Digitale Vulnerabilität und Selbstbestimmung – Vorgaben zur Sicherstellung der Selbstbestimmung vulnerabler Nutzendenden durch informierte Einwilligung und Rechtspflichten im Behinderten- und Datenrecht

Luisa Schmied und Maxi Nebel

Zusammenfassung
Die Gewährleistung der Selbstbestimmung als Folge einer informierten Entscheidung des Individuums durch die datenschutzrechtliche Einwilligung ist essenziell zur Förderung und Verwirklichung des Freiheitsrechts auf informationelle Selbstbestimmung. Jedoch bestehen erhebliche praktische Probleme in der Umsetzung, die zu unterschiedlichen digitalen Vulnerabilitäten führen. Der Beitrag beleuchtet digitale Vulnerabilität am Beispiel von AI-Companions. Im Rahmen des Privatheitsschutzes vulnerabler Personen muss die gängige Praxis der Einwilligung als datenschutzrechtliche Legitimationsgrundlage der Verarbeitung personenbezogener Daten kritisch hinterfragt werden, insbesondere in Bezug auf die Wirksamkeitsvoraussetzung der Informiertheit. Der Beitrag thematisiert aktuelle Fragestellungen zum Thema der Einwilligung, insbesondere im Hinblick auf den Anspruch auf situative und kontextbezogene Ausgestaltung der Informationsanforderungen. Anknüpfungspunkt bietet das Behindertenrecht, insbesondere die Vorgaben zur Barrierefreiheit. Anschließend werden rechtliche Verpflichtungen von Diensteanbietern aus dem europäischen Datenrecht untersucht, die ebenso der Sicherstellung der Selbstbestimmung vulnerabler Personen dienen sollen.

1. Einleitung

Digitale Infrastrukturen bilden die Grundlage für zahlreiche digitale Dienste und Anwendungen, die in der modernen Gesellschaft genutzt werden. Sie sind unerlässlich für das Funktionieren von Wirtschaft und Staat, Bildungs- und Gesundheitssystem und vielen anderen Bereichen. Ohne die der Digitalisierung zugrunde liegenden Infrastrukturen sind all die auf ihnen aufbauenden Dienste und Anwendungen undenkbar – von KI-Systemen wie Chatbots und AI-Companions über Social Media bis hin zu digitalen Zahlungs- und Transaktionssystemen, Cloud-Diensten und vielem mehr. Die ubiquitäre Durchdringung des Alltags durch digitale Infrastrukturen schafft dabei nicht nur neue Teilhabechancen, sondern bietet auch eine größere Angriffsfläche für Grundrechtseingriffe sowie die Exposition in Hinblick auf Vulnerabilitätsfaktoren.

Unterschiedliche Personen sind unterschiedlich vulnerabel gegenüber Verletzungen ihrer Selbstbestimmung, was neben strukturellen oder individuellen Gründen insbesondere auch auf ein situations- oder kontextabhängiges Nutzungsverhalten zurückzuführen ist. Digitalisierte Infrastrukturen wirken oft intrusiv in die Privatsphäre der Menschen hinein. Die Anforderungen an die Ausgestaltung digitaler Technik zur Gewährleistung der Selbstbestimmung fallen dabei weit auseinander. Pauschalisierungen, die den bestehenden Rechtskategorien zugrunde liegen, erfassen das Problem nicht ausreichend differenziert.

2. Digitale Vulnerabilität – Bedeutung der Selbstbestimmung

Vulnerabilität als menschliche Eigenschaft ist ein weiter und nicht ganz unumstrittener Begriff. In einer digitalisierten Welt werden neue Vulnerabilitäten erzeugt und alte verstärkt. Es gilt die Selbstbestimmung der Nutzenden zu stärken, um Vulnerabilitäten auszugleichen und abzubauen.

2.1 Vulnerabilität als conditio humana

Vulnerabilität bezeichnet die Eigenschaft, verletzlich zu sein, und bezieht sich im Allgemeinen auf Situationen, in denen das Risiko von Gefahren durch verschiedene Faktoren und Prozesse erhöht ist.[1] Das Ausmaß der Vulnerabilität kann dabei anhand der Wechselwirkung zwischen Risikoexposition und Bewältigungskapazität („coping capacity") gemessen werden.[2] Ansätze wie der von Martha Fineman basieren darauf, dass Vulnerabilität dem Menschen immanent ist (conditio humana), und strukturell oder situativ zum Ausdruck kommt.[3] Der Gesellschaft kommt dabei die Verant-

1 *Damm*, Vulnerabilität als Rechtskonzept?, MedR 2013, 201 (202); *Kruse*, Lebensphase hohes Alter, 2017, S. 170; *Strauß/Bettin*, Digitalisierung, Vulnerabilität und (kritische) gesellschaftliche Infrastrukturen, 2023, S. 14; anders der Ansatz in: *UN*, Living with Risk, 2004, S. 7, 16; *Roßnagel u.a.*, Die Verletzlichkeit der ‚Informationsgesellschaft', 2002/2009, S. 9, die unter Vulnerabilität „die erhöhte Anfälligkeit einer Gesellschaft für die Auswirkungen von Gefahren" verstehen.

2 *Turner u.a.*, A framework for vulnerability analysis in sustainability science, PNAS 2003, 8074; *Birkmann u.a.*, State of the Art der Forschung zur Verwundbarkeit Kritischer Infrastrukturen am Beispiel Strom/Stromausfall, 2010, S. 27; *Kruse*, Lebensphase hohes Alter, 2017, S. 170.

3 *Fineman*, The Vulnerable Subject, Yale Journal of Law & Feminism 1/2008, 1 (10 ff.); *Fineman*, Vulnerability and Inevitable Inequality, Oslo Law Review 2017, 133 (133 ff.); *Bielefeldt*, in: Bergemann/Frewer (Hrsg.), Autonomie und Vulnerabilität in der Medi-

wortung zu, auf die aus der Vulnerabilität resultierenden Abhängigkeiten zu reagieren. Neben der unvermeidlichen Abhängigkeit, die jedem Mensch aufgrund seines verkörperten Wesens innewohnt, betont Fineman in ihrem Ansatz auch die abgeleitete Abhängigkeit, die sich aus dem Zugang zu ausreichend materiellen, institutionellen und physischen Ressourcen ergibt, um den Verletzlichkeit der Person erfolgreich zu begegnen.[4] Versteht man Vulnerabilität als individuelle Eigenschaft, greift die im Diskriminierungskontext übliche Kategorisierung in feste Gruppen z. B. nach Alter, Geschlecht oder aufgrund einer Behinderung (vgl. Art. 21 GRCh, Art. 3 Abs. 3 GG; § 1 AGG) zu kurz, um dem jeweiligen Einzelfall gerecht zu werden. Die Vulnerabilität innerhalb dieser Gruppen ist zwar mit einer höheren Wahrscheinlichkeit gegeben.[5] Dennoch können verschiedene Mitglieder dieser Gruppen durch unterschiedlich stark ausgeprägte Vulnerabilitäten gekennzeichnet sein. Auch außerhalb dieser Gruppenkategorien ist eine erhöhte Vulnerabilität nicht ausgeschlossen.[6] Verletzlichkeit ist folglich nicht universell durch Zugehörigkeit zu einer Gruppe, sondern im Kontext des speziellen Anwendungsbereichs zu betrachten. Das Festhalten an generische Gruppenkategorien birgt die Gefahr, nicht alle Vulnerabilitätsaspekte adäquat zu adressieren. Dies sollte aber gerade vor dem Hintergrund eines effektiven Grundrechtsschutzes, der auch den Schutz besonders vulnerabler Personen indiziert, ausschlaggebend sein.[7]

2.2 Digitale Vulnerabilität: Risiken moderner Datenverarbeitung

Vulnerabilität im Rahmen digitaler Infrastrukturen liegt die Annahme zugrunde, dass digitale Infrastrukturen aufgrund ihrer Omnipräsenz automa-

zin, 2019, S. 21; *Kroschwald*, Nutzer-, kontext- und situationsbedingte Vulnerabilität in digitalen Gesellschaften, ZfDR 2023, 1 (5).

4 *Fineman*, Vulnerability and Social Justice, 53 Valparaiso University Law Review 2019, 1 (24); auch *Kruse*, Lebensphase hohes Alter, 2017, S. 170.

5 *Birnbacher*, Vulnerabilität und Patientenautonomie, MedR 2012, 560 (561); *Damm*, Vulnerabilität als Rechtskonzept?, MedR 2013, 201 (202); *Kruse*, Lebensphase hohes Alter, 2017, S. 170.

6 *Koch u.a.*, in: Friedewald u.a. (Hrsg.), Freiheit in digitalen Infrastrukturen, 2025, DiversPrivat 4.3.

7 *Bielefeldt*, in: Bergemann/Frewer (Hrsg.), Autonomie und Vulnerabilität in der Medizin, 2019, S. 21; *Geminn*, Deus ex machina?, 2023, S. 170.

tisch neue Verletzlichkeiten erzeugen.[8] Dazu findet der Diskurs zu Vulnerabilität im Privatheitsbereich verstärkt Einzug in die Literatur.[9] Vulnerabilität im Rahmen digitaler Infrastrukturen bezieht sich auf die datengetriebene Plattformökonomie, die auf Basis digitalisierter Infrastrukturen intrusiv in die Privatsphäre der Menschen hineinwirkt. Die Erfassung personenbezogener Daten hat zur Entstehung neuer Geschäftsmodelle geführt, die auf der Erstellung umfassender Identitätsprofile durch Tracking und Profiling der Nutzenden basieren.[10] Über Tracking-Tools wird das Verhalten der Nutzenden bis ins Detail aufgezeichnet und diese persönlichen Aspekte im Rahmen des Profiling interpretiert, was Rückschlüsse auf die wirtschaftliche Lage, persönliche Vorlieben und Interessen sowie auf das Verhalten der Person zulässt. Neben dem Ziel, damit die Kundenbindung zu erhöhen oder personalisierte Werbung zu schalten, entstehen Informations- und Machtasymmetrien.[11] Mit der zunehmenden Verbreitung intelligenter Technologien eröffnen sich immer mehr Wege, um menschliches Verhalten unauffällig zu lenken (Nudging) und zu beeinflussen.[12] Die Schadenspotenziale sind dabei jedoch sehr intransparent.[13] Zudem ist auch die ambivalente Wirkweise der Digitalisierung nicht zu unterschätzen und stets mitzudenken. Neben der Schaffung oder Verstärkung von Verletzlichkeiten können diese durch Technologien wie Dialogsysteme auch reduziert werden.[14]

2.3 Digitale Vulnerabilität am Beispiel von AI-Companions als „KI-Freunde“

Virtuelle Dialogsysteme verdeutlichen die Mechanismen digitaler Vulnerabilität besonders eindrücklich, da sie nicht nur durch vertrauenserwecken-

8 *Strauß/Bettin*, Digitalisierung, Vulnerabilität und (kritische) gesellschaftliche Infrastrukturen, 2023, S. 19.
9 *Geminn*, Deus ex machina?, 2023, S. 169 ff.; *Behrendt/Loh*, Informed consent and algorithmic discrimination, REVIEW OF SOCIAL ECONOMY, 2022, S. 58 (58 ff.).
10 *Strauß/Bettin*, Digitalisierung, Vulnerabilität und (kritische) gesellschaftliche Infrastrukturen, 2023, S. 19.
11 *Behrendt/Loh*, Informed consent and algorithmic discrimination, REVIEW OF SOCIAL ECONOMY, 2022, 58 (58 ff.); *Strauß/Bettin*, Digitalisierung, Vulnerabilität und (kritische) gesellschaftliche Infrastrukturen, 2023, S. 33, 48.
12 *Karaboga*, in: Friedwald u.a. (Hrsg.), Selbstbestimmung, Privatheit und Datenschutz, 2022, 275 (282); *Geminn*, Deus ex machina?, 2023, S. 174.
13 *Roßnagel u.a.*, Modernisierung des Datenschutzrechts, 2001, S. 28; *Roßnagel u.a.*, Die Verletzlichkeit der ‚Informationsgesellschaft‘, 2002/2009, S. 14.
14 *Geminn*, Deus ex machina?, 2023, S. 171.

de Layouts eine scheinbar sichere Interaktionsumgebung suggerieren, sondern auch gezielt individuelle Verwundbarkeiten – wie etwa Einsamkeit – adressieren und ausnutzen, was eine leichtfertige Preisgabe sensibler Daten begünstigt. Dialogsysteme, z.B. in Form von Chatbots, virtuellen Assistenten, AI-Companion oder ähnlichem, haben die Fähigkeit, durch generative KI-Systeme natürlichsprachige Antworten auf Anfragen zu liefern und so umfangreiche Gesprächsverläufe entstehen zu lassen. Basierend auf der Erforschung authentischer und menschenähnlicher Kommunikationsmuster mit Sprachmodellen werden Dienste angeboten, die das Konzept des „KI-Freundes" umsetzen. Über die Interaktion mit den Anwendenden werden menschenähnliche Beziehungen aufgebaut. Dies hat zur Folge, dass die Verantwortlichen an besonders sensible Informationen kommen können, wenn sich Anwendende dem artifiziellen Kommunikationspartner öffnen (Selbstoffenbarung). Ein prominentes Beispiel für AI-Companion ist die Smartphone-App Replika, welche als „KI-Freund" beworben wird. Innerhalb einer Pro-Mitgliedschaft können Nutzende einen romantischen Beziehungsmodus aktivieren. Dieser umfasst Funktionen wie Telefon- und Videoanrufe mit der zuvor konfigurierten artifiziellen Persona, virtuelle Überraschungen für die Nutzenden (vom „KI-Freund" initiiert) sowie die Beteiligung an emotionalen und sexualisierten Gesprächen. Intime Kommunikation mit AI-Companion muss nicht zwangsläufig sexualisiert sein, auch therapeutische Gespräche oder das schiere Anvertrauen des inneren Gefühlslebens bedeuten eine entsprechende Selbstoffenbarung. Dies führt zwangsläufig zu datenschutzrechtlichen Bedenken, wenn personenbezogene, noch dazu besonders sensible Informationen preisgegeben werden.

Die Selbstoffenbarung kann demgegenüber auch bedeutende Vorteile für den Anwendenden haben. Die Künstlichkeit des Gegenübers bietet gerade bei besonders intimen und sensiblen Themen, die in der Gesellschaft weniger offen besprochen oder akzeptiert werden, eine vermeintliche Sicherheit vor potenziellen sozialen Konsequenzen wie z.B. Unverständnis, Scham, Erklärungsnot oder Kontakteinschränkungen.[15] Sie bieten ein Mittel gegen Einsamkeit oder Unverständnis der Umwelt insbesondere für Menschen, die Schwierigkeiten haben, soziale Beziehungen im „real life" aufzubauen und zu pflegen – sei es aus Gründen wie Krankheit, psychischen Barrieren oder Mobilitätseinschränkungen. Dennoch begeben sich die Anwendenden

15 *Skjuve u.a.*, My Chatbot Companion, International Journal of Human-Computer Studies 2021, 102601.

in vulnerable Situationen, in denen sehr viele, äußerst sensible Daten anfallen; Datenschutzbedenken werden häufig beiseitegeschoben.[16]

2.4 Die Adressierung von Vulnerabilität im Datenschutzrecht

Der rechtliche Schutz der informationellen Selbstbestimmung stellt eine komplexe Herausforderung dar. Beim Versuch, den Begriff der Vulnerabilität als Rechtsbegriff zu greifen, wird dessen Unbestimmtheit deutlich. An Bedeutung könnte ein darauf aufbauendes Normkonzept aber an den Stellen gewinnen, an denen die individuellen, situativen und kontextbezogenen Schutzbedürfnisse differenzierter betrachtet werden müssten.[17] Die DSGVO begegnet Vulnerabilität insbesondere durch die inhaltliche Kategorisierung besonders sensibler Daten im Rahmen des Art. 9 DSGVO. Aufgrund ihres engen Bezugs zu Grundrechten und Grundfreiheiten unterwirft die Verordnung bestimmte Datenarten – etwa Gesundheitsdaten – einem besonderen Schutzregime, das über die allgemeinen Verarbeitungsgrundsätze hinausgehende Anforderungen stellt.[18] Eine kontextbezogene Betrachtung individueller oder situativer Schutzbedürftigkeit erfolgt hingegen nicht, sodass der Schutzrahmen auf typisierte Datenkategorien beschränkt bleibt. Die Regelungssystematik der Verordnung orientiert sich zudem primär an einem idealtypischen, durchschnittlich informierten Nutzenden. Eine ausdrückliche Berücksichtigung vulnerabler Personen ist in der DSGVO im Wesentlichen auf den Schutz von Kindern beschränkt, z. B. in Form von Art. 8 DSGVO. Dies erfasst den aufgeführten Schutzbedarf im Rahmen digitaler Vulnerabilität jedoch nicht ausreichend differenziert.[19] Es bleibt die Notwendigkeit einer adäquaten Adressierung von digitaler Vulnerabilität, um z. B. älteren oder kognitiv beeinträchtigten Menschen entsprechenden Selbstschutz zu ermöglichen. Insbesondere im Verbraucher-

16 *Skjuve u.a.*, My Chatbot Companion, International Journal of Human-Computer Studies 2021, 102601.

