Risiko

Carsten Orwat

(Preprint) erscheint in: Digitalität von A bis Z,
hrsg. von Florian Arnold, Johannes C. Bernhardt,
Daniel Martin Feige und Christian Schröter

Die Gegenwart ist von regelrechten Schüben der Digitalisierung geprägt. Damit einhergehend haben die Risiken der digitalen Technologien zugenommen und nehmen weiter zu: von Problemen für die informationelle Selbstbestimmung über die Substitution von Menschen durch Automatisierung bis hin zu Risiken für fast alle Grundrechte und Grundwerte wie Rechtsstaatlichkeit, Demokratie, nachhaltige Entwicklung oder wirtschaftlicher Wettbewerb. Die Entwicklungen haben viel mit dem Anwachsen digitaler Daten zu tun: Vor allem die Aneignung personenbezogener Daten als „Nebenprodukt" der Nutzung von Produkten und Diensten ist hervorzuheben, etwa bei Webseitenbesuchen, Nutzung von Sprachassistenten, digitalisierten Gegenständen wie Automobilen und, allgemein, durch das Internet der Dinge und digitalisierte Umgebungen wie *Smart Cities*. Auch das auf Gegenleistung beruhende Geschäftsmodell der Preisgabe personenbezogener Daten für die kostenlose Nutzung von Diensten hat stark zum Datenwachstum beigetragen. Das Anwachsen von datenbasierten Personen- und Gruppenprofilen erhöht Risiken der Informationsmacht, der Einschränkung der (informationellen) Selbstbestimmung und Missachtung der Menschenwürde. Ermöglicht wurde dies nicht zuletzt durch verbesserte Möglichkeiten der Kombination und Auswertung von sehr großen, auch heterogenen (strukturierten und unstrukturierten) Datenmengen (*Big Data*). Durch Datenakkumulation, Verkettung bzw. Weiterverwendungen, Aufweichung der Zweckbindungen oder Datenverarbeitungen nach sogenanntem berechtigtem Interesse sind extreme Informationsasymmetrien zwischen Datenverarbeitenden und Betroffenen entstanden.

Von der Daten- zur Risikoentgrenzung

Große Datenmengen und Fortschritte beim Maschinellen Lernen bieten die Möglichkeit, automatisiert Muster in Daten zu finden und diese mit Hilfe von Algorithmen etwa für die Differenzierung von Personen, zur Erkennung von optischen Mustern bei Menschen, anderen Lebewesen oder Gegenständen zu nutzen oder als Wortmuster in Sprachmodellen zur Erzeugung von synthetischen Inhalten zu verwenden. Dadurch wird zugleich die Identifikation und Nutzung neuer persönlichkeitsrelevanter Merkmale möglich, beispielsweise über emotionale Zustände, politische oder sexuelle Orientierungen; selbst scheinbar „harmlose" Daten wie die Kommunikation in den sozialen Medien können als Grundlage dienen. Solche Algorithmen sind auch die Basis von halb- oder vollautomatisierten Entscheidungen bei Produkten und Diensten, die für die Entfaltung der Persönlichkeit und die Verwirklichung von Lebenschancen essentiell sind (z.B. Kredite, Wohnraum, Bildung, Haftstrafen). Teilweise dienen sie der sogenannten Personalisierung, d.h. der Differenzierung von Informationen (z.B. Preise, Stellenanzeigen, Produktinformationen) für bestimmte Bevölkerungskategorien oder einzel-

ne Individuen, bis hin zur personalisierten Massenbeeinflussung in demokratischen Prozessen. Diesen Entwicklungen liegt die Quantifizierung von sozialen Sachverhalten und Persönlichkeitseigenschaften zugrunde, die Risiken der Reduktion von Individuen auf messbare Größen und Informationsobjekte mit sich bringt (vgl. Burrell/Fourcade 2020).

Auch die digitale Vernetzung hat sich stark verändert. Das Internet, das ursprünglich durch offene Standards und leichte technische Beteiligungsmöglichkeiten gekennzeichnet war, unterliegt einer zunehmenden Fragmentierung und Kommerzialisierung. In den frühen Jahren wurde die Senkung von Transaktionskosten, insbesondere des Suchaufwands diskutiert, was unter anderem zur Verlagerung von Handelstätigkeiten ins Internet führte. Später rückten das Phänomen der Plattformen und die zunehmende Marktkonzentration in den Vordergrund. Eine der Hauptursachen für die Konzentration sind Netzwerkeffekte, bei denen der Nutzen für den Einzelnen von der Anzahl der weiteren Nutzenden abhängt. Die Folge sind hohe Wechselkosten und Lock-in-Effekte (z.B. beim Wechsel von einem sozialen Netzwerk zu einem anderen), aber auch Barrieren für neue Anbieter. Abhängigkeiten von wenigen Anbietenden werden verstärkt und Vertragsparitäten gestört. Abhängigkeiten und Quellen personenbezogener Daten steigen auch durch die Verlagerung von Software und Hardware im dezentralen Besitz hin zu zentral, meist online angebotenen Diensten mit Lizenzmodellen (z.B. Cloud-Dienste oder *as-a-service*-Angebote).

