NomosHANDBUCH

Geminn | Johannes [Hrsg.]

Europäisches Datenrecht

DA | DGA | DS-GVO | DMA | DSA | KI-VO

Helbing Lichtenhahn

Nomos

Nomos **HANDBUCH**

Dr. Christian L. Geminn
Paul C. Johannes [Hrsg.]

Europäisches Datenrecht

DA | DGA | DS-GVO | DMA | DSA | KI-VO

Praxishandbuch

Dr. André Artelt, Universität Bielefeld | **Dr. Tamer Bile**, LL.M., Kassel | **Fabiola Böning**, Universität Kassel | **Dr. Ernestine Dickhaut**, Universität Kassel | **Prof. Dr. Kai Erenli**, LL.M. (it-law) (Wien), Fachhochschule des BFI Wien | PD **Dr. Christian Geminn**, Mag. iur., Universität Kassel | RA **Dominik Hoidn**, Frankfurt am Main | **Tom Hubert**, Universität Göttingen | **Johannes Jänicke**, Berlin | RA **Paul C. Johannes**, LL.M., Universität Kassel | **Dr. Murat Karaboga**, Fraunhofer-Institut für System- und Innovationsforschung ISI, Karlsruhe | RAin **Dr. Johanna M. Kirschnick**, LL.M. (KCL), Berlin | **Marcel Kohpeiß**, LL.M. (Glasgow), Universität Mainz | **Prof. Dr. Steffen Kroschwald**, LL.M., Hochschule Pforzheim | **Dr. Mahei Manhai Li**, Universität Kassel | **Prof. Dr. Jan Marco Leimeister**, Universität Kassel | **Luisa Lorenz**, LL.M., Universität Kassel | **Dr. Yannic Meier**, Universität Duisburg-Essen, Duisburg | RA **Jan-Philipp Muttach**, Frankfurt am Main | StA **Dr. Johannes K. M. Müller**, MLE., Mühlhausen/Thüringen | **Dr. Maxi Nebel**, Ass. iur., Universität Kassel | **Lars Pfeiffer**, LL.M., Universität Kassel | **Philipp Reinhard**, Universität Kassel | **Fabian Schaller**, Datenschutzbeauftragter, Kassel | **Till Schaller**, Universität Kassel | VorsRiVG i.R. **Hans-Hermann Schild**, Universität Kassel | **Dr. Stephan Schindler**, Universität Kassel | **Sabrina Schomberg**, Hessisches Ministerium des Inneren, für Sicherheit und Heimatschutz, Wiesbaden/Kassel | **Philip Schütz**, Datenschutzkoordinator Mercedes-Benz/Universität Göttingen, Stuttgart | **Linda Seyda**, Universität Kassel | SyndikusRA **Benjamin Stach**, LL.M. (KCL), Hamburg | RA **Robert Weinhold**, Düsseldorf | **Dr. Julia Zirfas**, LL.M., Kaden | **Paul Zurawski**, Universität Kassel

Helbing Lichtenhahn

Nomos

Zitiervorschlag: EU-DatenR-HdB/Autor § ... Rn. ...

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.d-nb.de abrufbar.

ISBN 978-3-8487-7404-3 (Nomos Verlagsgesellschaft mbH & Co. KG, Baden-Baden)

ISBN 978-3-7190-4664-4 (Helbing Lichtenhahn Verlag, Basel)

1. Auflage 2026

Vorwort der Herausgeber

Die zwanziger Jahre des 21. Jahrhunderts sollen für die Europäische Union ein digitales Jahrzehnt sein, eine Dekade der Daten. Dieses digitale Jahrzehnt und die digitale Zukunft Europas werden durch ein neues Rechtsgebiet gerahmt, das digitale Daten, aber auch digitale Dienste, digitale Märkte und künstliche Intelligenz zum Gegenstand hat – das europäische Datenrecht. Die Benennung des Rechtsgebiets erkennt an, dass die Wertschöpfung aus Daten (personenbezogen wie nicht personenbezogen) letztlich im Zentrum der Digitalisierung steht.

Daten wurden in einer (schiefen) Analogie als Rohstoff der Digitalisierung, als „neues Öl" bezeichnet – eine Analogie, die wohl einerseits auf der (weitgehenden) Verdrängung von Ölkonzernen von der Spitze der Liste der Unternehmen mit dem höchsten Marktwert durch die heutigen Digitalisierungsgiganten beruht und andererseits auf die gesamtgesellschaftliche Bedeutung von Daten verweist. Die digitale Marktwirtschaft wurde bisher trotz gegenläufiger Bemühungen von außerhalb Europas determiniert – eben durch die genannten Digitalisierungsgiganten und hier allen voran die U.S.-amerikanischen Unternehmen Microsoft, Apple, Amazon, Alphabet und Meta Platforms. Das europäische Datenrecht soll der Grundstein einer Wende sein, im Zuge derer Europa eine „digitale Souveränität" gewinnt, die bislang schmerzlich vermisst wurde.

Das europäische Datenrecht ist innovativ. Der Verordnungsgeber reguliert Bereiche, in denen anderswo bislang bestenfalls Soft Law besteht oder vereinzelt mitgliedsstaatliche Vorstöße gemacht wurden. Insbesondere mit der KI-Verordnung hat die Europäische Kommission Neuland betreten. Damit kann das Datenrecht letztlich zumindest in Teilen auch als ein legislatives Experiment charakterisiert werden, dessen Ausgang ungewiss bleibt. Offen ist der Ausgang dabei sowohl bezogen auf das Ziel einer Stärkung des Grundfreiheiten- und Grundrechtsschutzes im digitalen Raum als auch bezogen auf die intendierten wirtschaftsfördernden Effekte. Stellt das Datenrecht selbst in einzelnen Bestandteilen aber auch in seiner Gesamtheit eine Innovation dar, so soll es auch digitale Innovationen rund um die Verarbeitung von Daten fördern. Für die Entstehung neuer, innovativer Geschäftsmodelle und für innovativen Grundrechtsschutz soll ein Rahmen gegeben werden, wobei stets auch die Gefahr besteht, dass die Regulierung in das Gegenteil umschlägt und zu Zurückhaltung führt, die Innovationen behindert oder gar nicht erst entstehen lässt.

Das europäische Datenrecht ist allumfassend. Sein Anspruch besteht insgesamt darin, die Verarbeitung von Daten in allen denkbaren Kontexten und über die gesamte „Lebensspanne" eines Datums zu regulieren. Zudem werden die auf digitale Daten angewiesenen digitalen Dienste und digitalen Märkte reguliert. Regelungen unterworfen wird ferner auch die für eine Datenökonomie und eGovernment erforderliche Infrastruktur.

Das europäische Datenrecht ist hochkomplex und miteinander verwoben. Eine Vielzahl unmittelbar geltender Verordnungen schaffen im Zusammenspiel mit vielen weiteren Rechtsakten ein Dickicht an datenregulatorischen Anforderungen und Compliance-Vorgaben. Damit einher geht ein hohes Maß an Rechtsunsicherheit bei der Auslegung neuer Rechtsbegriffe und der Abgrenzung der Rechtsakte zueinander. Die Regelungen zu Datenzugang, -austausch und -nutzung stehen zudem vielfach quer zu den Vorgaben der Datenschutz-Grundverordnung.

