Corporate Digital Responsibility im Kontext eines entstehenden Datenrechts

Darius Ruff[*]

§ 1 Einleitung[**]

Die fortschreitende Digitalisierung verändert die Gesellschaft und Wirtschaft tiefgreifend. Zentrale Treiber dieses Wandels sind digitale Technologien wie Big Data-Analysen, der Einsatz von künstlicher Intelligenz (KI) und Distributed Ledger-Technologien, die Vernetzung von Objekten (Internet der Dinge) und virtuelle Realitäten, Fortschritte in der Robotik sowie neue digitale Geschäftsmodelle. Im Zentrum stehen dabei das Erzeugen, Sammeln, Verarbeiten, Analysieren und Nutzen von Daten. Diese werden deshalb häufig als „Rohstoff" des 21. Jahrhunderts bezeichnet und sind Ausgangspunkt der digitalen Transformation und Ökonomie. Die Digitalisierung verändert das Zusammenleben und Wirtschaften, indem sich bestehende Geschäftsmodelle wandeln, neue Wertschöpfungsformen entstehen und Art und Weise der gesellschaftlichen und privaten Kommunikation beeinflusst werden. Chancen und Risiken der digitalen Transformation liegen hierbei nah beieinander.

Zentrale Akteure und Treiber dieser digitalen Transformation sind Unternehmen, die digitale Anwendungen einsetzen bzw. deren Entwicklung und Einsatz vorantreiben. Jenseits von rechtlichen Regelungen stellt sich die Frage, ob Unternehmen eine besondere unternehmerische Verantwortung für die Entwicklung und den Einsatz von digitalen Technologien

* Darius Ruff, LL.M.oec. ist wissenschaftlicher Mitarbeiter am Institut für Wirtschaftsrecht des Juristischen Bereichs der Martin-Luther-Universität Halle-Wittenberg. Er promoviert ebenda zur Corporate Digital Responsibility aus juristischer Perspektive. Grundlage dieses Beitrags ist eine wissenschaftliche Studienarbeit, die der Autor im November 2022 verfasste. Für die Betreuung der Arbeit und die Ermöglichung dieser Veröffentlichung dankt der Autor Frau Prof. Dr. Anne-Christin Mittwoch herzlichst. Für diese Veröffentlichung wurde der Text zum Stichtag 1.12.2023 aktualisiert.

** Die in diesem Beitrag verwendeten Personenbezeichnungen beziehen sich, soweit nicht anders kenntlich gemacht, gleichberechtigt auf alle Geschlechter. Der Beitrag bemüht sich um geschlechtsneutrale Formulierungen. Auf eine Doppelnennung wird zugunsten einer besseren Lesbarkeit verzichtet.

zukommt und welchen Inhalt diese Verantwortung hat. Die Rede ist von einer *Corporate Digital Responsibility* (kurz: CDR). Dieser vergleichsweise neue Verantwortungsterminus ist bislang vor allem in der wirtschaftswissenschaftlichen Literatur diskutiert worden, weshalb hier bereits vielfältige Analysen existieren. Juristische Betrachtungen von CDR sind dagegen noch rar, welches wohl auch dem Umstand geschuldet ist, dass es sich um eine grundsätzlich freiwillige Verantwortung von Unternehmen handelt. Diese Arbeit soll den juristischen Debattenbeitrag ausbauen und ins Blickfeld nehmen, in welchem bestehenden und zukünftigen Rechtsrahmen sich eine digitale Unternehmensverantwortung bewegt.

Hierzu soll CDR in einem ersten Schritt inhaltlich und akteursbezogen erörtert werden (§ 2). In einem zweiten Schritt wird digitale Unternehmensverantwortung im Lichte des aktuellen und sich entwickelnden digital- und datenrechtlichen Regulierungsrahmens untersucht (§ 3). Im Anschluss werden die Rolle der Corporate Digital Responsibility im Kontext eines entstehenden Datenrechts beleuchtet und mögliche zukünftige Wege einer rechtlichen Implementierung von CDR aufgezeigt (§ 4).

§ 2 Corporate Digital Responsibility

Der Begriff *Corporate Digital Responsibility* wird erstmals 2015 in einer Veröffentlichung der Unternehmensberatung Accenture[1] verwendet und lässt sich sinngemäß als „digitale Unternehmensverantwortung" oder „unternehmerische Digitalverantwortung"[2] übersetzen. Wichtig ist, dass nicht eine *digital wahrgenommene* Verantwortung eines Unternehmens gemeint ist, sondern seine (umfassende) und freiwillige Verantwortung für die Entwicklung, den Einsatz und die damit verbundenen Auswirkungen von digitalen Technologien und Anwendungen.[3] Im deutschen Raum wurde der CDR-Begriff ab 2018 durch die „CDR-Initiative" des Bundesministeriums für Justiz und Verbraucherschutz[4] geprägt. Die Initiative hat das Ziel,

1 Cooper/Siu/Wei, Corporate Digital Responsibility, 2015, S. 1; zur Genese des Begriffs auch Möslein FS Hopt, 2020, 805 (806).

2 Vgl. dazu https://csr-news.org/2018/06/20/corporate-digital-responsibility/ (Stand 1.12.2023).

3 Zu den Begriffsdefinitionen von Corporate Digital Responsibility → § 2 B.

4 Zur Corporate Digital Responsibility-Initiative, aktuell im Ressortbereich des Bundesministeriums für Umwelt, Naturschutz, nukleare Sicherheit und Verbraucherschutz (BMUV), siehe den Webauftritt https://cdr-initiative.de (Stand 1.12.2023). An der

„digitale Verantwortung" branchenübergreifend in Unternehmen zu implementieren.[5] Die Dichte an wissenschaftlicher Literatur zu CDR nimmt – wohl auch vor diesem Hintergrund – seit 2018 stark zu. Da es sich bei CDR um ein vergleichsweise neues Konzept handelt, werden zunächst die Beweggründe für eine digitale Unternehmensverantwortung erörtert (A.). Nachfolgend werden aktuelle Begriffsdefinitionen vorgestellt (B.) und die CDR in den Kontext verwandter Konzepte eingeordnet, besonders der Corporate Social Responsibility und Digitalethik (C.). Schließlich werden die Handlungsformen, Akteure und die konkreten Inhalte der CDR dargelegt (D.).

A. CDR als freiwillige Unternehmensverantwortung

Eine wichtige Ausgangsfrage für eine freiwillige digitale Unternehmensverantwortung ist, aus welchen Gründen sich einerseits Unternehmen einer über den regulatorischen Rahmen hinausgehenden Verantwortung stellen und andererseits staatliche Initiativen freiwillige Verantwortungskonzepte entwickeln und fördern. Dies soll hier mit Fokus auf CDR-spezifische Beweggründe erfolgen.

Der verantwortungsvolle Umgang mit digitalen Technologien kann für Unternehmen in erster Linie betriebswirtschaftlich motiviert sein. So wird in einer nach außen kommunizierten, digitalen Unternehmensverantwortung regelmäßig ein Wettbewerbsvorteil für Unternehmen gesehen, weil diese eine Distinktion von Wettbewerbern ermögliche und deshalb letztendlich wirtschaftlich vorteilhaft sei.[6] Wettbewerbliche Distinktion ist dabei sowohl im nationalen wie auch im internationalen Zusammenhang denkbar. Im internationalen Rahmen wird in CDR deshalb auch die Chance für einen werteorientierten „europäischen Weg der Digitalisierung" gesehen,

CDR-Initiative nehmen mehrere große Unternehmen teil, ua die Otto Group, Zalando, Telefónica, Deutsche Telekom, ING DiBa und Barmer.

5 Vgl. dazu https://cdr-initiative.de/initiative (Stand 1.12.2023).

6 Diese Motivation wird durch eine Studie des Zentrum Digitalisierung.Bayern aus dem Jahr 2019 belegt, in der teilnehmende Unternehmen angaben, dass sie sich *„durch eine nach außen sichtbare ‚gelebte Verantwortung' eine Verbesserung ihrer Wettbewerbsposition"* erhoffen, vgl. Esselmann/Golle/Thiel/Brink, Corporate Digital Responsibility, 2020, S. 10; ebenfalls Cooper/Siu/Wei, Corporate Digital Responsibility, 2015, S. 4; Mueller Bus Inf Syst Eng 64 (2022), 689 (690); Möslein FS Hopt, 2020, 805 (808).

der sich vom liberalen, technikzentrierten Digitalisierungsverständnis in den USA bzw. dem restriktiven, staatszentrierten in China unterscheidet.[7]

Durch den verantwortungsvollen Umgang mit digitalen Technologien können Unternehmen das Vertrauen von Kunden und anderer Stakeholder (zB Mitarbeitende, Geschäftspartner) in das jeweilige Unternehmen bzw. seine (digitalen) Produkte und Dienstleistungen fördern.[8] Dies wird ua durch eine repräsentative Verbraucherbefragung in Deutschland aus dem Jahr 2021 belegt: In dieser gab nur etwa ein Drittel der Befragten an, dass der Umgang deutscher Unternehmen mit der Digitalisierung aktuell „eher oder sehr verantwortungsvoll" sei.[9] Zugleich gaben 70 % der Befragten an, dass ihnen die Übernahme einer digitalen Verantwortung durch Unternehmen „eher oder sehr wichtig" sei und einer noch größeren Mehrheit (78 %) war die Vertrauenswürdigkeit der Anbieter „eher oder sehr wichtig".[10] Die gelebte digitale Verantwortung eines Unternehmens und ein darauf aufbauendes Kundenvertrauen kann deshalb sowohl Unterscheidungsmerkmal zum Wettbewerb, als auch konstitutiv für den Erfolg eines Produkts oder einer Dienstleistung sein.[11] Wirtschaftliche Beweggründe können jedoch auch (vollständig) im Hintergrund stehen, wenn eine digitale Verantwortung aus ethischen und philanthropischen Überzeugungen der Unternehmensleitung bzw. der Mitarbeitenden wahrgenommen wird.[12]

Für staatliche Institutionen – zB bei der deutschen „CDR-Initiative" das Bundesministerium für Umwelt, Naturschutz, nukleare Sicherheit und Verbraucherschutz (BMUV) – ist die Förderung einer digitalen Unternehmensverantwortung von Interesse, weil einzelne Staaten nur bedingt in der

7 Esselmann/Golle/Thiel/Brink, Corporate Digital Responsibility, 2020, S. 10; Bertelsmann Stiftung Unternehmensverantwortung/Esselmann/Brink/Golle S. 249 (250); Noack ZHR 183 (2019), 105 (113).

8 Dörr Praxisleitfaden CDR S. 28ff.; Brandenburg/Waurick RDi 2023, 365f.; Herden et al. NachhaltigkeitsManagementForum 29 (2021), 13; Möslein FS Hopt, 2020, 805 (808); Bertelsmann Stiftung Unternehmensverantwortung/Kemmer S. 80 (83f.).

9 Kettner/Thorun, Corporate Digital Responsibility-Verbraucherbefragung, 2021, S. 4.

10 Kettner/Thorun, Corporate Digital Responsibility-Verbraucherbefragung, 2021, S. 4, 6; ähnlicher Befund bei einer Befragung im Jahr 2018, vgl. Thorun/Kettner/Merck, Ethik in der Digitalisierung, 2018, S. 2.

11 Esselmann/Golle/Thiel/Brink, Corporate Digital Responsibility, 2020, S. 8, 10; Herden et al. NachhaltigkeitsManagementForum 29 (2021), 13; ausführlich: Bertelsmann Stiftung Unternehmensverantwortung/Suchanek S. 17 (18f.); Bertelsmann Stiftung Unternehmensverantwortung/Kemmer S. 80 (83f.).

12 Herden et al. NachhaltigkeitsManagementForum 29 (2021), 13 (17); Mueller Bus Inf Syst Eng 64 (2022), 689 (692); zurückhaltend Dürr ZGE 2021, 165 (168).

Lage sind, große Digitalunternehmen bzw. digitale Anwendungen effektiv zu regulieren.[13] Hierfür gibt es zwei zentrale Gründe: Digitale Anwendungen zeichnen sich einerseits durch ihre Ubiquität bzw. Non-Territorialität aus, sind also potentiell weltweit zeitlich und örtlich unbegrenzt nutzbar.[14] Andererseits sind diese durch eine hohe Entwicklungs- und Innovationsgeschwindigkeit geprägt.[15] Eine effektive staatliche Regulierung steht damit vor der Herausforderung, dass sich Regulierungssubjekte und -objekte schnell verändern und sich zudem regelmäßig nicht im unmittelbaren staatlichen Zugriffsbereich (sondern „im digitalen Raum") befinden. Insofern ist treffend, dass *„der gesellschaftliche Veränderungsprozess der Digitalisierung rechtliche Lücken [provoziert]"*.[16] In der Konsequenz gewinnen freiwillige Steuerungs- und Selbstregulierungsmechanismen an Bedeutung.[17]

B. Definition von Corporate Digital Responsibility

Bei CDR handelt es sich um ein neueres Konzept unternehmerischer Verantwortung, eine „offizielle" Definition existiert bislang nicht. Deshalb ist für die inhaltliche Bestimmung und Abgrenzung eine Begriffsdefinition essentiell. Daher werden zunächst verschiedene Definitionen von CDR vorgestellt, um daraus wichtige Wesensmerkmale von CDR abzuleiten.

Die „CDR-Initiative" des BMUV versteht unter CDR *„freiwillige unternehmerische Aktivitäten, die [...] über das heute gesetzlich Vorgeschriebene hinausgehen und die digitale Welt aktiv zum Vorteil der Gesellschaft mitgestalten."*[18] CDR könne insofern zu einer nachhaltigen Entwicklung beitragen und sei *„Teil einer umfassenden Unternehmensverantwortung."*[19] Letzteres greift auch die Definition des Nachhaltigkeitsnetzwerks der deutschen

13 Dürr ZGE 2021, 165 (171f.); Esselmann/Golle/Thiel/Brink, Corporate Digital Responsibility, 2020, S. 6; Hoffmann-Riem Recht im Sog der digitalen Transformation S. 79ff., 124; zur Rolle von digitalen Plattformen als private Gesetzgeber: Schweitzer ZEuP 2019, 1 (4ff.).

14 Boehme-Neßler Unscharfes Recht S. 102ff., 112ff.; Dürr ZGE 2021, 165 (171); Esselmann/Golle/Thiel/Brink, Corporate Digital Responsibility, 2020, S. 6.

15 Dörr Praxisleitfaden CDR S. 9f.; Dürr ZGE 2021, 165 (171f.); Lobschat et al. Journal of Business Research 122 (2021), 875 (876).

16 So Dürr ZGE 2021, 165 (171).

17 Dürr ZGE 2021, 165 (171); ausführlich: Hoffmann-Riem Recht im Sog der digitalen Transformation S. 124ff., zu den Handlungsformen im Einzelnen → § 2 D. I.

18 BMUV, Corporate Digital Responsibility-Kodex, 2021, S. 2.

19 BMUV, Corporate Digital Responsibility-Kodex, 2021, S. 2.

Wirtschaft auf, laut dem CDR *„ein Teil der unternehmerischen Verantwortung [ist], welcher die Auswirkungen der digitalen Transformation auf Umwelt, Gesellschaft und Wirtschaft berücksichtigt."*[20] Diese Betrachtungstrias nennen auch andere, die CDR als *„eine Reihe von Praktiken und Verhaltensweisen, die einem Unternehmen helfen, Daten und digitale Technologien auf eine Weise zu nutzen, die als sozial, wirtschaftlich und ökologisch verantwortungsvoll wahrgenommen wird"*, definieren.[21] In weiteren Definitionen wird eine ethische Dimension eingeführt, wenn CDR als *„eine Erweiterung der Verantwortung eines Unternehmens, die die ethischen Chancen und Herausforderungen der Digitalisierung berücksichtigt"*[22] beschrieben wird. Auch der Bundesverband der Digitalwirtschaft (BVDW) greift dies auf und definiert CDR als *„freiwilligen Beitrag der Wirtschaft zu einer ethischen und nachhaltigen digitalen Entwicklung. [...] Ein wesentlicher Bestandteil der CDR ist die wertebasierte Auseinandersetzung mit positiven und negativen sowie direkten und indirekten Auswirkungen des Einsatzes digitaler Technologien."*[23] Nach dem Rahmenwerk „CDR Building Bloxx" des BVDW befasst sich CDR *„mit der Rolle unternehmerischer Verantwortung in einer zunehmend digitalisierten Welt"* und geht *„dabei oft über bestehende regulatorische Anforderungen hinaus und erforder[t] proaktive Selbstverpflichtungsmaßnahmen."*[24]

Die Definitionen zeigen, dass es sich bei CDR (noch) um einen weiten und pluriformen Begriff handelt, den unterschiedliche Akteure verschiedenartig ausfüllen und „betonen".[25] Dennoch wiederholen sich in den Defi-

20 Econsense, Umsetzung digitaler Verantwortung in Unternehmen, 2020, S. 8.

21 Internationales CDR Manifesto, vgl. dazu https://corporatedigitalresponsibility.net/cdr-definition-german (Stand 1.12.2023).

22 Herden et al. NachhaltigkeitsManagementForum 29 (2021), 13 (17) [Übersetzung des Verfassers aus dem Englischen].

23 Vgl. dazu https://www.bvdw.org/der-bvdw/gremien/corporate-digital-responsibility/cdr-building-bloxx/ (Stand 15.11.2022).