17 *Damm*, Vulnerabilität als Rechtskonzept?, MedR 2013, 201 (201 f.); *Kroschwald*, Nutzer-, kontext- und situationsbedingte Vulnerabilität in digitalen Gesellschaften, ZfDR 2023, 1 (6).

18 *Schiff*, in: Ehmann/Selmayr, DSGVO, 2024, Art. 9, Rn. 3; Zur Relevanz des Verarbeitungszusammenhangs vgl.: *Simitis*, in: Simitis, BDSG, 2011 § 3 Rn. 251 m. w. N.

19 *Roßnagel*, Der Datenschutz von Kindern in der Datenschutz-Grundverordnung, ZD 2020, 88; *Roßnagel/Geminn,* Datenschutzgrundverordnung verbessern, 2020, S. 55 ff.; *Geminn*, Deus ex machina? 2023, S. 193 ff.

schutzrecht wurde diese Vulnerabilität bereits erkannt und adressiert, um Personen wirksam vor Ausnutzung aufgrund körperlicher oder geistiger Einschränkungen, hohen Alters oder situativer Leichtgläubigkeit zu schützen.[20] Im Kontext digitaler Technologien werden diese Personen als Nutzende oder Verbrauchende oft nicht mitgedacht. Um einem individuellen Ansatz von Vulnerabilität gerecht zu werden, muss der klassische Diskriminierungsschutz auf Grundlage von abschließenden Merkmalslisten um eine Diversitätsperspektive ergänzt werden, die anhand der Vulnerabilitäten im Kontext des konkreten Gegenstandsbereichs entwickelt wird. Zur Ableitung entsprechender Schutzmaßnahmen müssen neben den schutzbedürftigen Individuen auch die gefährdenden Situationen und Kontexte identifiziert werden.[21]

2.5 Begegnung von Vulnerabilitäten durch die Stärkung von Resilienzen – mehr Selbstbestimmung durch Transparenz

Die Stärkung der Resilienz ist zudem ein wichtiger Ansatz, um Vulnerabilität zu begegnen.[22] Die klassischen Lösungsansätze zur Steigerung der Bewältigungskapazität im Schutzbereich der informationellen Selbstbestimmung beziehen sich vor allem auf die Förderung der Privacy Literacy. Privacy Literacy beschreibt die im Rahmen einer digitalen Bildung erlernten Fähigkeiten, selbstbestimmt Datenschutzentscheidungen zu treffen.[23] Ein angemessenes Schutzniveau kann damit jedoch nicht gewährleistet werden, da einerseits nicht alle Menschen gleichermaßen von digitaler Bildung erreicht werden können und andererseits nicht allen die gleichen Ressourcen zu Teil werden, sich entsprechend über Schutzvorkehrungen

---

20 *Helberger u.a.*, EU Consumer Protection 2.0, 2021, S. 8; *Kroschwald*, Nutzer-, kontext- und situationsbedingte Vulnerabilität in digitalen Gesellschaften, ZfDR 2023, 1 (6); *Damm*, Vulnerabilität als Rechtskonzept?, MedR 2013, 201 (203 f.).

21 *Kroschwald*, Nutzer-, kontext- und situationsbedingte Vulnerabilität in digitalen Gesellschaften, ZfDR 2023, 1 (1 ff.).

22 *Turner u.a.*, A framework for vulnerability analysis in sustainability science, PNAS 2003, 8074; *Birkmann u.a.*, State of the Art der Forschung zur Verwundbarkeit Kritischer Infrastrukturen am Beispiel Strom/Stromausfall, 2010, S. 26f.

23 *Brough/Kelly*, Critical roles of knowledge and motivation in privacy research. *Current opinion in psychology*, 2020, 11 (31); *Trepte u.a.*, in: Gutwirth u.a. (Hrsg.), Reforming European data protection law, 2015, S. 333 ff.; *Park,* Digital Literacy and Privacy Behavior Online, Communication Research 2013, 215 (215 ff.).

zu informieren.[24] Die informationelle Selbstbestimmung im Datenschutz ist ein Grundrecht, das allen Menschen unabhängig von ihren individuellen Fähigkeiten, ihrem sozioökonomischen Hintergrund oder der jeweiligen digitalen Umgebung zugänglich sein muss. Die Möglichkeit der Selbstbestimmung darf nicht auf Personen beschränkt werden, die ohne fremde Hilfe über die notwendigen Mittel verfügen, um sie auszuüben, wie z.B. die Fähigkeit, Datenschutzeinstellungen vorzunehmen oder Datenschutzhinweise zu lesen.[25] Ausschlaggebend für die Stärkung der Resilienz im Kontext der Selbstbestimmung ist die Fähigkeit der Menschen, Risiken und Vorteile einzuschätzen, um auf dieser Grundlage eine Entscheidung zu treffen.[26] Alle Menschen müssen in die Lage versetzt werden, informierte Entscheidungen treffen zu können. Ein Indikator für eine solche Bewältigungskapazität ist Transparenz,[27] die für vulnerable Personen insbesondere auch den Zugang und das Verständnis der Informationen inkludiert. Ein Fokus muss daher auf der Gewährleistung der situationsadäquaten Transparenz zur Herstellung der Selbstbestimmung durch das bestehende Recht liegen.[28]

3. Digitale Vulnerabilität und Selbstbestimmung: Die Notwendigkeit individueller und situationsadäquater Informationspräsentation im datenschutzrechtlichen Einwilligungskontext

Im Kontext digitaler Vulnerabilität bildet die Einwilligung regelmäßig die zentrale Rechtsgrundlage für die Verarbeitung personenbezogener Daten z. B. zu Zwecken des Trackings oder Profilings. Im Rahmen des Privatheitsschutzes vulnerabler Personen muss die gängige Praxis der Einwilligung als datenschutzrechtlicher Legitimationsgrundlage kritisch hinterfragt werden,

24 *Koch u.a.*, in: Roßnagel u.a. (Hrsg.), Freiheit in digitalen Infrastrukturen, 2025; *Livingstone u.a.*, Children's data and privacy online, 2019, S. 3 ff.; *Hagendorf*, in: Roßnagel u.a., Die Fortentwicklung des Datenschutzes, 2018, S. 99 (100 ff.).

25 *Kroschwald*, Nutzer-, kontext- und situationsbedingte Vulnerabilität in digitalen Gesellschaften, ZfDR 2023, 1 (4).

26 *Strauß/Bettin*, Digitalisierung, Vulnerabilität und (kritische) gesellschaftliche Infrastrukturen, 2023, S. 15.

27 *Lenz*, Vulnerabilität kritischer Infrastrukturen, 2009, S. 49, 60; *Strauß/Krieger-Lamina,* Digitaler Stillstand, 2017, S. 19.

28 Resilienz im Rahmen der Privacy Literacy stößt dort an ihre Grenzen, wo die Nutzung digitaler Infrastrukturen alternativlos ist und tatsächliche Wahlfreiheit fehlt.

insbesondere in Bezug auf die Gewährleistung der Transparenzanforderungen und somit der Wirksamkeitsvoraussetzung der Informiertheit.

3.1 Die informierte Einwilligung als Ausdruck datenschutzrechtlicher Selbstbestimmung

Die Selbstbestimmung im Umgang mit den eigenen personenbezogenen Daten wird als zentraler Aspekt des Datenschutzes bereits im Volkszählungsurteil[29] begründet und über Art. 8 Abs. 1 GRCh[30] normiert.[31] Das Verständnis der Einwilligung als „genuiner Ausdruck der informationellen Selbstbestimmung" knüpft mit Art. 8 Abs. 2 S. 1 GRCh daran an.[32] Eine Einwilligung auf Grundlage einer selbstbestimmten, autonomen Entscheidung stellt folglich eine Grundrechtsausübung im Sinne der GRCh dar.[33] Auf sekundärrechtlicher Ebene wird die Einwilligung durch Art. 6 Abs. 1 UAbs. 1 lit. a, Art. 4 Nr. 11, Art. 7 DSGVO ausgestaltet.

3.2 Die Voraussetzung der Informiertheit in der DSGVO: Umsetzung des grundrechtlichen Konzepts der Selbstbestimmung

Durch die Voraussetzung der Informiertheit wird in der DSGVO das grundrechtliche Konzept der Selbstbestimmung umgesetzt.[34] Der betroffenen Person muss gewährleistet werden, eine Entscheidung „in informierter Weise" treffen zu können. Das impliziert, dass die betroffene Person die Möglichkeit hat, alle Merkmale der Informationsverarbeitung einzusehen,[35]

29 BVerfG Urt. v. 15.12.1983 – 1 BvR 209/83 u.a., BVerfGE 65, 1, Rn. 74.
30 Charta der Grundrechte der Europäischen Union, ABl. (EU) C 326/392.
31 *Kühling/Buchner*, in: Kühling/Buchner, DSGVO, 2024, Art. 7, Rn. 19; *Liedke-Deutscher,* Die datenschutzrechtliche Einwilligung nach der DSGVO, 2014, S. 8; *Nebel*, Schutz der Persönlichkeit, ZD 2015, 517 (521).
32 *Roßnagel u.a.*, Modernisierung des Datenschutzrechts, 2001, 15, 72; *Schulz*, in: Gola/Heckmann, DSGVO/BDSG 2022, Art. 6, Rn. 21.
33 *Liedke-Deutscher*, Die datenschutzrechtliche Einwilligung nach der DSGVO, 2014, S. 8; *Klement,* in: Simitis u.a., Datenschutzrecht, 2025, Art. 7 DSGVO, Rn. 13.
34 *Klement*, in: Simitis u.a., Datenschutzrecht, 2025, Art. 7 DSGVO, Rn. 68.
35 *EuGH*, Einwilligung und Cookie Consent nur durch aktive, gesonderte und ausdrückliche Erklärung – Planet49, ZD 2019, 556 Rn. 74; *Ernst,* in: Paal/Pauly, DSGVO BDSG, 2021, Art. 4, Rn. 79; *Klement*, in: Simitis u.a., Datenschutzrecht, 2025, Art. 7 DSGVO, Rn. 67 betont, dass dies auch die Inanspruchnahme sachkundiger Beratung zur Erfüllung der Informationsbeschaffung inkludiert.

um zu verstehen, wofür die Einwilligung erteilt wurde, und auch z.B. von ihrem Recht auf Widerspruch Gebrauch machen zu können.[36] Ausschlaggebend ist die tatsächliche Möglichkeit der Informationsaneignung – nicht die tatsächliche Nutzung des Angebots.[37] Der Verantwortliche hat entsprechende Vorkehrungen zu treffen, um sicherzustellen, dass die betroffene Person wissen kann, dass und in welchem Umfang sie ihre Einwilligung erteilt (Erwägungsgrund 42 S. 2 DSGVO). Die Anforderungen daran ergeben sich aus Art. 7 Abs. 2 und Erwägungsgrund 32 DSGVO. Danach hat das Ersuchen um Einwilligung in verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache zu erfolgen. Zudem muss dies deutlich von anderen Sachverhalten abgrenzbar sein. Zur Erfüllung dessen hat der Verantwortliche auf das Verständnis der Zielgruppe des Einwilligungsersuchens abzustellen. Dieses hat er im Vorhinein zu ermitteln und die Darstellung der Informationen entsprechend anzupassen.[38] Daraus kann die Pflicht für Verantwortliche herausgelesen werden, entsprechende Informationsangebote zu schaffen, die nicht nur den „Durchschnittsbürger" in den Blick nehmen. Einer diesbezüglichen Adressierung von Vulnerabilität im Kontext der Informiertheit kommt der Europäische Datenschutzausschuss (EDSA) in seinen Leitlinien zur Einwilligung nur unzureichend nach, da er nur beispielhaft auf die besondere Informationspräsentation für minderjährige Personen hinweist.[39] Eine ausdrückliche Adressierung anderer potenziell vulnerabel Personen bleibt aus. Dennoch lässt der Wortlaut darauf schließen, dass der EDSA die Schutzbedürftigkeit weiterer vulnerabler Personen zumindest in Erwägung gezogen hat, da er Minderjährige nur beispielhaft nennt. Allerdings gefährdet der Verzicht auf die Nennung weiterer Vulnerabilitätsfaktoren dadurch die Wahrung der Selbstbestimmung.

Neben dem erforderlichen Maß zur Herstellung der Informiertheit gem. Art. 4 Nr. 11 DSGVO können weitere Anforderungen der informierten Einwilligung zudem aus den Transparenzpflichten des Verantwortlichen gem.

36 EDSA, Leitlinien 05/2020 zur Einwilligung v. 4.5.2020, Rn. 62.

37 Auch die Entscheidung, auf eine genaue Lektüre von Datenschutzbestimmungen zu verzichten, ist eine Ausübung dieses Grundrechts, vgl. dazu: *Klement*, in: Simitis u.a., Datenschutzrecht, 2025, Art. 7 DSGVO, Rn. 16, 68.

38 *Roßnagel/Geminn,* Datenschutz-Grundverordnung verbessern, 2020, S. 63; EDSA, Leitlinien 05/2020 zur Einwilligung v. 4.5.2020, Rn. 67 (Durchschnittsbürger), Rn. 70 (Art von Zielgruppe).

39 EDSA, Leitlinien 05/2020 zur Einwilligung v. 4.5.2020, Rn. 70.

Art. 12 ff. DSGVO abgeleitet werden.[40] Als Ausprägung des Grundsatzes der Transparenz aus Art. 5 Abs. 1 lit. a DSGVO und dem Recht auf Auskunft gemäß Art. 8 Abs. 2 S. 2 GRCh ist Transparenz als zentrale Voraussetzung der informationellen Selbstbestimmung zu verstehen.[41] Dem Transparenzgrundsatz folgend, müssen personenbezogene Daten „in einer für die betroffene Person nachvollziehbaren Weise" verarbeitet werden. Gem. Art. 12 Abs. 1 S. 1 DSGVO haben „Verantwortliche geeignete Maßnahmen zu treffen, um der betroffenen Person alle Informationen [...], die sich auf die Verarbeitung beziehen, in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache zu übermitteln". Art. 12 Abs. 1 S. 1 DSGVO verweist dabei in Hs. 2 auf eine Schutzbedürftigkeit insbesondere von Kindern.[42] Das Transparenzgebot verlangt dabei nicht nur formale Verständlichkeit im Sinne von Lesbarkeit, sondern auch die Sinnverständlichkeit.[43] Angesichts der wachsenden Datenverarbeitungskomplexität insbesondere im Bereich der Profilbildung und KI bringt die Umsetzung erhebliche Anforderungen an eine angemessene Reduktion dieser Komplexität. Die geforderte Einfachheit darf dabei aber weder an Präzision noch an Vollständigkeit verlieren und sollte zudem die jeweilige Aufnahmekapazität der betroffenen Person berücksichtigen.[44] Daneben kann auch ein Mehrebenenansatz das Spannungsverhältnis zwischen Verständlichkeit und Vollständigkeit abmildern.[45] Unterschiedliche Konkretisierungsstufen, die ergänzende Nutzung von Bildsymbolen (Art. 12 Abs. 7 DSGVO) sowie eine situationsadäquate Informationswiedergabe erst

40 Die Informationspflichten aus Art. 12 bis 14 DSGVO konkretisieren die Informationsanforderungen des Art. 4 Nr. 11 DSGVO. Die Mindestanforderungen des Merkmals der Informiertheit nach Art. 4 Nr. 11 DSGVO sind: die Identität des Verantwortlichen, der Verarbeitungszweck, die Art der verarbeiteten Daten, das Recht auf Widerruf sowie Informationen zu Art. 22 Abs. 2 lit. c oder Art. 49 Abs. 1 S. 1 lit. a DSGVO; vgl. dazu EDSA, Leitlinien 05/2020 zur Einwilligung v. 4.5.2020, Rn. 64.

41 *Albers/Veit*, in: Wolff u.a., BeckOK Datenschutzrecht, 2023, Art. 6, Rn. 36; *Heckmann/Paschke*, in: Ehmann/Selmayr, DSGVO, 2024, Art. 12, Rn. 1.

