Prof. Dr. Max von Grafenstein, LL.M.

Rechtswissenschaftliche Studie zu verarbeitungszweckspezifischen Grundrechtsrisiken im Bereich von personalisierter Werbung und personalisierter Inhalte im Internet

HIIG DISCUSSION PAPER SERIES 2025-04

ABSTRACT

Diese rechtswissenschaftliche Studie untersucht, welche Grundrechtsrisiken die Verarbeitung personenbezogener daten für Zwecke der personalisierten Werbung verursacht. Die Studie kommt zu dem Ergebnis, dass der Zweck „personalisierte Werbung“ in Ansehung der unterschiedlichen Grundrechtsrisiken, die verschiedene Formen personalisierter Werbung verursachen, ausdifferenziert werden muss, um dem datenschutzrechtlichen Verarbeitungsgrundsatz der Zweckspezifizierung und -bindung gerecht zu werden. Die Studie schlägt hierfür vor, zwischen den Unterzwecken „Retargeting“, „profilbasierte Werbung“, „kohortenbasierte Werbung“ und „kontextuelle Werbung“ zu unterscheiden. Der zusätzliche Zweck der Erfolgsmessung wird demgegenüber als Querschnittzweck verstanden, der jeweils mit einem oder mehreren der vorgenannten Zwecke kombiniert wird. Auf dieser Basis verortet die Studie zudem die Rolle und Funktion datenschutzfreundlicher Technologien und arbeitet Anschlussstellen für die empirische Messung der Wirksamkeit solcher Technologien heraus.

KEYWORDS

Personalisierung, Werbung, Datenschutz, Grundrechtsrisiken, Retargeting, profilbasierte Werbung, kohortenbasierte Werbung, kontextbezogene Werbung, Leistungsmessung

CITATION

v. Grafenstein, Max (2025). Rechtswissenschaftliche Studie zu verarbeitungszweckspezifischen Grundrechtsrisiken im Bereich von personalisierter Werbung und personalisierter Inhalte im Internet. HIIG Discussion Paper Series 2025-04. 20 Seiten. https://doi.org/10.5281/zenodo.16672068.

AUTOR / AFFILIATION / FÖRDERHINWEIS

Prof. Dr. Max von Grafenstein, LL.M., Regulierungswissenschaftler

Das vorliegende Gutachten wurde durch das Alexander von Humboldt Institut für Internet und Gesellschaft (HIIG) im Rahmen des vom Bundesministeriums für Forschung, Technologie und Raumfahrt (BMFTR) geförderten Forschungsprojekts „Sicher im Datenverkehr“ (SiD), Förderkennzeichen: 16KIS1968, beauftragt. Das Gutachten stellt den aktuellen Stand der Forschung (inklusive der eigenen publizierten Forschungsarbeiten des Auftragnehmers) in Bezug auf die gegebenen Ausgangsfragen dar.

DISCLAIMER

Die in diesem Gutachten enthaltenen Aussagen geben nicht notwendigerweise die Meinungen oder Positionen aller am Forschungsprojekt beteiligten Konsortialpartner wieder.

CONTENTS

1 INDIVIDUELLE RISIKEN FÜR VERBRAUCHER UND STRUKTURELLE RISIKEN FÜR DIE GESELLSCHAFT 4

1.1 Individuelle Risiken für die Privatsphäre: weder vorhersehbare noch kontrollierbare Einblicke in das Privatleben 4

1.2 Individuelle Risiken von Manipulation, Diskriminierung, materiellen und gesundheitlichen Schäden 6

1.3 Strukturelle Risiken für die Gesellschaft (insb. Demokratie, Solidarität, fairer Wettbewerb) 8

2 AUSDIFFERENZIERUNG DER ZWECKE ENTSPRECHEND DER SPEZIFISCHEN GRUNDRECHTSRISIKEN DES JEWEILIGEN TECHNISCH-ORGANISATORISCHEN VERFAHRENS 11

2.1 Re-Targeting zum Abschluss von Online-Einkaufsprozessen 11

2.2 Profiling-basierte Personalisierung von Online-Werbung 13

2.3 Kohortenbasierte Personalisierung von Online-Werbung 14

2.4 Kontextbezogene Online-Werbung 14

2.5 Leistungsmessung als Teilzweck 16

3 DIE ROLLE VON DATENSCHUTZFREUNDLICHEN TECHNOLOGIEN 17

4 ANKNÜPFUNGSPUNKTE FÜR DIE EMPIRISCHE MESSUNG 18

5 AUSBLICK AUF VERARBEITUNGSZWECKSPEZIFISCHE GRUNDRECHTSRISIKEN IM BEREICH VON SONSTIGEN PERSONALISIERTEN INHALTEN IM INTERNET 19

1 INDIVIDUELLE RISIKEN FÜR VERBRAUCHER UND STRUKTURELLE RISIKEN FÜR DIE GESELLSCHAFT[1]

Angesichts der aktuellen Praktiken des Ökosystems der personalisierten Werbung diskutieren sowohl Experten als auch Laien die folgenden Risiken, die durch die Verarbeitung personenbezogener Daten für die Zwecke der personalisierten Werbung entstehen. Die Risiken lassen sich vorab über folgendes Schaubild zusammenfassen:[2]

Abb. 1: Überblick: Risiken personalisierter Werbung.

1.1 Individuelle Risiken für die Privatsphäre: weder vorhersehbare noch kontrollierbare Einblicke in das Privatleben

Experten und Verbraucher betonen, dass **mögliche Einblicke in das Privatleben der Verbraucher und damit in die Privatsphäre** die größte Bedrohung durch personalisierte Werbung darstellen. In einem komplexen System wie dem derzeitigen Werbe-Ökosystem können die Nutzer weder vorhersehen noch wirksam kontrollieren, welche ihrer Online-Verhaltensweisen gezielt überwacht, mit wem diese Informationen geteilt und in welcher Form sie letztlich verwendet werden.[3] Die Risiken, die das System für den Einzelnen birgt, haben je nach den folgenden Parametern unterschiedliche Auswirkungen:

- dem Kontext der Datenerhebung oder der Art der erhobenen Daten,
- den aus der Datenanalyse abgeleiteten Informationen über die Verbraucher und
- dem Ausmaß, in dem und wie viele andere Personen von diesen Informationen Kenntnis erhalten.

Im Zusammenhang mit der Datenerhebung und der Art der erhobenen Daten lassen sich zudem die **klassischen Privatsphären, nämlich** Intimsphäre, Privatsphäre, Sozialsphäre und Öffentlichkeit

1 Kapitel 1–3 wurden in Übereinstimmung mit einer anderen durch den Verbraucherzentrale Bundesverband e.V. in Auftrag gegebenen Studie im Bereich der personalisierten Werbung erstellt.

2 Vgl. bereits Grafenstein, M. v., Jakobi, T., & Stevens, G. (2021). Effective data protection by design through interdisciplinary research methods: The example of effective purpose specification by applying user-Centred UX-design methods. Computer Law & Security Review, 46. DOI: 10.1016/j.clsr.2022.105722.

3 Margaritis, Online Behavioral Advertising as an Aggressive Commercial Practice, EuCML 2023, S. 244; Lancieri, Narrowing Data Protection's Enforcement Gap, MLR 2022, S. 31 ff.

unterscheiden. Grundsätzlich sind mit den verschiedenen Sphären und Arten von Daten unterschiedliche Erwartungen an den Schutz der Privatsphäre vor Eingriffen oder unbefugten Zugriffen und dementsprechend unterschiedliche rechtliche Schutzanforderungen verbunden.[4] Während beispielsweise Informationen über die Intimsphäre (z.B. Tagebücher, Krankheiten, sexuelle Interessen und Verhaltensweisen) und andere besondere räumliche, technische oder soziale Bereiche, die zum Kernbereich privater Lebensgestaltung gehören (z.B. häusliche Privatsphäre, Kommunikationsgeheimnis, Privatsphäre der Familie oder des Kindes) als besonders schützenswert gelten, ist der Schutz der Privatsphäre in der Öffentlichkeit deutlich geringer.[5] Aber auch in der Öffentlichkeit gibt es zweifellos einen Schutz der Privatsphäre vor der Erstellung von Profilen.[6] Ein bekanntes Beispiel für letzteres sind Bewegungsdaten, die, wenn sie dauerhaft und systematisch gespeichert werden, zu umfassenden Bewegungsprofilen zusammengestellt werden können, die weit über die übliche soziale „passing-by-Situation" hinausgehen.[7]

Neben den klassischen Bereichen der Privatsphäre gibt es auch spezielle Arten von Daten, die aufgrund ihres **erhöhten Missbrauchspotentials** als besonders schützenswert gelten. Zu dieser Kategorie gehören insbesondere die in Art. 9 DSGVO genannten Daten, die z.B. Aufschluss über die rassische und ethnische Herkunft, politische Meinungen oder religiöse Überzeugungen geben, aber auch andere Datenarten wie Bewegungsdaten.[8] Aufgrund der Allgegenwärtigkeit von Tracking-Technologien in unserem zunehmend digitalisierten Leben kann die Verarbeitung von Daten für personalisierte Werbung prinzipiell auf einen solchen Eingriff in all diese verschiedenen Privatsphären hinauslaufen.

