

Diversitätsgerechter Privatheitsschutz in digitalen Umgebungen

Heiner Koch, Clara Strathmann, Martin Hennig, Luisa Schmied, Christian L. Geminn, Jessica Heesen, Nicole Krämer und Karoline Reinhardt

Zusammenfassung

Im digitalen Zeitalter ist der Schutz der Privatheit besonders wichtig, doch bestehende Datenschutzmechanismen sind oft unzureichend. Menschen sind unterschiedlich vulnerabel, wenn es um Eingriffe in ihre Privatsphäre geht. Dies hat nicht nur strukturelle Ursachen, sondern ist auch durch individuelle Faktoren bedingt. Die Einwilligung und die damit verbundene informationelle Selbstbestimmung ist ein zentraler Aspekt des Datenschutzes. Ansätze, die sich hier auf „Privacy Literacy“ und die Fähigkeiten des „Durchschnittsnutzenden“ beziehen, sind für vulnerable Personen oft unzureichend. Weder schützt „Privacy Literacy“ immer ausreichend, noch ist diese für vulnerable Personen immer erreichbar. Um ein angemessenes Schutzniveau zu gewährleisten, ist es notwendig, die Vulnerabilität verschiedener Gruppen diversitätsgerecht zu berücksichtigen. Ein neuer Ansatz, der im Rahmen eines BMFTR-Projekts untersucht wird, ist der Einsatz viszeraler Reize, um das Bewusstsein für Privatheitsrisiken zu schärfen.

Empirische Studien und theoretische Überlegungen zeigen, dass der Schutzbedarf und die Vulnerabilität individualisiert betrachtet werden müssen. Anstelle von festen Kategorien wie Geschlecht oder Klasse ist es sinnvoller, mit dem offeneren Begriff der Diversität zu arbeiten. Die Entwicklung diversitätsgerechter Privatheitsunterstützung und die Kommunikation von Wissen über Privatheit an diverse Gruppen sind von großer Bedeutung. Der Schutz besonders vulnerabler Personen in digitalen Umgebungen ist dabei gleichzeitig oft auch ein Schutz aller.

1. Einleitung - Privatheit in digitalen Umgebungen

Deutschland feierte 2024 75 Jahre Grundgesetz; es gilt als Garant für Grund- und Menschenrechte, Demokratie und Rechtsstaatlichkeit und verspricht allen Bürgerinnen und Bürgern gleiche Teilhabe am politischen und gesellschaftlichen Leben. Betrachtet man Privatheitsschutz unter Gerechtigkeits- und Demokratieaspekten, wird insbesondere der Einbezug von marginalisierten und vulnerablen Bevölkerungsgruppen, die oft weniger Einfluss auf öffentliche Debatten und gesellschaftliche Gestaltungsprozesse haben, als notwendig bewertet (Castro Varela/Heinemann 2016). In Bezug auf den Privatheitsschutz besteht für die Gesellschaft insgesamt ein demokratietheoretisch begründetes Interesse an der Wahrung der informationellen Selbstbestimmung, selbst dann, wenn einzelne Personen Daten zu ihrer Person und ihrem Verhalten nicht schützen wollen oder können. Auch das Bundesverfassungsgericht hat die Bedeutung der informationellen Selbst-

bestimmung für die Demokratie von Anfang an betont (BVerfGE 65, 1, Rn.148).

Gerade im digitalen Zeitalter stellt der Schutz der Privatheit eine komplexe Herausforderung dar, die häufig über die bisher bestehenden datenschutzrechtlichen Schutzmechanismen hinausgeht. Unterschiedliche Personen sind unterschiedlich vulnerabel gegenüber Verletzungen ihrer Privat-sphäre. Diese Ungleichheit kann durch größere strukturelle Bedingungen zustande kommen (etwa Diskriminierungen oder ungleicher Ressourcenzugang) aber auch durch sehr individuelle Gründe, die insbesondere auf situations- und kontextabhängiges Nutzungsverhalten zurückzuführen sind (etwa Häufigkeit und Art der Internetnutzung) (Kroschwald 2023, S. 5; Strauß/Bettin 2023, S. 54).

Bestehende Instrumente zum Schutz vulnerabler Gruppen, wie z. B. in Form von Art. 8 DSGVO bezogen auf Kinder, erfassen diesen Schutzbedarf nicht ausreichend differenziert (Roßnagel 2020, S. 88; Roßnagel/Geminn 2020, S. 55 ff.; Geminn 2023, S. 193 ff.). Es bleibt die Notwendigkeit einer adäquaten Adressierung von Vulnerabilität auch von z. B. älteren Menschen oder Personen mit kognitiven Beeinträchtigungen (Geminn 2023, S. 203 ff.). Der klassische Diskriminierungsschutz auf Grundlage von abschließenden Merkmallisten muss um eine Diversitätsperspektive ergänzt werden, die anhand der Vulnerabilitäten im Kontext des konkreten Gegenstandsbereichs entwickelt wird. Ein zentrales Anliegen muss es sein, diversitätsgerecht der Vulnerabilität der Privatheit verschiedener Gruppen Rechnung zu tragen. Ein besserer Schutz vulnerabler Personen kommt dabei letztlich allen zugute.

2. Problemaufriss: Einwilligung als datenschutzrechtliche Legitimationsgrundlage der Verarbeitung personenbezogener Daten

Die Erfassung personenbezogener Daten hat zur Entstehung neuer Geschäftsmodelle geführt, die auf der Erstellung umfassender Identitätsprofile durch Tracking und Profiling der Nutzenden basieren. Neben den Zielen, damit die Kundenbindung zu erhöhen oder personalisierte Werbung zu schalten, entstehen Informations- und Machtasymmetrien (Strauß/Bettin 2023, S. 33, 48). Die digitalisierten Infrastrukturen wirken dabei intrusiv in die Privatsphäre der Menschen hinein und vergrößern damit die Angriffsfläche für Grundrechtseingriffe sowie die Exposition in Hinblick auf Vulnerabilitätsfaktoren (Geminn 2023, S. 172). Als gesetzlich legitime Rechts-

grundlage zur Verarbeitung personenbezogener Daten zu diesen Zwecken kommt in der Regel die Einwilligung zum Tragen. Im Rahmen des Privatheitsschutzes vulnerabler Personen (und nicht nur dort) muss die gängige Praxis der Einwilligung als datenschutzrechtliche Legitimationsgrundlage der Verarbeitung personenbezogener Daten jedoch kritisch hinterfragt werden.

