

Lukas Naegeli, Johanna Sinn, Karoline Reinhardt, Christian Geminn, Jessica Heesen, Martin Hennig, Luisa Schmied, Clara Strathmann, Nicole Krämer

DIVERSITÄTSGERECHTER PRIVATHEITSSCHUTZ

EMPFEHLUNGEN ZUM SCHUTZ DER PRIVATHEIT VULNERABLER GRUPPEN IN DIGITALEN UMGEBUNGEN

Policy Paper

Impressum

Forschungsberichte der Plattform Privatheit Nr. 7

Herausgeber

Plattform Privatheit

Michael Friedewald¹, Alexander Roßnagel^{2,3}, Christian Geminn², Murat Karaboga¹

- (1) Fraunhofer-Institut für System- und Innovationsforschung ISI, Karlsruhe
- (2) Universität Kassel, Projektgruppe verfassungsverträgliche Technikgestaltung (provet) im Wissenschaftlichen Zentrum für Informationstechnik-Gestaltung (ITeG)
- (3) Hessischer Beauftragter für Datenschutz und Informationsfreiheit, Wiesbaden

Autorinnen und Autoren

Lukas Naegeli¹, Johanna Sinn¹, Karoline Reinhardt¹, Christian Geminn², Jessica Heesen³, Martin Hennig³, Luisa Schmied², Clara Strathmann⁴, Nicole Krämer⁴

- (1) Universität Passau, Fachbereich Philosophie: Angewandte Ethik
- (2) Universität Kassel, Wissenschaftliches Zentrum für Informationstechnik-Gestaltung (ITeG), Fachgebiet Öffentliches Recht, IT-Recht und Umweltrecht
- (3) Universität Tübingen, Internationales Zentrum für Ethik in den Wissenschaften (IZEW), Forschungsgruppe Medienethik, Technikphilosophie & KI
- (4) Universität Duisburg-Essen, Fachgebiet Sozialpsychologie: Medien und Kommunikation

Reihe

ISSN (Print)	2199-8874
ISSN (Online)	2199-8882
DOI	https://doi.org/10.24406/publica-7592

Veröffentlichung

März 2026, 1. Auflage
Fraunhofer-Institut für System- und Innovationsforschung ISI, Karlsruhe

Zitierempfehlung

Naegeli et al. (2026): Diversitätsgerechter Privatheitsschutz. Empfehlungen zum Schutz der Privatheit vulnerabler Gruppen in digitalen Umgebungen. Forschungsberichte der Plattform Privatheit, Nr. 7, hrsg. v. Friedewald et al. Karlsruhe: Fraunhofer ISI.

Hinweise

Dieses Werk ist lizenziert unter einer Creative Commons Namensnennung – Nicht kommerziell – Keine Bearbeitungen 4.0 International Lizenz.

Die Informationen wurden nach bestem Wissen und Gewissen unter Beachtung der Grundsätze guter wissenschaftlicher Praxis zusammengestellt. Die Autorinnen und Autoren gehen davon aus, dass die Angaben in diesem Bericht korrekt, vollständig und aktuell sind, übernehmen jedoch für etwaige Fehler, ausdrücklich oder implizit, keine Gewähr. Die Darstellungen in diesem Dokument spiegeln nicht notwendigerweise die Meinung des Auftraggebers wider.



Inhaltsverzeichnis

1	Einleitung	4
2	Grenzen des Paradigmas der informierten Einwilligung	6
3	Grundlagen des diversitätsgerechten Privatheitsschutzes.....	9
4	Wie kann Privatheit diversitätsgerecht geschützt werden?	13
5	Empfehlungen für Benutzeroberflächendesign, Rechtsfortentwicklung und Wissenschaftskommunikation.....	16
6	Fazit	19
7	Literaturverzeichnis	20

1 Einleitung

„**Accept all cookies**“ – ein Klick, oft beiläufig, manchmal genervt, meist unter Zeitdruck. Kaum eine Interaktion steht sinnbildlicher für den alltäglichen Umgang mit Privatheit im Internet als unser Umgang mit Cookie-Einstellungen. Was als scheinbar harmlose Zustimmung erscheint, markiert in vielen Fällen den Eintritt in komplexe Datenökosysteme, in denen persönliche Informationen gesammelt, ausgewertet und weiterverarbeitet werden. Der Schutz der eigenen Privatheit wird dabei nicht bewusst ausgehandelt, sondern in routinisierten Entscheidungssituationen an voreingestellte Optionen delegiert, vor dem Hintergrund unübersichtlicher Informationslagen und asymmetrischer Machtverhältnisse zwischen Nutzenden und Anbietenden.

Privatheitsschutz ist ein Thema, das alle Menschen betrifft, online und offline. Dabei sind Menschen jedoch unterschiedlich anfällig für Privatheitsverletzungen, und diese Verletzungen können unterschiedlich folgenreich und folgenschwer sein. Diese Ungleichheiten können sowohl auf strukturelle Bedingungen zurückgeführt werden (etwa auf bestehende Diskriminierungsstrukturen oder ungleichen Zugang zu Ressourcen) als auch sehr individuelle Gründe haben, die insbesondere mit situations- und kontextabhängigem Nutzungsverhalten (etwa der Häufigkeit und Art der Internetnutzung) zusammenhängen (vgl. Kroschwald 2023, S. 5). Vor diesem Hintergrund wird deutlich: Privatheitsschutz im Internet ist nicht nur eine Frage individueller Verantwortung, sondern eine zentrale gesellschafts- und ordnungspolitische Herausforderung.

Im Zeitalter digital geprägter Gesellschaften steht der Privatheitsschutz vor besonderen Herausforderungen. Viele Prozesse und Infrastrukturen der Datenerhebung und -verarbeitung sind höchst komplex und abstrakt. Dies gilt beispielsweise für Cloudinfrastrukturen, die für die Speicherung und Analyse personenbezogener Daten zunehmend an Bedeutung gewinnen, sich dynamisch entwickeln und für Nutzende nur begrenzt überschaubar sind. Die Funktionsweise solcher Systeme ist in der Regel kaum nachvollziehbar und lässt sich nur eingeschränkt mit dem eigenen Handeln in digitalen Kontexten in Beziehung setzen. Für bereits vorhandene datenschutzrechtliche Bestimmungen bedeutet dies, dass ihre praktische Wirksamkeit begrenzt bleibt und sie entsprechend weiterzuentwickeln sind – insbesondere im Hinblick auf Personen mit erhöhter Vulnerabilität.

Vorhandene Instrumente zum Schutz vulnerabler Gruppen – etwa der auf Kinder bezogene Art. 8 der Datenschutz-Grundverordnung (DSGVO) – greifen häufig zu kurz, da sie keinen umfassenden und situationsübergreifenden Schutz gewährleisten (vgl. Roßnagel 2020, S. 88; Roßnagel/Geminn 2020, S. 55 ff.; Geminn 2023, S. 193 ff.). Darüber hinaus besteht Bedarf an einer angemessenen Berücksichtigung von Vulnerabilitäten unterschiedlicher Personengruppen, etwa älterer Menschen oder Personen mit kognitiven Beeinträchtigungen (vgl. Geminn 2023, S. 203 ff.). Der klassische Diskriminierungsschutz, der auf abschließenden Merkmalslisten beruht, reicht hierfür nicht aus. Er erkennt, dass Vulnerabilität kein statisches Personenmerkmal ist, sondern kontextabhängig entsteht und sich je nach technischer, sozialer und institutioneller Umgebung unterschiedlich ausprägt. Erforderlich ist daher eine Diversitätsperspektive, die Schutzbedarfe nicht allein anhand formaler Gruppenzugehörigkeiten bestimmt, sondern anhand konkreter, situativer Vulnerabilitäten im jeweiligen Gegenstandsbereich. Für den Bereich der Privatheit bedeutet dies, dass regulatorische Vorgaben stärker an tatsächliche Fähigkeiten, Ressourcen und Risiken der betroffenen Personen anknüpfen müssen. Ziel muss es sein, unterschiedlichen Formen der Vulnerabilität im Bereich der Privatheit diversitätsgerecht Rechnung zu tragen. Dies entspricht einer gerechtigkeitsorientierten Perspektive auf den Privatheitsschutz, der als grundrechtlich verankertes, gesamtgesellschaftliches Anliegen zu verstehen ist und nicht in der individuellen Disposition der Betroffenen aufgeht. Die informationelle Selbstbestimmung bildet eine zentrale Voraussetzung der demokratischen Ordnung.

Ein solcher Ansatz ermöglicht es, den Privatheitsschutz feinkörnig auf verschiedene Fähigkeiten und Schutzbedarfe abzustimmen. Dadurch wird nicht nur der Schutz besonders vulnerabler Personen

gestärkt, sondern auch das allgemeine Schutzniveau erhöht – denn Menschen sind ganz allgemein in sehr unterschiedlichem Maße dazu in der Lage, ihre Privatsphäre eigenständig zu schützen. Während einige gut darüber informiert sind, welche personenbezogenen Daten sie preisgeben, ist anderen kaum bewusst, dass überhaupt Informationen über sie erhoben und verarbeitet werden. Ein diversitätssensibler Privatheitsschutz trägt dieser Realität Rechnung und adressiert strukturelle Schutzdefizite, die sich aus Informationsasymmetrien, komplexen technologischen Verarbeitungsvorgängen und durch aus verschiedenen Gründen eingeschränkte Handlungsmöglichkeiten ergeben.