Aufgrund des Profilings, das der Personalisierung von Werbung zugrunde liegt, ist jedoch nicht nur der Kontext der Datenerhebung oder die Art der erhobenen Daten an sich, sondern sind auch die **Informationen, die aus der Datenanalyse abgeleitet werden**, besonders relevant. Um nur ein paar Beispiele zu nennen: Die von den Verbrauchern bestellten Lebensmittel können Aufschluss über ihre Religionszugehörigkeit geben, ebenso wie die Orte, an denen sie sich aufhalten, das soziale Netzwerk, dem sie angehören, und die Dinge, die sie tun, weitere Interessen, Neigungen und ähnliche Aspekte ihres Privatlebens offenbaren.[9] Es geht also nicht nur um die ursprünglich erhobenen Daten, sondern auch um die abgeleiteten Informationen, die bei der weiteren Analyse der Daten weitere Einblicke in das Privatleben der Verbraucher preisgeben.

Schließlich kann ein Eingriff in die Privatsphäre danach beurteilt werden, in welchem Umfang und wie

4 v. Grafenstein, Refining the Concept of the Right to Data Protection in Article 8 ECFR - Part I., EDPL 2020, S. 201 f.

5 Rupp, V./ Grafenstein v., M., Clarifying "personal data" and the role of anonymisation in data protection law: Ein- und Ausschluss von Daten aus dem Anwendungsbereich der DSGVO (deutlicher) durch Verfeinerung des Datenschutzbegriffs, Computer Law & Security Review, 2024, 1-25, DOI: 10.1016/j.clsr.2023.105932.

6 EGMR, 25.9.2001, Nr. 44787/98, para. 56 - P.G. und J.H. gegen das Vereinigte Königreich: „Es gibt also einen Bereich der Interaktion einer Person mit anderen, selbst in einem öffentlichen Kontext, der in den Bereich des ‚Privatlebens' fallen kann"; EGMR, 28.1.2003, Nr. 44647/98, para. 57 - Peck gegen das Vereinigte Königreich; EGMR, EGMR, 17.7.2003, Nr. 63737/00, Rn. 36 - Perry v. the United Kingdom.

7 EGMR, 2.12.2010, Nr. 35623/05 - Uzun gegen Deutschland.

8 EDPB, Leitlinien 5/2020 zur Einwilligung nach der Verordnung 2016/679.

9EuGH, 20.12.2017, C-434/16, para. 34 f.: „Die Verwendung des Ausdrucks ‚jede Information' in der Definition des Begriffs 'personenbezogene Daten' in Artikel 2 Buchstabe a der Richtlinie 95/46 spiegelt das Ziel des EU-Gesetzgebers wider, diesem Begriff einen weiten Anwendungsbereich zuzuweisen, der nicht auf sensible oder private Informationen beschränkt ist, sondern potenziell alle Arten von Informationen, nicht nur objektive, sondern auch subjektive, in Form von Meinungen und Bewertungen, umfasst, sofern sie sich auf die betroffene Person ‚beziehen'. Die letztgenannte Voraussetzung ist erfüllt, wenn die Information aufgrund ihres Inhalts, ihres Zwecks oder ihrer Wirkung einer bestimmten Person zugeordnet werden kann"; Ehmann/ Selmayr/ Klabunde/ Horváth, Art. 4 GDPR, Rn.10.

viele Personen Zugang zu diesen privaten Informationen haben. Für Laien macht es dabei einen Unterschied, ob diese Informationen nur von einer Maschine verarbeitet werden oder ob eine andere Person Zugang zu diesen Informationen erhält. Wenn eine andere Person Zugang zu Informationen erhält, ist es von Bedeutung, in welcher sozialen Rolle diese Person Zugang zu den Informationen erhält und wie viele Personen Zugang zu diesen Informationen erhalten. Wenn private Informationen „nur" von einer Maschine verarbeitet werden, heißt das nicht, dass dies für Laien kein Problem darstellen würde. Vielmehr muss berücksichtigt werden, dass diese Maschine in der Regel einer Person gehört und dass diese Person wahrscheinlich jederzeit auf diese Informationen zugreifen kann.[10] Es geht also nicht darum, dass es keinen Eingriff in die Privatsphäre gäbe, sondern darum, wie intensiv dieser Eingriff wäre und wie wahrscheinlich es ist, dass ein solcher Rückschluss realisiert wird. Damit geht es also um die Frage, wie groß das Risiko eines Rückschlusses auf die Privatsphäre ist.

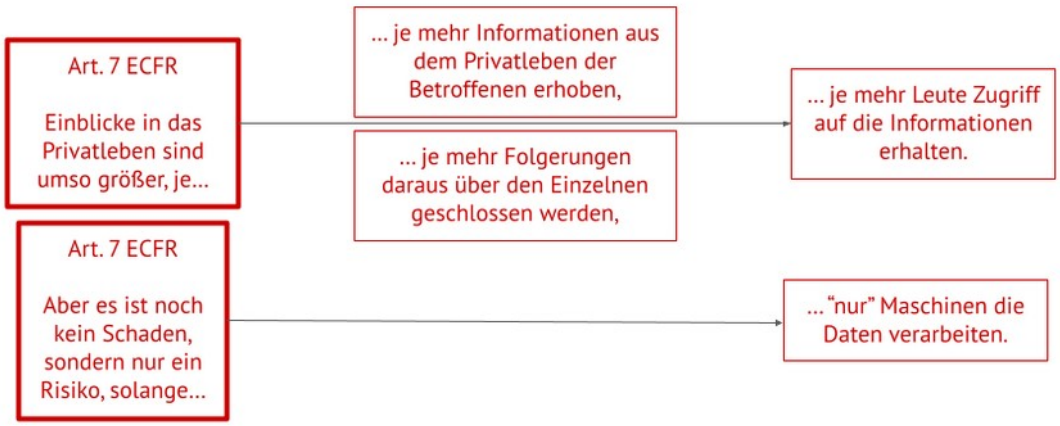

Abb. 2: Faktoren für Einblicke in das Privatleben.

1.2 Individuelle Risiken von Manipulation, Diskriminierung, materiellen und gesundheitlichen Schäden

Neben der Gefährdung der Privatsphäre birgt die personalisierte Werbung zahlreiche weitere Risiken für die Verbraucher. Mit dem Aufkommen der Informationstechnologien hat man längst erkannt, dass die Relevanz von Daten nicht nur durch die Art der erhobenen Daten oder den Kontext der Erhebung bestimmt wird, sondern vor allem durch den Zweck, für den die Daten verwendet werden. Die Sammlung, Analyse und Segmentierung von Nutzerdaten im Rahmen des derzeitigen Werbesystems ermöglicht es den beteiligten Akteuren, sich ein genaues Bild vom aktuellen Gemütszustand, den Überzeugungen und Meinungen eines jeden Nutzers zu machen, dass es ein Leichtes ist, seine Bedürfnisse, kognitiven Biases, Ängste und Schwachstellen für **Manipulationen** auszunutzen.[11] Das Risiko wird durch die Tatsache

10 v. Grafenstein/ Jakobi/ Stevens, Effektiver Datenschutz durch Design mit interdisziplinären Forschungsmethoden: The example of effective purpose specification by applying user-centred UX-design methods, Computer Law & Security Review, 2022, S. 18: „In Bezug auf die 'human in the loop'-Debatte um Sprachassistenten sagte beispielsweise ein Workshop-Teilnehmer, dass er die reine Verarbeitung privater Informationen durch einen Algorithmus nicht als Eingriff in seine Privatsphäre betrachte (denn ein solcher Eingriff in die Privatsphäre setzt seiner Meinung nach offenbar einen Menschen voraus, der die privaten Informationen erhält). Andererseits sagte ein anderer Teilnehmer, je mehr Menschen Zugang zu solchen Informationen hätten, desto auffälliger sei ihre Privatsphäre betroffen."

11 Margaritis, Online Behavioral Advertising as an Aggressive Commercial Practice, EuCML 2023, S. 245; Kopp, Is So-Called Contextual Advertising the Cure to Surveillance-Based "Behavioral" Advertising?, Tech Policy Press 26.9.2023.

verstärkt, dass der Empfang von Nachrichten, die in einer Weise personalisiert sind, die speziell auf die Persönlichkeit des Einzelnen abzielt, seine Fähigkeit erschwert, genau zu erkennen, wann und wie er manipuliert wird.[12]

Im Hinblick auf den Verbrauchermarkt birgt die Verarbeitung personenbezogener Daten für personalisierte Werbung die Gefahr, beim Kauf von Konsumgütern manipuliert zu werden.[13] Werden Tracking-Technologien und Profiling nicht nur für Werbung **im Zusammenhang mit dem Kauf von Konsumgütern, sondern auch in anderen Kontexten** eingesetzt, birgt dies ein Risiko für weitere Grundrechte. Im Zusammenhang mit Wahlen kann das so genannte politische Micro-Targeting eine Gefahr für die freie (d. h. nicht manipulierte) Wahlentscheidung des Einzelnen darstellen.[14] Das markanteste Beispiel hierfür ist wohl der Fall des britischen Beratungsunternehmens Cambridge Analytica, das personenbezogene Daten von Millionen von Facebook-Nutzern ohne deren Zustimmung gesammelt hat, um sie vor allem für politische Werbung zu nutzen.[15] Gleiches gilt für die Personalisierung von Nachrichten, bei der ein Risiko für die Informationsfreiheit des Einzelnen besteht.

