Teil III
Künstliche Intelligenz und Nutzendenverhalten

Privacy als Paradox? Rechtliche Implikationen verhaltenspsychologischer Erkenntnisse

Hannah Ruschemeier

Zusammenfassung

Das Privacy Paradoxon beschreibt das Phänomen, dass Menschen nach außen bekunden, ihre Privatsphäre und Datenschutz besonders zu wertschätzen, dieser Selbsteinschätzung aber keine Taten folgen lassen. Ihre innere Einstellung divergiert von ihren tatsächlichen Verhaltensweisen: Der betonten Wichtigkeit von Privatheit zum Trotz geben viele Personen niedrigschwellig oder gar anlasslos höchstpersönliche Informationen über sich Preis. Diese Diskrepanz zwischen Selbsteinschätzung und realem Verhalten kann vom Recht nicht unbeachtet bleiben, insbesondere in Bereichen von KI und Datenschutz, in denen über verschiedenste Regulierungsformen diskutiert wird. Das Privacy Paradox muss kein Paradoxon bleiben. Privatheit als Konzept in der Vorstellung vieler Menschen kann unendlich viele Facetten abdecken, die sich nur teilweise oder auch gar nicht mit konkreten persönlichen Verhaltensweisen überschneiden. Das Recht reflektiert diese realen Voraussetzungen von Privatheit bisher unzureichend, wie das Beispiel der datenschutzrechtlichen Einwilligung zeigt. Das Privacy Paradox verstärkt die Forderungen nach einer anderen Ausrichtung des Datenschutzes von einem höchstpersönlichen Gut hin zu kollektiven Auswirkungen und institutioneller Verantwortung.

1. Problemaufriss

Der Streit um Daten und Datennutzung ist eine der zentralen Machtfragen unseres Jahrhunderts. Datenschutz und Datennutzungsrechte stehen in komplexen Spannungsverhältnissen zueinander. Digitaler Privatheitsschutz und Datenschutz als Konzept sind kontroverse, politisierte Themenfelder. Auf der individuellen Ebene von Nutzer:innen hat sich Privatheitsschutz durch Datenschutz zudem zunehmend zu einer unlösbaren Aufgabe entwickelt: Die Verbreitung persönlicher Informationen erscheint nicht mehr kontrollierbar. Das ist vor allem dann problematisch, wenn diese Preisgabe und Verarbeitung persönlicher Daten nicht mehr der au-

tonomen Entscheidung der Betroffenen entsprechen. Die Annahme ist naheliegend, insbesondere in dem durch informationelle Machtasymmetrien und Vormachtstellung einzelner globaler Unternehmen geprägten digitalen Raum des Internets. Der Allgemeinplatz, dass Datenschutz nicht Daten, sondern Personen schützt, gerät aus dem Fokus.[1] Denn Privatheits- und Datenschutz wird oft als innovationshindernd, paternalistisch und ineffektiv wahrgenommen. Auch das so genannte *Privacy Paradox* scheint mit einer Argumentationsstruktur für effektiveren Schutz zu brechen. Menschen verhalten sich höchst widersprüchlich was den Schutz ihrer Privatsphäre betrifft: sie folgen schlicht nicht ihren eigenen, zumindest kommunizierten Präferenzen. Das *Privacy Paradox* ist damit ein relevantes und juristisch lohnenswertes Beispiel, um die Reflektion menschlichen Verhaltens durch Recht zu untersuchen. Der Beitrag skizziert Definition, Grundlagen, und Konsequenzen des Privacy Paradox aus rechtswissenschaftlicher Perspektive und entwirft Vorschläge für Reaktionen des Rechts.

Das *Privacy Paradox* beschreibt das Phänomen, dass Menschen nach außen bekunden, ihre Privatheit und den Schutz ihrer persönlichen Daten besonders zu wertschätzen, dieser Selbsteinschätzung aber keine Taten folgen lassen.[2] Ihre innere Einstellung divergiert von ihren tatsächlichen Verhaltensweisen: Der betonten Wichtigkeit von Privatheit zum Trotz geben viele Personen niedrigschwellig oder gar anlasslos höchstpersönliche Informationen über sich preis – das erscheint widersprüchlich. Das Credo, dass Privatsphäre schützenswert ist und vor allem akzessorisch an-

1 *von Lewinski*, Die Matrix des Datenschutzes, 2014, S. 4.

2 Kompakter Überblick bei: *Øverby*, in: Jajodia/Samarati/Yung (Hrsg.), Encyclopedia of Cryptography, Security and Privacy, 2019, S. 1- 2. Empirische Analysen bei *Acquisti/Grossklags* IEEE Secur. Privacy Mag. 3 (2005), 26 ff.; *Barth/Jong* Telematics and Informatics 34 (2017), 1038 ff.; *Norberg/Horne et al.* Journal of Consumer Affairs 41 (2007), 100; *Spiekermann/Grossklags et al.*, in: Proceedings of the 3rd ACM conference on Electronic Commerce - EC '01, 2001; *Taddicken* J Comput-Mediat Comm 19 (2014), 248 ff.; *Turow/Hennessy* New Media & Society 9 (2007), 300 ff.; *Wirth/Maier et al.* INTR 32 (2022), 24 ff. Literatur Review bspw. bei: *Gerber/Gerber et al.* Computers & Security 77 (2018), 226 ff.; *Kokolakis* Computers & Security 64 (2017), 122 ff. Aus rechtlicher Sicht: ; *Hermstrüwer*, Informationelle Selbstgefährdung, 2015, S. 232 ff.; *Solove* The George Washington Law Review 89 (2021), 1 ff.; *Waldman* Current Opinion in Psychology 31 (2020), 105 ff. Aus psychologischer Perspektive bspw.: *Dienlin*, in: Specht-Riemenschneider/Werry/Werry (Hrsg.), Datenrecht in der Digitalisierung, 2020, S. 305 ff. Kommunikationswissenschaftliche Einordnung: *Barnes*, A privacy paradox: Social networking in the United States, https://firstmonday.org/article/view/1394/1312; *Taddicken* J Comput-Mediat Comm 19 (2014), 248.

dere Rechtsgüter schützt,[3] scheint nicht mehr zu greifen. Die Divergenz zwischen inneren Einstellungen und Verhaltensweisen ist zunächst nichts Ungewöhnliches, sondern ein allbekanntes Alltagsphänomen. Das Privacy Paradox ist ebenfalls ein leicht erklärbares Verhaltensmuster, aber andererseits eine akademische Fragestellung, welche vielfach und interdisziplinär untersucht wird, jedoch immer noch umstritten ist.[4]

In Bezug auf Privatheit und rechtliche Regulierung ist das Privacy Paradox auch deshalb interessant, da Privatheitsschutz, grundrechtlich im Recht auf informationelle Selbstbestimmung verankert, als Ausfluss persönlicher Autonomie angesehen wird.[5] Dazu gehört auch, auf eben diese Privatheit zu verzichten.[6]

Muss das Recht dennoch die Menschen „vor sich selbst" schützen? Rechtliche Regulierung kann neben dem – online in großen Teilen versagenden individuellen Selbstschutz und der ebenfalls nicht sehr erfolgreichen Selbstregulierung der Industrie – ein Schutz- und Ermöglichungsmechanismus sein. Oder ist ein Regulierungsansatz, der wie im Datenschutzrecht den individuellen Rechtsgüterschutz abstrakt sehr stark betont, aber erheblichen Vollzugsdefiziten unterliegt, deshalb grundlegend falsch? Sollte Privatheit als Rechtsgut allgemein überdacht werden?

Meine Ausgangsthese ist, dass Privatheitsschutz durch Datenschutz erstrebenswert ist, auch wenn einzelne Personen sich nicht privatheitsschützend verhalten oder gar gegenläufige Präferenzen äußern; das vermeintliche Paradoxon der Privatheit ist hierfür kein Gegenargument.

2. *Grundlagen des Privacy Paradoxes*

Die Grundlagen des *Privacy Paradox* setzen sich aus dem theoretischen Verständnis von Privatheit (2.1) und der empirischen Erforschung von Verhalten zusammen (2.2), das im vermeintlichen Widerspruch zur Vorstellung von Privatheit steht.

---

3 dazu eingehend: *Britz*, in: Hoffmann-Riem/Brandt (Hrsg.), Offene Rechtswissenschaft, 2010, S. 561, 569 ff.

4 systematische Literaturauswertung z.B. bei *Gerber/Gerber et al.* Computers & Security 77 (2018), 226 ff.

5 BVerfGE 61, 1 (42); 78, 77 (84); 103, 21 (33); statt aller: *Kunig/Kämmerer*, in: Münch/Kunig (Hrsg.), , 7. Aufl. 2021, Art. 2 GG, Rn. 80. Umfassend zum Autonomiekonzept des Art. 2 I GG: *Britz*, Freie Entfaltung durch Selbstdarstellung, 2007, S. 16.

6 Umfassend: *Hermstrüwer* (Fn. 2), S. 31 ff.

2.1 Konzeption von Privatheit und Datenschutz im Kontext des Privacy Paradoxes

Privatheit[7] ist seit Jahrhunderten ein kontroverses Thema und wurde bereits lange vor dem Siegeszug digitaler Technologien diskutiert.[8] Grundsätzlich zielt Privatheit im Verständnis des Selbstbestimmungsrechts darauf ab, Menschen Autonomie zu ermöglichen und zu sichern.[9] Deshalb ist die Idee einer universellen Definition von Privatheit auch nicht realisierbar, da sie letztlich in der individuellen autonomen Entscheidung der einzelnen Person wurzelt.[10]

Juristisch betrachtet ist Privatheit ein unbestimmter Rechtsbegriff, der nicht explizit von Gesetzen definiert oder benannt wird.[11] Privatheit ist gewinnbringend aus rechtswissenschaftlicher Perspektive vor allem im Hinblick auf normative Konsequenzen zu beurteilen. Ein rechtlicher He-

---

7 Privatheit nach deutschen Rechtsverständnis sowie das Verständnis von Privatsphäre nach der Rechtsprechung des BVerfG sind nicht exakt deckungsgleich mit dem weiteren Begriff des Konzepts „Privacy", das auch in den englischsprachigen Abhandlungen zum Privacy Paradox thematisiert sind. Für die juristische Perspektive sind die Maßstäbe des jeweils relevanten Rechtsverständnisses des konkreten Regulierungskontextes besonders relevant.

8 *Øverby*, in: Jajodia/Samarati/Yung (Fn. 2), S. 1; Siehe nur: The Right to Privacy *Warren/Brandeis* Harvard Law Review 4 (1890), 193 (205) bereits mit dem Bezug zu persönlichen Daten ohne von Daten zu sprechen „The principle which protects personal writings and all other personal productions, not against theft and physical appropriation, but against publication in any form, is in reality not the principle of private property, but that of an inviolate personality".