Eine gesetzeskonforme Datennutzung erfordert eine kontinuierliche Überwachung und Überprüfung, um sicherzustellen, dass diese Datennutzung mit den sich ändernden rechtlichen und regulatorischen Anforderungen konform bleibt. Der europäische Rechtsrahmen stärkt die Datensouveränität, enthält aber auch Einschränkungen und bürokratische Anforderungen, die auf den ersten Blick überwältigend wirken können. Diese Einschränkungen sollen den Interessen der Betroffenen, der Datenanbieter und der Dateninhaber gleichermaßen dienen. Dies ist besonders wichtig im Zusammenhang mit der gemeinsamen Nutzung von Daten durch Organisationen. Die gemeinsame Nutzung von Daten kann zwar wirtschaftliche Vorteile

bringen, birgt aber auch Risiken für den Datenschutz und die Selbstbestimmung. Insofern ist das europäische Datenrecht stets auch eine Gratwanderung.

Dieses Handbuch möchte insbesondere Praktikern, die durch das neue Datenrecht vor große Herausforderungen gestellt werden, helfen, das entstandene Dickicht zu lichten.

Großer Dank gilt selbstverständlich allen Autorinnen und Autoren, dem Verlag sowie ferner den studentischen Hilfskräften Justus Nägele und Alfiya Zhunussova für Ihre tatkräftige Unterstützung bei der Fertigstellung des Handbuchs.

Kassel im Juni 2025 Die Herausgeber

Inhaltsübersicht

Teil 6:
Datensteuerungsrecht (Data Governance Act)

Teil 7:
Datennutzungsrecht (Data Act)

Teil 8:
Recht der KI und der digitalen Infrastrukturen

Teil 9:
Datenschutz und Datensicherheit

Teil 10:
Sektorübergreifende Betrachtungen

Teil 11:
Rechtsbehelfe und Sanktionen

Teil 12:
Ausblick

Inhaltsverzeichnis

Teil 3:
Der Handel mit Daten

Teil 4:
Macht durch Daten (Digital Markets Act)

Teil 5:
Datendienste und -produkte (Digital Services Act)

Bearbeiterverzeichnis

Dr. André Artelt Universität Bielefeld	§ 2
Dr. Tamer Bile, LL.M. Kassel	§§ 8, 10
Fabiola Böning Universität Kassel	§ 28 (mit *Schindler*)
Dr. Ernestine Dickhaut Universität Kassel	§ 9 (mit *Reinhard/Li/Leimeister*)
Prof. Dr. Kai Erenli, LL.M. (it-law) (Wien) Fachhochschule des BFI Wien	§§ 15 bis 17
PD Dr. Christian Geminn, Mag. iur. Universität Kassel	§§ 1, 6, 41
RA Dominik Hoidn Frankfurt am Main	§ 38 (mit *Kirschnick*)
Tom Hubert Universität Göttingen	§ 33 (mit *Schaller/Zurawski*)
Johannes Jänicke Berlin	§ 23
RA Paul C. Johannes, LL.M. Universität Kassel	§§ 3, 29, 30, 36
Dr. Murat Karaboga Fraunhofer-Institut für System- und Innovationsforschung ISI, Karlsruhe	§ 5 (mit *Schütz*)
RAin Dr. Johanna M. Kirschnick, LL.M. (KCL) Berlin	§ 38 (mit *Hoidn*) § 40
Marcel Kohpeiß, LL.M. (Glasgow) Universität Mainz	§ 35 (mit *Seyda*)
Prof. Dr. Steffen Kroschwald, LL.M. Hochschule Pforzheim	§§ 18, 34
Dr. Mahei Manhai Li Universität Kassel	§ 9 (mit *Reinhard/Dickhaut/Leimeister*)
Prof. Dr. Jan Marco Leimeister Universität Kassel	§ 9 (mit *Reinhard/Dickhaut/Li*)
Luisa Lorenz, LL.M. Universität Kassel	§ 22

Dr. Yannic Meier Universität Duisburg-Essen, Duisburg	§ 4
StA Dr. Johannes K. M. Müller, MLE. Mühlhausen/Thüringen	§§ 12 bis 14
RA Jan-Philipp Muttach Frankfurt am Main	§§ 7, 19 (mit *Schomberg*) § 20
Dr. Maxi Nebel Universität Kassel	§ 32
Lars Pfeiffer, LL.M. Universität Kassel	§ 21
Philipp Reinhard Universität Kassel	§ 9 (mit *Dickhaut/Li/ Leimeister*)
Fabian Schaller Datenschutzbeauftragter, Kassel	§ 37
Till Schaller Universität Kassel	§ 33 (mit *Hubert/Zurawski*)
VorsRiVG a.D. Hans-Hermann Schild Universität Kassel	§ 39
Dr. Stephan Schindler Universität Kassel	§ 28 (mit *Böning*)
Sabrina Schomberg Hessisches Ministerium des Inneren, für Sicherheit und Heimatschutz, Wiesbaden/Kassel	§§ 7, 19 (mit *Muttach*)
Philip Schütz Datenschutzkoordinator Mercedes-Benz (Stuttgart); Doktorand Universität Göttingen; Geschäftsführer data revolution (Karlsruhe)	§ 5 (mit *Karaboga*)
Linda Seyda Universität Kassel	§ 35 (mit *Kohpeiß*)
RA Benjamin Stach, LL.M. (KCL) Hamburg und Berlin	§ 11
RA Robert Weinhold Düsseldorf	§§ 24 bis 27
Dr. Julia Zirfas, LL.M. Kaden	§ 31
Paul Zurawski Universität Kassel	§ 33 (mit *Schaller/Hubert*)

Teil 1:
Einleitung

§ 1 Das europäische Datenrecht

Literatur: *Dettling/Krüger,* Erste Schritte im Recht der Künstlichen Intelligenz, MMR 2019, 211; *Ebers/Steinrötter* (Hrsg.), Künstliche Intelligenz und smarte Robotik im IT-Sicherheitsrecht, 2021; *Fleisch/Mattern* (Hrsg.), Das Internet der Dinge, 2005; *Floridi/Taddeo,* What is data ethics?, Philosophical Transactions of the Royal Society A 2083/2016; *Geminn/Roßnagel*, „Privatheit" und „Privatsphäre" aus der Perspektive des Rechts – ein Überblick, JZ 2015, 703; *Geminn*, Deus ex machina? – Grundrechte und Digitalisierung, 2023; *Gettier,* Is Justified True Belief Knowledge?, Analysis 1963, 121; *Hennemann*, Datenrecht, 2025; *Kühling/Sackmann*, Irrweg „Dateneigentum", ZD 2020, 24; *Reinermann/von Lucke*, Speyerer Definition von Electronic Government, 2000; *Roßnagel*, Kein „Verbotsprinzip" und kein „Verbot mit Erlaubnisvorbehalt" im Datenschutzrecht, NJW 2019, 1; *Roßnagel/Geminn*, Vertrauen in Anonymisierung, ZD 2021, 487; *Steinrötter,* Gegenstand und Bausteine eines EU-Datenwirtschaftsrechts, RDi 2021, 480; *von Lucke/Reinermann*, Speyerer Definition von Electronic Government, 2000; *Zuboff,* A Digital Declaration, in: FAZ, 15.09.2014; *Zuboff,* The Age of Surveillance Capitalism – The Fight for a Human Future at the New Frontier of Power, 2019.

