Einführung

Daten sind der zentrale Rohstoff der modernen Informationsgesellschaft. Sie bilden die Grundlage neuer Technologien und ermöglichen gesellschaftlichen Fortschritt. Zugleich werden sie von Unternehmen als Wirtschaftsgut behandelt. Es geht nicht nur darum, Dienste zu optimieren oder eine individuelle Werbeansprache zu ermöglichen. Das Recht hatte bisher den Datenschutz im Fokus. Datenwirtschaftliche Aspekte waren zwar bei richtiger Interpretation der DS-GVO gleichrangig zu berücksichtigen.[1] Ausgangspunkt der Abwägung war aber stets der Schutz des Menschen im Zentrum des Datenmarktes. In der jüngeren Vergangenheit hat sich die Erkenntnis durchgesetzt, dass der in der DS-GVO vorgezeichneten Gleichberechtigung von Datenschutz und Datenwirtschaft nicht allein durch diese einseitige Perspektive Rechnung getragen wird. Neben das Datenschutzrecht sind deshalb vermehrt Rechtsakte getreten, die an andere Aspekte der Verarbeitung und insbesondere der Verwertung von Daten anknüpfen. Ihnen liegen wirtschaftliche Erwägungen zugrunde, sie lassen aber die DS-GVO unberührt. Die gesetzgeberischen Initiativen sollen eine konkurrenzfähige Datenwirtschaft in der EU aufbauen, die das Wirtschaften mit Daten unter Wahrung des geltenden Datenschutzrechts fördert. Schließlich adressiert das entstehende Rechtsgebiet datenverarbeitende Technologien. Dazu zählen Angebote der Digitalwirtschaft wie beispielsweise Online-Plattformen, aber auch einzelne Technologien wie die Künstliche Intelligenz (KI). Alle Rechtsakte auf diesem Gebiet sollen den Menschen vor negativen Auswirkungen der technologischen Entwicklung schützen und zugleich einen fairen Wettbewerb ermöglichen. So wächst derzeit, geprägt von Rechtsvorschriften der Europäischen Union, ein Rechtsgebiet heran, das neben dem Datenschutz auch die Datenwirtschaft sowie die datenverarbeitenden Technologien der Digitalwirtschaft und der KI in den Blick nimmt.

Mit einem großen Teil der Vorschriften adressiert der Staat private Akteure und legt ihnen Pflichten auf. Dennoch darf das Datenrecht nicht allein als Teilrechtsgebiet des Öffentlichen Rechts verstanden werden. Immer wieder wirken datenrechtliche Verpflichtungen auf das Zivil- und sogar auf das Strafrecht ein, sodass ähnlich wie beim Medienrecht von einer Querschnittsmaterie zu sprechen ist.

I. Die Europäisierung des Datenrechts

Im Zentrum des entstehenden Datenrechts steht die Digitalstrategie der Europäischen Union (EU).[2] Seit ihrer Veröffentlichung im Jahr 2020 ist eine Vielzahl europäischer Rechtsakte in Kraft getreten, die das neue Rechtsgebiet prä-

1 Dazu *Kühling/Paal/Schwartmann* F.A.Z. v. 20.10.2022, 6.

2 *Europäische Kommission*, Gestaltung der digitalen Zukunft Europas, COM(2020) 67 final.

gen.[3] Die Arbeitsweise der EU beim Erlass dieser Rechtsakte wird vorgegeben durch den Vertrag über die Arbeitsweise der Europäischen Union (**AEUV** → Nr. 1), während ihre materiell-rechtlichen Grundlagen vor allem in der Charta der Grundrechte der Europäischen Union (**GRCh** → Nr. 2) zu finden sind. Zur Regulierung der datenrechtlichen Materie bedient sich die EU der in Art. 288 Abs. 1 AEUV vorgesehenen Rechtsakte. Von besonderer Relevanz sind dabei Verordnungen und Richtlinien. Verordnungen haben allgemeine Geltung, sind in allen ihren Teilen verbindlich und gelten unmittelbar in jedem Mitgliedstaat. Dagegen sind Richtlinien nur hinsichtlich des zu erreichenden Ziels verbindlich. Sie überlassen den Mitgliedstaaten der EU die Wahl der Form und der Mittel, um das vorgegebene Ziel zu erreichen. Richtlinien müssen deshalb durch die Mitgliedstaaten in nationalem Recht umgesetzt werden. Den Rechtsakten der EU sind üblicherweise Erwägungsgründe vorangestellt. Diese sind rechtlich nicht verbindlich.[4] Vielmehr handelt es sich um die Begründung des europäischen Normgebers. Erwägungsgründe sind deshalb zwar eine wichtige Auslegungshilfe, eine darauf gestützte Auslegung darf aber nicht dem Wortlaut der Norm widersprechen.