9 *Britz*, in: Hoffmann-Riem/Brandt (Fn. 3), S. 561, 569. Zu weiteren Zwecken und Formen von Privatheit: *Eichenhofer*, e-Privacy, 2021, S. 38 ff.

10 Grob lassen sich zwei Strömungen in der Forschung zur Privatsphäre identifizieren: Einmal wird Privatsphäre als Frage gesellschaftlicher und persönlicher Art begriffen *Bennett*, Privacy in the Political System: Perspectives from Political Science and Economics, 1995 revised 2001) und einmal als Zustand, der sich vor allem durch Freiheit von Kontrolle und Überwachung auszeichnet (*Westin* Columbia Law Review 66 (1966), 1003 ff.). Überblick zu verschiedenen Theorien der Privatheit bei: *Eichenhofer* (Fn. 9), S. 25 ff. Eingehende rechtliche Analyse bei: *Gusy* Jahrbuch des öffentlichen Rechts der Gegenwart. Neue Folge (JöR) 70 (2022), 415 ff.
Acquisti/Brandimarte et al. Science (New York, N.Y.) 347 (2015), 509 (512) geben zudem einen interessanten Kurzabriss über die Grundlagen der Privatheit bis hin zu Referenzen in der Bibel.

11 Zu Privatheit als Rechtsbegriff: *Roßnagel/Geminn* JZ 70 (2015), 703 ff. *Gusy* Jahrbuch des öffentlichen Rechts der Gegenwart. Neue Folge (JöR) 70 (2022), 415, 416 f. betont das Erfordernis der Begründung einer Schutzbedürftigkeit von Privatheit durch andere Disziplinen.

bel für die Umsetzung ist das Datenschutzrecht, denn dieses zielt durch den Schutz personenbezogener Daten *auch* auf Privatheitsschutz. Privatheitsschutz und Datenschutz sind nicht deckungsgleich, haben aber viele Überschneidungspunkte.[12] Datenschutz ist kein Selbstzweck, sondern wurzelt, ebenso wie Privatheit, im Autonomieschutz.[13] Diese Differenzierung und gleichzeitige Rückführbarkeit auf gemeinsame Schutzgüter ist auch in den Rechtsgrundlagen reflektiert. Sowohl das Recht auf informationelle Selbstbestimmung als auch das Recht auf Datenschutz in der Charta der Grundrechte der Europäischen Union zielen auf den Schutz autonomer Entscheidungen von Individuen über ihre persönlichen Daten ab.[14] Die Verfügungsgewalt über persönliche Daten kann den Schutz von Privatheit ermöglichen. Datenschutz hängt deshalb eng mit dem Verständnis von Privatheit und Privatheitsschutz zusammen.

Der Schutz von Privatheit dient in erster Linie der Bewahrung persönlicher Entscheidungsfreiräume, wobei die Funktionen vielfältig sind. Viele Konzeptionen von Privatheit fußten auf einer Trennung verschiedener Sphären, einem räumlich geprägten Verständnis von Öffentlichkeit und privaten Raum.[15] Das Private findet danach „hinter verschlossenen Türen" statt, durch die Fenster des eigenen Hauses sollte niemand schauen dürfen. Die dazu konträre öffentliche Sphäre war außerhalb dieses privaten Raumes angesiedelt, dadurch aber auch klar erkennbar. Die digitale Transformation verändert das Verständnis von Privatheit, die Vorstellung von individueller Kontrolle des Zugangs zu persönlichen Informationen ist letztlich überholt.[16] Denn digitale, online-basierte Anwendungen brechen mit dem Verständnis der Abgrenzung durch Räumlichkeit, da sie durch ihre Konzeption selbst entgrenzend wirken.

Bis heute werden diverse Konzepte von Privatheit diskutiert[17], welche die Entwicklungen von Privatheit in unterschiedlichen Kontexten beleuch-

---

12 Datenschutz ist nicht gleichzusetzen mit Privatheitsschutz. Nach dem Grundgesetz bspw. zielen auch andere Grundrechte als das Recht auf informationelle Selbstbestimmung auf den Schutz der Privatsphäre, z.B. Art. 13 GG. Auf unionsrechtlicher Ebene unterscheidet die GrCh zwischen Art. 7, dem Recht auf Privatsphäre, und Art. 8, dem Recht auf Datenschutz. Zu den Unterschieden zwischen Datenschutz und Privatheit: *Eichenhofer* (Fn. 9), S. 52 ff.

13 Zum funktionalen Wert von Privatheit als Sicherung der Autonomie: *Sandfuchs*, Privatheit wider Willen?, 2015 S. 8 ff.

14 Statt vieler: *Bretthauer*, in: Specht-Riemenschneider/Mantz (Hrsg.), Handbuch europäisches und deutsches Datenschutzrecht, 2019, Rn. 13 ff.;

15 *von Lewinski* (Fn. 1), S. 29 ff. zu physischen, logischen und sozialen Räumen.

16 *Leopold*, in: Piallat (Hrsg.), Der Wert der Digitalisierung, 2021, S. 167

17 Vgl. nur zur Public Privacy: *Stahl* Moral Philosophy and Politics 7 (2020), 73.

ten. Privatheit entfaltet auch eine gesellschaftliche, demokratietheoretische Dimension[18], die dafürspricht, auch Datenschutz nicht nur aus individueller Perspektive zu betrachten.[19]

Die meisten Autor:innen stimmen darin überein, dass Privatheit durch quantitative Datenanalysen in digitalen Kontexten gefährdet ist und daraus negative Konsequenzen für den ökonomischen und sozialen Zugang von Bürger:innen und deren gesellschaftliche Teilhabe folgen.[20] Andere hingegen meinen, dass nicht die gefährdete individuelle Privatheit problematisch ist, sondern fehlende Sicherheit und Sanktionen.[21] Die Verfügbarkeit von Informationen sei kein Problem, sondern ihr Missbrauch. Überwachung durch Staat und Wirtschaft seien kein Grund zur Beunruhigung. Denn es gäbe keine Anhaltspunkte dafür, dass Menschen weniger frei seien, wenn sie weniger Privatsphäre hätten.[22] Diese Ansicht gewichtet den Aspekt zu gering, dass die eigene Entscheidung darüber, welche Informationen preisgegeben werden, der autonome Akt ist und nicht die daraus folgenden Konsequenzen. Für die Folgen von Privatheitsverletzungen können auch der generelle Missbrauch wirtschaftlicher oder politischer Macht verantwortlich gemacht werden. Diese Faktoren beziehen sich aber auf die mittelbaren Folgen und nicht auf die Entscheidung des Individuums. Die Konsequenzen aus Privatheitsschutz sind auch nicht zwingende Geheimhaltung und Intransparenz auf allen Ebenen, sondern Entscheidungsalternativen über Informationspreisgabe.

Eine abschließende Klärung des Begriffs der Privatheit ist nicht erforderlich, um Grundlagen für die rechtliche Handhabung daraus abzuleiten.[23] Unzweifelhaft begegnet der Schutz von Privatheit in digitalen und vernetzten Umgebungen neuen individuellen und gesellschaftlichen Herausforde-

---

18 Vgl. nur: *Eichenhofer* (Fn. 9), S. 46; *Seubert* Datenschutz und Datensicherheit - DuD 36 (2012), 100 (101 f.).

19 Dazu unten D.

20 Bspw. die Beiträge in Hoffmann-Riem (Hrsg.), Big Data - Regulative Herausforderungen, 2018. Dazu auch Mühlhoff, S. 41 in diesem Band.

21 Vgl. *Belliger/Krieger*, in: dies. (Hrsg.), Network Publicy Governance, 2018, S. 45, 50.

22 *Belliger/Krieger*, in: dies. (Fn. 21), S. 45, 55. Zu Post-Privacy: *Ganz*, Die Netzbewegung, 2018, S. 235 ff.; *Gruschke*, in: Kappes/Krone/Novy (Hrsg.), Medienwandel kompakt 2011 - 2013: Netzveröffentlichungen zu Medienökonomie, Medienpolitik & Journalismus, 2014, S. 79, 81 ff.; *Hagendorff*, in: Behrendt/Loh/Matzner et al. (Hrsg.), Privatsphäre 4.0: Eine Neuverortung des Privaten im Zeitalter der Digitalisierung, 2019, S. 91, 96 ff.

23 *Schwichtenberg*, Datenschutz in drei Stufen: Ein Auslegungsmodell am Beispiel des vernetzten Automobils, 2018, S. 16.

rungen; schon deshalb, da bei allen Onlineaktivitäten z.B. auch ohne bewusste Preisgabe von Informationen Meta- und Nutzungsdaten generiert werden. Zudem werden behaviorale und psychologische Prozesse gezielt genutzt, um die Preisgabe persönlicher Informationen zu befördern.[24] Grundlegende Informationsasymmetrien können verhindern, dass das eigene Verhalten überhaupt den geäußerten Präferenzen angepasst werden kann.[25]

2.2 Empirische Grundlagen: Privacy Calculus oder Privacy Paradox?

Grundlage des *Privacy Paradox* ist auch das Verständnis darüber, was Menschen motiviert und wie sie Entscheidungen treffen, d.h. was leitend für menschliches Verhalten ist.[26] Dabei können persönliche Daten selbst freigegeben werden, oder es werden schlicht keine Maßnahmen getroffen, die persönlichen Daten zu schützen – was oft zwei Seiten derselben Medaille sind.

Zur Erklärung des *Privacy Paradox* werden unterschiedliche Theorien diskutiert.[27] Die Argumentationsstränge unterscheiden sich vor allem darin, wie viel Rationalität den Entscheidungsträger:innen zugesprochen wird: entweder richtet sich das Verhalten nach einer Gegenüberstellung von Risiken und Vorteilen[28] oder es erfolgt schlicht keine Risikoevaluation.[29] Ob sich die sich von der Selbsteinschätzung divergierenden Verhaltensweisen durch rationale Kosten-Nutzen-Abwägung (2.2.1), oder Impulsivität und Irrationalität (2.2.2) begründen lassen, ist umstritten.[30] Zudem sind Resignation und gewolltes Unwissen (2.2.3), Beeinflussung und Ma-

---

24 *Acquisti/Brandimarte et al.* Science (New York, N.Y.) 347 (2015), 509 (512); *Masur* M&K Medien & Kommunikationswissenschaft 66 (2018), 446 (447).

25 Nicht einmal die Nutzung eines sozialen Netzwerks ist Voraussetzung; auch über Nichtnutzer:innen können Daten gesammelt werden: *Garcia* Science advances 3 (2017), e1701172.

26 *Gerber/Volkamer et al.*, in: Dialogmarketing Perspektiven 2016/2017: Tagungsband 11. wissenschaftlicher interdisziplinärer Kongress für Dialogmarketing, 2017, S. 139 f.