A. Datenrecht – Was ist das?

Der Begriff des Datenrechts hat sich in der rechtswissenschaftlichen Diskussion etabliert. Dies wird ua durch die Institutionalisierung seiner Beforschung belegt; ein Beispiel ist hier die Forschungsstelle für Rechtsfragen neuer Technologien sowie Datenrecht (ForTech) e.V. Die Neue Juristische Wochenschrift hat sich bereits 2022 in einer Sonderausgabe dem „Neuen Digital- und Datenrecht" gewidmet. Erste juristische Lehrbücher,[1] Sammelbände[2] und Buchreihen[3] tragen den Begriff des Datenrechts im Titel. Aber was steckt eigentlich hinter dem Begriff? Welche Bereiche umfasst das Datenrecht? Und wie ordnet es sich in die Rechtsordnung ein? Hier gehen die Meinungen durchaus auseinander. Das Datenrecht kann eng oder weit verstanden werden. So kann es beispielsweise als Ergänzung des Daten*schutz*rechts gesehen werden oder als ein Überbegriff, der weit mehr erfasst als die Verarbeitung personenbezogener Daten, diese aber miteinschließt. 1

Klar zum Datenrecht gehörig sind jene Verordnungen, die die Europäische Kommission in der Folge des Geltungsbeginns der Datenschutz-Grundverordnung (DS-GVO)[4] auf den Weg gebracht hat und die den Begriff Daten bereits im Kurztitel tragen: die Datenverordnung (Data Act, DA)[5] und der Daten-Governance-Rechtsakt (Data Governance Act, DGA).[6] Sie sind wiederum Teil eines Pakets von Verordnungen, dem auch das Gesetz über digitale Märkte (Digital Markets Act, DMA),[7] das Gesetz über digitale Dienste (Data Services Act, DSA)[8] und die Verordnung über künstliche Intelligenz (KI-Verordnung, KI-VO)[9] angehören und die ebenfalls als dem Datenrecht zugehörig angesehen werden können. Die Inklusion von DMA, DSA und KI-Verordnung mag dabei vielleicht zunächst verwundern. Bei näherer Betrachtung finden sich jedoch in den drei Verordnungen zahlreiche Vorschriften, die sich klar dem Umgang mit Daten 2

1 ZB Hennemann, Datenrecht, 2025.
2 S. beispielhaft Specht-Riemenschneider/Werry/Werry (Hrgs.), Datenrecht in der Digitalisierung, 2019.
3 So etwa die Reihe Datenrecht und neue Technologien im Nomos Verlag, deren erster Band 2021 erschien: Ebers/Steinrötter (Hrsg.), Künstliche Intelligenz und smarte Robotik im IT-Sicherheitsrecht, 2021.
4 VO (EU) 2016/679.
5 VO (EU) 2023/2854.
6 VO (EU) 2022/868.
7 VO (EU) 2022/1925.
8 VO (EU) 2022/2065.
9 VO (EU) 2024/1689.

zurechnen lassen – so etwa Art. 40 DSA, der mit „Datenzugang und Kontrolle" überschrieben ist. Der DMA wiederum spricht vom Zugang zu großen Datenmengen als zentralem Faktor für wirtschaftliche Macht[10] und von Daten als einem in der digitalen Wirtschaft entscheidendem Input.[11] Bezogen auf die KI-Verordnung spricht bereits der Kommissionsentwurf in seiner Begründung davon, dass Künstliche Intelligenz „häufig auf großen und vielfältigen Datensätzen" beruhe und hebt die Bedeutung von hoher Datenqualität für KI-Anwendungen hervor.[12] Die für Hochrisiko-KI-Systeme geltenden Anforderungen sollen sich ausdrücklich auch auf Daten beziehen.[13] Mit Art. 10 KI-VO ist eine eigene Vorschrift ganz Daten und Daten-Governance gewidmet. Die genannten Verordnungen sind somit sowohl direkt als auch indirekt im Kontext des Datenrechts relevant und dürfen als **Teilregelungen des Datenrechts** gelten, wenngleich sie (mitunter sogar schwerpunktmäßig) auch anderen Regulierungsbereichen zugehörig sind – etwa dem Verbraucherrecht, dem Produktsicherheitsrecht oder dem Wettbewerbsrecht.

3 Mit diesen fünf Rechtsakten versucht die Kommission, Korrekturen an der digitalen Marktwirtschaft vorzunehmen, aber auch klare Regeln zur Datennutzung in vielen Bereichen, wie etwa der Forschung, zu setzen. Klarer wird der Bezug, wenn man die digitale Marktwirtschaft als **Datenkapitalismus** begreift.

4 Das Datenrecht wird zutreffend als „**Querschnittsmaterie**" charakterisiert, „dessen einendes Element das Regelungsobjekt Daten ist".[14] Andere verwenden mit Blick auf Data Act, Data Governance Act, Digital Markets Act, Digital Services Act und KI-Verordnung den Begriff des (Europäischen bzw. EU-)Daten*wirtschafts*rechts. Dieses wird zB definiert als ein Teilrechtsgebiet, das sich auf „digitalisierte Informationen" beziehe und neben dem Datenschutzrecht stehe.[15] Damit wäre das Datenwirtschaftsrecht ein Teil des Datenrechts.[16] Die Nomos Textsammlung Digitalrecht etwa trennt zwischen Datenrecht und Datenschutzrecht und fasst beide unter diesem Überbegriff zusammen.

5 Viel spricht für einen weiten und zugleich engen **Begriff des Datenrechts**, der explizit das Datenschutzrecht mit einbezieht, gleichzeitig aber auf die Modalitäten der Nutzung von Daten aller Art fokussiert bleibt. Dieser Begriff liegt diesem Werk zugrunde. In der Folge ist eine differenzierte Betrachtung erforderlich: Das Gesetz über digitale Märkte lässt sich – wie dargestellt – nicht in seiner Gesamtheit dem Datenrecht zurechnen; es enthält aber einzelne Regelungen, die zum Kernbestand des Datenrechts gehören. Aber auch bei dieser vermeintlich klaren Konkretisierung des Begriffs des Datenrechts bleiben an den Rändern Unschärfen und Überlappungen, so wie sie etwa auch zwischen dem Datenschutz und der Datensicherheit bestehen, die indes beide unter dem Dach des Datenrechts gefasst werden können und wohl auch sollten. Neben den genannten Verordnungen umfasst das Datenrecht jedenfalls auch weiteres Unionsrecht sowie viele mitgliedstaatliche Regelungen,[17] die vielfach Rechtsakte der EU umsetzen, aber auch eigene Regelungsansätze enthalten. Beispiele unter vielen sind die Richtlinie über offene Daten,[18] die Verordnung über den europäischen Gesundheitsdatenraum,[19]