24 Vgl. dazu https://www.cdr-building-bloxx.com/corporate-digital-responsibility/ (Stand 1.12.2023).

25 Diesen Befund teilen auch Dörr Praxisleitfaden CDR S. 38; Brandenburg/Waurick RDi 2023, 365; Herden et al. NachhaltigkeitsManagementForum 29 (2021), 13 (16f.) mit einer Übersicht über weitere Definitionen; Lobschat et al. Journal of Business Research 122 (2021), 875 (886); Panzer-Heemeier/Nemat CCZ 2022, 223 (227); Mueller Bus Inf Syst Eng 64 (2022), 689 (692); Hamadi/Manzo, Corporate Digital Responsibility, 2021, S. 10ff.; Panzer-Heemeier/Nemat/Meckenstock ESG 2022, 104 (106); laut Möslein FS Hopt, 2020, 805 (812) hat CDR aufgrund seiner Datenbezogenheit bereits eine „Kontur".

nitionen charakteristische Merkmale, die zu einer Begriffstopoi zusammengefasst werden können und aus der sich der Kern der CDR ableiten lässt:

- Es handelt sich um grundsätzlich freiwillige Unternehmensverantwortung.
- Die Verantwortung umfasst die (strikte) Einhaltung der gesetzlichen Vorgaben, geht aber inhaltlich über das gesetzlich vorgeschriebene hinaus.
- Die Verantwortung betrifft Digitalisierungsprozesse, insb. die Entwicklung und den Einsatz von digitalen Technologien in Unternehmen und deren Auswirkungen ggü. Stakeholdern und im gesellschaftlichen Kontext.
- Es werden die wirtschaftlichen, sozialen und ökologischen Auswirkungen von digitalen Technologien in den Blick genommen, weshalb CDR einen engen Bezug zu Nachhaltigkeitszielen hat.
- Im Fokus steht eine ethisch-moralische, wertorientierte Betrachtung des Unternehmenshandelns und dessen (Weiter-)Entwicklung.
- Die Digitalverantwortung ist eingebettet in einen breiteren Zusammenhang gesellschaftlicher Unternehmensverantwortung, namentlich Corporate Responsibility bzw. Corporate Social Responsibility (CSR).

Aus den letzten zwei Merkmalen geht hervor, dass CDR bestehende Konzepte der (Digital-)Ethik und andere Formen der unternehmerischen Verantwortung aufgreift. Daraus folgt die Frage, in welcher Beziehung die CDR zu diesen Konzepten steht.

C. Konzeptuelle Hintergründe

Zu diesem Zweck wird CDR in den Kontext der gesellschaftlichen Unternehmensverantwortung (I.) und der digitalen Ethik (II.) eingeordnet.

I. Corporate Social Responsibility (CSR)

Im Zuge von veränderten Erwartungen der Gesellschaft an Unternehmen entwickelte sich in den letzten Jahrzehnten sukzessive das Konzept der

CSR.[26] Auch wenn bis heute keine einheitliche Definition existiert,[27] handelt es sich laut der Europäischen Kommission bei der CSR um ein *„Konzept, das den Unternehmen als Grundlage dient, auf freiwilliger Basis soziale Belange und Umweltbelange in ihre Unternehmenstätigkeit und in die Wechselbeziehungen mit den Stakeholdern zu integrieren"*,[28] bzw. nach neuerer und erweiterter Definition *„die Verantwortung von Unternehmen für ihre Auswirkungen auf die Gesellschaft"*.[29] Mit dem Begriff eng verbunden ist das Prinzip der Nachhaltigkeit bzw. des nachhaltigen Wirtschaftens.[30]

Als grundsätzlich freiwilliges Verantwortungsformat wurde CSR zunächst durch unverbindliche Instrumentarien eingefasst, denen sich Unternehmen anschließen konnten.[31] Hierzu gehören ua der UN Global Compact,[32] die OECD-Leitsätze für multinationale Unternehmen[33] oder Standards der Internationalen Arbeitsorganisation[34]. Im jüngeren Verlauf wurden Inhalte der CSR in rechtliche Regelungen überführt, so zB 2014 in der EU-Richtlinie über nichtfinanzielle Berichterstattung.[35] In der Folge

26 Zur Genese verschiedener CSR-Konzeptionen ausführlich Spießhofer Unternehmerische Verantwortung S. 54ff.; mit einer rechtlichen Betrachtung Mittwoch Nachhaltigkeit und Unternehmensrecht S. 165ff.

27 Mittwoch Nachhaltigkeit und Unternehmensrecht S. 164 mwN; Spießhofer Unternehmerische Verantwortung S. 27ff. mit diversen CSR-Definitionen.

28 Definition der EU-Kommission von 2001, vgl. Grünbuch Europäische Rahmenbedingungen für die soziale Verantwortung der Unternehmen vom 18.7.2001, KOM(2001) 366 endgültig, 7.

29 Definition der EU-Kommission von 2011, vgl. Eine neue EU-Strategie (2011–14) für die soziale Verantwortung der Unternehmen (CSR) vom 25.10.2011, KOM(2011) 681 endgültig, 7.

30 Mittwoch Nachhaltigkeit und Unternehmensrecht S. 163f.; Teicke CCZ 2018, 274; ebenso die CSR-Initiative des Bundesministeriums für Arbeit und Soziales, vgl. dazu: https://www.csr-in-deutschland.de/DE/CSR-Allgemein/CSR-Grundlagen/csr-grundlagen.html (Stand 1.12.2023).

31 Teicke CCZ 2018, 274; Mittwoch Nachhaltigkeit und Unternehmensrecht S. 167ff.

32 Der UN Global Compact ist eine weltweite Initiative für verantwortungsvolle Unternehmensführung in den Bereichen Menschenrechte, Arbeit, Umwelt und Korruptionsbekämpfung, vgl. dazu https://www.unglobalcompact.org/what-is-gc (Stand 1.12.2023).

33 Die OECD-Leitsätze bieten umfassende Verhaltensregeln zur Förderung von verantwortungsvoller Unternehmensführung, vgl. dazu https://doi.org/10.1787/9789264122352-de (Stand 1.12.2023).

34 So ua die Kernarbeitsnormen der Internationalen Arbeitsorganisation, vgl. dazu https://www.ilo.org/berlin/arbeits-und-standards/kernarbeitsnormen/lang--de/index.htm (Stand 1.12.2023).

35 RL 2014/95/EU; die Richtlinie wurde in Deutschland umgesetzt mit dem Gesetz zur Stärkung der nichtfinanziellen Berichterstattung der Unternehmen in

sind heute bestimmte Unternehmen zu nichtfinanziellen Erklärungen über Umwelt-, Arbeitnehmer- und Sozialbelange sowie zu Menschenrechten und zur Korruptionsbekämpfung verpflichtet, vgl. § 289b und § 289c HGB. Auch mit Blick auf die neue EU-Richtlinie zur Nachhaltigkeitsberichterstattung von Unternehmen aus dem Jahr 2022 ist das CSR-Konzept von einer weiteren Verrechtlichung geprägt.[36]

Gemeinsam ist CDR und CSR die Verantwortung von Unternehmen für gesellschaftlich eingeforderte, gemeinwohlorientierte Belange und die Aufnahme von Verantwortungsdimensionen, die neue gesellschaftliche Problemfelder bzw. Modernisierungsfolgen betreffen (ökologische wie digitale Transformation). Anders als bei CDR handelt es sich bei CSR aber um ein bereits gewachsenes und institutionalisiertes Konzept. Es stellt sich folglich die Frage, welcher Zusammenhang zwischen CDR und CSR besteht und weshalb mit CDR ein eigenes Verantwortungsformat etabliert wird.

Die Notwendigkeit eines neuen, erweiterten Verantwortungsformats als CDR wird insb. mit den besonderen Herausforderungen und Charakteristika der digitalen Transformation und Technologien begründet.[37] Diese soll CDR explizit und fokussiert adressieren und die klassischen drei Perspektiven der CSR (wirtschaftlich, sozial, ökologisch) erweitern.[38] Es besteht dabei weitgehend Konsens, dass CDR strukturell und konzeptionell ähnlich zur CSR ist und Schnittmengen bestehen.[39] Uneinigkeit besteht jedoch darüber, inwieweit CDR als spezieller Bestandteil oder als eigenständiges Konzept neben CSR zu betrachten ist. So wird teilweise argumentiert,

---

ihren Lage- und Konzernlageberichten (CSR-Richtlinie-Umsetzungsgesetz) vom 11.4.2017 (BGBl. I 802); Verweise auf CSR finden sich in Erwägungsgrund Nr. 3 RL 2014/95/EU und BT-Drs. 18/9982, 26; insgesamt dazu Mittwoch Nachhaltigkeit und Unternehmensrecht S. 165f., 180ff.; Spießhofer Unternehmerische Verantwortung S. 277f.; Panzer-Heemeier/Nemat CCZ 2022, 223 (224f.); Spießhofer NZG 2018, 441 (443, 445); Teicke CCZ 2018, 274 (275).

36 RL (EU) 2022/2464; vgl. Mittwoch Nachhaltigkeit und Unternehmensrecht S. 184f.

37 Dürr ZGE 2021, 165 (172f.); Lobschat et al. Journal of Business Research 122 (2021), 875 (876); Mihale-Wilson et al. Bus Inf Syst Eng 64 (2022), 127 (128); eine umfangreiche Quellenübersicht gibt es bei Hamadi/Manzo, Corporate Digital Responsibility, 2021, S. 23ff.

38 Dörr Praxisleitfaden CDR S. 39; Dürr ZGE 2021, 165 (172f.); so auch die CSR-Initiative des Bundesministeriums für Arbeit und Soziales, vgl. dazu https://www.csr-in-deutschland.de/DE/CSR-Allgemein/Corporate-Digital-Responsibility/corporate-digital-responsibility.html (Stand 1.12.2023); zu den Wechselwirkungen von Digitalisierung und Nachhaltigkeit vgl. Mittwoch JZ 2023, 376 (381ff.).

39 Vgl. Lobschat et al. Journal of Business Research 122 (2021), 875 (876); Mihale-Wilson et al. Bus Inf Syst Eng 64 (2022), 127 (129).

dass CDR aufgrund der Besonderheiten der Digitalisierung ausdrücklich getrennt von CSR betrachtet werden müsse.[40] Demgegenüber erweitern andere Autoren CSR um Digitalisierungsthemen (letzteres als „CDR"), zB indem das dreigliedrige CSR-Modell für wirtschaftliche, soziale und ökologische Belange um eine vierte Dimension des „digitalen" ergänzt wird.[41] Vorzugswürdig erscheint jedoch eine integrierte Betrachtung, in der die Verantwortung für wirtschaftliche, soziale und ökologische Belange einerseits auf analoge, andererseits auf digitale Handlungsfelder (CDR) bezogen erfolgt.[42] Diese spiegelt richtigerweise wider, dass die Auswirkungen der Digitalisierung gerade die drei Perspektiven – wirtschaftlich, sozial, ökologisch – betreffen und sich in diese einordnen lassen. Zudem widerspräche die Abtrennung des „Digitalen" der fortschreitenden Integration von analoger und digitaler Welt.[43] Gleichermaßen spricht der CDR-Kodex von CDR als *„Teil einer umfassenden Unternehmensverantwortung."*[44]

Die genaue Abgrenzung muss für die vorliegende Themenfrage nicht entschieden werden und ist aufgrund des geringen Konkretisierungsgrads der CDR aktuell noch schwierig. Dennoch handelt es sich dabei zukünftig nicht nur um eine begriffliche Kontroverse, sondern um eine relevante Frage: Betrachtet man CDR als integriertes bzw. spezielles Konzept der CSR könnten oder müssten CDR-Thematiken (auch) über das „Vehikel" der CSR zur Anwendung gebracht werden. Geht man dagegen von einem eigenständigen Konzept aus, könnten Digitalisierungsthemen unter Umständen aus einer klassischen CSR-Betrachtung herausfallen. Dies kann zB mit Blick auf Pflichten zur nichtfinanziellen Berichterstattung von Unternehmen zukünftig zu einer (rechtlich) relevanten Unterscheidung führen. Zu denken ist an die Berichterstattungspflichten in § 289c HGB oder aus der europäischen Richtlinie zur Unternehmens-Nachhaltigkeitsbericht-

40 Lobschat et al. Journal of Business Research 122 (2021), 875 (876); wohl ebenfalls Mihale-Wilson et al. Bus Inf Syst Eng 64 (2022), 127 (128).

41 Esselmann/Golle/Thiel/Brink, Corporate Digital Responsibility, 2020, S. 5; auch Thorun/Kettner/Merck, Ethik in der Digitalisierung, 2018, S. 2.

42 So auch Dörr Praxisleitfaden CDR S. 39f.; Herden et al. NachhaltigkeitsManagement-Forum 29 (2021), 13 (14); Bertelsmann Stiftung Unternehmensverantwortung/Kemmer S. 80 (81).

43 Dörr hebt hervor, dass sich die „Wirkungen digitalen Handelns" auch in der physischen Welt niederschlagen können und eine Wechselbeziehung zwischen digitaler und analoger Welt besteht, vgl. Dörr Praxisleitfaden CDR S. 39.

44 BMUV, Corporate Digital Responsibility-Kodex, 2021, S. 2.

erstattung, die aktuell aber beide keine Unterscheidung zwischen digitalem und physischem Unternehmenshandeln treffen.[45]

Es lässt sich festhalten, dass CDR sowohl inhaltlich als auch konzeptionell deutliche Verbindungen zur CSR aufweist. Durch die Fokussierung auf digitale Technologien und ihre Auswirkungen werden mit CDR themen- und verantwortungsspezifische Problemfelder adressiert und für diese ein eigenständiger unternehmerischer Handlungsrahmen geschaffen. Strategisch gesehen ist eine ganzheitliche Unternehmensverantwortung, die klassische CSR und CDR-Themen verbindet, sicher erstrebenswert. Dies folgt aus praktischen Überlegungen zur Integration in Managementaufgaben und Unternehmensstrukturen, bei denen parallele Verantwortungskonzepte Zielkonflikte verursachen und die Integration erschweren können. Zudem kann die Verteilung von Verantwortung auf mehrere Funktionsstellen zu einer diffusen Verantwortungsfestlegung führen und die internen Transaktionskosten erhöhen. Auf der anderen Seite ist jedoch auch das konkrete Betätigungsfeld des Unternehmens zu betrachten: Für ausgeprägt digital getriebene Unternehmen sollte digitale Verantwortung sowohl zentral-integriert wie auch dezentral-prozessbezogen implementiert werden,[46] wohingegen bei weniger digitalisierten Unternehmen eine zentral-integrierte Verantwortung notwendige Anforderungen erfüllen sollte.

II. Digitale Ethik

Corporate Digital Responsibility hat weiterhin starke konzeptionelle Wurzeln in der digitalen Ethik bzw. Datenethik.[47] Die Daten- bzw. Digitalethik

45 RL (EU) 2022/2464; zu CDR und der nichtfinanziellen Berichterstattung Merbecks BB 2021, 2159 (2161ff.) und Brandenburg/Waurick RDi 2023, 365 (367); auch in der aktuellen Fassung der Empfehlungen der Regierungskommission Deutscher Corporate Governance Kodex (DCGK) vom 28.04.2022, zu denen sich börsennotierte Gesellschaften gemäß § 161 AktG erklären müssen, gibt es keine Bezugnahme auf eine digitale Verantwortung, vgl. dazu https://www.dcgk.de//files/dcgk/usercontent/de/download/kodex/220627_Deutscher_Corporate_Governance_Kodex_2022.pdf (Stand 1.12.2023); dazu Möslein FS Hopt, 2020, 805 (819); zur perspektivischen Aufnahme von CDR in den DCGK Noack ZHR 183 (2019), 105 (113).

46 In diese Richtung auch Pauly/Wichert DB-Beil. Heft 21/2023, 44; Mihale-Wilson et al. Bus Inf Syst Eng 64 (2022), 127 (129) grenzt die Perspektiven von CSR und CDR ua daran ab, ob es um untechnisch-strategische Managemententscheidungen oder konkretere (informations)technische Gestaltungen und Best Practices geht.

47 Vgl. Bahreini/Charton/Lukas RDi 2021, 548 (549); Bertelsmann Stiftung Unternehmensverantwortung/Esselmann/Brink/Golle S. 249 (250); Lobschat et al. Journal of

untersucht und bewertet *„moralische Probleme im Zusammenhang mit Daten [...], Algorithmen [...] und entsprechenden Praktiken (einschließlich verantwortungsvoller Innovation, Programmierung, Hacking und Berufskodizes), um moralisch richtige Lösungen [...] zu formulieren und zu unterstützen.“*[48]

Als zentraler Überschneidungspunkt von digitaler Ethik und CDR ergibt sich folglich der Betrachtungsgegenstand, also Daten, Algorithmen und dazugehörige (Unternehmens-)Praktiken sowie die in Bezug darauf formulierten Sollens-Sätze. Des Weiteren sind ethisch-moralische Überlegungen ein anerkannter Maßstab, um Verhalten und Handlungen zu bewerten. Somit können ethisch-moralische Überlegungen relativ unproblematisch zur Entwicklung, Argumentation und Legitimation von handlungsleitenden Sollens-Sätzen (einer CDR) herangezogen werden, auch in Ermangelung oder jenseits von rechtlichen Sollens- und Müssens-Sätzen.[49] Diese inhärente Verbindung von digitaler Verantwortung und digitaler Ethik spiegelt sich in den og Definitionen von CDR und in der Literatur wider.[50] Der CDR-Kodex ist ebenfalls von einer Wert- und Prinzipienorientierung geprägt, die zielsetzungs- und handlungsleitend sein soll und ua auf eine Menschzentrierung, Autonomie, Fairness und Transparenz aufbaut.[51]

Business Research 122 (2021), 875 (876, 879); Mueller Bus Inf Syst Eng 64 (2022), 689 (690f.); Panzer-Heemeier/Nemat/Meckenstock ESG 2022, 104 (106); Thorun/Kettner/Merck, Ethik in der Digitalisierung, 2018, S. 2f.; ausführlich: Dörr Praxisleitfaden CDR S. 30ff.; zu ethischen Fragen der Digitalisierung und insofern Anwendungsbereichen der digitalen Ethik: Schliesky NJW 2019, 3692 (3695ff.).

48 Floridi/Taddeo Phil. Trans. R. Soc A 374 (2016), 20160360 S. 3 [Übersetzung des Verfassers aus dem Englischen]; die digitale Ethik bzw. Datenethik baut ihrerseits wieder auf der Computer- und Informationsethik auf, vgl. Floridi/Taddeo Phil. Trans. R. Soc A 374 (2016), 20160360 S. 2f.