27 *Barth/Jong* Telematics and Informatics 34 (2017), 1038 ff. identifizieren 35 verschiedene Theorien, die das Privacy Paradox jeweils unterschiedlich erläutern. Übersicht auch bei *Gerber/Gerber et al.* Computers & Security 77 (2018), 226 ff.

28 *Barth/Jong* Telematics and Informatics 34 (2017), 1038 (1045 ff.).

29 *Barth/Jong* Telematics and Informatics 34 (2017), 1038 (1048 ff.).

30 Dazu: *Arpetti/Delmastro* Journal of Industrial and Business Economics 48 (2021), 505 ff.

nipulation (2.2.4) sowie informationelle Asymmetrien und Kontextabhängigkeit (2.2.5) zu beachten.

2.2.1 Ausfluss rationaler Entscheidung

Die Idee des *Privacy Calculus* beruht auf der *rational-choice theory* und geht davon aus, dass Personen eine Kosten-Nutzen-Analyse vornehmen, bevor sie persönliche Informationen offenlegen.[31] Die ökonomische Theorie beurteilt diese Einschätzung von Personen als handlungsleitend.[32] Danach geben Konsument:innen dann persönliche Daten preis, wenn sie davon ausgehen, dass der erwartete Nutzen die Risiken übersteigt.[33] Dieser kann in monetären (Rabatte, Gutschein), persönlichen (Anpassung, Individualisierung) oder sozialen Faktoren (Zugehörigkeit bei sozialen Netzwerken, Aufbau von Sozialkapital)[34] bestehen. Ziel ist es daher nicht, stets möglichst hohen Privatheitsschutz herzustellen, sondern dass eine Balance gefunden wird und Daten bereitgestellt werden, wenn es sich für die Person lohnt.[35]

Der *Privacy Calculus* hat allerdings keine Erklärung für die Preisgabe persönlicher Daten, wenn schlicht keine Vorteile bestehen, diese nicht erkennbar oder nur geringwertig sind. Denn wenn der Schutz personenbezogener Daten einen vergleichsweise hohen Stellenwert genießt, wäre nach dem Rationalitätsmodell eine Datenpreisgabe nur bei erheblichen Vorteilen zu erwarten.[36] Diese Erwartungen werden nicht durch das tat-

31 *Laufer/Wolfe* Journal of Social Issues 33 (1977), 22 ff.; *Dienlin/Metzger J.M.* Journal of Computer-Mediated Communication,, 368 ff.; *Wisniewski/Page*, in: Knijnenburg/Page/Wisniewski et al. (Hrsg.), Modern Socio-Technical Perspectives on Privacy, 2022, S. 15, 18 ff.

32 *Culnan/Armstrong* Organization Science 10 (1999), 104 ff.

33 Überblick verschiedener Theorien zur Risikowahrnehmung bei: *Gerber/Volkamer et al.*, in: Dialogmarketing Perspektiven 2016/2017: Tagungsband 11. wissenschaftlicher interdisziplinärer Kongress für Dialogmarketing, 2017, S. 139, 152 f.

34 *Holland* Widener Law Journal 19 (2010), 893 (913).

35 *Waldman* Current Opinion in Psychology 31 (2020), 105 (108) hält das Modell für untauglich im Kontext von Privatheit.

36 *Bunnenberg*, Privates Datenschutzrecht, 2020, S. 100 auch mit Bezug zu kollektiven Auswirkungen, wonach das Einwilligungsmodell auf kollektiver Ebene nach Rationalitätsgesichtspunkten solange ein hohes Datenschutzniveau gewährleisten kann, als Privatheit gesamtgesellschaftlich hoch geschätzt wird.

sächliche Verhalten von Verbraucher:innen bestätigt, insbesondere im Onlinebereich bzgl. Konsum[37]und in sozialen Netzwerken.[38]

2.2.2 Verzerrte Risikoabwägung

Zahlreiche verhaltenspsychologische Studien haben aufgezeigt, dass Menschen sich nicht stets rational verhalten, sondern Verhaltensanomalien auftreten.[39] Diese Urteilsfehler führen dazu, dass Informationen falsch eingeschätzt oder nicht korrekt verarbeitet werden. Es ist nicht möglich, stets alle Argumente und Informationen objektiv korrekt zu verarbeiten und danach zu entscheiden. Komplexere Risikoabwägungen sind für Menschen schwierig zu vollziehen; um Entscheidungen zu treffen, nutzen wir einfache Entscheidungsregeln, sog. Heuristiken.[40]. Diese sind Ausfluss einer begrenzten Rationalität, denn viele Personen tendieren dazu, Risiken, die mit positiv konnotierten Dingen verknüpft sind zu unterschätzen und gleichzeitig zu überschätzen, wenn sie mit Sachverhalten oder Dingen verknüpft sind, die sie nicht mögen.[41] Auch besteht eher die Bereitschaft, sogar sensible Informationen gegen Vergütung preiszugeben als diese gegen anfallende Kosten zu schützen.[42] Die zeitliche Dimension bzgl. der Schadenswahrscheinlichkeit kommt hinzu: Privatheit wird in *konkreten* Entscheidungssituationen ein sehr geringer Stellenwert beigemessen, selbst wenn der Preisgabe ein extrem geringer Nutzen gegenübersteht – dadurch wird eine Delegation der Kosten in die Zukunft ermöglicht.[43] Diese hyperbolische Diskontierung beschreibt, dass die zukünftigen Kosten den

37 *Beresford/Kübler et al.* Economics Letters 117 (2012), 25 ff., die in einem Feld Experiment nachgewiesen haben, dass eine umfangreiche Datenerhebung eines Onlineshops als einziger Unterschied zu einem Vergleichsangebot keinen Einfluss auf die Kaufentscheidung hat.

38 Acquisti/Gross, in: Danezis/Golle, Privacy enhancing technologies, S. 36 ff.

39 Vgl. *Englerth/Towfigh*, in: Towfigh/Petersen (Hrsg.), Ökonomische Methoden im Recht, 2. Auflage 2017, S. 237, Rn. 503 ff.; *Jolls/Sunstein et al.* Stanford Law Review 50 (1998), 1471 (1477).

40 Grundlegend: *Tversky/Kahneman* Science 185 (1974), 1124 ff.

41 „Affektheuristik", *Slovic, P., Finucane, M., Peters, E., & MacGregor, D.*, in: Gilovich/Griffin/Kahneman (Hrsg.), Heuristics and biases, 2002, S. 397 ff.

42 *Grossklags/Acquisti*, When 25 Cents is Too Much: An Experiment on Willingness-To-Sell and Willingness-To-Protect Personal Information, 7.6.2007.

43 *Müller/Flender et al.*, in: Internet Privacy, 2012, S. 143, 179.

Vorteilen der gegenwärtigen Nutzung überproportional unterliegen.[44] Im digitalen Bereich stellt sich die Problematik von unterschätzten Risiken und impulsivem Handeln (z.B. Clickbait[45]) in besonderem Maße. Danach läge also kein Widerspruch zwischen Selbsteinschätzung und Handeln vor, sondern eine verzerrte bzw. fehlerhafte handlungsleitende Risikoeinschätzung.[46]

2.2.3 Resignation und gewolltes Unwissen

Online basierte Warenkäufe und Dienstleistungen sowie *smart wearables* sind inzwischen so alltäglich geworden, dass die meisten Menschen diese Angebote auch wahrnehmen, wenn sie nur ein geringes Vertrauenslevel haben, es also „gar nicht so genau wissen wollen".[47] Neben dem praktisch unüberwindbaren Aufwand, stets die privatheitsfreundlichste Einstellung zu wählen[48] besteht ein Wissensdefizit, welches sich gerade im Internet multipliziert. Dauerhaft informierte Entscheidungen über die tausenden involvierten Webseiten unterschiedlicher Firmen, Apps und ihren Modalitäten der Datenverarbeitung zu treffen, kann durch Einzelpersonen nicht erreicht werden. Versuche des Privatheitsschutzes enden deshalb auch oft in Resignation. Wenn Nutzer:innen ständig selbst entscheiden müssen, ob ihre Daten verarbeitet werden dürfen, führt dies nicht in wenigen Fällen zu einer „Consent-Fatigue" und wahllosen Klicks, um weiter fortfahren zu können.[49] In diese Richtung zielen auch die Erklärungen der Konsistenztheorien, z.B. wenn online die Dissonanz zwischen allgemeinen

44 *Grossklags/Acquisti*, Losses, gains, and hyperbolic discounting: An experimental approach to information security attitudes and behavior, 2003S. 15; *Müller/Flender et al.*, in: (Fn. 43), S. 143, 179.

45 Übersicht und psychologische Analyse bei: *Mayer*, in: Appel (Hrsg.), Die Psychologie des Postfaktischen: Über Fake News, „Lügenpresse", Clickbait & Co, 2020, S. 67 ff.

46 *Holland* Widener Law Journal 19 (2010), 893 (906 ff.).

47 Eine Studie aus dem Jahr 2008 hat eine Studie für die USA berechnet, dass bei durchschnittlicher Internetnutzung 76 Tage pro Jahr erforderlich wären, um alle Datenschutzerklärungen zu lesen. Dabei würden Opportunitätskosten von 781 Milliarden Dollar entstehen: *McDonald/Cranor* I/S: A Journal of Law and Policy for the Information Society 2008, 543 (564).

48 Zur mandated choice: *Martini/Weinzierl* RW 2019, 287 (290 ff.).

49 Vgl. *Vidhani/Banahatti et al.* CSI Transactions on ICT 9 (2021), 185 (190).

Bedenken und situativen Hinweisreizen zugunsten letzterer aufgelöst wird und damit z.B. die Bedeutung einer Datenschutzrichtlinie ignoriert wird.[50]

2.2.4 Beeinflussung und Manipulation

Die rechtlichen Implikationen von Nudging und „Dark" Patterns werden kontrovers diskutiert.[51] Sowohl Nudging zugunsten der Nutzer:inneninteressen z.B. zur Wahl einer datenschutzrechtlichen Voreinstellung als auch Beeinflussung entgegen deren eigentlichen Interessen („Dark" Patterns) nutzen Verhaltensanomalien gezielt aus. Mechanismen und Gestaltungen, die Nutzer:innen keine echte Wahlmöglichkeit eröffnen, z.B. die Auswahl datenschutzfreundlicher Einstellungen erschweren oder Widerspruchsmöglichkeiten nicht auffindbar in Webseiten verstecken, sind ein weiterer Umstand, der bei der Bewertung des Widerspruchs zwischen geäußerten Präferenzen zu Privatheit und tatsächlichem Verhalten berücksichtigt werden sollte.[52]

2.2.5 Informationelle Asymmetrie und Kontextabhängigkeit

Das Privacy Paradox kann als Ausfluss fehlender bzw. begrenzter Rationalität gedeutet werden. Menschen werden von systematischen Verhaltensanomalien, sozialen Normen und Emotionen, persönlicher Erfahrung, Netzwerkeffekten und Persönlichkeitszügen beeinflusst.[53] Einige sind der Auffassung, dass sich die wahren Präferenzen der Verbraucher:innen nur in ihrem Verhalten widerspiegeln,[54] z.T. werden die Studien zum *Privacy Paradox* deshalb methodisch kritisiert.[55] Aus rechtlicher Perspektive lässt sich die Frage darauf zuspitzen, ob schutzbezogene Vorgaben sich an der

---

50 *Gerber/Volkamer et al.*, in: (Fn. 33), S. 139,156 f.