10 S. ErwG 3 S. 2 sowie 59 S. 1 DMA. Zur Bedeutung von personenbezogenen Daten s. ErwG 36 DMA.
11 ErwG 3 S. 4 DMA.
12 COM(2021) 206 final, Begründung, 2.2 und 2.3. S. insbes. auch ErwG 44 KI-VO-KOM-E sowie ErwG 67 KI-VO.
13 COM(2021) 206 final, Begründung, 3.3.
14 Vorwort, in: Specht-Riemenschneider/Werry/Werry (Hrgs.), Datenrecht in der Digitalisierung, 2019, S. 5.
15 So Steinrötter RDi 2021, 480.
16 S. auch Gloy/Loschelder/Danckwerts WettbR-HdB/Becker § 64 Rn. 6: „Datenrecht setzt sich als Rechtsgebiet aus dem Schutz personenbezogener und dem (noch jungen) Schutz nicht-personenbezogener Daten zusammen. Da Daten vermehrt in wirtschaftlichem Zusammenhang relevant sind, ist seit wenigen Jahren auch vom Zweig des ‚Datenwirtschaftsrechts' die Rede."
17 Wie etwa das Telekommunikation-Digitale-Dienste-Datenschutz-Gesetz – TDDDG; BGBl. I S. 1982; 2022 I S. 1045.
18 RL (EU) 2019/1024.
19 VO (EU) 2024/2847.

die NIS-2-Richtlinie[20] und weitere Rechtsakte aus dem Bereich Cyber-/IT-/Datensicherheit. Sie sind so zahlreich, dass in diesem Handbuch nur ein nicht abschließender Überblick gegeben werden kann. DA, DGA, DS-GVO, DMA, DSA und KI-VO stellen dabei ohne Zweifel einen zentralen Kernbereich des Datenrechts dar – sie sind eine Art „Nukleus" des Datenrechts. Ihnen ist dieses Handbuch deshalb schwerpunktmäßig gewidmet.

Durch die Regulierungsoffensive der Kommission bezogen auf den Umgang mit Daten im digitalen Binnenmarkt und darüber hinaus ist ein Dickicht entstanden, das nur schwer zu entwirren ist. Ein harmonisches Nebeneinander der zahlreichen Rechtsakte ist längst nicht immer gewährleistet. Ganz im Gegenteil stellen sich **Abgrenzungsfragen**, die nicht zuletzt auch gegenläufigen Zielsetzungen geschuldet sind. So stehen bereits die Grundsätze Datenminimierung und Speicherbegrenzung in einem natürlichen Konfliktverhältnis mit dem Ziel der Förderung von Datennutzung, das sich – wenn überhaupt – nur schwer auflösen lässt. 6

Bei einer Gegenüberstellung der Begriffe Datenrecht und Datenschutzrecht könnte unterstellt werden, dass die Verkürzung um den Begriffsteil „schutz" nicht (nur) vor dem Hintergrund einer Erweiterung des Regelungsgegenstandes erfolgt ist, sondern gerade auch einen **Paradigmenwechsel** weg vom Schutz und hin zu einer umfassenden Nutzbarmachung von Daten einläuten soll. In der Folge würde das Datenschutzrecht von dem Stoppschild, als das es zumindest in der Praxis häufig wahrgenommen wird, zu einem vermeintlich gleichberechtigten Bestandteil unter dem Dach des Datenrechts; der Datenschutz erführe also eine Relativierung. Bei näherer Betrachtung ist das Datenschutzrecht aber ein Ermöglicher der Verarbeitung personenbezogener Daten, nicht sein Verhinderer: „Das Datenschutzrecht wird dadurch geprägt, dass es die Datenverarbeitung unter bestimmten, in den datenschutzrechtlichen Erlaubnistatbeständen genannten Bedingungen erlaubt."[21] Dementsprechend kann nicht von einem Paradigmenwechsel gesprochen werden, sondern ganz im Gegenteil von einer konsequenten Linie, die vom Datenschutzrecht zum Datenrecht führt und keine Relativierung des Datenschutzrechts zum Ziel hat, sondern seine Stärkung. Dennoch wird ein solcher Paradigmenwechsel in der im Rahmen der Diskussion um das Datenrecht verwendeten Rhetorik immer wieder behauptet – in den einzelnen Rechtsakten des Datenrechts und ihrem Zusammenwirken spiegelt er sich nicht wider. Im Datenrecht stehen sich somit gerade nicht Datenschutzrecht und ein „Datennutzungsrecht" gegenüber. Der Begriff des Datenrechts darf ferner nicht verstanden werden als Ausdruck eines „Rechts an Daten" im Sinne eines Ausschließlichkeitsrechts.[22] Das Datenrecht ist das „Recht über Daten" und nicht ein „Recht an Daten". 7

Das Datenrecht schließt einerseits Lücken, die durch die ausschließliche Geltung des Datenschutzrechts für die Verarbeitung personenbezogener Daten entstanden sind; andererseits erweitert es aber auch die Regelungen des Datenschutzrechts um unterschiedlichste weitere zu beachtende Modalitäten. Ein zentraler Missstand ist allerdings nach wie vor nicht beseitigt: Es fehlt weiterhin an abstrakten und allgemeingültigen Regeln für den Umgang mit nicht personenbezogenen Daten.[23] 8

Zusammenfassend muss festgestellt werden, dass eine Verkürzung des Datenrechts auf ein Datenwirtschaftsrecht zu kurz greift. Trotz der Fragmentierung des Datenrechts sollten die Rechtssetzungsaktivitäten der jüngeren Zeit als Chance genutzt werden, mit dem Datenrecht ein neues Rechtsgebiet fest zu etablieren, das einer gesamtheitlichen Behandlung des Umgangs mit jeder Form von Daten gewidmet ist. 9

20 RL (EU) 2022/2555.
21 S. Roßnagel NJW 2019, 1.
22 S. hierzu Kühling/Sackmann ZD 2020, 24.
23 S. Roßnagel/Geminn ZD 2021, 487.

B. Der lange Weg zum europäischen Datenrecht

10 Die Wurzeln des Datenrechts reichen zurück bis zu den ersten Regelungen zum Umgang mit Daten. Seine Anfänge können in den ersten Überlegungen zu den Wechselwirkungen zwischen moderner (Computer-)Technik und Recht in den 1950er Jahren gesehen werden, die wiederum mit der beginnenden Verbreitung von Großrechenanlagen einhergehen. Hervorzuheben ist ferner der Abschlussbericht der **Bangemann-Gruppe**, einer vom FPD-Politiker und Kommissar für Industriepolitik, Informationstechnik und Telekommunikation Martin Bangemann geleiteten Expertengruppe, aus dem Jahr 1994. Hier hieß es noch: „Die Schaffung der Informationsgesellschaft sollte dem privaten Sektor und den Marktkräften überlassen werden."[24] Das Vertrauen in die Marktkräfte ist indes längst Vergangenheit; die hierin zum Ausdruck kommende Grundhaltung steht in einem klaren Gegensatz zu weiten Teilen des neuen Datenrechts.