Mit der Europäisierung des Datenrechts beschränkt sich die Aufgabe des nationalen Gesetzgebers immer stärker darauf, die Vorgaben des Rechts der EU im nationalen Recht umzusetzen. Im Fall einer Richtlinie ist eine umfassende Umsetzung erforderlich: Der nationale Gesetzgeber muss also Gesetze erlassen, die den Zielen der Richtlinie entsprechen. Im Falle einer Verordnung ist der Umsetzungsspielraum des nationalen Gesetzgebers dagegen begrenzt. Er kann eigene Regelungen im Anwendungsbereich der Verordnung nur erlassen, wenn die Verordnung eine sogenannte Öffnungsklausel vorsieht. Dabei handelt es sich um eine Vorschrift, die den Mitgliedstaaten ausdrücklich die Möglichkeit zuweist, eigene Bestimmungen für eine konkrete Regelungsmaterie zu erlassen. Außerhalb solcher Öffnungsklauseln verbleibt den Mitgliedstaaten – vorbehaltlich der verfassungsrechtlichen Grenzen aus Art. 23 GG – nur die Regelung der Aufsicht über die Durchsetzung der Verordnung, insbesondere durch die Benennung der zuständigen Behörden.

II. Grundrechte

Der individuelle Schutz im Datenrecht findet seine materiell-rechtliche Prägung in den Grundrechten. Sein primäres Ziel liegt im Schutz des Privatlebens natürlicher Personen.

1. Grundgesetz

Die grundrechtliche Basis des Datenschutzrechts im Grundgesetz (**GG** → Nr. 4) findet sich im Recht auf informationelle Selbstbestimmung, das das Bundesverfassungsgericht im Volkszählungsurteil 1983 aus dem allgemeinen

3 Umfassender Überblick bei *Zenner* RDV 2023, 72 f.
4 EuGH Urt. V. 19.6.2014 – C-345/13, ECLI:EU:C:2014:2013 Rn. 31.

Persönlichkeitsrecht abgeleitet hat.[5] Es schützt den Einzelnen vor der unbegrenzten Verarbeitung seiner persönlichen Daten unter den Bedingungen der modernen Datenverarbeitung. In seiner abwehrrechtlichen Dimension bietet es Schutz vor unangemessenen Überwachungsmaßnahmen des Staates gegenüber seinen Bürgern. Abzugrenzen ist das Recht auf informationelle Selbstbestimmung in erster Linie vom Brief-, Post- und Fernmeldegeheimnis des Art. 10 Abs. 1 GG sowie von der Unverletzlichkeit der Wohnung gemäß Art. 13 Abs. 1 GG. Ersteres schützt die Vertraulichkeit individueller Distanzkommunikation und damit vor einem staatlichen Zugriff auf die Kommunikationsinhalte sowie die Umstände der Kommunikation. Die Unverletzlichkeit der Wohnung schützt hingegen eine private, räumliche Sphäre vor staatlichem Eindringen und Überwachung. Da die genannten Grundrechte – und damit insbesondere das Recht auf informationelle Selbstbestimmung – nicht hinreichend vor einem Zugriff auf die riesigen Datenbestände schützen, die bei der modernen Nutzung vernetzter Produkte anfallen, hat das Bundesverfassungsgericht zudem im Jahr 2008 das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme aus dem allgemeinen Persönlichkeitsrecht abgeleitet.[6] Dieses gewährleitet einen subsidiären grundrechtlichen Schutz vor staatlichem Zugriff auf Computer, Smartphone und andere IT-Systeme.

Die Bedeutung der genannten Grundrechte nimmt zwar im Laufe der Europäisierung des Datenrechts ab, ist aber weiterhin nicht zu vernachlässigen. Grundsätzlich gehen das Primär- und Sekundärrecht der EU dem gesamten nationalen Recht und folglich auch dem GG vor. Sofern das europäische Recht dem nationalen Gesetzgeber aber einen Umsetzungsspielraum eröffnet, ist dieser an die Vorgaben des GG gebunden. Besteht kein Umsetzungsspielraum, muss der nationale Gesetzgeber die Vorgaben des Rechts der EU akzeptieren. Eine Prüfung dieser Vorgaben beschränkt sich dann auf die Kontrolle, ob die Identität der Verfassung unberührt bleibt.[7]

2. Charta der Grundrechte der Europäischen Union

Von wachsender Bedeutung ist dagegen die Charta der Grundrechte der Europäischen Union und ihre Auslegung durch den EuGH. Die EU hat die GRCh in Art. 6 Abs. 1 des EU-Vertrags anerkannt. Sie sind damit Bestandteil des europäischen Primärrechts. Sekundärrecht, also insbesondere Verordnungen und Richtlinien, muss sich daher an den in der GRCh niedergelegten Rechten, Freiheiten und Grundsätzen messen lassen. Von zentraler Bedeutung für das Datenschutzrecht ist insofern das Recht auf Schutz personenbezogener Daten. Dieses ist ausdrücklich in Art. 8 Abs. 1 GRCh verankert, wird aber vom EuGH regelmäßig in Verbindung mit dem Recht auf Achtung des Privatlebens aus Art. 7 GRCh geprüft. Das Grundrecht verlangt, dass Daten nur nach Treu und

5 BVerfG Urt. v. 15.12.1983 – 1 BvR 209/83, BVerfGE 65, 1.
6 BVerfG Urt. v. 27.2.2008 – 1 BvR 370/07, BVerfGE 120, 274.
7 BVerfG Beschl. v. 22.10.1986 – 2 BvR 197/83, BVerfGE 73, 339 (375 f.).