42 Siehe auch Erwägungsgrund 39 S. 3, 58 DSGVO.

43 Art.-29-Gruppe, WP 260 rev.01, Rn. 9; vgl. EuGH, Urt. 11.11.2020 – C 61/19, *EuGH*, Nachweis einer wirksamen Einwilligung, ZD 2021, 89, Rn. 45, 46.

44 *Dix*, in: Simitis u.a., Datenschutzrecht, 2025, Art. 12 DSGVO, Rn. 12; Art.-29-Gruppe, WP 260 rev.01, Rn. 34; *Roßnagel u.a.*, Einwilligung, Möglichkeiten und Fallstricke aus der Konsumentenperspektive, 2020, S. 22.

45 Vgl. Art.-29-Gruppe, WP 260 rev.01 Rn. 17f., 35 ff., 50; *Menzel*, Datenschutzrechtliche Einwilligung, DuD 2008, 400 (408); *Klement*, in: Simitis u.a., Datenschutzrecht, 2025, Art. 7 DSGVO, Rn. 70.

zum Zeitpunkt der Erhebung sind Forderungen, die sich in der Praxis aber bislang nicht durchsetzen konnten.[46]

3.3 Herausforderungen der Einwilligungspraxis: Entscheidungsautonomie und die Problematik des Durchschnittsnutzenden

Die Einwilligung prägt das Datenschutzrecht durch einen stark individualistischen Ansatz. Dem liegt die Annahme zugrunde, dass Transparenz und Eigenverantwortung ausreichend sind, um eine wirksame Einwilligung zu gewährleisten. Dabei wird unterstellt, dass die Grundrechte auf Datenschutz (Art. 7 und 8 GRCh) und informationelle Selbstbestimmung (Art. 2 Abs. 1 iVm Art. 1 Abs. 1 GG) dadurch gewahrt werden, dass gleichberechtigte Partner gemeinsam die Zwecke und Bedingungen der Datenverarbeitung festlegen.[47] Es führt jedoch dazu, dass die Verantwortung für die Legitimität der Datenverarbeitung, von den Datenverarbeitern auf die Nutzenden verlagert wird.[48] In der Praxis beruht die Einwilligung häufig nicht auf einer bewussten, informierten Entscheidung.[49] Strukturelle Probleme, wie überlange, komplexe und oft schwer verständliche Einwilligungserklärungen, lassen die Einwilligung zu einer Fiktion verkommen.[50] Da eine fundierte, individuelle Risikoeinschätzung kaum möglich ist, kann von einer wirklich „informierten" Einwilligung regelmäßig nicht ausgegangen werden. In der Praxis werden solche Erklärungen häufig ungelesen akzeptiert, wodurch die Einwilligung als Rechtfertigungsgrund weitgehend ihren

---

46 *Geminn u.a.*, Die Informationspräsentation im Datenschutzrecht, ZD-Aktuell 2021, 05335 m. w. N.; *Roßnagel/Geminn*, Datenschutz-Grundverordnung verbessern, 2020, S. 161, 178; *Krüger*, Datensouveränität und Digitalisierung, ZRP 2016, 190 (191).

47 *Roßnagel u.a.*, Einwilligung, Möglichkeiten und Fallstricke aus der Konsumentenperspektive, 2020, S. 7; *Krüger,* Datensouveränität und Digitalisierung, ZRP 2016, 190 (191).

48 *Roßnagel u.a.*, Einwilligung, Möglichkeiten und Fallstricke aus der Konsumentenperspektive, 2020, S. 18.

49 *Krüger*, Datensouveränität und Digitalisierung, ZRP 2016, 190; *Kühling/Buchner*, in: Kühling/Buchner, DSGVO, 2024, Art. 7, Rn. 10; *Paal/Hennemann*, in: Paal/Pauly, DSGVO, Art. 12, Rn. 77.

50 *Heckmann/Paschke*, in: Ehmann/Selmayr, DSGVO, Art. 7, Rn. 17; *Menzel*, Datenschutzrechtliche Einwilligung, DuD 2008, 400 (401); *Kühling/Buchner*, in: Kühling/Buchner, DSGVO, 2024, Art. 7, Rn. 10; *Stemmer*, in: Wolff u.a., BeckOK Datenschutzrecht, 2023, Art. 7, Rn. 57.

inhaltlichen Wert verliert und nur noch eine formale Funktion erfüllt.[51] Das notwendige Wissen über die Folgen einer Datenverarbeitung kann nicht unterstellt werden.[52] Folglich ist ein rein autonomiebasierter Ansatz, der auf der Fiktion des Durchschnittsnutzenden beruht, problematisch und führt zur Frage der Voraussetzungen, die eine angemessene Entscheidungsautonomie ermöglichen.

3.4 Anspruch auf eine kindesspezifische Ausgestaltung der Informationsbegebenheiten im Einwilligungsprozess gem. Art. 8 i. V. m. Art. 12 DSGVO

Für Kinder wurde durch das Merkmal der Einwilligungsfähigkeit (Art. 8 DSGVO) die Möglichkeit geschaffen, die Rechtmäßigkeit der Einwilligung an individuellen Fähigkeiten anzuknüpfen. Dazu wird auf die Einsichtsfähigkeit (Fähigkeit zur kognitiven Erfassung des Einwilligungsgegenstandes) des Kindes abgestellt.[53] Die besondere Schutzbedürftigkeit von Minderjährigen ergibt sich aus ihrer Unerfahrenheit, Beeinflussbarkeit und fehlenden geschäftlichen Erfahrung, was zur Folge haben kann, dass ihr Bewusstsein für Risiken, Folgen, Schutzmaßnahmen und die Wahrnehmung ihrer Rechte bei der Datenverarbeitung schwächer ausgeprägt ist.[54] Anknüpfungspunkte für diese Argumentationskette ergeben sich dabei auch aus Art. 17 UN-Kinderrechtskonvention oder Art. 24 GRCh. An das Merkmal der Einwilligungsfähigkeit anknüpfend, kann aus dem Zusammenspiel von Art. 8 iVm Art. 12 DSGVO grundsätzlich ein Anspruch auf eine kindspezifische Ausgestaltung der Informationsbegebenheiten im Einwilligungsprozess hergeleitet werden.

---

51 *Roßnagel* u.a., Einwilligung, Möglichkeiten und Fallstricke aus der Konsumentenperspektive, 2020, S. 5; *Gluck* u.a., How Short is Too Short?, SOUPS 2016, S. 321.

52 *Heckmann/Paschke*, in: Ehmann/Selmayr, DSGVO, Art. 7, Rn. 17; *Roßnagel u.a.*, Einwilligung, Möglichkeiten und Fallstricke aus der Konsumentenperspektive, 2020, S. 8.

53 *Klement*, in: Simitis u.a., Datenschutzrecht, 2025, Art. 7 DSGVO, Rn. 1; *Schulz*, in: Gola/Heckmann, DSGVO – BDSG, 2022, Art. 8, Rn. 10.

54 Erwägungsgrund 38 DGVO; *Taeger*, Einwilligung von Kindern gegenüber Diensten der Informationsgesellschaft, ZD 2021, 505 (506); *Schulz*, in: Gola/Heckmann, DSGVO – BDSG, 2022, Art. 8, Rn. 1; *Roßnagel u.a.*, Einwilligung, Möglichkeiten und Fallstricke aus der Konsumentenperspektive, 2020, S. 30; *Ernst*, Die Einwilligung nach der Datenschutzgrundverordnung, ZD 2017, 110 (111).

4. Barrierefreie Einwilligung: Anspruch auf individuelle Anpassung der Informationsbegebenheiten aus dem Behindertenrecht

Die Komplexität digitaler Infrastrukturen wirft vor diesem Hintergrund damit automatisch die Frage auf, inwiefern auch für Personen, die andere Vulnerabilitätsfaktoren aufweisen, Ansprüche auf eine individuelle, situationsadäquate Informationspräsentation im Einwilligungskontext bestehen. Unterrepräsentiert in der Diskussion sind die spezifischen Ansprüche, die sich für Menschen mit Behinderungen[55] aus dem Recht in Bezug auf einen gleichberechtigten, barrierefreien Zugang zu Informations- und Kommunikationstechnologien im Kontext der Informiertheit im Rahmen der Einwilligung ergeben.

Anders als Minderjährige ist die Begriffsdefinition von Menschen mit Behinderungen deutlich heterogener, da die Schutzbedürftigkeit hierbei nicht am Alter und den damit assozierten Fähigkeiten, sondern an der durch eine Beeinträchtigung herbeigeführten Teilhabeeinschränkung anknüpft. Die Anforderungen an digitale Technik im Rahmen der Informationspräsentation fallen dabei weit auseinander. Blinde Personen sind z. B. im Rahmen des Zugangs zu Informationen auf einen Screenreader oder auf Braillezeilen angewiesen[56] – im Hinblick auf das Merkmal der Informiertheit jedoch nicht in der tatsächlichen Möglichkeit der Informationsaneignung eingeschränkt. Anders gestaltet sich dies für Menschen mit kognitiven Beeinträchtigungen. Diese können Schwierigkeiten damit haben, schwere

55 Als Menschen mit Behinderungen können im Sinne des Art. 1 S. 2 und lit. e der Präambel der UN-BRK Menschen verstanden werden, die langfristige körperliche, seelische, geistige oder Sinnesbeeinträchtigungen haben, welche sie in Wechselwirkung mit verschiedenen Barrieren an der vollen, wirksamen und gleichberechtigten Teilhabe an der Gesellschaft hindern können. Siehe dazu: *Tolmein,* in: MAH SozialR, § 29, Rn. 59; *von Boetticher/Kuhn-Zuber*, Rehabilitationsrecht, S. 29, Rn. 21, die in Anlehnung an diese Vorgaben betonen, dass eine Behinderung nicht mehr als die Abweichung vom Normalzustand der Körperfunktionen angesehen werden soll, sondern es auf die Zusammenhänge zwischen den Gesundheitsproblemen und den damit verbundenen Einschränkungen an der Teilhabe am Leben in der Gesellschaft ankommt; vgl. auch: Gesetzentwurf der Bundesregierung zum Bundesteilhabegesetz (BTHG), BT-Drs. 18/9522, S. 226, wonach die Möglichkeit der Interaktion mit der Umwelt als Kriterium für die Beurteilung einer Behinderung Berücksichtigung finden muss.

56 *Carstens*, in: Deinert u.a., SWK Behindertenrecht, 2022, Barrierefreie Informationstechnik, Rn. 2; vgl. *Geminn*, Deus ex machina?, 2023, S. 175.

oder komplexe Informationen zu erfassen,[57] was die Frage aufwirft, ob auch ihnen im Rahmen der Einwilligung ein höheres Schutzniveau zugestanden werden sollte. Im Folgenden soll daher untersucht werden, ob ein solcher Anspruch auf individuelle Anpassung der Einwilligungsvoraussetzungen in Hinblick auf die Gewährleistung der Sinnverständlichkeit einer Einwilligung aus dem Behindertenrecht hergeleitet werden kann.

4.1 Pflicht zum digitalen Privatheitsschutz von Menschen mit Behinderung – Bestehende Privatheitsrisiken

Im Europäischen Recht wurde, neben Art. 7 und 8 GRCh, auf denen der primäre Schutz in der digitalen Welt gründet, durch Art. 26 GRCh eine spezifische Vorschrift geschaffen, die explizit die Rechte von Menschen mit Behinderungen kodifiziert und damit deren Schutzbedürftigkeit betont. Art. 26 GRCh verpflichtet die Union und die Mitgliedsstaaten bei der Ausführung von Unionsrecht nach Art. 51 Abs. 1 GRCh zur Integration von Menschen mit Behinderungen. Dies umfasst neben Maßnahmen zur Gewährleistung ihrer Eigenständigkeit und ihrer sozialen und beruflichen Eingliederung auch Maßnahmen zur Teilhabe am Leben in der Gemeinschaft. Im Mittelpunkt steht dabei der Abbau von Barrieren, um die Lebensumwelt den Bedürfnissen von Menschen mit Behinderungen anzupassen.[58] Barrierefreiheit in Hinblick auf digitale Infrastrukturen kann im weitesten Sinne als Ausgestaltung der Eigenständigkeit und der Gewährleistung der gesellschaftlichen Teilhabe gesehen werden. Untermauert wird dies durch das Diskriminierungsverbot aufgrund einer Behinderung aus Art. 21 Abs. 1 GRCh.

Auch in Art. 22 UN-Behindertenrechtskonvention (UN-BRK)[59] erkennen die Vertragsstaaten das gleiche Recht von Menschen mit Behinderungen auf Achtung der Privatsphäre an. Damit wird der Schutz der Privat-

---

57 Vgl. mental retardation (F70-F79), International Statistical Classification of Diseases and Related Health Problems 10th Revision (ICD-10) – WHO; *Uziel-Karl/Tenne-Rinde*, Making language accessible for people with cognitive disabilities, 2018, S. 845 ff.; *Han u.a.*, Mild Cognitive Impairment Is Associated with Poorer Decision-Making in Community-Based Older Persons, 2015–VOL. 63, NO. 4 JAGS, 676 (681).

58 *Kingreen*, in: Calliess/Ruffert, EUV/AEUV, 2022, Art. 26 GRCh, Rn. 2.

59 UN-Übereinkommen über die Rechte von Menschen mit Behinderungen (UN-Behindertenrechtskonvention) v. 13.12.2006, für die Bundesrepublik Deutschland in Kraft getreten am 26.3.2009, BGBl. 2008 II, 1419.

heit als internationales Menschenrecht aus Art. 12 AEMR[60] und Art. 17 IPbpR für Menschen mit Behinderungen konkretisiert.[61] Die UN-BRK dient als Erweiterung des Menschenrechtskatalogs der sog. „Universal Bill of Rights"[62] für die spezifischen Standards zur Gewährleistung eines vollen, gleichberechtigten Zugangs zu Menschenrechten und Grundfreiheiten für Menschen mit Behinderungen.[63] Deutschland hat die UN-BRK 2009 ratifiziert. Seitdem ist sie geltendes Recht im Rang eines Bundesgesetzes.[64] Die Vertragsstaaten müssen dafür sorgen, dass Menschen mit Behinderungen ihre Rechte wahrnehmen können, ohne dafür den Schutz ihrer Privatsphäre aufgeben zu müssen, und zwar gemäß Art. 22 Abs. 1 S. 1 UN-BRK ausdrücklich „unabhängig vom Aufenthaltsort oder der Wohnform".[65] Dies umfasst auch die Vertraulichkeit von Informationen über die Person, die Gesundheit und die Rehabilitation von Menschen mit Behinderungen (Abs. 2). Durch das Fehlen angemessener Schutzvorgaben und Kontrollen zur Wahrung der Privatheit, entstehen für Menschen mit Behinderungen erhebliche Diskriminierungsrisiken z. B. durch Profiling-Algorithmen oder ADM-Systeme, die aus Online-Daten persönliche Informationen ableiten und Entscheidungen zu Jobs, Krediten oder Versicherungen beeinflussen können.[66]

In den Abschließenden Bemerkungen zum kombinierten zweiten und dritten Staatenbericht Deutschlands weist der Ausschuss für die Rechte von Menschen mit Behinderungen der Vereinten Nationen in seinen Ausführungen zu Art. 22 UN-BRK auf seine Besorgnis über den Mangel an umfassenden Maßnahmen zum Schutz der persönlichen, medizinischen

60 UN-Resolution der Generalversammlung 217 A (III). Allgemeine Erklärung der Menschenrechte v. 10.12.1948.

61 *Trenk-Hinterberger*, in: Kreutz u.a., Die UN-Behindertenrechtskonvention in der Praxis, 2013, S. 218.

62 Aus dem Zivilpakt (IPbpR) und dem Sozialpakt (IPwskR) v. 16.12.1966 sowie der Allgemeinen Erklärung der Menschenrechte v. 10.12.1948.

63 *Denecke*, in: Franzen u.a., Kommentar zum europäischen Arbeitsrecht, 2024, Art. 1 CRPD, Rn. 2; *Banafsche*, in: Deinert u.a., SWK Behindertenrecht, 2022, Behindertenrechtskonvention, Rn. 7.

64 Art. 45 Abs. 2 UN-BRK und Art. 13 Abs. 2 des Fakultativprotokolls; Bekanntmachung über das Inkrafttreten des Übereinkommens der Vereinten Nationen über die Rechte von Menschen mit Behinderungen, 05.06.2009, BGBl. 2009 II, 812.

65 *Meier/Naguib,* in: Naguib u.a., UNO-Behindertenrechtskonvention, 2023, Art. 22, Rn. 10.