11 Ein erster wichtiger Meilenstein für die Entwicklung des heutigen europäischen Datenrechts war die 2010 veröffentlichte **Digitale Agenda**.[25] Ihre eigenen Wurzeln reichen zurück zum Aktionsplan eEurope 2002 aus dem Jahr 2000.[26] Bereits vor der Vorstellung der Digitalen Agenda hatten die Arbeiten an der Datenschutz-Grundverordnung begonnen, die im Bereich des Datenschutzrechts eine unionsweite Harmonisierung erreichen wollte, die ihre Vorgängerin, die Datenschutzrichtlinie 95/46/EG, trotz entsprechender Bemühungen nicht bewirkt hatte. Ein wichtiger Trittstein auf dem Weg zur Datenschutz-Grundverordnung war die Mitteilung der Kommission zum Schutz der Privatsphäre in einer vernetzten Welt – Ein europäischer Datenschutzrahmen für das 21. Jahrhundert.[27] Hier steckte die Kommission öffentlichkeitswirksam den Rahmen der angestrebten Reform des EU-Datenschutzrechts ab.

12 2014 veröffentlichte die Europäische Kommission dann die Mitteilung „Für eine florierende datengesteuerte Wirtschaft".[28] Darin griff sie Schlussfolgerungen des Europäischen Rats aus dem Oktober 2013 auf, in denen dieser „Rahmenbedingungen für einen Binnenmarkt für Big Data und Cloud-Computing" forderte.[29] 2015 folgte die Strategie für einen digitalen Binnenmarkt für Europa;[30] 2017 die Mitteilung „Aufbau einer Europäischen Datenwirtschaft".[31] Weitere wichtige Meilensteine waren ua:

- „Gestaltung der digitalen Zukunft Europas";[32]
- „Conclusions on the Future of a highly digitised Europe beyond 2020";[33] sowie die
- „Berlin Declaration on Digital Society and Value-Based Digital Government".[34]

13 Ein Jahrzehnt nach der Digitalen Agenda folgte schließlich die 2020 vorgestellte **Europäische Datenstrategie**.[35] Sie ruht auf vier Säulen: 1. Einem sektorübergreifenden Governance-Rahmen für Datenzugang und Datennutzung; 2. Investitionen in Daten und in die Stärkung der europäischen Kapazitäten und Infrastrukturen für das Hosting, die Verarbeitung und die Nutzung von Daten sowie der Interoperabilität; 3. der Stärkung der Handlungskompetenz des Einzelnen, Investitionen in Kompetenzen und in KMU; 4. gemeinsamen europäischen

24 Bangemann u.a., Europa und die globale Informationsgesellschaft, Empfehlungen für den Europäischen Rat v. 26.5.1994, S. 35; s. auch S. 30.
25 Eine Digitale Agenda für Europa, KOM(2010) 245 endg.
26 eEurope 2002, Eine Informationsgesellschaft für alle, Entwurf eines Aktionsplans, KOM(2000) 330 endg.
27 COM(2012) 9.
28 COM(2014) 442 final.
29 EUCO 169/13, S. 2.
30 COM(2015) 192 final. S. auch „Ein vernetzter digitaler Binnenmarkt für alle", COM(2017) 228 final.
31 COM(2017) 9 final. S. auch das Begleitdokument SWD(2017) 2 final.
32 COM(2020) 67 final.
33 Ratsdok. 10102/19 v. 7.6.2019.
34 Erklärung v. 8.12.2020. In Anknüpfung an die „Tallinn Declaration" (Ministerial Declaration on eGovernment) v. 6.10.2017.

Datenräumen in strategischen Sektoren und Bereichen von öffentlichem Interesse.[36] Zur Motivation führte die Kommission aus: „Digitale Technik hat in den letzten Jahren die Wirtschaft und Gesellschaft verändert und wirkt sich auf alle Tätigkeitsbereiche und das tägliche Leben aller Europäerinnen und Europäer aus. Daten stehen im Mittelpunkt dieses Wandels, und dies ist erst der Anfang. Die von Daten vorangetriebene Innovation wird den Bürgerinnen und Bürgern enorme Vorteile bringen, beispielsweise durch eine verbesserte personalisierte Medizin, durch eine neue Mobilität und durch ihren Beitrag zum europäischen Grünen Deal. In einer Gesellschaft, in der jeder Einzelne immer größere Datenmengen erzeugt, muss die Art und Weise, wie Daten gesammelt und verwendet werden, zuallererst den Interessen des Einzelnen entsprechen – ganz im Einklang mit den europäischen Werten, Grundrechten und Vorschriften. Die Bürgerinnen und Bürger werden sich nur dann auf datengetriebene Innovationen einlassen und ihnen Vertrauen entgegenbringen, wenn sie zuversichtlich sind, dass bei jeder Weitergabe personenbezogener Daten in der EU die strengen EU-Datenschutzvorschriften strikt eingehalten werden. Zugleich entsteht mit der zunehmenden Menge nicht personenbezogener industrieller und öffentlicher Daten in Europa in Verbindung mit den technologischen Veränderungen bei der Speicherung und Verarbeitung der Daten eine potenzielle Quelle für Wachstum und Innovation, die unbedingt genutzt werden sollte."[37] Zielsetzung ist somit letztendlich nicht weniger als ein Ausgleich zwischen ökonomischen Interessen und durch Datenverarbeitung betroffenen Grundrechten sowie einfachgesetzlichen Schutzrechten. Wirtschaftspolitisches Ziel ist es dabei, dass bis zum Jahr 2030 „der Anteil der EU an der Datenwirtschaft (dh die in Europa gespeicherten, verarbeiteten wertschöpfend genutzten Daten) mindestens ihrem wirtschaftlichen Gewicht entspricht".[38] Grundlage dafür soll „die Schaffung eines einheitlichen europäischen Datenraums, eines echten Binnenmarktes für Daten," sein, „der für Daten aus aller Welt offensteht, in dem sowohl personenbezogene als auch nicht personenbezogene Daten, darunter auch sensible Geschäftsdaten, sicher sind und in dem Unternehmen auch leicht Zugang zu einer nahezu unbegrenzten Menge hochwertiger industrieller Daten erhalten".[39] Datenräume werden dabei auch sektorspezifisch geschaffen, so zB in den Bereichen Gesundheit und Mobilität.

14 Entsprechende gesetzgeberische Bemühungen sieht die Kommission in einer Linie mit der **Datenschutz-Grundverordnung**, die sie trotz deutlich älterer Regulierungsbemühungen selbst **als Ausgangspunkt** benennt.[40] Zudem benennt die Kommission die Verordnung über den freien Verkehr nicht personenbezogener Daten,[41] den Rechtsakt zur Cybersicherheit[42] und die Richtlinie über offene Daten[43] sowie bereichsspezifische Regelungen.