Sowohl Experten als auch Laien sehen darüber hinaus weitere Risiken für die Verbraucher. Dazu gehört die **Gefahr der Diskriminierung**, die daraus resultiert, dass personalisierte Werbung nur für bestimmte Personengruppen und nicht für die Allgemeinheit angezeigt wird.[16] Dies kann nicht nur zu einer Diskriminierung von Gruppen mit bestimmten Merkmalen führen, die als „unangemessen" („sachwidrig") und gesellschaftlich nicht tolerierbar gilt (vgl. z.B. die verfassungsrechtlich garantierten Diskriminierungsfreiheiten nach Art. 20 ff. EGV und die Antidiskriminierungsgesetze auf der Ebene des einfachen Rechts). Vielmehr kann die Personalisierung auch weitere **Freiheits- und Beteiligungsrechte aushöhlen**. So können z.B. (meist ohnehin sozial benachteiligte) Gruppen bei der Arbeits- oder Wohnungssuche durch personalisierte Werbung für diese Stellen oder Wohnungen von diesen ausgeschlossen werden.[17]

Die Personalisierung der Werbung kann auch zu **materiellen sowie physischen und psychischen Schäden** für die Verbraucher führen. Die Gefahr eines materiellen Schadens ergibt sich zumindest daraus, dass die Verbraucher möglicherweise Dienstleistungen oder Produkte kaufen, die sie ursprünglich nicht kaufen wollten oder die nicht ihren Interessen entsprechen.[18] Im Falle der Preisdiskriminierung bedeutet dies, dass die Verbraucher Waren oder Produkte zu einem höheren Preis kaufen als andere Personengruppen, denen ein niedrigerer Preis angezeigt wird.[19] Einigen Beobachtern zufolge begünstigt

12 Strycharz/ Duivenvoorde, Die Ausnutzung der Verletzlichkeit durch personalisierte Marketingkommunikation: Sind die Verbraucher geschützt?, IPR 4/2021, S. 7.

13 Google spricht euphemistisch von „[...] shape your consumer's decision [...] Anticipate the micro-moments for your target audience, and commit to being there to help when those moments occur", Google, The Basics of Micro-Moments, 2016; Kopp, Is So-Called Contextual Advertising the Cure to Surveillance-Based "Behavioral" Advertising? Tech Policy Press 26.9.2023; AWO Belgien, Study on the impact of recent developments in digital advertising on privacy, publishers and advertisers, 2023, S. 85 ff.

14 Scott, Cambridge Analytica did work for Brexit groups, says ex-staffer, Politico 30.7.2019; AWO Belgien, Study on the impact of recent developments in digital advertising on privacy, publishers and advertisers, 2023, S. 86 ff.

15 Eine Untersuchung der ICO vor der Einführung der DSGVO führte zu einer Geldstrafe von 500.000 britischen Pfund, https://ico.org.uk/action-weve-taken/investigation-into-data-analytics-for-political-purposes/.

16 AWO Belgien, Study on the impact of recent developments in digital advertising on privacy, publishers and advertisers, 2023, S. 82 ff.

17 Dunphy, Women are seen fewer STEM job ads than men: are marketing algorithms promoting gender bias?, European Scientist 28.7.2018.

18 Margaritis, Online Behavioral Advertising as an Aggressive Commercial Practice, EuCML 2023, S. 245.

19 Siehe z. B. Rützel, Rechtsfragen algorithmischer Preisdiskriminierung: eine rechtsgebietsübergreifende Untersuchung. 2023.

die personalisierte Werbung auch **Betrug**.[20] Nicht zuletzt kann die gezielte Ansprache besonders gefährdeter Gruppen (z. B. Kinder oder Suchtkranke) zu **physischen und psychischen Gesundheitsschäden** führen. Zum Beispiel, wenn die Werbung gezielt auf geistige oder körperliche Schwächen abzielt, um bestimmte Produkte wie echte oder Pseudo-Medikamente, Suchtmittel (z. B. legale Drogen) oder Dienstleistungen (z. B. Spiele) an Menschen mit diesen vermuteten Schwächen zu verkaufen.[21]

In diesem Zusammenhang ist es wichtig zu betonen, dass alle Menschen unabhängig von gruppenbezogenen Schwachstellen gefährdet sein können.[22] Je nach Situation oder Kontext können ältere Menschen, die mit der Geschwindigkeit der sich ändernden und neu entstehenden digitalen Anforderungen überfordert sind, verwundbar sein. Oder Kinder, die zwar wissen, wie sie Geräte und neue Dienste nutzen können, aber nicht, wie sie mit den plötzlichen Bedrohungen durch die digitale Kommunikation umgehen sollen. Aber auch digital versierte Menschen können in der digitalen Gesellschaft situativ verwundbar sein, beispielsweise wenn sie in unerwarteten Situationen mit Informationen überfrachtet werden oder durch ständige Aufforderungen zu Entscheidungen demoralisiert werden.[23] Oder noch trivialer: Mangelndes Verständnis der Zielgruppenansprache kann Verbraucher angreifbar machen.[24]

Der Einsatz von KI bedeutet eine weitere Verschärfung der bereits bestehenden individuellen, wirtschaftlichen und sozialen Risiken.[25] Sie droht, Prozesse noch undurchsichtiger, unfairer und noch schwieriger anfechtbar zu machen. Zu den fortschreitenden und unvorhersehbaren Möglichkeiten der KI-Nutzung gehören auch datenschutz- und regulierungsbezogene Herausforderungen. Nicht zuletzt deshalb, weil KI die Erstellung von hyperpersonalisierten Werbebotschaften und die Ausrichtung auf einzelne Verbraucher ermöglicht.[26]

1.3 Strukturelle Risiken für die Gesellschaft (insb. Demokratie, Solidarität, fairer Wettbewerb)

Neben den Risiken für einzelne Verbraucher oder Verbrauchergruppen birgt die Verarbeitung personenbezogener Daten für persönliche Werbung auch **Risiken für Dritte oder strukturelle Risiken für die Gesellschaft als Ganzes**. Die erste Situation wird häufig mit dem Begriff „Drittwirkung" umschrieben, der den ethischen Anspruch beschreibt, dass eine Vereinbarung, ein Austausch oder auch nur Handlungen zwischen zwei Parteien nicht dazu führen sollen, dass eine andere geschädigt wird.[27] Dieses Phänomen ist jedoch nicht unüblich, insbesondere im Datenschutzrecht, da nicht nur aus Daten, sondern

20 Meyer, Warum seriöse Websites Werbung von Fake-Shops schalten, Deutschlandfunk 11.4.2023; Mayer, Manipulierte Bilder, falsche Nachrichten: Wie es betrügerische Werbeanzeigen immer wieder in Online-Medien schaffen, Tagesspiegel 21.3.2023.

21 AWO Belgien, Studie über die Auswirkungen der jüngsten Entwicklungen in der digitalen Werbung auf den Datenschutz, die Verleger und die Werbetreibenden, 2023, S. 86.

22 Kroschwald, Nutzer-, kontext- und situationsbedingte Vulnerabilität in digitalen Gesellschaften, ZfDR 2023, S. 5; Strycharz/ Duivenvoorde, The exploitation of vulnerability through personalised marketing communication: are consumers protected?, IPR 4/2021, S. 6.

23 Zum Beispiel durch die Verwendung sogenannter Dark Patterns bei der Abfrage von Einwilligungen im Zusammenhang mit Online-Diensten und Plattformen, siehe EDPB, Guidelines 03/2022 on deceptive design patterns in social media platform interfaces: how to recognise and avoid them, Version 2.0, 2023.

24 Strycharz/ Duivenvoorde, Die Ausnutzung der Verletzlichkeit durch personalisierte Marketingkommunikation: Sind die Verbraucher geschützt?, IPR 4/2021, S. 7 ff.

25 Vigliarolo, Turns out AI chatbots are way more persuasive than humans, The Register, 3.4.2024.

26 IAB Inc, Legal Issues and Business Considerations - When Using Generative AI in Digital Advertising, 2024, S. 12.

27 Engle, Drittwirkung von Grundrechten, HanseLR 2009, S. 165 ff.

auch aus dem Fehlen von Daten Schlüsse gezogen werden können. So ist es beispielsweise möglich, dass nur denjenigen Verbrauchern, die Einblicke in ihr Privatleben gewähren, ein niedrigerer Preis angezeigt wird. Alle anderen würden standardmäßig den „normalen" Preis erhalten. Wann ein Preis niedriger ist als ein „normaler" Preis und wann der niedrigere Preis zum „normalen" Preis wird und alle anderen nun den höheren Preis zahlen, ist freilich umstritten. Wir wollten mit diesem Beispiel jedenfalls nur verdeutlichen, dass solche Drittwirkungen auch im Bereich der personalisierten Werbung auftreten können. Das Beispiel zeigt auch, dass die Grenzen zwischen Selbst- und Fremdbestimmung recht fließend sind und zu entsprechenden Problemen bei der Suche nach geeigneten Schutzmechanismen führen.