Dies wird besonders deutlich am Beispiel von Kindern sowie von Menschen mit kognitiven Beeinträchtigungen. Für sie sind digitale Einwilligungssituationen wie Cookie-Banner, Datenschutzbestimmungen oder personalisierte Einstellungen häufig kaum verständlich und praktisch nicht selbstbestimmt zu bewältigen (vgl. Chalghoumi et al. 2019; Wang et al. 2022). Zugleich sind sie in besonderem Maße darauf angewiesen, dass ihre Daten nicht missbräuchlich genutzt oder in Kontexte überführt werden, die sie weder überblicken noch kontrollieren können. Privatheitsverletzungen können hier langfristige Folgen haben – etwa durch frühe Profilbildung, Stigmatisierung oder eingeschränkte Teilhabemöglichkeiten – und wirken oft weit über den Moment der Datenerhebung hinaus. Der Privatheitsschutz wird damit auch zu einer Frage des besonderen Schutzbedarfs vulnerabler Gruppen, denn bestehende digitale Entscheidungsarchitekturen sind nicht für alle Menschen gleichermaßen zugänglich, verständlich oder fair ausgestaltet.

Betrachtet man den Privatheitsschutz unter Gerechtigkeitsaspekten, muss der Einbezug marginalisierter und/oder vulnerabler Bevölkerungsgruppen zu einem zentralen Anliegen werden (vgl. Castro Varela/Heinemann 2016). Diese Gruppen haben oft weniger Einfluss auf politische Debatten und gesellschaftliche Gestaltungsprozesse, wodurch ihre spezifischen Schutzbedarfe systematisch unterrepräsentiert bleiben. Der Privatheitsschutz ist dabei nicht nur als ein individuell unterschiedlich ausgeprägtes Interesse zu verstehen, sondern stellt von vornherein ein gesamtgesellschaftliches Anliegen dar: Die Wahrung der informationellen Selbstbestimmung ist aus demokratietheoretischer Sicht selbst dann zentral, wenn Einzelne ihre personenbezogenen Daten nicht schützen wollen oder können. So schützt sie etwa vor totalitären Strukturen (vgl. Rössler 2001) und gehört damit zu den grundlegenden Voraussetzungen einer funktionierenden Demokratie.

Dieses im Rahmen des Forschungsprojekts „DiversPrivat – Diversitätsgerechter Privatheitsschutz in digitalen Umgebungen“ erarbeitete Policy Paper enthält erste Vorschläge dazu, wie sich Privatheit diversitätsgerecht schützen lässt (vgl. auch Koch et al. 2025). Im Vordergrund steht dabei die Orientierung an vielfältigen und kontextabhängigen Vulnerabilitäten, aus denen sich jeweils spezifische Schutzbedarfe ergeben. Zunächst wird aufgezeigt, inwiefern ein Modell des Privatheitsschutzes, das primär auf individuellen Einwilligungen beruht, in digitalen Umgebungen an seine Grenzen stößt (Abschnitt 2). Anschließend wird dargelegt, warum nur ein diversitätsgerechter Privatheitsschutz ein angemessenes Schutzniveau für alle Nutzenden gewährleisten kann (Abschnitt 3). Darauf aufbauend werden konzeptionelle und ethische Empfehlungen zur diversitätsgerechten Ausgestaltung des Privatheitsschutzes entwickelt (Abschnitt 4). Vor diesem Hintergrund werden schließlich Empfehlungen zum Design von Benutzeroberflächen, zur Fortentwicklung des rechtlichen Rahmens sowie zur Wissenschaftskommunikation unterbreitet (Abschnitt 5).

2 Grenzen des Paradigmas der informierten Einwilligung

In digital geprägten Gesellschaften werden personenbezogene Daten in vielfältigen Kontexten erhoben und genutzt, etwa durch staatliche Behörden, internationale Organisationen oder private Akteure. So erheben Technologieunternehmen beispielsweise Daten, um Informationen über die Nutzung ihrer Produkte zu erhalten und das Verhalten von Kundinnen und Kunden durch personalisierte Werbung gezielt zu beeinflussen. Eine Einwilligung wird dabei häufig als ausreichende Rechtfertigung für die Verarbeitung personenbezogener Daten betrachtet: Sofern Nutzende – so die verbreitete Auffassung – einwilligen, dass ihre Daten erfasst werden, bleibt ihre informationelle Selbstbestimmung gewahrt und Unternehmen sind berechtigt, diese Daten zu verwenden. Auf dieser Grundlage können Konzerne wie Alphabet (Google) oder Meta (Instagram, Facebook, WhatsApp) auf enorme Datenmengen zugreifen und diese für eine Vielzahl kommerzieller Zwecke nutzen. Zunehmend gewinnen auch interaktive KI-Systeme und Chatbots als neue Wege der Datenerhebung an Bedeutung: In der Kommunikation mit Chatbots geben Nutzende häufig umfangreiche, teils hochsensible Informationen preis – etwa zu persönlichen Lebensumständen, gesundheitlichen Fragen oder beruflichen Herausforderungen. Anders als bei klassischen digitalen Diensten erfolgt diese Datenweitergabe oft in dialogischer Form und in einer Situation, die Nähe, Vertraulichkeit oder Unterstützung suggeriert. Dies kann dazu führen, dass Nutzende die Tragweite ihrer Angaben, die möglichen Weiterverwendungen der Daten sowie bestehende Macht- und Informationsasymmetrien noch stärker unterschätzen (vgl. Geminn et al. 2026).

Insbesondere mit Blick auf die Anforderungen des Privatheitsschutzes vulnerabler Personen zeigt sich daher, dass die etablierte Praxis, die Einwilligung von Nutzenden als datenschutzrechtliche Legitimationsgrundlage heranzuziehen, kritisch hinterfragt werden muss, da Personen die Risiken für Privatheitsverletzungen in solchen Kontexten oft nicht mehr einschätzen können oder ihnen bestimmte Anwendungen und Dienstleistungen nicht zur Verfügung stehen, wenn sie die bestehenden Risiken nicht hinnehmen. Außerdem unterscheiden sich Menschen erheblich darin, in welchem Maße sie Risiken einschätzen und kontrollieren können, sowie darin, wie gravierend sich Privatheitsverletzungen für sie auswirken. Entsprechend wird in der Folge zunächst skizziert, wie der Privatheitsschutz auf der Basis individueller Einwilligungen konzipiert wird, und anschließend gezeigt, weshalb dieses Modell im digitalen Zeitalter an seine Grenzen stößt (vgl. Koch et al. 2025, S. 224 ff.).

Die Einwilligung wird im Datenschutzrecht traditionell als „genuiner Ausdruck der informationellen Selbstbestimmung“ (Roßnagel et al. 2001, S. 15; zur Ethik der Einwilligung vgl. Miller/Wertheimer 2009; Müller/Schaber 2018; Kiener 2023) verstanden. Sie gilt als zentrales Instrument, mit dem Individuen autonom über die Weitergabe personenbezogener Daten entscheiden können. Dies wird bereits im Volkszählungsurteil des deutschen Bundesverfassungsgerichts aus dem Jahr 1983 deutlich, in dem Einzelpersonen zugestanden wird, „selbst über die Preisgabe und Verwendung [ihrer] persönlichen Daten zu bestimmen“ (BVerfGE 65, 1, Rn. 74). Ähnlich verhält es sich in der Grundrechtscharta der Europäischen Union (GRCh), die ebenfalls ein Recht auf informationelle Selbstbestimmung anerkennt (vgl. Kühling/Buchner, in: Kühling/Buchner 2024; Liedke-Deutscher 2024, S. 8; Nebel 2015, S. 517 ff.). Liegt demnach eine auf einer autonomen Entscheidung beruhende Einwilligung in die Verarbeitung persönlicher Daten vor, so steht diese mit den Grundrechten der EU-Charta in Einklang (vgl. Art. 8 Abs. 2 DSGVO; vgl. dazu etwa Liedke-Deutscher 2024, S. 8).

Für eine wirksame Einwilligung müssen jedoch, wie in der Datenschutz-Grundverordnung konkretisiert wird (Art. 4 Nr. 11 DSGVO), unter anderem die Voraussetzungen der Freiwilligkeit und Informiertheit erfüllt sein. Betroffene Personen dürfen nicht dazu gezwungen werden, in etwas einzuwilligen, was sie nicht wollen, und sie müssen verstehen, dass und wozu sie ihre Einwilligung erteilen. Nur unter diesen Bedingungen sind sie in der Lage, von ihrem Recht Gebrauch zu machen, die Einwilligung zu verweigern oder gegebenenfalls zu widerrufen. Die Gewährleistung dieser

Voraussetzungen obliegt den Verantwortlichen und ist durch geeignete Vorkehrungen sicherzustellen (vgl. ErwG 42 Satz 2 DSGVO).

Informierte Einwilligung liegt nur vor, wenn ein hinreichendes Verständnis aller relevanten Informationen gegeben ist, sodass die einwilligende Person die damit verbundenen Konsequenzen abschätzen kann.

Informationelle Selbstbestimmung ist damit nur unter Bedingungen hinreichender Transparenz sinnvoll ausübbar: Personenbezogene Daten müssen in einer „für die betroffene Person nachvollziehbaren Weise“ verarbeitet werden (Art 5. Abs. 1 lit. a DSGVO). Entsprechend sind Verantwortliche gehalten, „geeignete Maßnahmen“ zu treffen, um den Personen, deren Daten verarbeitet werden, sämtliche relevanten Informationen „in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache zu übermitteln“ (Art. 12 Abs. 1 S. 1 DSGVO). Dabei beschränkt sich dieses Transparenzgebot nicht nur auf formale Verständlichkeit im Sinne bloßer Lesbarkeit, sondern umfasst auch die Anforderung inhaltlicher Verständlichkeit.

Wie lässt sich der Privatheitsschutz demzufolge auf der Grundlage individueller informierter Einwilligungen konzipieren? Die Datenschutz-Grundverordnung folgt einem implizit auf *Privacy Literacy* ausgerichteten Ansatz, der davon ausgeht, dass durch Transparenz und die Eigenverantwortung der betroffenen Person eine wirksame Einwilligung in die Verarbeitung personenbezogener Daten gewährleistet werden kann (vgl. Roßnagel et al. 2020, S. 7). Bei der Beurteilung, welche Maßnahmen zum Privatheitsschutz ergriffen werden sollten, können sich die Verantwortlichen entsprechend an „Durchschnittsnutzenden“ und deren *Privacy Literacy* orientieren.