15 Daneben und ergänzend steht die Diskussion um die Regulierung von Künstlicher Intelligenz. **Meilensteine** sind hier ua:[44]

- Mitteilung der Europäischen Kommission, Künstliche Intelligenz für Europa, COM(2018) 237 final;

35 COM(2020) 66 final.
36 COM(2020) 66 final, 13 ff.
37 COM(2020) 66 final, 1.
38 COM(2020) 66 final, 5.
39 COM(2020) 66 final, 5.
40 COM(2020) 66 final, 4. Dabei wird das Datum 2014 genannt (und damit das Jahr der Verabschiedung der Verordnung durch das Europäische Parlament), wenngleich die Entwicklungsgeschichte der Datenschutz-Grundverordnung bereits im Jahr 2010 beginnt (mit der Vorstellung des Gesamtkonzepts für den Datenschutz in der Europäischen Union, KOM(2010) 609 endg.).
41 VO (EU) 2018/1807.
42 VO (EU) 2019/881.
43 RL (EU) 2019/1024.
44 Für einen umfassenden Überblick über die Aktivitäten der Europäischen Union im Bereich Künstliche Intelligenz s. COM(2021) 205 final, Appendix 1.

- Koordinierter Plan für künstliche Intelligenz, COM(2018) 795 final;[45]
- OECD Recommendation on Artificial Intelligence[46] mit ihren fünf „Principles for Responsible Stewardship of Trustworthy AI" aus dem Mai 2019;[47]
- G20 AI Principles;[48]
- 2019–2020: Veröffentlichung der Deliverables der Hochrangigen Expertengruppe für künstliche Intelligenz (1. Ethics guidelines for trustworthy AI; 2. Policy and investment recommendations for trustworthy Artificial Intelligence; 3. Assessment List for Trustworthy Artificial Intelligence (ALTAI) for self-assessment; 4. Sectoral Considerations on Policy and Investment Recommendations for Trustworthy AI);
- Ad Hoq Committee on Artificial Intelligence (CAHAI), Feasibility Study, CAHAI(2020)23;[49]
- Weißbuch zur Künstlichen Intelligenz – ein europäisches Konzept für Exzellenz und Vertrauen, COM(2020) 65 final
- UNESCO Recommendation on the ethics of artificial intelligence, SHS/BIO/REC-AI-ETHICS/2;
- Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law als erstes verbindliches internationales Vertragswerk zum Thema KI.[50]

Grundrechtliche Überlegungen stellen die Schlussfolgerungen zur Charta der Grundrechte im Zusammenhang mit künstlicher Intelligenz und dem digitalen Wandelaus dem Oktober 2020 an[51] sowie bereits zuvor die Studie des Europarates „Algorithms and Human Rights".[52] Ebenfalls aus dem Oktober 2020 stammt eine Entschließung des Europäischen Parlaments zu „ethischen Aspekte von künstlicher Intelligenz, Robotik und damit zusammenhängenden Technologien".[53] Das Parlament forderte hier eine Verordnung über ethische Grundsätze für die Entwicklung, den Einsatz und die Nutzung der genannten Technologien. Hier wurde bereits eine „erschöpfende und kumulative Liste von Bereichen sowie Verwendungen mit hohem Risiko, die das Risiko der Verletzung von Grundrechten und Sicherheitsvorschriften in sich bergen", formuliert.[54]

16 Zu den Bemühungen um die Regulierung von Künstlicher Intelligenz treten zahlreiche weitere **bereichsspezifische Aktivitäten** mit Relevanz für das Datenrecht, so zB:

- Europäische Cloud-Initiative;[55]
- Strategie für ein digitales Finanzwesen in der EU;[56]
- Die Cybersicherheitsstrategie der EU für die digitale Dekade;[57]

45 Ein Review des Plans wurde 2021 zeitgleich mit dem Entwurf eines Artificial Intelligence Act vorgestellt; COM(2021) 205 final.
46 Recommendation of the Council on Artificial Intelligence, OECD/LEGAL/0449.
47 Eine Aktualisierung erfolgte schließlich im Mai 2024. Die Definition von KI-Systemen in Art. 3 Nr. 1 KI-VO ist sehr eng an die hier vorgestellte Definition angelehnt.
48 G20 Ministerial Statement on Trade and Digital Economy v. 16. Juli 2019, Annex, S. 11.
49 Diese identifiziert die folgenden „key values, rights and principles" als essenziell: Human dignity; Prevention of harm to human rights, democracy and the rule of law; Human Freedom and Human Autonomy; Non-Discrimination, Gender Equality, Fairness and Diversity; Principle of Transparency and Explainability of AI systems; Data protection and the right to privacy (ebd., S. 27 ff.).
50 CM(2024)52-final v. 17.05.2024. Zur Kritik an der Convention s. beispielhaft die Pressemitteilung des Europäischen Datenschutzbeauftragten v. 11.05.2024. Insbesondere sei die Convention vornehmlich deklarativer Natur.
51 Ratsdok. 11481/20 v. 21. Oktober 2020.
52 Council of Europe study, DGI(2017) 12.
53 Legislative Entschließung des Europäischen Parlaments vom 20. Oktober 2020 mit Empfehlungen an die Kommission zu dem Rahmen für die ethischen Aspekte von künstlicher Intelligenz, Robotik und damit zusammenhängenden Technologien (2020/2012(INL)).
54 S. den Anhang zum Verordnungsentwurf.
55 COM(2016) 178 final.
56 COM(2020) 591 final.

- Eine digitale Dekade für Kinder und Jugendliche: die neue europäische Strategie für ein besseres Internet für Kinder (BIK+);[58]
- Strategische Vorausschau 2022 – Verzahnung des grünen und des digitalen Wandels im neuen geopolitischen Kontext[59] sowie die
- EU-Initiative für das Web 4.0 und virtuelle Welten: mit Vorsprung in den nächsten technologischen Wandel.[60]

Vor allem aber hat die Kommission die 2020er Jahre im „2030 Digital Compass" zum „**digitalen Jahrzehnt**" erklärt und Ziele formuliert, die einen „europäischen Weg" durch dieses Jahrzehnt weisen sollen.[61] 2022 folgte die hier bereits angekündigte „Europäische Erklärung zu den digitalen Rechten und Grundsätzen für die digitale Dekade".[62] Dieses digitale Jahrzehnt ist auch das Jahrzehnt des europäischen Datenrechts. 17

Die **Motive** für das Tätigwerden des Gesetzgebers waren und sind dabei so vielfältig wie die einzelnen (sich zudem noch überlappenden und verwobenen) Teilbereiche und -aspekte des Datenrechts. Sie reichen vom technischen Fortschritt und marktwirtschaftlichen oder gesellschaftlichen Dynamiken – ausgedrückt zB im Aufkommen neuer digitaler Dienstleistungen oder sozialer Phänomene (oft auch nur als Neufassung bekannter Phänomene) – bis hin zu weltpolitischen Ereignissen wie Krieg, Pandemie oder Wahlbeeinflussung. Zentrale Motive sind jedoch ohne Zweifel digitale Souveränität und Datensouveränität in Europa zu gewährleisten, einen europäischen und dritten Weg (neben den USA und der VR China) zu beschreiten und den Schutz der europäischen Grundrechte und -freiheiten zu gewährleisten. Um diese Ziele zu erreichen, muss vor allem Vertrauen durch effektive Rechtsetzung geschaffen werden. Daran muss sich das Datenrecht messen lassen. 18