Dies gilt umso mehr, wenn es um strukturelle Risiken für die Gesellschaft als Ganzes geht. Insbesondere werden Risiken für die **(IT-)Sicherheit** nicht nur für einzelne Systeme oder Organisationen beobachtet, sondern erstrecken sich auf kritische Infrastrukturen insgesamt, z.B. durch die effizientere Verbreitung von Schadsoftware[28] oder die Verfolgung von Personen innerhalb des Sicherheitssektors[29]. Darüber hinaus diskutieren Beobachter auch die Verbreitung von **Fehlinformationen** / schädlichen Inhalten, die den öffentlichen Diskursraum schädigen können.[30] Ebenso kann sich die Manipulation individueller Wahlentscheidungen nicht nur auf die Wahlfreiheit des Einzelnen, sondern auch **auf das demokratische System** insgesamt **auswirken**,[31] ebenso wie die immer feinere Individualisierung von Versicherungspolicen das Prinzip der **gesellschaftlichen Solidarität** untergraben kann.[32] Nicht zuletzt verweisen die Kritiker auch auf die **negativen** Umweltauswirkungen der Personalisierung von Werbung.[33]

Bei all diesen gesellschaftlichen Risiken stellt sich die Frage, ob ihre Kontrolle von der Entscheidungsfreiheit des Einzelnen abhängen soll oder ob hier objektive Maßnahmen erforderlich sind. Diese Frage hängt letztlich von der Kausalkette ab, auf der diese Risiken und mögliche Beeinträchtigungen kollektiver Rechtsgüter wie die Sicherheit kritischer Infrastrukturen, das Demokratie- und Solidaritätsprinzip oder ein funktionierender öffentlicher Diskurs beruhen. So hat das Bundesverfassungsgericht in seiner Entscheidung zum Volkszählungsurteil von 1983 es als unabdingbare Voraussetzung für eine demokratisch verfasste Gesellschaft angesehen, dass ihre einzelnen Mitglieder, d.h. jeder einzelne Bürger, in der Lage bleibt, autonom zu entscheiden und entsprechend zu handeln.[34] Das Funktionieren eines demokratischen Systems beruht also konzeptionell auf der Fähigkeit des einzelnen Bürgers, autonome Entscheidungen zu treffen. Ähnliche Zusammenhänge werden im deutschen Wettbewerbsrecht (UWG) konstruiert. Auch wenn die meisten Regelungen inzwischen auf europäischen Harmonisierungsrichtlinien beruhen, folgt ihre Umsetzung in Deutschland noch immer der grundsätzlichen Unterscheidung zwischen einer mikro- und einer makroökonomischen Ebene: Der Schutz autonomer Kaufentscheidungen der Verbraucher auf der mikroökonomischen Ebene führt zu einem fairen

28 BSI, Cyber-Angriffe über Online-Werbung, https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/Updates-Browser-Open-Source-Software/Der-Browser/Adblocker-Tracking/adblocker_tracking.html?nn=130950#doc504232bodyText3.

29 Dachwitz/ Meineck, Datenhändler verticken Handy-Standorte von EU-Bürger*innen, Netzpolitik, 17.1.2024.

30 AWO Belgien, Study on the impact of recent developments in digital advertising on privacy, publishers and advertisers, 2023, S. 78 ff.

31 Strycharz/ Duivenvoorde, Die Ausnutzung der Verletzlichkeit durch personalisierte Marketingkommunikation: Sind die Verbraucher geschützt?, IPR 4/2021, S. 5.

32 Iversen/ Rehm, Big Data und der Wohlfahrtsstaat: Wie die Informationsrevolution die soziale Solidarität bedroht, 2022, S. 188 ff.

33 AWO Belgien, Study on the impact of recent developments in digital advertising on privacy, publishers and advertisers, 2023, S. 89 ff.

34 Bundesverfassungsgericht, 15.12.1983, 1 BvR 209, 269, 362, 420, 440, 484/83, Abs. 127 – Volkszählungsurteil.

Wettbewerb auf der makro- oder zumindest meso-ökonomischen Ebene.[35] Das deutsche Wettbewerbsrecht bleibt freilich nicht dabei stehen, sondern findet weitere Ansatzpunkte für eine Regulierung, die über diesen individualentscheidungszentrierten Ansatz hinausgeht (vgl. insbesondere das Gesetz gegen Wettbewerbsbeschränkungen - GWB) und einen eher strukturellen Ansatz verfolgt.

Ob das (europäische) Datenschutzrecht eher individualistisch mit subjektiven Rechten konzipiert werden sollte und dann quasi als Annex kollektive Interessen durch objektive Pflichten des für die Datenverarbeitung Verantwortlichen schützt oder ob umgekehrt das Datenschutzrecht in erster Linie als objektive Pflicht der für die Datenverarbeitung Verantwortlichen verstanden werden sollte, aus der dann individuelle subjektive Rechte der Verbraucher abgeleitet werden, ist ohnehin ein eher theoretischer Streit.[36] Denn in der Praxis setzt der Gesetzgeber in der Regel beide Ansätze um, entweder in einem einzigen Gesetz oder im Wege verschiedener Gesetze. So schützt die DSGVO nicht nur die Interessen der Betroffenen (vgl. Art. 1 Abs. 2 DSGVO), sondern auch die der Gesellschaft insgesamt (vgl. z.B. die zu respektierenden Interessen der Öffentlichkeit in Art. 6 Abs. 1 lit. f DSGVO).[37] Gleiches gilt für das neue KI-Gesetz, das nicht nur die Grundrechte der Verbraucher, sondern auch die Demokratie und die Sicherheit der Gesellschaft als Ganzes schützt (Art. 1 Abs. 1 KI-Gesetz). Auch das Gesetz über digitale Dienste schützt sowohl die einzelnen Nutzer der Plattformen als auch allgemeine Interessen wie den öffentlichen Diskurs (Art. 34 Abs. 1 DSG). Ebenso schützt die Verordnung über die politische Werbung sowohl den einzelnen Wähler vor der Manipulation seiner Stimme als auch das demokratische System als Ganzes (Art. 12 ff. sowie Erwägungsgründe 4 und 6 PTR). Der Data Governance Act hilft ebenfalls dem Einzelnen, seine Daten zu teilen, zielt aber auch darauf ab, das Innovationspotenzial des europäischen Datenraums zum Nutzen der gesamten Gesellschaft besser auszuschöpfen (Art. 12 ff. sowie Erwägungsgründe 1 ff. DGA). In ähnlicher Weise schützt das Gesetz über digitale Märkte den einzelnen Verbraucher vor dem Missbrauch von Marktmacht durch so genannte „Gatekeeper“ und sichert gleichzeitig den freien Wettbewerb (Art. 1 und 5 Abs. 2 DMA). Wichtig ist, an dieser Stelle festzuhalten, dass sich ein wirksamer Schutz auf individueller und gesamtgesellschaftlich-struktureller Ebene in der Regel gegenseitig bedingt und entsprechend ausgestaltet werden muss.

35 v. Grafenstein/ Hölzel/ Irgmaier/ Pohle, Nudging – Regulierung durch Big Data und Verhaltenswissenschaften, 2018.

36 Britz, Informationelle Selbstbestimmung – zwischen rechtswissenschaftlicher Grundsatzkritik und Beharren des Bundesverfassungsgerichts, 2010, S. 594, 595.

37 EDPB, Leitlinien 1/2024 zur Verarbeitung personenbezogener Daten auf der Grundlage von Artikel 6 Absatz 1 Buchstabe f) DSGVO, Absatz. 128.

2 AUSDIFFERENZIERUNG DER ZWECKE ENTSPRECHEND DER SPEZIFISCHEN GRUNDRECHTSRISIKEN DES JEWEILIGEN TECHNISCH-ORGANISATORISCHEN VERFAHRENS

Grundsätzlich muss der für die Verarbeitung Verantwortliche die Zwecke so festlegen, dass die Zwecke als geeigneter Ausgangspunkt für die rechtlichen Anforderungen dienen und die Betroffenen in der Lage sind, zu beurteilen, ob sie diese für angemessen oder unangemessen halten und sich dementsprechend auf die Verarbeitung ihrer Daten einstellen können. Zu diesem Zweck müssen die für die Verarbeitung Verantwortlichen die Zwecke so spezifizieren und differenzieren, dass sie die verschiedenen Risiken erkennen, die die entsprechenden Verarbeitungen für die betroffenen Personen und schließlich für die Gesellschaft insgesamt mit sich bringen. Dementsprechend folgt die hier vorgeschlagene Spezifizierung der Zwecke dem Grundsatz, dass diese angesichts der typischerweise zugrundeliegenden technischen und organisatorischen Abläufe die verschiedenen Risiken explizit machen und insoweit von den anderen Zwecken abgrenzbar sein müssen. Aus diesem Grund schlagen wir vor, im Bereich der personalisierten Werbung grundsätzlich zwischen den folgenden Teilzwecken zu differenzieren. Wir beschränken uns im Rahmen dieser Studie auf die Definition von Zwecken, die der Personalisierung im engeren Sinne dienen. Das bedeutet, dass „Annexzwecke“, wie die Gewährleistung der IT-Sicherheit oder die Dimensionierung von Online-Werbeflächen, hier nicht berücksichtigt werden. Natürlich können die nachfolgend vorgeschlagenen Zwecke miteinander kombiniert werden, was in der Praxis auch geschieht. Auf die Kombination von Zwecken muss dann entsprechend hingewiesen werden.