Glauben für festgelegte Zwecke und mit Einwilligung der betroffenen Person oder auf einer sonstigen gesetzlich geregelten Rechtsgrundlage verarbeitet werden.

III. Datenschutzrecht

Bundesverfassungsgericht und EuGH können mittlerweile eine ausdifferenzierte Rechtsprechung zu den datenschutzrechtlichen Grundrechten vorweisen. Eine Ausweitung erfährt das Datenschutzrecht in der Datenschutz-Grundverordnung der EU und im einfachen nationalen Recht.

1. Datenschutz-Grundverordnung

Die Datenschutz-Grundverordnung (**DS-GVO** → Nr. 6) bildet seit 2018 das zentrale Element des Datenschutzrechts in der EU. Die Verordnung ist nur anwendbar, wenn personenbezogene Daten verarbeitet werden. Dann aber adressiert sie nicht nur staatliche Stellen, sondern nimmt grundsätzlich jede Datenverarbeitung in den Blick. Die Antwort auf die Frage, ob ein bestimmtes Datum einen Personenbezug aufweist, ist deshalb eine essenzielle Weichenstellung für die Bedingungen seiner Verarbeitung. Sie entscheidet darüber, ob die umfassenden Vorgaben der DS-GVO beachtet werden müssen. Auf anonymisierte und genuin nichtpersonenbezogene Daten findet die DS-GVO keine Anwendung. Obwohl dem Personenbezug von Daten damit eine zentrale Bedeutung zukommt, herrscht über seine Reichweite Unklarheit. Personenbezogene Daten sind in Art. 4 Nr. 1 DS-GVO legaldefiniert als „alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person" beziehen. Bei der Prüfung der Identifizierbarkeit sind laut Erwägungsgrund 26 S. 3 der DS-GVO alle Mittel zu berücksichtigen, die nach allgemeinem Ermessen wahrscheinlich genutzt werden, um die natürliche Person direkt oder indirekt zu identifizieren. Nach der Rechtsprechung des EuGH basierend auf der Rechtssache Breyer können der Identifizierbarkeit gesetzliche Verbote oder etwa ein unverhältnismäßiger Aufwand an Zeit, Kosten und Arbeitskraft entgegenstehen.[8] Die Unbestimmtheit des unverhältnismäßigen Aufwands führt allerdings zu Rechtsunsicherheit in einer zentralen Frage des Datenschutzrechts.[9]

Sofern ein personenbezogenes Datum verarbeitet wird, muss insbesondere die Person, die über die Zwecke und Mittel der Verarbeitung entscheidet, die Vorgaben der DS-GVO beachten. Sie ist Verantwortlicher im Sinne der Verordnung. Ihre konkreten Pflichten leiten sich aus den Grundsätzen der Datenverarbeitung ab, die der Verordnungsgeber in Art. 5 Abs. 1 DS-GVO niedergelegt hat. Von herausragender Bedeutung ist der Grundsatz der Rechtmäßigkeit der Datenverarbeitung. Es handelt sich dabei um ein Verbot mit Erlaubnisvorbehalt: Nur wenn eine passende Rechtsgrundlage vorliegt, ist die Verarbeitung personenbezogener Daten erlaubt. Einzelne Rechtsgrundlagen sieht die DS-

8 EuGH Urt. v. 19.10.2016 – C-582/14, ECLI:EU:C:2016:779 Rn. 46.

9 Einschlägige Gesetzestexte, ein Leitfaden und Grundregeln für die Praxis finden sich in *Stiftung Datenschutz*, Anonymisierung und Pseudonymisierung von Daten, 2023.

GVO in Art. 6 Abs. 1 DS-GVO vor.[10] Sie umfassen etwa die Einwilligung der betroffenen Person, die Erforderlichkeit der Verarbeitung zur Vertragserfüllung oder auch überwiegende Interessen des Verantwortlichen an der Datenverarbeitung. Die Verarbeitung sensibler Daten, aus denen etwa die politische Meinung oder der Gesundheitszustand hervorgeht, darf nur auf den speziellen Rechtsgrundlagen des Art. 9 Abs. 2 DS-GVO beruhen. Ein Verstoß gegen die DS-GVO kann zu Bußgeldern führen oder, wenn dadurch ein Schaden entstanden ist, einen Schadensersatzanspruch auslösen. Letzterer ergibt sich vorrangig aus der speziellen Anspruchsgrundlage des Art. 82 Abs. 1 DS-GVO.

2. Nationales Datenschutzrecht

Nationale Kompetenzen im Datenschutzrecht bestehen für Regelungsmaterien, für die die DS-GVO eine Öffnungsklausel vorsieht oder die außerhalb des Anwendungsbereichs der DS-GVO liegen. Von besonderer Bedeutung ist das Bundesdatenschutzgesetz (**BDSG** → Nr. 7). Das BDSG füllt zunächst die Spielräume des nationalen Gesetzgebers im Anwendungsbereich der DS-GVO aus, indem es die Datenschutzaufsichtsbehörden auf Bundes- und Länderebene festlegt. Darüber hinaus sieht es Rechtsgrundlagen für Verarbeitungskontexte vor, für die die DS-GVO eine Öffnungsklausel enthält und konkretisiert die Rechte der betroffenen Personen. Außerdem setzt das BDSG die Vorgaben der JI-Richtlinie für öffentliche Stellen des Bundes um. Es geht dabei um die Verarbeitung personenbezogener Daten durch die für die Verhütung, Ermittlung, Aufdeckung, Verfolgung oder Ahndung von Straftaten oder Ordnungswidrigkeiten zuständigen öffentlichen Stellen des Bundes. Diese Verarbeitungssituation ist ausdrücklich vom Anwendungsbereich der DS-GVO ausgenommen. Für die öffentlichen Stellen der Länder finden sich entsprechende Vorschriften zur Umsetzung der JI-Richtlinie in den Landesdatenschutzgesetzen und in den jeweiligen Polizeigesetzen.