Die Einwilligung gilt als „genuiner Ausdruck der informationellen Selbstbestimmung“ (Roßnagel u. a 2001, S.15, 72; Schulz, in: Gola/Heckmann 2022). Die Betonung der Selbstbestimmung als zentraler Aspekt des Datenschutzes findet sich bereits im Volkszählungsurteil des BVerfG aus dem Jahr 1983, das durch die Konzipierung des Rechts auf informationelle Selbstbestimmung aus Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG dem Einzelnen die Befugnis einräumt, „selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen“ (BVerfGE 65, 1, Rn. 74). Auch aus dem europäischen Grundrecht auf Datenschutz aus Art. 8 Abs.1 der Charta der Grundrechte der Europäischen Union (GRCh) lässt sich ein Recht des Einzelnen auf Selbstbestimmung im Hinblick auf den Umgang mit den ihn betreffenden personenbezogenen Daten ableiten (Kühling/Buchner, in: Kühling/Buchner 2024; Liedke-Deutscher 2024, S. 8; Nebel 2015, S. 517-521). Art. 8 Abs. 2 Satz 1 GRCh nennt die Einwilligung als eigenständigen Rechtfertigungsgrund zur Verarbeitung von Daten. Eine auf Grundlage einer selbstbestimmten, autonomen Entscheidung getroffene Erteilung der Einwilligung kann folglich als Grundrechtsausübung im Sinne der GRCh gesehen werden (Klement, in: Simitis/Hornung/Spiecker gen. Döhmman 2025; Liedke-Deutscher 2024, S. 8).

Zur Umsetzung der grundrechtlichen Vorgaben zum Datenschutz wird die Einwilligung als Rechtsgrundlage zur Verarbeitung personenbezogener Daten in der Datenschutz-Grundverordnung (DSGVO) konkretisiert. Die Wirksamkeitsvoraussetzungen der Einwilligung ergeben sich aus Art. 4 Nr. 11 DSGVO. Für Menschen, die aufgrund struktureller oder individueller Faktoren eine erhöhte Vulnerabilität aufweisen, stellt sich die Frage nach den Voraussetzungen für eine wirksame Einwilligung, insbesondere hinsichtlich der Freiwilligkeit und der Informiertheit, mit besonderer Dringlichkeit. Eine informierte Einwilligung setzt voraus, dass die betroffene Person versteht, dass und in welchem Umfang sie ihre Einwilligung erteilt hat und damit auch z. B. von ihrem Recht auf Widerspruch Gebrauch machen kann. Dies hat der Verantwortliche durch entsprechende Vorkehrungen sicherzustellen (vgl. ErwG 42 Satz 2 DSGVO).

Transparenz kann dabei als zentrale Voraussetzung der Ausübung der informationellen Selbstbestimmung verstanden werden (Albers/Veit, in: BeckOK Datenschutzrecht 2024). Dem Grundsatz der Transparenz aus Art. 5 Abs. 1 lit. a DSGVO folgend, müssen personenbezogene Daten „in einer für die betroffene Person nachvollziehbaren Weise“ verarbeitet werden. Gemäß 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“. Das Transparenzgebot verlangt dabei nicht nur formale Verständlichkeit im Sinne von Lesbarkeit, sondern auch Sinnverständlichkeit (Heberlein, in: Ehmann/Selmayr 2024).

Die Einwilligung prägt das Datenschutzrecht durch einen stark individualistischen Ansatz. Dem liegt die Annahme zugrunde, dass Transparenz und Eigenverantwortung ausreichen, um eine wirksame Einwilligung und damit die Rechtmäßigkeit der Verarbeitung personenbezogener Daten zu gewährleisten (Friedewald u. a 2020, S. 7). Als Bezugspunkt für Verantwortliche wird dazu auf den „Durchschnittsnutzer“ (Artikel-29-Datenschutzgruppe 2018, S. 16) und dessen Privacy Literacy abgestellt. Privacy Literacy bezeichnet das Wissen und die Fähigkeiten, die erforderlich sind, um Datenschutzentscheidungen informiert zu treffen. Sie umfasst verschiedene Dimensionen, darunter prozedurales Wissen (z. B. über Schutzstrategien), Erfahrungswissen (z. B. eigene Erlebnisse mit Datenschutzverletzungen) und Faktenwissen über gesetzliche Grundlagen, technische Datenschutzmaßnahmen sowie Unternehmenspraktiken (Brough/Martin 2020; Trepte u. a 2015). Ein angemessenes Schutzniveau kann auf diesem Wege jedoch zumindest nicht durchgehend gewährleistet werden. Besonders vulnerable Personen, wie z. B. Menschen mit kognitiven Beeinträchtigungen, haben oft nicht die gleichen Voraussetzungen, um informierte Entscheidungen über ihre Daten zu treffen. Das Konzept der Privacy Literacy greift hier zu kurz, da es voraussetzt, dass alle Nutzenden über die notwendigen Ressourcen verfügen können, um sich entsprechend zu informieren. Selbstbestimmung im Datenschutz muss jedoch allen Menschen möglich sein, unabhängig von ihren individuellen Fähigkeiten, sozioökonomischem Hintergrund oder der jeweiligen digitalen Umgebung. Sie darf nicht nur Personen zu Teil werden, die über die notwendigen Mittel verfügen, um sie auszuüben, wie z. B. die Fähigkeit, Datenschutzeinstellungen vorzunehmen oder Datenschutzhinweise zu lesen und zu verstehen (BVerfGE 65, 1, Rn. 148).

Die Gründe für das Fehlen der Informiertheit bei Datenschutzentscheidungen sind so divers wie die Vulnerabilität, die den betroffenen Personen eigen ist. Oftmals wird das Problem in einem Mangel an Privacy Literacy gesehen. Doch Privacy Literacy und das damit verbundene Wissen ist nur eine von vielen notwendigen Ressourcen. Zeit, Geld, digitale Erfahrung und kognitive Kapazitäten spielen eine entscheidende Rolle dabei, ob jemand in der Lage ist, die komplexen Dynamiken der digitalen Marktwirtschaft zu begreifen und entsprechend zu handeln. Während Bildungsangebote zwar einen sicheren Umgang mit dem Internet unterstützen können, stößt das Konzept für einige Bevölkerungsgruppen an seine Grenzen. Nicht alle Menschen können etwa gleichermaßen erreicht werden; andere haben spezielle Bedürfnisse, denen man nicht universell gerecht werden kann. Auch in Bezug auf Einwilligungsfragen muss demnach aus Diversitätsperspektive kritisch untersucht werden, wo Schutzlücken entstehen und wie diese geschlossen werden können. Herkömmliche Ansätze, die auf Privacy Literacy setzen, berücksichtigen dabei oft nicht, dass hierdurch kein angemessenes Schutzniveau für alle Gruppen hergestellt werden kann.