Privacy Literacy meint die Datenschutzkompetenz, die erforderlich ist, um Entscheidungen bezüglich der Weitergabe und Verarbeitung personenbezogener Daten informiert treffen zu können. Dazu gehören sowohl spezifische Kenntnisse (z. B. zum Zweck der Erfassung von Daten, zu rechtlichen Rahmenbedingungen und möglichen Schutzmaßnahmen) als auch verschiedene Fähigkeiten im Umgang mit Daten (z. B. der Folgen- und Risikoabschätzung, der Beurteilung der Schutzwürdigkeit sensibler Daten oder der Reflexion von Machtverhältnissen; vgl. Grimm/Krah 2016, 184 f.).

„Durchschnittsnutzende“ bringen nach dieser Konzeption spezifische Kenntnisse und Fähigkeiten mit, um informierte Datenschutzentscheidungen zu treffen. Die ihnen zugeschriebene *Privacy Literacy* umfasst verschiedene Dimensionen: von prozeduralem Wissen (z. B. zu Selbstschutzmaßnahmen und privatheitsbewahrenden Kommunikationsmitteln) über Erfahrungswissen (z. B. zu persönlichen Erlebnissen mit Privatheitsverletzungen) bis hin zu Faktenwissen über gesetzliche Rahmenbedingungen, technische Datenschutzmaßnahmen und Praktiken von datensammelnden Unternehmen (vgl. Trepte et al. 2015; Grimm/Krah 2016; Brough/Martin 2020; Koch et al. 2025). Auf dieser Grundlage können „Durchschnittsnutzende“, sofern die Datenerfassung und -verarbeitung ihnen gegenüber transparent gemacht wird, ihre Privatsphäre eigenverantwortlich schützen. Dem *Privacy Literacy*-Ansatz zufolge genügt es daher, wenn (i) das Transparenzgebot eingehalten und (ii), falls nötig, die *Privacy Literacy* der Nutzenden gestärkt wird, indem ihnen entsprechende Bildungsangebote gemacht werden.

Auf diese Weise lässt sich jedoch kein durchgehend angemessenes Schutzniveau sicherstellen (vgl. Koch et al. 2025, S. 226 f.). Gerade für vulnerable Personengruppen – etwa Menschen mit kognitiven Beeinträchtigungen – sind die Voraussetzungen, um informierte Entscheidungen über die Weitergabe personenbezogener Daten zu treffen, häufig nicht gegeben (vgl. Behrendt/Loh 2022; Geminn 2023). Der *Privacy Literacy*-Ansatz erweist sich insofern als unzureichend, als er davon ausgeht, dass Nutzende in vergleichbarem Maße über die erforderlichen Kompetenzen verfügen, um sich eigenständig zu informieren. Dabei verkennt diese Diagnose, dass die Informiertheit individueller

Einwilligungen nicht allein von vermittelbaren Kenntnissen und Fähigkeiten abhängt, sondern auch maßgeblich durch verfügbare Ressourcen geprägt ist. Ob Personen dazu in der Lage sind, die komplexen Mechanismen der digitalen Ökonomie zu verstehen und ihr Handeln danach auszurichten, hängt unter anderem von zeitlichen, finanziellen, kognitiven und erfahrungsbezogenen Voraussetzungen ab (vgl. Eubanks 2018; Brough/Martin 2020; Smahel et al. 2020; Masur 2020; Wiesemann et al. 2020; Sindermann et al. 2021). Datenschutzrechtliche Selbstbestimmung darf jedoch nicht an individuelle Kenntnisse oder günstige soziale, finanzielle und technische Bedingungen gebunden sein. Sie muss allen Menschen offenstehen, unabhängig von ihren persönlichen Fähigkeiten, ihrem sozioökonomischen Hintergrund oder der digitalen Umgebung, in der sie sich bewegen. Entsprechend darf sie nicht nur denjenigen vorbehalten bleiben, die faktisch dazu in der Lage sind, komplexe Datenschutzhinweise zu erfassen oder Datenschutzeinstellungen an individuelle Präferenzen anzupassen.

Zudem rückt der *Privacy Literacy*-Ansatz durch seine starke Fokussierung auf die Verantwortung einzelner Nutzenden die strukturelle und institutionelle Dimension des Privatheitsschutzes in den Hintergrund (vgl. Hagendorff 2018). Digitale Dienste sind häufig so gestaltet, dass die Weitergabe personenbezogener Daten standardmäßig erleichtert wird, während datenschutzfreundliche Handlungsoptionen mit zusätzlichem Aufwand verbunden sind. Systemische Problemlagen dieser Art lassen sich nicht durch individuelle Kompetenzvermittlung bewältigen. Um ein ausreichendes Schutzniveau zu erreichen, sind ergänzende Maßnahmen erforderlich, die etwa regulatorische Vorgaben oder weniger kognitiv voraussetzungsreiche Schutzmechanismen einschließen.

Daneben können Bildungsangebote in der Gesellschaft zwar durchaus einen kompetenteren Umgang mit digitalen Diensten und Plattformen fördern. Doch stößt dieser Ansatz für verschiedene Bevölkerungsgruppen an Grenzen. Nicht alle Menschen lassen sich in gleicher Weise erreichen und manche haben spezielle Bedürfnisse, denen durch standardisierte Vorkehrungen nur begrenzt Rechnung getragen werden kann. Die Ursachen dafür, dass Datenschutzentscheidungen häufig nicht auf informierter Grundlage getroffen werden, sind ebenso vielfältig wie Formen der Vulnerabilität, denen betroffene Personen ausgesetzt sind. Vor diesem Hintergrund ist aus einer Diversitätsperspektive sorgfältig zu prüfen, wo Schutzdefizite vorhanden sind, und welche ergänzenden Maßnahmen benötigt werden, um diese zu schließen. Ein Ansatz, der lediglich auf die Stärkung der *Privacy Literacy* von „Durchschnittsnutzenden“ setzt, verfehlt dieses Ziel und kann kein umfassendes und gerechtes Schutzniveau für alle gewährleisten.

3 Grundlagen des diversitätsgerechten Privatheitsschutzes

Wenn der Privatheitsschutz für alle Nutzenden angemessen sein soll, ist zu berücksichtigen, wie vielfältig Vulnerabilitäten in digital geprägten Gesellschaften beschaffen sein können. Zunächst bestehen Vulnerabilitäten, die allen Menschen in digitalen Umgebungen gemeinsam sind, etwa durch intransparente Datenverarbeitung, komplexe KI-gestützte Entscheidungsprozesse oder weitreichende Verknüpfungen personenbezogener Daten, deren Risiken auch bei grundsätzlich informierten und handlungsfähigen Nutzenden nur begrenzt kontrollierbar sind. Hinzu kommen Vulnerabilitäten, die unterschiedlichen Menschen in unterschiedlichem Maß zu eigen sind. So können Menschen etwa aufgrund struktureller Benachteiligungen besonders schutzbedürftig sein, etwa Angehörige marginalisierter Gruppen, die einem erhöhten Risiko von Überwachung, Profilbildung oder diskriminierenden Datennutzungen ausgesetzt sind. Andere weisen spezifische Schutzbedarfe auf, die aus individuellen Merkmalen resultieren, etwa eingeschränkten kognitiven oder sprachlichen Fähigkeiten oder gesundheitlichen Beeinträchtigungen, die es erschweren, datenverarbeitende Praktiken zu verstehen oder informierte Entscheidungen zu treffen. Im Lichte dieser vielfältigen Formen von Vulnerabilität wird deutlich, dass der Privatheitsschutz diversitätsgerecht gestaltet werden sollte. Spezifischen Vulnerabilitäten ist Rechnung zu tragen, indem relevante Dimensionen gesellschaftlicher Diversität herangezogen werden, um vorhandene Schutzdefizite zu ermitteln und geeignete Maßnahmen abzuleiten. Nur ein diversitätsgerechter Privatheitsschutz bietet ein angemessenes Schutzniveau für alle Nutzenden, deren Schutzbedarfe sich je nach sozialen Umständen, individuellen Voraussetzungen oder Kontexten der Datenerfassung erheblich unterscheiden können. Bevor im vierten Abschnitt konzeptionelle und ethische Empfehlungen formuliert werden, ist zunächst grundlegend zu klären, was diversitätsgerechter Privatheitsschutz bedeutet und wie die Begriffe der Vulnerabilität, der Intersektionalität und der Diversität im vorliegenden Zusammenhang zu verstehen sind.

Vulnerabilität

Während im Privatheitsbereich eine gewisse Vulnerabilität von allen Nutzenden digitaler Technologien geteilt wird, bestehen zugleich große Unterschiede darin, wie ausgeprägt diese Vulnerabilität ist (vgl. Koch et al. 2025, S. 232). Sowohl einzelne Personen als auch verschiedene Personengruppen können (i) in unterschiedlichen Hinsichten und (ii) in mehr oder weniger erhöhtem Maße vulnerabel sein. So kann freilich eine ungleiche gesellschaftliche Verteilung von *Privacy Literacy* dazu führen, dass verschiedene Personengruppen nicht gleichermaßen dazu in der Lage sind, ihre Privatsphäre zu schützen. Viel entscheidender ist aber, dass identische Eingriffe in die informationelle Selbstbestimmung für verschiedene Personen sehr unterschiedliche Folgen haben können. So wiegt es oft erheblich schwerer, wenn sensible Gesundheitsdaten einer erkrankten Person offengelegt werden, als wenn vergleichbare Informationen eine gesunde Person betreffen. Zudem kommt es häufig vor, dass Personen unterschiedlich stark gefährdet sind, durch Privatheitsverletzungen geschädigt zu werden – beispielsweise, wenn Standort- oder Kommunikationsdaten von politisch aktiven Personen, Journalist:innen oder Angehörigen diskriminierter Minderheiten bekannt werden und dadurch Risiken von Repression, Stigmatisierung oder sozialer Ausgrenzung entstehen.