66 Vgl. *Behrendt/Loh*, Informed consent and algorithmic discrimination, REVIEW OF SOCIAL ECONOMY, 2022, 58 (58 ff.).

und rehabilitativen Daten von Menschen mit Behinderungen und ihres Rechts auf Privatsphäre hin.[67] Im Schwerpunkt bezieht sich diese Kritik jedoch nur auf die Datenverarbeitung in Einrichtungen und Werkstätten für behinderte Menschen (WfbM). Auch in der daraus resultierenden Empfehlung, alle erforderlichen Maßnahmen zu ergreifen, einschließlich der Überarbeitung der Datenschutzgesetze, um den Datenschutz und das Recht auf Privatsphäre in Krankenhäusern, Einrichtungen und WfbM zu gewährleisten, und Datenschutzverfahren und sichere Systeme einzurichten, die Menschen mit Behinderungen denselben Schutz ihrer persönlichen, gesundheitlichen und rehabilitativen Daten garantieren wie anderen,[68] greift der Ausschuss nicht weit genug. Die Schutzlücke einer situationsadäquaten Informationspräsentation in allen alltäglichen Bereichen, insbesondere im Rahmen der ubiquitären Einwilligung, bleibt unbenannt. Eine Beschränkung auf eine sichere Datenverarbeitung im Kontext von Einrichtungen oder WfbM blendet Privatheitsrisiken in anderen Bereichen aus. Dies lässt sich weder mit dem Wortlaut noch mit den allgemeinen Verpflichtungen der UN-BRK vereinbaren, die in Art. 4 Abs. 1 lit. g UN-BRK ausdrücklich die Forschung und Entwicklung von Informations- und Kommunikationstechnologien sowie die Förderung deren Verfügbarkeit und Nutzung hervorheben.

4.2 Digitale Barrierefreiheit als Voraussetzung der informierten Einwilligung: Völkerrechtliche Anforderungen an eine gleichberechtigte Teilhabe

Eine konkretere Benennung der Zugangsmöglichkeiten zu digitalen Infrastrukturen findet sich in der UN-BRK. Art. 4 lit. a UN-BRK verpflichtet die Vertragsstaaten alle geeigneten Gesetzgebungs-, Verwaltungs- und sonstigen Maßnahmen zu treffen, um Menschen mit Behinderungen eine unabhängige Lebensführung und die volle Teilhabe in allen Lebensbereichen zu ermöglichen. Dies inkludiert gem. Art. 4 lit. g iVm Art. 9 UN-BRK auch

67 *UN*, Ausschuss für die Rechte von Menschen mit Behinderungen, Abschließende Bemerkungen zum kombinierten zweiten und dritten Staatenbericht Deutschlands, 2023, CRPD/C/DEU/CO/2-3, S. 13.

68 UN, Ausschuss für die Rechte von Menschen mit Behinderungen, Abschließende Bemerkungen zum kombinierten zweiten und dritten Staatenbericht Deutschlands, 2023, CRPD/C/DEU/CO/2-3, S. 13f.

die Gewährleistung eines gleichberechtigten Zugangs zu Informations- und Kommunikationstechnologien und -systemen (einschließlich des Internets) sowie zu anderen elektronisch bereitgestellten oder öffentlich zugänglichen Angeboten sowie die Beseitigung vorhandener Zugangshindernisse und -barrieren (digitale Barrierefreiheit auch: digitale Teilhabe[69]). Dies umfasst gem. Art. 21, Art. 4 lit. h UN-BRK auch die Bereitstellung von Informationen, die für die Allgemeinheit bestimmt sind, über zugängliche Formate und Technologien z. B. in leichter Sprache oder durch Vorlesen der Information in Gestalt einer Sprachausgabe. Dabei sind die unterschiedlichen Arten der Behinderung, wie z. B. eine Körperbehinderung oder eine geistige Behinderung, differenziert zu berücksichtigen. Menschen mit Behinderungen dürfen somit beim Verständnis der Informationen im Vergleich zu nicht behinderten Menschen nicht benachteiligt werden.[70] Zur Verwirklichung einer gleichberechtigten Zugänglichkeit und Teilhabe an digitalen Infrastrukturen kann das in Art. 2 UN-BRK normierte Konzept des „universal design“ herangezogen werden. „Universal design“ beschreibt die Gestaltung von Produkten, Umgebungen, Programmen und Dienstleistungen so, dass sie für alle Menschen möglichst weitgehend ohne spezielle Anpassungen nutzbar sind. Dabei schließt es erforderliche Hilfsmittel für bestimmte Gruppen von Menschen mit Behinderungen nicht aus. Nach Art. 4 Abs. 1 lit. g und Art. 9 Abs. 2 lit. h UN-BRK sind die Vertragsstaaten in der Pflicht, dies bei der Förderung und Entwicklung von Informations- und Kommunikationstechnologien mitzudenken, sodass das Ziel mit geringem Kostenaufwand erreicht werden kann.[71] Die Realisierung der sozialen, wirtschaftlichen und kulturellen Rechte der UN-BRK unterfallen dem Progressionsvorbehalt aus Art. 4 Abs. 2 UN-BRK, wonach die Verwirklichung unter Ausschöpfung der zur Verfügung stehenden Mittel nach und nach zu erfolgen hat.[72] Eine unmittelbare Anwendung ergibt sich lediglich im Rahmen des Diskriminierungsschutzes aus Art. 3 lit. b, Art. 5 Abs. 2, Art. 2

69 *Busch*, Digitale Teilhabe für Menschen mit Behinderungen nach der UN-Behindertenrechtskonvention, ZESAR 2021, 484 (487).

70 *Trenk-Hinterberger*, in Kreutz u.a., Die UN-Behindertenrechtskonvention in der Praxis, 2013, S. 220, Rn. 8.

71 *Busch*, Digitale Teilhabe für Menschen mit Behinderungen nach der UN-Behindertenrechtskonvention, ZESAR 2021, 484 (488).

72 *Masuch*, „Die UN-Behindertenrechtskonvention anwenden“, Forum D-Diskussionsbeitrag Nr. 5/2012, S. 2; *Denecke*, in: Franzen u.a., Kommentar zum europäischen Arbeitsrecht, 2024, Art. 4 CRPD, Rn. 4, 5.

Abs. 3 UN-BRK.[73] Die Verwirklichung der Zugänglichkeit verpflichtet auch private Rechtsträger öffentlich zugänglicher Einrichtungen und Dienste (Art. 9 Abs. 1 lit. b UN-BRK). Gem. Art. 21 lit. c, d UN-BRK sind zudem private Rechtsträger und Massenmedien von den Vertragsstaaten nachdrücklich zu einer barrierefreien Ausgestaltung ihrer Dienstleistungen aufzufordern. Das damit bezweckte Einwirken über Vertreter in Aufsichtsgremien oder die Zusammenarbeit mit dem Bundesbehindertenbeauftragen, hat bisher nicht zu einer umfänglichen Verwirklichung von Barrierefreiheit beigetragen.[74]

4.3 Barrierefreie Einwilligung: Umsetzung in Deutschland

Vor dem Hintergrund der UN-BRK kommt der Sicherstellung einer barrierefreien und damit informierten Einwilligung zentrale Bedeutung zu. In Deutschland bilden das Behindertengleichstellungsgesetz und das Barrierefreiheitsstärkungsgesetz die gesetzlichen Grundlagen für die Umsetzung dieses Anspruchs.

4.3.1 Barrierefreiheit von Webseiten und mobilen Anwendungen öffentlicher Stellen durch das Behindertengleichstellungsgesetz

Die Basis für einen barrierefreien Zugang zu öffentlichen Informationen bilden die Richtlinie (EU) 2016/2102 „über den barrierefreien Zugang zu den Webseiten und mobilen Anwendungen öffentlicher Stellen“[75] und die Harmonisierte Europäische Norm (EN) 301 549, die die einschlägigen Barrierefreiheitsanforderungen an die Informations- und Kommunikationstechnik beinhaltet.[76] Umgesetzt werden die Vorgaben der EU-Richtlinie 2016/2102 in Deutschland durch das Behindertengleichstellungsgesetz

73 BT-Drs. 16/10808, S. 48; BSG Urt. v. 6.3.2012 – B 1 KR 10/11 R, BSGE 110, 194, SozR 4-1100 Art. 3 Nr. 69, Rn. 31; BSG Urt. v. 15.10.2014 – B 12 KR 17/12 R, BSGE 117, 117, SozR 4-2500 § 5 Nr. 24, Rn. 31; *Roller*, UN-Behindertenrechtskonvention in der sozialgerichtlichen Praxis, NZS 2019, 368 (371 f.).

74 *Trenk-Hinterberger*, in: Kreutz u.a., Die UN-Behindertenrechtskonvention in der Praxis, 2013, S. 221, Rn. 12, S. 223, Rn. 16; *Busch*, Digitale Teilhabe für Menschen mit Behinderungen nach der UN-Behindertenrechtskonvention, ZESAR 2021, 484 (488).

75 Richtlinie (EU) 2016/2102 v. 26.10.2016 über den barrierefreien Zugang zu den Webseiten und mobilen Anwendungen öffentlicher Stellen, ABl. (EU) L 327/1.

76 BfIT, Digitale Barrierefreiheit, 2025.

(BGG)[77] und die Umsetzungsverordnung des § 12d BGG, die Barrierefreie-Informationstechnik-Verordnung (BITV 2.0)[78]. Das BGG verpflichtet die Träger öffentlicher Gewalt insbesondere über §§ 12a, 12b BGG zur Herstellung digitaler Barrierefreiheit auf ihren Webseiten und mobilen Anwendungen (Barrierefreie Informationstechnik). Dies verlangt, dass Anwendungen der Informations- und Kommunikationstechnik für Menschen mit Behinderungen in der allgemein üblichen Weise, ohne besondere Erschwernis und grundsätzlich ohne fremde Hilfe auffindbar, zugänglich und nutzbar sein müssen (Barrierefreiheit, § 4 BGG). Die Anforderungen an die barrierefreie Gestaltung der Webseiten und mobilen Anwendungen werden durch § 3 Abs. 1 BITV 2.0 dahingehend konkretisiert, dass sie wahrnehmbar, bedienbar, verständlich und robust sein müssen. Dies wird unterstellt, wenn sie dem verbindlichen europäischen Standard der EN 301 549 entsprechen (Abs. 2) oder den Stand der Technik mit den entsprechenden DIN-ISO-Normen (Abs. 3) genügen. Insbesondere für die zentralen Navigations- und Einstiegsangebote, wie die Startseiten (Home), sowie Funktionen, die eine Nutzerinteraktion ermöglichen, soll das höchstmöglichste Maß an Barrierefreiheit nach den Erfolgskriterien der Web Content Accessibility Guidelines (WCAG 2.1)[79] mit der Konformitätsstufe AAA angestrebt werden.[80] Eine konkrete Benennung des hier fraglichen Formats der informierten Einwilligung, die in den meisten Fällen über einen Cookie-Banner auf den entsprechenden Webseiten eingebaut ist, findet sich in der BITV 2.0 nicht. Jedoch wird bei den Anforderungen an Angebote der Nutzerinteraktion auf Authentifizierungs-, Identifizierungs- oder Zahlungsprozesse verwiesen (§ 2a Abs. 1 S. 2, 3; Abs. 2 S. 3 BITV 2.0). Eine analoge Anwendung für ein höchstmögliches Maß an Barrierefreiheit kann folglich angenommen werden. Zudem werden die öffentlichen Stellen über § 4 BITV 2.0 dazu verpflichtet, Informationen über die wesentlichen Inhalte der Webseite in Deutscher Gebärdensprache und in leichter Sprache zur Verfügung zu stellen. Ausnahmen, die sich aufgrund unverhältnismäßiger Belastungen i. S. d

77 Gesetz zur Gleichstellung von Menschen mit Behinderungen (Behindertengleichstellungsgesetz – BGG) v. 27. 4.2002, BGBl. I, 1467; zuletzt geändert durch Art. 7 des Gesetzes v. 23.5.2022, BGBl. I, 760.

78 Barrierefreie-Informationstechnik-Verordnung 2.0 (BITV) v. 12.9.2011, BGBl. I, 1843; zuletzt geändert durch Art. 1 der Verordnung v. 21.5.2019, BGBl. I, 738; vgl. dazu die Begründung der Änderungs-VO, bekanntgemacht vom BMAS, BAnz AT 29.5.2019 B1.

79 Abrufbar unter http://www.w3.org/TR/WCAG21.

80 § 3 Abs. 4 BITV 2.0; *Carstens*, in: Deinert u.a., SWK Behindertenrecht, 2022, Barrierefreie Informationstechnik, Rn. 16 ff.

§ 12a Abs. 6 BGG zur Herstellung von Barrierefreiheit ergeben, sind restriktiv auszulegen und in der Erklärung zur Barrierefreiheit zu veröffentlichen (§ 12b Abs. 2 Nr. 1 BGG). Das Nichtvorhandensein geeigneter Software sowie der Mangel an Priorität, Zeit oder Kenntnis sind als unzureichende Gründe anzusehen. Eine anderweitige Auslegung der §§ 12a ff. BGG und §§ 3 ff. BITV 2.0 steht dem Ziel der Gewährleistung einer umfassenden und grundsätzlich uneingeschränkten barrierefreien Gestaltung gem. § 1 Abs. 1 BITV 2.0 entgegen.[81] Die durch das BGG geschaffenen Durchsetzungsmechanismen, wie die Verpflichtung der öffentlichen Stellen eine Erklärung zur Barrierefreiheit zu veröffentlichen (§ 12b BGG) sowie einen Feedbackmechanismus zur Meldung von Barrieren (§ 12b Abs. 2 Nr. 2 BGG) bereitzustellen, führt dazu, dass sich die öffentlichen Stellen mit der Pflicht zur Barrierefreiheit auseinandersetzen müssen.[82] Dennoch wird der Pflicht einer adäquaten barrierefreien Informationspräsentation im Rahmen der Einwilligung zur Datenerhebung bei Webseitennutzung nicht nachgekommen. Um Umständen wie diesen zu begegnen, besteht für Bund und Länder die Obliegenheit, Ombudsstellen, wie Schlichtungsstellen (§ 16 BGG) oder Beauftragte für barrierefreie Informationstechnik, zu schaffen.[83] Diese dienen als niedrigschwellige Form der außergerichtlichen Konfliktlösung.[84]

Zudem kennt das BGG in § 15 das Instrument der Verbandsklage. Die Erhebung eines solchen Feststellungsverfahrens ist aufgrund der Subsidiarität zum individuellen Rechtsschutz in aller Regel nur bei Fällen von allgemeiner Bedeutung gegeben (§ 15 Abs. 2 S. 2 BGG). Dies ist insbesondere bei einer „Vielzahl gleichgelagerter Fälle“ (§ 15 Abs. 2 S. 3 BGG) wie der Verletzung einer bundesrechtlichen Vorschrift zur Barrierefreiheit (Zugänglichkeit und Nutzbarkeit von Webseiten) anzunehmen.[85] Die Potenziale eines solchen Verbandsklageverfahrens bleiben in der Praxis allerdings weitgehend ungenutzt.[86] Die Barrierefreiheitsanforderungen des BGG be-

81 Siehe Erwägungsgrund 39 der RL (EU) 2016/2102; *Carstens*, in: Deinert u.a., SWK Behindertenrecht, 2022, Barrierefreie Informationstechnik, Rn. 23.

82 BT-Drs. 20/4440, S. 155.

83 *Carstens*, in: Deinert u.a., SWK Behindertenrecht, 2022, Barrierefreie Informationstechnik, Rn. 29; BT-Drs. 20/4440, S. 163 ff.

84 *Schaumberg*, in: Deinert u.a., SWK Behindertenrecht, 2022, Schlichtungsstelle, Rn. 1 ff.

85 BT-Drs. 20/4440, S. 156, 158; BT-Drs. 18/7824, S. 43; *Hlava*/Trienekens, in: Kahle u.a., Digitale Teilhabe und personenzentrierte Technologien im Kontext von Menschen mit Behinderungen, 2025, S. 56; ,*Hlava*, Barrierefreie Gesundheitsversorgung, 2018, S. 400 f.

86 BT-Drs. 20/4440, S. 162.

schränken sich in erster Linie auf öffentliche Stellen. Privatwirtschaftliche Online-Angebote, bleiben dadurch unreguliert, da es ohne gesetzliche Verpflichtung am Anreiz mangelt, barrierefreie Lösungen umzusetzen. Die digitale Exklusion von Menschen mit Behinderungen verhindert eine gleichberechtigte gesellschaftliche Teilhabe. Vorgaben zur Gewährleistung von Barrierefreiheit durch Private ergeben sich zwar aus Art 4 lit. a UN-BRK iVm Art. 9 Abs. 2 lit. b, Art. 4 lit. e und Art. 21 lit. c UN-BRK.[87] Da aber das BGG den Forderungen der UN-BRK nicht umfänglich nachkommt, ist eine Ausweitung des BGG auf private Akteure geboten. Dieser faktischen Ungleichbehandlung wurde versucht durch die Vorgaben der RL (EU) 2019/882 und dem Barrierefreiheitsstärkungsgesetz zu begegnen.