Darüber hinaus wird im Rahmen von Privacy Literacy durch die starke Betonung individueller Verantwortung (Responsibilisierung) die strukturelle Dimension des Privatheitsschutzes ausgeblendet. Viele digitale Dienste und Plattformen sind aber so gestaltet, dass die standardmäßige Datenweitergabe erleichtert und datenschutzfreundliche Alternativen erschwert werden. Solche systematischen Probleme können nicht allein durch individuelle Kompetenzbildung gelöst werden. Vielmehr bedarf es ergänzender Maßnahmen, wie regulatorischer Vorgaben und weniger kognitionsbasierter Ansätze, um ein umfassendes und gerechtes Schutzniveau für alle zu erreichen.

3. Viszerale Reize als mögliche Lösung

Vor dem Hintergrund der oben geführten Diskussion möchten wir den Ansatz der Privacy Literacy zur Unterstützung des Privatheitsmanagements um weniger kognitionsbasierte Möglichkeiten ergänzen. Neue Ansätze wie der Einsatz viszeraler (also körperlich-wahrnehmbarer) Reize könnten das Bewusstsein für Privatheitsrisiken schärfen und Menschen dabei unterstützen, informierte Entscheidungen über ihre Privatsphäre zu treffen (Acquisti u. a. 2022). Dabei geht es z. B. darum, Erfahrungen aus dem Kontext analoger Privatheitsverletzungen auf die Online-Welt zu übertragen, wie

etwa, sich bei einem vertraulichen Gespräch beobachtet zu fühlen, weil eine fremde Person zu nah kommt. Dafür wurde im Kontext von digitaler Privatheit das Konzept der *viszeralen Hinweise* (visceral notice) vorgestellt (Calo 2011). Dabei geht es, im Gegensatz zum traditionellen symbol- und textgeprägten Hinweis, um eine Informationsvermittlung durch Erfahrung bei Gefahr. Ein anschauliches Beispiel dafür findet sich in Baustellensituationen: Um die Verkehrsteilnehmer:innen dort zur Vorsicht aufzurufen, werden Verkehrsschilder aufgestellt, die bildlich oder per Text auf die Notwendigkeit besonderer Aufmerksamkeit hinweisen sollen. Als Alternative bietet sich der Einsatz von Rüttelschwellen an, die unmittelbar „aufrütteln“, ohne kognitiv verarbeitet werden zu müssen und somit einen intuitiveren Charakter innehaben. Calo (2011) unterscheidet dabei zwischen drei Kategorien: Vertrautheit als Warnung, psychologische Reaktion als Warnung, und Zeigen als Warnung. Bei Vertrautheit geht es darum, dass die Nutzenden das Verhalten von bestimmten Technologien kennen und deshalb dasselbe Verhalten in anderen, ähnlichen Interaktionen erwarten. Ein Beispiel dafür sind digitale Kameras, die mit einem Auslösegeräusch ausgestattet sind, das ertönt, wenn ein Foto gemacht wird. Dieses sollte an die analoge Kamera erinnern und so eine Warnung vor potenziellem Eindringen in die Privatsphäre geben. Die Kategorie der psychologischen Reaktion umfasst biologisch bzw. evolutionär bedingte Reaktionen auf bestimmte Designelemente (z. B. die Rüttelschwelle, wobei ein besonderes Aufmerken die Reaktion darstellt). Solche Reaktionen können auch durch die anthropomorphe (also menschenähnliche) Gestaltung von Technologien ausgelöst werden. Dadurch könnten z. B. soziale Skripte getriggert werden, wie dass man sich beobachtet fühlt (Rodriguez-Priego u. a. 2021). Die dritte Kategorie, Zeigen als Warnung, kann gestaltet werden durch konkretes Sichtbarmachen von Konsequenzen, z. B., wie bestimmte Daten genutzt werden. Dadurch sollen die Gefahren, die mit einer bestimmten Entscheidung einhergehen (können), transparenter und anschaulicher gestaltet werden.

Drei Probleme bestehen nun bei dem möglichen Einsatz viszeraler Reize: (i) viszerale Reize können ein paternalistisches „Nudging“ von Privatheitsentscheidungen darstellen, (ii) viszerale Reize sind Teil eines individuellen Selbstschutzes und lösen damit keine strukturellen Probleme und (iii) ob der Einsatz viszeraler Reize wirksam ist, wird sich erst noch zeigen müssen, was jedoch kein konzeptionelles Problem des Ansatzes darstellt.

Grundsätzlich gilt, dass Paternalismus nicht immer falsch sein muss (Birnbacher 2012, S. 564). Paternalismus hat jedoch einen deutlich erhöhten Rechtfertigungsbedarf und muss kontinuierlich auf seine Notwendig-

keit hin untersucht werden. Paternalismusprobleme können auftreten, weil viszerale Reize gerade dazu da sein sollen, eine Schutzlücke durch fehlende Privacy Literacy zu schließen. Privacy Literacy soll jedoch dazu dienen, selbstbestimmte Entscheidung über Privatheitsfragen zu treffen. Viszerale Reize können damit Personen zu Entscheidungen zu drängen, die in ihrem Interesse sind, die sie aber ohne diese Reize anders treffen würden. Damit entsteht eine Offenheit dafür, dass viszerale Reize festlegen, was im Interesse der jeweiligen Personen ist. Zwei Lösungsstrategien sind sinnvoll: erstens sollte den Nutzenden die Möglichkeit gegeben werden einzustellen, welche Privatheitspräferenzen durch viszerale Reize unterstützt werden. Damit wären die Präferenzen zweiter Ordnung berücksichtigt und eine damit verbundene Selbstbestimmung gewährleistet. Zweitens können viszerale Reize auch so gestaltet werden, dass sie einen Beitrag zur Privacy Literacy und damit zum Selbstschutz leisten, beispielsweise, indem sie einen konkreten Bezug zur Gefahrensituation herstellen oder indem man diese um einen Hinweis ergänzt, welcher mehr Informationen anbietet. In diesem Sinne würde es sich dann nicht einfach um Paternalismus handeln, sondern um eine Form des „Mothering“ (Wartenberg 1990, S. 192-193), das die Personen befähigen soll, selbstbestimmte Entscheidungen treffen zu können. Auch Damm (2013, S. 213) weist allgemeiner darauf hin, dass es beim Konflikt zwischen Schutz und Freiheit oder Selbstbestimmung sinnvoll ist, „Fürsorge gerade auch ihrerseits als Instrument der Förderung und „Ermöglichung der Selbstbestimmung“ zu greifen“.