Vulnerabilität liegt im Privatheitsbereich vor, wenn Menschen anfällig sind für datenschutzrelevante Eingriffe, die ihre informationelle Selbstbestimmung beeinträchtigen und mit Schäden oder Risiken einhergehen, denen sie nur begrenzt selbst begegnen können.

Ein Privatheitsschutz, der ein angemessenes Schutzniveau für alle gewährleisten soll, ist darauf abzustimmen, welche Vulnerabilitäten in digital geprägten Gesellschaften universell vorhanden sind und welche bestimmten Personen oder Personengruppen in besonderem Maße zukommen. Beide

Dimensionen sind relevant, um bestehende Schutzbedarfe zu identifizieren und zu prüfen, welche Maßnahmen zum Schutz der Privatheit ergriffen werden sollten. Es darf weder ausgeblendet werden, dass alle Menschen bis zu einem gewissen Grad vulnerabel sind, noch kann davon ausgegangen werden, dass reine Gleichbehandlung ausreicht, um angemessen auf Vulnerabilitäten zu reagieren (vgl. Fineman 2008; Fineman 2017). Stattdessen ist ein Ansatz zu verfolgen, der Schutzmechanismen vorsieht, welche sowohl der allgemein geteilten Vulnerabilität als auch jeweils spezifischen und kontextabhängigen Schwachstellen Rechnung tragen.

Welche Anhaltspunkte lassen sich aber heranziehen, um Personen mit besonderer Vulnerabilität zu erfassen? In der bisherigen Diskussion wurde etwa auf einzelne soziale Kategorien wie Geschlecht, Klasse, Herkunft, Alter oder „race“ verwiesen, die aus dem Diskriminierungsdiskurs bekannt sind (vgl. Art. 21 GRCh, Art. 3 Abs. 3 GG; § 1 Allgemeines Gleichbehandlungsgesetz). Dies ist im vorliegenden Kontext allerdings aus mehreren Gründen problematisch (vgl. Luna 2009, S. 124 f.; Martin 2023, S. 23; Koch et al. 2025, S. 234 f.). Die genannten Kategorien sind in vielen Fällen zu grob, um die tatsächlichen Unterschiede in der Verwundbarkeit verschiedener Personen angemessen abzubilden. Dadurch kann es passieren, dass bei manchen Menschen übersehen wird, wie vulnerabel sie eigentlich sind, während andere aufgrund bestimmter Merkmale pauschal als vulnerabel eingestuft werden (vgl. Birnbacher 2012; Damm 2013). Politisch engagierte Personen sind in autoritären Regimen beispielsweise besonders gefährdet, was ihre informationelle Selbstbestimmung betrifft, obwohl sie gegebenenfalls nicht durch klassische Diskriminierungskategorien erfasst werden. Umgekehrt können Menschen mit Lernschwierigkeiten durchschnittlich eine erhöhte Vulnerabilität im Bereich der Privatheit aufweisen, ohne dass dies aber auf alle Einzelpersonen dieser Gruppe zutreffen muss. Abhängig von individuellen Ressourcen – etwa Bildung oder Unterstützung – können manche gleichwohl in der Lage sein, privatheitsbezogene Risiken ebenso gut zu bewältigen wie andere.

Intersektionalität

Der Begriff der Intersektionalität geht auf Arbeiten der US-amerikanischen Rechtswissenschaftlerin Kimberlé Crenshaw zurück und bezeichnet einen analytischen Ansatz, der darauf abzielt, Überschneidungen und Zusammenwirken verschiedener sozialer Kategorien und Machtverhältnisse sichtbar zu machen. Intersektionale Ansätze ermöglichen ein differenzierteres Verständnis der sozialen Wirklichkeit, indem sie Wechselwirkungen zwischen verschiedenen sozialen Kategorien beleuchten (vgl. Crenshaw 1989; Collins/Bilge 2016; Hancock 2016; Collins 2019).

Intersektionalität meint, dass unterschiedliche soziale Kategorien und entsprechende Machtverhältnisse nicht isoliert wirken, sondern sich überlagern und in ihrer Kombination eigene Formen der Vulnerabilität hervorbringen.

Soziale Kategorien wie Geschlecht, Klasse und Alter überschneiden sich und können in ihrer Kombination spezifische Formen der Vulnerabilität erzeugen. Linabary und Corple (2019) verdeutlichen dies am Beispiel von Online-Belästigungen im Umfeld der Plattform Wikipedia, auf der Nutzende Inhalte bearbeiten können und diese Bearbeitungen von anderen kommentiert werden: Die Erfahrungen von Frauen unterscheiden sich dort erheblich – je nachdem, wie Geschlecht mit weiteren sozialen Merkmalen und Machtverhältnissen zusammenwirkt. Zugleich orientieren sich auch intersektionale Ansätze häufig an etablierten Diskriminierungskategorien und deren Kombinationen. Die verwendeten Kategorien werden nicht aus spezifischen Vulnerabilitäten im Bereich der Privatheit entwickelt, sondern aus allgemeinen gesellschaftlichen Benachteiligungslagen abgeleitet. Entsprechend stoßen auch herkömmliche intersektionale Ansätze an Grenzen, wenn es darum geht, die Vielfalt der Vulnerabilitäten im Privatheitskontext angemessen abzubilden.

Diversitätsdimensionen

Anstelle starr festgelegter Diskriminierungskategorien empfiehlt es sich, den offeneren Begriff der Diversität zu verwenden (vgl. Koch et al. 2025, S. 235 f.). Dieser eröffnet die Möglichkeit, relevante Kategorien erst im Rückgriff auf Vulnerabilitäten im Bereich der Privatheit zu entwickeln.

Diversität erfasst die Vielfalt relevanter Unterschiede zwischen Personen und Personengruppen, die in Verbindung mit den jeweiligen soziotechnischen Rahmenbedingungen zu unterschiedlich ausgeprägten Vulnerabilitäten im Privatheitsbereich führen.

Verschiedene Personen und Personengruppen können sich auf vielfältige Weise so voneinander unterscheiden, dass sie unter bestimmten soziotechnischen Bedingungen unterschiedlich stark für privatheitsbezogene Eingriffe anfällig sind, denen sie nur begrenzt selbst begegnen können. Dies lässt sich etwa im Kontext digitaler Gesundheitsanwendungen und der Verarbeitung sensibler Gesundheitsdaten deutlich machen: Während die Nutzung einer Fitness-, Zyklus- oder Mental-Health-App für manche Personen primär der Selbstoptimierung oder Prävention dient, kann sie für andere mit erheblichen sozialen und ökonomischen Risiken verbunden sein. Besonders deutlich wird dies bei Personen in prekären Arbeitsverhältnissen, etwa mit befristeten Verträgen, unsicherem Aufenthaltsstatus oder hoher ökonomischer Abhängigkeit vom Arbeitsplatz. In einer solchen Lage sind Betroffene unter Umständen stärker darauf angewiesen, gesundheitliche Beeinträchtigungen oder Belastungen nicht sichtbar werden zu lassen, um keine Nachteile im Beschäftigungsverhältnis zu riskieren. Gelangen sensible Gesundheitsdaten – sei es durch Datenweitergabe an Dritte, durch Sicherheitslücken oder durch indirektes Profiling – in Kontexte, in denen sie für Versicherungen, Arbeitgeber*innen oder Plattformbetreiber ökonomisch relevant werden, können sie sich in faktische Druckmittel verwandeln. Die betroffenen Personen haben in solchen Konstellationen häufig nur begrenzte Möglichkeiten, sich gegen intransparente Datenflüsse oder algorithmische Risikobewertungen zur Wehr zu setzen. Demgegenüber verfügen Personen in stabilen Beschäftigungsverhältnissen oder mit größerer finanzieller Absicherung regelmäßig über mehr Handlungsspielräume: Sie können datenschutzfreundlichere Alternativen wählen, kostenpflichtige Dienste nutzen, Rechtsmittel einlegen oder im Konfliktfall den Arbeitsplatz wechseln.

Die unterschiedliche privatheitsbezogene Vulnerabilität ergibt sich hier nicht aus einer abstrakten Zugehörigkeit zu einer bestimmten sozialen Kategorie, sondern aus der konkreten Verschränkung von ökonomischer Abhängigkeit, arbeitsrechtlicher Unsicherheit, datengetriebenen Bewertungspraktiken und der Sensibilität der verarbeiteten Informationen. Erst die Analyse dieser Konstellation macht sichtbar, welche Diversitätsdimensionen – etwa Beschäftigungsstatus, ökonomische Resilienz oder institutionelle Abhängigkeiten – für die Bewertung des Privatheitsschutzes im jeweiligen Kontext relevant sind. Diese Dimensionen gilt es zu erfassen, wenn der Privatheitsschutz für alle wirksam und gerecht gestaltet werden soll. Gesellschaftliche Diversität allein begründet dabei zwar noch keinen besonderen Schutzbedarf. Allerdings erweist sich gerade die Kombination von Diversität und Vulnerabilität als sehr gut geeignet, um ethische Fragestellungen im Privatheitsbereich ohne vorgegebene Kategorisierungen zu bearbeiten. Die zu berücksichtigenden Diversitätsdimensionen sind folglich nicht abstrakt festzulegen, sondern im Kontext des jeweiligen Gegenstandsbereichs zu ermitteln.