Ein weiteres Phänomen der Digitalisierung ist, dass soziale Regeln wie Normen oder Verträge zunehmend in Software implementiert und durch diese durchgesetzt werden (Deutscher Ethikrat 2023). Dies ist fast vollständig bei Blockchain-Anwendungen (z.B. *smart contracts*) der Fall, trifft aber auch auf automatisierte Entscheidungen in Verwaltung und Wirtschaft zu. Soziale Regeln werden automatisiert durchsetzbar sowie adaptiv und differenziert auf verschiedene Kontexte und Situationen anwendbar. Regelabweichungen werden technisch nahezu „verunmöglicht“. Gleichzeitig sind soziale Regeln nicht mehr leicht durch die Betroffenen überprüfbar und anfechtbar, so dass sich die Frage stellt, ob Entwickelnde und Anwendende überhaupt die Legitimation zur Regelsetzung haben. Ebenso kann die technische Regeldurchsetzung die moralische Motivation zur Regelbefolgung verdrängen. Greift darüber hinaus der Staat auf Softwaremechanismen zurück, um seinen Aufgaben der Risikovermeidung nachzukommen (z.B. mit Uploadfiltern für rechtlich unzulässige Inhalte), ist er zunehmend von privaten Akteuren abhängig.

Im Gegensatz zu analogen Daten haben digitale Daten und Programme die grundlegende Eigenschaft, ohne Qualitätsverlust prinzipiell unendlich kopierbar zu sein und damit einer Vielzahl von Verwendungen zur Verfügung zu stehen. Der „natürliche“ Schutz durch den Qualitätsverlust analoger Kopien ist weggefallen. Dies hat zu einer mehrfachen Entgrenzung der Risiken geführt. In zeitlicher Hinsicht können durch die quasi unerschöpfliche Weiterverwendung persistenter digitaler Daten Risiken auch zu weit entfernten Zeitpunkten entstehen, deren Konsequenzen zum Zeitpunkt der Datenerzeugung kaum abzuschätzen sind. In räumlicher Hinsicht sind Daten und Programme durch Vernetzung prinzipiell uneingeschränkt nutzbar, wodurch einzelne Systeme bzw. Plattformen und mit ihnen ihre Risiken enorme, sogar globale Reichweiten erlangen können. In sozialer Hinsicht kann die technisch prinzipiell uneingeschränkte Weitergabe an und Weiterverwendung durch eine Vielzahl von Nutzenden und Nutzungen erfolgen. Zunehmend werden datenbasierte Schlussfolgerungen über dritte Personen möglich, so dass Risiken auch Personen betreffen, die nicht an den Entscheidungen über die Datenverarbeitung beteiligt sind.

Regulatorische Risikovermeidung ist immer auch eine Begrenzung der technisch entgrenzten Möglichkeiten, etwa durch Zweckbindungsregeln oder Löschpflichten. Eine scheinbare Begrenzung der Nutzung könnte in den Aneignungs-, Exklusions- und Verwertungsstrategien (Burrell/Fourcade 2020) einzelner Akteure (oft von Big-Tech-Unternehmen) gesehen werden. Doch handelt es sich vielmehr um eine Verlagerung der Risiken entgrenzter Nutzungen in Unternehmen und Unternehmensnetzwerke sowie staatliche Einrichtungen hinein, die für außenstehende Betroffene oder Regulierende kaum mehr nachvollziehbar und kontrollierbar sind.