51 *Ettig*, in: Taeger/Gabel (Hrsg.), , 4., völlig neu bearbeitete und wesentlich erweiterte Auflage 2022, § 25 TTDSG, Rn. 30 m.w.N.; *Weinzierl* NVwZ-Extra 2020, 1 ff.

52 *Waldman* Current Opinion in Psychology 31 (2020), 105 ff.

53 Überblick zu Verhaltensheuristiken und kognitivem Bias bei: *Gerber/Volkamer et al.*, in: (Fn. 33), S. 139, 148.

54 Dazu *Hermstrüwer* (Fn. 2), S. 233.

55 *Bunnenberg* (Fn. 36), S. 103; *Kokolakis* Computers & Security 64 (2017), 122 (130) regt an, dass Studien zum Privacy Paradox weniger auf Selbstberichten in Umfragen als auf Verhaltensanalysen beruhen sollten.

Selbsteinschätzung und ggf. auch den Wünschen der betroffenen Gruppe oder nach deren Verhalten orientieren sollten.

Hierbei ist wichtig, dass die Kontextabhängigkeit insbesondere bei Entscheidungen von Verbraucher:innen eine besondere Rolle spielt. Präferenzen werden schon deshalb nicht stets konsistent sein können, da die Situationen der Präferenzkundgabe und der tatsächlichen Datenfreigabe im digitalen Raum nicht deckungsgleich sind. Generelle Bedenken sind nicht mit situativen Bedenken gleichzusetzen. Die Absicht, sich selbst privatheitsschützend zu verhalten, kann mit situativen Problemen in Konflikt geraten und durch fehlendes Wissen, fehlende technische Expertise oder mangels Alternativen verstärkt werden.[56] Es kommt deshalb darauf an, welche Daten wem gegenüber offenbart werden. Auch die Persönlichkeitsmerkmale der Nutzer:innen können eine entscheidende Rolle spielen.[57] Unabhängig von den verschiedenen Theorien zu handlungsleitenden Faktoren besteht im digitalen Raum ein erhebliches Ungleichgewicht zwischen Nutzer:innen und Anbieter:innen digitaler Produkte. Deshalb ist eine rationale Entscheidungsfindung aufgrund unvollständiger Informationen, höchst komplexen Verarbeitungsvorgängen und Unkenntnis über die Datenverarbeitungen erheblich erschwert.

Rechtlich entscheidend für eine Einordnung des Privacy Paradoxes sind zudem die abstrakte Erkennbarkeit und das Verständnis darüber, welche Daten überhaupt wem gegenüber preisgegeben werden. Informationelle Asymmetrien und das systemische Ungleichgewicht zwischen Verbraucher:innen und Firmen bspw. im Kontext von Onlinedienstleistungen müssen bei der Bewertung des Verhaltens berücksichtigt werden.[58]

3. Rechtliche Implikationen des Privacy Paradox

Dass sich die Selbsteinschätzung nicht oder nur geringfügig im Verhalten von Nutzer:innen niederschlägt, führt zu der Frage, mit welchen Verhaltensannahmen Schutz durch Recht operiert und wie sich diese auf rechtliche Vorgaben auswirken. Das *Privacy Paradox* beschreibt damit im digitalen Bereich wohl vor allem ein Problem der mangelnden Informationsgrundlage und die erschwerte Möglichkeit rationaler Entscheidungen.

---

56 *Gerber/Volkamer et al.*, in: (Fn. 33), S. 139, 155.

57 *Wirth/Maier et al.* INTR 32 (2022), 24 ff. zu „Laziness" als Erklärung für das Privacy Paradox.

58 *Arpetti/Delmastro* Journal of Industrial and Business Economics 48 (2021), 505 (515).

Das Recht reflektiert diese realen Voraussetzungen von Privatheit bisher unzureichend, wie die Beispiele der datenschutzrechtlichen Einwilligung und des Wettbewerbsrechts zeigen.

3.1 Datenschutzrecht: Einwilligung als untaugliches rechtliches Instrument im digitalen Raum

Die DSGVO fordert stets eine Rechtsgrundlage für die Verarbeitung personenbezogener Daten nach der Grundregel des Art. 6 Abs. 1 DSGVO. Praktisch höchst relevant ist die zweckgebundene Einwilligungserklärung der von der Datenverarbeitung betroffenen Person nach Art. 6 Abs. 1 UAbs. 1 lit. a) DSGVO. Im digitalen Raum wird von dieser Ermächtigung zur Datenverarbeitung flächendeckend Gebrauch gemacht (Cookie-Banner, die bei jedem Webseitenbesuch über die Verarbeitung personenbezogener Daten informieren und dazu entsprechende Einwilligungen erfordern)[59] Die Kritik am Instrument der Einwilligung bleibt nicht auf die DSGVO beschränkt: Auch das TTDSG in Umsetzung der e-Privacy-Richtlinie[60] setzt in § 25 auf die Einwilligung als zentrales Instrument bei der Regulierung von Cookies und Tracking, wobei dort aber dieselben Anforderungen wie nach Art. 4 Nr. 11 DSGVO gelten.[61]

Die datenschutzrechtliche Einwilligung wird durch das *Privacy Paradox* weiter entwertet. Denn dass Personen in digitalen, durch Algorithmen kreierten oder gesteuerten Kontexten eine tatsächlich freie und vor allem informierte Entscheidung über die Zustimmung zur Verarbeitung ihrer persönlichen Daten treffen, kann nur schwer angenommen werden. Die Einwilligung geht, wie die *Rational Choice Theory*, von einer informierten Entscheidung aus.[62] Rational kalkulierte Kosten-Nutzen-Analysen sind bei Informationsasymmetrien aber in vielen Fällen nicht möglich. Nutzer:innen müssten umfassend unsichere, kaum greifbare und durch kom-

59 Vgl. nur EuGH, Urteil vom 1.10.2019 – C-673/17 – Planet-49 zur aktiven Einwilligungspflicht bei Cookiebannern.

60 RL 2022/58/EG.

61 Zur möglichen Ausgestaltung in der e-Privacy Verordnung, inbs. zur Frage der verpflichtenden Einwilligung (Cookie-Wall): *Schuhmacher/Sydow et al.* MMR 2021, 603 (608). Auch der Entwurf der e-Privacy Verordnung hält an der Einwilligung fest, COM 2017/010 final.

62 „informierte Einwilligung als Fiktion" m.w.N. *Kutscha*, in: Roßnagel/Friedewald/Hansen (Hrsg.), Die Fortentwicklung des Datenschutzes: Zwischen Systemgestaltung und Selbstregulierung, 2018, S. 123, 127; *Holland* Widener Law Journal 19 (2010), 893 (908).

plexe Prozesse entstehende Folgen ihrer Entscheidung berücksichtigen.[63] Eine vollständig rationale Entscheidung wird umso unwahrscheinlicher, je komplexer und unübersichtlicher der zu entscheidende Sachverhalt und die daraus folgenden Konsequenzen sind, z.B. auch die Auswirkung der eigenen Datenfreigabe auf andere Personen.[64]

Die Komplexität und Quantität der Datenverarbeitung wird durch transparenzsteigernde Maßnahmen wie Bildsymbole und *privacy agents*[65] auch nur bedingt reduziert, sondern vor allem verlagert. Denn auch eine gut illustrierte Datenschutzerklärung, die u.U. mehrere dutzend Verarbeiter:innen und Zwecke umfasst, wird wieder unübersichtlich. Auch Einwilligungsmanagementsysteme (Personal Information Management Systems – PIMS), müssen für eine informierte Nutzer:innenentscheidung über alle möglichen Folgen der Datenverarbeitungsvorgänge, z.B. des Trackings, informieren.[66] Dies erfordert einen erheblichen Detailgrad , der sich konträr zu dem abstrakt-generellen Ansatz solcher stellvertretenden Systeme verhält.[67]

Das *Privacy Paradox* spricht deshalb für eine Untauglichkeit der Einwilligung bei den großen social-media- und anderen Plattformen, im Onlineshopping und -dienstleistungsbereich und allen digitalen Umgebungen, die weitreichende quantitative Datenanalysen für und über Dritte ermöglichen.[68] Daneben spielen sozialer Druck und Monopolstellungen eine Rolle. Dadurch produzierte Informationsasymmetrien verhindern, dass eine informierte Entscheidung getroffen werden kann, weil z.B. die Konsequenzen der eigenen Datenpreisgabe für andere Nutzer:innen gar nicht bekannt ist. Somit kann das eigene Verhalten auch nicht adäquat den geäußerten Präferenzen angepasst werden.

Zudem ist die Einschätzung der Privatheitsrelevanz und damit die informierte Einwilligung praktisch gesehen auch deshalb erschwert, weil Maßstäbe zur Bewertung fehlen. Bei monetär-basierten Austauschgeschäften ist eine größere Vergleichbarkeit gegeben: Ein teureres Produkt verspricht, vereinfacht gesagt, oft eine höhere Qualität. Bei der Inanspruch-

63 *Hermstrüwer* (Fn. 2), S. 227 f.
64 Dazu *Mühlhoff*, S. 43 in diesem Band.
65 siehe dazu auch § 26 TTDSG.
66 *Botta* MMR 2021, 946 (948 f.).
67 *Botta* MMR 2021, 946 (949).
68 vgl. *Holland* Widener Law Journal 19 (2010), 893 (903). Dies gilt auch für smart wearables wie smart watches und andere Mobilgeräte, die sehr viele Daten verarbeiten und vor allem untereinander vernetzt sind. *Mühlhoff*, S. 44 f. in diesem Band.

nahme vermeintlich kostenloser Dienste gibt es hingegen keine Preisvergleichbarkeit. Verstärkt wird diese durch eine die Monopolstellung der globalen Plattformbetreiber, da es bereits an unterschiedlichen Angeboten fehlt. Es gibt beispielsweise keine Möglichkeit Google kostenpflichtig zu nutzen, ohne dass Daten gesammelt werden. Auch lassen die Anbieter:innen keine Verhandlungen über die Nutzungsbedingungen zu, auch wenn diese offenkundig rechtswidrig sind.

