



MAXIMILIAN LUKAT, GESA FELDHUSEN, PHILIPP HAGEN, JÖRG POHLE,
LUANA THOR

Zwischen Komfort und Vulnerabilität

Potentielle Grundrechtsrisiken personalisierter Online-Dienste

ABSTRACT

Personalisierte Werbung kann Risiken bergen, die die in der EU Grundrechtecharta zugesicherten Grundrechte betreffen (von Grafenstein, 2025). Personalisierung findet jedoch nicht nur bei Werbung, sondern auch bei anderen Online-Diensten statt, beispielsweise um Inhalte auszuwählen oder Empfehlungen auszugeben. In diesem Text wollen wir uns mit den Grundrechtsrisiken befassen, die bei der Personalisierung durch verschiedene Verarbeitungsweisen in den Bereichen Kultur, Nachrichten und Gesundheit auftreten könnten. Diese Verarbeitungsweisen werden in Einwilligungen zur Datenverarbeitung als Verarbeitungszwecke bezeichnet. Bei den hier besprochenen Risiken handelt es sich um potenzielle Risiken, die als Anhaltspunkte für je eine Literaturanalyse pro Bereich (Kultur, Nachrichten, Gesundheit) dienen sollen. In diesen Analysen sollen die tatsächlichen Risiken ermittelt werden. Die Auswahl der prominentesten Verarbeitungszwecke sowie die Zuordnung der Grundrechtsrisiken zu den Verarbeitungszwecken erfolgte in einem projektinternen Workshop. Der Text ist nach den Verarbeitungszwecken gegliedert, um an die vorangegangene Analyse der Grundrechtsrisiken von personalisierter Werbung anzuschließen. Bei der Betrachtung der Risiken über alle besprochenen Verarbeitungszwecke hinweg fällt auf, dass für den jeweiligen Bereich meistens die gleichen Risiken denkbar sind. Da die Datenverarbeitungsweisen in ihrer Funktion und ihren Ergebnissen jedoch sukzessive größer werden und weniger personenbezogene Daten verwenden, könnte sich auch die Qualität oder Intensität der Risiken minimieren. Die Ergebnisse der weiterführenden Analysen sollen im weiteren Projektverlauf mit unserer vorherigen Untersuchung zu den subjektiv wahrgenommenen Risiken von Nutzer*innen und Expert*innen im Hinblick auf Personalisierung und personalisierte Werbung (Lukat et. al., 2025) zusammengeführt werden, um ein umfassendes Risikomodell zu erstellen.

KEYWORDS

Personalisierung, Personalisierte Werbung, Grundrechte, Risiken, Verarbeitungszwecke

CITATION

Lukat, M., Feldhusen, G., Hagen, P., Thor, L. (2025). Zwischen Komfort und Vulnerabilität: Potentielle Grundrechtsrisiken personalisierter Online-Dienste. 29 pages. <https://doi.org/10.5281/zenodo.17569680>

LICENCE

This work is distributed under the terms of the Creative Commons Attribution 4.0 Licence (International) which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited (<https://creativecommons.org/licenses/by/4.0/>). Copyright remains with the authors.

AUTHOR INFO / AFFILIATION / FUNDING ETC.

Maximilian Lukat, wissenschaftlicher Mitarbeiter, Alexander von Humboldt Institut für Internet und Gesellschaft, Berlin

Gesa Feldhusen, wissenschaftliche Mitarbeiterin, nexus Institut für Kooperationsmanagement und interdisziplinäre Forschung, Berlin

Philipp Hagen, Director Legal Affairs & Data Privacy, Bundesverband Digitale Wirtschaft e.V., Berlin

Luana Thor, studentische Mitarbeiterin, nexus Institut für Kooperationsmanagement und interdisziplinäre Forschung, Berlin

Sicher im Datenverkehr ist gefördert vom Bundesministerium für Forschung, Technologie und Raumfahrt, Förderkennzeichen 16KIS1968