4.3.2 Barrierefreiheitsanforderungen für Produkte und Dienstleistungen nach dem Barrierefreiheitsstärkungsgesetz

Das Barrierefreiheitsstärkungsgesetz (BFSG)[88] verpflichtet neben den öffentlichen Stellen auch ausgewählte Wirtschaftsakteure der Produktangebotskette (z. B. Hersteller oder Dienstleister) zur Herstellung von Barrierefreiheit. Durch das BFSG werden die Barrierefreiheitsanforderungen der Richtlinie (EU) 2019/882 (European Accessibility Act (EAA))[89] in nationales Recht umgesetzt. Eine Konkretisierung der Anforderungen wurde gem. § 3 BFSG durch die Verordnung zum Barrierefreiheitsstärkungsgesetz (BFSGV)[90] vorgenommen. Adressiert werden ausgewählte Produkte (§ 1 Abs. 2 BFSG), z. B. Computer, Mobiltelefone, Tablets, Geldautomaten, Spielekonsolen, E-Book-Reader, sowie Dienstleistungen (§ 1 Abs. 3 Nr. 1 bis 5 BFSG), z. B. Video-Konferenz-Software, Messenger-Dienste, E-Ticket-Systeme oder Online-Shops.[91] Das Gesetz gilt ausschließlich für Produkte und Dienstleistungen, die nach dem 28.6.2025 in den Verkehr gebracht werden. Produkte sind in § 1 Abs. 2 BFSG abschließend aufgelistet und setzen einen

87 So auch: *Ritz*, in: Kossens u.a., SGB IX mit BGG, 2023, § 12a BGG, Rn. 21.

88 Gesetz zur Umsetzung der Richtlinie (EU) 2019/882 des Europäischen Parlaments und des Rates über die Barrierefreiheitsanforderungen für Produkte und Dienstleistungen (Barrierefreiheitsstärkungsgesetz – BFSG) v. 16.7.2021, BGBl. I, 2970.

89 Richtlinie (EU) 2019/882 v. 17.4.2019 über die Barrierefreiheitsanforderungen für Produkte und Dienstleistungen, ABl. (EU) L 151/70.

90 Verordnung über die Barrierefreiheitsanforderungen für Produkte und Dienstleistungen nach dem Barrierefreiheitsstärkungsgesetz (Verordnung zum Barrierefreiheitsstärkungsgesetz – BFSGV) v. 15.6.2022, BGBl. I, 928.

91 *Franke*, Digitale Barrierefreiheit von Produkten und Dienstleistungen, ZfPC 2024, 21.

Fertigungsprozess voraus. KI-Chatbots und AI-Companions fallen also beispielsweise nicht darunter. Auch der Begriff der Dienstleistung ist eng zu verstehen und setzt gemäß Art. 4 Nr. 1 RL 2006/123/EG[92], Art. 50 EGV[93] in der Regel ein Entgelt voraus (meist Vertragsabschlüsse).[94] Fraglich ist hierbei, inwiefern Geschäftsmodelle darunter subsumiert werden können, die darauf beruhen, dass die Verbrauchenden mit ihren personenbezogenen Daten statt mit Geld bezahlen. Ob es sich beim Bezahlen mit Daten um eine „wirtschaftliche Gegenleistung für die betreffende Leistung" handelt, die eine Entgeltersatzfunktion erfüllt, ist nicht abschließend geklärt.[95] Es sollte aber davon ausgegangen werden, dass der Gesetzgeber diese Fälle nicht aus dem Anwendungsbereich des BFSG exkludieren wollte. Für Webseiten wurde der Anwendungsbereich konkreter geregelt. Diese fallen nur in den Anwendungsbereich, wenn sie entweder „Element eines Personenbeförderungsdienstes" sind (§ 1 Abs. 3 Nr. 2 BFSG) oder mindestens eine „Dienstleistung im elektronischen Geschäftsverkehr" beinhalten (§ 1 Abs. 3 Nr. 5 BFSG).[96] Unter Bezugnahme des Anwendungsszenarios ist noch fraglich, ob eine Anwendung wie die eines AI-Companions als Telekommunikationsdienst i.S.d § 1 Abs. 3 Nr. 1 BFSG unter die Vorgaben des BFSG fällt. Da es sich bei einem AI-Companions weder um einen gegen Entgelt über elektronische Kommunikationsnetze erbrachten Dienst gem. § 2 Nr. 7 BFSG iVm Art. 2 Nr. 4 RL (EU) 2018/1972 handelt, noch um einen interpersonelle Kommunikationsdienst, wie z.B. Skype,[97] kann auch dies verneint werden. In Bezug auf die Frage der Ausgestaltung einer informierten Einwilligung kann jedoch insbesondere die BFSG-VO zur allgemeinen Konkretisierung der Barrierefreiheitsanforderungen an eine Informationspräsentation herangezogen werden. Hervorzuheben ist dabei der Verweis der Informationsdarstellung über das Zwei-Sinne-Prinzip, wonach die Bereitstellung über mehr als einen sensorischen Kanal gewährleistet

---

92 Richtlinie 2006/123/EG v. 12.12.2006 über Dienstleistungen im Binnenmarkt (ABl. L 376 S. 36).

93 Vertrag zur Gründung der Europäischen Gemeinschaft idF bis 30. November 2009.

94 *Tabbara*, Barrierefreiheit für elektronische Produkte und Dienstleistungen, NZS 2021, 497 (498); *Kapoor/Klindt*, Das Barrierefreiheitsstärkungsgesetz, NJW 2024, 3545, Rn. 3; *Franke*, Digitale Barrierefreiheit von Produkten und Dienstleistungen, ZfPC 2024, 21.

95 Vgl. *Fries*, BeckOGK, 2025, § 327 BGB, Rn. 21; *Ehlen/Möllnitz-Dimick*, Datenfinanzierte digitale Produkte, CR 2023, 455 (456ff.); *Randelzhofer/Forsthoff,* Das Recht der Europäischen Union, 2009, Art. 50 EGV, Rn. 43.

96 Vgl. *Kapoor/Klindt*, Das Barrierefreiheitsstärkungsgesetz, NJW 2024, 3545 (3545ff.).

97 BT-Drs. 19/28653, S. 64.

werden soll (§ 4 Abs. 1 BFSGV). Dies gilt in erster Linie für Alternativen zu visuellen, auditiven, gesprochenen und taktilen Elementen, sollte aber auch im Bezug zur Gewährleistung der Verständlichkeit im Allgemeinen nicht unterschätzt werden.

5. Zwischenfazit zur barrierefreien informierten Einwilligung

Während der Grundrechtsschutz für Kinder im Rahmen der Einwilligung in Art. 8 DSGVO ausdrücklich durch den Gesetzgeber adressiert wurde, bleibt die besondere Schutzbedürftigkeit anderer vulnerabler Gruppen, insbesondere von Menschen mit Behinderung, weitgehend unberücksichtigt. Dabei ergibt sich aus Art. 26 GRCh sowie Art. 22 UN-Behindertenrechtskonvention (UN-BRK) eine Pflicht zum Schutz der digitalen Privatheit auch für diese Personengruppe. Ergänzend verpflichten Art. 4 lit. g i. V. m. Art. 9 UN-BRK zur Gewährleistung eines gleichberechtigten Zugangs zu Informations- und Kommunikationstechnologien. Dies umfasst auch die barrierefreie Gestaltung von informierten Einwilligungsprozessen, etwa durch die Bereitstellung von Informationen in zugänglichen Formaten wie leichter Sprache oder auditiver Sprachausgabe. Die Regelungen zur Barrierefreiheit im deutschen Recht (BGG, BFSG) beschränken sich lediglich auf die barrierefreie Ausgestaltung von Webseiten. Es findet sich kein Bezug zur Einwilligung oder ihrer barrierefreien Gestaltung. Dies führt zu einer mangelhaften praktischen Ausgestaltung in Bezug auf die Erteilung von informierten Einwilligungen durch Menschen mit Behinderung (z. B. mit kognitiven Beeinträchtigungen). Neben einer Diskriminierung im Sinne des Art. 5 Abs. 2 UN-BRK kann darin auch eine Benachteiligung gem. Art. 3 Abs. 3 S. 2 GG sowie Art. 21 GRCh gesehen werden. Darüber hinaus sollte eine kritische Reflexion darüber erfolgen, inwiefern die individuellen Voraussetzungen der Einwilligenden, wie sie in Art. 8 DSGVO in Bezug auf die Einwilligungsfähigkeit und Einsichtsfähigkeit von Kindern beschrieben sind, auch für den „Durchschnittsnutzer“ angepasst werden sollten. Angesichts zunehmender digitaler Vulnerabilität – etwa durch überfordernde Informationsdichte, manipulative Interface-Gestaltung oder unzureichende Privacy Literacy – erscheint es geboten, die Wirksamkeitsvoraussetzung der Einwilligung ‚in informierter Weise‘ nicht schematisch am Modell des durchschnittlich informierten Nutzenden auszurichten, sondern stärker an die individuellen Bedürfnisse der Betroffenen anzupassen. Gerade beim

Einsatz von Dialogsystemen wie AI-Companions besteht andernfalls ein erhöhtes Risiko, dass Nutzende personenbezogene Daten unbedacht offenlegen, ohne sich der Tragweite ihrer Einwilligung vollumfänglich bewusst zu sein. Ausgehend von der Grundannahme, dass Vulnerabilität ein Teil des menschlichen Daseins ist, lässt sich aus den Grundrechten aus Art. 7 und 8 GRCh und Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG ein über die etablierten Schutzkonzepte hinausgehender Anspruch auf eine individuelle, situative und kontextbezogene Anpassung der Informations- und Einwilligungsvoraussetzungen konzipieren. Dieser sollte auch auf der Ebene der zu treffenden Maßnahmen nach Art. 25 DSGVO im Rahmen von „Privacy by Design" ansetzen.[98]

6. *Hoffnungsträger Einwilligungsverwaltungsverordnung?*

Ein Ansatzpunkt, zumindest Einwilligungsbanner auf Webseiten zu reduzieren, zu vereinfachen und Nutzende damit bei der Abgabe und Verwaltung von Einwilligungen zu unterstützen, ist die Einwilligungsverwaltungsverordnung (EinwV)[99]. Dienste zur Einwilligungsverwaltung gemäß § 26 TDDDG[100] sollen Nutzende dabei entlasten, täglich eine Vielzahl von Einzelentscheidungen darüber treffen zu müssen, ob Informationen im Endgerät gespeichert werden sollen oder Zugriff auf diese erfolgen darf (§ 25 Abs. 1 TDDDG).

Allerdings ist der Anwendungsbereich einigermaßen beschränkt, da es nur um Einwilligungen nach § 25 TDDDG zur Speicherung von oder den Zugriff auf Informationen in Endeinrichtungen des Nutzenden geht (§ 2 Abs. 1 Nr. 4 EinwV), nicht hingegen um sonstige Einwilligungen nach der DSGVO. Außerdem ist die Nutzung eines nach der EinwV anerkannten Dienstes für Webseitenbetreiber freiwillig (§ 18 EinwV). Es fehlen daher

98 *Kroschwald*, Nutzer-, kontext- und situationsbedingte Vulnerabilität in digitalen Gesellschaften, ZfDR 2023, 1 (9 ff.).

99 Verordnung über Dienste zur Einwilligungsverwaltung nach dem Telekommunikation-Digitale-Dienste-Datenschutz-Gesetz (Einwilligungsverwaltungsverordnung – EinwV) v. 6.2.2025, BGBl. I Nr. 32. Zum Referentenentwurf bereits *Nebel*, Alles abwählen: Mit der Einwilligungsverwaltungs-Verordnung gegen den Cookie-Banner-Dschungel, ZD-Aktuell 2022, 01321.

100 Gesetz über den Datenschutz und den Schutz der Privatsphäre in der Telekommunikation und bei digitalen Diensten (Telekommunikation-Digitale-Dienste-Datenschutz-Gesetz – TDDDG) v. 23.6.2021, BGBl. I, 1982, zuletzt geändert durch Art. 44 des Gesetzes zur weiteren Digitalisierung der Justiz v. 12.7.2024, BGBl. I Nr. 234.

Anreize sowohl für Entwickler, entsprechende Systeme zur Marktreife zu bringen, als auch für Webseitenbetreiber, da der Nichteinsatz ohne Konsequenz bleibt. Daher ist es äußerst fraglich, ob das Ziel der Verordnung erreicht werden kann.[101]

Gerade für vulnerable Gruppen könnte ein entsprechendes Einwilligungsverwaltungssystem jedoch eine immense Entlastung im Alltag bedeuten, da nicht mehr eine Vielzahl von informierten Einzelentscheidungen getroffenen werden müssten, sobald eine Webseite aufgerufen, Cookies gespeichert oder Informationen abgerufen werden sollen. Individuelle Präferenzen könnten einmalig, gegebenenfalls mit Unterstützung durch betreuende Personen, gesetzt werden und anschließend Berücksichtigung finden. Ohne das Mitwirken einer betreuenden Person müsste das System Nutzerdaten, wie z.B. das Alter oder den Bildungsstand, erfassen, um benutzerspezifische Informationen über seine Funktionsweise bereit stellen zu können. Dies würde jedoch die Informationsasymmetrie zwischen Anbieter und Nutzenden vergrößern, da der Gewinn an Verständlichkeit und Selbstbestimmung mit einem gleichzeitigen Verlust durch die Erhebung personenbezogener Daten einhergeht.[102]

Es bleibt festzuhalten, dass die EinwV einen guten Ansatz bereithält, um vulnerablen Nutzenden das Management der Einwilligungen zu erleichtern. Leider ist sie im Anwendungsbereich zu eingeschränkt, um einen nennenswerten Unterschied zu machen.

7. Selbstbestimmung vulnerabler Nutzender im europäischen Datenrecht: Rechtspflichten und Verbesserungsbedarf am Beispiel von AI-Companions

Die Wirksamkeit der Einwilligung vulnerabler Nutzender sicherzustellen, ist – wie festgestellt – keine triviale Aufgabe. Um die Selbstbestimmung der betroffenen Personen zu stärken und damit auch die Potenziale, die der wirksamen Einwilligung hierbei zukommen, zu unterstützen, wurden eine Reihe von Compliance-Pflichten im neuen europäischen Datenrecht geschaffen. Dieses hat in jüngster Zeit, insbesondere durch die KI-VO, den Digital Services Act und den Digital Markets Act, erhebliche Veränderungen erfahren und ein ausdifferenziertes Umfeld hervorgebracht. Der

101 *Landesbeauftragte für Datenschutz Niedersachsen*, Pressemitteilung 20/2024 vom 27.12.2024. So auch bereits *DSK*, Stellungnahme zum Referentenentwurf vom 11.7.2023.

102 *Geminn*, Deus ex machina?, 2023, S. 175.

folgende Abschnitt stellt an ausgewählten Regelungen dar, ob und wie das europäische Datenrecht die Selbstbestimmung vulnerabler Nutzender durch zusätzliche Verpflichtungen am Beispiel von Anbietern von AI-Companions gewährleisten kann und wo Verbesserungsbedarf besteht.

7.1 Verordnung für Künstliche Intelligenz

Am 21.5.2024 wurde die Verordnung für Künstliche Intelligenz (KI-VO) verabschiedet.[103] Es handelt sich um die weltweit erste umfassende Regelung für den Einsatz von Künstlicher Intelligenz und gilt damit als Vorreiter für eine risikoorientierte Regulierung des Einsatzes Künstlicher Intelligenz in der Gesellschaft. Die Verordnung soll das gesamtgesellschaftliche Vertrauen in Künstliche Intelligenz stärken.[104] Die KI-VO regelt technikspezifisch Künstliche Intelligenz in Abhängigkeit von ihrem Risiko und unterteilt dabei in vier Gruppen: „verbotene Praktiken im KI-Bereich", „Hochrisiko-KI-Systeme", KI-Systeme mit begrenztem Risiko und KI-Systeme mit geringem oder keinem Risiko. Nicht akzeptable Risiken sind gemäß Art. 5 KI-VO verboten. Die Hauptlast der Regulierung liegt in der KI-VO bei Hochrisiko-KI-Systemen gemäß Art. 6 KI-VO. Wird ein KI-System als solches eingestuft, obliegen den Anbietern und Betreibern umfangreiche Sorgfalts-, Kontroll- und Informationspflichten. Für KI-Systeme mit begrenztem Risiko gelten demgegenüber abgeschwächte Vorgaben. KI-Systeme mit geringem oder keinem Risiko bleiben unreguliert.[105]

Der Regelungsgehalt der KI-VO fokussiert sich im Wesentlichen auf Risikobewertungen und Maßnahmen, um entsprechende Risiken einzudäm-

103 Verordnung (EU) 2024/1689 des Europäischen Parlaments und des Rates vom 13.6.2024 zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz und zur Änderung der Verordnungen (EG) Nr. 300/2008, (EU) Nr. 167/2013, (EU) Nr. 168/2013, (EU) 2018/858, (EU) 2018/1139 und (EU) 2019/2144 sowie der Richtlinien 2014/90/EU, (EU) 2016/797 und (EU) 2020/1828 (Verordnung über künstliche Intelligenz), ABl. L, 2024/1689, 12.7.2024.