49 Panzer-Heemeier/Nemat CCZ 2022, 223 (227); für Bahreini/Charton/Lukas RDi 2021, 548 (548f.) geht der Inhalt von digital-ethischen Leitlinien in Unternehmen über rechtliche Inhalte hinaus bzw. können diese rechtliche Lücken füllen; zum Verhältnis von Recht und Ethik siehe Schliesky NJW 2019, 3692 (3694f.).

50 Vgl. Bahreini/Charton/Lukas RDi 2021, 548 (549); Bertelsmann Stiftung Unternehmensverantwortung/Esselmann/Brink/Golle S. 249 (250); Lobschat et al. Journal of Business Research 122 (2021), 875 (876, 879); Mueller Bus Inf Syst Eng 64 (2022), 689 (690f.); Panzer-Heemeier/Nemat/Meckenstock ESG 2022, 104 (106); Thorun/Kettner/Merck, Ethik in der Digitalisierung, 2018, S. 2f.; ausführlich: Dörr Praxisleitfaden CDR S. 30ff.; zu ethischen Fragen der Digitalisierung und insofern Anwendungsbereichen der digitalen Ethik: Schliesky NJW 2019, 3692 (3695ff.).

51 BMUV, Corporate Digital Responsibility-Kodex, 2021, S. 3; dazu Möslein FS Hopt, 2020, 805 (809f.).

CDR greift also zu ihrer inhaltlichen Ausrichtung und Gestaltung auf digital- bzw. datenethische Normen und Diskurse zurück. Dies zeigt, dass es sich bei CDR um ein interdisziplinäres Konzept an der Schnittstelle von unternehmerischer Verantwortung und digitaler Ethik handelt. Die Wert- bzw. Prinzipienorientierung ist dabei von großer Wichtigkeit. Zum einen gibt diese einer digitalen Unternehmensverantwortung einen normativen und legitimierenden Unterbau und zum anderen erleichtert dieser Rahmen die praktische Formulierung von kohärenten und konkreten Handlungszielen.[52]

D. Handlungsformen, Akteure und Handlungsfelder

Gleichermaßen vielfältig wie die Definitionen von CDR ist die Quellenlandschaft für ihre konkreten Inhalte. Im Folgenden wird daher zunächst beleuchtet, welche Handlungsformen abseits von hoheitlicher Rechtssetzung für CDR zur Verfügung stehen (I.). In einem zweiten Schritt werden konkrete Akteure der CDR und ihre Handlungsformen vorgestellt (II.). Daran anschließend werden die Handlungsfelder der CDR konkretisiert (III.).

I. Handlungsformen nicht-hoheitlicher Normsetzung

Einer freiwilligen Normsetzung iRd Corporate Digital Responsibility liegen inhärent andere Handlungsformen zugrunde als hoheitlicher Normsetzung, die zuvorderst durch Gesetze und Verordnungen bzw. auf EU-Ebene durch Richtlinien und Verordnungen erfolgt → § 3. Davon unterscheiden sich die Erscheinungsformen von privater Regelsetzung.[53]

Im Bereich der Selbstregelung entwickeln die Akteure eigene Verhaltensregeln (etwa Selbstverpflichtungen oder Verhaltenskodizes), die ihre Geltung typischerweise nur im eigenen Wirkungskreis des jeweiligen Akteurs entfalten.[54] Demgegenüber wirkt die (gesellschaftliche) Selbstregulierung über den einzelnen regelsetzenden Akteur hinaus, weil auch andere Perso-

52 Schliesky NJW 2019, 3692 (3697).

53 Dazu Hoffmann-Riem Recht im Sog der digitalen Transformation S. 114ff.; spezifisch für CDR siehe Dürr ZGE 2021, 165 (173ff.).

54 Hoffmann-Riem Recht im Sog der digitalen Transformation S. 114, 116ff.; zur Rolle von digitalen Plattformen als private Gesetzgeber Schweitzer ZEuP 2019, 1 (4ff.).

nen die gesetzten Regeln für sich anerkennen.[55] Hierzu können zB technische Standards oder Verhaltenskodizes von Verbänden gehören, deren Missachtung mit einem Nachteil für den Abweichenden verbunden ist.[56] Schließlich kann eine Koregulierung vorliegen, wenn hoheitliche Stellen an der Gestaltung und Implementierung von selbstregulativ zustande gekommene Regeln mitwirken.[57] Im Folgenden wird sich zeigen, dass CDR in den verschiedenen Spielarten privater Regelsetzung in Erscheinung tritt.

II. Akteure der CDR und ihre Handlungsformen

1. Unternehmen

Als zentrale Akteure von CDR sind in erster Linie (große) Unternehmen zu nennen, sie sind Treiber und Adressaten zugleich. In ihrer Adressatenrolle geht es für Unternehmen zentral um die Frage, *wie* sie digitale Verantwortung übernehmen – welchen Inhalt hat die eigene Verantwortung, wie wird diese im Unternehmen implementiert und mit welchem Verbindlichkeitsgrad? Im Unternehmen lässt sich CDR grob auf drei Ebenen einordnen und realisieren.[58]

Zunächst geht es um die übergeordnete Bestimmung, welche grundsätzlichen Werte, Ziele und Strategien das Unternehmen leiten sollen.[59] Hierzu gehören interne Strategien und Leitlinien, aktuell meist für KI-Anwendungen oder Datenethik.[60] Diese müssen dann in einer zweiten Stufe in kon-

55 Hoffmann-Riem Recht im Sog der digitalen Transformation S. 114, 118f.; teilweise wird in diesem Zusammenhang auch von Soft Law gesprochen, so Dürr ZGE 2021, 165 (176).

56 Hoffmann-Riem Recht im Sog der digitalen Transformation S. 118f.; Dürr ZGE 2021, 165 (176).

57 Hoffmann-Riem Recht im Sog der digitalen Transformation S. 115, 119f., weitere Begriffe sind „hybride Regulierung" oder „regulierte Selbstregulierung"; dazu ebenfalls Dürr ZGE 2021, 165 (174f.).

58 So Lobschat et al. Journal of Business Research 122 (2021), 875 (880ff.); ähnlich Esselmann/Brink Ökologisches Wirtschaften 33, 2 (2020), 11 (12).

59 Lobschat et al. Journal of Business Research 122 (2021), 875 (880).

60 Siehe zB Deutsche Telekom, Leitlinien für Künstliche Intelligenz, 2018, vgl. dazu https://www.telekom.com/resource/blob/544508/ca70d6697d35ba60fbcb29aeef4529e8/dl-181008-digitale-ethik-data.pdf; Telefónica S.A., Principles of Artificial Intelligence, 2018, vgl. dazu https://www.telefonica.com/en/wp-content/uploads/sites/5/2021/08/ia-responsible-governance.pdf; Merck KGaA, Code of Digital Ethics, 2021, zu letzterem ausführlich Bahreini/Charton/Lukas RDi 2021, 548 (549); Bosch, KI-Kodex, 2020, vgl. dazu https://www.bosch.com/de/stories/ethische-leitlinien-fu

krete Normen übersetzt werden, um für den Einzelnen und die Anwendung im Unternehmen handhabbar zu werden.[61] Auf einer dritten Ebene zeigt sich die übernommene Verantwortung anhand konkreter und vielgestaltiger Prozesse, Verhaltensweisen oder Objekte.[62] Dies können zB regelmäßige Pflichtschulungen von Mitarbeitenden, interne Qualitäts- und Controllingschleifen oder Handbücher sein. Die unternehmensspezifische Integration von CDR stellt somit einen Ausgangspunkt dar, um CDR inhaltlich zu gestalten und zu bestimmen.

Die formulierten selbstregelnden Leitlinien und Kodizes reflektieren die Normbildung innerhalb eines Unternehmens und treiben gleichzeitig die Ausformung von CDR voran. Auf die Normbildung wirken gleichzeitig verschiedene unternehmensexterne Akteure ein, sodass es sich um ein Wechselspiel von Unternehmen und weiterer Akteure handelt.[63] Hierzu gehören unternehmensübergreifende Initiativen,[64] in denen sich Unternehmen selbstregulierend zu verantwortlichem Handeln in der digitalen Welt verpflichten, sowohl explizit auf CDR als auch iwS auf die verantwortungsvolle Gestaltung der Digitalisierung bezogen. Im Rahmen der CDR-Initiative des BMUV verpflichten sich deutsche Unternehmen ua dazu, über ihr Engagement im Bereich von CDR zu berichten.[65] Erste Berichte wurden 2022 veröffentlicht[66] und ergänzen gesetzliche Berichtspflichten, in denen sich digitales Verantwortungshandeln bislang nicht ausdrücklich widerspiegelt.[67] Ein weiteres Beispiel ist die „Charta digitale Vernetzung" von 2014, die von mehr als 80 Institutionen unterschrieben wurde und deren Grund-

er-kuenstliche-intelligenz/; SAP, Leitlinien für KI, 2018 und Global AI Ethics Policy, 2022, vgl. dazu https://news.sap.com/germany/2022/03/kuenstliche-intelligenz-ethik/; eine Suchmaschine für KI-ethische Leitlinien bietet das AI Ethics Guidelines Global Inventory von Algorithm Watch vgl. dazu https://inventory.algorithmwatch.org (Stand für alle 1.12.2023).

61 Lobschat et al. Journal of Business Research 122 (2021), 875 (880ff.).

62 Lobschat et al. Journal of Business Research 122 (2021), 875 (882).

63 Ausführlich Lobschat et al. Journal of Business Research 122 (2021), 875 (883ff.); eine Übersicht über Stakeholder gibt Dörr Praxisleitfaden CDR S. 135ff.

64 Übersichten finden sich ua bei Dörr Praxisleitfaden CDR S. 139ff.; Econsense, Umsetzung digitaler Verantwortung in Unternehmen, 2020, S. 17ff.

65 BMUV, Corporate Digital Responsibility-Kodex, 2021, S. 9; im Detail vgl. dazu https://cdr-initiative.de/cdr-berichte (Stand 1.12.2023).

66 Die CDR-Berichte können online abgerufen werden, vgl. dazu https://cdr-initiative.de/cdr-berichte (Stand 1.12.2023).

67 Dazu → § 2 C. I.

sätze für eine *„verantwortungsvolle Gestaltung der digitalen Gesellschaft"*[68] teilweise mit Zielen der CDR übereinstimmen.[69] Schließlich wirken Unternehmen über die kommunikativ-strategische Mitarbeit in Verbänden, Foren und Think Tanks an der Ausgestaltung von digitaler Verantwortung mit.[70] Ferner sind Unternehmensberatungen zu nennen, die CDR und ihre unternehmensinterne Realisierung als Betätigungsfeld erkennen und Unternehmen dazu beraten.[71]

2. Politik, öffentliche und private Stakeholder

Wichtige unternehmensexterne Akteure sind öffentliche und private Stakeholder, die sich in Initiativen, Verbänden und Netzwerken zusammengeschlossen haben und – teilweise mit Unternehmen zusammen – digitale Unternehmensverantwortung aus verschiedenen Blickwinkeln untersuchen, ausgestalten und implementieren. Exemplarisch seien hier die CDR-Initiativen des BMUV,[72] des Bundesverbands Digitale Wirtschaft[73]

68 Idee und Entstehung der Charta digitale Vernetzung siehe https://charta-digitale-vernetzung.de/idee-und-entstehung/ (Stand 1.12.2023); dazu Nietsch CSR Compliance/Anzinger § 27 Rn. 18.

69 So zB mit Blick auf die Verantwortung für personenbezogene Daten, die Nutzbarmachung von Daten, Teilhabe und Digitalkompetenz, siehe Charta digitale Vernetzung, abrufbar unter: https://charta-digitale-vernetzung.de/die-charta-im-wortlaut/ (Stand 1.12.2023).

70 Das econsense – Forum Nachhaltige Entwicklung der Deutschen Wirtschaft e.V. hat 49 große Mitgliedsunternehmen und adressiert die CDR, vgl. dazu https://econsense.de/digitale-verantwortung/ (Stand 1.12.2023); der Bundesverband Digitale Wirtschaft hat ein Ressort für Digital Responsibility und die sog. CDR Building Bloxx als besondere CDR-Themenplattform des Verbands, vgl. dazu https://www.bvdw.org/gremien/digital-responsibility/ und https://www.cdr-building-bloxx.com/cdr-building-bloxx-framework/ (Stand 1.12.2023); mit weiteren Beispielen Nietsch CSR Compliance/Anzinger § 27 Rn. 17ff.; Dörr Praxisleitfaden CDR S. 140ff.

71 So zB Deloitte, vgl. dazu https://www2.deloitte.com/de/de/pages/innovation/contents/corporate-digital-responsibility.html; PricewaterhouseCoopers, vgl. dazu https://www.pwc.de/de/digitale-transformation/corporate-digital-responsibility-cdr.html; das ConPolicy-Institut, vgl. dazu https://www.conpolicy.de/themen/digitalisierung/, WiseWay, vgl. dazu https://wiseway.de/angebote/ (Stand 1.12.2023).

72 Vgl. dazu https://cdr-initiative.de/initiative (Stand 1.12.2023).

73 Der Bundesverband Digitale Wirtschaft hat ein Ressort für Digital Responsibility und die sog. CDR Building Bloxx als besondere CDR-Themenplattform des Verbands, vgl. dazu https://www.bvdw.org/gremien/digital-responsibility/ und https://www.cdr-building-bloxx.com/cdr-building-bloxx-framework/ (Stand 1.12.2023).

und des Zentrum Digitalisierung Bayern[74] genannt, das CDR Online-Magazin[75] oder das CDR Manifesto[76]. Diese Akteure wirken an der Gestaltung von CDR durch Kodizes, themenbezogene Veröffentlichungen, Positionspapiere und Rahmenwerke oder auch durch die Verleihung von Preisen mit („CDR Award"[77]). Im weiteren Zusammenhang sind auch Initiativen zu nennen, die sich mit den Herausforderungen der KI, der Digitalethik oder der Digitalisierung im Allgemeinen befassen. Auf Stakeholder-Seite ist dies zB die Bertelsmann Stiftung,[78] die AG Ethik der Initiative D21[79] oder die og „Charta digitale Vernetzung" und auf politischer Ebene die hochrangige Expertengruppe für Künstliche Intelligenz der Europäischen Kommission,[80] die Enquete-Kommission für KI[81] oder die Datenethikkommission der Bundesregierung[82].

Eine Studie im Jahr 2022 hat 91 digital-ethische Leitlinien in Europa zum verantwortungsvollen Umgang mit digitalen Anwendungen untersucht und stellte seit 2016 eine kontinuierliche Zunahme dieser fest.[83] Die Leitlinien werden demnach vor allem durch Non-Profit-Organisationen (42 %) und Unternehmen (33 %) herausgegeben,[84] welches die obige Beobachtung

74 Vgl. dazu https://www.bayern-innovativ.de/de/seite/corporate-digital-responsibility (Stand 1.12.2023).

75 Vgl. dazu https://corporate-digital-responsibility.de (Stand 1.12.2023).

76 Vgl. dazu https://corporatedigitalresponsibility.net/cdr-manifesto (Stand 1.12.2023).

77 Der CDR-Award wird vom Bundesverband Digitale Wirtschaft und der Innovationsplattform Bayern Innovativ ausgerichtet, vgl. dazu https://www.cdr-award.digital/ (Stand 1.12.2023).

78 Die Bertelsmann-Stiftung hat sich in einem Projekt mit der Unternehmensverantwortung im digitalen Zeitalter befasst, abrufbar unter https://www.bertelsmann-stiftung.de/de/unsere-projekte/betriebliche-arbeitswelt-digitalisierung/projektnachrichten/ein-debattenbeitrag-zu-corporate-digital-responsibility (Stand 1.12.2023).

79 Die AG-Ethik der Initiative D21 e.V. als „Netzwerk für die Digitale Gesellschaft" befasst sich mit verschiedenen digital-ethischen Fragestellungen, abrufbar unter: https://initiatived21.de/arbeitsgruppen/ag-ethik/ (Stand 1.12.2023).

80 Diese erarbeitete ua Ethik-Leitlinien für vertrauenswürdige KI (2019), Richtlinien und Investitionsempfehlungen für vertrauenswürdige KI (2019) und eine Bewertungsliste für vertrauenswürdige KI (2020), vgl. dazu https://digital-strategy.ec.europa.eu/de/policies/expert-group-ai (Stand 1.12.2023).

81 Die Kommission stellte ihren Abschlussbericht am 28.10.2020 vor, vgl. dazu https://www.bundestag.de/webarchiv/Ausschuesse/ausschuesse19/weitere_gremien/enquete_ki (Stand 1.12.2023).

82 Die Kommission stellte ihren Abschlussbericht am 23.10.2019 vor, vgl. dazu https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/it-digitalpolitik/gutachten-datenethikkommission.pdf (Stand 1.12.2023).

83 idigiT, Leitlinien zu digitaler Ethik in Europa, 2022, S. 5, 8.

84 idigiT, Leitlinien zu digitaler Ethik in Europa, 2022, S. 9.

stützt. Die Leitlinien sind mehrheitlich an Unternehmen adressiert (56 %) und betreffen vor allem algorithmische Systeme bzw. Künstliche Intelligenz (66 %) wie auch den Umgang mit Daten (34 %).[85]

3. Wissenschaft

Diese Aktivitäten werden schließlich durch wissenschaftliche Auseinandersetzungen eingefasst, welche das Konzept der CDR interdisziplinär und aus unterschiedlichen Blickwinkeln untersuchen. Hier sind insb. wirtschafts- und sozialwissenschaftliche Fachpublikationen zu nennen, die CDR ua für die Praxis in Unternehmen bzw. die Integration ins unternehmerische Handeln und das Management des Unternehmens aufbereiten.[86]

4. Zwischenfazit

Die zentralen Akteure sind also Unternehmen, staatliche Institutionen, Stakeholder-Gruppen und die Wissenschaft. Die Handlungsformen sind geprägt von Selbstregelung und gesellschaftlicher Selbstregulierung im erläuterten Sinne mit ua Leitlinien und Kodizes. Es zeigt sich, dass die Quellenlandschaft für die Inhalte von CDR vielfältig und bislang wenig konsolidiert ist, wobei es zwischen den Quellen wechselseitige Einflüsse gibt. Letzteres birgt die Chance für einen interdisziplinären und wissenschaftlich-praktischen Austausch über die Herausforderungen der Digitalisierung und eine darauf bezogene Unternehmensverantwortung, aber auch das Risiko, dass sich divergierende Verantwortungskonzepte herausbilden.