INHALT

1 EINLEITUNG	4
1.1 Personalisierung im Werbebereich	4
1.2 Personalisierung in der Verbreitung von Kultur (Bücher, Musik, Filme)	5
1.3 Personalisierung von Nachrichten	5
1.4 Personalisierung im Bereich Gesundheit	5
2 POTENTIELLE RISIKEN VON DATENVERARBEITUNGSZWECKEN BEI ONLINE-DIENSTEN	6
2.1 Recommender Systems auf Basis von Re-Targeting	6
2.1.1 Werbung	7
2.1.2 Kulturbereich	7
2.1.3 Nachrichtenbereich	7
2.1.4 Gesundheitsbereich	8
2.2 Recommender Systems auf Basis von Accounts	9
2.2.1 Werbung	9
2.2.2 Kulturbereich	10
2.2.3 Nachrichtenbereich	11
2.2.4 Gesundheitsbereich	12
2.3 Recommender Systems auf Basis von Profilen	13
2.3.1 Werbung	13
2.3.2 Kulturbereich	13
2.3.3 Nachrichtenbereich	14
2.3.4 Gesundheitsbereich	15
2.4 Recommender Systems auf Basis von Kohorten	16
2.4.1 Werbung	16
2.4.2 Kulturbereich	16
2.4.3 Nachrichtenbereich	17
2.4.4 Gesundheitsbereich	19
2.5 Recommender Systems auf Basis von Kontexten	20
2.5.1 Werbung	20
2.5.2 Kulturbereich	20
2.5.3 Nachrichtenbereich	21
2.5.4 Gesundheitsbereich	22
2.6 Sonstige relevante Zwecke	23
2.6.1. IT-Sicherheit	23
2.6.1.1. Werbung	23
2.6.1.2. Kultur	23
2.6.1.3. Nachrichten	24
2.6.1.4. Gesundheit	24
2.6.2. Performance-Messung und Optimierung	24
2.6.2.1. Werbung	24
2.6.2.2. Kultur	24
2.6.2.3. Nachrichten	25
2.6.2.2. Gesundheitsbereich	25
3 ZUSAMMENFASSUNG UND AUSBLICK AUF SUBJEKTIVE RISIKEN	26

1 EINLEITUNG

Personalisierung im Internet ist vielen wahrscheinlich als personalisierte Werbung bekannt. Sie begegnet uns stetig, wenn wir uns digital bewegen. Doch nicht nur Werbung ist personalisiert, sondern auch die Auswahl der Inhalte welche Nutzer*innen sehen, kann personalisiert sein. Damit ist gemeint, dass auf Grundlage der Interessen und Informationen, die bei der Nutzung erhoben oder von Nutzer*innen eingegeben werden, eine Empfehlung von Inhalten oder eine Anpassung des Angebots stattfindet. Damit einhergehend ergeben sich Risiken, die zu einer Einschränkung der in der Grundrechtecharta der Europäischen Union (EU-GRC) zugesicherten Grundrechte führen können. Für den Bereich der personalisierten Werbung haben wir uns im Rahmen des Projektes „Sicher im Datenverkehr“ (SiD) bereits mit den Grundrechtsrisiken beschäftigt (siehe von Grafenstein, 2025). Für eine bessere Übersichtlichkeit der Ergebnisse werden wir sie in diesem Text erneut aufführen. Gegenstand dieses Textes sind die Bereiche außerhalb der Werbung, in denen personalisierte Angebote oder Empfehlungen ausgegeben werden. Dabei fokussieren wir uns auf Personalisierung in den Bereichen Kultur, Nachrichten und Gesundheit. Den Bereich Social Media klammern wir in diesem Text aus, da dort alle vier Bereiche, sowie Inhalte und Werbung miteinander vermischt sein können. Die Risiken, die aus so einer Vermischung entstehen können, sollten auf Grund der Komplexität des Themas gesondert betrachtet werden.

Zunächst beschäftigen wir uns damit, welche Ausprägungen Personalisierung in den oben genannten Bereichen Kultur, Nachrichten und Gesundheit, sowie in der Werbung haben kann. Anschließend betrachten wir die potentiellen Risiken, die sich aus den prominentesten Verarbeitungszwecken von Daten für ein personalisiertes Angebot ergeben. Diese Verarbeitungszwecke haben wir in einem projektinternen Workshop herausgearbeitet. Abschließend folgt eine Zusammenfassung unter Betrachtung der größten Gemeinsamkeiten und Unterschiede der potentiellen Risiken.

