierung** in Bezug auf die verwendeten Datensätze und Modelle, die Granularität, die Aufbewahrungszeiten und die Verwendungszwecke sollten konkretisiert werden, damit die Verantwortlichen und Auftragsverarbeiter Rechtsklarh
anderen sollte für sensible Anwendungen
etabliert werden, die Programmabläufe ei
nachhaltige Schäden verursachen können,
ren und zu protokollieren. Die verwendete
Modelle sind so zu beschreiben, dass diese
tutionen im Falle einer Kontrolle nachvollz
hinsichtlich der Herkunft und Aufbereitun
oder der Optimierungsziele der Modelle).

Beim Einsatz algorithmischer Systeme ir
menschlicher Entscheidungen sieht die
Klarstellungs- und Konkretisierungsbed
die Anwendungsvoraussetzungen und R
von Art. 22 DSGVO. Darüber hinaus emp
Schutzmechanismen auch für algorithm
-getriebene Entscheidungssysteme vor
der Einfluss dieser Systeme in der Praxis
stark auswirken kann wie bei algorithme
Anwendungen. Diesbezüglich empfiehlt
von Art. 22 DSGVO bislang verfolgten Ve
flexibleres, risikoadaptiertes Regulierung
Einzelnen angemessene Schutzgarantier
Falle von Profiling) und Verteidigungsmi
Fehler und Bedrohungen seiner Rechte

53

Es ist erwägenswert, den **Anwendungsbereich des Antidiskriminierungsrechts** in situativer Hinsicht auf Diskriminierungen auszudehnen, die auf einer automatisierten Datenauswertung oder einem automatisierten Ent-

56

Darüber hinaus empfiehlt die DEK der Bundesregierung die Schaffung eines **bundesweiten Kompetenzzentrums Algorithmische Systeme**, welches die sektoralen Aufsichtsbehörden durch technischen und regulatorischen Sachverstand in ihrer Aufgabe unterstützt, algorithmische Systeme im Hinblick auf die Einhaltung von Recht und Gesetz zu kontrollieren.

57

Aus Sicht der DEK sollten Initiativen unterstützt werden, die – ggf. differenziert nach kritischen Anwendungsbereichen – technisch-statistische **Standards für die Qualität von Testverfahren und Audits** festlegen. Für die Überprüfbarkeit algorithmischer Systeme können derartige Testverfahren künftig eine zentrale Rolle spielen, wenn sie hinreichend aussagekräftig, verlässlich und sicher ausgestaltet sind.

58

Innovative Formen der **Ko- und Selbstregulierung** verdienen aus Sicht der DEK neben und in Ergänzung zu staatlichen Formen der Regulierung besondere Aufmerksamkeit. Die DEK empfiehlt der Bundesregierung die Prüfung verschiedener Modelle der Ko- und Selbstregulierung, die für bestimmte Konstellationen adäquate Antworten liefern können.

59

Die DEK hält es für erwägenswert, den Betreibern – nach dem Regulierungsmodell „Comply or Explain" – die gesetzliche Pflicht aufzuerlegen, sich zu den Regeln eines **Algorithmic Accountability Codex** zu bekennen. Die Erarbeitung eines solchen bindenden Codex für die Betreiber von algorithmischen Systemen könnte dabei durch eine unabhängige, paritätisch besetzte Kommission erfolgen, die nicht unter staatlichem Einfluss stehen dürfte. Vertreter der Zivilgesellschaft sollten bei der Erarbeitung eines solches Codex in angemessener Weise beteiligt werden.

60

Auch ein spezifisches **Gütesiegel** als freiwilliges oder verpflichtendes Schutzzeichen kann Verbrauchern Orientierung über vertrauenswürdige algorithmische Systeme geben und gleichzeitig marktwirtschaftliche Anreize für Entwickler und Betreiber setzen, vertrauenswürdige Systeme zu entwickeln und zu verwenden.

61

Ähnlich wie schon heute Unternehmen ab einer bestimmten Größe einen Datenschutzbeauftragten benennen müssen, sollten nach Auffassung der DEK künftig auch solche Unternehmen und Behörden, die kritische algorithmische Systeme betreiben, einen **Ansprechpartner** benennen müssen. Er soll für die Kommunikation mit Behörden zur Verfügung stehen und zu einer Mitwirkung verpflichtet sein.

62

Um sicherzustellen, dass bei der behördlichen Überprüfung algorithmischer Systeme auch die Interessen der Zivilgesellschaft und betroffener Unternehmen angemessen berücksichtigt werden, sollten geeignete **Beiräte bei den sektoralen Aufsichtsbehörden** gebildet werden.

63

Die DEK stuft technische Standards **akkreditierter Normungsorganisationen** als ein grundsätzlich sinnvolles Instrument zwischen staatlicher Regulierung und rein privater Selbstregulierung an. Sie empfiehlt daher der Bundesregierung, in geeigneter Weise auf die Entwicklung und Verabschiedung technischer Standards hinzuwirken.