III. Handlungsfelder

Auf Grundlage der dargestellten Akteure und ihrer Beiträge werden nun Handlungsfelder von Corporate Digital Responsibility dargestellt.

85 idigiT, Leitlinien zu digitaler Ethik in Europa, 2022, S. 10f.

86 So insb. Dörr Praxisleitfaden CDR S. 21ff.; Lobschat et al. Journal of Business Research 122 (2021), 875ff.; Herden et al. NachhaltigkeitsManagementForum 29 (2021), 13ff.; Mueller Bus Inf Syst Eng 64 (2022), 689ff.; Hamadi/Manzo, Corporate Digital Responsibility, 2021, S. 3ff.; einen Überblick zum noch geringen juristischen Literaturbestand zu CDR gibt Dürr ZGE 2021, 165 (166 Fn. 2).

I. Umgang mit Daten

Zentrales Handlungsfeld von CDR ist der verantwortungsvolle Umgang mit Daten.[87] Dies ist Ausdruck der immensen Relevanz von Daten für digitale Anwendungen und Geschäftsmodelle sowie des großen Schutzbedürfnisses von personenbezogenen Daten, aus denen sich zB detaillierte Profile von Personen erstellen lassen.

Der unternehmerische Umgang mit Daten reicht vom Sammeln und Abspeichern (Stufe 1) über das Aufbereiten und Analysieren (Stufe 2) bis hin zum Zugänglichmachen, Weitergeben und ihrer Verwendung in Geschäftsentscheidungen (Stufe 3).[88] Verantwortungsvoller Umgang mit Daten lässt sich in den einzelnen Stufen in verschiedene Fragen und Zielsetzungen übersetzen, welche vielfach untrennbar mit datenschutzrechtlichen Fragestellungen verwoben sind:[89]

In der *ersten Stufe* kann CDR zB das Ziel verfolgen, Personen selbstbestimmte Einwilligungsentscheidungen zu ermöglichen, indem mithilfe von Symbolen oder Grafiken über die Datenschutzpolitik informiert wird oder Wahlmöglichkeiten eröffnet werden, wie und welche Daten verwendet werden.[90] Mit Blick auf die Speicherung von Daten ist auch die IT-Sicherheit von betrieblichen Infrastrukturen relevant, um Daten vor Diebstahl oder Manipulation zu schützen.[91]

In der *zweiten Stufe* kann CDR darauf abzielen, beim Einsatz von algorithmischen Systemen die *„Verzerrung von Datenanalysen"* durch sog. „Biases" zu mitigieren,[92] die Erstellung von Profilen (Profiling) *„transparent*

87 BMUV, Corporate Digital Responsibility-Kodex, 2021, S. 4f.; Bahreini/Charton/Lukas RDi 2021, 548 (548f.); Esselmann/Brink Ökologisches Wirtschaften 33, 2 (2020), 11 (12); Cooper/Siu/Wei, Corporate Digital Responsibility, 2015, S. 2f.; Dörr Praxisleitfaden CDR S. 109f., 111f., 115; Herden et al. NachhaltigkeitsManagementForum 29 (2021), 13 (19ff.); Richter PinG 6 (2018), 237 (238).

88 Vgl. Dörr Praxisleitfaden CDR S. 17f.

89 Zu den Schnittstellen zum Datenschutz sogleich → § 2 D. III. 4. und → § 3 B.

90 BMUV, Corporate Digital Responsibility-Kodex, 2021, S. 4; Maßnahmenvorschläge im Feld „Umgang mit Daten" beim Handlungsfeld „Verbrauchersouveränität und Autonomie sicherstellen", vgl. dazu https://cdr-initiative.de/kodex (Stand 1.12.2023).

91 BMUV, Corporate Digital Responsibility-Kodex, 2021, S. 5; Nietsch CSR Compliance/Anzinger § 27 Rn. 65ff.

92 BMUV, Corporate Digital Responsibility-Kodex, 2021, S. 4; speziell für künstliche Intelligenz Herden et al. NachhaltigkeitsManagementForum 29 (2021), 13 (20).

und fair [zu] gestalten" und zB die Analyse von Daten nach persönlichkeitsbezogenen Merkmalen zu unterlassen.[93]

Schließlich kann sich verantwortungsvoller Umgang mit Daten in der *dritten Stufe* daran zeigen, dass solches Verhalten auch über das eigene Unternehmen hinaus bei Geschäftspartnern, ggf. mit entsprechenden Verhaltenskodizes, eingefordert wird.[94] Digitale Verantwortung kann sich auch in der Bereitschaft äußern, bestimmte Daten im rechtlich zulässigen Rahmen ggü. Dritten (bspw. Forschende) bereitzustellen[95] oder auf bestimmte Formen manipulativen Marketings zu verzichten.[96]

Den genannten Zielen können sich Unternehmen durch vielfältige technische und organisatorische Maßnahmen nähern, die hier nur allgemein angedeutet werden können.[97] So kann die Gestaltung von Benutzeroberflächen oder die Programmierung der dahinterstehenden Systemarchitektur auf CDR-Kriterien hin angepasst werden und hierfür zB die Mitarbeitenden geschult und sensibilisiert werden. Relevant sind auch Schutzmaßnahmen vor physischen Einwirkungen auf Serverinfrastrukturen iRd Corporate Cyber Security.

Im Sinne einer vollständigen Darstellung von CDR werden nachfolgend weitere Handlungsfelder beschrieben, die nicht unmittelbar den Umgang mit Daten betreffen, aber eine teils enge bzw. systeminhärente Verbindung zu Daten aufweisen.

2. Digitale Bildung, Inklusion, Wandel der Arbeitswelt

Die Handlungsfelder der digitalen Bildung und Inklusion adressieren Wissens- und Kompetenzdisparitäten, die mit Blick auf neue digitale Technolo-

93 BMUV, Corporate Digital Responsibility-Kodex, 2021, S. 4; Dörr Praxisleitfaden CDR S. 110.

94 BMUV, Corporate Digital Responsibility-Kodex, 2021, S. 4f.; zur „Datenermächtigung" im Einzelnen auch Dörr Praxisleitfaden CDR S. 111.

95 Dörr Praxisleitfaden CDR S. 109.

96 Dörr Praxisleitfaden CDR S. 115f.

97 Im Detail Dörr Praxisleitfaden CDR S. 101ff. mit Hinweisen zu möglichen Engagements; Herden et al. NachhaltigkeitsManagementForum 29 (2021), 13 (18ff.); zu weiteren konkreten Maßnahmenvorschlägen vgl. https://cdr-initiative.de/kodex (Stand 1.12.2023); beispielhaften Überblick über praktische Maßnahmen liefern die CDR-Berichte der an der Initiative teilnehmenden Unternehmen, vgl. dazu https://cdr-initiative.de/cdr-berichte (Stand 1.12.2023).

gien bei Nutzerinnen und Nutzern wie auch Mitarbeitenden in Unternehmen bestehen.

Die zunehmende Digitalisierung verändert die individuellen Lebenswelten und kann für Personen eine Zugangshürde zu bestimmten Produkten und Dienstleistungen darstellen, etwa wenn diese nur digital zugänglich sind.[98] Um Nutzer auf digitalisierungsspezifische Veränderungen vorzubereiten und einer schleichenden Exklusion aus der (digitalisierten) Gesellschaft vorzubeugen, ist das Ziel von CDR, diese bedarfsgerecht im Umgang mit digitalen Technologien (fort) zu bilden, über Chancen und Risiken sowie ethische Fragen der Digitalisierung aufzuklären und zu einem souveränen Handeln zu befähigen sowie digitale Zugangshürden zu beseitigen.[99]

Auch für Mitarbeitende in digitalisierten Arbeitswelten besteht die Gefahr von Zugangshürden und Exklusion, zB durch eine zunehmende Automatisierung von Produktions- und Arbeitsprozessen, eine verstärkte Mensch-Maschine-Interaktion sowie neue Qualifikationsanforderungen.[100] Dass diesen Veränderungen der Arbeitswelt eine besondere Bedeutung auch für digitale Unternehmensverantwortung zukommt, zeigt sich daran, dass der CDR-Kodex des BMUV die „Mitarbeitenden-Einbindung" als eigenes Handlungsfeld aufführt.[101] Ziel ist hier, die Mitarbeitenden bei der Gestaltung von Transformationsprozessen zu beteiligen und zB durch Weiterbildungsmaßnahmen zu unterstützen.[102]

3. Umwelt-, Klima- und Ressourcenschutz

Schließlich hat CDR auch eine ökologische Dimension.[103] Digitale Technologien verbrauchen einerseits Energie und Ressourcen mit stark steigender Tendenz. So ist der digitale Sektor weltweit geschätzt für rund 2–4

98 BMUV, Corporate Digital Responsibility-Kodex, 2021, S. 6, 9; Herden et al. NachhaltigkeitsManagementForum 29 (2021), 13 (21).

99 BMUV, Corporate Digital Responsibility-Kodex, 2021, S. 6, 9; vgl. auch https://www.cdr-building-bloxx.com/digitale-befaehigung/ (Stand 1.12.2023).

100 Dazu Dörr Praxisleitfaden CDR S. 24ff.; vgl. auch https://www.cdr-building-bloxx.com/zukunft-arbeit/ (Stand 1.12.2023).

101 BMUV, Corporate Digital Responsibility-Kodex, 2021, S. 8.

102 BMUV, Corporate Digital Responsibility-Kodex, 2021, S. 8.

103 BMUV, Corporate Digital Responsibility-Kodex, 2021, S. 7; Herden et al. NachhaltigkeitsManagementForum 29 (2021), 13 (18f.) mwN; Lobschat et al. Journal of Business Research 122 (2021), 875 (879); vgl. dazu auch https://www.cdr-building-bloxx.com/umwelt-ressourcen/ (Stand 1.12.2023).

Prozent der globalen Treibhausgas-Emissionen verantwortlich.[104] Auch der Ressourceneinsatz für die Produktion von digitalen Produkten ist beträchtlich. Auf der Inputseite werden zahlreiche seltene Metalle und Mineralien benötigt, die unter hoch problematischen ökologischen, politischen und sozialen Bedingungen gefördert werden und auf der Output-Seite entstehen große Mengen an Elektronikschrott, von denen nur ein kleiner Teil recycelt wird.[105] Andererseits leisten digitale Technologien große Beiträge zur Lösung bzw. Abfederung von Umwelt-, Klima- und Ressourcenproblemen.[106] Sie sind also auch eine notwendige Voraussetzung für die Erreichung umfassender Nachhaltigkeitsziele.[107] Die ökologische Dimension digitaler Technologien ist damit ein eminent wichtiges Handlungsfeld von CDR. Unternehmen sollen dabei den durch die Herstellung und den Betrieb von technischen Geräten verursachten Verbrauch von Energie und Ressourcen reduzieren und gleichzeitig digitale Anwendungen entwickeln, die umweltfreundliches Verhalten unterstützen.[108]

---

104 Coalition for Digital Environmental Sustainability (CODES), Action Plan for a Sustainable Planet in the Digital Age, 2020, vgl. dazu https://doi.org/10.5281/zenodo.6573509, S. 20 (Stand 1.12.2023) betrachtet den digitalen Sektor insgesamt und kommt zur Einschätzung, dass er je nach Berechnungsmethode für ca. 1,8–3,9 Prozent der globalen Treibhausgas-Emissionen verantwortlich ist. Nach den Schätzungen von McKinsey ist Informationstechnik in Unternehmen weltweit für die jährliche Emission von 350–400 Megatonnen CO_2-Äquivalente verantwortlich. Das sind 1 Prozent der weltweiten jährlichen Treibhausgas-Emissionen. Der größte CO_2-Emittent sind dabei nicht die Rechenzentren vor Ort, sondern die Herstellung und Betrieb aller Endgeräte der Mitarbeiter wie Laptops, Tablets, Smartphones und Drucker. Diese Endnutzergeräte erzeugen weltweit 1,5 bis 2 Mal mehr CO_2 als Rechenzentren, vgl. dazu https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/the-green-it-revolution-a-blueprint-for-cios-to-combat-climate-change, S. 2f. (Stand 1.12.2023).

105 UNEP, Foresight Brief Nr. 27, The growing footprint of digitalisation, vgl. dazu https://wedocs.unep.org/handle/20.500.11822/37439, S. 4 (Stand 1.12.2023).

106 Laut World Economic Forum, Davos Agenda 2022, 3 ways digital technology can be a sustainability game changer, 19.1.2022, vgl. dazu https://www.weforum.org/agenda/2022/01/digital-technology-sustainability-strategy/ (Stand 1.12.2023) können digitale Technologien ua genutzt werden, um Fortschritte bei Nachhaltigkeit zu messen und verfolgen, die Nutzung von Ressourcen zu optimieren, Treibhausgasemissionen zu reduzieren und eine Kreislaufwirtschaft möglich machen; siehe auch Dörr Praxisleitfaden CDR S. 114ff.

107 Detailliert dazu Mittwoch JZ 2023, 376 (376, 381ff.).

108 Vgl. BMUV, Corporate Digital Responsibility-Kodex, 2021, S. 7; Herden et al. NachhaltigkeitsManagementForum 29 (2021), 13 (18f.); Lobschat et al. Journal of Business Research 122 (2021), 875 (879).

4. Spannungsfeld zwischen gesetzlichen Regelungen und CDR

Mit Blick auf Inhalte von CDR und deren Zusammenwirken mit rechtlichen Anforderungen ist bemerkenswert, dass die Web-Version des CDR-Kodex des BMUV bei mehreren Maßnahmenvorschlägen auf die Voraussetzungen der Datenschutz-Grundverordnung (DSGVO)[109] verweist.[110] Für den Maßnahmenvorschlag, *„Kundinnen und Kunden [zu] informieren, wenn Kundendaten genutzt werden, um Profile über sie zu erstellen"* wird zB darauf verwiesen, dass dies *„bei personenbezogenen Daten der Informationspflicht aus Art. 13 Abs. 2 Buchstabe f, Art. 14 Abs. 2 Buchstabe g DSGVO [entspricht]."*[111] Der Vorschlag, dass Unternehmen *„sicherstellen, dass persönliche Daten nur von Personen verwendet werden, die über entsprechende Berechtigungen verfügen"*, entspräche *„bei personenbezogenen Daten den TOMs (Technische und Organisatorische Maßnahmen) im Sinne des Art. 32 DSGVO."*[112] Auch in der CDR-Literatur wird die DSGVO wiederholt als wichtiges Instrument für den Datenschutz angeführt.[113]

Hier zeigt sich ein durchaus problematisches Spannungsfeld von CDR zum gesetzlichen Regelungsrahmen. Zwar kann die Aufnahme von wichtigen gesetzlichen Anforderungen in ein freiwilliges Verantwortungsregime einerseits ihre besondere Bedeutung hervorheben und andererseits auf *„die verbraucherfreundliche Umsetzung gesetzlicher Anforderungen"*[114] abzielen, wie es der CDR-Kodex des BMUV formuliert. Die genügende Erfüllung

109 VO (EU) 2016/679.

110 Maßnahmenvorschläge im Feld „Umgang mit Daten" in der Webversion des Corporate Digital Responsibility-Kodex, vgl. dazu https://cdr-initiative.de/kodex (Stand 1.12.2023). Weiterhin finden sich Verweise auf ein Gutachten der Datenethikkommission (DEK). In der PDF-Version des CDR-Kodex finden sich keine entsprechenden Verweise.

111 Maßnahmenvorschlag um *„Profilanalysen („Profiling") verantwortlich, transparent und fair gestalten"* und dazugehörige Fußnote 2 im Feld „Umgang mit Daten" in der Webversion des Corporate Digital Responsibility-Kodex, vgl. dazu https://cdr-initiative.de/kodex (Stand 1.12.2023).

112 Maßnahmenvorschlag um *„Verantwortlichen Umgang mit Daten im Unternehmen sicherstellen"* und dazugehörige Fußnote 10 im Feld „Umgang mit Daten" in der Webversion des Corporate Digital Responsibility-Kodex, vgl. dazu https://cdr-initiative.de/kodex (Stand 1.12.2023).

113 Nietsch CSR Compliance/Anzinger § 27 Rn. 55; Esselmann/Golle/Thiel/Brink, Corporate Digital Responsibility, 2020, S. 10, 12; Herden et al. NachhaltigkeitsManagementForum 29 (2021), 13 (17f., 22); Lobschat et al. Journal of Business Research 122 (2021), 875 (878f., 883); Mueller Bus Inf Syst Eng 64 (2022), 689 (692); Panzer-Heemeier/Nemat CCZ 2022, 223 (227); Richter PinG (2018) 6, 237 (238).

114 BMUV, Corporate Digital Responsibility-Kodex, 2021, S. 4.

der geltenden gesetzlichen Anforderungen ist jedoch die Pflicht eines jeden Unternehmens und Ausdruck ihrer Regelkonformität. Es kann sich dabei nicht um ein freiwilliges unternehmerisches Engagement handeln. Besonders problematisch erscheint, dass eine staatliche Initiative damit dem ersten Anschein nach die gesetzlichen Anforderungen zu „Maßnahmenvorschlägen" herabstuft und die Unternehmen im Mantel der Freiwilligkeit *„über das gesetzlich Vorgeschriebene hinaus[gehende]"* Aktivitäten berichten können, obwohl diese Aktivitäten die gesellschaftlich erwartete Regeleinhaltung widerspiegeln.

Aus diesem Spannungsfeld ergibt sich die Notwendigkeit, CDR in den bestehenden und zukünftigen rechtlichen Kontext einzubetten und ihre Wechselwirkung zum Recht zu bestimmen. Der regulatorische Kontext ist für den Anwendungsbereich und Inhalt einer freiwilligen Unternehmensverantwortung gerade konstitutiv, da dieser den Spielraum bestimmt, in dem Unternehmen tatsächlich freiwillig tätig werden können und eigene, nicht hoheitlich vorgegebene „Sollens-" und „Müssens-Sätze" formulieren können. Dies ist Gegenstand des nachfolgenden Kapitels.