Vorschriften zum Schutz des Fernmeldegeheimnisses und zum Datenschutz bei Telekommunikationsdiensten und digitalen Diensten enthält das Gesetz über den Datenschutz und den Schutz der Privatsphäre in der Telekommunikation und bei digitalen Diensten (**TDDDG** → Nr. 8). Der ursprüngliche Name des Gesetzes, Telekommunikations-Telemedien-Datenschutzgesetz (TTDSG) wurde im Zuge der Umsetzung des Digital Services Acts im nationalen Recht geändert. Das TDDDG beruht zum Teil auf der sogenannten ePrivacy-Richtlinie, die durch die seit geraumer Zeit geplante ePrivacy-Verordnung abgelöst werden soll. Die Richtlinie und damit auch das TDDDG, soweit es auf der Richtlinie beruht, gehen der Anwendung der DS-GVO gemäß Art. 95 DS-GVO vor. Von besonderer praktischer Bedeutung ist § 25 Abs. 1 TDDDG, der die Einwilligung des Nutzers verlangt, wenn Informationen in seiner Endeinrichtung gespeichert werden sollen oder auf Informationen in seiner Endeinrichtung zugegriffen werden soll. Die technisch für solche Vorgänge erforderli-

10 *Schwartmann/Jacquemain* in *Schwartmann/Jaspers/Thüsing/Kugelmann*, HK DS-GVO/BDSG, 3. Aufl. 2024, Art. 6 Rn. 6.

chen „Cookies“ sind begriffsbildend für die sogenannten Cookie-Banner, die dem Zugriff auf Websites regelmäßig vorgeschaltet sind. Eine neue, nationale Rechtsverordnung mit dem Spitznamen Cookie-Banner-Verordnung[11] soll die Zahl der Cookie-Banner reduzieren, indem die Präferenzen der Nutzer von Diensten zur Einwilligungsverwaltung gespeichert werden.

Einige Verletzungen des persönlichen Lebens- und Geheimbereichs sind im Strafgesetzbuch (**StGB** → Nr. 9) mit strafrechtlichen Sanktionen bewährt. Dazu zählen etwa die Verletzung der Vertraulichkeit des Wortes oder des höchstpersönlichen Lebensbereichs oder das Ausspähen und Abfangen von Daten.

IV. Datenwirtschaftsrecht

Ziel der DS-GVO ist gemäß Art. 1 Abs. 1 DS-GVO neben dem Schutz personenbezogener Daten ausdrücklich der Schutz des freien Verkehrs solcher Daten. Mit diesen Zielen korrespondierend haben die Aufsichtsbehörden gemäß Art. 51 Abs. 1 DS-GVO die Aufgabe, die Grundrechte und Grundfreiheiten natürlicher Personen bei der Verarbeitung personenbezogener Daten zu schützen und den freien Verkehr personenbezogener Daten in der Union zu erleichtern. Trotzdem wird die DS-GVO oftmals als Hindernis für den Aufbau einer starken europäischen Datenwirtschaft wahrgenommen. Nach der Konzeption der Verordnung ist das nachvollziehbar. Anknüpfungspunkt der DS-GVO ist der Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten. Entsprechend wird der Rechtsakt durch den EuGH ausgelegt und entsprechend legen die Aufsichtsbehörden regelmäßig ihren Fokus auf diesen Aspekt. Aus diesem Grund ist es nicht verwunderlich, dass in der Wirtschaft personenbezogene Daten in vorauseilendem Gehorsam bisweilen mit übermäßiger Vorsicht behandelt werden. In der Folge wird die mangelnde Gewichtung der gegenläufigen unternehmerischen Freiheiten beklagt, deren Gleichrangigkeit in der Abwägung insbesondere Erwägungsgrund 4 der DS-GVO betont.[12] Da auch beim Gesetzgeber die Erkenntnis Platz gegriffen hat, dass eine funktionierende Datenwirtschaft aus den eingangs beschriebenen Gründen von großer Bedeutung für die wirtschaftliche Konkurrenzfähigkeit der EU ist, soll deren Aufbau nun durch neue Rechtsakte vorangetrieben werden.