Neben Paternalismus besteht das Problem, dass unter den realen Nutzungsbedingungen keine selbstbestimmten Entscheidungen über Privatheit getroffen werden können. Entweder wird gar nicht erst eine Entscheidungsmöglichkeit angeboten oder die Entscheidung ist zu komplex und zeitaufwendig, als dass diese wirklich getroffen werden könnte. Dort, wo schon Privacy Literacy keine Lösung ist (Hagendorff 2018), kann auch ein viszeraler Reiz, der die individuellen Entscheidungen unterstützen soll, keine Lösung sein. Regulierungen und gesetzliche Vorgaben bleiben damit ein unverzichtbares Instrument des Schutzes vulnerabler Personen. Viszerale Reize sollten damit in diesen Kontexten nicht zu einer Rechtfertigung individueller und eigenverantwortlicher Lösungen werden (Responsibilisierung). Gleichzeitig wäre es jedoch auch ein fragwürdiger Paternalismus, wenn durch Regulierungen vulnerablen Personen grundsätzlich die Entscheidungsmöglichkeiten genommen würden. Vulnerablen Personen gesellschaftliche Teilhabe zu nehmen, indem ihnen etwa der Zugang zu sozialen Medien untersagt wird (etwa das Verbot für unter 16-Jährige, soziale

Medien zu nutzen), ist ethisch problematisch. Gesellschaftliche Teilhabe bedeutet immer auch ein gewisses Maß an Vulnerabilität, bei dem ein paternalistischer Schutz, der mit dieser Vulnerabilität auch die gesellschaftliche Teilhabemöglichkeit beseitigt, Freiheit zu sehr beschränken kann.

Zuletzt muss sich empirisch zeigen, ob viszerale Reize tatsächlich eine geeignete Lösung für Schutzlücken durch eine fehlende Privacy Literacy sein können. Es besteht hier die Gefahr, dass technische Innovationen Lösungen für soziale Probleme sein sollen. Bei der Evaluation viszeraler Reize sind damit Fragen des Paternalismus, der Responsibilisierung und der Eignung technischer Lösungsansätze zu berücksichtigen.

4. Notwendigkeit einer kontextbezogenen Diversitätsperspektive

4.1 Empirische Evidenzen

Um zunächst zu verstehen, welchen Schutzbedarf unterschiedliche vulnerable Gruppen im Umgang mit ihrer Privatsphäre im Internet haben, wurden insgesamt neun Fokusgruppen durchgeführt. Dabei wurden drei besonders vulnerable Kohorten miteinbezogen: Grundschulkinder, Senior:innen sowie Personen mit kognitiven Beeinträchtigungen. Zwei Gruppen mit Personen zwischen 18 und 65 dienten darüber hinaus als Vergleichsgruppe. Innerhalb der Fokusgruppen wurde eruiert, inwiefern bei den Teilnehmenden ein Bewusstsein für systematische Datensammelpraktiken von Unternehmensseite vorliegt. Darüber hinaus sollte ein Eindruck darüber gewonnen werden, welcher Risiken und Schutzmaßnahmen sich die Teilnehmenden bewusst sind, wobei der Einsatz von Cookie-Bannern als Mechanismus zum Schutz der eigenen Daten diskutiert wurde. Zuletzt wurden die Teilnehmenden dazu ermuntert, eigene Ideen für den Schutz vor Privatsphärisiken zu generieren.

Die Analyse des Bewusstseins für und Wissens der Teilnehmenden über Datenschutz ergab ein diverses Bild. Kinder beispielsweise attribuierten Datensammelpraktiken eher auf einer horizontalen Ebene (z. B. in Bezug auf Influencer:innen, die mit erhöhten Zuschauer:innenzahlen mehr Geld verdienen könnten). Unter den Personen mit kognitiven Einschränkungen zeigte sich das diverseste Spektrum an Wissen: von Einzelnen, die schon mal von der Sammlung persönlicher Daten gehört hatten, bis hin zu jenen, die sich nicht vorstellen konnten, dass YouTube auf irgendwelche Informationen über sie zugreifen kann oder diese gar sammelt (oft begründet

im mangelnden Verständnis des Werts von Daten). Bei den Senior:innen beobachteten wir, dass Teile ihres Verständnisses auf populären Gerüchten basierten, so etwa, dass das eigene Handy einen ständig belausche und auf Basis des Gehörten entsprechende Werbung geschaltet würde. Andererseits hatte diese Gruppe von den drei untersuchten vulnerablen Gruppen das höchste Bewusstsein dafür, dass große Firmen wie Google Zugang zu verschiedenen Datenquellen haben und, dass Werbeunternehmen auf Basis verschiedener Nutzer:innendaten personalisierte Empfehlungen ausgeben können. Das Wissen der Senior:innen stieß dann an seine Grenzen, wenn es um komplexere Prozesse wie Big Data oder Algorithmen ging, was üblicherweise bereits weit über das Verständnis der Kinder und Personen mit kognitiven Einschränkungen hinausging. Bei diesen ließ sich beobachten, welchen Wert physische Greifbarkeit in Privatheitsvorstellungen hat: So äußerten einige Kinder, man könne Datensammlungen durch das Zerstören eines entsprechenden Geräts verhindern. Auch bei den Personen mit kognitiven Einschränkungen zeigte sich allenfalls ein grundlegendes Verständnis. So beobachteten manche beispielsweise, dass die Google-Suche nach einem Produkt oft zu Werbung für diesen oder ähnliche Konsumartikel führt. Andere erkannten, dass ein Zusammenhang zwischen dem aktuellen Video auf YouTube und den personalisierten Empfehlungen am Rand der Seite besteht.

Darüber hinaus fiel die Attribution der Verantwortung im Hinblick auf Privatheitsschutz im Internet unterschiedlich aus. Sowohl bei den Kindern als auch bei den Personen mit kognitiven Beeinträchtigungen standen Hilfestellungen bei der Navigation der eigenen Privatheit durch Vertrauenspersonen im Vordergrund. Das Verständnis für die Verletzung der Privatheit durch Institutionen oder Unternehmen unterschied sich stark interindividuell, war aber gerade in diesen Gruppen durchschnittlich gering und spiegelte teils wider, was von Vertrauenspersonen übernommen worden war. So war einigen Personen bekannt, dass Cookies abgelehnt werden sollten, worum es sich dabei allerdings handele und warum sie abgelehnt werden sollten, entzog sich oft dem allgemeinen Verständnis. Senior:innen auf der anderen Seite lokalisierten die Verantwortung tendenziell bei sich und dem eigenen Wissen. Im Vergleich zu den beiden vorgenannten Gruppen wurde zwar gelegentlich der Wunsch nach einer externen Schutzinstanz geäußert, die das Individuum um die eigene Verantwortung erleichtern solle (ähnlich wie bei den Vergleichsgruppen), diese Möglichkeit wurde aber tendenziell als nicht umsetzbar wahrgenommen. Bildungsangebote wurden insbesondere von den Senior:innen als wertvoll betrachtet und am ehesten

als realistische externe Schutzmöglichkeit angesehen. Grundsätzlich fand sich in dieser Gruppe jedoch auch ein starker Bezug auf die eigene Lebenserfahrung, der ein großer Stellenwert im Hinblick auf das Erkennen von und den Umgang mit Gefahren zugeschrieben wurde.