§ 3 Corporate Digital Responsibility im Kontext eines entstehenden Datenrechts

Digitale Unternehmensverantwortung ist inhaltlich vielfältig und bewegt sich infolgedessen in einem ebenso vielseitigen Regulierungsrahmen: Für die Handlungsfelder der digitalen Bildung und Inklusion sowie des Wandels der Arbeitswelt bilden zB das Sozial- und Arbeitsrecht mögliche rechtliche Anknüpfungspunkte. Für das Handlungsfeld Umwelt- und Klimaschutz spielt dagegen das Umwelt- und Produktrecht ua eine Rolle.[115] Die vorliegende Arbeit fokussiert den Umgang mit Daten und den dazugehörigen rechtlichen Rahmen.

Die Regulierung von digital- und datenbezogenen Sachverhalten hat in der jüngeren Zeit an Fahrt aufgenommen, insb. auf europäischer Ebene.

115 Etwa wenn es um die Gestaltung nachhaltiger Produkte geht, vgl. Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zur Schaffung eines Rahmens für die Festlegung von Ökodesign-Anforderungen für nachhaltige Produkte und zur Aufhebung der Richtlinie 2009/125/EG vom 30.3.2022, COM(2022) 142 final.

Die Europäische Kommission stellte im Februar 2020 eine Digitalstrategie zur Gestaltung von Europas digitaler Zukunft vor.[116] Parallel legte sie auch eine Datenstrategie vor, in welcher sie die Herausforderungen einer datenzentrierten Wirtschaft und Gesellschaft skizziert und strategische Leitlinien formuliert.[117] Zudem hat sie im Januar 2022 mit der politischen „Erklärung zu den digitalen Rechten"[118] wichtige Rechte und Grundsätze proklamiert, die sich auch Unternehmen zu eigen machen sollen, weil diese *„im digitalen Raum Verantwortung tragen"*.[119] Hierzu gehören zB die Menschzentrierung und Inklusivität des digitalen Wandels, die Entscheidungsfreiheit und Befähigung der Nutzenden wie auch die Sicherheit im digitalen Raum und die digitale Nachhaltigkeit. Dieser strategische Rahmen wird durch ein breites Spektrum an bereits geltender oder gerade im Gesetzgebungsprozess befindlicher Regulierung zu digitalen Plattformen, Technologien und Daten ausgefüllt.

Wichtige Bausteine dieser Gesetzgebung sind das 2022 verabschiedete Gesetz über digitale Märkte und das Gesetz über digitale Dienste (A.), mit denen die Regulierung von großen digitalen Plattformen und Unternehmen forciert wird.[120] Datenrechtlich kommt dem europäischen Datenschutzrecht eine zentrale Bedeutung zu (B.). Des Weiteren ist der freie Zugang zu Daten bzw. ihre gemeinsame Nutzung ein Regelungsanliegen des europäischen Gesetzgebers (C.), das durch das im Mai 2022 verabschiedete Daten-Governance-Gesetz und das im November 2023 verabschiedete Datengesetz adressiert wird. Weiterhin soll die Sicherheit von digitalen Technologien und Daten erhöht werden, indem zB Hard- und Softwareprodukte durch einen „Cyber Resilience Act" strenger reguliert werden (D.). Der

116 Gestaltung der digitalen Zukunft Europas vom 19.2.2020, COM(2020) 67 final; daran anknüpfend wurden die Zielvorstellungen im „Digitalen Kompass 2030" weiter ausformuliert, vgl. Digitaler Kompass 2030: der europäische Weg in die digitale Dekade vom 9.3.2021, COM(2021) 118 final.

117 Eine europäische Datenstrategie vom 19.2.2020, COM(2020) 66 final, 2ff., 13ff.

118 Europäische Erklärung zu den digitalen Rechten und Grundsätzen für die digitale Dekade vom 26.1.2022, COM(2022) 28 final; Nüßing MMR 2022, 341 (341f.) erblickt in der Erklärung wenig neue Forderungen bzw. Grundsätze.

119 Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen, Eine europäische Erklärung zu den digitalen Rechten und Grundsätzen für die digitale Dekade vom 26.1.2022, COM(2022) 27 final, 7.

120 Beide Rechtsakte sind Schlüsselmaßnahmen, die die Kommission bereits in ihrer Digitalstrategie formulierte, vgl. COM(2020) 67 final, 11, 14; zum Regelungsziel Gielen/Uphues EuZW 2021, 627.

datengetriebene Einsatz von KI-Systemen wird derzeit ebenfalls rechtlich eingefasst, ua durch eine EU-Verordnung über Künstliche Intelligenz (E.).

Im Folgenden wird der (entstehende) regulatorische Rahmen aufgezeigt und in Bezug zu den Zielen und Inhalten der CDR gesetzt. Hierbei wird eine Makro-Perspektive gewählt, um der Regelungs- und Detailfülle des regulatorischen Rahmens, dem begrenzten Umfang dieser Arbeit und dem weiten Handlungsspielraum der CDR zum Umgang mit Daten gerecht zu werden.

A. Gesetze über digitale Märkte und digitale Dienste

Das Gesetz über digitale Märkte (DMA)[121] und das Gesetz über digitale Dienste (DSA)[122] betreffen einerseits die wettbewerbliche Ausrichtung digitaler Märkte und andererseits die Moderation von illegalen Inhalten in digitalen Plattformen und Diensten. Beide Rechtsakte traten im November 2022 in Kraft.

Das Gesetz über digitale Märkte reguliert ausgewählte „Torwächter"-Unternehmen, die über eine besonders dominante Stellung in digitalen Märkten verfügen und erlegt ihnen verschiedene Verhaltenspflichten auf.[123] Damit soll sichergestellt werden, dass digitale Märkte fair und für andere Wettbewerber „bestreitbar" sind.[124] So dürfen Torwächter ua keine personenbezogenen Daten miteinander zusammenführen, die aus dem Anbieten verschiedener Plattformdienste resultieren (zB Daten von WhatsApp und Instagram, die beide zu Meta gehören).[125] Demgegenüber ist das Ziel des Gesetzes über digitale Dienste, rechtswidrige Inhalte wie Hassrede und Desinformationen im Internet unionsweit wirksamer zu bekämpfen

121 VO (EU) 2022/1925.

122 VO (EU) 2022/2065.

123 Zur Definition siehe Art. 3 DMA, der Kriterien für Torwächter nennt (Abs. 1) und diese um quantitative Vermutungsregeln ergänzt (Abs. 2); zentrale Verpflichtungen für Torwächter finden sich in Art. 5 und 6 DMA, im Detail dazu Gielen/Uphues EuZW 2021, 627 (629ff.); Podszun/Bongartz/Kirk NJW 2022, 3249 (3250ff.).

124 Siehe Art. 1 Abs. 1 DMA; zur Einordnung des DMA als Wettbewerbsrecht oder Binnenmarkt-Regulierung mit eigenen Zielen, siehe Gielen/Uphues EuZW 2021, 627 (628); Podszun/Bongartz/Kirk NJW 2022, 3249 (3249f.).

125 Siehe Art. 5 Abs. 2 lit. b DMA, der insoweit Ähnlichkeit zu dem 2021 einführten deutschen § 19a GWB aufweist; problematisierend zu einer Normkollision Gielen/Uphues EuZW 2021, 627 (631f.).

und insofern bereits bestehende Regelungsregime zu harmonisieren.[126] Dafür werden Vermittlungsdienste abgestimmten Haftungsprivilegierungen (Art. 4–6 DSA) und Sorgfaltspflichten (Art. 11ff. DSA) unterworfen.[127]

Auch wenn wettbewerbliche Ziele keinen Kerninhalt von CDR darstellen, ist „faires" Verhalten gegenüber Mitbewerbern bzw. Nutzern sowie ein sensibler Umgang mit rechtswidrigen Inhalten generell einer verantwortungsvollen Unternehmensführung zuzuordnen. Zudem handelt es sich bei DMA und DSA um zentrale digitalpolitische Rechtsakte,[128] die in der Darstellung der digital- und datenrechtlichen Landschaft auf EU-Ebene nicht fehlen dürfen. Für Unternehmen mit digitalen Geschäftsmodellen werden bestehende Rechtspflichten aus dem Kartell- und Wettbewerbsrecht und zur Moderation von Inhalten also unionsweit (weiter) harmonisiert bzw. ausgestaltet.

B. Datenschutz

Die Datenschutz-Grundverordnung (DSGVO)[129] bestimmt als unmittelbar geltendes Unionsrecht seit Mai 2018 maßgeblich die Regeln zum Schutz personenbezogener Daten in der EU.[130] Die DSGVO formuliert dabei insb. Grundsätze für die Verarbeitung von personenbezogenen Daten (I.) und verschiedene Rechte von betroffenen Personen (II.). Darüber hinaus werden denjenigen diverse Pflichten auferlegt, die für die Datenverarbeitung verantwortlich bzw. mit dieser beauftragt sind (III.).

126 So führten mehrere EU-Mitgliedstaaten bereits nationale Gesetze zur Bekämpfung rechtswidriger oder strafbarer Inhalte im Internet ein, zB Deutschland mit dem Netzwerkdurchsetzungsgesetz (NetzDG), vgl. Gielen/Uphues EuZW 2021, 627 (632f.).

127 Art. 1 Abs. 2 DSA; zu den verschiedenen Arten von Vermittlungsdiensten und den dazugehörigen Sorgfaltspflichten Gielen/Uphues EuZW 2021, 627 (634ff.).

128 Beide Rechtsakte sind für die EU-Kommission „Schlüsselmaßnahmen" ihrer Digitalstrategie, vgl. COM(2020) 67 final, 11, 14.

129 VO (EU) 2016/679.

130 Neben der DSGVO gibt es weitere spezialgesetzliche Vorschriften zum Datenschutz, die Vorschriften der DSGVO ggf. verdrängen. Hierzu gehört in Deutschland ua der Datenschutz bei Telekommunikation und Telemedien (§§ 1ff. TTDSG), besondere Regelungen im Bundesdatenschutzgesetz (§§ 1ff. BDSG) oder zu digitalen Gesundheitsanwendungen (§ 4 Digitale Gesundheitsanwendungen-Verordnung).

I. Grundsätze der DSGVO

In Art. 5 Abs. 1 DSGVO finden sich die grundsätzlichen Anforderungen an die Verarbeitung von personenbezogenen Daten. Zu den Grundsätzen gehört, dass die Daten erstens rechtmäßig, also auf Grundlage einer Einwilligung oder einer anderen gesetzlichen Befugnis, und transparent verarbeitet werden müssen (lit. a). Zweitens unterliegen die Daten einer Zweckbindung, dürfen also nicht für andere als die festgelegten bzw. legitime Zwecke verwendet werden (lit. b). Weiterhin gilt der Grundsatz der Datenminimierung, also dass Daten für den jeweiligen Zweck angemessen und erheblich sind und nicht über das notwendige Maß hinaus verarbeitet werden (lit. c). Auch dürfen Daten nur solange nicht-anonymisiert gespeichert werden, wie es für die Zwecke der Verarbeitung „erforderlich" ist (lit. e) und müssen durchgängig sicher und vertraulich verarbeitet werden (lit. f).

Die Verarbeitung von personenbezogenen Daten nach der DSGVO unterliegt damit kurz gefasst ua den Grundsätzen der Rechtmäßigkeit, Transparenz, Zweckbindung, Datenminimierung sowie Integrität und Vertraulichkeit.[131] Das Datenschutzrecht der DSGVO ist also „prinzipiengeleitet"[132] und weist damit Ähnlichkeiten zu den Prinzipien auf, die sich im CDR-Kodex des BMUV, aber auch anderen Leitlinien zum verantwortungsvollen Umgang mit digitalen Anwendungen, finden.[133] Zudem gibt es inhaltliche Überschneidungen zwischen den Grundsätzen der DSGVO und den für

131 Siehe Art. 5 Abs. 1 DSGVO am Ende der jeweiligen Absätze. Weitere Grundsätze sind die Verarbeitung nach Treu und Glauben (lit. a), Richtigkeit (lit. d) und Speicherbegrenzung (lit. e); ob es sich dabei um rechtsverbindliche Grundsätze oder um Prinzipien i.S.v. Optimierungsgeboten handelt, ist umstritten: für verbindliche Grundsätze BeckOK DatenschutzR/Schantz DS-GVO Art. 5 Rn. 2; Ehmann/Selmayr/Heberlein DS-GVO Art. 5 Rn. 1; für Optimierungsgebote wohl: Paal/Pauly/Frenzel DS-GVO Art. 5 Rn. 9; ebenfalls dazu Nietsch CSR Compliance/Anzinger § 27 Rn. 56.

132 Zu den Prinzipien des Datenschutzrechts und ihrer Bedeutung: BeckOK DatenschutzR/Wolff DS-GVO Grundlagen Rn. 1ff.; Ehmann/Selmayr/Heberlein DS-GVO Art. 5 Rn. 2; mit Blick auf CDR vgl. Nietsch CSR Compliance/Anzinger § 27 Rn. 55.

133 Siehe Prinzipien im BMUV, Corporate Digital Responsibility-Kodex, 2021, S. 3; für den Code of Digital Ethics der Merck KGaA ausführlich Bahreini/Charton/Lukas RDi 2021, 548 (550f.); andere sprechen von „Werten", vgl. idigiT, Leitlinien zu digitaler Ethik in Europa, 2022, S. 13.

die CDR formulierten Prinzipien, so mit Blick auf Transparenz,[134] Integrität und Vertraulichkeit[135] oder Autonomie[136].

II. Rechte von betroffenen Personen

Die Art. 12–23 DSGVO verleihen Personen verschiedene Rechte, wenn ihre personenbezogenen Daten verarbeitet werden. Die Rechte umfassen den gesamten Prozess der Datenverarbeitung und beginnen mit einer Information über die Datenerhebung *„in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache"* (Art. 12 Abs. 1 DSGVO). Es bestehen sodann Auskunftsrechte, ein Recht auf Berichtigung von unrichtigen Daten, ein Recht auf Löschung bzw. „Vergessenwerden" und auf Datenübertragbarkeit (Art. 15–18 DSGVO). Beachtenswert ist außerdem das *„Recht, nicht einer ausschließlich auf einer automatisierten Verarbeitung – einschließlich Profiling – beruhenden Entscheidung unterworfen zu werden"* in Art. 22 Abs. 1 DSGVO.[137]

Mit diesen Rechten ermöglicht die DSGVO betroffenen Personen umfassend über die eigenen personenbezogenen Daten sowie Art und Umfang ihrer Verarbeitung zu entscheiden. Die souveräne und autonome Entscheidung über eigene Daten von Nutzern wird als wichtiger Bestandteil der CDR gesehen.[138] Aufgrund der weitreichenden gesetzlichen Gewährleistungen ist der Spielraum einer freiwilligen CDR für die „Rechtsstellung" von Nutzern aber begrenzt.

---

134 Der Grundsatz „Transparenz" (Art. 5 Abs. 1 lit. a DSGVO) ist ebenfalls ein Prinzip im CDR-Kodex und anderen europäischen Leitlinien, vgl. BMUV, Corporate Digital Responsibility-Kodex, 2021, S. 3; idigiT, Leitlinien zu digitaler Ethik in Europa, 2022, S. 13.

135 Der Grundsatz „Integrität und Vertraulichkeit" (Art. 5 Abs. 1 lit. f DSGVO) könnte dem Prinzip „Schaden vermeiden" und „Verantwortlichkeit" im CDR-Kodex zugeordnet werden, vgl. BMUV, Corporate Digital Responsibility-Kodex, 2021, S. 3; in anderen europäischen Leitlinien findet sich der Wert „Sicherheit", vgl. idigiT, Leitlinien zu digitaler Ethik in Europa, 2022, S. 13.

136 Das Prinzip „Autonomie" aus dem CDR-Kodex könnte den Grundsätzen der Rechtmäßigkeit und Zweckbindung in Art. 5 Abs. 1 lit. a und lit. b DSGVO entsprechen, vgl. BMUV, Corporate Digital Responsibility-Kodex, 2021, S. 3.

137 Auch wenn dieses Recht nicht ausnahmslos gilt (Abs. 2), ist der für die Datenverarbeitung Verantwortliche dennoch zu „angemessene[n] Maßnahmen" verpflichtet, um die Rechte, Freiheiten und berechtigten Interessen der betroffenen Person zu schützen; dazu Ehmann/Selmayr/Hladjk DS-GVO Art. 22 Rn. 11ff.

138 BMUV, Corporate Digital Responsibility-Kodex, 2021, S. 4; Dörr Praxisleitfaden CDR S. 11lf.; Herden et al. NachhaltigkeitsManagementForum 29 (2021), 13 (22).

III. Verantwortung für die Datenverarbeitung

Das vierte Kapitel der DSGVO (Art. 24–43) enthält vielgestaltige Pflichten für datenverarbeitende Instanzen bzw. Personen.[139] Zunächst ist mehreren Pflichten gemein, dass diese *„geeignete technische und organisatorische Maßnahmen"* des für die Datenverarbeitung Verantwortlichen erfordern.[140] Bei der Auswahl der Maßnahmen sind idR der Stand der Technik, Implementierungskosten sowie Umstände der Verarbeitung und die mit ihr verbundenen Risiken zu berücksichtigen und abzuwägen.[141]

Solche technischen und organisatorischen Maßnahmen hat der Verantwortliche ua zu treffen, um zB durch Pseudonymisierung *„die Datenschutzgrundsätze wie etwa Datenminimierung wirksam umzusetzen"* oder um *„sicher[zu]stellen, dass durch Voreinstellung nur personenbezogene Daten, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist, verarbeitet werden"* (Art. 25 Abs. 1 und Abs. 2 S.1 DSGVO). Bei diesen Pflichten handelt es sich um sog. Datenschutz „by design" bzw. „by default".[142]

Ebenfalls ist die Sicherheit der Datenverarbeitung durch technische und organisatorische Maßnahmen zu gewährleisten, um ein für das jeweilige Risiko *„angemessenes Schutzniveau zu gewährleisten"* (Art. 32 Abs. 1 DSGVO). Hierzu werden beispielhaft mögliche Maßnahmen aufgeführt, wie Pseudonymisierung und Verschlüsselung von Daten.