1. Data Act

Einen Grundstein des neuen Datenwirtschaftsrechts bildet der Data Act (**DA** → Nr. 11). Im Fokus dieser Verordnung stehen Daten, die bei der Nutzung von

11 Verordnung nach § 26 Absatz 2 des Telekommunikation-Digitale-Dienste-Datenschutz-Gesetzes und zur Änderung der Besonderen Gebührenverordnung Telekommunikation (Einwilligungsverwaltungsverordnung – EinwV). Der von der Bundesregierung beschlossene Entwurf ist abrufbar unter https://dserver.bundestag.de/btd/20/127/2012718.pdf (zuletzt abgerufen am 16.10.2024). Zu den Anforderungen des § 26 Abs. 1 TDDDG (vormals TTDSG) an entsprechende Dienste *Benedikt/Weiß* in *Schwartmann/Jaspers/Eckhardt* HK TTDSG, 1. Aufl. 2022, § 26 TTDSG Rn. 7–24.

12 *Kühling/Paal/Schwartmann* F.A.Z. v. 20.10.2022, 6.

Produkten, die mit dem Internet verbunden sind, erhoben werden. Beispiele für derart vernetzte Produkte sind etwa Lifestyle-Produkte wie Smartwatches, Haushaltsgeräte wie Kühlschränke oder Saugroboter, aber auch Fahrzeuge und Schiffe. Bei der Nutzung dieser Produkte und der mit ihnen verbundenen Dienste fällt ein enormes Datenvolumen an, das mithilfe des DA zugänglich und nutzbar gemacht werden soll. Dazu wird dem Nutzer ein Recht auf Zugang zu den erhobenen Daten gewährt. Er soll gemäß Art. 3 Abs. 1 DA direkt von dem betreffenden Produkt oder Dienst aus auf die Daten zugreifen können. Zumindest aber muss der Dateninhaber dem Nutzer die entsprechenden Daten kontinuierlich und in Echtzeit bereitstellen, Art. 4 Abs. 1 DA. Der Nutzer kann gemäß Art. 5 Abs. 1 DA auch verlangen, dass die Daten unmittelbar an Dritte weitergegeben werden. So sollen andere Anbieter die Möglichkeit erhalten, Reparaturdienstleistungen anzubieten oder ihre Produktionslinien und ihr Lieferkettenmanagement zu optimieren. Konkurrenzprobleme zwischen den Rechtsakten des Datenschutzrechts und des Datenwirtschaftsrechts sind vorgezeichnet, sofern mit personenbezogenen Daten gehandelt wird. Das Verhältnis zwischen den Teilrechtsgebieten ist zwar in einigen Vorschriften des DA angelegt, es wird aber in der Rechtsanwendung zu konkretisieren sein.

Die Vorschriften des DA verdeutlichen die neue Interpretation von Daten im Recht. Sie werden nicht mehr nur als Einfallstor für Eingriffe in den privaten Lebensbereich natürlicher Personen verstanden, sondern zunehmend als Wirtschaftsgut anerkannt. Diese Entwicklung hat sich bereits vor Inkrafttreten des DA an der Richtlinie über bestimmte vertragsrechtliche Aspekte der Bereitstellung digitaler Inhalte und digitaler Dienstleistungen gezeigt, die im BGB umgesetzt ist und die Möglichkeit des Zahlens mit Daten vorsieht. Daten als Wirtschaftsgut werden auch in der jüngeren Rechtsprechung des EuGH anerkannt. Demnach kann der Anbieter einer Website grundsätzlich eine Einwilligung in die Verarbeitung personenbezogener Daten zu Werbezwecken verlangen, wenn er zugleich eine kostenpflichtige Alternativnutzung ohne entsprechende Datenverarbeitungen anbietet (sogenannte „Pay or Consent"-Modelle).[13] Wie teuer die kostenpflichtige Nutzung sein darf, damit die alternativ erforderliche Einwilligung als freiwillig erteilt gilt, wird derzeit noch austariert.

2. Data Governance Act

Anders als der DA verpflichtet der Data Governance Act (**DGA** → Nr. 12) nicht zum Datenaustausch, sondern sieht einen Rahmen vor, der das Vertrauen in den freiwilligen Datenaustausch fördern soll. Dazu werden in Art. 5 DGA Bedingungen für die Weiterverwendung bestimmter Kategorien geschützter Daten festgelegt, die sich im Besitz öffentlicher Stellen befinden. Außerdem wird das Erbringen von Datenvermittlungsdiensten in Art. 10 ff. DGA besonderen Anforderungen unterstellt. Bei Datenvermittlungsdiensten handelt sich um Dienste, die potenzielle Datennutzer mit Dateninhabern oder natürlichen Personen in Kontakt bringen und einen Datenaustausch fördern. Schließlich

13 EuGH Urt. v. 4.7.2023 – C-252/21, ECLI:EU:C:2023:537 Rn. 150.

werden die Mitgliedstaaten in Art. 16 DGA ermächtigt, Datenaltruismus durch organisatorische oder technische Regelungen zu fördern

V. Digitalrecht

Basierend auf datenverarbeitenden Technologien hat sich ein eigener Wirtschaftszweig herausgebildet, die sogenannte Digitalwirtschaft. Diese finanziert sich zu einem großen Teil aus Daten als Wirtschaftsgütern. Kurz gesagt erheben die Anbieter digitaler Dienste Daten ihrer Nutzer und verkaufen sie an Dritte, etwa zu Werbezwecken oder zur Produktoptimierung. Besonders viele Daten können in der Digitalwirtschaft erhoben werden, wenn die Interaktionsdauer des Nutzers mit dem digitalen Dienst erhöht wird. Im Kampf um die begrenzte Aufmerksamkeit der Nutzer haben die Akteure der Digitalwirtschaft deshalb Praktiken entwickelt, die der europäische Gesetzgeber für spezifisch regulierungsbedürftig hält.