Im Zusammenhang mit den Fokusgruppen hat sich empirisch gezeigt, dass es sinnvoll sein kann, Schutzbedarf und Vulnerabilität individualisierter zu denken. Diese Position soll im Folgenden - insbesondere für den Privatheitsbereich - auch theoretisch begründet werden.

4.2 Vulnerabilität und Privatheit

Oft wird angenommen, dass Menschen einerseits universell vulnerabel sind, aber andererseits auch partikulare Personengruppen oder einzelne Personen eine besondere Vulnerabilität aufweisen (Albertson Fineman 2017). Vulnerabilität bedeutet, dass Personen sich nicht allein schützen können und damit einen Schutzbedarf haben. Zunehmend wird hierbei Vulnerabilität auch im Privatheitsbereich diskutiert (Geminn 2023; Behrendt/Loh 2022). Insofern Personen ein Interesse an informationeller Selbstbestimmung haben und sich nicht allein und mit absoluter Sicherheit schützen können, sind sie in dieser Hinsicht vulnerabel. Damit ist auch klar, dass Personen immer nur in bestimmten Hinsichten besonders vulnerabel sind. Vulnerabel im Bereich der Privatheit zu sein bedeutet etwa nicht, auch im Gesundheitsbereich vulnerabel zu sein.

Privacy Literacy beispielsweise kann die Vulnerabilität im Privatheitsbereich abschwächen, aber nicht beseitigen. Während wir eine gewisse Vulnerabilität im Privatheitsbereich universell teilen, bestehen jedoch auch wichtige Unterschiede darin, wie ausgeprägt vulnerabel die einzelnen Personen sind. Eine ungleiche Verteilung von Privacy Literacy kann zu einer solchen ungleichen Vulnerabilität führen. Auch kann die gleiche Verletzung der informationellen Selbstbestimmung sehr unterschiedliche Konsequenzen nach sich ziehen. So ist es ungleich problematischer, wenn die Gesundheitsdaten einer kranken Person ungewollt zugänglich werden, als wenn dies bei einer gesunden Person passiert. Weiterhin kann das Ausmaß, in dem Personen Gefahren ausgesetzt sind, sehr unterschiedlich verteilt sein. Personen des öffentlichen Lebens etwa sind oft dauerhaft intensiven Angriffen auf ihre Privatsphäre ausgesetzt.

Zumindest zwei Probleme treten hierbei jedoch auf: erstens kann Privacy Literacy unzureichend sein, um sich zu schützen. Zweitens ist es

verschiedenen Personengruppen erschwert, eine hinreichende Privacy Literacy zu erwerben.

Schon auf der Ebene von Privacy Literacy liegt nicht nur ein einziger Mechanismus vor, der dazu führt, dass diese nicht ausreicht, um sich angemessen schützen zu können. Dass Probleme und die betroffenen Personengruppen vielfältig sind, bedeutet jedoch nicht automatisch, dass die Lösungsansätze genauso vielfältig sein müssen. Wird etwa durch Regulation die Erhebung von Daten durch Unternehmen in einem bestimmten Bereich effektiv untersagt, so wird durch diesen Schutz eine bestimmte Form der Vulnerabilität mindestens deutlich abgeschwächt. Auch Verfahren zum Schutz von partikularen Vulnerabilitätsgruppen können dazu geeignet sein, auch andere Gruppen zu schützen. Während die viszerale Reize, die wir in diesem Kontext diskutieren, dazu entwickelt werden, Privacy Literacy-Probleme bei Personen mit eingeschränkten kognitiven Fähigkeiten zu bewältigen, können diese viszerale Reize auch für andere Personen geeignet sein, sie bei dem Schutz ihrer Privatsphäre zu unterstützen.

Für den Privatheitsbereich stellen außerdem die Einwilligung und die damit verbundenen Aspekte der Informiertheit und Freiwilligkeit einen wesentlichen Bereich der Vulnerabilität dar. In Bezug auf Freiwilligkeit lässt sich im Anschluss an Kiener (2023) argumentieren, dass sich diese nur in konkreten Interaktionen zwischen der Person, die die Einwilligung erteilt und der einwilligungserhaltenden Stelle feststellen lässt. Dies bedeutet auch, dass Vulnerabilitäten auf den ganz konkreten Interaktionskontext bezogen sein müssen. Erst wenn diesen Vulnerabilitäten angemessen von der einwilligungserhaltenden Stelle begegnet worden ist, kann überhaupt von Freiwilligkeit in diesem Interaktionskontext ausgegangen werden. Dies lässt sich analog auch auf die Informiertheit übertragen. Auch hier gibt es Anforderungen des konkreten Interaktionskontextes, denen begegnet werden muss, damit Vulnerabilitäten in Bezug auf Informiertheit die Einwilligung nicht ungültig werden lassen. Insofern die Verschiedenheit der einzelnen Interaktionen bei Einwilligungen in Datennutzung relevant sind, stützt dies die Anforderung, Vulnerabilität anhand kontextspezifischer Kriterien zu entwickeln.

4.3 Kategorienbildung und Vulnerabilität

Verbreitet ist die Annahme, dass Vulnerabilitäten sich nicht anhand von festen vorgegebenen Kategorien feststellen lassen, sondern individuelle

Eigenschaften sind (Birnbacher 2012, S. 561). Damit soll über Vulnerabilität eine moralisch richtige Einschätzung von Einzelfällen stattfinden und eine Einzelfallgerechtigkeit erreicht werden können (Damm 2013, S. 212). Gruppenkategorien können jedoch auch im Bereich der Vulnerabilität aus später noch diskutierten Gründen unverzichtbar sein. Dabei bleibt jedoch festzuhalten, dass Personen, die zu einer dieser Gruppen gehören, nur mit einer höheren Wahrscheinlichkeit eine größere Vulnerabilität aufweisen (Birnbacher 2012, S. 561). Einzelne Gruppenmitglieder können durch eine geringere Vulnerabilität gekennzeichnet sein und genauso können auch Personen, die nicht in eine dieser Gruppenkategorien fallen, eine höhere Vulnerabilität aufweisen.