1.1 Personalisierung im Werbebereich

In unserer vorherigen Untersuchung „Zwischen Bauchgefühl und Fachwissen: Risiken personalisierter Werbung im Internet“ (Lukat et al., 2025) haben wir uns mit der subjektiven Sicht von Nutzer*innen und Expert*innen auf die Risiken von personalisierter Werbung beschäftigt. Dort haben wir vielfältige Vorstellungen von vermuteten Risiken, sowie erwünschten und unerwünschten Auswirkungen von personalisierter Werbung vorgefunden. Nutzer*innen haben häufig fatalistische Überwachungsnarrative reproduziert. In Anbetracht ihrer Erfahrungen mit personalisierter Werbung sind die berichteten Auswirkungen aber weit weniger gravierend und Nutzer*innen sind sich der Vorteile, wie erhöhter Komfort, Relevanz und Zeitersparnis bewusst. Risiken werden vor allem im Missbrauch der erhobenen Daten und in unerwünschten Folgen, wie einem Gefühl des Kontrollverlustes oder einer potentiellen Diskriminierung gesehen. Aus unseren Interviews mit Expert*innen aus der Wirtschaft, Informatik, Soziologie und der Rechtswissenschaft ergibt sich ebenfalls ein heterogenes, fragmentiertes Verständnis davon, was technisch und sozial bei Personalisierung passiert, wer beteiligt ist und welche Risiken bestehen können. Große Unterschiede zu dem Wissen der Nutzer*innen ergaben sich vor allem in dem Detailgrad des Wissens einzelner Personen und der Eloquenz der Beschreibungen.

Aus juristischer Perspektive betonen Expert*innen und Nutzer*innen, dass mögliche Einblicke in das Privatleben der Nutzer*innen und damit in der Privatsphäre die größte Bedrohung durch personalisierte Werbung darstellen. In dem derzeitigen komplexen Werbe-Ökosystem können die Nutzer*innen weder vorhersehen noch wirksam kontrollieren, welche ihrer Online-Verhaltensweisen gezielt überwacht, mit wem diese Informationen geteilt und in welcher Form sie letztlich verwendet werden (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.). Die Risiken, die das System für Einzelne birgt,

haben unterschiedliche Auswirkungen je nach Parameter, wie zum Beispiel dem Kontext der Datenerhebung oder der Art der erhobenen Daten; den aus der Datenanalyse abgeleiteten Informationen über die Verbraucher; und dem Ausmaß, wie viele andere Personen von diesen Informationen Kenntnis erhalten (vgl. von Grafenstein, 2025).

1.2 Personalisierung in der Verbreitung von Kultur (Bücher, Musik, Filme)

Personalisierung in der Verbreitung von Kunst und Kultur basiert heute primär auf algorithmischen Empfehlungssystemen, die verschiedene Datenquellen nutzen, um individuell zugeschnittene kulturelle Inhalte auszuspielen. Plattformen wie Spotify analysieren Hörgewohnheiten, Playlist-Erstellungen und Interaktionsmuster, um personalisierte Musik-Empfehlungen zu generieren, während SoundCloud zusätzlich Kommentare, Reposts und Follow-Beziehungen zu Künstler*innen auswertet. Netflix und ähnliche Streaming-Dienste kombinieren Verläufe, Bewertungen und sogar Pausenverhalten, um Film- und Serienvorschläge zu erstellen. Buchhandelsplattformen nutzen Kaufhistorien, Bewertungen und Browsing-Verhalten für Literaturempfehlungen, während spezialisierte Plattformen wie Goodreads Lesebewertungen analysieren um neue Empfehlungen zu geben. Filmplattformen wie IMDb oder Letterboxd werten Watchlists, Ratings und Review-Verhalten aus, um Filmempfehlungen zu generieren. Diese Systeme arbeiten oft mit hybriden Ansätzen, die kohortenbasierte ("Nutzer*innen mit ähnlichen Präferenzen mögen auch..."), inhaltsbasierte (Analyse von Genremerkmalen, Künstlereigenschaften) und kontextbasierte Faktoren (Tageszeit, Gerätenutzung, geografischer Standort) kombinieren.