Ein Datenschutz „by design" bzw. „by default" und informationstechnisch sichere Systeme werden auch als Gestaltungsaufgaben einer CDR gesehen.[143] Ihrem Grundsatz nach sind dies jedoch Pflichten unter der DSGVO, sofern personenbezogene Daten betroffen sind. Diese Pflichten gelten uneingeschränkt auch für neue digitale Technologien. So orientieren sich die technischen und organisatorischen Maßnahmen idR am Stand der

139 Die DSGVO spricht von für die Verarbeitung „Verantwortliche" und von „Auftragsverarbeitern", vgl. nur Art. 24 und 28 DSGVO.

140 So in Art. 24 Abs. 1, Art. 25 Abs. 1, Art. 32 Abs. 1, Art. 34 Abs. 3 lit. a DSGVO; zum Begriff der technischen und organisatorischen Maßnahmen: Paal/Pauly/Martini DS-GVO Art. 24 Rn. 20ff.

141 Siehe Art. 24 Abs. 1, Art. 25 Abs. 1, Art. 32 Abs. 1 DSGVO.

142 BeckOK DatenschutzR/Paulus DS-GVO Art. 25 Rn. 4f., 8; Ehmann/Selmayr/Baumgartner DS-GVO Art. 25 Rn. 1f.

143 Dörr Praxisleitfaden CDR S. 111; Maßnahmenvorschlag 2 beim Ziel *„Verantwortliche Technikgestaltung im Umgang mit Daten fördern"* im Feld „Umgang mit Daten" in der Webversion des Corporate Digital Responsibility-Kodex, vgl. dazu https://cdr-initiative.de/kodex (Stand 1.12.2023).

Technik, sodass Unternehmen fortlaufend zu einer (Re-)Evaluation der ergriffenen Schutzmaßnahmen angehalten sind. Für neuartige Technologien, die bei der Datenverarbeitung zu einem hohen Risiko für die Rechte und Freiheiten von Personen führen,[144] sind zudem gemäß Art. 35 Abs. 1 DSGVO die Folgen für den Datenschutz abzuschätzen.[145] Die DSGVO unterwirft Unternehmen damit verschiedenen Pflichten zum Schutz von personenbezogenen Daten, welche insb. auch präventiven Charakter haben und ihrem Inhalt und Umfang nach im Einzelfall ausfüllungsbedürftig sind. Deshalb ist der Spielraum für freiwillige Maßnahmen im Rahmen einer digitalen Unternehmensverantwortung hier ebenfalls überschaubar.

IV. Zwischenfazit

Für den Schutz von personenbezogenen Daten gibt die DSGVO einen weitreichenden Regulierungsrahmen vor, der umfassend Rechte von betroffenen Personen festlegt und verantwortliche Unternehmen verpflichtet. Deshalb sind die Möglichkeiten für Unternehmen, über ihre Verpflichtungen aus der DSGVO hinaus wesentliche eigene Schutzmaßnahmen im Rahmen einer CDR zu ergreifen, begrenzt.[146]

Daraus folgt erstens, dass es aufgrund des hohen Schutzniveaus der DSGVO unsachgemäß wäre, diese im Hinblick auf digitale Unternehmensverantwortung als „bloß" grundlegenden rechtlichen Maßstab einzuordnen.[147] Diese ist vielmehr der Ausgangspunkt und *„important guideline[s]"*[148] für eine unternehmensinterne Auseinandersetzung mit CDR, auf

144 Die DSGVO verweist insb. auf Fälle des systematischen und umfassenden Profilings und der Verarbeitung von besonders sensiblen Daten, Art. 35 Abs. 3 lit. a und b DSGVO.

145 Zur Anwendung der Datenschutz-Folgeabschätzung gemäß Art. 35 DSGVO beim Einsatz von personenbezogenen Trainingsdaten für ein KI-System: Schürmann ZD 2022, 316 (317ff.); im Einzelnen ferner Paal/Pauly/Martini DS-GVO Art. 35 Rn. 44ff.

146 In diese Richtung ebenfalls: Nietsch CSR Compliance/Anzinger § 27 Rn. 55ff.; Mueller Bus Inf Syst Eng 64 (2022), 689 (696); Pauly/Wichert DB-Beil. Heft 21/2023, 44 (45); Richter PinG 6 (2018), 237 (238); für Esselmann/Golle/Thiel/Brink, Corporate Digital Responsibility, 2020, S. 10 überwiegt im Bereich Privacy bislang die DSGVO-Compliance mit wenigen darüberhinausgehenden Unternehmensaktivitäten.

147 Herden et al. NachhaltigkeitsManagementForum 29 (2021), 13 (17f.; 22); in diese Richtung wohl auch Mueller Bus Inf Syst Eng 64 (2022), 689 (692).

148 Lobschat et al. Journal of Business Research 122 (2021), 875 (879); wohl auch Panzer-Heemeier/Nemat CCZ 2022, 223 (227).

dessen Grundlage eine entsprechende CDR-Kultur und dazugehörige Normen im Unternehmen entwickelt werden können.[149] Dass der CDR-Kodex seine Ziele bzw. Maßnahmenvorschläge teils analog zu Pflichten in der DSGVO formuliert (→ § 2 D. III. 4.), kann einerseits als Ausdruck ihres hohen Schutzniveaus und ihrer Leitfunktion und andererseits als mögliche regulatorische „Sättigung" im Bereich des Datenschutzes gesehen werden. Vor diesem Hintergrund bleibt zu konstatieren, dass in Veröffentlichungen zur CDR kaum eine Auseinandersetzung mit den Regelungen der DSGVO stattfindet. Zweitens ist die DSGVO ein Ergebnis von zurückliegenden Regulierungsdebatten und -prozessen zum Datenschutz,[150] die für andere digitale Technologien gerade geführt werden bzw. bevorstehen. Entsprechend ist die DSGVO eine Blaupause dafür, dass Freiräume einer freiwilligen Unternehmensverantwortung abhängig vom Regelungsumfeld sind.

Dies soll nicht darüber hinwegtäuschen, dass zwischen der DSGVO und freiwilliger digitaler Unternehmensverantwortung Verknüpfungen bestehen: So beruht ihr Schutzanspruch auf teils gleichen und teils ähnlichen Grundprinzipien (insb. Transparenz, Sicherheit von Daten und Autonomie der Nutzenden). Daneben ermöglicht die DSGVO gewisse Selbstregulierung durch sog. Verhaltensregeln. Diese Regeln können Verbände und andere Vereinigungen ausarbeiten und damit die Anwendung der gesetzlichen Vorschriften konkretisieren (Art. 40 DSGVO).[151]

Neben der DSGVO gibt es auf unionsrechtlicher Ebene weitere datenschutzrechtliche Regeln, insb. für elektronische Kommunikationsdienste, die in der E-Privacy-Richtlinie bzw. nationalem Recht reguliert werden.[152] Die E-Privacy-Richtlinie sollte 2018 zeitgleich zum Inkrafttreten der DSGVO durch eine E-Privacy-Verordnung ersetzt werden, um die Vor-

149 Lobschat et al. Journal of Business Research 122 (2021), 875 (879); Panzer-Heemeier/Nemat CCZ 2022, 223 (228); Pauly/Wichert DB-Beil. Heft 21/2023, 44 (45); Richter PinG 6 (2018), 237 (238).

150 Lobschat et al. Journal of Business Research 122 (2021), 875 (885); Econsense, Umsetzung digitaler Verantwortung in Unternehmen, 2020, S. 7, 12.

151 Detailliert dazu Dürr ZGE 2021, 165 (175f.); mit Beispielen Wittmann/Haidenthaler MMR 2022, 8 (10ff.).

152 RL 2002/58/EG; in Deutschland aktuell umgesetzt durch das Gesetz zur Regelung des Datenschutzes und des Schutzes der Privatsphäre in der Telekommunikation und bei Telemedien (TTDSG) vom 23.6.2021 (BGBl. I 1982); im Detail zum Verhältnis zur DSGVO: BeckOK DatenschutzR/Holländer DS-GVO Art. 95 Rn. 2ff.; Paal/Pauly/Pauly DS-GVO Art. 95 Rn. 2f.

schriften der DSGVO zu ergänzen.[153] Das Gesetzgebungsverfahren läuft aktuell noch.[154] Aufgrund des besonderen Anwendungsbereichs und der Anknüpfung an das Schutzniveau der DSGVO wird an dieser Stelle auf eine nähere Darstellung beider Rechtsakte verzichtet.[155]

C. Datenzugang und -nutzung

Die EU-Kommission hat 2020 in ihrer Datenstrategie die hohe wirtschaftliche und gesellschaftliche Bedeutung von Daten hervorgehoben und gefordert, dass diese „*Quelle für Wachstum und Innovation*" in einer europäischen Datenwirtschaft genutzt werden solle.[156] Um einen EU-Binnenmarkt für Daten zu schaffen, wurden in der Strategie verschiedene politische Maßnahmen angekündigt,[157] die nun in zwei Gesetzesinitiativen mündeten:

Das Daten-Governance-Gesetz (DGG)[158] trat am 23.6.2022 in Kraft und zielt darauf ab, die Verfügbarkeit von Daten zu erhöhen, in dem datenvermittelnde Akteure reguliert und Möglichkeiten für die gemeinsame Datennutzung in der EU gestärkt werden.[159] Komplementär zur seit 2019 bestehenden Richtlinie über offene Daten, die die Weiterverwendung von Daten öffentlicher Stellen, von Unternehmen und von Forschungsdaten betrifft,[160] regelt das DGG die Weiterverwendung von „geschützten" Daten, die Rechten Dritter unterliegen.[161] Hierzu werden insbesondere sog. Da-

153 Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über die Achtung des Privatlebens und den Schutz personenbezogener Daten in der elektronischen Kommunikation und zur Aufhebung der Richtlinie 2002/58/EG (Verordnung über Privatsphäre und elektronische Kommunikation) vom 10.1.2017, COM(2017) 10 final; dazu Paal/Pauly/Pauly DS-GVO Art. 95 Rn. 4f.

154 Der letzte Stand ist eine Diskussion im Rat der Europäischen Union am 10.02.2021, vgl. dazu https://eur-lex.europa.eu/legal-content/EN/HIS/?uri=COM:2017:10:FIN (Stand 1.12.2023).

155 Im Detail dazu BeckOK DatenschutzR/Holländer DS-GVO Art. 95 Rn. 1, 4; Ehmann/Selmayr/Klabunde/Selmayr DS-GVO Art. 95 Rn. 8ff.; Paal/Pauly/Pauly DS-GVO Art. 95 Rn. 2f.

156 COM(2020) 66 final, 1ff.

157 COM(2020) 66 final, 5, 13ff.

158 VO (EU) 2022/868, welche gemäß Art. 38 DGG ab dem 24.9.2023 gilt.

159 Siehe Erwägungsgründe 3 und 5 VO (EU) 2022/868; näher Schildbach ZD 2022, 148 (148f.); Tolks MMR 2022, 444.

160 RL (EU) 2019/1024.

161 Art. 3 Abs. 1 lit. d und Erwägungsgrund Nr. 6 der RL (EU) 2019/1024; vgl. auch Tolks MMR 2022, 444 (445); Schildbach ZD 2022, 148 (149).

tenvermittlungsdienste reguliert, die „*Geschäftsbeziehungen zwischen einer unbestimmten Anzahl von betroffenen Personen oder Dateninhabern einerseits und Datennutzern andererseits*" anbahnen, um „*die gemeinsame Datennutzung [...] zu ermöglichen*" (Art. 2 Nr. 11 DGG). Diese spezielle Form der unternehmerischen Tätigkeit unterliegt einem verpflichtenden Anmeldeverfahren (Art. 10f. DGG) und weiteren Verhaltenspflichten nach Art. 12 DGG.[162] Weiterhin werden sog. „datenaltruistische Organisationen" durch das DGG geregelt, die entgeltlos die gemeinsame Datennutzung für Ziele von allgemeinem Interesse (zB Gesundheitsversorgung, Bekämpfung des Klimawandels) ermöglichen.[163] In Folge seines spezifischen Anwendungsbereichs ist das Daten-Governance-Gesetz nur selektiv für die Ausgestaltung von digitaler Unternehmensverantwortung relevant, namentlich wenn Datenintermediäre und ihre Tätigkeiten betroffen sind.

Größerem Interesse kommt dem im November 2023 verabschiedeten Data Act bzw. Datengesetz (DaG)[164] zu, das sich mit konkreten Rechten und Verfahren für den Datenzugang und damit notwendigen Bedingungen der Datenwertschöpfung befasst.[165] Das Datengesetz zielt also darauf, Daten – unabhängig von ihrem Personenbezug[166] – einfacher zugänglich und nutzbar zu machen.[167]

Dazu regelt das zweite Kapitel des Datengesetzes die Grundmodalitäten der Datenweitergabe und die Rechte und Pflichten der daran Beteiligten. Zunächst müssen Hersteller und Entwickler ihre vernetzten Produkte und verbundenen Dienste so gestalten, dass die bei ihrer Nutzung erzeugten

162 Hierzu gehören zB ein Diskriminierungsverbot, ein Neutralitäts- und Transparenzgebot, das Verbot von Kopplungsgeschäften, Anforderungen an die Umwandlung von Datenformaten oder die Interoperabilität von Daten, vgl. Hennemann/Ditfurth NJW 2022, 1905 (1908ff.), Tolks MMR 2022, 444 (446).

163 Für diese regeln die Art. 18ff. DGG ua Anforderungen für ihre Eintragung, die Transparenz und zum Schutz der Rechte und Interessen betroffener Personen und Dateninhaber; kritisch Schildbach ZD 2022, 148 (151f.).

164 VO (EU) 2023/2854.

165 COM(2022) 68 final, 5f.; vgl. auch Wiebe GRUR 2023, 1569; Tolks MMR 2022, 444 (449).

166 Siehe Art. 1 Abs. 5 Datengesetz und Erwägungsgrund Nr. 7: „*[Das Datengesetz] ergänzt das Unionsrecht zum Schutz personenbezogener Daten und zum Schutz der Privatsphäre, insbesondere die Verordnungen (EU) 2016/679 und (EU) 2017/1725 und die Richtlinie 2002/58/EG, und lässt es unberührt*"; die Grenze für die Datenverwendbarkeit ist also der Datenschutz, vgl. Bomhard/Merkle RDi 2022, 168 (169); Specht-Riemenschneider MMR 2022, 809 (810); Assion/Willecke MMR 2023, 805 (809f.).

167 COM(2022) 68 final, 3.

Daten für die Nutzenden *„einfach, sicher, unentgeltlich und [...] direkt zugänglich"* sind (Art. 3 DaG), sog. „Access by Design".[168] Hierauf aufbauend sollen Nutzer den Zugang zu Daten, die bei der Nutzung eines Produktes oder Dienstes erzeugt werden, verlangen können (Art. 4 DaG). Auch sollen Nutzer verlangen können, dass ihre Daten direkt an Dritte weitergegeben werden, die in diesem Fall besonderen Pflichten unterliegen (Art. 5 und 6 DaG). Das dritte Kapitel enthält die Pflichten der Dateninhaber, welche Daten bereitstellen müssen. Diese betreffen die Modalitäten, wie eine Datenbereitstellung (vertraglich) zu vereinbaren ist (Art. 8 DaG) und Vergütungsfragen (Art. 9 DaG). Im fünften Kapitel bestimmt das Datengesetz, dass Daten aufgrund einer außergewöhnlichen Notwendigkeit für öffentliche Stellen bereitgestellt werden müssen, zB bei einem öffentlichen Notstand.[169] Im sechsten Kapitel finden sich weitreichende Vorschriften für (cloud-basierte) Datenverarbeitungsdienste, die insb. den Wechsel des Anbieters erleichtern und etwaige *„gewerbliche, technische, vertragliche und organisatorische Hindernisse"* beseitigen sollen (Art. 23 DaG).[170] Schließlich werden im achten Kapitel umfangreiche Regelungen zur Interoperabilität für Anbieter von Datenräumen und Datenverarbeitungsdiensten getroffen. Damit knüpft das Datengesetz an die Verordnung über den freien Verkehr nicht personenbezogener Daten[171] von 2018 an, gemäß der einerseits nichtpersonenbezogene Daten frei in der EU verwendet werden können und die Selbstregulierung des erleichterten Wechsels von insb. Cloud-Anbietern durch Verhaltensregeln (wohl erfolglos)[172] forciert wurde.

Das europäische Datengesetz führt damit zu einer umfassenden rechtlichen Einfassung des Zugangs zu Daten aus der Nutzung von vernetzten Produkten und verbundenen Diensten, auch wenn es im Einzelnen ver-

168 Assion/Willecke MMR 2023, 805 (806f.); detailliert Wiebe GRUR 2023, 1569 (1570f.); Bomhard/Merkle RDi 2022, 168 (173) sprechen insofern von *„erheblich[en] Auswirkungen auf die technische Gestaltung von Produkten und Leistungen"*.

169 Vgl. Wiebe GRUR 2023, 1569 (1575f.); Specht-Riemenschneider MMR 2022, 809 (812, 824ff.).

170 Vgl. Wiebe GRUR 2023, 1569 (1576); kritisch Bomhard/Merkle RDi 2022, 168 (175).

171 VO (EU) 2018/1807.

172 So hebt die EU-Kommission im Entwurf ihres Datengesetzes hervor: *„[I]n Bezug auf Cloud-Dienste scheint der Selbstregulierungsansatz [der Verordnung über den freien Verkehr nicht personenbezogener Daten] die Marktdynamik nicht wesentlich beeinflusst zu haben; daher enthält dieser Vorschlag [zu einem Datengesetz] einen Regulierungsansatz für das Problem"*, COM(2022) 68 final, 5.

schiedener Kritik ausgesetzt ist.[173] Für CDR heißt dies, dass die Autonomie bzw. Selbstbestimmung über den Umgang mit Daten („Datenermächtigung"[174]) perspektivisch über regulatorische Datenzugangsansprüche und korrespondierende unternehmerische Pflichten verwirklicht wird.