Wie können wir nun über die partikularen Vulnerabilitäten sprechen? In der Vergangenheit wurde dies oft anhand von Kategorien getan (klassisch etwa Geschlecht, Klasse und „Rasse“), die wir auch aus dem Diskriminierungskontext kennen (kritisch hierzu: Luna 2009, S. 124-125). Albertson Fineman (2017) argumentiert, dass Diskriminierungsansätze davon ausgehen würden, dass Menschen gleichbehandelt werden müssten und nur bestimmte diskriminierte Gruppen einen Schutzbedarf hätten. Damit werde ignoriert, dass einerseits alle vulnerabel seien und andererseits eine Gleichbehandlung nicht genüge, um spezifischen Vulnerabilitäten zu begegnen. Anstelle individueller Gleichbehandlung zur Vermeidung von Diskriminierung benötige es aktive staatliche Schutzmaßnahmen, die die Vulnerabilität aller und gleichzeitig auch die je spezifischen und kontextabhängigen besonderen Vulnerabilitäten bestimmter Gruppierungen vermindere. Insofern auf partikulare Vulnerabilität abgezielt werde, würde jedoch nur das Paradigma der Diskriminierung aufgerufen, ohne die universelle Vulnerabilität und die damit erforderlichen systemisch-strukturellen Aspekte zu thematisieren (Albertson Fineman 2017, S. 133). Solange die universelle Vulnerabilität berücksichtigt wird und nicht einfach auf Gleichbehandlung abgezielt wird, ist trotz Albertson Finemans Kritik die Thematisierung partikularer Vulnerabilitäten in bestimmten Fällen notwendig und angemessen.

Insofern jedoch Diskriminierungskategorien zur Thematisierung der Vulnerabilitäten herangezogen werden, bleiben weitere Probleme bestehen. Diese Diskriminierungskategorien sind sehr grob und werden den tatsächlichen partikularen Vulnerabilitäten nicht gerecht. Es entsteht die Gefahr, dass die Vulnerabilität von Personen, die nicht in diese Kategorien fallen, übersehen wird und die Vulnerabilität von Personen in einer solchen Kategorie essentialisiert wird (Martin 2023, S. 23; Luna 2009, S. 123). Personen, die sich – insbesondere in autoritären Regimen – politisch engagieren,

sind beispielsweise besonders vulnerabel in Bezug auf ihre informationelle Selbstbestimmung, ohne dass diese Personen von klassischen Diskriminierungskategorien erfasst werden. Gleichzeitig kann es sein, dass Menschen mit Lernschwierigkeiten zwar durchschnittlich eine höhere Vulnerabilität im Privatheitsbereich aufweisen, dies aber nicht auf jede Einzelperson dieser Gruppe zutreffen muss und sich dies auch bei einzelnen Personen dieser Gruppe im Laufe der Zeit ändern kann. Daher lehnen etwa Albertson Fineman (2017) und Luna (2009) solche Vulnerabilitätskategorien ab. Damit stellt sich jedoch die Herausforderung, diejenigen Personen zu benennen, die besonders vulnerabel sind und eines besonderen Schutzes bedürfen (Wrigley 2014, S. 6).

Intersektionale Ansätze sehen das Problem und thematisieren daher Überschneidungen dieser Kategorien, die zu eigenständigen Formen der Vulnerabilität führen. Linabary und Corple (2019) zeigen dies etwa anhand unterschiedlicher Erfahrungen, die Frauen in Bezug auf Online-Belästigungen im Kontext von Wikipedia machen, je nachdem, welche Überschneidungen mit weiteren Merkmalen vorliegen. Damit gelingt es, ein komplexeres Bild der Wirklichkeit zu erhalten. Es bleibt jedoch das Problem, dass auch intersektionale Ansätze oft bei typischen Diskriminierungskategorien und deren Überschneidungen stehen bleiben. Damit bleibt auch die Abbildung von Wirklichkeit in diesen Kategorien verhaftet. Die Kategorien werden nicht anhand von Vulnerabilitäten im Bereich der Privatheit entwickelt, sondern entlang großer gesamtgesellschaftlicher Benachteiligungen. Auch intersektionale Ansätze können damit die Vielfältigkeit der Vulnerabilitäten im Privatheitsbereich nicht unbedingt abbilden.

Hier bietet es sich an, stattdessen mit dem offeneren Begriff der Diversität zu arbeiten. Diversitätskategorien können zwar auch über endliche Listen gegeben sein (siehe etwa die „4 Layers of Diversity“ von Gardenswartz/Rowe 2003), doch Diversität kann auch als grundsätzlich offen verstanden werden. Dies würde die Entwicklung von Diversitätskategorien in Auseinandersetzung mit Vulnerabilitäten im Privatheitsbereich erlauben. Diversität hat jedoch den Nachteil, dass, anders als bei Diskriminierung und Intersektionalität, die moralische Problemdimension ausgeblendet wird. Diversität begründet schließlich noch keinen Schutzbedarf. Daher ist die Kombination von Diversität mit Vulnerabilität besonders geeignet, wenn man ohne Vorannahmen über Kategorien ethische Probleme im Privatheitsbereich thematisieren will. Die Diversitätskategorien, mit denen sich Vulnerabilitäten im Privatheitsbereich beschreiben lassen, müssen

dementsprechend in Auseinandersetzung mit dem konkreten Gegenstandsbereich entwickelt werden.

4.4 Gleichheit und Schutzbedarf

Ethisch gesehen ist es von besonderer Relevanz, um welche Vulnerabilitäten es gehen soll. Oft wird eine besondere Vulnerabilität thematisiert, sei es durch eine erhöhte Schadenswahrscheinlichkeit oder einen erhöhten Schaden (Racine/Bracken-Roche 2019), welche einen Schutzbedarf oder eine Schutzpflicht nach sich ziehen. Als Vergleichsgröße können „normale Situationen“ oder „normale Personen“ herangezogen werden. Dies ist jedoch problematisch, da es eine solche „Normalität“ für gewöhnlich nicht gibt und diese außerdem als eine Art normativer Standard gelesen werden könnte (Koch 2014). Ein weiteres Problem ist, dass schon „normale“ Risiken nicht akzeptabel sein müssen und deshalb auch bei „normalen“ Risiken schon ein Schutzbedarf bestehen kann. Dies ist im Privatheitsbereich offensichtlich: insofern etwa große Technologiekonzerne systematisch einen defizitären Datenschutz realisieren, ist die überwältigende Mehrheit bei der alltäglichen Nutzung von sozialen Medien im Bereich der informationellen Selbstbestimmung vulnerabel. Insofern Vulnerabilitätstheorien im Privatheitsbereich Anwendung finden sollen, muss dieses verbreitete und alltägliche Risiko miterfasst werden können.

Wenn es ethisch also darum geht, einen Schutzbedarf festzustellen, dann kann es hierbei weder allein um einfache Gleichheit (etwa ein gleiches, aber zu geringes Schutzniveau), noch um irgendeine Form der „Normalität“ gehen. Stattdessen muss es um ein ethisch begründetes maximales Risiko gehen, dem Menschen bei ihrer gesellschaftlichen Teilhabe ausgesetzt sein dürfen. Wird dieses maximale Risiko überschritten und damit die gesellschaftliche Teilhabe gefährdet, so besteht ein Schutzbedarf. Darüber hinaus müssen selbstverständlich auch Ungleichheiten thematisiert werden. Vulnerabilität erlaubt es einerseits, Mindeststandards einzufordern, und andererseits Ungleichheiten zu problematisieren. Der Schutzbedarf kann hierbei unabhängig von vorgegebenen Kategorien in der konkreten Auseinandersetzung mit dem Gegenstandsbereich ergründet werden.