Risikoverständnisse und ihre Konsequenzen

Ein allgemein geteiltes Verständnis des Begriffs Risiko existiert nicht (Renn et al. 2007, 7–62; Hansson 2013, 7–20). Einem mathematisch-ökonomischen Verständnis folgend, ist Risiko für viele das Produkt aus Eintrittswahrscheinlichkeit eines Schadens und Schadensausmaß. Damit geht auch die Vorstellung einher, dass Risiken kalkulierbar sind und sich von der nicht kalkulierbaren Unsicherheit unterscheiden. Gelegentlich findet sich auch eine auf Niklas Luhmann zurückgehende Abgrenzung des Begriffs Risiko (die eigene Entscheidung ist die Ursache für Schäden) zur Gefahr (eigenes Entscheiden ist nicht die Ursache, z.B. bei Naturgefahren). Inzwischen wird der Risikobegriff jedoch alltagssprachlich und in mehreren wissenschaftlichen Disziplinen auch für solche Sachverhalte verwendet, bei denen die eigene Entscheidung nicht die Risikoursache ist sowie Eintrittswahrscheinlichkeiten und Schäden nicht quantitativ ausgedrückt werden können. Risiko bezeichnet dann die Möglichkeit, dass ein unerwünschtes Ereignis eintreten kann oder auch nicht.

Mangelnde Quantifizierbarkeit von Risiken resultiert beispielsweise aus nicht ausreichend vorhandenen empirischen Erkenntnissen, um Eintrittswahrscheinlichkeiten oder Schadensausmaße kalkulieren zu können; relevante Ereignisse sind bisher zu selten oder noch gar nicht eingetreten. Bei der Digitalisierung sind die empirischen Erkenntnisse über komplexe Ursache-Wirkungszusammenhänge bisher nur fragmentarisch vorhanden und halten mit den hochdynamischen soziotechnischen Entwicklungen kaum Schritt. Zwischen den vielfältigen Risikoursachen in Form von Datenverarbeitungen, Schlussfolgerungen und Entscheidungen und den vielfältigen Schadensformen (z.B. Drackert 2014) liegen mehrere Wirkungspfade, Prozesse der Risikoakkumulation sowie Auswirkungen auf unbeteiligte Dritte. Einzelne Risikoursachen und ihre Einflüsse lassen sich teilweise analytisch nur schwer trennen. Zudem entziehen sich Risikoursachen in Form von Datenverarbeitungen als Betriebs- und Geschäftsgeheimnisse oft einer wissenschaftlichen oder zivilgesellschaftlichen Untersuchung. Nicht zuletzt handelt es sich bei den Risiken der Digitalisierung häufig um Grundrechtseinschränkungen, die sich nur schwer oder gar nicht quantifizieren lassen, da z.B. einzelne Grundrechte mehrere rechtliche Ansprüche beinhalten können, deren Verlust in Zahlenwerte ausgedrückt oder die untereinander gewichtet werden müssten.

Die meisten Risikokonzeptionen implizieren, dass ein Risiko für etwas besteht, das Menschen als wertvoll erachten (Fischhoff/Kadvany 2011). Da dies sehr Unterschiedliches sein kann wie Grundrechte, moralische Normen oder ethische Konzepte, aber auch Gewinne, Innovationen oder Wettbewerb, ergibt sich daraus eine große Vielfalt dessen, was als Risiko definiert werden kann. Doch die Definition des Risikos bestimmt die Ausgestaltung und die Ergebnisse der

Risikoabschätzung und des Risikomanagements, ebenso der Risikogovernance bzw. Risikoregulierung (ebd.). Die Definition und Abschätzung von Risiken ist zwar häufig wissenschaftlich fundiert und strebt Objektivität an, ist aber gleichzeitig mit Werturteilen durchzogen bzw. normativ (Hansson 2013, 10f.). Technik- und Wertekonflikte können nicht nur dann auftreten, wenn bestimmt wird, wer welchen Risiken und in welchem Ausmaß ausgesetzt wird, sondern bereits bei den Entscheidungen, was als Wertmaßstab herangezogen wird. Entscheidend ist daher, wer mit welchen Bewertungsmaßstäben und Interessen die Risikoabschätzung und das Risikomanagement durchführt. Die Ergebnisse hängen insbesondere davon ab, ob dies im privaten oder im öffentlichen Interesse geschieht.