D. Cybersicherheit

Auf EU-Ebene wird mit der Cybersicherheit ein weiteres Handlungsfeld der CDR adressiert. Mit der sog. NIS-Richtlinie[175] von 2016 existieren Regelungen, um die Sicherheit von Netz- und Informationssystemen sektorbezogen zu erhöhen und kritische (Digital-)Infrastrukturen besser zu schützen. Hierzu werden insb. die EU-Mitgliedstaaten verpflichtet, entsprechende nationale Strategien zu erarbeiten und Sicherheits- und Meldevorschriften für Betreiber kritischer Digitalinfrastrukturen definiert.[176] Dieser Rechtsrahmen wurde durch die 2023 in Kraft getretene NIS2-Richtlinie modernisiert und ihr Anwendungsbereich ausgeweitet und verschärft.[177] Weiterhin wurde 2019 der „Rechtsakt zur Cybersicherheit" verabschiedet.[178] Dieser harmonisierte ua den Rahmen für freiwillige Zertifizierung der Cybersicherheit von Produkten, Diensten und Prozessen der Informations- und Kommunikationstechnik, der Unternehmen betrifft, die sich entsprechend zertifizieren lassen.[179]

---

173 Assion/Willecke MMR 2023, 805 (810) kritisieren viele unbestimmte Rechtsbegriffe; detailliert auch Wiebe GRUR 2023, 1569 (1577f.); für die Entwurfsfassung kamen Bomhard/Merkle RDi 2022, 168 (176) bereits zum Ergebnis, dass *„[z]entrale Tatbestandsmerkmale und Anforderungen des Data Act aktuell derart unklar sind, dass sie sich kaum rechtssicher umsetzen ließen"* und für Specht-Riemenschneider MMR 2022, 809 (826) waren für die Erreichung der Regelungsziele noch *„mehr als vorsichtige Korrekturen"* erforderlich.

174 Zum Begriff und Einzelaspekten Dörr Praxisleitfaden CDR S. 111f.; Herden et al. NachhaltigkeitsManagementForum 29 (2021), 13 (22); ebenfalls zur „Verbrauchersouveränität und Autonomie": BMUV, Corporate Digital Responsibility-Kodex, 2021, S. 4.

175 RL (EU) 2016/1148; in Deutschland umgesetzt mit dem Gesetz zur Umsetzung der Richtlinie (EU) 2016/1148 vom 23.6.2017 (BGBl. I 1885).

176 Siehe Art. 7, 14, 16 RL (EU) 2016/1148.

177 RL (EU) 2022/2555; detailliert Schmidt K&R 2023, 705 (706ff.); vgl. dazu auch https://digital-strategy.ec.europa.eu/de/policies/nis2-directive (Stand 1.12.2023).

178 VO (EU) 2019/881.

179 Siehe Art. 46ff. der VO (EU) 2019/881.

Für Unternehmen, die Hard- und Softwareprodukte entwickeln und vertreiben, könnte jedoch das im September 2022 vorgeschlagene Gesetz über Cyberresilienz (GCR-E)[180] einschneidende Bedeutung bekommen. Dieses soll Sicherheitsvorschriften für sicherere Hard- und Softwareprodukte schaffen und damit die jährlich durch Cyberangriffe und -kriminalität entstehenden Kosten und Schäden für Nutzer und die Gesellschaft senken.[181] Für dieses Ziel legt der Gesetzesentwurf ua *„grundlegende Anforderungen an die Konzeption, Entwicklung und Herstellung von Produkten mit digitalen Elementen sowie Pflichten der Wirtschaftsakteure in Bezug auf diese Produkte hinsichtlich der Cybersicherheit"* fest und enthält Vorschriften zum Inverkehrbringen solcher Produkte (Art. 1 lit. a und b GCR-E). Auch für Sicherheitsupdates während des Lebenszyklus eines Produkts werden grundlegende Anforderungen an Hersteller festgelegt (Art. 1 lit. c GCR-E). Hersteller sollen ihre Produkte mit digitalen Elementen so gestalten, dass *„sie angesichts der Risiken ein angemessenes Cybersicherheitsniveau gewährleisten"*[182] und dafür eine Bewertung der Sicherheitsrisiken durchführen, zu der sie ggf. in einem Anhang aufgezählte Maßnahmen treffen müssen (zB Authentifizierungssysteme oder Verschlüsselung), Art. 10 Abs. 1 und 2 GCR-E.[183]

Auch wenn das Gesetzgebungsverfahren noch nicht abgeschlossen ist, lässt der Entwurf zum Gesetz über Cyberresilienz erwarten, dass die EU in den kommenden Jahren einen strengen Rechtsrahmen für die sichere Gestaltung von digitaler Hard- und Software schaffen wird. Dieser könnte viele der Ziele und Maßnahmen, die bislang einer freiwilligen Digitalverantwortung von Unternehmen zugeordnet werden (→ § 2 D. III.), in rechtliche Pflichten transformieren.

180 Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über horizontale Cybersicherheitsanforderungen für Produkte mit digitalen Elementen und zur Änderung der Verordnung (EU) 2019/1020 vom 15.9.2022, COM(2022) 454 final.

181 COM(2022) 454 final, 1.

182 Anhänge des Vorschlags für eine Verordnung des Europäischen Parlaments und des Rates über horizontale Cybersicherheitsanforderungen für Produkte mit digitalen Elementen und zur Änderung der Verordnung (EU) 2019/1020 vom 15.9.2022, COM(2022) 454 final, 1.

183 Anhang zu COM(2022) 454 final, 1.

E. Künstliche Intelligenz

Im April 2021 stellte die EU-Kommission ihren Vorschlag für ein Gesetz über künstliche Intelligenz (KIG-E) vor.[184] Ziel des Vorschlags ist es, zur *„Entwicklung einer sicheren, vertrauenswürdigen und ethisch vertretbaren künstlichen Intelligenz"* beizutragen und Vorteile sowie Risiken von KI-Systemen angemessen zu regeln.[185] In der Vorbereitungsphase wurden die Eingaben von zahlreichen Stakeholdern einbezogen, auch um im Hinblick auf bestehende Ethik-Kodizes einen gemeinsamen, wertorientierten Ansatz zu finden.[186] Die gesetzliche Haftung für KI-Systeme ist nicht Bestandteil des KIG-E und soll in einer Richtlinie harmonisiert werden.[187]

Im Mittelpunkt des Kommissionsentwurfs steht ein risikobasierter Ansatz, der KI-Systeme anhand ihres Risikos einstuft und ihren Einsatz mit abgestuften Anforderungen und Pflichten belegt.[188] Verboten werden sollen KI-Systeme mit einem „unannehmbaren Risiko" für die Werte der Union bzw. für Grundrechte.[189] Hierzu gehören Systeme mit hohem Manipulationspotential, mit denen Behörden die Vertrauenswürdigkeit von Personen benachteiligend bewerten oder klassifizieren könnten (sog. Social Scoring) oder die zur „biometrischen Echtzeit-Fernidentifizierung" im öffentlichen Raum dienen.[190] Grundsätzlich erlaubt werden sollen Systeme mit einem „hohen Risiko".[191] Diese sollen jedoch besonderen rechtlichen

184 Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zur Festlegung harmonisierter Vorschriften für Künstliche Intelligenz (Gesetz über Künstliche Intelligenz) und zur Änderung bestimmter Rechtsakte der Union vom 21.4.2021, COM(2021) 206 final.

185 COM(2021) 206 final, 2.

186 Der Vorschlag beruht ua auf den Arbeiten der Hochrangigen Expertengruppe für KI, die wichtige Anforderungen in Ethik-Leitlinien für vertrauenswürdige KI integriert hat, vgl. COM(2021) 206 final, 9f.

187 Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates zur Anpassung der Vorschriften über außervertragliche zivilrechtliche Haftung an künstliche Intelligenz (Richtlinie über KI-Haftung) vom 28.9.2022, COM(2022) 496 final.

188 COM(2021) 206 final, 8, 15ff.; siehe auch Geminn ZD 2021, 354 (356ff.); Orssich EuZW 2022, 254 (257ff.).

189 COM(2021) 206 final, 15.

190 COM(2021) 206 final, 15, 50ff. (Art. 5); im Detail Orssich EuZW 2022, 254 (257f.).

191 COM(2021) 206 final, 15; die Einstufung als „Hochrisiko-KI-System" hängt von seiner Funktion, ihrem konkreten Anwendungszweck und -modalitäten ab. Der Entwurf unterscheidet zwischen KI-Systemen als „Sicherheitskomponenten von Produkten" und „eigenständigen KI-Systemen", die in einem Anhang zum Entwurf explizit genannt werden, siehe COM(2021) 206 final, 15, 52f. (Art. 6, 7); dazu Geminn ZD 2021, 354 (357ff.); Orssich EuZW 2022, 254 (258ff.).

Anforderungen unterliegen, sodass qualifizierte „Risikomanagementsysteme" eingerichtet (Art. 9 KIG-E) und die in das System eingespeisten Daten besonders ausgewählt und verwaltet werden müssen (Art. 10 KIG-E). Weiterhin sollen ua Pflichten zur Dokumentation, zur Aufzeichnung, zur Transparenz und menschlichen Aufsicht sowie zur Resilienz und Sicherheit der Systeme gelten (Art. 11–15 KIG-E). Bei KI-Systemen mit spezifischen Manipulationsrisiken soll der Einsatz einer KI offengelegt werden.[192] Für KI-Systeme mit einem geringen oder minimalen Risiko sieht der KIG-E keine besonderen regulatorischen Anforderungen vor, sodass sie im bestehenden Rechtsrahmen betrieben werden können. Ein Großteil der aktuell in der EU eingesetzten KI-Systeme dürfte in diese Kategorie fallen.[193] Gleichzeitig soll der KIG-E für den verantwortungsvollen Einsatz von künstlicher Intelligenz nicht abschließend sein und fördert daher die freiwillige Erfüllung bzw. Übererfüllung der gesetzlichen Regeln (Art. 69 KIG-E). So soll die Aufstellung von Verhaltenskodizes erleichtert werden, um die Anforderungen an Hochrisiko-Systeme auf Systeme mit geringen Risiken zu übertragen (Art. 69 Abs. 1 KIG-E) oder um freiwillig weitere Anforderungen zu erfüllen, die sich zB *„auf die ökologische Nachhaltigkeit, die barrierefreie Zugänglichkeit für Personen mit Behinderungen, die Beteiligung von Interessenträgern an der Konzeption und Entwicklung von KI-Systemen [...] beziehen"* (Art. 69 Abs. 2 KIG-E).

Aufgrund des laufenden Gesetzgebungsverfahrens sind sowohl der Beschluss als auch die finalen Regelungsinhalte eines europäischen KI-Gesetzes noch offen.[194] Der ursprüngliche Kommissionsentwurf ist aufgrund von sich verändernden politischen Agenden und verstärkten Forderungen nach weniger Bürokratie und Regelungslast infolge von gesamtwirtschaftlichen Entwicklungen zuletzt zunehmend unter Druck geraten. In jedem Fall wird der unionsrechtliche Rechtsrahmen darüber entscheiden, welche Handlungsspielräume einer CDR in Bezug auf Anwendungen künstlicher Intelligenz zukommen.

Nach derzeitigem Stand würden diese Spielräume korrespondierend zu dem abgestuften Regulierungsregime des KIG-E variieren. Für Systeme mit geringen Risiken verbliebe ein wesentlicher Handlungsspielraum für digi-

192 Art. 52 KIG-E nennt KI-Systeme, die mit natürlichen Personen interagieren (Abs. 1), die Emotionen erkennen oder biometrisch kategorisieren (Abs. 2) oder die Bild-, Ton- oder Videoinhalte als „Deepfakes" erzeugen (Abs. 3), COM(2021) 206 final, 78.

193 Orssich EuZW 2022, 254 (255).

194 Zum derzeitigen Stand vgl. https://oeil.secure.europarl.europa.eu/oeil/popups/ficheprocedure.do?reference=2021/0106(OLP) (Stand 1.12.2023).

tale Unternehmensverantwortung, in dem entweder (ausgewählte) gesetzliche Vorgaben freiwillig erfüllt werden, diese als Orientierung für unternehmensinterne Leitlinien dienen oder jenseits dessen eine eigene Auseinandersetzung mit verantwortungsvollem KI-Einsatz erfolgt. Für Hochrisiko-Systeme unterlägen Unternehmen dagegen diversen gesetzlichen Pflichten, die Handlungsspielräume einer CDR einschränken. Die in Art. 69 KIG-E genannten Ziele wie der ökologisch bewusste Technologieeinsatz, die Barrierefreiheit oder Stakeholder-Beteiligung – gleichzeitig zentrale Ziele einer CDR (→ § 2 D. III.) – würden aber weiterhin freiwilligem Unternehmensengagement überlassen bleiben. Damit verbliebe der verantwortungsvolle Einsatz von KI auch bei Inkrafttreten des KIG-E für eine digitale Unternehmensverantwortung weiterhin hochrelevant.

F. Zwischenfazit

Die europäische Regulierungslandschaft prägt zum einen, dass für bestimmte Bereiche bereits ein grundlegender bis weitreichender Rechtsrahmen besteht wie zB im Bereich des Datenschutzes, der Cybersicherheit oder der Regulierung von digitalen Plattformen und Vermittlungsdiensten. Bereits länger bestehende Regulierungen wurden in den vergangenen Jahren ausgeweitet, zB durch die DSGVO (2018) oder den DMA (2022). Zum anderen forciert der europäische Gesetzgeber intensiv die Regulierung weiterer digital- und datenbezogener Sachverhalte durch diverse Gesetzesinitiativen. So werden Eckpfeiler für eine europäische Datenwirtschaft gelegt (DGG, DaG) und Schlüsseltechnologien wie algorithmische Systeme (ua KIG-E) reglementiert. Damit zeigt sich die zunehmende Entstehung eines europäischen Datenrechts bzw. „Datenwirtschaftsrechts“[195].

Für digitale Unternehmensverantwortung folgt daraus, dass die Spielräume freiwilliger Regelsetzung kleiner werden und eine zunehmende Verrechtlichung einsetzt. Hierbei gewinnt die „rechtliche Verantwortung“ iSd vollständigen Beachtung und Umsetzung gesetzlicher Regeln an Bedeutung. Die gesetzliche Normbildung erfolgt dabei nicht im „luftleeren Raum“, sondern in Wechselwirkung mit Stakeholdern – der Entwurf zum KIG belegt eindrücklich, dass Grundsätze aus Ethik-Kodizes von privaten

195 Hennemann/Ditfurth NJW 2022, 1905; Specht-Riemenschneider MMR 2022, 809 (811); Steinrötter RDi 2021, 480 (482ff.).

und öffentlichen Initiativen in gesetzliche Anforderungen einfließen.[196] In die legislative Willensbildung werden über unternehmerische und weitere Interessenvertreter zukünftig auch Erwägungen der CDR einfließen. Als Triebfeder könnte sich dabei erweisen, dass sich die Ziele von europäischer Regulierung und von CDR an mehreren Stellen (ua Datenschutz, Datenzugang) überschneiden und somit einem gleichförmigen Zielbild folgen.

Weiterhin fördert der europäische Gesetzgeber an verschiedenen Stellen die Erarbeitung von Verhaltenskodizes, die gesetzliche Pflichten konkretisieren (→ Art. 40 Abs. 2 DSGVO) oder freiwillige Selbstverpflichtungen betreffen (→ Art. 69 Abs. 2 KIG-E). Hier verbleiben also nicht nur rechtliche „Lücken", sondern explizite Spielräume für selbstregulierende Normbildung iRd Corporate Digital Responsibility.[197]

G. Ausblick ins nationale Recht

Auch EU-Mitgliedstaaten regeln digital- und datenbezogene Sachverhalte, entweder in Vorgriff oder als Ergänzung etwaiger EU-Vorschriften. In Deutschland existiert insb. für öffentliche Datenbereitsteller bereits ein Datennutzungsgesetz.[198] Im aktuellen Koalitionsvertrag werden ua ein Datengesetz, Datentreuhandgesetz und ein Forschungsdatengesetz angekündigt.[199] Von Interesse ist auch ein Blick nach Dänemark: in das dortige Gesetz über Jahresabschlüsse wurde 2020 eine Pflicht für große Unternehmen aufgenommen, nach dem „Comply or Explain"-Prinzip über ihre Arbeit und ihre Politik in Bezug auf datenethische Fragen zu berichten.[200]

196 Vgl. COM(2021) 206 final, 9f.; zur Durchführung von Folgeabschätzungen und Beteiligung von Stakeholdern bei EU-Initiativen, siehe https://ec.europa.eu/info/law/law-making-process/planning-and-proposing-law/impact-assessments_de (Stand 1.12.2023).

197 Dazu auch Dürr ZGE 2021, 165 (174ff.); Pauly/Wichert DB-Beil. Heft 21/2023, 44 (47).

198 Gesetz für die Nutzung von Daten des öffentlichen Sektors (Datennutzungsgesetz) vom 16.07.2021, BGBl. I 2941, 2946.

199 Koalitionsvertrag 2021–2025 zwischen der SPD, Bündnis 90 / Die Grünen und der FDP, Mehr Fortschritt wagen, Bündnis für Freiheit, Gerechtigkeit und Nachhaltigkeit, abrufbar unter: https://www.spd.de/fileadmin/Dokumente/Koalitionsvertrag/Koalitionsvertrag_2021-2025.pdf (Stand 1.12.2023), S. 14, 18.

200 Siehe § 99d im Gesetz zur Änderung des Jahresabschlussgesetzes vom 26.05.2020, Nr. L 124 B, abrufbar unter: https://www.ft.dk/ripdf/samling/20191/lovforslag/l124b/20191_l124b_som_vedtaget.pdf (Stand 1.12.2023).