So kann beispielsweise auch die verpflichtende Nutzung einer schulischen Lernplattform für Hausaufgaben und Leistungsrückmeldungen unterschiedliche privatheitsbezogene Vulnerabilitäten erzeugen: Schülerinnen und Schüler, die über ein eigenes, passwortgeschütztes Endgerät verfügen, können ihre Zugänge vergleichsweise eigenständig kontrollieren. Lernende hingegen, die sich ein Gerät mit Geschwistern oder Eltern teilen oder auf öffentliche Internetzugänge angewiesen sind, haben faktisch weniger Möglichkeiten, sensible Leistungsdaten, Kommunikationsverläufe oder Rückmeldungen vertraulich zu halten. Hinzu kommt, dass Erziehungsberechtigte mit höherer

digitaler Kompetenz oder größerem zeitlichen Spielraum eher in der Lage sind, Datenschutzeinstellungen zu prüfen, Auskunftsrechte wahrzunehmen oder problematische Datenverarbeitungen zu adressieren. Familien in belasteten Lebenslagen verfügen demgegenüber häufig über geringere Ressourcen, um privatheitsbezogene Risiken zu erkennen und ihnen wirksam zu begegnen. Die unterschiedliche Anfälligkeit für Eingriffe in die Privatheit ergibt sich hier nicht primär aus einer vorab festgelegten sozialen Kategorie, sondern aus dem Zusammenspiel von technischer Infrastruktur, institutioneller Verpflichtung zur Nutzung und ungleich verteilten materiellen sowie kompetenzbezogenen Ressourcen. Erst im Rückgriff auf diese Vulnerabilitätskonstellation werden die relevanten Diversitätsdimensionen sichtbar.

Ein diversitätsgerechter Privatheitsschutz muss so konzipiert sein, dass er diesen spezifischen und kontextabhängigen Vulnerabilitäten Rechnung trägt. Diversitätsdimensionen dienen dabei als Grundlage, um bestehende Schutzbedarfe zu identifizieren und angemessene Schutzmaßnahmen abzuleiten. Zugleich erlaubt dieser Ansatz, intersektionale Zusammenhänge zu berücksichtigen, ohne auf vorgegebene Diskriminierungskategorien zurückzugreifen. Stattdessen können Vulnerabilitäten entlang von Spektren erfasst werden, die sich aus unterschiedlichen Ausprägungen und Konstellationen relevanter Merkmale ergeben. Vulnerabilität ist daher nicht als Eigenschaft zu verstehen, die allein aus der Zugehörigkeit zu einer Personengruppe resultiert, sondern als Ergebnis unterschiedlicher Merkmale, die in verschiedenen Kombinationen und Intensitäten zusammentreffen. Besonders im Privatheitsbereich zeigen sich die Grenzen klassischer Kategorien, etwa wenn sich erhöhte Risiken aus spezifischen Nutzungssituationen ergeben oder wenn nicht die Zugehörigkeit zu einer bestimmten Gruppe, sondern eine besondere Form der digitalen Exposition ausschlaggebend für eine erhöhte Schutzbedürftigkeit ist. Vor diesem Hintergrund wird im Folgenden näher ausgeführt, wie Privatheit diversitätsgerecht geschützt werden kann.

4 **Wie kann Privatheit diversitätsgerecht geschützt werden?**

Ein angemessener Privatheitsschutz sollte vielfältigen Formen der Vulnerabilität Rechnung tragen, indem der jeweils erforderliche Schutz unter Rückgriff auf relevante Dimensionen gesellschaftlicher Diversität bestimmt und in entsprechende Maßnahmen übersetzt wird. Dabei ist zu berücksichtigen, dass sich Schutzbedarfe von Nutzenden in Abhängigkeit von sozialen Umständen, individuellen Voraussetzungen und Kontexten der Datenerhebung oder -verarbeitung erheblich unterscheiden können. Während in diesem Abschnitt konzeptionelle und ethische Empfehlungen formuliert werden, die als Leitlinien für die praktische Weiterentwicklung des Privatheitsschutzes dienen können, werden im nächsten Abschnitt Vorschläge zum Design von Benutzeroberflächen, zur Fortentwicklung des rechtlichen Rahmens und zur Wissenschaftskommunikation unterbreitet.

Privatheitsschutz auf gesellschaftliche Diversität ausrichten

Damit privatheitsbezogene Vulnerabilitäten angemessen erfasst werden können, ist der klassische Diskriminierungsschutz, der auf abschließenden Merkmalslisten beruht, um eine weitergehende Diversitätsperspektive zu ergänzen. Anstatt nur auf etablierte Diskriminierungskategorien zurückzugreifen, die aus allgemeinen gesellschaftlichen Benachteiligungslagen abgeleitet sind, sollten relevante Kategorien in Auseinandersetzung mit spezifischen Vulnerabilitäten bestimmt werden, die sich im jeweiligen digitalen Kontext ergeben – sei es etwa durch intransparente Praktiken der Datenverarbeitung, aufgrund kognitiver Beeinträchtigungen oder mangels ausreichender Sprachkompetenzen. Schutzmaßnahmen können entsprechend an denjenigen Dimensionen gesellschaftlicher Diversität ausgerichtet werden, die im Privatheitsbereich zu unterschiedlich ausgeprägten Vulnerabilitäten bei verschiedenen Gruppen führen. So lässt sich ein diversitätsgerechter Privatheitsschutz entwickeln, der auch Phänomene der Intersektionalität berücksichtigt.

Diversität und Vulnerabilität kombinieren

Im Unterschied zu klassischen Diskriminierungs- und Intersektionalitätsansätzen ist der Diversitätsbegriff allein nicht mit einer moralischen Problemdiagnose verbunden und begründet daher für sich genommen keinen besonderen Schutzbedarf. Es gibt Formen der Diversität, die weder mit gesellschaftlichen Machtverhältnissen zusammenhängen noch mit einer erhöhten Gefährdung einhergehen. Um ethische Probleme des Privatheitsschutzes adressieren zu können, ist es daher entscheidend, Diversität systematisch mit dem Begriff der Vulnerabilität zu verknüpfen. Welche Dimensionen gesellschaftlicher Diversität dabei relevant sind, lässt sich nicht abstrakt vorgeben, sondern muss angesichts konkret vorliegender Bedürfnisse, Anforderungen, Kompetenzen und Ressourcen sowie den jeweiligen soziotechnischen Umständen herausgearbeitet werden. In Kombination ermöglichen die Begriffe der Diversität und Vulnerabilität es so, ethisch relevante Schutzbedarfe zu identifizieren.

Vulnerabilität nicht anhand von Durchschnittsnutzenden bestimmen

Während manche Formen der Vulnerabilität bestimmte Personen oder Personengruppen in besonderem Maße betreffen, sind andere in digital geprägten Gesellschaften universell vorhanden. Ein Privatheitsschutz, der ein angemessenes Schutzniveau für alle gewährleisten soll, muss beide Dimensionen berücksichtigen. Häufig wird Vulnerabilität allerdings nur dort verortet, wo entweder die Eintrittswahrscheinlichkeit von Schäden erhöht ist oder mögliche Schadensfolgen besonders gravierend sind (vgl. Racine/Bracken-Roche 2019; Koch et al. 2025, S. 236). Als Referenzpunkt wird dabei nicht selten auf Vorstellungen vermeintlich normaler Situationen oder durchschnittlicher Personen Bezug genommen. Dieser Maßstab erscheint jedoch zum einen fragwürdig, da er auf problematischen Prozessen der Normalisierung beruht (vgl. Reinhardt 2020). Zum anderen müssen auch

Risiken, die als gewöhnlich gelten, keineswegs akzeptabel sein und können bereits einen Schutzbedarf begründen. Gerade im Privatheitskontext zeigt sich, dass selbst sehr verbreitete und insofern als normal wahrgenommene Risiken Anlass für Schutzmaßnahmen bieten: Etablieren große Technologieunternehmen systematisch unzureichende Datenschutzpraktiken, wie es sich etwa bei den eingangs erwähnten Cookie-Einstellungen zeigt, ist die Mehrheit der Nutzenden bei der alltäglichen Nutzung sozialer Medien in ihrer informationellen Selbstbestimmung gefährdet. Wenn ein vulnerabilitätsbezogener Ansatz im Bereich der Privatheit tragfähig sein soll, dann muss er auch solche alltäglichen und weit verbreiteten Risiken erfassen. Maßgeblich scheint hier, welche Risiken Menschen im Rahmen ihrer gesellschaftlichen Teilhabe zugemutet werden dürfen. Wird dieses Niveau überschritten, sodass die Voraussetzungen gesellschaftlicher Teilhabe beeinträchtigt sind, ist ein Schutzbedarf vorhanden.

Besondere Vulnerabilitäten erkennen und adressieren

Verschiedene Personen und Personengruppen sind allerdings, was datenschutzrelevante Eingriffe anbelangt, in sehr unterschiedlicher Weise vulnerabel. Sie können ihre Privatsphäre nicht gleich gut schützen und sind unterschiedlich stark gefährdet, durch Privatheitsverletzungen geschädigt zu werden. So sind manche Menschen vielleicht als Angehörige marginalisierter Gruppen einem höheren Risiko diskriminierender Datenverarbeitung ausgesetzt, während andere sich aufgrund gesundheitlicher Beeinträchtigungen kaum gegen problematische Praktiken zur Wehr setzen können. Entsprechend kommt es aus ethischer Sicht darauf an, diese besonderen Vulnerabilitäten als solche zu erkennen und angemessen zu adressieren. Für die Weiterentwicklung des Privatheitsschutzes sollten daher weder die Idee einer bloßen Gleichbehandlung – etwa in Form eines einheitlichen, aber unzureichenden Schutzniveaus – noch Vorstellungen vermeintlicher Normalität leitend sein. Vielmehr ist entscheidend, dass sowohl Mindestanforderungen an den Privatheitsschutz angelegt werden, die allgemein vorhandenen Schutzbedarfen entsprechen, als auch weitergehende Maßnahmen ergriffen werden, die ungleiche Risikoverteilungen adressieren, indem sie besonders vulnerable Gruppen schützen.