Mittlerweile werden auch gesellschaftliche Risiken für digitale Produkte und Dienste diskutiert (z.B. Yeung 2019; Smuha 2021), die mit Untersuchung von systemischen Risiken ergänzt werden. Mit systemischen Risiken werden häufig Risiken beschrieben, die über einfache, lokale oder punktuelle Risiken einzelner technischer Systeme, Anlagen, Unternehmen oder betroffener Individuen hinausgehen. Vielmehr gehen sie aus den Strukturen, Interaktionen und Interdependenzen eines soziotechnischen oder gesellschaftlichen Systems hervor und beschreiben häufig die Dysfunktion oder das komplette Versagen eines mehr oder weniger weit abgegrenzten Systems (z.B. Finanzsystem oder Klimasystem; vgl. Renn et al. 2007, 176–185). Bei digitalen soziotechnischen Entwicklungen können systemische Risiken etwa dadurch entstehen, dass sich „systemrelevante“ Akteure mit großen Reichweiten und Abhängigkeiten anderer Akteure bilden und digitale Güter zunehmend aufeinander aufbauen können (z.B. bei Plattformen oder *Foundation Models*). Andere Formen können durch Akkumulations- und Rückkopplungseffekte in komplexen Zusammenhängen der Datenverarbeitung entstehen, etwa beim Maschinellen Lernen, das verzerrte Datensätze verarbeitet, die dadurch entstehen, dass vorhergehende verzerrte Ergebnisse durch die Systeme wieder erfasst und unkorrigiert für weitere Datenanalysen und Schlussfolgerungen verarbeitet werden.

Umgang mit Risiken

Beim Umgang mit Risiken ist die individuelle Risikoakzeptanz von der gesellschaftlichen Risikoakzeptabilität zu unterscheiden. Gerade bei der Akzeptanz digitaler Gütern zeigt sich, dass individuelle Entscheidungen über die Akzeptanz von Risiken mehrfach verzerrt sein können, insbesondere durch starke Informationsasymmetrien zwischen Datenverarbeitenden und Betroffenen, der unzureichenden Kenntnis komplexer Datenverwertungsprozesse und deren Konsequenzen auf Seiten der Betroffenen oder durch Zwangslagen aufgrund der Abhängigkeit von einem bestimmten digitalen Produkt oder Dienst. Von der individuellen Risikoakzeptanz kann daher nicht auf die gesellschaftliche Risikoakzeptabilität geschlossen werden. Die gesellschaftliche Risikoakzeptabilität wird an den einer Gesellschaft zugrundeliegenden Normen untersucht, fragt nach der Verteilung von Risiken und Vorteilen, der Zumutbarkeit der Risikoexpositionen, den Möglichkeiten der Einflussnahme auf oder des Ausweichens vor Risikoexpositionen durch die Betroffenen sowie nach der Legitimität von Entscheidungen über Risiken (Grunwald 2005; Hansson 2013).

Mit den Schüben der soziotechnischen Digitalisierung verändern sich immer wieder die Möglichkeiten der Zustimmung zu Risiken, der Einflussnahme oder des Ausweichens. In

Verhältnissen zwischen Staat und Betroffenen sind die Einfluss- und Ausweichmöglichkeiten einzelner Betroffener ohnehin gering oder nicht vorhanden. Im Allgemeinen hängt dort die Legitimität der Entscheidungen über Risikoexpositionen insbesondere von der Ausgestaltung der jeweiligen politischen Verfahren ab. Abgesehen von Gesetzgebungsverfahren gibt es bei vielen Digitalisierungsvorhaben etwa in der Verwaltung oder Schulen aber nur selten politische Verfahren, in denen Zwecksetzungen (Welches Problem soll mit einzelnen Digitalisierungsmaßnahmen eigentlich gelöst werden?) und Risiken (Mit welchen gesellschaftlichen Kosten und für wen?) öffentlich debattiert und abgewogen würden. In Verhältnissen zwischen Privaten verändern sich häufig die Paritäten in den Verhandlungs- und Vertragspositionen, in denen zwischen Nutzen und Risiken digitaler Güter abgewogen wird, ebenso die Möglichkeiten der Wahlfreiheit, der Zustimmung und der Durchsetzung ihrer Rechte durch die Betroffenen selbst.

Als Wertmaßstab für Risikoabschätzungen und Risikomanagement werden häufig Menschen- und Grundrechte herangezogen, da sie weithin akzeptiert und durch ihre Institutionalisierung sowohl verbindlich als auch vom Staat zu gewährleisten sind. Von besonderer Relevanz für die Digitalisierung ist das Recht auf informationelle Selbstbestimmung. Es dient dem Schutz der Menschenwürde und der freien Entfaltung der Persönlichkeit und sieht die weitestgehend selbstbestimmte Kontrolle der Betroffenen über ihre personenbezogenen Daten vor. Insbesondere soll damit verhindert werden, dass ungeeignete Fremdbilder bzw. Profile einer Person zugeschrieben oder umfassende Fremdbilder einer Person „übergestülpt“ werden, auf diese Weise Handlungen unangemessen eingeschränkt werden und die Entfaltung der Identität einer Person nicht mehr als selbstbestimmt empfunden werden kann (Britz 2010).