104 *Chibanguza/Steege*, Die KI-Verordnung – Überblick über den neuen Rechtsrahmen, NJW 2024, 1769.

105 Übersichten zur KI-VO z. B. *Geminn*, Die Regulierung künstlicher Intelligenz, ZD 2021, 354; *Chibanguza/Steege*, Die KI-Verordnung – Überblick über den neuen Rechtsrahmen, NJW 2024, 1769; *Horstmann*, KI-VO und Datenschutz: Überblick und ausgewählte Fragen, ZD-Aktuell 2024, 01580.

men und ist damit eher produktsicherheitsrechtlich motiviert.[106] Entsprechend regelt Art. 2 Abs. 7 S. 1 KI-VO, dass Unionsvorschriften zum Schutz personenbezogener Daten, Privatsphäre und Vertraulichkeit der Kommunikation weitergelten und die DS-GVO gemäß Satz 2 unberührt bleibt.[107] Anwendbar ist die KI-VO gemäß Art. 2 Abs. 1 KI-VO für alle Anbieter, Betreiber, Einführer, Händler, Hersteller von KI-Systemen. Anbieter, die Chatbots oder AI Companions in der Union anbieten, sind in der Regel Anbieter und/oder Betreiber von KI-Systemen.

Verboten sind Chatbots oder AI-Companions nach der KI-VO, wenn sie unter die Anwendungsfälle des Art. 5 KI-VO fallen. Relevant sind insbesondere Abs. 1 lit. a bis c:[108] Gemäß Art. 5 Abs. 1 lit. a KI-VO sind Techniken der unterschwelligen Beeinflussung (Dark Patterns) verboten, die auf eine Verhaltensänderung abzielen, indem die Fähigkeit der freien Entscheidungsfindung beeinträchtigt wird und wenn dies einer Person[109] erheblichen Schaden zufügt oder zufügen würde. Schaden ist als Begriff des Unionsrechts autonom auszulegen.[110] Erwägungsgrund 29 S. 2 KI-VO spricht von "große[n] Schäden, insbesondere erhebliche nachteilige Auswirkungen auf die physische oder psychische Gesundheit oder finanzielle Interessen". Umfasst sind also sowohl materielle als auch immaterielle Schäden. Es ist von einem eher engen Schadensbegriff auszugehen,[111] der sowohl „groß“ als auch „erheblich“ sein muss und kausal mit der Beeinflussung zusammenhängt. Wann ein Schaden erheblich ist, dazu äußert sich die Verordnung nicht. Schutzgut ist weniger die Selbstbestimmung der Nutzenden als ein physischer, psychischer oder finanzieller Schaden.[112] Im Hinblick auf

106 *Hacker/Berz,* Der AI Act der Europäischen Union – Überblick, Kritik und Ausblick, ZRP 2023, 226; *Horstmann*, KI-VO und Datenschutz: Überblick und ausgewählte Fragen, ZD-Aktuell 2024, 01580.
107 Vgl. auch Erwägungsgrund 10 KI-VO. Ausführlich zum Verhältnis der KI-VO zur DS-GVO *Nebel*, in: Geminn/Johannes (Hrsg.), Europäisches Datenrecht, 2025 i.E.
108 *Böhning/Schindler*, Verbotene Praktiken im KI-Bereich – Wann ist was verboten?, ZD-Aktuell 2024, 01793.
109 S. zur Frage, welche Person im Einzelfall gemeint sein könnte, *Böhning/Schindler*, Verbotene Praktiken im KI-Bereich – Wann ist was verboten?, ZD-Aktuell 2024, 01793.
110 Vgl. zum Schadensbegriff in der DSGVO EuGH, Urteil vom 4.5.2023, Rs. C-300/21, ECLI:EU:C:2023:370.
111 *Martini/Kramme/Kamke,* KI-VO, DMA und DA als Missing Links im Kampf gegen dunkle Designmuster?, MMR 2023, 399 (400) zu KI-VO-E.
112 So bereits *Martini/Kramme/Kamke,* KI-VO, DMA und DA als Missing Links im Kampf gegen dunkle Designmuster?, MMR 2023, 399 (400) zu Art. 5 KI-VO-E.

Verbraucherschutz im Allgemeinen und Schutz vulnerabler Gruppen im Besonderen scheint dies etwas zu kurz gedacht, wobei zumindest der Schaden – anders als noch im Verordnungsentwurf[113] – nunmehr finanzielle Aspekte mit umfasst. Das ist zu begrüßen. Die Regelung lässt trotzdem viele Fragen offen und ist in seiner praktischen Wirkweise zu Lasten von Dark Pattern deutlich mehr eingeschränkt, als auf den ersten Blick vermuten lässt. Fraglich ist auch, ob die Vorschrift einen individuellen Anspruch auf Schadenersatz verleiht; dann wäre die Person aber hinsichtlich des Schadens wahrscheinlich beweisbelastet. AI-Companions werden jedenfalls in aller Regel nicht im Ganzen unter das Verbot fallen – bestimmte Praktiken des KI-Systems aber möglicherweise schon.

Verboten ist gemäß Art. 5 Abs. 1 lit. b KI-VO außerdem ein KI-System, das eine Vulnerabilität oder Schutzbedürftigkeit einer Person aufgrund ihres Alters, einer Behinderung oder ihrer sozialen oder wirtschaftlichen Situation ausnutzt mit dem Ziel einer Verhaltensbeeinflussung und dieser Person dadurch ein erheblicher Schaden droht oder zugefügt wird. Bezüglich des Schadens gilt das eben Gesagte, so dass nicht jedes KI-System, das eine Vulnerabilität ausnutzt, unter lit. b fallen wird.

Art. 5 Abs. 1 lit. c KI-VO statuiert ein Verbot der Schlechterstellung oder Benachteiligung durch soziale Bewertung aufgrund von Social Scoring, aber nur bei Zweckentfremdung der Daten oder Unverhältnismäßigkeit. Der Unionsgesetzgeber eruiert nicht näher, was Unverhältnismäßigkeit umfasst und wie zwischen gerechtfertigter oder verhältnismäßiger und ungerechtfertigter oder unverhältnismäßiger Schlechterstellung oder Benachteiligung unterschieden werden soll.[114] Bestimmte Einsatzfelder von Social Scoring sieht der Unionsgesetzgeber jedenfalls als durchaus akzeptabel an.[115]

In der Regel werden AI-Companions nicht unter das Verbot in Art. 5 KI-VO fallen, da dessen Voraussetzungen sehr spezifisch und eng sind und insbesondere der kausale, große und erhebliche Schaden schwer nachweisbar sein wird. Art. 5 Abs. 1 lit. a bis c KI-VO gibt aber rote Linien insbesondere hinsichtlich der Verhaltensbeeinflussung und freien Entscheidungsfindung vor, die Diensteanbieter beachten müssen, um nicht unter das Verbot von Art. 5 KI-VO zu fallen.

113 Vgl. KI-VO-E, COM(2021) 206 final, Punkt 5.2.2. im Vergleich zu Erwägungsgrund 29 S. 2 KI-VO (VO 2024/1689).

114 *Böhning/Schindler*, Verbotene Praktiken im KI-Bereich – Wann ist was verboten?, ZD-Aktuell 2024, 01793.

115 Kritisch hierzu *Becker/Feuerstack,* Die EU-KI-Verordnung, KIR 2024, 62.

Als Hochrisiko-KI wären AI-Companions dann einzustufen, wenn sie unter die Kategorisierung des Art. 6 KI-VO fallen. Da solche Dialogsysteme weder in den in Art. 6 Abs. 1 iVm Anhang I und II KI-VO aufgeführten Produktbereichen genannt sind noch bisher als Sicherheitsbauteil gelten, bleibt nur Art. 6 Abs. 2 iVm Anhang III KI-VO. Anhang III nennt acht spezifische Einsatzbereiche für den Hochrisiko-KI-Bereich. Das sind etwa Biometrie, Kritische Infrastruktur, der Bildungsbereich, Beschäftigung und Personalmanagement oder Strafverfolgung. Keiner der genannten Einsatzbereiche tangiert Dialogsysteme, die im privaten Umfeld aus reinen Privatinteressen heraus genutzt werden, auch nicht, wenn sie intime Kommunikation ermöglichen.

Daher sind die hier betrachteten AI-Companions sonstige KI-Systeme, die lediglich den leicht umzusetzenden Transparenzpflichten aus Art. 50 Abs. 1 KI-VO unterfallen.[116] Die AI-Companions sind also als KI-System zu kennzeichnen, damit Nutzende wissen, dass sie mit einem KI-System kommunizieren.

7.2 Digital Services Act

Der Digital Services Act (DSA)[117] fördert durch diverse Maßnahmen die Selbstbestimmung in digitalen Infrastrukturen. Gegenstand des DSA sind Vermittlungsdienste. Je nach Qualifizierung des jeweiligen Dienstes legt der DSA diesen Diensten Haftungsbefreiungen und Sorgfaltspflichten für ein transparentes und sicheres Online-Umfeld auf. Die Anbieterpflichten des DSA bleiben auch durch die KI-VO unberührt.[118]

Um unter den DSA zu fallen, müssten AI-Companions und sonstige Chatbots Vermittlungsdienste im Sinne des Art. 3 lit. g DSA sein. Inwiefern Dienste, die rein auf einem KI-System basieren, unter den DSA zu subsumieren sind, bedarf einer genaueren Untersuchung. Voraussetzung aller Vermittlungsdienste im Sinne des Art. 3 lit. g DSA ist, dass es sich um

116 Vgl. *Chibanguza/Steege*, Die KI-Verordnung – Überblick über den neuen Rechtsrahmen, NJW 2024, 1769 (1774).

117 Verordnung (EU) 2022/2065 des Europäischen Parlaments und des Rates vom 19.10.2022 über einen Binnenmarkt für digitale Dienste und zur Änderung der Richtlinie 2000/31/EG.

118 Art. 2 Abs. 5 KI-VO.

Dienste der Informationsgesellschaft handelt[119] und dass sie vom Nutzenden bereit gestellte Daten als „reine Durchleitung", „Caching-„ oder „Hosting-Dienst" verarbeiten. Bei generativen KI-Systemen wird nur ein sehr kleiner Teil der Daten vom Nutzenden bereitgestellt, da hauptsächlich aus den Inputs der Nutzenden neue Daten abgeleitet werden, die die Kernanwendung oder den Kernnutzen des KI-Systems ausmachen. Diese Daten sind jedoch nicht vom Nutzenden bereitgestellt, sondern vom System inferiert. Nur in dem begrenzten Umfang der tatsächlichen Bereitstellung ist der Diensteanbieter als Anbieter eines Vermittlungsdienstes im Sinne des DSA anzusehen; da die vom Nutzer bereitgestellten Informationen in dessen Auftrag gespeichert werden, ist der Dienst als Hosting-Dienst einzustufen. Diejenigen Informationen, die aus den bereit gestellten Daten der Nutzenden durch die generative KI abgeleitet werden, z. B. Nachrichten und Aufforderungen des AI-Companions an den Nutzenden, sind jedoch nicht vom Nutzenden bereitgestellt, sondern von der KI erzeugt, und fallen damit nicht unter den DSA.[120]

Die generative KI könnte als Anwendung je nach konkreter Ausgestaltung als Empfehlungssystem im Sinne des Art. 3 lit. s DSA oder als Verbot von Dark Patterns im Sinne des Art. 25 DSA eingestuft werden.[121]

Empfehlungssysteme sind gemäß Art. 3 lit. s DSA „vollständig oder teilweise automatisierte Systeme definiert, die von einer Online-Plattform verwendet werden, um auf ihrer Online-Schnittstelle den Nutzern bestimmte Informationen vorzuschlagen oder diese Informationen zu priorisieren". Bei der Verwendung von solchen Empfehlungssystemen sind Anbieter von Online-Plattformen verpflichtet, bestimmte Transparenzanforderungen im Sinne des Art. 27 Abs. 1 DSA umzusetzen.

Bei dem Verbot von Dark Patterns im Sinne des Art. 25 DSA handelt es sich nach Erwägungsgrund 67 DSA um „Praktiken, mit denen darauf abgezielt oder tatsächlich erreicht wird, dass die Fähigkeit der Nutzenden, eine autonome und informierte Entscheidung oder Wahl zu treffen, erheblich verzerrt oder beeinträchtigt wird". Das Verbot in Art. 25 DSA bezieht sich auf sogenannte Online-Schnittstellen. Ob es sich bei einem AI-Com-

119 Art. 3 lit. a DSA iVm Art. 1 Abs. 1 lit. b RL (EU) 2015/1535. Diese Voraussetzungen liegen bei AI-Companions vor.

120 *Berz/Engel/Hacker*, Generative KI, Datenschutz, Hassrede und Desinformation – Zur Regulierung von KI-Meinungen, ZUM 2023, 586 (590 f.) zu generativer KI im Rahmen der Meinungsbildung.

121 *Wehde*, Regulierung von Large Language Models in DSA und AIA-E, MMR-Aktuell 2023, 455171.

panion, also einem auf einem KI-System basierenden Chatbot, um eine Online-Schnittstelle im Sinne des Art. 3 lit. m DSA handelt, ist jedoch nicht abschließend geklärt. Bei Online-Schnittstellen handelt es sich um „Software [...] sowie Anwendungen, einschließlich Mobil-Apps". Gemeint ist damit wohl das Software-Interface[122], also die Gestaltung der Benutzeroberfläche;[123] aber auch nicht ohne weiteres wahrnehmbare Gestaltungselemente einer Software können darunterfallen.[124] Auch ein KI-System könnte ein solches Gestaltungselement sein und fällt zudem unter den Begriff Software. Die Rechtsfolge bezogen auf AI-Companions wäre jedenfalls, dass die Nutzenden nicht getäuscht, manipuliert oder in ihrer freien Entscheidung beeinträchtigt werden dürfen. Nicht die Interaktion mit dem AI-Companion an sich wäre verboten, da die Nutzenden wissen und sich mehr noch freiwillig für die Nutzung eines AI-Companions entschieden haben. Möglicherweise könnten aber bestimmte Praktiken des KI-Systems unter das Verbot fallen, wenn sie eine entsprechende Wirkung auf den Nutzenden haben. Denkbar ist dies etwa in Fällen, dass das KI-System den Nutzenden dazu verleitet, Bilder von sich herauszugeben, die beispielsweise für die Generierung von Nacktbildern genutzt werden könnten,[125] oder Nutzende zum Suizid verleitet.[126] Diese Regelung ergänzt gut die verbotenen Praktiken der KI-VO um solche Fälle abzufangen, die mangels Schaden nicht in den engen Anwendungsbereich des Art. 5 KI-VO fallen, deren Verhinderung aber durchaus im Interesse des Unionsgesetzgebers und der Gesellschaft sein sollte.

Im Ergebnis bleibt festzuhalten, dass Anbieter von AI-Companions als Vermittlungsdienste nur in begrenztem Umfang unter den DSA fallen, aber zumindest für diejenigen Informationen, die die Nutzenden aktiv bereitstellen, gemäß Art. 11 ff. DSA sorgfaltsverpflichtet sind. Relevante Verpflichtungen, denen Diensteanbieter von AI-Companions nachkommen müssen und die insbesondere den Aspekt der Sicherstellung der Selbstbestimmung unterstützen können, sind die allgemeinen Bestimmungen der Art. 11 ff. DSA z. B. zum Einrichten von Kontaktstellen, AGB-Erfordernisse,

---

122 *Köhler/Holznagel/Müller-Terpitz*, in: Müller-Terpitz/Köhler, 2024, Digital Services Act, Art. 3 DSA, Rn. 114.

123 *Hofmann*, in: Hofmann/Raue, 2024, Digital Services Act, Art. 3 DSA, Rn. 114.