Entwurf KI-Verordnung

64

Die in Deutschland bewährten **Klagerechte von Wettbewerbern** und von **Wettbewerbs- und Verbraucherverbänden** sind ein zentraler Baustein für eine zivilgesellschaftliche Kontrolle des Einsatzes von algorithmischen [illegible] Besonders legitimierte zivilgesellschaftliche [illegible] solche privaten Klagerechte [illegible] orschriften im Bereich des [illegible] srechts oder des Antidis- [illegible] len, ohne hierbei auf das [illegible] der die Mandatierung durch [illegible] gewiesen zu sein.

Verbands-klagen-RL

Besonderes Augenmerk: Algorithmische Systeme bei Medienintermediären

65

Vor dem Hintergrund der besonderen Gefahren von Medienintermediären mit **Torwächterfunktion für die Demokratie** empfiehlt die DEK, auch mit Blick auf eine Einwirkung auf den EU-Gesetzgeber (→ siehe oben Empfehlung Nr. 43) zu prüfen, wie den mit einer solchen Torwächterfunktion verbund[illegible] begegnet werden kann. [illegible] nabwehr- [illegible] einer [illegible] rechtliche Pflicht, die [illegible] erfahren für die freie demokratische und plurale Meinungsbildung, die von Anbietern mit Torwächterfunktion ausgehen, durch **Etablierung einer positiven Medienordnung** zu schützen. Die DEK empfiehlt, die Anbieter in diesem engen Bereich zum Einsatz solcher algorithmischer Systeme zu verpflichten, die den Nutzern zumindest als zusätzliches Angebot auch einen Zugriff auf eine tendenzfreie, ausgewogene und die plurale Meinungsvielfalt abbildende Zusammenstellung von Beiträgen und Informationen verschaffen.

Gesetz Digitale Dienste

67

Für alle [illegible] Torwä[illegible] poten[illegible] Bunde[illegible] tischen Ge[illegible] könnte Mechanis[illegible] (z.B. Einblick in technische Verfahren der Nachrichtenauswahl und -priorisierung, **Kennzeichnungspflichten für Social Bots**) und ein Recht auf Gegendarstellung in Timelines umfassen.

Gesetz Digitale Dienste

Der Einsatz von algorithmischen Systemen durch staatliche Stellen

68

Der Staat ist im Interesse seiner Bürger zur Nutzung der besten verfügbaren Technik – einschließlich algorithmischer Systeme – verpflichtet, muss dabei jedoch im Lichte seiner Grundrechtsbindung sowie der Vorbildfunktion allen staatlichen Handelns besondere Sorgfalt walten lassen. Der Einsatz algorithmischer Systeme durch Hoheitsträger ist daher **im Allgemeinen** [illegible] **des Kritikalitätsm**[illegible] destens eine u[illegible]

Diverse nationale Maßnahmen

69

Aufgaben in der **Rechts**[illegible] dürfen algorithmischen Systemen allenfalls in Randbereichen übertragen werden. Insbesondere dürfen algorithmische Systeme nicht genutzt werden, um die freie Willensbildung im demokratischen Prozess und die sachliche Unabhängigkeit der Gerichte zu unterminieren. Große Potenziale für den Einsatz algorithmischer Systeme bestehen hingegen in der **Verwaltung**, vor allem in der Leistungsverwaltung. Um dem Rechnung zu tragen, sollte der Gesetzgeber verstärkt teil- und vollautomatisierte Verwaltungsverfahren zulassen. Dazu bedarf es auch einer vorsichtigen Fortentwicklung des zu engen § 35a VwVfG sowie der entsprechenden einfachrechtlichen Normen. Bei alledem gilt es, hinreichende Schutzmaßnahmen für die Bürger vorzusehen.

70

Staatliche Entscheidungen, die unter Nutzung algorithmischer Systeme zustande kommen, müssen **transparent und begründbar** bleiben. Dazu bedarf es ggf. Klarstellungen bzw. Erweiterungen der bestehenden Informationsfreiheits- und Transparenzgesetze. Ferner entbindet der Einsatz algorithmischer Systeme nicht vom Grundsatz, dass hoheitliche Entscheidungen regelmäßig im Einzelfall begründet werden müssen; im Gegenteil kann dieser Grundsatz dem Einsatz allzu komplexer algorithmischer Systeme G[illegible] Schließlich trägt die Nutzung von O[illegible] wesentlich zur Transparenz staat[illegible] sollte daher verstärkt angestreb[illegible]

Nicht gelöst: Zurechnung von KI

71

Zwar ist aus ethischer Sicht ein generelles Recht auf Freiheit zur Nichtbefolgung von Normen nicht anzuerkennen. Gleichzeitig wirft ein automatisierter Totalvollzug des Rechts eine Reihe ethischer Bedenken auf. Daher ist regelmäßig ein technisches Design zu fordern, bei dem der Mensch im Einzelfall den **technischen Vollzug** außer Kraft setzen kann. Ferner muss stets die Verhältnismäßigkeit zwischen der potenziellen Normübertretung und der automatisierten (ggf. präventiven) Vollzugsmaßnahme gewahrt sein.