Außer beim Recht auf Schutz der Menschenwürde können Grundrechte auch eingeschränkt werden, wenn die Verwirklichung anderer Grundrechte in Konflikt gerät (z.B. informationelle Selbstbestimmung versus öffentliche Sicherheit). Bei Entscheidungen über Grundrechtseinschränkungen und damit quasi über zumutbare Risikoexpositionen spielt das Verhältnismäßigkeitsprinzip eine zentrale Rolle. Beispielsweise werden staatliche Überwachung und Datenverknüpfung häufig durch Urteile des Bundesverfassungsgerichts oder des Europäischen Gerichtshofs mit Verweis auf die Unverhältnismäßigkeit der Tiefe der Eingriffe in Grundrechte begrenzt. In den Urteilen wird auch deutlich, dass sich die Eingriffstiefe bzw. das Ausmaß des Risikos nicht nur aus den möglichen Schäden für die direkt Betroffenen ergibt, sondern auch das Risiko für Unbeteiligte berücksichtigt wird. Man kann hier an das Risiko der Überwachung und Verdächtigung Unschuldiger oder Risiken in Form von Abschreckungseffekten (*chilling effects*) denken, die durch die Unsicherheit über die Datenverarbeitung entstehen und zur Zurückhaltung etwa bei politischer Beteiligung führen können.

Im Verhältnis zwischen Privaten steht oft das Recht auf informationelle Selbstbestimmung der Vertragsfreiheit gegenüber. Die Festlegung des akzeptierten Risikoniveaus soll in Aushandlungs- und Einwilligungsprozessen zwischen Datenverarbeitenden und Betroffenen erfolgen. Dabei sollen die Betroffenen selbst über die Verhältnismäßigkeit der Risiken und des Nutzens eines digitalen Gutes entscheiden. Der Gesetzgeber hat hierzu insbesondere datenschutzrechtliche Pflichten zur Information der Betroffenen durch die Datenverarbeitenden und Betroffenenrechte etwa zur Korrektur oder Löschung geschaffen. Doch die informierte Einwilligung, die man in Form von langen und schwer verständlichen Datenschutzerklärungen kennt, hat angesichts der

Vielzahl und Komplexität der Datenverarbeitungen und verknüpften Auswertungen ihre Funktionsfähigkeit weitgehend verloren. Gerade bei der zunehmenden Verwendung von Algorithmen für Entscheidungen zur Differenzierung von Personen ist es den Betroffenen nicht möglich, die Entscheidungskriterien zu kennen und in diese einzuwilligen, wenn selbst Entwickelnde oder Anwendende diese nicht nachvollziehen können oder wenn sie durch Betriebs- und Geschäftsgeheimnisse geschützt sind. Unverhältnismäßige individuelle Abwägungen von Risiken und Nutzen können sich gesellschaftlich als schleichende Erosion von Grundrechten akkumulieren (z.B. in einem abgesenkten Datenschutzniveau).

Angesichts der Probleme der informierten Einwilligung wurden unter anderem Pflichten zur technischen Risikovermeidung durch Design (z.B. *privacy by design and default*) und Pflichten zum Risikomanagement geschaffen, wie sie in der Datenschutzgrundverordnung (Hansen 2023) und der KI-Verordnung vorgesehen sind. Dadurch werden die Risiko- bzw. Verhältnismäßigkeitsentscheidungen quasi an die Betreibenden oder Anbietenden delegiert (vgl. Gellert 2020), es sei denn die zu akzeptierenden Risikoniveaus werden in weiteren Regulierungen oder Standardisierungen festgelegt. Dabei ist zu erwarten, dass in den Risikoabschätzungen privater Akteure in erster Linie nur solche Risikofaktoren berücksichtigt werden, die sich unmittelbar auf die Gewinnsituation auswirken. Inwieweit gesellschaftliche oder systemische Risiken tatsächlich berücksichtigt werden, ist unklar.