Die Personalisierung erfolgt dabei auf verschiedenen Ebenen der kulturellen Wertschöpfungskette: Von der Kuration und Sichtbarkeit kultureller Inhalte über die Preisgestaltung (dynamic pricing basierend auf Zahlungsbereitschaft) bis hin zur Gestaltung der Nutzer*innen-Erfahrung selbst. Empfehlungssysteme entscheiden nicht nur, was Nutzenden vorgeschlagen wird, sondern auch in welcher Reihenfolge, zu welcher Zeit und in welchem visuellen oder auditiven Kontext sie präsentiert werden. Diese Entwicklung verändert sowohl die Rezeption als auch die Produktion von Kunst und Kultur grundlegend: Künstler*innen orientieren sich an den Logiken der Empfehlungssysteme, während Kulturkonsument*innen immer seltener mit unerwarteten oder herausfordernden Inhalten konfrontiert werden, die außerhalb der vermuteten Interessensphäre liegen.

1.3 Personalisierung von Nachrichten

Nachrichtenportale, News-Apps oder digitale Medienplattformen schlagen ihren Nutzer*innen auf verschiedenen Datenquellen basierend Inhalte vor, die sie interessieren könnten, um relevantere Beiträge zu zeigen und so die Verweildauer auf der Seite zu erhöhen. Durch die erhöhte Verweildauer kann zudem mehr Werbung angezeigt werden, was dem ökonomischen Interesse der Anbieter zugutekommt. Diese Auswahl der Inhalte könnte einige Risiken mit sich bringen, die wir in diesem Beitrag durchdenken möchten.

1.4 Personalisierung im Bereich Gesundheit

Personalisierung im Bereich Gesundheit kann sich auf digitale Gesundheitsangebote, Fitness- und Wellness-Apps beziehen, bei denen das Angebot mithilfe den von Nutzer*innen eingegebenen Informationen oder erhobenen Nutzungsinformationen angepasst wird beziehungsweise worauf basierend Empfehlungen ausgegeben werden. Die in diesem Text besprochenen potentiellen Risiken beziehen sich vor allem auf die Risiken, die sich aus der Nutzung solcher Dienste ergeben könnten.

Gesundheits-Apps können eine Vielzahl persönlicher Informationen erfassen, wie Symptome und Medikamenteneinnahme über Ernährungsgewohnheiten bis hin zu Schlafmustern und daraus individuelle Gesundheitsprofile generieren. Beispiele dafür sind Diabetes-Management-Apps, die Blutzuckerwerte,

Mahlzeiten und Aktivitätsdaten analysieren können, um Dosierungsempfehlungen für Insulin zu geben oder auch digitale Gesundheitsanwendungen, wie Mental-Health-Apps, die Stimmungen und Verhaltensmuster bewerten, um individuelle Therapieempfehlungen oder Meditationsübungen anzubieten.

Die seit einigen Jahren beliebten Fitness- und Wellness-Apps könnten auf Basis von Fitnesszielen, körperlichen Voraussetzungen und persönlichen Vorlieben maßgeschneiderte Trainingspläne und Ernährungsempfehlungen erstellen. Dabei könnten nicht nur objektive Körperdaten, sondern auch subjektive Präferenzen und Motivationsmuster in die Empfehlungen einfließen. Wearables wie Smartwatches und Fitness-Tracker sammeln ebenfalls analysierbare Daten, die in detaillierte Gesundheitsprofile fließen könnten.

Im Bereich der Telemedizin könnten personalisierte Überwachungs- und Anpassungssysteme entstehen. Die gesammelten Daten könnten genutzt werden, um Behandlungsempfehlungen zu geben oder Therapieverläufe anzupassen. Besonders chronisch Kranke könnten von Alarmsystemen profitieren, die kontinuierlich Vitaldaten auswerten und bei individuell definierten Abweichungen automatisch Warnungen oder Behandlungsvorschläge ausgeben.

Diese möglichen Formen der Personalisierung versprechen eine effizientere und angepasste Gesundheitsversorgung. Gleichzeitig bestehen unbestreitbare Risiken für den Schutz der Privatsphäre und fundamentale Fragen zum Umgang mit hochsensiblen Gesundheitsdaten in digitalen Ökosystemen.

Welche Risiken durch die Datenverarbeitung in den vier zuvor aufgeführten Bereichen bestehen könnten, wollen wir im folgenden Kapitel erörtern.