2.1 Re-Targeting zum Abschluss von Online-Einkaufsprozessen

Wir halten Retargeting für eine der intensivsten Arten der Personalisierung von Werbung. Beim Retargeting geht es um die erneute Identifizierung eines Verbrauchers in verschiedenen Browsern und Geräten auf der Grundlage eines bestimmten Ereignisses. Wenn ein Verbraucher beispielsweise auf eine Anzeige geklickt oder sogar einen Warenkorb gefüllt hat, ohne auf die Schaltfläche „Kaufen“ zu klicken, zielt das Retargeting darauf ab, diesen Verbraucher dazu zu bewegen, den Kaufvorgang über einen bestimmten Zeitraum abzuschließen, unabhängig davon, wo er sich im Internet befindet. Auf der Grundlage des Retargeting wird dem Verbraucher daher über einen längeren Zeitraum und auf verschiedenen Websites und digitalen Diensten, die mit dem Retargeting-System verbunden sind, Werbung für Produkte oder Dienstleistungen angezeigt, die mit dem auslösenden Ereignis in Zusammenhang stehen.[38]

Im Hinblick auf die daraus resultierenden Risiken für die Grundrechte der Betroffenen ist Retargeting daher weniger durch die Tiefe der verhaltensbasierten Interessenprofile als durch das Ausmaß der Re-Identifikationsmöglichkeiten gekennzeichnet. Die Werbewirtschaft ermöglicht diese Re-Identifizierung technisch und organisatorisch, indem sie möglichst viele Identifikatoren eines Verbrauchers sammelt und miteinander verknüpft. Dabei kann zwischen deterministischen oder dauerhaften Identifikatoren und probabilistischen Identifikatoren unterschieden werden. Deterministische Identifikatoren werden für die Zwecke der Re-Identifizierung gegenüber probabilistischen Identifikatoren bevorzugt, da sie mit einem höheren Grad an Genauigkeit verbunden sind. Zu den deterministischen Identifikatoren gehören

38 Wang/ Zhang/ Yuan, Display Advertising with Real-Time Bidding (RTB) and Behavioural Targeting, FTIR 2017, S. 11.

insbesondere Anmeldedaten, E-Mail-Adressen, Telefonnummern, Postadressen, Zahlungsdaten, Geräte- und Netzidentifikationsnummern (insbesondere IMEI- und MAC-Nummern), Cookies, die in den Browsern der einzelnen Endgeräte gespeichert werden, und natürlich IP-Adressen.

Probabilistische Methoden hingegen stützen sich auf Identifikatoren, die aufgrund ihrer geringeren Genauigkeit nicht als deterministisch gelten, aber dennoch eine aus Sicht der Werbeindustrie ausreichende Wiedererkennungswahrscheinlichkeit aufweisen. Dazu gehört insbesondere das Fingerprinting, das eine Kombination verschiedener nicht-deterministischer Merkmale wie die eingestellte Sprache, die Zeitzone, den Browser, die Browserversion oder die Bildschirmgröße des vom Verbraucher verwendeten Geräts und vieles mehr verwendet.

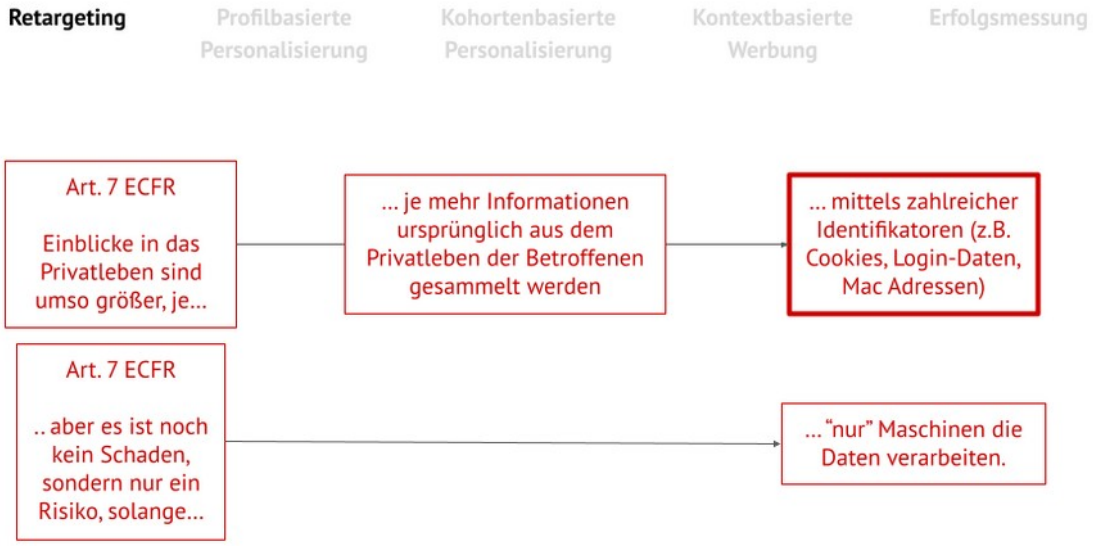

Abb. 3: Risiken des Retargetings.

Angesichts der Risiken für ihr Recht auf Privatsphäre empfinden die Verbraucher Retargeting oft als aufdringlich und sogar unheimlich, weil sie zwar eine vage Verbindung zwischen der angezeigten Werbung und ihrem früheren Klick- oder Kaufverhalten herstellen können, aber nicht verstehen, wie dies technisch funktioniert. Dies gibt den Verbrauchern manchmal das Gefühl, heimlich verfolgt zu werden.[39]

Was den Mehrwert angeht, so teilen die Verbraucher nicht immer die Ansicht der Werbeindustrie, dass Retargeting Werbung relevanter macht. Ein bekanntes Beispiel sind Anzeigen für Dienstleistungen oder Produkte, die den Verbrauchern wochenlang angezeigt werden, obwohl sie diese längst gekauft haben und daher nicht mehr an den entsprechenden Anzeigen interessiert sind. Das liegt natürlich daran, dass die technischen Systeme in diesen Fällen möglicherweise nicht unterscheiden können, ob der Verbraucher das Produkt bereits gekauft hat oder nicht. Hier kommt es aber nicht darauf an, was technisch machbar ist, sondern darauf, ob der Verbraucher den Mehrwert des Retargeting für ihn wert ist.[40]

39 v. Grafenstein, M., Smieskol, P., and Jakobi, T. (pre-print). From Consent to Control by Closing the Feedback Loop: Enabling Data Subjects to Directly Compare Personalized and Non-Personalized Content Through an On/Off Toggle. Available at SSRN: https://ssrn.com/abstract=5021149 or http://dx.doi.org/10.2139/ssrn.5021149.

40 Siehe Fn zuvor.

2.2 Profiling-basierte Personalisierung von Online-Werbung

Ähnlich, aber auf andere Weise intrusiv ist die Personalisierung von Werbung auf der Grundlage von Interessenprofilen, die durch Beobachtung des Verhaltens eines Verbrauchers über einen längeren Zeitraum hinweg erstellt werden. Die Werbeindustrie erstellt diese Profile, indem sie beobachtet, welche Websites die Verbraucher besuchen, welche Inhalte sie anklicken, wie lange sie diese nutzen, was sie letztendlich kaufen, mit welchen anderen Personen sie interagieren usw. Aus diesen Informationen können dann Rückschlüsse auf die Interessen, Einstellungen, Eigenschaften und natürlich auch auf das mögliche künftige Verhalten des Verbrauchers gezogen werden. Wie viel Einblick diese Informationen in das Privatleben eines Verbrauchers geben, hängt insbesondere von folgenden Aspekten ab:

1. Wie lange die Beobachtung dauert,
2. wie umfassend diese Beobachtung ist, d. h. bei wie vielen Gelegenheiten die betroffenen Personen beobachtet werden,
3. wie umfassend und tiefgreifend die Analyse dieser Informationen ist und
4. das Ausmaß, in dem die erhobenen und/oder abgeleiteten Informationen in die soziale, private und intime Sphäre der betroffenen Personen eingreifen.

Bei der profilbasierten Personalisierung von Werbung geht es also nicht in erster Linie darum, einen Verbraucher aufgrund eines gezeigten Kaufinteresses zum Abschluss des Kaufprozesses zu bewegen. Vielmehr geht es darum, die Wünsche und Bedürfnisse des Verbrauchers herauszufinden und ihm passende Dienstleistungen und Produkte anzubieten, die diese Wünsche oder Bedürfnisse befriedigen. Da sich der Verbraucher seiner Wünsche und Bedürfnisse möglicherweise gar nicht bewusst ist, können die Vorschläge überraschend oder anregend, aber auch sehr manipulativ sein.