4.5 Grenzen individualisierter Ansätze

Während Vulnerabilität durch die Vermeidung klassischer Kategorienbildung eine Einzelfallgerechtigkeit gewährleisten soll, gehen mit diesem Ansatz auch Nachteile einher, die eine solche Kategorienbildung dennoch notwendig machen kann. Hierzu gehört die Aggregation von Benachteiligungen, eine erschwerte politische Organisation entlang von Kategorien, eine fehlende Komplexitätsreduktion und eine individualisierte Verantwortung, Vulnerabilitäten zu begegnen, die auch zu einer geringeren Rechtssicherheit führen kann. Darüber hinaus weisen Davis and Aldieri (2021) auch darauf hin, dass Vulnerabilität zu unspezifisch sei, eine positive Deutung offenlasse und zumindest in Albertson Finemans Lesart zu sehr auf staatliche Schutzmaßnahmen hinauslaufe. Dabei sei es gerade der Staat, der mit seinen Schutzmaßnahmen oft vulnerable Gruppen schädigt oder deren Vulnerabilität erzeuge oder verstärke.

Vulnerabilität und Diversität erlauben es zwar, sachgerechtere und kontextspezifische Analysen eines Schutzbedarfes im Privatheitsbereich durchzuführen, doch dies darf nicht bedeuten, die größeren gesellschaftlichen Diskriminierungsstrukturen zu vernachlässigen. Dies liegt daran, dass aggregierte Benachteiligungen aus verschiedenen Bereichen eine besondere Last darstellen können, die es zu berücksichtigen gilt. Eine queere Person, die über eine besonders hohe Privacy Literacy verfügt, mag keine besondere Vulnerabilität aufweisen, wenn man allein den Privatheitsbereich betrachtet. Ist jedoch klar, dass diese Person in anderen Lebensbereichen diskriminiert wird und Vulnerabilitäten aufweist, kann selbst eine vergleichsweise geringe Vulnerabilität im Privatheitsbereich eine unzumutbare zusätzliche Belastung darstellen, die einen Schutzbedarf nach sich zieht.

Diskriminierungskategorien anstelle von kontextspezifischen Vulnerabilitätskategorien zu verwenden kann auch dann notwendig sein, wenn die Einzelfälle zu komplex sind, um diesen jeweils Rechnung tragen zu können. (Intersektionale) Diskriminierungskategorien zu verwenden, kann damit auch im Privatheitsbereich eine pragmatisch gerechtfertigte Entscheidung sein. So ist etwa kaum möglich, bei der Nutzung jeder Internetseite eine umfassende Einzelfallprüfung von kontextspezifischen Vulnerabilitäten vorzunehmen.

Ein weiteres Problem bei dem Bezug auf Vulnerabilität besteht darin, dass politische Organisationen entlang von Vulnerabilität schlechter funktionieren könnten, als wenn sich entlang großer gesellschaftlicher Diskri-

minierungsachsen organisiert wird. Dies ist bereits im Zusammenhang mit intersektionalen Analysen ein bekanntes Problem (Koch 2013).

Die Abhebung auf individuelle Vulnerabilitäten kann außerdem dazu führen, dass keine allgemeinen Schutzvorkehrungen getroffen werden können, sondern individualisierte Lösungen angestrebt werden. Dies könnte jedoch bedeuten, dass es etwa bei Einwilligungen in Datennutzung die einwilligungserhaltende Stelle ist, die die individuelle Vulnerabilität feststellen und für den Einzelfall angemessenen Schutzmaßnahmen treffen muss. Dies lässt jedoch viel Willkürspielraum zu, der letztendlich zu einem geringeren Schutzniveau führen könnte. So weist Damm (2013, S. 213) zurecht darauf hin, dass es bei Einzelfallgerechtigkeit und Kategorienbildung zentral darauf ankommt, welcher Ansatz ein höheres Schutzniveau gewährleisten kann.

5. Fazit

Insgesamt verdeutlichen unsere ersten Befunde, dass ein effektiver Privatheitsschutz eine interdisziplinäre Herangehensweise erfordert. Nur so kann sowohl ethisch fundiert als auch rechtlich gestützt ein Ansatz gefunden werden, welcher empirisch geprüft den Weg zu einem diversitätsgerechten Privatheitsschutz ebnen kann.¹

Um einen effektiven Privatheitsschutz zu gewährleisten, sind zielgruppengerechte und auf die individuellen Nutzenden zugeschnittene Ansätze erforderlich. Hier hat sich gezeigt, dass rechtliche und ethische Debatten, die an allgemein bestehende Benachteiligungskategorien anknüpfen, oft zu kurz greifen. Stattdessen ist es zielführender, mit den Ansätzen von Diversität und Vulnerabilität zu arbeiten, da diese erlauben, die Vielfältigkeit

1 Zusätzlich kann der Bereich der Kommunikation von Wissensbeständen über Privatheit an diverse Gruppen von einem integrativen Ansatz profitieren, der vulnerable Gruppen stets im Wissenschaftsdialog mitdenkt. In der Empirie und Theorie (vgl. Schrögel et al. 2018) wird deutlich, dass Bedarf besteht, grundlegende Zusammenhänge stärker auch für Personen mit wenig Vorwissen oder kognitiven Beeinträchtigungen zugänglich zu machen. Eine inklusive Wissenschaftskommunikation fördert dabei nicht nur die Demokratisierung des Wissens, sondern verbessert im besten Fall auch die Qualität und Relevanz von Forschung. Statt einer Konzeption von Wissenschaft als objektiv und universell, als Vermittlung von ‚reinen‘ Fakten, geht es bei einem solchen Verständnis um die Berücksichtigung von Perspektivität, Praxiswissen und dezentraler Wissensbestände. Das Projekt *DiversPrivat* arbeitet auch in dieser Hinsicht an entsprechenden Vorschlägen und Maßnahmen.

des Schutzbedarfs abzubilden. Hierbei sind Kategorien erst anhand der Gefahren und Schutzbedarfe in den konkreten Situationen zu entwickeln. Gerade Privacy Literacy und das Abstellen auf „Durchschnittsnutzende“ wird den konkret vorliegenden Vulnerabilitäten und Schutzbedarfen nicht gerecht. Viszerale Reize könnten hierbei ein Ansatz sein, um Grenzen der Privacy Literacy zu begegnen. Doch auch viszerale Reize sind dort keine Lösungen, wo strukturelle oder regulatorische Ansätze anstelle individualisierter Lösungen notwendig sind. Viszerale Reize könnten jedoch nicht nur bestimmte vulnerable Personen mit geringer Privacy Literacy bei der Wahrung ihrer Privatheit unterstützen, sondern grundsätzlich alle. Der Schutz besonders vulnerabler Personen ist schließlich oft auch ein Schutz aller.