Das gängige Bild, wonach Vebraucher:innen mit ihren Daten „bezahlen“[69], trägt deshalb nicht.[70] Es besteht kein vergleichbares Bewusstsein über die Modalitäten der Datenverarbeitung wie bei der monetären Bezahlung über einen bestimmten Betrag, weil die „Kosten“ der Daten nicht sichtbar sind. Unternehmen verarbeiten Daten auf unterschiedliche Weise, weshalb aus Perspektive der Verbraucher:innen eine Einschätzung, die mit einer einheitlichen Währung vergleichbar wäre, nicht möglich ist.[71] Digitale Dienstleistungen sind deshalb näher an Vertrauensgütern, deren Wirkung weder vor noch nach dem Bezug valide eingeschätzt werden kann, ähnlich wie andere Bereiche in denen Expertise erforderlich ist, z.B. im medizinischen Sektor.[72] Solange Menschen Onlinedienste nutzen, online mit anderen interagieren oder staatliche Leistungen in Anspruch nehmen werden zudem stets neue Daten erzeugt, die dann keine begrenzte oder erschöpfliche Ressource mehr darstellen.[73]

Aus einer ökonomischen Perspektive stellt sich die Frage, ob digitale Märkte mit ihren jetzigen Angeboten die Privatsphäre-Präferenzen von Nutzer:innen erfüllen oder ob ein Marktversagen vorliegt. Dies führt zu Datenschutz als Wettbewerbsfaktor[74] und zum Verbraucher:innenschutz.

---

69 Zu Daten als Gegenleistung im Kontext des Schuldrechts: *Hacker* ZfPW 2019, 148 ff.; *Lohsse/Schulze et al.*, in: dies. (Hrsg.), Data as counter-performance - contract law 2.0?, 2020, S. 9 ff. *Scheibenpflug*, Personenbezogene Daten als Gegenleistung, 2022. Zur Einwilligung im Schuldrecht: *Riehm*, in: Specht-Riemenschneider/Buchner/Heinze et al. (Hrsg.), Festschrift für Jürgen Taeger, 2020, S. 55, 64 ff.

70 *Strandburg* University of Chicago Legal Forum 2013 (2015), 95 (130 ff.).

71 Vgl. *Grothe*, Datenmacht in der kartellrechtlichen Missbrauchskontrolle, 2019, S. 96. Die Annahme, dass Verbraucher:innen davon profitieren, dass ihnen personalisierte Werbung angezeigt wird, überzeugt hingegen auch vor dem Hintergrund des Privacy Paradoxs nicht. Denn die Personalisierung beruht auf der Verarbeitung personenbezogener bzw. gruppenbezogener Daten, widerspricht dann zumindest dem erwünschten Zustand des höheren Privatheitsschutzes.

72 *Strandburg* University of Chicago Legal Forum 2013 (2015), 95 (132).

73 *Grothe* (Fn. 71), S. 53.

74 Dazu auch: *Blankertz*, in: Selbstbestimmung, Privatheit und Datenschutz, 2022, S. 11 ff.

3.2 Wettbewerb und Verbraucherschutz

Privatheitsschutz durch Datenschutz kann theoretisch ein relevanter Wettbewerbsfaktor sein.[75] Durch das fehlende privatheitsschützende Verhalten der Nutzer:innen hat sich ein hohes Datenschutzniveau aber bisher kaum praktisch auf die Marktstellung von Unternehmen auswirken können: datensparsame Angebote haben sich trotz eines höheren Datenschutzniveaus nicht flächendeckend gegenüber datenintensiven Unternehmen und Angeboten durchsetzen können.[76] Bisher ist damit allein die Datenmacht bzw. der Datenbestand selbst ein positiver Wettbewerbsfaktor.[77]

Große Datenmengen, konzentriert bei wenigen Unternehmen, können den Wettbewerb hingegen negativ beeinflussen und ggf. auch Missbrauch fördern.[78] Das Privacy Paradox verstärkt diesen Effekt noch, wenn die Wahl der Verbraucher:innen nicht auf datenschützende Angebote fällt.[79] Fraglich ist aber, ob Verbraucher:innen überhaupt noch eine echte Wahl haben.[80] Durch die Konzentration auf Plattformen (insbesondere in sozialen Netzwerken) ist eine Abhilfe durch Wettbewerb schwierig.[81] Gerade dort, wo es um Vernetzung und Austausch geht, profitieren Anbieter:innen von Diensten mit besonders vielen Nutzer:innen; eine größere Anzahl an Alternativen ist gerade nicht gewünscht, sondern andernfalls eine alternative Konzentration.[82] Für Verbraucher:innen bestehen damit hohe Kosten, wenn sie sich über die Vor- und Nachteile informieren wollen. Lock-In- und Netzwerkeffekte erschweren einen Wechsel und damit ebenfalls eine andere Nachfrage.[83]

---

75 *Grothe* (Fn. 71), S. 60.

76 *Karaboga M./Martin et al.*, in: Roßnagel/Friedewald (Hrsg.), Die Zukunft von Privatheit und Selbstbestimmung, 2022, S. 49, 69 f.; *Körber* NZKart 2016, 303 (305).

77 Auf die Einzelheiten der wettbewerbsrechtlichen Implikationen kann hier nicht weiter eingegangen werden, aus der Rspr. vgl. nur BGHZ 226, 67 = GRUR 202, 1318 ff. zum missbräuchlichen Ausnutzen einer marktbeherrschenden Stellung durch Facebook.

78 *Grothe* (Fn. 71), S. 61; 67 ff.

79 Dies soll allerdings den Marktfunktionen selbst nicht entgegen stehen: *Weisser*, Datenbasierte Märkte im Kartellrecht, 2021, S. 108.

80 *Nocun*, in: Roßnagel/Friedewald/Hansen (Hrsg.), Die Fortentwicklung des Datenschutzes: Zwischen Systemgestaltung und Selbstregulierung, 2018, S. 39, 42.

81 *Kutscha*, in: Roßnagel/Friedewald/Hansen (Fn. 62), S. 123, 128.

82 Weiterführend: *Weisser* (Fn. 80), S. 253.

83 *Nocun*, in: Roßnagel/Friedewald/Hansen (Fn. 81), S. 39, 55.

3.3 Argument gegen Regulierung?

Aus dem *Privacy Paradox* wird zum Teil gefolgert, dass Privatheitsschutz von der überwiegenden Mehrheit nicht gewünscht wird, Privatheit ein überholtes Rechtsgut sei und die rechtliche Regulierung mit dem Schutzziel Privatheit, insbesondere durch Datenschutzrecht, ins Leere laufe. Dies fügt sich in eine generelle Kritik an Privatheitsschutz ein, wonach die Instrumente des Datenschutzes den Herausforderungen der digitalen Transformation nicht mehr gewachsen seien; rechtliche Regulierung sei stets zu spät oder ausgeschlossen. Andere sehen die digitale Transformation als zwingende Entwicklung, die unumkehrbaren systemischen Logiken folgt. Entscheidend für Legitimität und Akzeptanz sei allein das Funktionieren digitaler Technik.[84]

Die Einwände tragen aus verschiedenen Gründen nicht, denn die Entscheidungsfindung von Individuen ist von zahlreichen Faktoren abhängig, die im Kontext von privatheitsrelevantem Verhalten z.T. verzerrt oder nicht gegeben sind. Unvollständige oder asymmetrische Informationen führen dazu, dass viele Personen sich den mit ihrem Verhalten verbundenen Datenanalysen nicht bewusst sind, aber dennoch der Datenweitergabe an Dritte zustimmen.[85] Durch die Unmöglichkeit eines monetären Referenzpunktes für die eigenen Daten wird die Einschätzung von „Leistung und Gegenleistung" zusätzlich erschwert. [86] Bereits die Unterscheidung zwischen Metadaten, Nutzungsdaten und selbst freigegebenen persönlichen Daten (self-disclosure) spielt eine entscheidende Rolle. Denn die verschiedenen Arten von Daten sind unterschiedlich kontrollierbar. Es geht eben nicht nur darum, keine sensiblen persönlichen Informationen auf sozialen Netzwerken zu posten, sondern es werden Daten durch die schlichte Nutzung verarbeitet und neue Daten entstehen durch den Vorgang der Kommunikation an sich.[87] Die Verarbeitung von Meta- und Nutzungsdaten hat mit der rechtlichen Idee der autonomen Entscheidung des Individuums über persönliche Informationen nicht mehr viel gemein, da sie individuelle Eigenschaften und Verhaltensweisen ebenso offenlegen können.

---

84 *Leopold*, in: Piallat (Fn. 16), S. 167, 170.

85 *Arpetti/Delmastro* Journal of Industrial and Business Economics 48 (2021), 505 (511).

86 *Arpetti/Delmastro* Journal of Industrial and Business Economics 48 (2021), 505 (507).

87 Zum Real-Time Bidding: *Herbrich/Niekrenz* CR 2021, 129

Diese Diskrepanz zwischen Selbsteinschätzung und realem Verhalten sollte vom Recht nicht unbeachtet bleiben, entscheidend ist aber die Frage der Konsequenz. Zum einen legt das *Privacy Paradox* das Dilemma offen, dass die Einschätzung und das tatsächliche Verhalten von Menschen stets kontextabhängig zu betrachten sind, Kontextverlust aber gerade das Ziel von quantitativer Datenverarbeitung ist, weil gerade eine multifunktionale Verwendung angestrebt wird. Als tragfähiges Argument gegen Regulierung, Daten- und Privatheitsschutz taugt das *Privacy Paradox* deshalb nicht. Das *Privacy Paradox* spricht nicht gegen eine Regulierung, sondern nur dafür, dass die bisherigen Mechanismen unzureichend sind. Denn gegen die Straßenverkehrsordnung (StVO) spricht auch nicht, dass sich viele Menschen nicht an Verkehrsregeln halten, das Erfordernis für die Regelungen der StVO ist, dass viele Menschen am Verkehr teilnehmen. Dies ist auf den Daten- und Privatheitsschutz im digitalen Zeitalter übertragbar.[88]

3.4. Privacy Paradox als Mythos?

Die Kritik am *Privacy Paradox* zielt primär auf unzutreffende Grundannahmen aufgrund der bereits geschilderten Gegebenheiten in digitalen Sphären. Verhaltenspsychologische Implikationen sollten nicht generell-abstrakt, sondern kontextualisiert betrachtet werden. Das *Privacy Paradox* hingegen sei ein Mythos.[89]

Das *Privacy Paradox* ist weder Mythos noch ein tatsächliches Paradox, sondern ein Dilemma. Es illustriert, parallel zu vielen rechtlichen Vorgaben, dass im digitalen Bereich immer noch aufgrund unzutreffender Grundannahmen operiert wird, die im analogen Bereich effektiv sein mögen, aber in online-basierten Umgebungen ins Leere laufen.