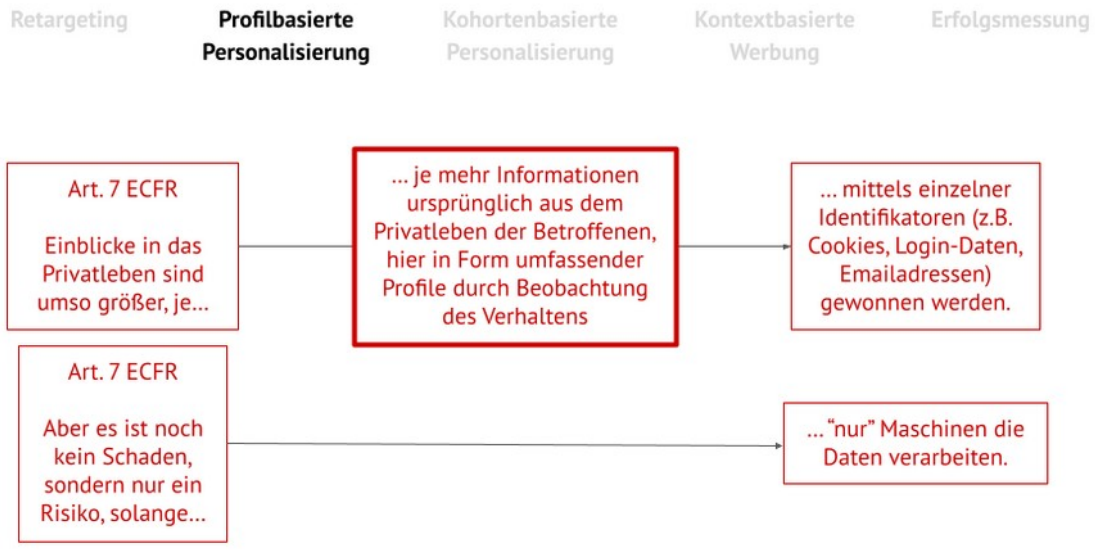

Abb. 4: Risiken der profilbasierten Personalisierung.

In diesem Zusammenhang ist noch einmal zu betonen, dass die Praktiken des Retargeting und der profilbasierten Personalisierung von Werbung in der Praxis durchaus kombiniert werden können. Das Gleiche gilt für die weiter unten beschriebene kohortenbasierte Werbung. Auch diese Art von Werbung

wird häufig sowohl mit Retargeting als auch mit profilbasierter Werbung kombiniert.

2.3 Kohortenbasierte Personalisierung von Online-Werbung

Obwohl die kohortenbasierte Werbung der profilbasierten Werbung ähnelt, ist sie weniger intrusiv. Wie oben beschrieben, werden bei der kohortenbasierten Werbung die Phasen der Datenerhebung und -analyse einerseits und die Zuordnung der abgeleiteten Kaufinteressen zu bestimmten Verbrauchern andererseits voneinander getrennt, was zwei grundsätzlich unterschiedliche Gruppen von Betroffenen betrifft. Was die erste Gruppe anbelangt, so kann das Risiko, dass jemand anderes Zugang zu den Beobachtungsdaten erhält, tatsächlich recht gering sein, wenn die Verarbeitungsverfahren angemessen gestaltet sind. Es liegt jedoch auf der Hand, dass die kohortenbasierte Werbung immer noch ein Risiko für die Grundrechte der anderen Verbrauchergruppe darstellt, d. h. der Verbraucher, denen die statistischen Interessenprofile zugeordnet werden. Je nachdem, wie umfangreich diese Zuordnung ist, besteht daher für diese zweite Gruppe ein Risiko für die Privatsphäre. Neben dem Recht auf Privatsphäre birgt die kohortenbasierte Werbung Risiken für die autonomen Kaufentscheidungen dieser zweiten Gruppe. In dieser Hinsicht unterscheidet sich die kohortenbasierte Werbung nicht von den beiden anderen Formen, dem Retargeting und der profilbasierten Werbung. Die Unterschiede liegen also eher in der Frage, wie und in welchem Ausmaß die drei Formen der Werbung in die Privatsphäre der Betroffenen eingreifen.

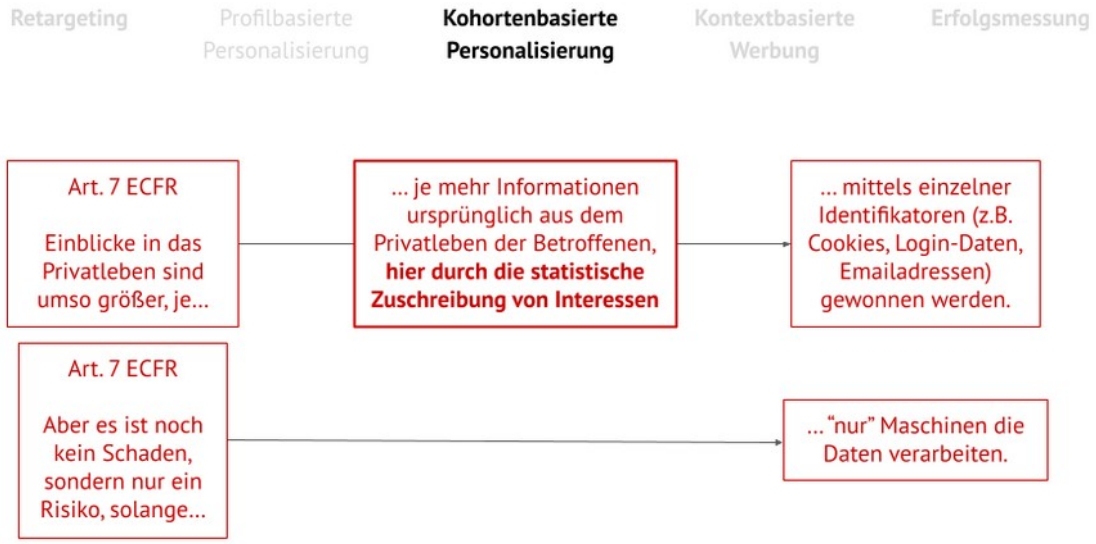

Abb. 5: Risiken der kohortenbasierten Personalisierung.

2.4 Kontextbezogene Online-Werbung

Die am wenigsten intrusive Methode zur Personalisierung von Anzeigen ist (nach traditionellem Verständnis) kontextbezogene Werbung. Dabei handelt es sich um eine Praxis der Platzierung von Anzeigen auf Seiten, die auf einer Übereinstimmung mit dem jeweiligen Inhalt basieren, was durch eine relativ einfache Schlüsselwort- oder URL-Analyse erreicht wird. Daher wird sie oft als Lösung angesehen, um verschiedenen Problemen und Risiken zu entgehen, die mit den vorgenannten Arten personalisierter Werbung verbunden sind, und zwar nicht nur für Nutzer, sondern auch für Werbetreibende und Herausgeber.

Kontextbasierte Werbung ist in der Tat eine vielversprechende Alternative, die es wert ist, aus regulatorischer Sicht näher betrachtet zu werden. Dennoch ist es kein sicherer Erfolg, da das Verständnis von „kontextuell“ in der Branche sehr unscharf ist. Der Begriff wird inflationär für Methoden verwendet, die in Wirklichkeit die Verarbeitung von personenbezogenen Daten, Geo- oder Sitzungsdaten beinhalten. Um diese Methode für Regulierungsansätze in Betracht zu ziehen, ist es jedoch unabdingbar, eine umfassende und aktuelle Definition von kontextbezogener Werbung zu formulieren, die die technischen Entwicklungen in Bezug auf den Einsatz von KI berücksichtigt.[41] Wenn wir im Folgenden von kontextbezogener Werbung sprechen und dafür Regelungen und Rechtsfolgen vorschlagen, beziehen wir uns auf ein extrem enges Verständnis des Begriffs. Wir bewerten daher nur Methoden, die keine Verarbeitung personenbezogener Daten beinhalten (es sei denn, es werden ausdrücklich Ausnahmen genannt).

Zugegeben, die Festlegung einer engen Definition hat einen praktischen Nachteil: Da keine Daten über die Nutzer gesammelt werden, kann es zu Problemen bei der Begrenzung der Häufigkeit kommen (d. h. es muss vermieden werden, dass demselben Nutzer dieselbe Anzeige mehrmals gezeigt wird). Ebenso kann es schwierig sein, bestimmte Inhalte in einen bestimmten Kontext zu setzen.[42] Kontextbasierte Werbung kann also aus Sicht der Verbraucher weniger relevante Werbung führen. Ob dies tatsächlich der Fall ist, bleibt freilich im Auge des Betrachters. Die Verbraucher müssten also selbst erst einmal in die Lage versetzt werden, die Relevanz der für sie angezeigten Werbung zu ermitteln und im besten Fall zu vergleichen.

Auch ist darauf hinzuweisen, dass wenn kontextbezogene Daten als Ersatz für (mitunter sensible) personenbezogene Daten verwendet werden, Menschen nach wie vor profiliert und überwacht werden, und zwar nicht aufgrund dessen, was sie tun, sondern aufgrund der Inhalte, die sie sich ansehen.[43] Die Methode kann daher theoretisch sogar manipulativer sein als es den Anschein hat – man denke nur an kontextbezogene Werbung für Abnehmprogramme, die neben Inhalten zu Diäten und Essstörungen geschaltet werden.