Mit der Ausweitung der Risiken der Digitalisierung haben sich umfangreiche institutionelle Arrangements entwickelt. Neben dem Datenschutz- und Verbraucherschutzrecht haben mit dem Sichtbarwerden von Diskriminierungsrisiken von Algorithmen auch Fragen des Antidiskriminierungsrechts an Bedeutung gewonnen. Allerdings ist der bisherige individualrechtliche Ansatz, wonach Diskriminierungsopfer zunächst selbst aktiv werden müssen und bei der Durchsetzung von Schadensersatzansprüchen von Antidiskriminierungsstellen unterstützt werden können, nur begrenzt geeignet, algorithmische Diskriminierungen zu bekämpfen (Orwat 2019). Schließlich wird dem Problem der Marktkonzentration und systemischen Risiken von Plattformen mit einer Reihe von regulatorischen Maßnahmen zu begegnen versucht, insbesondere mit der *KI-Verordnung*, dem *Digital Service Act*, dem *Data Act*, dem *Digital Market Act* und dem *Data Governance Act*. Unter anderem sollen die Wahlfreiheit bei digitalen Gütern und damit die Möglichkeiten, Risiken zu beeinflussen oder auszuweichen, gestärkt werden und Zugangs- und Nutzungsmöglichkeiten von Daten aus vernetzten Geräten, die meist in den Händen von privaten Unternehmen liegen, an die Nutzenden zurückgegeben werden. Offen bleibt, wer die neuen Möglichkeiten der Datennutzung tatsächlich ergreifen kann und wird.

Zitierte Literatur

Britz, Gabriele (2010). Informationelle Selbstbestimmung zwischen rechtswissenschaftlicher Grundsatzkritik und Beharren des Bundesverfassungsgerichts. In: Wolfgang Hoffmann-Riem (Hg.). Offene Rechtswissenschaft. Tübingen, Mohr Siebeck, 561–596.

Burrell, Jenna/Fourcade, Marion (2020). The Society of Algorithms. Annual Review of Sociology 47, 213–237. https://doi.org/10.1146/annurev-soc-090820-020800.

Deutscher Ethikrat (2023). Mensch und Maschine – Herausforderungen durch Künstliche Intelligenz. Berlin, Deutscher Ethikrat.

Drackert, Stefan (2014). Die Risiken der Verarbeitung personenbezogener Daten. Eine Untersuchung zu den Grundlagen des Datenschutzrechts. Berlin, Dunker & Humblot.

Fischhoff, Baruch/Kadvany, John (2011). Risk: A Very Short Introduction. Oxford, OUP.

Gellert, Raphaël (2020). The Risk-Based Approach to Data Protection. Oxford, OUP.

Grunwald, Armin (2005). Zur Rolle von Akzeptanz und Akzeptabilität von Technik bei der Bewältigung von Technikkonflikten. Technikfolgenabschätzung – Theorie und Praxis 14, 54–60. https://doi.org/10.14512/tatup.14.3.54.

Hansen, Marit (2023). Der lange Weg von digitaler Selbstverteidigung bis zum eingebauten Datenschutz. In: Benedikt Buchner/Thomas Petri (Hg.). Informationelle Menschenrechte und digitale Gesellschaft. Tübingen, Mohr-Siebeck, 57–75.

Hansson, Sven Ove (2013). The Ethics of Risk: Ethical Analysis in an Uncertain World. Cham, Palgrave Macmillan.

Orwat, Carsten (2019). Diskriminierungsrisiken durch Verwendung von Algorithmen. Studie erstellt mit einer Zuwendung der Antidiskriminierungsstelle des Bundes. Berlin, Nomos.

Renn, Ortwin/Schweizer, Pia-Johanna/Dreyer, Marion/Klinke, Andreas (2007). Risiko: über den gesellschaftlichen Umgang mit Unsicherheit. München, Oekom.

Smuha, Nathalie A. (2021). Beyond the Individual: Governing AI's Societal Harm. Internet Policy Review 10. https://doi.org/10.14763/2021.3.1574.

Yeung, Karen (2019). Responsibility and AI. A Study of the Implications of Advanced Digital Technologies (Including AI Systems) for the Concept of Responsibility within a Human Rights Framework. Council of Europe Study DGI(2019)05. https://rm.coe.int/a-study-of-the-implications-of-advanced-digital-technologies-including/168096bdab.

Weiterführende Literatur

Deutscher Ethikrat (2023). Mensch und Maschine – Herausforderungen durch Künstliche Intelligenz. Berlin, Deutscher Ethikrat.

Fischhoff, Baruch/Kadvany, John (2011). Risk: A Very Short Introduction. Oxford, OUP.

Hansen, Marit (2023). Der lange Weg von digitaler Selbstverteidigung bis zum eingebauten Datenschutz. In: Benedikt Buchner/Thomas Petri (Hg.). Informationelle Menschenrechte und digitale Gesellschaft. Tübingen, Mohr-Siebeck, 57–75.