Es gibt inzwischen immer weniger Möglichkeiten online aktiv zu sein, ohne Daten mit den global führenden Onlineunternehmen zu teilen. Alternativangebote z.B. zu Googles Suchmaschine, haben sich zwar gehalten, sind aber Nischenprodukte geblieben. Zudem wird die Onlinepräsenz immer mehr mit sozialem Kapital verbunden. Technologien wie biome-

88 Zum Datenschutz als Kommunikationsordnung: *Roßnagel*, Datenschutz in einem informatisierten Alltag, 2007.

89 *Solove* The George Washington Law Review 89 (2021), 1 ff. „Relikt der Vergangenheit" *Dienlin*, The psychology of privacy: Analyzing processes of media use and interpersonal communication, 2017, S. 78. Hingegen Forderung nach mehr Forschung, um Kausalbeziehungen aufzudecken: *Dienlin/Masur et al.* New Media & Society 2021, 1 (18).

trische Gesichtserkennung in Echtzeit bieten den Menschen gar nicht die Möglichkeit, Privatheit überhaupt paradox erscheinen zu lassen – sie haben schlicht keine Wahl solchen Maßnahmen, wenn sie bspw. auf öffentlichen Plätzen angewendet werden, zu entgehen. Für Widersprüche zwischen Selbsteinschätzung und Verhalten bleibt dann kein Raum mehr. Selbiges gilt für das omnipräsente Tracking als unwissentliche Speicherung von Daten in digitalen Umgebungen, was zu einer Intransparenz gegenüber den Folgen des eigenen Handelns führt, da keine Nachvollziehbarkeit mehr gegeben ist, und Verhaltensmanipulationen ermöglicht werden.

Die Grundannahme des *Privacy Paradox*, dass es Ausdruck der eigenen Autonomie ist, Daten selbst preiszugeben, setzt reale und effektive Entscheidungsmöglichkeiten voraus. Um entscheiden zu können, sind Alternativen und Informationen erforderlich. Die Funktionsweise der prädiktiven Analytik führt dazu, dass Verhaltensweisen und Charakteristiken von Personen dauerhaft prognostiziert werden. Die Verletzung der Privatsphäre erfolgt dann nicht durch die gezielte Zweckentfremdung oder Entwendung vorhandener Daten, sondern dadurch, dass sensible Informationen vorhergesagt werden.[90] Die Privatsphäre wird nicht durch die Preisgabe, sondern durch die Entstehung neuer Daten verletzt: durch die Prognose bestimmter Verhaltensweisen aus einem kollektiven Datenpool.[91] Selbst wenn der eigenen Datenverarbeitung widersprochen wird, kann die kollektive Datenanalyse Rückschlüsse auf die eigene Person zulassen. Damit haben es Bürger:innen sowohl bei staatlichen als auch bei privaten prädiktiven Analysen nicht mehr selbst in der Hand, durch eigenes Verhalten einer Erfassung und digitalen Datenverarbeitung zu entgehen.[92] Dies führt ebenfalls dazu, dass bereits keine Divergenz zwischen Selbsteinschätzung und Verhalten entstehen kann, da die Privatheitsverletzung bereits vor dem tatsächlichen Verhalten stattfindet.[93]

---

90 Dazu *Mühlhoff*, S. 40 ff. in diesem Band.

91 Zum Konzept der prädiktiven Privatheit bereits auch: *Mühlhoff* Ethics Inf Technol 2021, 675.

92 *Hermstrüwer*, in: Hoffmann-Riem (Hrsg.), Big Data - Regulative Herausforderungen, 2018, S. 99, 100 f. ordnet dies als Marktversagen ein.

93 *Mühlhoff* Ethics Inf Technol 2021, 675 (679).

4. Reaktionen des Rechts: Privacy kein Paradox

Das *Privacy Paradox* ist ein Anwendungsfall für Grundfragen der Verhaltensannahmen im Recht und durch Recht.[94] Rechtswissenschaft betrachtet menschliches Verhalten nicht voraussetzungslos, sondern unter dem Blickwinkel einer Norm, weshalb auch kein rechtswissenschaftliches Verhaltensmodell existiert.[95] Die Diskussion effizienter rechtlicher Regulierungen setzt unter anderem voraus, dass zutreffende Annahmen über menschliches Verhalten gemacht werden müssen.

Als Strategien gegen das Privacy Paradox wird die verstärkte Nutzbarkeit von Wissen, insbesondere auch von prozeduralem Wissen, keine Pathologisierung von Onlineverhalten sowie anwendungsbezogene Strategien im Umgang mit Internetangeboten diskutiert.[96]

Das größte Problem sind aber weiterhin solche Daten, die Personen ohnehin nicht kontrollieren können. Dagegen schafft das Bewusstsein darüber, an welchen Stellen persönliche Informationen generiert und verarbeitet werden nur bedingt Abhilfe, wenn dies ohnehin Dauerzustand ist. Die Schaffung von mehr Wissen hilft Ausflüssen wie dem Real-Time Bidding[97] nicht ab und führt ohne reale Handlungsmöglichkeiten zur Resignation. Dass digitale Umgebungen inzwischen wichtige Infrastrukturen sind, entkräftet das Argument einer individuellen Entscheidung, diese Dienste nicht zu nutzen. Der gesellschaftliche Aspekt des sozialen Kapitals und der Auswirkungen digitaler Anwendungen spricht gegen die schlichte Ablehnung der Nutzung datenintensiver Dienste in der Verantwortung des Einzelnen. Entsprechend ist eine institutionelle oder systemisch Regulierung auch erforderlich, die bspw. durch Zertifizierung, datenschutzfreundliche Entscheidungen erleichtert.

Privatheit als Konzept in der Vorstellung vieler Menschen kann unendlich viele Facetten abdecken, die sich nur teilweise oder auch gar nicht mit konkreten persönlichen Verhaltensweisen überschneiden. Der Schluss von menschlichem Verhalten als nach außen gerichtetem Akt auf innere

---

94 eingehend dazu bspw.: *van Aaken*, in: Führ/Bizer/Feindt (Hrsg.), Menschenbilder und Verhaltensmodelle in der wissenschaftlichen Politikberatung, 2007, S. 70 ff.; *Lepsius*, in: Führ/Bizer/Feindt (Hrsg.), Menschenbilder und Verhaltensmodelle in der wissenschaftlichen Politikberatung, 2007, S. 168 ff.; Towfigh/Petersen (Hrsg.), Ökonomische Methoden im Recht, , 2. Aufl., 2017, § 8 Verhaltensökonomik, S. 237 ff.;

95 *Lepsius*, in: Führ/Bizer/Feindt (Fn. 95), S. 168, 169.

96 *Gerber/Volkamer et al.*, in: (Fn. 33), S. 139, 158 ff.

97 *Herbrich/Niekrenz* CR 2021, 129 ff.

Einstellungen wie das Verständnis von Privatheit muss kritisch hinterfragt werden. Das *Privacy Paradox* illustriert diese verschiedenen Probleme von Privatheitsschutz in digitalen Kontexten.

Maßstab für die Regulierung im Datenschutzrecht kann deshalb nicht nur sein, dass Nutzer:innenverhalten zu untersuchen, sondern zu klären, welche Normen und Erwartungen durch die Datenverarbeitung verletzt werden. Vielmehr sollte Regulierung sich auch auf die andere Seite der Datennutzung konzentrieren und nicht alles in Nutzer:innenhand legen.

Transparenz wird oft angeführt, z.B. wenn es um Datenschutzerklärungen geht. Transparenz allein ist nicht ausreichend, es braucht Verständlichkeit und freie Wahl mehrerer Optionen. Mehr Entscheidungsoptionen führen nicht automatisch zu mehr Kontrolle. Nur wenn auch tatsächlich vollständige Informationen als Entscheidungsgrundlage vorliegen, ist die kalkulierte „informationelle Selbstgefährdung“[98] Ausdruck der individuellen Autonomie. Eine umfassende Transparenz und Offenlegung über alle relevanten Faktoren erreichen allein noch keine informierte Entscheidung. Im Kontext von Onlinediensten erscheint dies ohnehin illusorisch, da die Vorgänge der Datenverarbeitung schlicht zu komplex sind. Die Menge an Informationen würde nicht zu tatsächlichem Verständnis führen, sondern ins nächste Paradox: nach dem „transparency paradox“ wird zwar Transparenz durch detaillierte Aufklärung erzeugt, die Quantität der Informationen erschwert aber den Blick auf das Wesentliche.

Es sollte deshalb **generelle Ziele** des Privatheitsschutzes geben, der möglicherweise nicht nur als subjektives Recht zu konstruieren ist. Das kann auf Tatbestands- oder Vollzugsebene passieren, wie durch privacy by default and by design, Art. 25 ff. DSGVO. Situationsspezifische Besonderheiten sind zu berücksichtigen, z.B. durch besondere Darlegungspflichten in der konkreten Transaktion. Die europäische Verbandsklagerichtlinie hat zudem bspw. erstmals über Art. 80 DSGVO hinaus explizite kollektive Rechtsschutzmöglichkeiten gegen Datenschutzverstöße eingeführt.[99]

Zudem ist das Credo **der rein individuellen Risikobewertung** in digitalen Kontexten nicht ausreichend. Das Internet führt zwangsläufig zu einem Kontrollverlust über die eigene Selbstdarstellung, da es keinen zumutbaren Überblick mehr über die personenbezogenen gespeicherten

98 *Eichenhofer* (Fn. 9), S. 98; *Hermstrüwer* (Fn. 2).

99 RL 2020/1828, Anhang I (56) nennt die DSGVO als Anwendungsbereich. Zum kollektiven Rechtsschutz und strategischer Prozessführung gegen Datenschutzkonzerne: *Ruschemeier* MMR 2021, 942 ff.

Daten gibt. Dem wirken Entwicklungen wie das „Recht auf Vergessen“[100] oder dem „Right to reasonable inferences“[101] nur sehr punktuell entgegen und setzen vor allem die Kenntnis der Datenspeicherung voraus. Neben individuellen Faktoren sind **systemische Gegebenheiten,** wie faktische Monopolstellungen großer Digitalkonzerne in bestimmten Bereichen der Sozialen Medien oder Messengerdienste, relevante Einflüsse. Rechtliche Regulierungsansätze sollten systemische Risiken und die Strukturen von Datenverarbeitung, -übermittlung und -bereitstellung stärker in den Blick nehmen anstatt den Privatheitsschutz als rein subjektive Angelegenheit des jeweiligen Verarbeitungsvorgangs zu begreifen. In einigen Bereichen, wie z.B. bei Kindern, sollte die Einwilligung als Rechtmäßigkeit der Datenverarbeitung ausgeschlossen sein.[102] Zudem sollte erwogen werden, die Einwilligung in Situationen, in denen sie offensichtlich ihren Zweck nicht erfüllt (Beispiel: Cookie-Banner) unter erhöhte Rechtmäßigkeitsanforderungen zu stellen, wie eine Evaluation der tatsächlichen Wahrnehmung und Verarbeitung der Informationen durch vorgegebene Zeiten zur Anzeige der Einwilligungserklärung oder Kontrollfragen, die sich auf das Verständnis beziehen. Dadurch wird die Einwilligung im Massengeschäft unattraktiv und Anbieter:innen wären angehalten, sich z.B. um eine Zertifizierung zu bemühen.