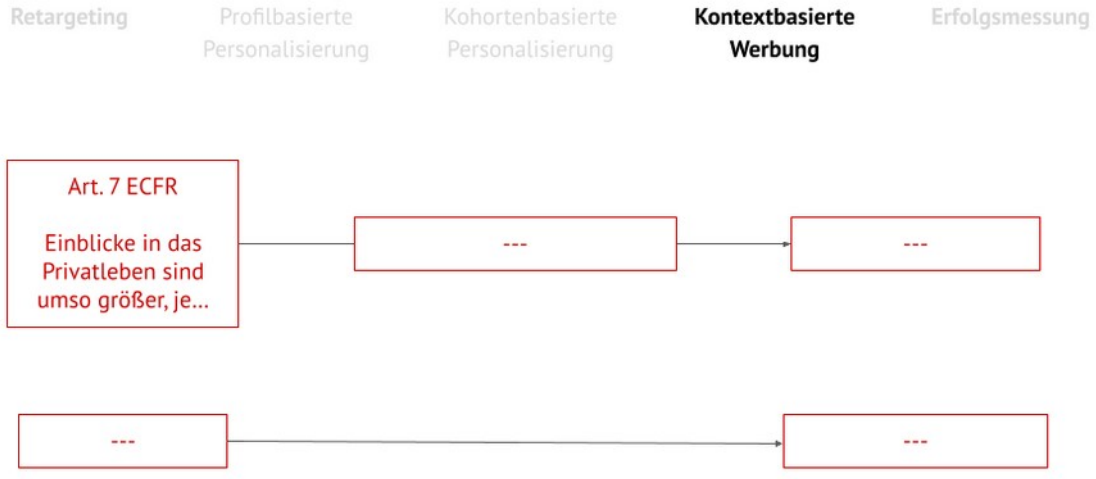

Abb. 6: Risiken der kontextbasierten Werbung.

41 Kopp, Is So-Called Contextual Advertising the Cure to Surveillance-Based “Behavioral” Advertising?, Tech Policy Press 26.9.2023.

42 Iwańska, Aufspüren oder nicht aufspüren, S. 33.

43 AWO Belgien, Studie über die Auswirkungen der jüngsten Entwicklungen in der digitalen Werbung auf den Datenschutz, die Verleger und die Werbetreibenden, 2023, S. 141.

2.5 Leistungsmessung als Teilzweck

Auch sollte kontextbasierte Werbung nicht darüber hinwegtäuschen, dass auch hier personenbezogene Daten verarbeitet werden, sobald ihr Erfolg gemessen wird. Die Erfolgsmessung wird hier nicht als eigenständiger Zweck, sondern als Nebenzweck zu einem oder mehreren der vorgenannten Zwecke angesehen. Der Grund dafür ist nicht nur, dass die genannten Werbeformen wirtschaftlich eine Erfolgsmessung erfordern, sondern auch, dass dies im Grunde die gleiche Verarbeitung personenbezogener Daten erfordert. Allerdings unterscheiden sich die Verfahren je nach dem für die Erfolgsmessung maßgeblichen Parameter in ihrer Eingriffsintensität.[44] So kann z.B. die Reichweitenmessung, d.h. die Anzahl der Websites, auf denen die Werbung erscheint, völlig unabhängig von den einzelnen Besuchern der Websites gemessen werden. Dasselbe gilt im Prinzip auch für die Messung von Impressionen. Für eine Impression muss zwar beobachtet werden, wie viele Nutzer sich auf der Website befinden, während die Werbung angezeigt wird, und dies geschieht in der Regel durch die Verarbeitung der IP-Adressen der Website-Besucher. Dabei ist es unerheblich, ob die einzelnen Personen die Werbung gesehen haben oder nicht. Die Anzahl der IP-Adressen auf allen Websites, auf denen die Werbung angezeigt wird, kann daher zusammengefasst werden, ohne dass das Verhalten der einzelnen Nutzer weiter beobachtet werden muss. Die Einblicke in das Privatleben der einzelnen Nutzer und andere Risiken sind daher relativ gering. Anders sieht es natürlich aus, wenn es um die Messung der Konversionsrate geht. Dazu muss man das Verhalten der einzelnen Nutzer genauer beobachten können, nämlich wie viele Personen auf eine Anzeige klicken und dann eine entsprechende Aktion auf der Zielwebsite durchführen (in der Regel durch Drücken der Kaufschaltfläche).

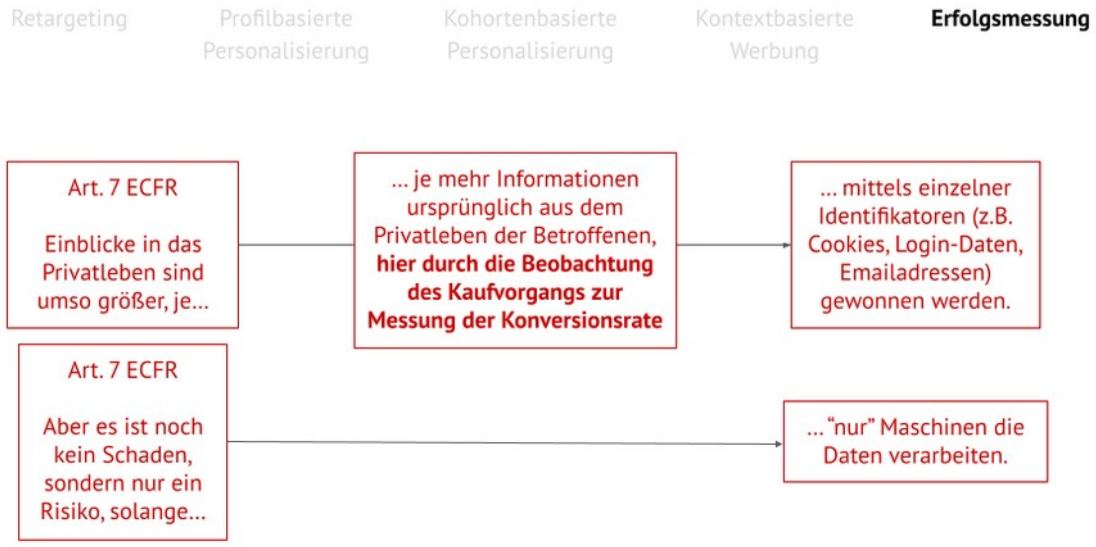

Abb. 7: Risiken der Erfolgsmessung.

Bei der Messung der Konversionsrate stellt sich daher die Frage, ob diese angesichts der damit verbundenen Risiken tatsächlich, wie zunächst angenommen, nur ein Nebenrisiko zu den Risiken der eigentlichen Werbeform darstellt. Oder ob die Messung der Konversionsrate eigene Risiken mit sich bringt, so dass dieses zusätzliche Risiko durch eine eigene Zweckbestimmung identifiziert werden muss. Bei näherer

44 Siehe die verschiedenen Schlüsselparameter unter https://www.netzdenke.de/blog/online-marketing/erfolgsmessung-im-online-marketing-diese-kennzahlen-solltest-du-kennen/.

Betrachtung sind die Einblicke in das Privatleben der Nutzer bei genauerer Betrachtung aber nur das kleinere Übel. Dies gilt zweifellos für Retargeting und profilbasierte personalisierte Werbung. Aber auch bei kohortenbasierter Werbung scheint die Zuordnung von mindestens einem Kaufinteresse zu einer Person immer noch gleichwertig zu sein mit der Beobachtung, ob diese Person dann auf der Werbung und auf der Zielwebsite auf den Kaufknopf klickt. In Anbetracht dieser Risikoanalyse schlagen wir daher vor, die Erfolgsmessung, auch im Falle der Messung der Konversionsrate, nur als Nebenzweck eines oder mehrerer der vorgenannten Werbezwecke zu behandeln. Da es keine gesondert hervorzuhebenden Risiken für die betroffene Person gibt, hat dies den Vorteil, dass sie nicht zusätzlich zu den ohnehin zahlreichen Informationen, die aus Sicht des Verbraucher- und Datenschutzes erforderlich sind, noch zusätzlich belastet wird. Lediglich bei kontextbasierter Werbung ist es notwendig, eine eigenständige Zweckspezifizierung vorzunehmen, da hier erstmals personenbezogene Daten verarbeitet werden.

Aber auch wenn die Erfolgsmessung als Unterkategorie des eigentlichen Werbezwecks gesehen wird, spielt die Art und Weise, wie dieser Zweck datenschutzgerecht erreicht wird, eine Rolle. Die oben beschriebene Mozilla PPA-Technologie für den Firefox-Browser ist ein gutes Beispiel dafür, wie diese Risiken auch bei einer solchen Verarbeitung deutlich reduziert werden können. Dies führt uns zum nächsten Punkt.