124 *Hofmann*, in: Hofmann/Raue, 2024, Digital Services Act, Art. 3 DSA, Rn. 114.

125 *Mozilla Foundation*, EVA AI Chat Bot und Soulmate, 2024. *Kühl*, Das Nacktbild, das man nie geschossen hat, Zeit Online vom 14. Dezember 2023.

126 Z.B. *Payne*, An AI chatbot pushed a teen to kill himself, a lawsuit against its creator alleges, Associated Press vom 24. Oktober 2024.

Transparenzpflichten, Melde- und Abhilfeverfahren nach Art. 16 DSA. Da AI-Companions mangels der öffentlichen Verbreitung der vom Nutzenden bereitgestellten Daten nicht als Online-Plattform im Sinne des Art. 3 lit. i DSA zu qualifizieren sind, gelten die zusätzlichen Regelungen der Art. 20 ff. DSA nicht für AI-Companions.

Sollte aber eine Online-Plattform im Sinne des DSA einen Chatbot nutzen, gelten zusätzlich die Regelungen zur Errichtung eines internen Beschwerdemanagements nach Art. 20 DSA. Zudem wären Online-Schnittstellen nach den Vorgaben des Art. 25 DSA zu gestalten, beim Platzieren von Werbung ist Art. 26 DSA zu beachten und beim Einsatz von Empfehlungssystemen Art. 27 DSA. Art. 28 DSA macht Vorgaben zum Online-Schutz Minderjähriger. Andere vulnerable Gruppen sind leider im DSA nicht mitgedacht.

Mit dem Fokus auf Vulnerabilität lohnt sich ein Blick auf Art. 34 Abs. 1 lit. d DSA. Art. 33 ff. DSA stellt spezifische zusätzliche Pflichten für sehr große Online-Plattformen und sehr große Online-Suchmaschinen auf. Art. 34 Abs. 1 lit. d DSA sticht hervor, da dieser bei der verpflichtenden Analyse zur systemischen Risikobewertung und Risikominderung „nachteilige Folgen für das körperliche und geistige Wohlbefinden einer Person" berücksichtigt sehen möchte. Dies öffnet den Blick auf andere vulnerable Gruppen als nur Minderjährige und verspricht großes Potenzial um nachteilige Auswirkungen auf vulnerable Gruppen zu eruieren und zu verhindern. Gleiches gilt für die zusätzlichen Transparenzanforderungen für Online-Werbung nach Art. 39 DSA. Dieser verpflichtet Anbieter dazu, öffentlich zugängliche, durchsuchbare Archive zu Werbeanzeigen mit den in Abs. 2 genannten Angaben zu erstellen. Besonders interessant ist im Hinblick auf vulnerable Gruppen Abs. 2 lit. e Demnach sind Angaben dazu zu machen, ob und welchen bestimmten Gruppen von Nutzern die Werbung angezeigt werden sollte. Der Begriff Gruppe ist nicht weiter definiert und damit offen; umfasst sein könnten also auch alle denkbaren vulnerablen Gruppen, die durch die Werbewirtschaft explizit angesprochen werden könnten, neben Minderjährigen etwa Senioren, Menschen mit Behinderungen oder Menschen mit Suchtgefährdungspotenzial. Zweck der Regelung ist es gemäß Erwägungsgrund 95 DSA, „die Aufsicht und die Forschung zu neu entstehenden Risiken im Zusammenhang mit der Online-Verbreitung von Werbung zu unterstützen". Dies spricht jedenfalls dafür, vulnerable Personen mit in Betracht zu ziehen.

Da AI-Companions nicht unter den Begriff der Online-Plattformen, können die Regelungen der Art. 33 ff. DSA nicht zur Anwendung kommen.

Dies erscheint angesichts der Auswirkungen, die AI-Companions auf (vulnerable) Nutzende haben können, als eine eklatante Regelungslücke.

7.3 Digital Markets Act

Der Digital Markets Act (DMA)[127] ist Teil eines Regelungspakets der Europäischen Union. Der DMA soll gleiche Wettbewerbsbedingungen in digitalen Märkten schaffen, indem Anbieter zentraler Plattformdienste stärker reguliert werden. Adressat der Regelungen des DMA sind gemäß Art. 1 Abs. 2 DMA Torwächter (Gatekeeper) im Sinne des Art. 2 Nr. 1 DMA, also Unternehmen, die einen zentralen Plattformdienst bereitstellen und von der Kommission nach Art. 3 DMA als solche benannt wurden. Da der DMA eher wettbewerbspolitisch geprägt ist, liegt der Fokus nicht auf datenschutzrechtlichen Aspekten; er nimmt nicht bestimmte Nutzergruppen in den Blick, sondern fokussiert auf spezifische Maßnahmen, um Infrastrukturen für alle fairer zu machen und Marktmissbrauch zu verhindern.

Allerdings fallen AI-Companions nicht unter die in Art. 2 Nr. 2 DMA abschließend aufgezählten Plattformdienste. Es handelt sich nicht um einen Online-Vermittlungsdienst nach Art. 2 Nr. 5 iVm Art. 2 Nr. 2 VO (EU) 2019/1150[128]. Trotz der Wortgleichheit mit Vermittlungsdiensten des DSA liegt hier eine andere Definition zu Grunde: Online-Vermittlungsdienste gemäß Art. 2 Nr. 2 lit. a bis c VO (EU) 2019/1150 sind Dienste der Informationsgesellschaft, die es gewerblichen Nutzern ermöglichen, Verbrauchern Waren oder Dienstleistungen anzubieten, indem sie eine Transaktion zwischen diesen vermitteln. Dies trifft auf AI-Companions nicht zu, so dass sie keine Online-Vermittlungsdienste im Sinne des DMA sind. Sie sind auch kein Online-Dienst eines sozialen Netzwerks im Sinne des Art. 2 Nr. 7 DMA, da sie keine Kontakte mit anderen Nutzern ermöglichen, sondern nur Interaktion mit einem KI-System. Schließlich gelten sie auch nicht als virtueller Assistent im Sinne des Art. 2 Nr. 12 DMA, da sie keine Aufträge, Aufgaben oder Fragen verarbeiten zu dem Zweck Zugang zu

127 Verordnung (EU) 2022/1925 des Europäischen Parlaments und des Rates vom 14.9.2022 über bestreitbare und faire Märkte im digitalen Sektor und zur Änderung der Richtlinien (EU) 2019/1937 und (EU) 2020/1828 (Gesetz über digitale Märkte), ABl. vom 12.10.2022, L 265, 1. Kommissionsvorschlag abrufbar unter: https://eur-lex.europa.eu/legal-content/en/ALL/?uri=COM:2020:842:FIN.

128 Verordnung (EU) 2019/1150 des Europäischen Parlaments und des Rates vom 20. Juni 2019 zur Förderung von Fairness und Transparenz für gewerbliche Nutzer von Online-Vermittlungsdiensten. ABl. EU vom 11.7.2019, L 186/57.

anderen Diensten zu ermöglichen oder angeschlossene physische Geräte zu steuern. Der DMA findet mithin im Kontext von AI-Companions keine Anwendung.

8. Fazit

Die Gewährleistung der Selbstbestimmung als Folge einer informierten Entscheidung des Individuums in solchen digitalen Infrastrukturen ist keine triviale Aufgabe und lässt sich nicht auf Knopfdruck bewältigen. Die Relevanz ist vor dem Hintergrund des politischen und wirtschaftlichen Einflusses der Datenverarbeitenden auf das demokratisch-rechtsstaatliche Gemeinwesen nicht zu unterschätzen. Gerade in Kontexten, in denen die Vulnerabilität ein entscheidender Faktor ist, muss dem Merkmal der Informiertheit noch mehr Aufmerksamkeit geschenkt werden.

Nach wie vor spielt die datenschutzrechtliche Einwilligung eine entscheidende Rolle zur Förderung und Verwirklichung des Freiheitsrechts auf informationelle Selbstbestimmung, da sie die kollidierenden Freiheiten der von der Datenverarbeitung betroffenen Personen und den Interessen der Verantwortlichen zu vereinen versucht. Dies darf jedoch nicht darüber hinwegtäuschen, dass praktische Probleme in der Umsetzung die Bedeutung der Einwilligung erheblich schmälern. Bestehende Machtdisparitäten, Konditionen oder strukturelle Probleme wie überlange, komplizierte oder unverständliche Einwilligungserklärungen wirken sich zumeist nachteilig für die betroffene Person aus. Hier müssen neue Wege beschritten werden, um dem Bedeutungsverlust der datenschutzrechtlichen Einwilligung entgegenzutreten.

Das europäische Datenrecht hat in den letzten Jahren einen enormen Wandel erfahren – wo zunächst die DSGVO als große Innovation gefeiert werden konnte, um das Datenschutzrecht auf ein neues Niveau zu heben, war bald klar, dass dies im Angesicht der sich rasant entwickelnden Technologien nicht ausreichen wird. Allerdings bringen die neuen Verordnungen KI-VO, DSA und DMA nur sehr eingeschränkten Nutzen für vulnerable Nutzende insbesondere im Anwendungsbereich von AI-Companions. Zwar werden umfangreiche Verpflichtungen für Diensteanbieter statuiert. AI-Companions und Chatbots werden weder in der KI-VO nennenswert reguliert noch fallen sie unter den DMA und auch bezüglich des DSA ist der Anwendungsbereich nur sehr eingeschränkt. Der Sicherstellung der Wirksamkeit der Einwilligung kommt daher nur umso mehr Bedeutung zu.

Literatur

Art.-29-Gruppe, Leitlinien für Transparenz gemäß der Verordnung 2016/679, WP 260 rev.01,https://www.datenschutzkonferenz-online.de/media/wp/20180411_wp260_rev01.docx.

Becker, Daniel und Feuerstack, Daniel (2024): Die EU-KI-Verordnung. *Künstliche Intelligenz und Recht*, 2/2024, S. 62-69.

Behrendt, Hauke und Loh, Wulf (2022): Informed consent and algorithmic discrimination – is giving away your data the new vulnerable? *Review of Social Economy*, 80(1), S. 58-84. https://doi.org/10.1080/00346764.2022.2027506.

Berz, Amelie, Engel, Andreas und Hacker, Philipp (2023): Generative KI, Datenschutz, Hassrede und Desinformation – Zur Regulierung von KI-Meinungen. *Zeitschrift für Urheber- und Medienrecht*, 8-9/2023, S. 586-594.

Bielefeldt, Heiner (2019): Vulnerabilität als Menschenrechtsthema – Eine Problemskizze. In: Bergemann, Lutz und Frewer, Andreas (Hrsg.): *Autonomie und Vulnerabilität in der Medizin*. Bielefeld: transcript, S. 21-38.

Bieresborn, Dirk und Schafhausen, M. (Hrsg.) (2024): *Münchener Anwaltshandbuch Sozialrecht*. 6. Auflage. München: Beck.

Birkmann, Jörn; Bach, Claudia; Guhl, Silvie; Witting, Maximilian; Welle, Torsten und Schmude, Miron (2010): *State of the Art der Forschung zur Verwundbarkeit Kritischer Infrastrukturen am Beispiel Strom/Stromausfall*. Berlin: Forschungsforum Öffentliche Sicherheit. URL: https://www.sicherheit-forschung.de/forschungsforum/schriftenreihe_neu/sr_v_v/SchriftenreiheSicherheit_02.pdf (besucht am 26.03.2025).

Birnbacher, Dieter (2012): Vulnerabilität und Patientenautonomie – Anmerkungen aus medizinethischer Sicht. *Medizinrecht*, 9/2012, S. 560–565.

Böhning, Fabiola und Schindler, Stephan (2024): Verbotene Praktiken im KI-Bereich – Wann ist was verboten? *ZD-Aktuell* 2024, 01793.

Brough, Aaron und Kelly, Martin (2020): Critical roles of knowledge and motivation in privacy research. *Current opinion in psychology*, (31), S. 11-15. https://doi.org/10.1016/j.copsyc.2019.06.021.

Bundesregierung (2022): Bericht der Bundesregierung über die Wirkungen der Novellierung des Gesetzes zur Weiterentwicklung des Behindertengleichstellungsrechts. URL: https://www.bmas.de/DE/Service/Presse/Meldungen/2022/bericht-weiterentwicklung-behindertengleichstellungsgesetz.html.

Busch, Dörte (2021): Digitale Teilhabe für Menschen mit Behinderungen nach der UN-Behindertenrechtskonvention. *Zeitschrift für europäisches Sozial- und Arbeitsrecht*, 20(11), S. 484-492.

Calliess, Christian und Ruffert, Matthias (Hrsg.) (2022): *EUV/AEUV*. 6. Auflage. München: Beck.

Chibanguza, Kuuya und Steege, Hans (2024): Die KI-Verordnung – Überblick über den neuen Rechtsrahmen. *Neue Juristische Wochenschrift*, 25/2024, S. 1769-1775.

Damm, Reinhard (2013): Vulnerabilität als Rechtskonzept? *Medizinrecht*, 4/2013, S. 201-214. DOI: 10.1007/s00350-013-3389-1

Deinert, Olaf; Welti, Felix; Luik, Steffen und Brockmann, Judith (Hrsg.) (2022): *Stichwort-Kommentar Behindertenrecht*. 3. Auflage. Baden-Baden: Nomos.

Der Bundesbeauftragte der Bundesregierung für Informationstechnik (BfIT) (29.01.25): Digitale Barrierefreiheit. URL: https://www.barrierefreiheit-dienstekonsolidierung.bund.de/Webs/PB/DE/barrierefreie_it/digitale-barrierefreiheit/digitale-barrierefreiheit-node.html (besucht am 15.02.2025).

Deutsches Institut für Menschenrechte (DIfM) (03.10.2023): UN, Ausschuss für die Rechte von Menschen mit Behinderungen, Abschließende Bemerkungen zum kombinierten zweiten und dritten Staatenbericht Deutschlands, CRPD/C/DEU/CO/2-3. URL: https://www.institut-fuer-menschenrechte.de/fileadmin/Redaktion/Publikationen/Weitere_Publikationen/Abschl.Bemerkungen_Deutsche_UEbersetzung_Entwurf_DIMR_barrierefrei.pdf (besucht am: 15.02.2025).

Drygalski, Clarissa von und Welti, Felix: Erkenntnisse aus der UN-BRK zur geschützten Beschäftigung. In: Schachler, Viviane; Schlummer, Werner und Weber, Roland (Hrsg.): *Zukunft der Werkstätten. Perspektiven für und von Menschen mit Behinderung zwischen Teilhabe-Auftrag und Mindestlohn*. Bad Heilbrunn: Verlag Julius Klinkhardt; Lebenshilfe Verlag der Bundesvereinigung 2023, S. 85-100. URN: urn:nbn:de:0111-pedocs-267656, DOI: 10.25656/01:26765; 10.35468/6002-06.

DSK, Stellungnahme zum Referentenentwurf vom 11.7.2023. https://www.datenschutzkonferenz-online.de/media/st/23-07-11_DSK-Stellungnahme_Einwilligungsverwaltung_TTDSG.pdf.

EDSA (2020): Leitlinien 05/2020 zur Einwilligung gemäß Verordnung 2016/679, Version 1.1, angenommen am 4. Mai 2020. https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_de.pdf.

Ehlen, Theresa und Möllnitz-Dimick, Christina (2023): Datenfinanzierte digitale Produkte: Herausforderungen des „Zahlens“ mit Daten nach dem neuen Verbraucherschutzregime in der Praxis — Ein – nicht abschließender – Überblick über offene Fragen und Risiken und wie mit ihnen in der Beratung umgegangen werden kann. *Computer und Recht*, 7/2023, S. 455-461. https://doi.org/10.9785/cr-2023-390716.

Ehmann, Eugen und Selmayr, Martin (Hrsg.) (2024): DSGVO. 3. Auflage. München: Beck.

Fineman, Martha (2008): The Vulnerable Subject: Anchoring Equality in the Human Condition. *Yale Journal of Law & Feminism*, 20(1), S. 1-23. https://ssrn.com/abstract=1131407.

Fineman, Martha (2017): Vulnerability and Inevitable Inequality. *Oslo Law Review*, 4(3), S. 133-149. https://doi.org/10.18261/issn.2387-3299-2017-03-02.

Fineman, Martha (2019): Vulnerability and Social Justice. 53 *Valparaiso University Law Review*, S. 1-34. https://ssrn.com/abstract=3352825.

Franke, Lucia (2024): Digitale Barrierefreiheit von Produkten und Dienstleistungen. *Zeitschrift für Product Compliance*, 1/2024, S. 21-27.

Franzen, Martin; Gallner, Inken und Oetker, Hartmut (Hrsg.) (2024): *Kommentar zum europäischen Arbeitsrecht*. 5. Auflage. München: Beck.