Haftung für algorithmische Systeme

72

Neben strafrechtliche[illegible] tungssanktionen ist au[illegible] unverzichtbarer Bestand[illegible] Ordnungsrahmens. Es ist bere[illegible] algorithmische Systeme – u.a. aufgrund der Komplexität und Dynamik der Systeme sowie aufgrund ihrer wachsenden „Autonomie" – das bestehende Haftungsrecht vor Herausforderungen stellen. Die DEK empfiehlt daher eine umfassende Prüfung und, soweit erforderlich, **Anpassung des geltenden Haftungsrechts**. Der Blick sollte sich dabei nicht allein auf bestimmte technologische Merkmale – wie etwa auf das Merkmal Maschinellen Lernens oder Künstlicher Intelligenz – verengen.

Neue ProdHaft-RL

73

Der Gedanke, algorithmischen Systemen hoher Autonomie künftig Rechtspersönlichkeit zuzuerkennen und sie selbst für Schäden haften zu lassen („**elektronische Person**"), sollte **nicht weiterverfolgt** werden. Soweit dieser Gedanke auf eine Analogie zwischen Mensch und Maschine gestützt wird, ist er schon ethisch nicht vertretbar, und soweit es schlicht um die Anerkennung einer neuen Gesellschaftsform im Sinne des Gesellschaftsrechts geht, [illegible] eine Probleme.

[illegible] oten, für den Einsatz sog. autonomer [illegible] ngig von der Natur der dem System über- [illegible] Aufgaben – auch eine Zurechnung schädigender Vorgänge entsprechend den Regelungen über die Haftung für **Gehilfen** (vgl. insbes. § 278 BGB) vorzunehmen. Beispielsweise sollte eine Bank, die sich für die Prüfung der Kreditwürdigkeit eines autonomen Systems bedient, gegenüber ihrem Kunden mindestens in gleichem Maße haften, wie wenn sie sich eines menschlichen Mitarbeiters bedient hätte.

75

Daneben erscheint es nach derzeitigem Stand der Diskussion sehr wahrscheinlich, dass zusätzlich zu einer sachgerechten Anpassung der aus den 1980er Jahren stammenden **Produkthaftungsrichtlinie** und Verknüp- [illegible] mit neuen Standards der Produktsicherheit auch [illegible] le Modifikationen der **Verschuldenshaftung** [illegible] neue Tatbestände der **Gefährdungshaftung** [illegible] ch sein werden. Dabei wird jeweils zu klären [illegible] welche Produkte, digitalen Inhalte und digitalen Dienstleistungen welches Haftungsregime sachgerecht und wie dieses konkret auszugestalten ist, wobei es wiederum wesentlich u.a. auf die Kritikalität des betreffenden algorithmi[illegible] wird. Dabei sollten auch [illegible] zeit auf eur[illegible] gezog[illegible]

Entwurf KI-Haftungs-RL

Resümee

- Die DEK kann mit der Umsetzung ihrer Empfehlungen generell zufrieden sein – die überwältigende **Mehrzahl der Empfehlungen ist in der einen oder anderen Form adressiert** worden.
- Allerdings fällt auf, dass die Umsetzung **weitgehend durch den EU-Gesetzgeber** erfolgt ist – national ist Bewegung fast nur dort zu verzeichnen, wo erheblicher Druck von Interessenvertretungen besteht.
- Sowohl betreffend Daten (Rechte an co-generierten Daten, Datenintermediäre) als auch betreffend algorithmische Systeme (Kritikalitätspyramide, risikobasierter Regulierungsansatz) hat sich der EU-Gesetzgeber **an den theoretischen Konzepten der DEK** orientiert
- Wo Lösungen am Ende eines **demokratischen Willensbildungsprozesses** teilweise von Empfehlungen abweichen, ist dies prinzipiell zu akzeptieren.

Lohnt sich ein Update?

- So gut wie alle Empfehlungen sind mittlerweile **durch neuere Entwicklungen überholt** und müssten entweder als „erledigt“ markiert oder jedenfalls in der Formulierung erheblich angepasst werden.
- Flächendeckende Behandlung derselben Digitalisierungsthemen nicht mehr erforderlich, eher **punktuelle Bearbeitung von Schwerpunktthemen** aus der „Vogelperspektive“ wie z.B.:
  - Digitalisierung, Demokratie und gesellschaftlicher Zusammenhalt
  - Der „europäische Weg“ im globalen Kontext
  - …
- Letztlich ginge es um einen weitgehend neuen Arbeitsauftrag, der auch eine **teilweise neue personelle Besetzung** mit **zusätzlicher Expertise** erfordern würde (v.a. aus verschiedenen Sozialwissenschaften).

Vielen Dank für Ihre Aufmerksamkeit!