3 DIE ROLLE VON DATENSCHUTZFREUNDLICHEN TECHNOLOGIEN

Die Ausführungen zu den verschiedenen Formen der personalisierten Werbung haben gezeigt, dass es selbst innerhalb dieser definierten Kategorien noch Abstufungen geben kann, wie umfassend und tief die Einblicke in das Privatleben der Verbraucher sind. Gleiches gilt für die Manipulationsgefahr, die grundsätzlich bei allen Formen gleich ist. Auch hier kommt es darauf an, wie gut die Verbraucher über die jeweilige Werbeform informiert sind und wie leicht sie eingreifen können, um sich wirksam gegen das Manipulationsrisiko zu schützen. Dabei spielen datenschutzfreundliche Technologien eine zentrale Rolle. Beim Schutz der Privatsphäre sind dies vor allem Verfahren der Pseudonymisierung und Anonymisierung. Für die übrigen Risiken sind dies vor allem Maßnahmen der Transparenz, Fairness und Nutzerkontrolle. Ihre Wirksamkeit hängt freilich von ihrer Usability ab (siehe zur empirischen Messung der Wirksamkeit sogleich).

Abb. 8: Weitere Grundrechtsrisiken bei den unterschiedlichen Verfahren.

Wie oben dargelegt, sind diese Technologien nicht nur aus Sicht der Verbraucher wichtig. Sie sind auch aus der Sicht der Werbeindustrie wichtig, da ihre Umsetzung einen erheblichen Einfluss darauf haben kann, wie sehr die Verbraucher der jeweiligen Form der Werbung vertrauen. Dies wirkt sich nicht nur auf das Vertrauen der Verbraucher in die Marken von Verlegern, Werbetreibenden und Werbediensten aus, sondern hat auch ganz konkrete Auswirkungen auf die Zustimmungsrate.

4 ANKNÜPFUNGSPUNKTE FÜR DIE EMPIRISCHE MESSUNG

Der vorstehende Vorschlag für eine Kategorisierung der Grundrechtsrisiken entlang differenzierterer Zweckspezifizierungen im Bereich der Online-Werbung wirft für das SiD-Forschungsprojekt allerdings zwei wesentliche Fragen auf:

Erstens stellt sich die Frage, wie sich methodisch sicherstellen lässt, dass die Risiken den verschiedenen Verarbeitungszwecken richtig zugeordnet werden. Da die Risikozuordnung wesentlich ist für die rechtliche Einordnung und daran anknüpfende technisch-organisatorische Maßnahmen, besteht die Gefahr, dass bestimmte Risiken entweder übersehen oder übertrieben werden. Das Gleiche gilt für die Vorteile, die mit den jeweiligen Zwecken für die Betroffenen verbunden sind. Verbraucher äußern sich in verschiedenen Studien darüber, dass sie einen grundsätzlichen Mehrwert in der Personalisierung von Werbung sehen, dass dies nämlich die Werbung für sie tatsächlich relevanter machen könnte. Außerdem wägen Verbraucher bei ihrer Entscheidung, Informationen über sich preiszugeben, diese Vorteile gegen die wahrgenommenen Risiken ab. Es stellt sich also auch für die Vorteile die Frage, wie diese möglichst wahrheitsgetreu den verschiedenen Verarbeitungszwecken zugeordnet werden und mit den Risiken in ein stimmiges Verhältnis gebracht werden können.

Eine Möglichkeit ist, die Zuordnung der Vorteile und Risiken zu den unterschiedlichen Verarbeitungszwecken über eine möglichst breite Beteiligung von Experten sowohl aus dem Datenschutz- als auch dem Bereich der Online-Wirtschaft vorzunehmen. So ließe sich sicherstellen, dass keine Vorteile

bzw. Risiken übersehen oder übertrieben werden und die letztlich vorgenommene Zuordnung von möglichst vielen Stakeholdern mitgetragen werden.

Eine zweite Frage stellt sich in Hinsicht auf die visuelle und textliche Darstellung der Vorteile und Risiken für die Betroffenen. Gerade Jurist*innen tendieren dazu, rechtliche Sachverhalte über juristische Texte darzustellen. Diese führen aber in den seltensten Fällen zu einem besseren Verständnis bei den betroffenen Laien. Zur Lösung dieses Problems ist die Hinzuziehung von Experten aus der visuellen Gestaltung und der Sozialforschung denkbar. Mit deren konzeptionellen Wissen und Methoden könnte man sicherstellen, dass die Vorteile und Risiken der jeweiligen Datenverarbeitungszwecke von den Laien tatsächlich auch verstanden werden. Die durch die Experten zuvor festgestellten Vorteile und Risiken bilden damit die Metrik, anhand derer die Wirksamkeit des jeweiligen Informationsgestaltung gemessen wird. Hierbei lässt sich auch über quantitative A/B-Tests vorgehen. Im Rahmen dieser lassen sich etwa klassische Cookie Banner oder juristische Texte mit neuen Informationsgestaltungen dahingehend vergleichen, welche Darstellungsform die betroffenen Laien am besten über die festgestellten Vorteile und Risiken des jeweiligen Zwecks informiert. Genauso ließe sich vergleichend feststellen, welche auf der Informationsgestaltung aufbauende Kontrollarchitektur die betroffenen Laien am besten befähigt, die jeweiligen Risiken zu kontrollieren.

5 AUSBLICK AUF VERARBEITUNGSZWECKSPEZIFISCHE GRUNDRECHTSRISIKEN IM BEREICH VON SONSTIGEN PERSONALISIERTEN INHALTEN IM INTERNET

In den vorstehenden Ausführungen haben wir immer wieder auch auf Risiken hingewiesen, die nicht durch die Personalisierung von Werbung, sondern durch die Personalisierung sonstiger Inhalte auftreten können. Genannt wurden dabei Risiken für freie Wahlen und demokratische Willensbildungsprozesse. Klarzustellen ist dabei, dass diese in der Regel zu den vorgenannten Risiken hinzutreten. Nachwievor verursachen die technisch-organisatorischen Verfahren auch bei der Personalisierung sonstiger Inhalte also Risiken für die Privatsphäre der Betroffenen, der Manipulation, Diskriminierung sowie eventuell materielle und gesundheitliche Schäden. Hinzu treten nun aber weitere Risiken für bestimmte Freiheitsrechte, je nachdem in welchem Kontext die Personalisierung stattfindet. Werden etwa Nachrichtenseiten personalisiert, birgt dies das Risiko für die Informationsfreiheit der Betroffenen. Werden im schulischen Kontext Lernwerkzeuge an die individuellen Bedürfnisse und Fähigkeiten algorithmisch angepasst, stellt dies ein Risiko für die Ausbildungsfreiheit dar. Werden Inhalte im Unternehmenskontext individualisiert, kann dies ein Risiko für die unternehmerische Freiheit oder die Berufsausübungsfreiheit darstellen. Bei personalisierten Routenvorschlägen ließe sich theoretisch an Risiken für die autonome Fortbewegungsfreiheit denken usw. Entsprechend verlagern sich auch die Schwerpunkte der gesellschaftlich-strukturellen Risiken auf solche der freien Meinungsbildungsprozesse, des Bildungssystems als Ganzes, der freien Marktordnung etc.

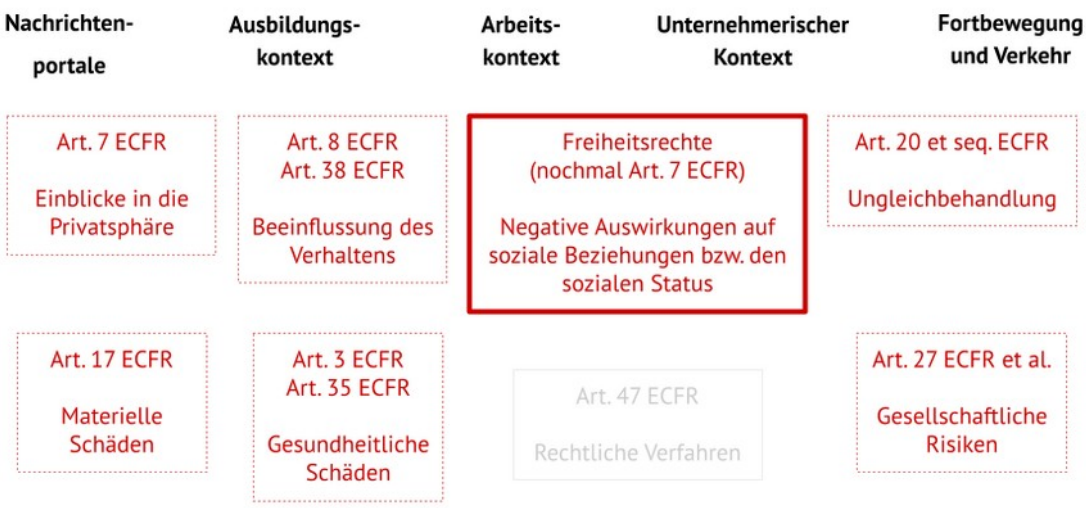

Abb. 9: Weitere soziale Kontexte und Grundrechtsrisiken.

Ob und inwiefern diese zusätzlichen Risiken andere oder erweiterte Schutzmaßnahmen erfordert, bedarf freilich einer eingehenderen Untersuchung.