Vermeintliche Regulierungen von Technik allein sind nicht zielführend, tatsächlich adressieren diese ohnehin die rechtsrelevanten Auswirkungen von Technik. Zukünftige Regelwerke sollten den Einfluss auf Privatheit individuell und in der Breite stärker in den Blick nehmen. Dazu gehört es auch, sozialwissenschaftliche und psychologische Implikationen stärker zu reflektieren.[103] Konkrete datenschutzrelevante Anwendungsszenarien, insbesondere bei der Verhaltensbeeinflussung oder -steuerung können risikobasiert klassifiziert werden. In diese Richtung deutet auch der Vorschlag der Europäischen Kommission zum Artificial Intelligence Act, der allerdings in der jetzigen Fassung zu weitreichende Ausnahmen für bestimmte KI-Anwendungsszenarien vorsieht, welche grundrechtlich problematisch sind.[104] Bestimmte, besonders privatheitsgefährdende Praktiken,

100 EuGH, Urteil vom 13.5.2014 – C-131/12 = CELEX 62012CJ0131. Der EuGH verwendet den Begriff „Recht auf Vergessenwerden“.

101 *Wachter/Mittelstadt* Columbia Business Law Review 2019, 1 ff.

102 *Roßnagel/Geminn*, Datenschutz-Grundverordnung verbessern, 2020, S. 118.

103 Dazu auch *Martini/Weinzierl* RW 2019, 287 ff. Zu den sozio-technischen Aspekten: *Mühlhoff* New Media & Society 22 (2020), 1868.

104 COM/2021/206 final.

wie z.B. KI-basierte Echtzeitgesichtserkennung oder andere biometrische Analysen sollten mit Verboten belegt werden.[105]

5. Conclusio

Das sogenannte *Privacy Paradox* ist kein Paradox, sondern ein Dilemma, welches durch digitale Umgebungen, Techniken und ihre Strukturen bedingt ist, auf die Einzelpersonen keinen oder nur wenig Einfluss haben. *Privacy by default and by design*[106] sind ergänzende, verheißungsvolle technische Lösungen, müssten aber konkretisiert und durchsetzbar gemacht werden. Das *Privacy-Dilemma* lässt sich durch den Abbau asymmetrischer Machtstrukturen zumindest abschwächen, bspw.. wenn die Gruppe der Verbraucher:innen eine tatsächliche Kalkulation aufgrund einer vollständigen Informationsgrundlage und daraus abgeleiteten informierten Risikoeinschätzung treffen kann, durch institutionelle Unterstützung, wie z.B. Zertifizierung. Letztlich sollte der Fokus auf kollektive Aspekte von Privatheit und Datenschutz gelenkt werden, um die Konzentration auf die Verantwortlichkeit des Individuums aufzulösen und dadurch schließlich auch das *Privacy Paradox*.[107] Das Ziel, Machtasymmetrien auszugleichen, ist keine paternalistische Bevormundung, sondern die notwendige Schaffung eines Freiheitsraumes. Ein anderer Weg ist es, anonyme Kommunikationsräume für die breite Nutzung zu popularisieren. Eine vollständige Ökonomisierung oder Tokenisierung aller Güter und damit auch der persönlichen Daten, über die Nutzer:innen ihre Daten dann an Anbieter:innen im Web 3.0 verkaufen können, wird hingegen das Problem der Machtasymmetrie nicht lösen, sondern reproduzieren.

Literatur

Acquisti, A./*Grossklags*, J., Privacy and rationality in individual decision making, IEEE Secur. Privacy Mag. 3 (2005), S. 26–33.

105 *Ebers/Hoch et al.* RDi 2021, 528 (530 ff.). Der Entwurf der KI-Verordnung umfasst allerdings nur sehr enge Anwendungsbereiche, z.B. ist das Verbot des „social scorings" in Art. 5 Abs. 1 c) auf staatliche Stellen begrenzt.

106 *Rubinstein* Berkeley Technology Law Journal 26 (2011), 1409 (1414 ff.)

107 Vgl. nur *Ben-Shahar* Journal of Legal Analysis 11 (2019), 104 (107 ff.)

Acquisti, Alessandro/*Brandimarte*, Laura/*Loewenstein*, George, Privacy and human behavior in the age of information, Science (New York, N.Y.) 347 (2015), S. 509–514.

Arpetti, Jacopo/*Delmastro*, Marco, The privacy paradox: a challenge to decision theory?, Journal of Industrial and Business Economics 48 (2021), S. 505–525.

Barth, Susanne/*Jong*, Menno D.T. de, The privacy paradox – Investigating discrepancies between expressed privacy concerns and actual online behavior – A systematic literature review, Telematics and Informatics 34 (2017), S. 1038–1058.

Belliger, Andréa/*Krieger*, The Privacy Paradox, in: Belliger, Andréa/Krieger, David J. (Hrsg.), Network Publicy Governance, 2018, S. 45–76.

Bennett, Colin J., Privacy in the Political System: Perspectives from Political Science and Economics 1995, revised 2001.

Ben-Shahar, Omri, Data Pollution, Journal of Legal Analysis 11 (2019), S. 104–159.

Beresford, Alastair R./*Kübler*, Dorothea/*Preibusch*, Sören, Unwillingness to pay for privacy: A field experiment, Economics Letters 117 (2012), S. 25–27.

Bretthauer, Sebastian, § 2 Verfassungsrechtliche Grundlagen, Europäisches und nationales Recht, in: Specht-Riemenschneider, Louisa/Mantz, Reto (Hrsg.), Handbuch europäisches und deutsches Datenschutzrecht, Bereichsspezifischer Datenschutz in Privatwirtschaft und öffentlichem Sektor, München, 2019.

Britz, Gabriele, Freie Entfaltung durch Selbstdarstellung, Eine Rekonstruktion des allgemeinen Persönlichkeitsrechts aus Art. 2 I GG, Tübingen 2007.

dies., Informationelle Selbstbestimmung zwischen rechtswissenschaftlicher Grundsatzkritik und Beharren des Bundesverfassungsgerichts, in: Hoffmann-Riem, Wolfgang (Hrsg.), Offene Rechtswissenschaft, Tübingen 2010, S. 561-596.

Bunnenberg, Jan Niklas, Privates Datenschutzrecht, Über Privatautonomie im Datenschutzrecht - unter besonderer Berücksichtigung der Einwilligung und ihrer vertraglichen Kopplung nach Art. 7 Abs. 4 DS-GVO, Baden-Baden 2020.

Culnan, Mary J./*Armstrong*, Pamela K., Information Privacy Concerns, Procedural Fairness, and Impersonal Trust: An Empirical Investigation, Organization Science 10 (1999), S. 104–115.

Dienlin, Tobias, The psychology of privacy: Analyzing processes of media use and interpersonal communication 2017. *ders*., Das Privacy Paradox aus psychologischer Perspektive, in: Specht-Riemenschneider, Louisa/Werry, Nikola/Werry, Susanne (Hrsg.), Datenrecht in der Digitalisierung, Berlin, 2020, S. 305–323.

Dienlin, Tobias/*Masur*, Philipp K./*Trepte*, Sabine, A longitudinal analysis of the privacy paradox, New Media & Society 2021, S. 1–22.

Dienlin, Tobias/*Metzger J.M.*, An extended privacy calculus model for SNSs—Analyzing self-disclosure and privacy behaviors in a representative U.S. sample, Journal of Computer-Mediated Communication,, S. 368–383.

Ebers, Martin/*Hoch*, Veronica/*Rosenkranz*, Frank/*Ruschemeier*, Hannah/*Steinrötter*, Björn, Der Entwurf für eine EU-KI-Verordnung: Richtige Richtung mit Optimierungsbedarf, RDi 2021, S. 528–537.

Eichenhofer, Johannes, e-Privacy, Theorie und Dogmatik eines europäischen Privatheitsschutzes im Internet-Zeitalter, Tübingen 2021.

Englerth, Markus/*Towfigh*, Emanuel V., § 8 Verhaltensökonomik, in: Towfigh, Emanuel V./Petersen, Niels (Hrsg.), Ökonomische Methoden im Recht, Eine Einführung für Juristen. 2. Auflage, Tübingen, 2017, S. 237–274.

Führ, Martin/*Bizer*, Kilian/*Feindt*, Peter H. (Hrsg.), Menschenbilder und Verhaltensmodelle in der wissenschaftlichen Politikberatung, Möglichkeiten und Grenzen interdisziplinärer Verständigung, Baden-Baden 2007.

Ganz, Kathrin, Die Netzbewegung, Subjektpositionen im politischen Diskurs der digitalen Gesellschaft, Leverkusen 2018.

Garcia, David, Leaking privacy and shadow profiles in online social networks, Science Advances 2017, e1701172.

Gerber, Nina/*Gerber*, Paul/*Volkamer*, Melanie, Explaining the privacy paradox: A systematic review of literature investigating privacy attitude and behavior, Computers & Security 77 (2018), S. 226–261.

Gerber, Paul/*Volkamer*, Melanie/*Gerber*, Nina, Das Privacy-Paradoxon - Ein Erklärungsversuch und Handlungsempfehlungen, in: Dialogmarketing Perspektiven 2016/2017: Tagungsband 11. wissenschaftlicher interdisziplinärer Kongress für Dialogmarketing, , Wiesbaden, 2017, S. 139–167.

Gilovich, Thomas/*Griffin*, Dale W./*Kahneman*, Daniel (Hrsg.), Heuristics and biases, The psychology of intuitive judgment, Cambridge 2002.

Grothe, Nela, Datenmacht in der kartellrechtlichen Missbrauchskontrolle, Baden-Baden 2019.

Gruschke, Daniel, Über Post-Privacy, in: Kappes, Christoph/Krone, Jan/Novy, Leonard (Hrsg.), Medienwandel kompakt 2011 - 2013: Netzveröffentlichungen zu Medienökonomie, Medienpolitik & Journalismus, Wiesbaden, 2014, S. 79–85.

Gusy, Christoph, Was schützt Privatheit?, in: Jahrbuch des öffentlichen Rechts der Gegenwart. Neue Folge 70 (2022), S. 415-451.

Hacker, Philipp, Daten als Gegenleistung, Rechtsgeschäfte im Spannungsfeld von DS-GVO und allgemeinem Vertragsrecht, ZfPW 2019, S. 148–197.

Hagendorff, Thilo, Post-Privacy oder der Verlust der Informationskontrolle, in: Behrendt, Hauke/Loh, Wulf/Matzner, Tobias u. a. (Hrsg.), Privatsphäre 4.0: Eine Neuverortung des Privaten im Zeitalter der Digitalisierung, Stuttgart, 2019, S. 91–106.

Herbrich, Tilman/*Niekrenz*, Elisabeth, Privacy Litigation Against Real-Time Bidding, CR 2021, S. 129–141.