Danksagung

Diese Arbeit wurde im Rahmen des vom BMFTR geförderten Projekts *DiversPrivat* (Förderkennzeichen: 16KIS1879) durchgeführt.

Literatur

- Acquisti, Alessandro; Brandimarte, Laura und Hancock, Jeff (2022): How privacy's past may shape its future. *Science*, 375, S. 270-272. <https://doi.org/10.1126/science.abj0826>
- Albertson 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>
- Aktikel-29-Datenschutzgruppe (2018): Leitlinien in Bezug auf die Einwilligung gemäß Verordnung 2016/679. Working Paper 259 rev. 01. Brüssel. URL: https://www.datenschutz-bayern.de/datenschutzreform2018/wp259rev01_de.pdf.
- 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>.
- Birnbacher, Dieter (2012): Vulnerabilität und Patientenautonomie – Anmerkungen aus medizinethischer Sicht. *MedR*, 30(9), S. 560–565. <https://doi.org/10.1007/s00350-012-3223-1>.
- Brough, Aaron R. und Martin, Kelly 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, Ryan (2011): Against notice skepticism in privacy (and elsewhere). *Notre Dame L. Rev.*, 87, S. 1027.
- Castro Varela, María do Mar und Heinemann, Alina (2016): Globale Bildungsbewegungen – Wissensproduktionen verändern. *ZEP: Zeitschrift für internationale Bildungsforschung und Entwicklungspädagogik*, 39(2), S. 17–22. <https://doi.org/10.25656/01:15447>.

- Damm, Reinhard (2013): Vulnerabilität als Rechtskonzept? *Medizinrecht*, 31(4), S. 201–214. <https://doi.org/10.1007/s00350-013-3389-1>.
- Davis, Benjamin P. und Aldieri, Eric (2021): Precarity and Resistance: A Critique of Martha Fineman's Vulnerability Theory. *Hypatia*, 36(2), S. 321–337. <https://doi.org/10.1017/hyp.2021.25>.
- Gardenswartz, Lee und Rowe, Anita (2003): *Diverse teams at work. Capitalizing on the power of diversity*. Alexandria, Virginia, USA.: Society for Human Resource Management.
- Geminn, Christian L. (2023): *Deus ex machina? Grundrechte und Digitalisierung*. Tübingen: Mohr Siebeck.
- Hagendorff, Thilo (2018): Privacy Literacy and Its Problems. *Journal of Information Ethics*, 27(2), S. 127–145.
- Kiener, Maximilian (2023): *Voluntary consent. Theory and practice*. New York: Routledge Taylor & Francis.
- Koch, Heiner (2013): Gemeinsame antipatriarchale Kämpfe und die Ontologie von Gender und Herrschaft. *Kollektivität nach der Subjektkritik. Geschlechtertheoretische Positionierungen*, 153–176.
- Koch, Heiner (2014): Probleme der Normalisierung. In: Regina Ammicht Quinn (Hg.): *Sicherheitsethik*. Wiesbaden: Springer VS (Studien zur Inneren Sicherheit, Band 16), S. 167–181.
- 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.
- Liedke-Deutscher, Bernd (Hrsg.): (2024): *Die datenschutzrechtliche Einwilligung nach der DSGVO*. Oldenburg: OIWIR.
- Linabary, Jasmine R. und Corple, Danielle 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, Florencia (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, Angela K. (2023): *The Moral Implications of Human and Animal Vulnerability*. Cham: Springer International Publishing.
- Nebel, Maxi (2015): Schutz der Persönlichkeit – Privatheit oder Selbstbestimmung? Verfassungsrechtliche Zielsetzungen im deutschen und europäischen Recht. *Zeitschrift für Datenschutz*, 11/2015, S. 517–521.
- Racine, Eric und Bracken-Roche, Dearbhail (2019): Enriching the concept of vulnerability in research ethics: An integrative and functional account. *Bioethics*, 33(1), S. 19–34. <https://doi.org/10.1111/bioe.12471>.
- Rodriguez-Priego, Nuria; van Bavel, René, und Monteleone, Shara (2021): Nudging online privacy behaviour with anthropomorphic cues. *Journal of Behavioral Economics for Policy*, 5(1), 45–52.

- 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_GarstkaPfitzmannRosnagel_Modernisierung_des_Datenschutzrechts.pdf (besucht am 27.02.2025).
- Roßnagel, Alexander; Bile, Tamer; Nebel, Maxi; Gemin, 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): White Paper Einwilligung. Möglichkeiten und Fallstricke aus der Konsumentenperspektive. Karlsruhe: Fraunhofer ISI. URL: <https://doi.org/10.24406/publica-fhg-300317>.
- Roßnagel, Alexander und Gemin, Christian (2020): *Datenschutz-Grundverordnung verbessern: Änderungsvorschläge aus Verbrauchersicht*. Baden-Baden: Nomos.
- Roßnagel, Alexander (2020): Der Datenschutz von Kindern in der Datenschutz-Grundverordnung: Vorschläge für die Evaluierung und Fortentwicklung. *Zeitschrift für Datenschutz (ZD)*, S. 88.
- Schrögel, Philipp; Humm, Christian; Leßmöllmann, Annette; Kremer, Bastian; Adler, Jona und Weißkopf, Markus (2018): Nicht erreichte Zielgruppen in der Wissenschaftskommunikation: Literatur-Review zu Exklusionsfaktoren und Analyse von Fallbeispielen. Berlin: Wissenschaft im Dialog gGmbH; Karlsruher Institut für Technologie (KIT), Institut für Technikzukünfte (ITZ), Teilinstitut Wissenschaftskommunikation. URL: <https://doi.org/10.5445/IR/1000094529>.
- Strauß, Stefan und Bettin, Steffen (2023): Digitalisierung, Vulnerabilität und (kritische) gesellschaftliche Infrastrukturen. Wien: Institut für Technikfolgen-Abschätzung der Österreichischen Akademie der Wissenschaften. <https://doi.org/10.1553/ITA-pb-2023-01>.
- Trepte, Sabine; Teutsch, Doris; Masur, Philipp K.; Eicher, Christopher; Fischer, Mona; Hennhöfer, Alisa und Lind, Fabienne (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>.
- Wartenberg, Thomas E. (1990): *The forms of power: From domination to transformation*. Philadelphia, USA: Temple University Press, U.S.
- Wrigley, Anthony (2014): An Eliminativist Approach to Vulnerability. *Bioethics*, 29(7), S. 478-487. <https://doi.org/10.1111/bioe.12144>