1. Digital Services Act

Der Digital Services Act (**DSA** → Nr. 14) dient in erster Linie dem Schutz von Grundrechten im Internet. Ein zentrales Anliegen der Verordnung ist die Eingrenzung der Verbreitung rechtswidriger Inhalte über digitale Dienste. Der DSA adressiert dazu verschiedene Dienste der Informationsgesellschaft und verfolgt dabei einen risikobasierten Regulierungsansatz, wie er für die Daten- und Digitalregulierung der EU mittlerweile als typisch bezeichnet werden kann.

Auf der untersten Stufe der Regulierung befinden sich Vermittlungsdienste, die eine reine Durchleitung von Informationen anbieten. Dazu zählen beispielsweise Internetanbieter. Auch das Angebot sogenannter Caching-Leistungen wird im DSA mit einem vergleichsweise kleinen Pflichtenkatalog belegt. Bei einer Caching-Leistung werden die übermittelten Informationen für einen bestimmten Zeitraum zwischengespeichert, damit ein erneuter Abruf schneller erfolgen kann. Für diese Vermittlungsdienste gelten die in Art. 4–10 DSA festgelegten Haftungserleichterungen, die im deutschen Recht bisher im Telemediengesetz geregelt waren, nun aber vom DSA verdrängt wurden. Die Vermittlungsdienste müssen im Gegenzug eine Kontaktstelle benennen und sicherstellen, dass ihre Allgemeinen Geschäftsbedingungen (AGB) den Anforderungen des Art. 14 DSA genügen.

Die genannten Vorschriften gelten auch für sogenannte Hosting-Dienste, die darin bestehen, von einem Nutzer bereitgestellte Informationen in dessen Auftrag zu speichern. Typische Hosting-Dienste sind etwa Cloud-Dienste. Über die allgemeinen Vorgaben für alle Vermittlungsdienste hinaus müssen die Anbieter derartiger Hosting-Dienste gem. Art. 16 DSA auch ein Melde- und Abhilfeverfahren zur Bekämpfung rechtswidriger Inhalte einrichten. Beschränkt der Anbieter des Hosting-Diensts dessen Nutzbarkeit gegenüber einem Nutzer oder sperrt er ein Konto, so muss er diese Maßnahmen gemäß Art. 17 DSA begründen.

Ebenfalls zu den Hosting-Diensten zählt die Bereitstellung sogenannter Online-Plattformen. Dabei handelt es sich beispielsweise um Online-Marktplätze, App-Stores oder Soziale Netzwerke. Neben den genannten Pflichten für alle Hosting-Dienste müssen die Anbieter von Online-Plattformen weitere spezifische Pflichten erfüllen. Dazu zählen die Einrichtung eines umfassenden internen Beschwerdemanagementsystems (Art. 20 DSA), besondere Transparenzberichtspflichten (Art. 24 DSA) sowie die Offenlegung der wichtigsten Parameter der eingesetzten Empfehlungssysteme (Art. 27 DSA).

Sehr große Online-Plattformen (engl.: very large online platforms, VLOPs) und Suchmaschinen bergen nach Ansicht des Verordnungsgebers ein systemisches Risiko. Zu diesen Diensten zählen etwa besonders große Soziale Netzwerke wie TikTok, Instagram oder LinkedIn, Online-Marktplätze wie Amazon, Zalando und AliExpress und die Suchmaschinen von Google und Bing. Die Anbieter dieser Dienste müssen gemäß Art. 34 Abs. 1 DSA eine Risikobewertung vornehmen und gemäß Art. 35 Abs. 1 DSA Maßnahmen zur Minderung erkannter Risiken ergreifen. Für zahlreiche Nutzer hat sich außerdem die Pflicht des Art. 38 DSA bemerkbar gemacht, wonach die Anbieter der genannten Dienste verpflichtet sind, mindestens eine Option für jedes ihrer Empfehlungssysteme anzubieten, die nicht auf der datenbezogenen Analyse persönlicher Aspekte beruht (sogenanntes Profiling, legaldefiniert in Art. 4 Nr. 4 DS-GVO).

2. Digital Markets Act

Der Digital Markets Act (**DMA** → Nr. 15) adressiert Online-Plattformen, die zwischen Nutzern und Unternehmen vermitteln und in dieser Rolle eine besonders starke Position am Markt einnehmen. Sie werden als Torwächter (engl.: Gatekeeper) bezeichnet. Designierte Gatekeeper in der EU sind beispielsweise zahlreiche Google-Dienste, Amazon, der AppStore von Apple sowie booking.com. Aufgrund ihrer Marktmacht können diese Gatekeeper ihre Interessen in marktschädigender Weise durchsetzen, etwa indem sie die eigenen Produkte oder Dienstleistungen auf den Plattformen bevorzugt anbieten, einzelne Konkurrenten gezielt verdrängen oder die auf der Plattform vertretenen Unternehmen zur Unterzeichnung sogenannter Bestpreisklauseln zwingen. Um einen fairen Wettbewerb sicherzustellen, verbietet der DMA ihnen deshalb in Art. 6 Abs. 5 S. 1 DMA eine bevorzugte Behandlung der eigenen Produkte und Dienstleistungen. Darüber hinaus dürfen sie unter anderem ihre Geschäftskunden nicht daran hindern, ihre Produkte und Dienstleistungen auf Drittplattformen zu anderen Konditionen und Preisen anzubieten (Art. 5 Abs. 3 DMA).