2 POTENTIELLE RISIKEN VON DATENVERARBEITUNGSZWECKEN BEI ONLINE-DIENSTEN

Die Risiken der Verarbeitungszwecke, die wir hier darstellen und besprechen, sind zunächst nur potentielle Risiken, welche die in der EU-GRC zugesicherten Grundrechte betreffen und einschränken könnten. Diese potentiellen Risiken müssen bei der Gestaltung und dem Betrieb von echten Personalisierungssystemen, im Sinne einer vorausgehenden Risikominimierung, mit Hilfe von technischen und organisatorischen Maßnahmen (TOMs) adressiert und bewältigt werden. Durch dieses Vorgehen sollten „nur“ noch nicht ausschließbare (Rest-)Risiken übrig bleiben. Die potentiellen Risiken werden wir jeweils für den Bereich der Werbung, der Kultur, der Nachrichten und der Gesundheit besprechen. Da sich bestimmte Themenbereiche und Logiken überschneiden, kann es vorkommen, dass bestimmte Risiken mehrfach pro Themenbereich und Verarbeitungszweck genannt werden.

Durch die verschiedenen Logiken der Verarbeitungsweisen ergeben sich unterschiedliche Risiken, die damit einhergehen können. Die fünf folgenden Verarbeitungszwecke personenbezogener Daten beziehen sich allesamt auf Recommender Systems, also Empfehlungsdienste, die auf Grundlage unterschiedlicher Daten und Auswertungslogiken Empfehlungen für Inhalte, Werbung usw. ausgeben. Der sechste und siebte Verarbeitungszweck, die IT-Sicherheit und die Optimierung und Performancemessung von Diensten, erheben ebenfalls personenbezogene Daten, weswegen wir uns auch die Risiken für diese Bereiche anschauen.

2.1 Recommender Systems auf Basis von Re-Targeting

Der erste Verarbeitungszweck, den wir betrachten wollen, ist die Bereitstellung von Empfehlungen auf Basis von Re-Targeting. Re-Targeting bedeutet, dass Endgeräte auf Grund bestimmter Merkmale, die sie

aufweisen und an Dienste übertragen, erkannt und wiedererkannt werden können. Diese Wiedererkennung kann zum Beispiel mit Identifikationsnummern geschehen, die in Cookies gespeichert werden. Durch diese Wiedererkennung kann gezählt werden, wie oft eine Seite bereits besucht wurde und so ein Interesse abgeleitet werden. Sie kann aber auch dazu genutzt werden, gezielt Empfehlungen auszuspielen, die auf zuvor erhobenen Interessen beruhen. So kann beispielsweise auch die Häufigkeit von Empfehlungen pro Endgerät ausgewählt werden.

2.1.1 Werbung

Für den Bereich der Werbung könnten in erster Linie Risiken für die in Art. 7 EU-GRC zugesicherte Achtung des Privat- und Familienlebens herausgestellt werden. Dies ist dadurch begründet, dass Nutzer*innen Re-Targeting durch die Intransparenz der Funktionsweise als aufdringlich wahrnehmen und sich dadurch verfolgt fühlen können (von Grafenstein, 2025, S. 12).

Denkbar wäre auch, dass Werbung, die von Re-Targeting-Systemen ausgegeben wird, gegen Art. 20 EU-GRC verstoßen könnte, wenn sie zu einer systematischen Ungleichbehandlung verschiedener Nutzer*innengruppen führen würde. Dies wäre dann problematisch, wenn Re-Targeting-Systeme bestimmten Personen aufgrund ihrer Profile systematisch andere Produkte, Preise oder Informationen anzeigen würden als anderen Personen und dies transparent vom Händler kommuniziert wird. Bedenklich wäre es auch, wenn Re-Targeting-Systeme an geschützte Merkmale wie Geschlecht, ethnische Herkunft oder Religion anknüpfen würden und dadurch beispielsweise Frauen andere Stellenangebote oder Kreditkonditionen präsentiert bekämen als Männer. In einem solchen Szenario wäre die personalisierte Werbung eine digitale Form der Diskriminierung, die den Gleichheitsgrundsatz untergraben würde. Selbst wenn keine direkte Benachteiligung beabsichtigt ist, könnte die intransparente Funktionsweise der Tracking-Systeme dazu führen, dass bestehende gesellschaftliche Ungleichheiten reproduziert und verfestigt würden, wodurch bestimmte Bevölkerungsgruppen strukturell benachteiligt blieben.