Es bleibt abzuwarten, ob solche oder ähnliche Berichterstattungspflichten in anderen Mitgliedstaaten oder auf EU-Ebene eingeführt werden. Der bestehende deutsche und unionsrechtliche Rahmen sieht bislang keine spezifische Berichterstattungspflicht von Unternehmen zu digitalethischen oder CDR-bezogenen Fragen vor.[201]

§ 4 Fazit

Auf Grundlage der vorangegangenen Untersuchung ergeben sich für die Rolle der Corporate Digital Responsibility im Kontext eines entstehenden Datenrechts und mögliche zukünftige Wege einer rechtlichen Implementierung von CDR derzeit folgende Schlussfolgerungen.

In der Europäischen Union bewegt sich das Konzept der CDR in einem dynamischen rechtlichen Kontext, der sich durch einen zunehmenden digital- und datenrechtlichen Regulierungsdruck auszeichnet. Die zu erwartende und voranschreitende Verrechtlichung kann die Aktionsräume einer freiwilligen digitalen Unternehmensverantwortung reduzieren. Dadurch kann sich unternehmerisches CDR-Engagement perspektivisch verändern und sich der Fokus auf rechtliche Compliance verlagern. Gleichzeitig zeigt der Gesetzgebungsprozess zur europäischen KI-Verordnung beispielhaft, dass digitalrechtliche Gesetzesvorhaben und ihre Regulierungstiefe kontrovers diskutiert werden und sich die verfolgten Regulierungsansätze dynamisch verändern können. Letzteres vor allem vor dem Hintergrund von sich verändernden politischen Agenden und gesamtwirtschaftlichen Entwicklungen, die mit verstärkten Forderungen nach weniger Bürokratie und Regelungslast einhergehen.

Damit kommen CDR zwei wichtige rechtliche Funktionen zu: Einerseits ermöglicht CDR proaktive Selbstregulierung und kann Orientierung in einem hoch dynamischen Handlungsfeld sichern, in dem viele Fragen gesetzlich noch nicht reguliert sind oder unternehmerischer Eigenverantwortung überlassen werden. Andererseits können Unternehmen bestehende oder entstehende Lücken und Unsicherheiten in der rechtlichen Regulierung[202] mit CDR-Strategien und -Maßnahmen proaktiv ausfüllen. Wäh-

201 Ausführlich dazu → § 2 C. I.; vgl. RL (EU) 2022/2464 und § 289c HGB; detailliert auch Merbecks BB 2021, 2159 (2161ff.).

202 Zu diesem Aspekt ausführlich: Bahreini/Charton/Lukas RDi 2021, 548 (549); Dürr ZGE 2021, 165 (182f.).

rend gesetzliche Vorschriften vor allem regeln, „was" gemacht oder befolgt werden muss, kann CDR dies ins unternehmerische „wie" übersetzen.

Passend dazu lässt sich im CDR-Diskurs eine starke Fokussierung auf die unternehmenspraktische Integration von digitalverantwortlichen Verhaltensweisen konstatieren. Aus wissenschaftlicher Perspektive ist dabei eine teils nur oberflächliche Auseinandersetzung mit dem gesetzlichen Regulierungsumfeld und eine noch flexible und dogmatisch nicht in sich geschlossene Konzeptualisierung der CDR festzustellen. Die Vielfalt der CDR-Initiativen und eine mögliche heterogene Implementierung in verschiedenen Sektoren und Unternehmen birgt gleichzeitig das Risiko einer desintegrierten Entwicklung von CDR. Eine verstärkte Zusammenführung der unterschiedlichen CDR-Konzeptionen wäre daher wünschenswert, insbesondere auch im Hinblick auf das Potenzial der CDR, zur Transformation von digital- und datenbezogenen Pflichten in „hartes" Recht beizutragen.

Anders als es sich im Bereich der CSR beobachten lässt, scheint das CDR-Konzept als solches bislang (noch) keine Triebfeder für gesetzliche Regulierung zu sein oder ihre inhaltliche Ausgestaltung zu befruchten. So könnten Zielsetzungen der CDR zu verantwortungsvollem digitalen Unternehmenshandeln in gesetzlicher Regulierung implementiert werden, indem beispielsweise Berichterstattungspflichten der CDR-Initiative perspektivisch und in Anlehnung an die digital-ethischen Berichterstattungspflichten in Dänemark ins Recht aufgenommen würden.

Auf der Basis der in dieser Arbeit durchgeführten Bestandsaufnahme zur CDR ergeben sich für zukünftige Wege einer rechtlichen Implementierung von CDR drei Hypothesen:

Erstens werden sich CDR und entstehende Rechtsakte verstärkt gegenseitig sensibilisieren und stimulieren und darüber Zielsetzungen der CDR in die rechtliche Regulierung von digital- und datenbezogenen Sachverhalten einfließen.

Zweitens wird zunehmendes CDR-Engagement in Unternehmen auf andere Marktteilnehmer ausstrahlen, sodass sich für bislang freiwillige Handlungsoptionen der CDR eine wahrgenommene oder faktische Verbindlichkeit[203] ergibt. Die dadurch entstehenden quasi-verbindlichen Handlungsstandards können die Auslegung von gesetzlichen Anforderungen beein-

203 Zu einer faktischen Bindungswirkung Dürr ZGE 2021, 165 (182); Hoffmann-Riem Recht im Sog der digitalen Transformation S. 114; für den Bereich der CSR Spießhofer NZG 2018, 441 (442f.).

flussen oder durch Gesetzgeber aufgegriffen und in „hartes" Recht transformiert werden.

Drittens wird digitale Verantwortung von Unternehmen in einem dynamischen (europäischen und nationalen) Regulierungsumfeld wichtige Beiträge für eine proaktive Selbstregulierung im (entstehenden) Rechtskontext leisten. Zugleich ermöglichen und fördern bestimmte Rechtsakte eine „regulierte Selbstregulierung" (vgl. DSGVO, KIG-E). Beides läuft hoheitlicher Regulierung voraus bzw. parallel und kann deren Normbildung beeinflussen.

Insgesamt zeigen diese Ergebnisse und Schlussfolgerungen, dass CDR für die rechtswissenschaftliche Forschung, das Unternehmenshandeln und die gesellschaftliche Diskussion zu Technologiefolgen ein komplexes und dynamisches Forschungs- und Praxisfeld eröffnet.

Literatur- und Quellenverzeichnis

Assion, Simon/Willecke, Lukas, Der EU Data Act, Die neuen Regelungen zu vernetzten Produkten und Diensten, MMR 2023, 805–810.

Bahreini, Dariush/Charton, Jean Enno/Lucas, Simon, Unternehmensethik 4.0, Eine Darstellung von Zielen, Entwicklung und Inhalt eines Prinzipien-basierten Code of Digital Ethics sowie eine Analyse der normativen Wirkung dieser Leitlinien, RDi 2021, 548–554.

Bertelsmann Stiftung, Wittenberg-Zentrum für Globale Ethik (Hrsg.), Unternehmensverantwortung im digitalen Wandel, Ein Debattenbeitrag zu Corporate Digital Responsibility, Gütersloh 2020, abrufbar unter https://www.bertelsmann-stiftung.de/fileadmin/files/user_upload/UN_Verantwortung_im_digitalen_Wandel.pdf (Stand 1.12.2023).

Boehme-Neßler, Volker, Unscharfes Recht: Überlegungen zur Relativierung des Rechts in der digitalisierten Welt, Berlin 2008.

Bomhard, David/Merkle, Marieke, Der Entwurf eines EU Data Acts, Neue Spielregeln für die Data Economy, RDi 2022, 168–176.

Bundesministerium für Umwelt, Naturschutz, nukleare Sicherheit und Verbraucherschutz (BMUV) (Hrsg.), Corporate Digital Responsibility-Kodex, Freiwillige Selbstverpflichtung mit Bericht, 2021, abrufbar unter https://cdr-initiative.de/uploads/files/2022-02_Kodex_CDR-Initiative.pdf (Stand 1.12.2023).

Brandenburg, Anne/Waurick, Steffen, Corporate Digital Responsibility – freiwillig zu mehr digitaler Verantwortung?, RDi 2023, 365–368.

Cooper, Tim/Siu, Jade/Wei, Kuangyi, Corporate digital responsibility, Doing well by doing good, in: Accenture Outlook, 2015, abrufbar unter https://www.criticaleye.com/inspiring/insights-servfile.cfm?id=4431 (Stand 1.12.2023).

Dörr, Saskia, Praxisleitfaden Corporate Digital Responsibility, Unternehmerische Verantwortung und Nachhaltigkeitsmanagement im Digitalzeitalter, Berlin 2020.

Dürr, Paul, Corporate Digital Responsibility, Digitale Unternehmensverantwortung zwischen Rechtsverbindlichkeit und Selbstregulierung, ZGE 2021, 165–187.

Econsense – Forum Nachhaltige Entwicklung der Deutschen Wirtschaft e.V. (Hrsg.), econsense-Blueprint zur Umsetzung digitaler Verantwortung in Unternehmen, November 2020, abrufbar unter https://econsense.de/wp-content/uploads/2020/11/201119_econsense_Blueprint_D.pdf (Stand 1.12.2023).

Ehmann, Ansbach/Selmayer, Martin, Datenschutz-Grundverordnung, Kommentar, 2. Auflage 2018.

Esselmann, Frank/Brink, Alexander, Digitalverantwortung als Chance, Ökologisches Wirtschaften 33, 2 (2020), 11–13, abrufbar unter https://doi.org/10.14512/OEW350211 (Stand 1.12.2023).

Esselmann, Frank/Golle, Dominik/Thiel, Christian/Brink, Alexander, Corporate Digital Responsibility, Unternehmerische Verantwortung als Chance für die deutsche Wirtschaft, in: Zentrum Digitalisierung.Bayern (Hrsg.), ZD.B Digital Dialogue, Positionspapier, 2020, abrufbar unter https://zentrum-digitalisierung.bayern/wp-content/uploads/ZD.B-Positionspapier_Final_web.pdf (Stand 1.12.2023).

Floridi, Luciano/Taddeo, Mariarosaria, What is data ethics?, Philosophical Transactions of the Royal Society A, 374: 20160360, 2016, abrufbar unter https://doi.org/10.1098/rsta.2016.0360 (Stand 1.12.2023).

Geminn, Christian, Die Regulierung Künstlicher Intelligenz, Anmerkungen zum Entwurf eines Artificial Intelligence Act, ZD 2021, 354–359.

Gielen, Nico/Uphues, Steffen, Digital Markets Act und Digital Services Act, Regulierung von Markt- und Meinungsmacht durch die Europäische Union, EuZW 2021, 627–637.

Hamadi, Hassan/Manzo, Claudia, "Corporate Digital Responsibility", A Study on Managerial Challenges for AI integration in Business, 2021, abrufbar unter https://lup.lub.lu.se/student-papers/search/publication/9052507 (Stand 1.12.2023).

Hennemann, Moritz/von Ditfurth, Lukas, Datenintermediäre und Data Governance Act, NJW 2022, 1905–1910.

Herden, Christina/Alliu, Ervin/Cakici, André/Cormier, Thibaut et al., "Corporate Digital Responsibility", New corporate responsibilities in the digital age, NachhaltigkeitsManagementForum 29 (2021), 13–29, abrufbar unter https://link.springer.com/article/10.1007/s00550-020-00509-x (Stand 1.12.2023).

Hoffmann-Riem, Wolfgang, Recht im Sog der digitalen Transformation, Tübingen 2022.

idigiT – Institute for Digital Transformation in Healthcare (Hrsg.), Zwischen Unternehmenswerten und Operationalisierung – Digital-ethischer Umgang mit neuen Technologien, idigiT Studie: Leitlinien zu digitaler Ethik in Europa, August 2022, abrufbar unter https://www.transforming-healthcare.com/insights/ (Stand 1.12.2023).

Kettner, Sara Elisa/Thorun, Christian, Corporate Digital Responsibility, Ergebnisse eine repräsentativen Verbraucherbefragung, in: ConPolicy Institut für Verbraucherpolitik (Hrsg.), 27.4.2021, abrufbar unter https://cdr-initiative.de/uploads/files/210503_Umfrage_FInal_Faktenblatt_CDR.pdf (Stand 1.12.2023). (zitiert: Kettner/Thorun, Corporate Digital Responsibility-Verbraucherbefragung)

Lobschat, Lara/Mueller, Benjamin/Eggers, Felix/Brandimarte, Laura et al., Corporate digital responsibility, Journal of Business Research 122 (2021), 875–888, abrufbar unter https://doi.org/10.1016/j.jbusres.2019.10.006 (Stand 1.12.2023).

Merbecks, Ute, Corporate Digital Responsibility: neue Herausforderungen für die nichtfinanzielle Berichterstattung, BB 2021, 2159–2163.

Mihale-Wilson, Cristina/Hinz, Oliver/van der Aalst, Wil/Weinhardt, Christof, Corporate Digital Responsibility, Relevance and Opportunities for Business and Information Systems Engineering, Business & Information Systems Engineering 64 (2022), 127–132, abrufbar unter https://doi.org/10.1007/s12599-022-00746-y (Stand 1.12.2023).

Mittwoch, Anne-Christin, Digitalisierung und Nachhaltigkeit – Praktische Konvergenzen zweier Leitdiskurse im Unternehmensrecht, JZ 2023, 376–384.

Mittwoch, Anne-Christin, Nachhaltigkeit und Unternehmensrecht, Tübingen 2022.

Möslein, Florian, Corporate Digital Responsibility: Eine aktienrechtliche Skizze, in: Grundmann, Stefan/Merkt, Hanno/Mülbert, Peter O. (Hrsg.), Festschrift für Klaus J. Hopt zum 80. Geburtstag am 24. August 2020, Berlin/Boston 2020, 805–823.

Mueller, Benjamin, Corporate Digital Responsibility, Business & Information Systems Engineering 64 (2022), 689–700, abrufbar unter https://doi.org/10.1007/s12599-022-00760-0 (Stand 1.12.2023).

Nietsch, Michael, Corporate Social Responsibility Compliance, München 2021.

Noack, Ulrich, Organisationspflichten und -Strukturen kraft Digitalisierung, ZHR 183 (2019), 105–144.

Nüßing, Christoph, Eine digitale Magna Carta? Die Europäische Erklärung zu digitalen Rechten, MMR 2022, 341–342.

Orssich, Irina, Das europäische Konzept für vertrauenswürdige Künstliche Intelligenz, EuZW 2022, 254–261.

Paal, Boris/Pauly, Daniel, Datenschutz-Grundverordnung, Bundesdatenschutzgesetz, 3. Auflage, München 2021.

Panzer-Heemeier, Andrea/Nemat, André T., Digitale Ethik – Eine neue Chance für ESG-Compliance, CCZ 2022, 223–230.

Panzer-Heemeier, Andrea/Nemat, André T./Meckenstock, Cordula, ESG 2.0 – Digitale Ethik als neue Dimension der Nachhaltigkeit, ESG 2022, 104–109.

Pauly, Daniel/Wichert, Felix, Corporate Digital Responsibility, digitale Ethik & Co., Datenverarbeitungen und digitale Technologie in der ESG-Strategie, DB-Beil. Heft 21/2023, 44–47.

Podszun, Rupprecht/Bongartz, Philipp/Kirk, Alexander, Digital Markets Act – Neue Regeln für Fairness in der Plattformökonomie, NJW 2022, 3249–3254.

Richter, Frederick, Aus Sicht der Stiftung Datenschutz: CDR – More Than Just a Hype?, Privacy in Germany (PinG) 2018 Nr. 6, 237–238.

Schildbach, Roman, Zugang zu Daten der öffentlichen Hand und Datenaltruismus nach dem Entwurf des Daten-Governance-Gesetzes, ZD 2022, 148–153.

Schliesky, Utz, Digitale Ethik und Recht, NJW 2019, 3692–3697.

Schmidt, Stephan, Neue europäische Anforderungen im Cybersicherheitsrecht – die NIS2-Richtlinie im Überblick, Kommunikation & Recht (K&R) 2023, 705–710.

Schürmann, Kathrin, Datenschutz-Folgenabschätzung beim Einsatz Künstlicher Intelligenz, ZD 2022, 316–321.

Schweitzer, Heike, Digitale Plattformen als private Gesetzgeber: Ein Perspektivwechsel für die europäische „Plattform-Regulierung", ZEuP 2019, 1–12.

Specht-Riemenschneider, Louisa, Der Entwurf des Data Act, Eine Analyse der vorgesehenen Datenzugangsansprüche im Verhältnis B2B, B2C und B2G, MMR 2022, 809–826.

Spießhofer, Birgit, Compliance und Corporate Social Responsibility, NZG 2018, 441–447.

Spießhofer, Birgit, Unternehmerische Verantwortung, Zur Entstehung einer globalen Wirtschaftsordnung, Baden-Baden 2017.

Steinrötter, Björn, Gegenstand und Bausteine eines EU-Datenwirtschaftsrechts, RDi 2021, 480–486.

Teicke, Tobias, CSR meets Compliance – Über die zunehmende Verrechtlichung der Corporate Social Responsibility, CCZ 2018, 274–275.

Tolks, Daniel, Die finale Fassung des Data Governance Act, Erste Schritte in Richtung einer europäischen Datenwirtschaft, MMR 2022, 444–449.

Thorun, Christian/Kettner, Sara Elisa/Merck, Johannes, Ethik in der Digitalisierung, Der Bedarf für eine Corporate Digital Responsibility, in: Friedrich-Ebert-Stiftung (Hrsg.), WISO Direkt, 17/2018, abrufbar unter https://library.fes.de/pdf-files/wiso/14691.pdf (Stand 1.12.2023).

Wiebe, Andreas, Der Data Act – Innovation oder Illusion?, GRUR 2023, 1569–1578.

Wittmann, Jörn/Haidenthaler, Gregor, IT-Compliance in der Cloud – Rechtssicherheit durch Codes of Conduct?, Anerkannte Verhaltensregeln als Garantie und Nachweis bei der DS-GVO-konformen Cloud-Nutzung, MMR 2022, 8–18.

Wolff, Heinrich Amadeus/Brink, Stefan/von Ungern-Sternberg, Antje (Hrsg.), Beck'scher Online-Kommentar Datenschutzrecht, 45. Edition (Stand: 1.8.2023), München 2023.