3. Nationales Digitalwirtschaftsrecht

Auch das außerhalb dieser speziellen Rechtsakte geltende, insbesondere nationale Recht enthält eine Vielzahl von Vorschriften, die das Verhältnis der Digitalunternehmen untereinander und zu ihren Nutzern regeln. So sind hinsichtlich des Nutzungsvertrags zwischen dem digitalen Dienst und seinem Nutzer

die Vorschriften des Bürgerlichen Gesetzbuchs (**BGB** → Nr. 17) zu berücksichtigen. Rechtsprobleme ergeben sich hier etwa bei der Frage, ob der Diensteanbieter unliebsame Beiträge seiner Nutzer löschen darf. Die Meinungsfreiheit des Nutzers entfaltet eine mittelbare Drittwirkung auf das Vertragsverhältnis und schränkt das sogenannte virtuelle Hausrecht des Diensteanbieters ein.[14]

Besondere wettbewerbsrechtliche Vorgaben bei Vorliegen einer marktbeherrschenden Stellung oder einer überragenden marktübergreifenden Bedeutung für den Wettbewerb enthält das Gesetz gegen Wettbewerbsbeschränkungen (**GWB** → Nr. 18). Das GWB gilt komplementär zum DMA. Das nationale Wettbewerbsrecht greift deshalb nur, wenn Unternehmen nicht als Gatekeeper benannt, zugleich aber die Voraussetzungen des GWB erfüllt sind oder wenn Maßnahmen des nationalen Wettbewerbsrechts aufgrund der besonderen Marktstellung eines Unternehmens über die Vorgaben des DMA hinausgehen (Art. 1 Abs. 6 DMA).

Schließlich verbietet das Gesetz gegen den unlauteren Wettbewerb (**UWG** → Nr. 19) unlautere Geschäftspraktiken. In der Digitalwirtschaft ist insofern vor allem das in § 7 Abs. 1 UWG vorgesehene Verbot von Werbung zu beachten, die den Verbraucher in unzumutbarer Weise belästigt.

VI. KI-Recht

Eine besondere datenverarbeitende Technologie, die in der jüngeren Vergangenheit einen enormen Aufschwung erfahren hat, ist KI. Die Programmierung einer Software verlangt herkömmlicherweise eine genaue Beschreibung des Arbeitsablaufs. Der Programmierer muss also im Sinne einer Wenn-Dann-Regel für jeden Arbeitsschritt festlegen, wie das Computerprogramm zu verfahren hat. Für manche Aufgaben ist eine derart explizite Definition von Handlungsanweisungen aber nicht möglich. Ihre Programmierung wäre zu aufwendig oder der Mensch kennt die erforderlichen Regeln selbst nicht. In diesen Fällen werden Methoden benötigt, mit denen ein Computerprogramm die erforderlichen Handlungsanweisungen selbst aus vorhandenem Wissen oder vorgegebenen Daten ableiten kann. Bei Systemen, die mithilfe solcher Methoden entwickelt wurden, handelt es sich nach der Begriffsbestimmung in Art. 3 Nr. 1 KI-VO um KI-Systeme. Meist ist nicht nachvollziehbar, auf Grundlage welcher Regeln KI-Systeme ihre Ergebnisse generieren. Diese sogenannte Opazität birgt Diskriminierungsrisiken und Gefahren für die Grundrechte und rechtfertigt eine spezifische Regulierung der Systeme und ihres Einsatzes.

1. KI-Verordnung

Die KI-Verordnung (**KI-VO** → Nr. 21) reguliert nach produktsicherheitsrechtlichem Vorbild die Entwicklung und den Betrieb von KI-Systemen. Sie ver-

14 BGH Urt. v. 29.7.2021 – III ZR 179/20, NJW 2021, 3179 (3184 Rn. 54); dazu *Dörr/Schwartmann/Mühlenbeck*, Medienrecht, 2023, Rn. 464–468.

folgt dabei einen risikobasierten Regulierungsansatz.[15] Konkret sieht die KI-VO nach eigener Aussage vier Risikoklassen vor: KI-Systeme, von denen ein unannehmbares Risiko ausgeht, sind grundsätzlich verboten (Art. 5 KI-VO). Für sogenannte Hochrisiko-KI-Systeme gelten strenge Anforderungen. Manche KI-Systeme bergen spezifische Risiken, denen durch die Erfüllung bestimmter Transparenzpflichten begegnet wird (Art. 50 KI-VO). Auf der untersten Stufe der Risikopyramide stehen KI-Systeme, die ein lediglich geringes Risiko bergen. Ihre Entwicklung und ihr Betrieb werden von der KI-VO nicht reguliert. Hinsichtlich der Vierteilung der Risikoklassen gilt zu beachten, dass auch von Hochrisiko-KI-Systemen spezifische Risiken ausgehen können, die die Transparenzpflichten des Art. 50 KI-VO auslösen.