2.1.2 Kulturbereich

Im Kulturbereich ist die Ausspielung von Empfehlungen mit Hilfe von Re-Targeting besonders häufig. Bekannt sind unter anderem Erinnerungen, sich noch nicht zu Ende konsumierte Inhalte anzuschauen, bereits konsumierte Inhalte, die erneut aufgerufen werden können oder das wiederholte Vorschlagen von Inhalten.

Die Schwelle zwischen Information und Werbung kann unter Umständen ziemlich schmal sein. Ein Risiko, das dabei bestehen könnte, wäre ein materieller Schaden nach Art. 17 EU-GRC, wenn nicht ersichtlich ist, dass es sich bei einer Empfehlung um Werbung handelt und Personen so zu einem Kauf bewegt werden.

Ein weiteres potentiell Risiko bei der Empfehlung von kulturellen Inhalten auf Basis von Re-Targeting ist, dass das Recht auf Informationsfreiheit nach Art. 11 EU-GRC beeinträchtigt werden könnte. Dies kann der Fall sein, wenn Personen gewisse Inhalte aufgedrängt werden oder bestimmte Inhalte nicht mehr gefunden werden können, beispielsweise durch explizite Shadow Bans. Das Wiederauffinden von Inhalten oder das aktive Ausschließen bestimmter Inhalte, da diese nicht mehr angezeigt werden, da sie nicht den vermuteten Interessen entsprechen, kann eine weitere Beeinflussung der Informationsfreiheit sein.

2.1.3 Nachrichtenbereich

Im Nachrichtenbereich könnte ebenfalls das Risiko bestehen, dass die Informationsfreiheit nach Art. 11 EU-GRC durch den Verarbeitungszweck eingeschränkt wird. In diesem Kontext sind die im öffentlichen

Diskurs oft angesprochenen Filterblasen und Echokammern zu nennen, die stellvertretend für eine befürchtete Einschränkung von Meinungsppluralismus stehen. Damit geht die Vorstellung einher, dass durch die fehlende Konfrontation mit verschiedenen Perspektiven die Fähigkeit der Gesellschaft verloren geht, sich differenziert mit komplexen Themen auseinanderzusetzen und Ambiguität auszuhalten. In letzter Instanz könnte dies auch das Demokratieprinzip gefährden, wenn aus dem Akzeptieren von Meinungsverschiedenheiten ein grundlegender Antagonismus wird. Aus dieser Befürchtung heraus ist es denkbar, dass durch Nachrichtenvorschläge auf Basis von Re-Targeting häufig dieselben Meinungspositionen einer Debatte empfohlen werden und so Sichtweisen verhärtet werden könnten. Eine Einschränkung der Informationsfreiheit könnte dann vorliegen, wenn auf Grundlage der vermuteten Interessen kein pluralistisches Meinungsbild und Informationsangebot ausgespielt und empfohlen wird. Da Personalisierung nicht nur auf dezidierten Empfehlungsseiten zum Einsatz kommt, sondern auch bei Suchanfragen, ist es denkbar, dass dies auch Einfluss auf die gezielte Suche von Nachrichten haben kann, wodurch Art. 11 erneut tangiert würde.

2.1.4 Gesundheitsbereich

Re-Targeting bei digitalen Gesundheitsangeboten und Fitness-Apps könnte zu einer systematischen Informationsasymmetrie führen, die das Recht auf Informationsfreiheit (Art. 11 EU-GRC) untergraben könnte. Es ist denkbar, dass durch das Re-Targeting bestimmte Gesundheitsinformationen, Präventionsangebote oder Behandlungsoptionen einer Person besonders oft angezeigt werden und andere gar nicht. Dadurch entstünde eine gefilterte Realität, in der wichtige Gesundheitsinformationen vorenthalten werden könnten. Dies wäre besonders problematisch, da Gesundheitsentscheidungen auf vollständigen und objektiven Informationen basieren sollten. Die Vorauswahl könnte dazu führen, dass Menschen keine Kenntnis von alternativen Behandlungsmethoden, günstigeren Therapieoptionen oder präventiven Maßnahmen erhielten, die für ihre Situation relevant wären.