Hermstrüwer, Yoan, Informationelle Selbstgefährdung, Tübingen 2015.

ders., Die Regulierung prädiktiver Analytik: eine juristisch-verhaltenswissenschaftliche Skizze, in: Hoffmann-Riem, Wolfgang (Hrsg.), Big Data – Regulative Herausforderungen, Baden-Baden 2018.

Holland, Brian H., "Privacy Paradox 2.0," Widener Law Journal 19, no. 3 (2010), S. 893-932.

Jajodia, Sushil/*Samarati*, Pierangela/*Yung*, Moti (Hrsg.), Encyclopedia of Cryptography, Security and Privacy, Berlin, Heidelberg 2019.

Jolls, Christine/*Sunstein*, Cass/*Thaler*, Richard H., A Behavioral Approach to Law and Economics, Stanford Law Review 50 (1998), S. 1471–1489.

Kappes, Christoph/*Krone*, Jan/*Novy*, Leonard (Hrsg.), Medienwandel kompakt 2011 - 2013: Netzveröffentlichungen zu Medienökonomie, Medienpolitik & Journalismus, Wiesbaden 2014.

Kokolakis, Spyros, Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon, Computers & Security 64 (2017), S. 122–134.

Körber, Torsten, „Ist Wissen Marktmacht?" Überlegungen zum Verhältnis von Datenschutz, „Datenmacht" und Kartellrecht - Teil 1, NZKart 2016, S. 303–310.

Kutscha, Martin, Schutzpflicht des Staates für die informationelle Selbstbestimmung?, in: Roßnagel, Alexander/Friedewald, Michael/Hansen, Marit (Hrsg.), Die Fortentwicklung des Datenschutzes: Zwischen Systemgestaltung und Selbstregulierung, Wiesbaden, 2018, S. 123–137.

Laufer, Robert S./*Wolfe*, Maxine, Privacy as a Concept and a Social Issue: A Multidimensional Developmental Theory, Journal of Social Issues 33 (1977), S. 22–42.

Leopold, Nils, Privatheit, in: Piallat, Chris (Hrsg.), Der Wert der Digitalisierung, 2021, S. 167–186.

Lepsius, Oliver, Menschenbilder und Verhaltensmodelle – Ergebnisse aus der Perspektive der Rechtswissenschaft, in: Führ, Martin/Bizer, Kilian/Feindt, Peter H. (Hrsg.), Menschenbilder und Verhaltensmodelle in der wissenschaftlichen Politikberatung, , Möglichkeiten und Grenzen interdisziplinärer Verständigung, Baden-Baden, 2007, S. 168–179.

Lohsse, Sebastian/*Schulze*, Reiner/*Staudenmayer*, Dirk, Data as Counter-Performance – Contract Law 2.0? An Introduction, in: Lohsse, Sebastian/Schulze, Reiner/Staudenmayer, Dirk (Hrsg.), Data as counter-performance - contract law 2.0?, , Münster Colloquia on EU Law and the Digital Economy V, Baden-Baden, London, 2020, S. 9–22.

Martini, Mario/*Weinzierl*, Quirin, Mandated Choice: der Zwang zur Entscheidung auf dem Prüfstand von Privacy by Default (Art. 25 Abs. 2 S. 1 DSGVO), RW 2019, S. 287–316.

Masur, Philipp K., Mehr als Bewusstsein für Privatheitsrisiken. Eine Rekonzeptualisierung der Online- Privatheitskompetenz als Kombination aus Wissen, Fähig- und Fertigkeiten, M&K Medien & Kommunikationswissenschaft 66 (2018), S. 446–465.

Mayer, Fabian, Wie viel wissen Sie wirklich über Clickbait? – 7 überraschende Fakten, von denen Sie so noch nie gehört haben!, in: Appel, Markus (Hrsg.), Die Psychologie des Postfaktischen: Über Fake News, „Lügenpresse", Clickbait & Co, , Berlin, Heidelberg, 2020, S. 67–79.

McDonald, Aleecia M.; *Cranor*; Lorrie Faith, The Cost of Reading Privacy Policies, I/S: A Journal of Law and Policy for the Information Society 2008, S. 543-568.

Mühlhoff, Rainer, Predictive privacy: towards an applied ethics of data analytics, Ethics Inf Technol 2021, S. 675-690.

Münch, Ingo von/*Kunig*, Philip (Hrsg.), Grundgesetz Kommentar, 7. Aufl., München 2021.

Nocun, Katharina, Datenschutz unter Druck: Fehlender Wettbewerb bei sozialen Netzwerken als Risiko für den Verbraucherschutz, in: Roßnagel, Alexander/Friedewald, Michael/Hansen, Marit (Hrsg.), Die Fortentwicklung des Datenschutzes: Zwischen Systemgestaltung und Selbstregulierung, Wiesbaden, 2018, S. 39–58.

Norberg, Patricia./*Horne*, Daniel/*Horne*, David, The Privacy Paradox: Personal Information Disclosure Intentions versus Behaviors, Journal of Consumer Affairs 41 (2007), S. 100–126.

Øverby, Harald, The Privacy Paradox, in: Jajodia, Sushil/Samarati, Pierangela/Yung, Moti (Hrsg.), Encyclopedia of Cryptography, Security and Privacy, Berlin, Heidelberg, 2019, S. 1–2.

Riehm, Thomas, Daten als Gegenleistung?, in: Specht-Riemenschneider, Louisa/Buchner, Benedikt/Heinze, Christian u. a. (Hrsg.), Festschrift für Jürgen Taeger, IT-Recht in Wissenschaft und Praxis, Frankfurt am Main, 2020, S. 55–77.

Rubinstein, Ira S., Regulating Privacy by Design, Berkeley Technology Law Journal 26 (2011), S. 1409–1456.

Ruschemeier, Hannah, Kollektiver Rechtsschutz und strategische Prozessführung gegen Digitalkonzerne. Viele Davids gegen Goliath?, MMR 2021, S. 942–946.

Sandfuchs, Barbara, Privatheit wider Willen?, Verhinderung informationeller Preisgabe im Internet nach deutschem und US-amerikanischem Verfassungsrecht, Tübingen 2015.

Scheibenpflug, Andreas, Personenbezogene Daten als Gegenleistung. Ein Beitrag zur rechtlichen Einordnung datengetriebener Austauschverhältnisse, Berlin 2022.

Schuhmacher, Pascal/*Sydow*, Lennart/*Schönfeld*, Max von, Cookie Compliance, quo vadis? Datenschutzrechtliche Perspektiven für den Einsatz von Cookies und Webtracking nach TTDSG und ePrivacy-VO, MMR 2021, S. 603–609.

Schwichtenberg, Simon, Datenschutz in drei Stufen: Ein Auslegungsmodell am Beispiel des vernetzten Automobils, Wiesbaden 2018.

Slovic, P., Finucane, M., Peters, E., & MacGregor, D., The Affect Heuristic, in: Gilovich, Thomas/Griffin, Dale W./Kahneman, Daniel (Hrsg.), Heuristics and biases, The psychology of intuitive judgment, Cambridge, 2002, S. 397–420.

Solove, Daniel J., The Myth of the Privacy ParadoxThe George Washington Law Review 89 (2021), S. 1–51.

Spiekermann, Sarah/*Grossklags*, Jens/*Berendt*, Bettina, E-privacy in 2nd generation E-commerce, in: Proceedings of the 3rd ACM conference on Electronic Commerce - EC ,01, 2001.

Stahl, Titus, Privacy in Public: A Democratic Defense, Moral Philosophy and Politics 7 (2020), S. 73–96.

Strandburg, Katherine, Free Fall: The Online Market's Consumer Preference Disconnect, University of Chicago Legal Forum 2013 (2015), https://chicagounbound.uchicago.edu/uclf/vol2013/iss1/5.

Taddicken, Monika, The 'Privacy Paradox' in the Social Web: The Impact of Privacy Concerns, Individual Characteristics, and the Perceived Social Relevance on Different Forms of Self-Disclosure, J Comput-Mediat Comm 19 (2014), S. 248–273.

Taeger, Jürgen/*Gabel*, Detlev (Hrsg.), DSGVO - BDSG - TTDSG, Kommentar, 4. Auflage, Frankfurt am Main 2022.

Towfigh, Emanuel V./*Petersen*, Niels (Hrsg.), Ökonomische Methoden im Recht, Eine Einführung für Juristen, 2. Auflage, Tübingen 2017.

Turow, Joseph/*Hennessy*, Michael, Internet privacy and institutional trust, New Media & Society 9 (2007), S. 300–318.

Tversky, Amos/*Kahneman*, Daniel, Judgment under Uncertainty: Heuristics and Biases, Science 185 (1974), S. 1124–1131.

van Aaken, Anne, Recht und Realanalyse – welches Modell menschlichen Verhaltens braucht die Rechtswissenschaft?, in: Führ, Martin/Bizer, Kilian/Feindt, Peter H. (Hrsg.), Menschenbilder und Verhaltensmodelle in der wissenschaftlichen Politikberatung, , Möglichkeiten und Grenzen interdisziplinärer Verständigung, Baden-Baden, 2007, S. 70–95.

Vidhani, Kumar/*Banahatti*, Vijayanand/*Lodha*, Sachin, Challenges in enabling privacy self management, CSI Transactions on ICT 9 (2021), S. 185–191.

von Lewinski, Kai, Die Matrix des Datenschutzes, Tübingen 2014.

Waldman, Ari Ezra, Cognitive biases, dark patterns, and the ‚privacy paradox', Current Opinion in Psychology 31 (2020), S. 105–109.

Warren, Samuel D./*Brandeis*, Louis D., The Right to Privacy Harvard Law Review 4 (1890), S. 193–220.

Weinzierl, Quirin, Dark Patterns als Herausforderung für das Recht Rechtlicher Schutz vor der Ausnutzung von Verhaltensanomalien, NVwZ-Extra 2020, S. 1–11.

Weisser, Kim Josefine, Datenbasierte Märkte im Kartellrecht, Eine Untersuchung zu Marktbegriff, Marktabgrenzung und Marktmacht, Berlin 2021.

Westin, Alan F., Science, Privacy and Freedom: Issues and Proposals for the 1970's., Part I - The Current Impact of Surveillance on Privacy, Columbia Law Review 66 (1966), S. 1003–1050.

Wirth, Jakob/*Maier*, Christian/*Laumer*, Sven/*Weitzel*, Tim, Laziness as an explanation for the privacy paradox: a longitudinal empirical investigation, INTR 32 (2022), S. 24–54.

Wisniewski, Pamela; *Page*, Xinru, Privacy Theories and Frameworks, in: Knijnenburg, Bart P.; Page, Xinru; Wisniewski, Pamela; Lipford, Heather Richter; Proferes, Nicholas; Romano, Jennifer, Modern Socio-Technical Perspectives on Privacy, Cham 2022.