Mit dem umfangreichsten Pflichtenprogramm versehen sind die Entwicklung und der Betrieb von Hochrisiko-KI-Systemen. Die Klassifizierung eines KI-Systems als hochriskant kann nach der Konzeption der KI-VO auf zwei Wegen erfolgen: Zunächst kann sie an bestehendes Produktsicherheitsrecht anknüpfen (Art. 6 Abs. 1 KI-VO). Dient ein KI-System beispielsweise als Sicherheitsbauteil einer Seilbahn, gilt es als hochriskant im Sinne der KI-VO. Alternativ kann sich die Klassifizierung aus einer risikobehafteten Zweckbestimmung des KI-Systems ergeben. Soll das System beispielsweise mit spezifischer Relevanz im Bildungs- oder Beschäftigungskontext, im Bereich der kritischen Infrastruktur oder in der Rechtspflege eingesetzt werden, gilt es gemäß Art. 6 Abs. 2 KI-VO als hochriskant. Die risikobehafteten Zweckbestimmungen sind abschließend in Anhang III der KI-VO aufgelistet.

Sofern nach diesen Bestimmungen ein hohes Risiko festgestellt wurde, muss der Anbieter (Art. 3 Nr. 3 KI-VO) des Hochrisiko-KI-Systems sicherstellen, dass die besonderen Anforderungen der KI-VO erfüllt sind. Diese Anforderungen sind in Art. 8 ff. KI-VO aufgeführt und umfassen beispielsweise eine Auswahl relevanter und hinreichend repräsentativer Trainingsdaten (Art. 10 KI-VO), die automatische Aufzeichnung bestimmter Ereignisse (Art. 12 KI-VO) und die Bereitstellung einer Betriebsanleitung (Art. 13 Abs. 2 KI-VO). Nachgelagert muss der Betreiber (Art. 3 Nr. 4 KI-VO) eines Hochrisiko-KI-Systems bestimmte technische und organisatorische Maßnahmen ergreifen, um einen sicheren Betrieb des Systems zu gewährleisten (Art. 26 Abs. 1 KI-VO). Dazu zählen etwa die Installation einer menschlichen Aufsicht, die den Betrieb des Systems überwacht und die sichere Aufbewahrung der automatisch erzeugten Protokolle.

2. Verhältnis der KI-VO zum sonstigen Recht

Die KI-VO reguliert die Entwicklung und den Betrieb von KI-Systemen. In weiten Teilen unberührt bleibt aber die Regulierung des In- sowie des Outputs. So erfordert die Entwicklung von KI-Systemen die Verarbeitung großer Daten-

15 Dazu *Schwartmann/Köhler* in *Schwartmann/Keber/Zenner*, KI-VO. Leitfaden für die Praxis, 2. Aufl. 2024, 2. Teil 1. Kap. Rn. 51–54.

mengen, die regelmäßig zumindest teilweise einen Personenbezug aufweisen. Dabei gelten die Vorgaben der DS-GVO. Außerdem kann das Training eines KI-Systems mit urheberrechtlich geschützten Werken von den Vorschriften des Urheberrechtsgesetzes (**UrhG** → Nr. 22) erfasst sein.

Ähnliches gilt für den Output eines KI-Systems, also die KI-generierten Ergebnisse. Die KI-VO statuiert zwar besondere Pflichten für Betreiber von KI-Systemen. Sie legt aber nicht fest, ob und inwiefern der Output eines KI-Systems unter den Vorschriften der geltenden Rechtsordnung verwendet werden darf. Die Grenzen der Verwendbarkeit können sich je nach konkret generiertem Ergebnis beispielsweise wiederum aus dem Datenschutz- oder dem Urheberrecht, aber auch aus dem Geschäftsgeheimnisschutzrecht und zahlreichen weiteren Rechtsquellen ergeben. Besondere Bedeutung kommt in diesem Zusammenhang dem Verbot der automatisierten Einzelentscheidung in Art. 22 Abs. 1 DS-GVO zu. Demnach dürfen Entscheidungen, die eine rechtliche Wirkung entfalten oder die betroffene Person in ähnlicher Weise erheblich beeinträchtigen, nicht ausschließlich auf einer automatisierten Datenverarbeitung beruhen. Von dem Verbot umfasst sind nach der Rechtsprechung des EuGH auch entscheidungsvorbereitende Maßnahmen, sofern sie das Ergebnis der Entscheidungsfindung maßgeblich bestimmen.[16]

Weitere Grenzen der Verwendbarkeit KI-generierter Ergebnisse lassen sich unmittelbar aus der Verfassung ableiten: So verlangt das GG beispielsweise einen menschlichen Richter, weshalb die richterliche Entscheidung von einem Menschen getroffen werden muss und nicht vollständig auf ein KI-System übertragen werden darf. Bis zu welchem Grad des Einsatzes von KI-Systemen in diesen Fällen von einer menschlichen Entscheidung ausgegangen werden kann, ist eine Frage des Einzelfalls. Das entsprechende Recht befindet sich noch in der Entwicklung.

16 EuGH Urt. v. 7.12.2023 – C-634/21, ECLI:EU:2023:957 Rn. 44–48.