Das Diskriminierungsverbot (Art. 21) könnte besonders durch die gezielte Ausspielung oder das bewusste Vorenthalten von Gesundheitsinformationen an bestimmte Personengruppen verletzt werden. Re-Targeting-Systeme könnten bestimmte demographische Gruppen von wichtigen Gesundheitsangeboten ausschließen, etwa wenn älteren Menschen innovative Behandlungsmethoden nicht angezeigt würden oder Menschen mit niedrigem Einkommen kostenintensive, aber effektive Therapien nicht vorschlagen würden. Diese Diskriminierung könnte sich auch auf den Schutz innerer Überzeugungen (Art. 10) auswirken, falls religiöse oder weltanschauliche Überzeugungen als Grundlage für die Einschränkung des Informationszugangs dienen, beispielsweise bei reproduktionsmedizinischen Angeboten oder bestimmten Behandlungsmethoden.

Ein besonders kritischer Aspekt wäre die potenzielle Exklusion vom Zugang zu Gesundheits-, Pflege- und Sozialleistungen, was die Art. 34 (Soziale Sicherheit) und 35 (Gesundheitsschutz) betreffen könnte. Wenn durch Re-Targeting Informationen über Sozialleistungen, Präventionsprogramme oder kostenlose Gesundheitsdienste nicht an relevante Personen ausgespielt würden, da fehlerhafte Annahmen zu Grunde liegen, könnten vulnerable Gruppen systematisch ausgeschlossen werden. Dies könnte den Informationszugang zu Gesundheitsinformationen betreffen und damit auch indirekt den Zugang zu Leistungen.

Die Manipulationsgefahr (Art. 38 EU-GRC Verbraucherschutz) könnte sich durch die Beeinflussung vulnerabler Personen zum Kauf oder zur Nutzung bestimmter Gesundheitsangebote manifestieren. Re-Targeting könnte auf Grund von bereits erfassten Informationen Lösungen für Gesundheitsprobleme anbieten, die möglicherweise nicht evidenzbasiert oder sogar schädlich wären. Besonders kritisch wäre dies bei Menschen in Krankheitssituationen, die aufgrund ihrer emotionalen Verfassung besonders empfänglich

für manipulative Praktiken sein könnten und beispielsweise in Verschwörungserzählungen verhaftet sind.

IT-Sicherheitsrisiken könnten eine fundamentale Bedrohung für das Recht auf Achtung des Privat- und Familienlebens (Art. 7) darstellen. Die für Re-Targeting notwendige Sammlung und Verarbeitung von allen möglichen Informationen könnte umfangreiche Datenbestände schaffen, aus denen sich Gesundheitsinformationen ableiten lassen oder direkt erfasst werden. Bei Sicherheitsverletzungen der Dienste könnte dies einen enormen Schaden anrichten. Diese "Downstream-Risiken" würden nicht nur für die unmittelbar Betroffenen relevant sein, sondern könnten auch Familienmitglieder und soziale Netzwerke in Mitleidenschaft ziehen. Ein Datenleck könnte zu Diskriminierung am Arbeitsplatz, bei Versicherungen oder in sozialen Beziehungen führen, zum Beispiel wenn eine Person unabsichtlich geoutet wird. Des Weiteren könnten Datenlecks Art. 21 (Nichtdiskriminierung), 23 (Gleichstellung der Geschlechter), sowie die besonderen Schutzrechte vulnerabler Gruppen nach den Art. 24 (Kinderrechte), 25 (Rechte älterer Menschen) und 26 (Integration von Menschen mit Behinderung) verletzen.

Schließlich könnten fehlerhafte Ergebnisse erhebliche Risiken für das Recht auf körperliche und geistige Unversehrtheit (Art. 3) bergen. Würden Re-Targeting-Systeme aufgrund unvollständiger oder fehlerhafter Daten falsche Gesundheitsempfehlungen ausspielen oder Menschen von wichtigen medizinischen Informationen fernhalten, könnten direkte Gesundheitsschäden entstehen. Dies wäre besonders gravierend, da Gesundheitsentscheidungen unter Umständen irreversible Konsequenzen haben und Fehler in der Informationsbereitstellung zu verzögerten Diagnosen, inadäquaten Behandlungen oder gesundheitsschädlichen Verhaltensweisen führen könnten.