Friedewald, Michael; Kreutzer, Michael und Hansen, Marit (Hrsg.): Selbstbestimmung, Privatheit und Datenschutz. Wiesbaden: Springer Nature.

Geminn, Christian L. (2021): Die Regulierung Künstlicher Intelligenz, Anmerkungen zum Entwurf eines Artificial Intelligence Act. *Zeitschrift für Datenschutz*, 7/2021, S. 354-359.

Geminn, Christian L. (2023): *Deus ex machina? Grundrechte und Digitalisierung*. Tübingen: Mohr Siebeck.

Geminn, Christian L.; Francis, Leon und Herder Karl-Raban (2021): Die Informationspräsentation im Datenschutzrecht. *ZD-Aktuell,* 05335.

Gluck, Joshua; Schaub, Florian; Friedman, Amy; Habib, Hana; Sadeh, Norman; Cranor, Lorrie-Faith und Agarwal, Yuvraj (2016): How Short is Too Short? Implications of Length and Framing on the Effectiveness of Privacy Notices. *Proceedings of theTwelfth Symposium on Usable Privacy and Security (SOUPS 2016).* URL: https://www.usenix.org/system/files/conference/soups2016/soups2016-paper-gluck.pdf.

Gola, Peter und Heckmann, Dirk (Hrsg.) (2022): *DSGVO/BDSG*. 3. Auflage. München: Beck.

Grabitz, Eberhard; Hilf, Meinhard und Nettesheim, Martin (Hrsg.) (2009): *Das Recht der Europäischen Union*. 40. Auflage, München: Beck.

Gsell, Beate; Krüger, Wolfgang; Lorenz, Stephan und Reymann, Christoph (Hrsg.) (2025): *beck-online.Großkommentar (BeckOGK) BGB*. München: Beck.

Hacker, Philipp und Berz, Amelie (2023): Der AI Act der Europäischen Union – Überblick, Kritik und Ausblick. *Zeitschrift für Rechtspolitik*, 8/2023, S. 226-229.

Hagendorf, Thilo (2018): Übersehene Probleme des Konzepts der Privacy Literacy. In: Roßnagel, Alexander; Friedewald, Michael und Hansen, Marit (Hrsg.): *Die Fortentwicklung des Datenschutzes. Zwischen Systemgestaltung und Selbstregulierung.* Wiesbaden: Springer, S. 99-120.

Han, S. Duke; Boyle, Patricia A; James, Bryan D; Yu, Lei und Bennett, David A (2015): Mild cognitive impairment is associated with poorer decision-making in community-based older persons. *Journal of the American Geriatrics Society*, 63(4), S. 676-683. doi: 10.1111/jgs.13346.

Helberger, Natali; Lynskey, Orla; Micklitz, Hans-W.; Rott, Peter; Sax, Marjin und Strycharz, Joanna (2021): *EU Consumer Protection 2.0 – Structural asymmetries in digital consumer markets*. Brussels: The European Consumer Organisation, URL: https://www.beuc.eu/sites/default/files/publications/beuc-x-2021-018_eu_consumer_protection_2.0.pdf.

Hlava, Daniel (2018): *Barrierefreie Gesundheitsversorgung, Rechtliche Gewährleistung unter besonderer Berücksichtigung der Rechtsdurchsetzung.* Baden-Baden: Nomos.

Hofmann, Franz und Raue, Benjamin (Hrsg.) (2023): *Digital Services Act.* Baden-Baden: Nomos.

Horstmann, Jan (2024): KI-VO und Datenschutz: Überblick und ausgewählte Fragen. *ZD-Aktuell*, 01580.

Kahle, Ute; Schädler, Johannes (Hrsg.) (2025): Digitale Teilhabe und personenzentrierte Technologien im Kontext von Menschen mit Behinderungen, Marburg: Lebenshilfe-Verlag

Kapoor, Arun und Klindt, Thomas (2024): Das Barrierefreiheitsstärkungsgesetz – Anforderungen an Webseiten und mobile Anwendungen. *Neue Juristische Wochenschrift,* 49/2024, S. 3545-3550.

Karaboga, Murat (2022): Datenschutzrechtliche Gestaltungsmöglichkeiten jenseits der Ermächtigung des Individuums: Die Multi-Stakeholder-Datenschutz-Folgenabschätzung. In: Friedewald, Michael; Kreutzer, Michael; Hansen, Marit (Hrsg.): *Selbstbestimmung, Privatheit und Datenschutz*. S. 275-302.

Koch, Heiner; Strathmann, Clara; Hennig, Marti; Schmied, Luisa; Geminn, Christian; Heesen, Jessica; Krämer, Nicole und Reinhardt, Karoline (2025): Diversitätsgerechter Privatheitsschutz in digitalen Umgebungen. In: Friedewald, Michael; Roßnagel, Alexander; Karaboga, Murat; Geminn, Christian (Hrsg.): *Freiheit in digitalen Infrastrukturen*. Im Erscheinen.

Kossens, Michael; Heide, Dirk von der und Maaß, Michael (Hrsg.) (2023): *SGB IX Rehabilitation und Teilhabe Menschen mit Behinderungen mit Behindertengleichstellungsgesetz*. 5. Auflage. München: Beck.

Kreutz, Marcus; Lachwitz, Klaus und Trenk-Hinterberger, Peter (Hrsg.) (2013): *Die UN-Behindertenrechtskonvention in der Praxis Erläuterungen der Regelung und Anwendungsgebiete*. Köln: Luchterhand.

Kroschwald, Steffen (2023): Nutzer-, kontext- und situationsbedingte Vulnerabilität in digitalen Gesellschaften Schutz, Selbstbestimmung und Teilhabe „by Design“ vor dem Hintergrund des Art. 25 DSGVO und dem KI-Verordnungsentwurf. *Zeitschrift für Digitalisierung und Recht*, 1/2023, S. 1-22.

Krüger, Philipp-L. (2016): Datensouveränität und Digitalisierung, Probleme und rechtliche Lösungsansätze. *Zeitschrift für Rechtspolitik*, 7/2016, S. 190-192.

Kruse, Andreas (2017): *Lebensphase hohes Alter: Verletzlichkeit und Reife*. Heidelberg: Springer.

Kühl, Eike (2023): Das Nacktbild, das man nie geschossen hat. *Zeit Online* vom 14. Dezember 2023. URL: https://www.zeit.de/digital/internet/2023-12/deepnudes-nacktbilder-kuenstliche-intelligenz-deepfakes.

Kühling, Jürgen und Buchner, Benedikt (Hrsg.) (2024): *DSGVO – BDSG*. 4. Auflage. München: BECK.

Landesbeauftragte für Datenschutz Niedersachsen, Pressemitteilung 20/2024 vom 27.12.2024. https://www.lfd.niedersachsen.de/startseite/infothek/presseinformationen/verabschiedete-einwilligungsverwaltungsverordnung-verfehlt-ihr-eigentliches-ziel-238383.html.

Lenz, Susanne (2009): *Vulnerabilität kritischer Infrastrukturen. Forschung im Bevölkerungsschutz*. Band 4, Bundesamt für Bevölkerungsschutz und Katastrophenhilfe, Bonn.

Liedke-Deutscher, Bernd (Hrsg.) (2024): *Die datenschutzrechtliche Einwilligung nach der DSGVO*. Oldenburg: OlWIR.

Livingstone, Sonia; Stoilova, Mariya und Nandagiri, Rishita (2019): *Children’s data and privacy online: Growing up in a digital age. An evidence review.* London: London School of Economics and Political Science.

Martini, Mario, Kramme, Inken und Kamke, Anton (2023): KI-VO, DMA und DA als Missing Links im Kampf gegen dunkle Designmuster? Das Digitalpaket der Union und seine vielschichtigen Regelungsansätze gegen Dark Patterns. *Zeitschrift für IT-Recht und Recht der Digitalisierung*, 6/2023, S. 399-403.

Masuch, Peter (20.03.2012): „Die UN- Behindertenrechtskonvention anwenden". *Forum D,* Diskussionsbeitrag Nr. 5 /2012. URL: www.reha-recht.de (besucht am: 15.02.2025).

Menzel, Hans-Joachim (2008): Datenschutzrechtliche Einwilligung. *Datenschutz und Datensicherheit,* 32(6), S. 400-408.

Mozilla Foundation (7. April 2024): EVA AI Chat Bot und Soulmate. URL: https://foundation.mozilla.org/de/privacynotincluded/eva-ai-chat-bot-soulmate/.

Müller-Terpitz, Ralf und Köhler, Markus (Hrsg.) (2024): *Digital Services Act.* München: Beck.

Naguib, Tarek; Pärli, Kurt; Landolt, Hardy; Demir, Eylem und Filippo, Martina (Hrsg.) (2023): *UNO-Behindertenrechtskonvention.* Bern: Stämpfli Verlag AG.

Nebel, Maxi (2015): Schutz der Persönlichkeit – Privatheit oder Selbstbestimmung? Verfassungsrechtliche Zielsetzungen im deutschen und europäischen Recht. *Zeitschrift für Datenschutz*, 11/2015, S. 517-521.

Nebel, Maxi (2022): Alles abwählen: Mit der Einwilligungsverwaltungs-Verordnung gegen den Cookie-Banner-Dschungel. *ZD-Aktuell*, 01321.

Nebel, Maxi (2025): Datenschutzrecht. In: Geminn, Christian L. und Johannes, Paul C. (Hrsg.): *Europäisches Datenrecht*. Baden-Baden: Nomos, im Erscheinen.

Paal, Boris P. und Pauly, Daniel A. (Hrsg.) (2021): *DSGVO/BDSG*. 3. Auflage. München: Beck.

Park, Yong Jin (2013): Digital Literacy and Privacy Behavior Online. *Communication Research,* 40(2), S. 215-236. https://journals.sagepub.com/doi/10.1177/0093650211418338.

Payne, Kate (2024): An AI chatbot pushed a teen to kill himself, a lawsuit against its creator alleges. *Associated Press* vom 24. Oktober 2024. URL: https://apnews.com/article/chatbot-ai-lawsuit-suicide-teen-artificial-intelligence-9d48adc572100822fdbc3c90d1456bd0.

Roller, Steffen (2019): UN-Behindertenrechtskonvention in der sozialgerichtlichen Praxis – anwaltliche Trumpfkarte oder juristische Nebelkerze? *Neue Zeitschrift für Sozialrecht*, 10/2019, S. 368-377.

Roßnagel, Alexander (2020): Der Datenschutz von Kindern in der Datenschutz-Grundverordnung: Vorschläge für die Evaluierung und Fortentwicklung. *Zeitschrift für Datenschutz*, 2/2020, S. 88-92.

Roßnagel, Alexander und Geminn, Christian (2020): *Datenschutz-Grundverordnung verbessern: Änderungsvorschläge aus Verbrauchersicht.* Baden-Baden: Nomos.

Roßnagel, Alexander; Bile, Tamer; Nebel, Maxi; Geminn, Christian; Karaboga, Murat; Ebbers, Frank; Bremert, Benjamin; Stapf, Ingrid; Teebken, Mena; Thürmel, Verena; Ochs, Carsten; Uhlmann, Markus; Krämer, Nicole; Meier, Yannic; Kreutzer, Michael; Schreiber, Linda und Simo, Hervais (2020): *Einwilligung – Möglichkeiten und Fallstricke aus der Konsumentenperspektive* [White Paper]. Forum Privatheit und selbstbestimmtes Leben in der digitalen Welt. Herausgeber: Michael Friedewald, Regina Ammicht Quinn, Marit Hansen, Jessica Heesen, Thomas Hess, Nicole Krämer, Jörn Lamla, Christian Matt, Alexander Roßnagel, Michael Waidner. Karlsruhe: Fraunhofer ISI.

Roßnagel, Alexander; Pfitzmann, Andreas und Garstka, Hansjürgen (2001): Gutachten im Auftrag des Bundesministeriums des Innern. Modernisierung des Datenschutzrechts. Berlin. URL: http://www.datenschutzgeschichte.de/pub/dphistory/2001_GarskaPfitzmannRossnagel_Modernisierung_des_Datenschutzrechts.pdf (besucht am 27.2.2025).

Roßnagel, Alexander; Wedde, Peter; Hammer, Volker und Pordesch, Ulrich (2002/2009): *Die Verletzlichkeit der ‚Informationsgesellschaft'*. 3. Auflage (elektronische Fassung). https://d-nb.info/998894990/34.

Simitis, Spiros (Hrsg.) (2011): Bundesdatenschutzgesetz, 7 Auflage. Baden-Baden: Nomos.

Simitis, Spiros; Hornung, Gerrit und Spiecker gen. Döhmann, Indra (Hrsg.) (2025): *Datenschutzrecht*. 2. Auflage. Baden-Baden: Nomos.

Skjuve, Marita; Følstad, Asbjørn; Fostervold, Knut und Brandtzaeg, Petter (2021): My Chatbot Companion – a Study of Human-Chatbot Relationships. *International Journal of Human-Computer Studies,* 149/2021, 102601. https://doi.org/10.1016/j.ijhcs.2021.102601.

Strauß, Stefan und Bettin, Steffen (2023): Digitalisierung, Vulnerabilität und (kritische) gesellschaftliche Infrastrukturen – Entwicklungsstand, Trends und zentrale Herausforderungen (Projektbericht). Wien: Institut für Technikfolgen-Abschätzung der Österreichischen Akademie der Wissenschaften. URL: https://epub.oeaw.ac.at/0xc1aa5576%200x003e44d2.pdf (besucht am 27.2.2025).

Strauß, Stefan und Krieger-Lamina, Jaro (2017): Digitaler Stillstand: Die Verletzlichkeit der digital vernetzten Gesellschaft – Kritische Infrastrukturen und Systemperspektiven. Wien: Institut für Technikfolgen-Abschätzungen der Österreichischen Akademie der Wissenschaften. URL: https://www.researchgate.net/publication/316487129_Digitaler_Stillstand_Die_Verletzlichkeit_der_digital_vernetzten_Gesellschaft_-_Kritische_Infrastrukturen_und_Systemperspektiven.

Tabbara, Annette (2021): Barrierefreiheit für elektronische Produkte und Dienstleistungen – das Barrierefreiheitsstärkungsgesetz. *Neue Zeitschrift für Sozialrecht*, 13/2021, S. 497-502.

Taeger, Jürgen (2021): Einwilligung von Kindern gegenüber Diensten der Informationsgesellschaft. *Zeitschrift für Datenschutz,* 9/2021, S. 505-508.

Trepte, Sabine; Teutsch, Doris; Masur, Philipp K.; Eicher, Carolin; Fischer, Mona und Hennhöfer, Alisa (2015): Do people know about privacy and data protection strategies? Towards the "Online Privacy Literacy Scale"(OPLIS). In: Gutwirth, Serge; Leenes, Ronald und de Hert, Paul (Hrsg.): *Reforming European data protection law.* Dordrecht: Springer, S. 333-365. https://doi.org/10.1007/978-94-017-9385-8_14.

Turner, B. L.; Kasperson, Roger; Matson, Pamela; McCarthy, James; Corell, Robert; Christensen, Lindsey; Eckley, Noelle; Kasperson, Jeanne; Luers, Amy; Martello, Marybeth; Polsky, Colin; Pulsipher, Alexander und Schiller, Andrew (2003): A framework for vulnerability analysis in sustainability science. *Proceedings of the National Academy of Sciences of the United States of America,* 100(14), S. 8074-8079. https://doi.org/10.1073/pnas.1231335100.

UN (2004): Living with Risk – A global review of disaster reduction initiatives. New York/Genf: United Nations. URL: https://www.unisdr.org/files/657_lwr1.pdf (besucht am 26.03.2025).

Uziel-Karl, Sigal und Tenne-Rinde, Michal (2018): Making language accessible for people with cognitive disabilities: Intellectual disability as a test case. In: Bar-On, Amalia und Dorit, Ravid (Hrsg.): *Handbook of Communication Disorders Theoretical, Empirical, and Applied Linguistic Perspectives.* Boston/Berlin: Walter de Gruyter Inc, S. 845-862.

Von Boetticher, Arne und Kuhn-Zuber, Gabriele (2021): *Rehabilitationsrecht ein Studienbuch für soziale Berufe*. 2. Auflage, Baden-Baden: Nomos.

Wehde, Alexander (2023): Regulierung von Large Language Models in DSA und AIA-E. *MMR-Aktuell*, 455171.

Wolff, Heinrich A.; Brink, Stefan und v. Ungern-Sternberg, Antje (Hrsg.) (2023): *BeckOK Datenschutzrecht*. 51. Edition. München: Beck.