Ergänzende Maßnahmen partizipativ entwickeln und empirisch untersuchen

Vor dem Hintergrund einer Analyse spezifischer Schutzbedarfe vulnerabler Personengruppen sind geeignete Schutzmaßnahmen zu entwickeln, die den allgemeinen Privatheitsschutz sinnvoll ergänzen. Dabei sollten partizipatorische Ansätze gewählt werden, welche die Betroffenen und ihre Bezugspersonen aktiv und iterativ in den Prozess der Ideengenerierung und Ausarbeitung einbeziehen. Nur so kann eine bedarfsgerechte Entwicklung ergänzender Maßnahmen garantiert werden. Als vielversprechend eingestufte Maßnahmen sind empirisch daraufhin zu untersuchen, ob sie eine hinreichende Wirksamkeit aufweisen. Dies sollte vor allem im Rahmen realweltlicher Settings und in Form von Langzeitstudien erfolgen, um auch eine langfristige Wirksamkeit realistisch einschätzen zu können.

Intersektionale Zusammenhänge berücksichtigen

Soziale Kategorien und entsprechende Machtverhältnisse wirken nicht isoliert, sondern überlagern sich und erzeugen in ihrer Kombination neue Formen der Vulnerabilität. Dies ist bei der Weiterentwicklung des Privatheitsschutzes insofern zu berücksichtigen, als privatheitsbezogene Vulnerabilitäten selbst durch intersektionale Zusammenhänge mitkonstituiert sein können oder im Zusammenwirken mit anderen Benachteiligungen womöglich zu neuen Vulnerabilitäten führen. Dies zeigt sich etwa, wenn eine chronisch kranke Person in einer Zweit- oder Drittsprache digitale Verwaltungs- oder Gesundheitsdienste nutzen muss, weil diese nicht in ihrer Erstsprache vorliegen: Sprachliche Barrieren, Abhängigkeit von digitalen Schnittstellen und eingeschränkte Möglichkeiten, Datenschutzinformationen zu verstehen oder Rechte geltend zu machen, können sich hier

überlagern und zu einer erhöhten Exposition gegenüber Datenmissbrauch oder Fehlverarbeitungen führen. Indem Phänomene der Intersektionalität berücksichtigt werden, lässt sich der Privatschutz so gestalten, dass er keine Vulnerabilitäten übergeht und mithilft, zusätzlich entstehende Formen der Vulnerabilität zu verhindern.

Diskriminierungskategorien prüfend einbeziehen

Die eingenommene Diversitätsperspektive erlaubt es, Schutzbedarfe im Privatheitsbereich differenzierter und stärker kontextbezogen zu identifizieren. Dies darf jedoch nicht dazu führen, strukturelle Formen gesellschaftlicher Benachteiligung aus dem Blick zu verlieren. Ein einseitiger Fokus auf problematische Fälle, die unabhängig von etablierten Diskriminierungskategorien betrachtet werden, ist daher zu vermeiden. Auf diese Weise können entsprechende Phänomene der Intersektionalität miterfasst werden, während zugleich eine drohende Überkomplexität der Analyse begrenzt und der Tendenz entgegengewirkt wird, die Verantwortung zur Bekämpfung von Vulnerabilitäten auf Individuen abzuwälzen. Insofern ist es weiterhin sinnvoll, auf Diskriminierungskategorien zurückzugreifen, um einen diversitätsorientierten Ansatz zu ergänzen und auf mögliche Schwachstellen und „blinde Flecke“ hin zu prüfen (vgl. Heesen et al. 2021). Besonders relevant sind dabei zusammenwirkende Benachteiligungen, die aus verschiedenen Lebensbereichen stammen und in ihrer Kombination eine erhebliche Belastung darstellen können. So mag eine queere Person mit hoher *Privacy Literacy*, isoliert betrachtet, vielleicht keine ausgeprägte Vulnerabilität im Privatheitsbereich aufweisen. Wird diese Person allerdings in weiteren gesellschaftlichen Kontexten systematisch diskriminiert, kann selbst eine vergleichsweise geringe Gefährdung der informationellen Selbstbestimmung zu einer Belastung führen, die einen zusätzlichen Schutzbedarf begründet.

Hieraus folgt, dass der Schutz der Privatheit nicht allein an der Fähigkeit einer Person zur Wahrnehmung ihrer informationellen Selbstbestimmung festgemacht werden darf. Selbst sehr gut informierte Personen können in bestimmten Kontexten stark vulnerabel sein, wenn andere Faktoren – etwa gesellschaftliche Diskriminierungen oder strukturelle Benachteiligungen – wirksam werden. Zugleich zeigt sich, dass Merkmale, die auf den ersten Blick keine Digitalitätsrelevanz besitzen, im spezifischen Kontext von Privatheitsrisiken eine erhebliche Rolle spielen können: Alter, gesundheitliche Einschränkungen, soziale Stellung oder marginalisierte Identitäten können die Folgen selbst kleiner Datenschutzverletzungen erheblich verstärken. Für den Privatheitsschutz bedeutet dies, dass Risiken stets im Zusammenspiel von individuellen Fähigkeiten, sozialen Lagen und kontextuellen Bedingungen bewertet werden müssen. Ein intersektionaler, diversitätsorientierter Ansatz erfasst nicht nur abstrakte Fähigkeiten, sondern berücksichtigt, wie unterschiedliche Merkmale und Benachteiligungen zusammenwirken – auch dann, wenn einzelne Faktoren isoliert betrachtet eher unproblematisch erscheinen für die Fähigkeiten, die eigene Privatheit zu schützen.

5 Empfehlungen für Benutzeroberflächendesign, Rechtsfortentwicklung und Wissenschaftskommunikation

Vor dem Hintergrund der grundlegenden Vorschläge des vierten Abschnitts werden im Folgenden praktische Empfehlungen dazu gegeben, wie sich das Design digitaler Benutzeroberflächen anpassen lässt, um Privatheit diversitätsgerecht zu schützen, welche Aspekte bei der Fortentwicklung des rechtlichen Rahmens zu beachten sind und wie die Wissenschaft besser über Privatheit und Privatheitsschutz kommunizieren kann.

Erfahrbare und intuitive Warnungen entwickeln

Was das *Benutzeroberflächendesign* betrifft, könnten neue Ansätze wie der Einsatz viszeraler (also körperlich-wahrnehmbarer) Reize das Bewusstsein für Privatheitsrisiken schärfen und Menschen dabei unterstützen, privatheitsschützende Entscheidungen zu treffen (vgl. Calo 2011; Acquisti et al. 2022; Koch et al. 2025, S. 227 ff.). Im Gegensatz zum traditionellen symbol- und textgeprägten Datenschutzhinweis geht es hier um eine Gefahrenvermittlung durch Auslösen körperlicher Reaktionen. Dies kann etwa durch Analogien aus der analogen Welt gewährleistet werden, beispielsweise durch ein Auslösegeräusch, das ertönt, wenn eine digitale Kamera ein Foto macht (Calo 2011). Durch Einsatz eines solchen Geräuschs im digitalen Kontext kann eine Brücke zwischen verschiedenen Arten des Privatheitseingriffs geschlagen werden (von analog zu digital), und das Bewusstsein für einen solchen erhöht werden. Ebenso könnten auf Webseiten bestimmte Designelemente mit visuellen oder akustischen Reizen eingesetzt werden, die gezielt soziale Reaktionen bei den Nutzenden hervorrufen. Eine beispielhafte Ausgestaltung wäre in Form eines Augenpaares möglich, welches ein Gefühl des Beobachtetwerdens vermittelt und somit zu einem vorsichtigeren Umgang mit den eigenen Daten führt (vgl. Rodriguez-Priego et al. 2021). Bisherige Erkenntnisse deuten darauf hin, dass viszerale Reize sowohl bei Grundschulkindern als auch bei Personen mit kognitiven Einschränkungen das Potenzial haben, das Datenschutzbewusstsein zu stärken.

Paternalismus vermeiden

Zwei Strategien sind dabei sinnvoll, um zu verhindern, dass viszerale Hinweise in problematischer Weise als paternalistisch wahrgenommen werden (vgl. Koch et al. 2025, S. 229). Erstens sollte den Nutzenden die Möglichkeit gegeben werden, individuell auszuwählen, welche Privatheitspräferenzen durch viszerale Reize unterstützt werden. So könnten Nutzende zum Beispiel einstellen, dass sie bei der Aktivierung von Kamera oder Mikrofon durch ein auffälliges visuelles Signal gewarnt werden, nicht jedoch bei der Verwendung anonymisierter Daten. Zweitens könnten viszerale Reize so gestaltet werden, dass sie einen Beitrag zur *Privacy Literacy* und damit zum zukünftigen Selbstschutz leisten, beispielsweise indem man sie um einen Hinweis ergänzt, welcher mehr Informationen zur Gefährdungslage anbietet. Im Rahmen von ersten Studien zeigte sich, dass dies auch unter vulnerablen Gruppen erwünscht ist.

Responsibilisierung entgegenwirken

Zu beachten ist außerdem, dass der Einsatz viszeraler Reize nicht zu einer Rechtfertigung rein individueller und eigenverantwortlicher Lösungen von Privatheitsproblemen (Responsibilisierung) führen sollte und gegen strukturelle (politische) Maßnahmen abgewogen werden muss. Es besteht nämlich die Gefahr, dass allein technische Innovationen als Lösungen für soziale Probleme betrachtet werden. Daneben muss empirisch weiter gefestigt werden, inwiefern viszerale Reize eine geeignete Lösung für Schutzlücken durch eine fehlende *Privacy Literacy* sein können (oder *Privacy*

Literacy-Ansätze sinnvoll unterstützen können). Bei der Evaluation viszeraler Reize sind damit Fragen der Responsibilisierung und der Eignung technischer Lösungsansätze zu berücksichtigen (vgl. Koch et al. 2025, S. 228 f.). Technische Lösungen sind durch partizipatorische Ansätze zu informieren sowie durch empirische Studien auf ihre (langfristige) Wirksamkeit zu überprüfen und gegebenenfalls anzupassen.