C. Zentrale (nicht-rechtliche) Definitionen des Datenrechts

Jenseits der unzähligen Begriffsdefinitionen, die sich in den einzelnen Rechtsakten des Datenrechts finden und in den nachfolgenden Kapiteln ausführlich behandelt werden, werden in der Diskussion auch Begriffe verwendet, die entweder ohne rechtliche Definition bleiben oder deren rechtlichen Definitionen andere Definitionen zur Seite gestellt werden (oder diesen vorausgingen). Einige ausgewählte Definitionen ohne rechtliche Bindungswirkung sind im Folgenden aufgeführt. 19

Big Data – „consists of extensive datasets – primarily in the characteristics of volume, velocity, variety, and/or variability – that require a scalable architecture for efficient storage, manipulation, and analysis."[63] 20

Blockchain – „ein verteiltes Register, in dem digitale Datensätze, Ereignisse oder Transaktionen in chronologischer Reihenfolge für alle Teilnehmer nachvollziehbar in Datenblöcken gespeichert (‚Block') und unveränderbar miteinander verkettet (‚Chain') werden".[64] 21

Corporate Digital Responsibility – „freiwillige unternehmerische Aktivitäten, die über das heute gesetzlich Vorgeschriebene hinausgehen und die digitale Welt aktiv zum Vorteil der Gesellschaft mitgestalten".[65] 22

57 JOIN(2020) 18 final.
58 COM(2022) 212 final.
59 COM(2022) 289 final.
60 COM(2023) 442 final.
61 2030 Digital Compass: the European way for the Digital Decade, COM(2021) 118 final.
62 COM(2022) 28 final.
63 NIST Big Data Interoperability Framework: Volume 1, Definitions, NIST Special Publication 1500–1r2, Version 3, S. 10.
64 Bundesnetzagentur, Die Blockchain-Technologie – Grundlagen, Potenziale und Herausforderungen, 2021, S. 5.
65 BMJV, CDR-Initiative, S. 3.

23 **Data asset/Datenbestand** – „A data asset is any collection of data, any data set or any information that is somehow linked, e.g. by common codes or metadata, which has been created by the Commission, collected from Member States or other stakeholders, or acquired from third parties in the context of projects, policy or administrative processes. Data assets may be structured or unstructured, static or dynamic, raw or curated. Data assets are in digital formats."[66]

24 **Data policies/Datenrichtlinien** – „Data policies are a set of broad, high level principles which form the guiding framework in which data assets […] can be managed. More specifically, data policies govern data management, data interoperability and standards, data quality, data protection and information security."[67]

25 **Daten** – „Der Begriff ‚Daten' versammelt eine immense Diversität von Erscheinungsformen unter einem Begriffsdach. So lassen sich Daten etwa anhand des Datentyps (zB binäre, nominale, ordinale, metrische und textuelle Daten), des datengenerierenden Prozesses (zB Umfragedaten, Sensordaten), des Erhebungsbereichs (zB Finanzdaten, Wetterdaten) oder ihrer Funktion in einem digitalen System (zB Log-in-Daten, Trainingsdaten) einteilen. Eine weitere Einteilung setzt am Grad der Verarbeitung (Veredelung) an: Ohne eine weitere Verarbeitung spricht man auch von ‚Rohdaten', je nach dem Grad der Strukturierung (Normalisierung) von ‚strukturierten' oder ‚unstrukturierten' Daten. Daten können der Input in ein System sein oder auch der Output, der wiederum der Input in das nächste System sein mag. Daten können zugleich digitale Vermögensgüter (digital assets) repräsentieren, wie multimediale Inhalte oder Einheiten von Kryptowährungen."[68]

26 **Datenethik** – „branch of ethics that studies and evaluates moral problems related to data (including generation, recording, curation, processing, dissemination, sharing and use), algorithms (including artificial intelligence, artificial agents, machine learning and robots) and corresponding practices (including responsible innovation, programming, hacking and professional codes), in order to formulate and support morally good solutions (e.g. right conducts or right values)".[69]

27 **Datengovernance** – „A set of processes that ensures that data assets are formally managed throughout the enterprise. A data governance model establishes authority and management and decision making parameters related to the data produced or managed by the enterprise."[70]; „Data governance entails defining, implementing and monitoring strategies, policies and shared decision-making over the management and use of data assets."[71]

28 **Datenraum** – „Eine föderierte, offene Infrastruktur für souveränen Datenaustausch, die auf gemeinsamen Vereinbarungen, Regeln und Standards beruht."[72]

29 **Datenschutz** – „Datenschutz ist die Gesamtheit von Regeln, Institutionen und Maßnahmen, um die informationelle Selbstbestimmung der Bürger zu schützen. Er schützt nicht die Daten (des Datenverarbeiters), sondern die Grundrechte der von einer Datenverarbeitung ‚betroffenen Person' (gegen den Datenverarbeiter)."[73]

66 European Commission, Data governance and data policies at the European Commission, Juni 2020, S. 7.
67 European Commission, Data governance and data policies at the European Commission, Juni 2020, S. 6.
68 Gutachten der Datenethikkommission, 2019, S. 52.
69 Floridi/Taddeo, Philosophical Transactions of the Royal Society A, 374(2083), 2016, S. 3.
70 Committee on National Security Systems (CNSS) Glossary, CNSSI No. 4009, S. 41 unter Verweis auf NSA/CSS Policy 11–1.
71 European Commission, Data governance and data policies at the European Commission, Juni 2020, S. 6.
72 Reiberg/Niebel/Kraemer, Was ist ein Datenraum? – Definition des Konzeptes Datenraum, Gaia-X Hub Germany, White Paper 1/2022.
73 Roßnagel, Datenschutz, in: Andersen/Gobumil/Marschall/Woyke (Hrsg.), Handwörterbuch des politischen Systems der Bundesrepublik Deutschland, S. 172–177 (172).

Datensicherheit – „Mit Datensicherheit wird der Schutz von Daten hinsichtlich gegebener Anforderungen an deren Vertraulichkeit, Verfügbarkeit und Integrität bezeichnet. Ein modernerer Begriff dafür ist ‚Informationssicherheit'." 30

Datenwirtschaft – „The Data Economy measures the overall impacts of the data market on the economy as a whole. It involves the generation, collection, storage, processing, distribution, analysis elaboration, delivery, and exploitation of data enabled by digital technologies. The data economy also includes the direct, indirect, and induced effects of the data market on the economy." 31

Desinformation – „all forms of false, inaccurate, or misleading information designed, presented and promoted to intentionally cause public harm or for profit". 32

Digital Single Market/digitaler Binnenmarkt – „A Digital Single Market is one in which the free movement of goods, persons, services and capital is ensured and where individuals and businesses can seamlessly access and exercise online activities under conditions of fair competition, and a high level of consumer and personal data protection, irrespective of their nationality or place of residence. Achieving a Digital Single Market will ensure that Europe maintains its position as a world leader in the digital economy, helping European companies to grow globally." 33