Schutzbedürftigkeit kontextbezogen betrachten

Hinsichtlich der *Rechtsfortentwicklung* ist zunächst Folgendes zu beachten: Die Datenschutz-Grundverordnung als zentraler Basis des Datenschutzrechts in der Europäischen Union begegnet Vulnerabilität insbesondere durch die inhaltliche Kategorisierung besonders sensibler Daten (Art. 9 DSGVO), wobei sich die Regelungssystematik primär an einem idealtypischen, durchschnittlich informierten Nutzenden orientiert. Eine differenzierte kontextbezogene Betrachtung individueller oder situativer Schutzbedürftigkeit erfolgt weitgehend nicht; eine Ausnahme bildet der Schutz von Kindern, z. B. in Form von Art. 8 DSGVO. Dies erfasst den aufgeführten Schutzbedarf im Rahmen digitaler Vulnerabilität jedoch nicht ausreichend differenziert (vgl. Roßnagel 2020; Roßnagel/Geminn 2020). Daher bleibt eine adäquate Adressierung digitaler Vulnerabilität notwendig, um z. B. älteren oder kognitiv beeinträchtigten Menschen entsprechenden Selbstschutz zu ermöglichen.

Individuen- und kontextabhängige Schutzmaßnahmen ableiten

Insbesondere im Verbraucherrecht wurden besondere Vulnerabilitäten bereits erkannt und adressiert, um Personen wirksam vor Ausnutzung aufgrund körperlicher oder geistiger Einschränkungen, hohen Alters oder situativer Leichtgläubigkeit zu schützen (vgl. Kroschwald 2023; Damm 2013). Im Kontext digitaler Technologien werden diese Personen als Nutzende oder Verbrauchende aber oft nicht mitgedacht. Um individuellen Vulnerabilitäten 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 Gegenstandsreichs entwickelt wird. Zur Ableitung entsprechender Schutzmaßnahmen müssen neben den schutzbedürftigen Individuen auch die gefährdenden Situationen und Kontexte identifiziert werden (vgl. Kroschwald 2023).

Einwilligungsprozesse barrierefrei gestalten

Um die Selbstbestimmung betroffener Personen zu stärken und die mit einer wirksamen Einwilligung verbundenen Schutzpotenziale auszuschöpfen, sollten vulnerable Personen von Beginn an systematisch mitgedacht werden. Hierzu bedarf es konkreter Leitlinien für Anbieter digitaler Dienste, die individuelle oder situative Schutzbedürftigkeit ausdrücklich berücksichtigen. Orientierung können dabei die Vorgaben aus Art. 4 lit. g iVm Art. 9 der UN-Behindertenrechtskonvention zur Gewährleistung eines gleichberechtigten Zugangs zu Informations- und Kommunikationstechnologien für Menschen mit Behinderungen bieten. Diese umfassen insbesondere die barrierefreie Ausgestaltung informierter Einwilligungsprozesse, etwa durch die Bereitstellung von Informationen in zugänglichen Formaten wie leichter Sprache oder auditiver Sprachausgabe (vgl. Schmied/Nebel 2025). Verfahren, die auf den Schutz spezifischer Vulnerabilitätsgruppen ausgerichtet sind, können zugleich auch einen Mehrwert für den Schutz anderer Personengruppen entfalten.

Inklusiv über Privatheit und Privatheitsschutz kommunizieren

Auch der Bereich der *Wissenschaftskommunikation* über Privatheit und Privatheitsschutz an diverse Gruppen kann von einem integrativen Ansatz profitieren. Wie aufgezeigt, sind Perspektiven, Bedürfnisse und Erfahrungen vielfältig. Das Ziel von Wissenschaftskommunikation im Kontext eines diversitäts- und kontextsensiblen Privatheitskonzepts sollte deshalb nicht bloß in der Vermittlung von Forschungsergebnissen bestehen, sondern Brücken schlagen zu vorhandenem Praxiswissen

und dezentralen Wissensbeständen. Vor diesem Hintergrund hat eine möglichst inklusive Wissenschaftskommunikation nicht nur eine Demokratisierung des Wissens zum Ziel, sondern verbessert im besten Fall auch die Qualität und Relevanz von Privatheitsforschung: Gerade in Fällen, in denen explizit vulnerable Gruppen betroffen sind, ist es unumgänglich, diese bereits in der Konzeptionsphase von Kommunikationsformaten zu adressieren und jene im Abgleich mit den Wünschen und Erwartungen der Betroffenen zu entwickeln. Idealerweise wird es durch diesen Einbezug verschiedener Perspektiven und Lebenserfahrungen in den Wissenschaftsdialog auch möglich, blinde Flecken im Forschungskonzept zu identifizieren, neue Fragen aufzuwerfen und innovative Lösungen für vulnerable Gruppen zu entwickeln.

Ethische Verantwortung wahrnehmen

Darüber hinaus trägt die kommunikative Adressierung vulnerabler Gruppen und/oder der jeweiligen Interessenvertretungen zur ethischen Verantwortung der Wissenschaft bei. Forschung sollte bestehende Ungleichheiten nicht verstärken. Indem vulnerable Gruppen in einem dialogorientierten Verständnis von Wissenschaft aktiv in den Prozess der Wissensgenerierung und -verbreitung einbezogen sind, wird sichergestellt, dass Forschung verantwortungsbewusst und inklusiv handelt: „Strategien für ein gerechtes Framing umfassen die Aufforderung an Wissenschaftskommunikatoren, (1) sich ihrer eigenen Positionalität und ihrer partikulären Perspektiven bewusst zu werden, (2) Ursachen für Ungleichheit zu benennen, die aus ungleichen Machtverhältnissen resultieren, und (3) Schnittstellen zu Initiativen zu finden, die auf den Erfahrungen benachteiligter Gemeinschaften basieren“ (Polk/Diver 2020, Übersetzung der Autor:innen).

Machtstrukturen und Einfluss kontinuierlich reflektieren

Dabei ist es zentral zu betonen, dass die Einbeziehung vulnerabler Gruppen in die Wissenschaftskommunikation nicht lediglich oberflächlicher Natur sein darf. Der Ansatz erfordert eine kontinuierliche Reflexion über Machtstrukturen, Status und gesellschaftlichen oder politischen Einfluss der beteiligten (und eben gerade nicht-beteiligten) Akteure – was mit Blick auf die politischen Rahmenbedingungen auch einen entsprechenden Willen und spezifische Förderinstrumente voraussetzt. Zusätzlich erfordert dialogorientierte Wissenschaft auch den Aufbau von zivilgesellschaftlichen Partnerschaften und die ganz grundsätzliche Schaffung von Räumen, in denen vulnerablen Gruppen eine echte Stimme gegeben wird.

6 Fazit

Im Zeitalter digitaler Technologien ist der Schutz von Privatheit besonders wichtig, während bestehende Datenschutzmechanismen häufig unzureichend sind. Die Einwilligung einzelner Personen und die damit verbundene informationelle Selbstbestimmung sind zwar zentrale Aspekte des Datenschutzes. Ein auf *Privacy Literacy* ausgerichteter Ansatz, der sich primär an den Fähigkeiten von „Durchschnittsnutzenden“ orientiert, genügt aber insbesondere für vulnerable Personen nicht. Weder schützt *Privacy Literacy* stets ausreichend noch ist diese für vulnerable Personen immer erreichbar. Um ein durchgängig angemessenes Schutzniveau sicherzustellen, ist es daher erforderlich, unterschiedliche Formen von Vulnerabilität im Privatheitsbereich diversitätsgerecht zu berücksichtigen.

Schutzbedarfe bestehen im Bereich der Privatheit weder für alle gleichermaßen noch können sie allein entlang vorgegebener sozialer Kategorien bestimmt werden. Menschen sind in unterschiedlichem Maße anfällig für Eingriffe in ihre Privatsphäre, wobei sowohl strukturelle Bedingungen als auch individuelle Faktoren eine Rolle spielen. Statt auf starre Kategorien wie Geschlecht, Herkunft oder Klasse zurückzugreifen, bietet der offenere Diversitätsbegriff die Möglichkeit, Schutzbedarfe kontextabhängig und entlang konkreter Vulnerabilitäten zu erfassen. Eine diversitätsgerechte Ausgestaltung des Privatheitsschutzes sowie eine entsprechend differenzierte Wissenschaftskommunikation sind daher zentrale Bausteine eines wirksamen Datenschutzes. Der gezielte Schutz vulnerabler Personen trägt dabei in vielen Fällen auch zu einem insgesamt höheren Schutzniveau bei.