Digitalisierung – „Unter dem Begriff der Digitalisierung werden unterschiedliche Phänomene zusammengefasst, die zumeist aus technologischen Entwicklungen im Umfeld von Computern und Datennetzen resultieren. Grundlegend wird dabei von der Umwandlung analoger Informationen in verschiedene digitale Formate ausgegangen, wobei nicht allein die kommunikative Dimension („digitale Medien") relevant ist, sondern zunehmend auch Produktion und Distribution immaterieller Güter, die Prozessierung großer Datenmengen sowie die Entwicklung und der Einsatz von Algorithmen eingeschlossen werden." 34

E-Government – „Abwicklung geschäftlicher Prozesse im Zusammenhang mit Regieren und Verwalten (Government) mit Hilfe von Informations- und Kommunikationstechniken über elektronische Medien" 35

Fake News – „absichtlich falsche Nachrichten, die eigens zum Zweck der viralen Verbreitung über das Internet und soziale Netzwerke produziert wurden" mit dem Ziel „die Öffentlichkeit für bestimmte politische und/oder kommerzielle Zwecke zu manipulieren".[80] Der Begriff wird jedoch vielfach abgelehnt;[81] stattdessen findet der Begriff der Desinformation Verwendung.[82] 36

Hate Speech – „The term encompasses a wide array of hateful messages, ranging from offensive, derogatory, abusive and negative stereotyping remarks and comments, to intimidating, inflammatory speech inciting violence against specific individuals and groups. Only the most egregious forms of hate speech, namely those constituting incitement to discrimination, hostility and violence, are generally considered unlawful."[83] 37

74 Bundesamt für Sicherheit in der Informationstechnik, IT-Grundschutz-Kompendium, 2023, Glossar, S. 2.
75 European Data Market, SMART 2013/0063, 2017, S. 123.
76 A multi-dimensional approach to disinformation, Report of the independent High level Group on fake news and online disinformation, März 2018, S. 3.
77 A Digital Single Market Strategy for Europe, COM(2015) 192 final.
78 Bieber, Digitalisierung, in: Andersen/Gobumil/Marschall/Woyke (Hrsg.), Handwörterbuch des politischen Systems der Bundesrepublik Deutschland, S. 234–240 (234).
79 Von Lucke/Reinermann, Speyerer Definition von Electronic Government, 2000, S. 1.
80 Fake News, Definition und Rechtslage, WD 10 – 3000 – 003/17, 6.
81 S. beispielhaft House of Commons, Digital, Culture, Media and Sport Committee, Disinformation and „fake news", S. 2. S. auch HC 1791 v. 18.2.2019.
82 S. beispielhaft A multi-dimensional approach to disinformation, Report of the independent High level Group on fake news and online disinformation, März 2018, S. 3 sowie COM(2018) 236 final.
83 Report of the Special Rapporteur on minority issues, A/HRC/28/64, UN Human Rights Council.

38 **Industrie 4.0** – „bezeichnet die sog. vierte industrielle Revolution auf der Basis cyber-physischer Systeme (intelligente technische Systeme aus der Elektronik, Softwaretechnologie, Informationssysteme, Mechatronik). Demgegenüber fußt die erste industrielle Revolution auf der Nutzung von Dampfmaschinen und der Einführung mechanischer Produktionsanlagen am Ende des 18. Jahrhunderts, die zweite industrielle Revolution ua auf dem Einsatz elektrischer Energie, die Massenproduktion erlaubte. Die dritte industrielle Revolution wird durch den umfangreichen Einsatz von Elektronik und Informationstechnologie (IT) zur weitreichenden Automatisierung charakterisiert."[84]

39 **Information** – „Information ist Wissen in Aktion und Kontext."[85] (informationswissenschaftliche Definition)

40 **Informations- und Kommunikationstechnologie** (**IKT**) – „Includes all categories of ubiquitous technology used for the gathering, storing, transmitting, retrieving, or processing of information (e.g., microelectronics, printed circuit boards, computing systems, software, signal processors, mobile telephony, satellite communications, and networks)."[86]

41 **Internet of Things** – „Vision einer Welt smarter Alltagsgegenstände, welche mit digitaler Logik, Sensorik und der Möglichkeit zur Vernetzung ausgestattet ein ‚Internet der Dinge' bilden, in dem der Computer als eigenständiges Gerät verschwindet und in den Objekten der physischen Welt aufgeht"[87]

42 **Kleine und mittlere Unternehmen** – „Die Größenklasse der Kleinstunternehmen sowie der kleinen und mittleren Unternehmen (KMU) setzt sich aus Unternehmen zusammen, die weniger als 250 Personen beschäftigen und die entweder einen Jahresumsatz von höchstens 50 Mio. EUR erzielen oder deren Jahresbilanzsumme sich auf höchstens 43 Mio. EUR beläuft."[88]

43 **Künstliche Intelligenz** – „Systeme mit einem ‚intelligenten' Verhalten, die ihre Umgebung analysieren und mit einem gewissen Grad an Autonomie handeln, um bestimmte Ziele zu erreichen"[89]

44 **Metaverse** – „The term ‚Metaverse' stems from Neal Stephenson's 1992 novel Snow Crash, and describes a collective virtual shared space that's created by the convergence of virtually enhanced physical reality and persistent virtual space. In its fullest form, the Metaverse experience would span most, if not all virtual words, be foundational to real-world AR experiences and interactions, and would serve as an equivalent ‚digital' reality where all ‚physical' humans would simultaneously co-exist. It is an evolution of the Internet. More commonly, the Metaverse is understood to resemble the world describe by Ernest Cline's Ready Player One."[90]

45 **Smart Contract** – „a computerized transaction protocol that executes the terms of a contract".[91]

46 **Suchmaschine** – „Online-Index von Dokumenten und Bildern, die auf mit dem weltweiten Internet verbundenen Computern veröffentlicht und gespeichert sind. Diese Suchindizes werden

84 Deutscher Bundestag, Wissenschaftliche Dienste, Aktueller Begriff Nr. 23/16 (26.9.2016), S. 1.
85 Kuhlen, Information – Informationswissenschaft, in: Kuhlen/Semar/Strauch (Hrsg.): Grundlagen der praktischen Information und Dokumentation, S. 1 (4).
86 Committee on National Security Systems (CNSS) Glossary, CNSSI No. 4009, S. 62 unter Verweis auf DoDI 5200.44.
87 Fleisch/Mattern, Vorwort, in: Fleisch/Mattern (Hrsg.), Das Internet der Dinge, 2005.
88 Empfehlung der Kommission vom 6.5.2003 betreffend die Definition der Kleinstunternehmen sowie der kleinen und mittleren Unternehmen, 2003/361/EG, Art. 2 Abs. 1.
89 Hochrangige Expertengruppe für Künstliche Intelligenz, Eine Definition der KI: Wichtigste Fähigkeiten und Wissenschaftsgebiete, S. 1 unter Bezugnahme auf COM(2018) 237 final; zur Kritik an der gewählten Definition s. beispielhaft Dettling/Krüger MMR 2019, 211 (211 f.).
90 Ball, Fortnite Is the Future, but Probably Not for the Reasons You Think, Blogeintrag v. 5.2.2019 (matthewball.vc).
91 Szabo, Smart Contracts, 1994.

Stichwortverzeichnis

Die **fetten** Zahlen verweisen auf den Paragrafen, die mageren auf die Randnummer.