7 Literaturverzeichnis

- Acquisti, A.; Brandimarte, L.; Hancock, J. (2022): How privacy's past may shape its future. *Science*, 375, S. 270-272. <https://doi.org/10.1126/science.abj0826>
- Behrendt, H. und Loh, W. (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>.
- Birnbacher, D. (2012): Vulnerabilität und Patientenautonomie – Anmerkungen aus medizin-ethischer Sicht. *MedR* 30 (9), S. 560–565. <https://doi.org/10.1007/s00350-012-3223-1>.
- Brough, A. R. und Martin, K. D. (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.2019.06.02>
- Calo, R. (2011): Against notice skepticism in privacy (and elsewhere). *Notre Dame L. Rev.*, 87, S. 1027.
- Castro Varela, M. und Heinemann, A. (2016): Globale Bildungsbewegungen – Wissensproduktionen verändern. *ZEP: Zeitschrift für internationale Bildungsforschung und Entwicklungspädagogik*, 39(2), S. 17–22. <https://doi.org/10.25656/01:15447>.
- Chalghoumi, H.; Cobigo, V.; Dignard, C.; Gauthier-Beaupré, A.; Jutai, J. W.; Lachapelle, Y.; Lake, J.; Mcheimech, R.; Perrin, M. (2019): Information Privacy for Technology Users With Intellectual and Developmental Disabilities: Why Does It Matter? *Ethics & Behavior*, 29(3), 201–217. <https://doi.org/10.1080/10508422.2017.1393340>
- Collins, P. H. und Bilge, S. (2016): Intersectionality. *Polity*.
- Collins, P. H. (2019): Intersectionality as Critical Social Theory. *Duke University Press*.
- Crenshaw, K. (1989): Demarginalizing the Intersection of Race and Sex: A Black Feminist Critique of Antidiscrimination Doctrine, Feminist Theory and Antiracist Politics. *University of Chicago Legal Forum*, 1989(1), Article 8. <http://chicagounbound.uchicago.edu/uclf/vol1989/iss1/8>.
- Damm, R. (2013): Vulnerabilität als Rechtskonzept?. *Medizinrecht*, 31(4), S. 201-214.
- Eubanks, V. (2018): Automating inequality: How high-tech tools profile, police, and punish the poor. *St. Martin's Press*.
- Fineman, M. (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, M. (2017): Vulnerability and Inevitable Inequality. *Oslo Law Review*, 4(3), S. 133-149. <https://doi.org/10.18261/issn.2387-3299-2017-03-02>.
- Geminn, C. L. (2023): Deus ex machina? Grundrechte und Digitalisierung. *Jus Publicum (JusPubl)* 316. Tübingen: Mohr Siebeck.
- Geminn, C.; Baumann, J.; Heesen, J.; Mühl, L.; Wenten, K. (2026): Konversationelle KI-Agenten: Gegenwärtige und zukünftige Herausforderungen, in: M. Friedewald, A. Roßnagel, M. Karaboga, C. Geminn (Hrsg.): *Datenschutz und Digitalpolitik in krisenhaften Zeiten. Ausgewählte Beiträge der 10. Konferenz der Plattform Privatheit. Privatheit und Selbstbestimmung in der digitalen Welt 7*. Baden-Baden: Nomos.
- Grimm, P. und Krahn, H. (2016): Privatsphäre. In: Jessica Heesen (Hg.): *Handbuch Informations- und Medienethik*. Stuttgart/Weimar: Metzler, S. 178-185.
- Hagendorff, T. (2018): Privacy Literacy and Its Problems. *Journal of Information Ethics* 27 (2), S. 127–145.

- Hancock, A.-M. (2016): *Intersectionality: An Intellectual History*. Oxford University Press.
- Heesen, J.; Reinhardt, K.; Schelenz, L. (2021): Diskriminierung durch Algorithmen vermeiden. Analysen und Instrumente für eine demokratische digitale Gesellschaft, in: G. Bauer, M. Kechaja, S. Engelmann, L. Haug (Hrsg.): *Diskriminierung und Antidiskriminierung: Beiträge aus Wissenschaft und Praxis*, Bielefeld: transcript, 129-147.
- Kiener, M. (2023): *Voluntary consent. Theory and practice*. New York, London: Routledge Taylor & Francis Group (Routledge annals of bioethics).
- Koch, H.; Strathmann, C.; Hennig, M.; Schmied, L.; Geminn, C.; Heesen, J.; Krämer, N.; Reinhardt, K. (2025): Diversitätsgerechter Privatschutz in digitalen Umgebungen, in: Friedewald, M. et al. (Hrsg.): *Freiheit in digitalen Infrastrukturen*, Baden-Baden: Nomos, 223-241.
- Kroschwald, S. (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.
- Kühling, J. und Buchner, B. (Hrsg.) (2024): *Datenschutz-Grundverordnung/ Bundesdatenschutzgesetz. Kommentar*, 4. Auflage. München: C. H. Beck.
- Liedke-Deutscher, B. (Hrsg.) (2024): *Die datenschutzrechtliche Einwilligung nach der DSGVO*. Oldenburg: OIWR.
- Linabary, J. R. und Corple, D. J. (2019): Privacy for whom?: a feminist intervention in online research practice. *Information, Communication & Society* 22 (10), S. 1447–1463. <https://doi.org/10.1080/1369118X.2018.1438492>.
- Luna, F. (2009): Elucidating the concept of vulnerability: Layers not labels. *IJFAB: International Journal of Feminist Approaches to Bioethics* 2 (1), S. 121–139. <https://doi.org/10.3138/ijfab.2.1.121>.
- Martin, A. K. (2023): *The Moral Implications of Human and Animal Vulnerability*. Cham: Springer International Publishing.
- Masur, P. K. (2020): How online privacy literacy supports self-data protection and self-determination in the age of information. *Media and Communication*, 8(2), 258–269. <https://doi.org/10.17645/mac.v8i2.2855>
- Miller, F. und Wertheimer, A. (2009): *The Ethics of Consent*. New York: Oxford University Press.
- Müller, A. und Schaber, P. (2018): *The Routledge Handbook of the Ethics of Consent*. Abingdon und New York: Routledge.
- Nebel, M. (2015): Schutz der Persönlichkeit – Privatheit oder Selbstbestimmung? Verfassungsrechtliche Zielsetzungen im deutschen und europäischen Recht. *Zeitschrift für Datenschutz*, 11/2015, S. 517-521.
- Polk, E. und Diver, S. (2020): Situating the Scientist: Creating Inclusive Science Communication Through Equity Framing and Environmental Justice. *Frontiers in Communication*, 5(6), <https://doi.org/10.3389/fcomm.2020.00006>.
- Racine, E. und Bracken-Roche, D. (2019): Enriching the concept of vulnerability in research ethics: An integrative and functional account. *Bioethics*, 33(1), 19–34. <https://doi.org/10.1111/bioe.12471>.
- Reinhardt, K. (2020): Between Identity and Ambiguity. Some Conceptual Considerations on Diversity, in: *Symposion* 7 (2), 261-283.

Naegeli et al. (2026): Diversitätsgerechter Privatheitsschutz: Empfehlungen zum Schutz der Privatheit vulnerabler Gruppen in digitalen Umgebungen

Rodriguez-Priego, N.; van Bavel, R.; Monteleone, S. (2021): Nudging online privacy behaviour with anthropomorphic cues. *Journal of Behavioral Economics for Policy*, 5(1), 45-52.

Roßnagel, A.; Pfitzmann, A.; Garstka, H. (2001): Gutachten im Auftrag des Bundesministeriums des Innern. Modernisierung des Datenschutzrechts. Berlin. URL: http://www.datenschutzgeschichte.de/pub/dphistory/2001_GarskaPfitzmannRosnagel_Modernisierung_des_Datenschutzrechts.pdf (besucht am 27.02.2025).

Roßnagel, A.; Bile, T.; Nebel, M.; Geminn, C. L.; Karaboga, M.; Ebberts, F.; Bremert, B.; Stapf, I.; Teebken, M.; Thürmel, V.; Ochs, C.; Uhlmann, M.; Krämer, N. C.; Meier, Y.; Kreuzer, M.; Schreiber, L.; Simo, H. (2020): Einwilligung: Möglichkeiten und Fallstricke aus der Konsumentenperspektive; White Paper. Karlsruhe: Forum Privatheit. <https://doi.org/10.24406/publica-fhg-300317>.

Roßnagel, A. und Geminn, C. (2020): Datenschutz-Grundverordnung verbessern: Änderungsvorschläge aus Verbrauchersicht. Baden-Baden: Nomos.

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

Rössler, B. (2001): *Der Wert des Privaten*. Suhrkamp.

Schmied, L. und Nebel, M. (2025): Digitale Vulnerabilität und Selbstbestimmung – Vorgaben zur Sicherstellung der Selbstbestimmung vulnerabler Nutzender durch informierte Einwilligung und Rechtspflichten im Behinderten- und Datenrecht, in: Friedewald, M. et al. (Hrsg.): *Freiheit in digitalen Infrastrukturen*, Baden-Baden: Nomos, 107-148.

Sindermann, C.; Schmitt, H. S.; Kargl, F.; Herbert, C.; Montag, C. (2021): Online privacy literacy and online privacy behavior – The role of crystallized intelligence and personality. *International Journal of Human-Computer Interaction*, 37(15), 1455-1466.

Smahel, D.; Machackova, H.; Mawcheroni, G.; Dedkova, L.; Staksrud, E.; Ólafsson, K.; Livingstone, S.; Hasebrink, U. (2020): EU Kids Online 2020: Survey results from 19 countries. EU Kids Online. <http://hdl.handle.net/20.500.12162/5299>

Trepte, S.; Teutsch, D.; Masur, P. K.; Eicher, C.; Fischer, M.; Hennhöfer, A.; Lind, F. (2015): Do people know about privacy and data protection strategies? Towards the "Online Privacy Literacy Scale"(OPLIS). *Reforming European data protection law*, S. 333-365. <https://doi.org/10.1007/978-94-017-9385-8>.

Wang, G.; Zhao, J.; van Kleek, M.; Shadbolt, N. (2022): „Don't make assumptions about me!": Understanding Children's Perception of Datafication Online. *Proceedings of the ACM on Human-Computer Interaction*, 6(CSCW2), Article 419. <https://doi.org/10.1145/3555144>

Wiesemann, J.; Eisenmann, C.; Fürtig, I.; Lange, J.; Mohn, B.E. (2020): Digitale Kindheiten. Kinder-Familien-Medien, in: J. Wiesemann, C.; Eisenmann, I.; Fürtig, J.; Lange, J.; B. E. Mohn (Hrsg.): *Digitale Kindheiten* (pp. 3-17). Springer. https://doi.org/10.1007/978-3-658-31725-6_1

Beteiligte Institutionen



U N I K A S S E L
V E R S I T Ä T



DiversPrivat



UNIVERSITÄT
DUISBURG
ESSEN

Offen im Denken