2.2 Recommender Systems auf Basis von Accounts

In diesem Abschnitt soll es zunächst um Risiken gehen, die beim Einsatz von Recommender Systems auf Basis von Accounts auftreten könnten. Bei Accounts handelt es sich um Konten, die Nutzer*innen selber angelegt und dort Informationen eingetragen haben. Wir können daher annehmen, dass Nutzer*innen davon ausgehen, dass Systeme sie als Person wiedererkennen, wenn sie in ihrem Konto angemeldet sind. Accounts sind jedoch von Profilen abzugrenzen. Profile werden eher von Datenverarbeitenden gesteuert und haben weniger Steuerung durch Nutzer*innen.

2.2.1 Werbung

Werbung, die auf Accountdaten basiert, könnte das durch Art. 7 der EU-Grundrechtecharta geschützte Recht auf Achtung des Privatlebens beeinträchtigen. Wenn Plattformen detaillierte Profile aus Nutzungsverhalten, Kommunikationsinhalten, Standortdaten und persönlichen Präferenzen erstellen würden, um zielgerichtete Werbung auszuspielen, könnte dies einen Eingriff in die Privatsphäre darstellen (von Grafenstein, 2025, S. 13). Besonders problematisch wäre es, wenn sensible Informationen über Gesundheitszustand, politische Überzeugungen, sexuelle Orientierung oder religiöse Ansichten aus den Accountdaten abgeleitet und für Werbezwecke genutzt würden. Die Auswertung des digitalen Verhaltens könnte eine Atmosphäre schaffen, in der Nutzer*innen sich beobachtet fühlen würden und ihr Verhalten entsprechend anpassen. Selbst wenn eine formale Einwilligung zur Auswertung der Accountdaten vorläge, wäre fraglich, ob diese angesichts der Komplexität der Datenverarbeitung und der faktischen Alternativlosigkeit vieler digitaler Dienste wirklich freiwillig und informiert erfolgen könnte. Die Unverhältnismäßigkeit zwischen dem Zweck der Finanzierung durch Werbung und dem Ausmaß der Datenerfassung könnte somit einen Verstoß gegen das Grundrecht auf Privatsphäre begründen.

Die Verwendung von Accountdaten für personalisierte Werbezwecke könnte auch mit Art. 17 der EU-GRC in Konflikt geraten, der das Recht auf Eigentum schützt, wenn dadurch ein materieller Schaden für die Nutzer*innen entstehen würde. Wenn personalisierte Werbung auf Basis umfassender

Accountdaten gezielt psychologische Schwachstellen, momentane emotionale Zustände oder Verhaltenstendenzen ausnutzen würde, könnten Nutzer*innen zu Käufen verleitet werden, die sie ohne äußeren Einfluss nicht getätigt hätten. Besonders problematisch wäre dies, wenn die Recommender Systems erkennen würden, wann Personen besonders empfänglich für Impulskäufe sind, etwa in Stresssituationen, bei Einsamkeit oder nach Analyse von Konsummustern. Die daraus resultierenden Ausgaben würden das Vermögen der Betroffenen konkret schmälern und könnten bei systematischer Anwendung zu erheblichen finanziellen Belastungen führen. Wenn vulnerable Gruppen wie Jugendliche, Personen mit Suchterkrankungen oder Menschen in prekären finanziellen Situationen durch datengetriebene Werbung gezielt angesprochen würden, könnte dies deren wirtschaftliche Existenz gefährden. Die Manipulationswirkung solch präzise zugeschnittener Werbung würde die Entscheidungsfreiheit der Konsumenten untergraben und zu einer Schädigung ihres Eigentums führen, ohne dass ein physischer Zwang oder Betrug im klassischen Sinne vorläge.

Accountbasierte Werbung könnte ebenso gegen den in Art. 20 der EU-Grundrechtecharta verankerten Gleichheitsgrundsatz verstoßen, wenn sie zu systematischer Ungleichbehandlung verschiedener Nutzer*innengruppen führen würde. Recommender Systems, die Empfehlungen auf Grundlage von Accountdaten ausgeben, könnten bestimmten Personen privilegierten Zugang zu Informationen, Produkten oder Dienstleistungen gewähren, während andere systematisch benachteiligt würden. In den Bereichen des Arbeitsmarktes, der Wohnungssuche, der Bildung oder bei Finanzdienstleistungen könnten unterschiedliche Angebote auf Basis von Profildaten zu struktureller Diskriminierung führen. Selbst wenn nicht explizit geschützte Merkmale wie Geschlecht, ethnische Herkunft oder Alter einbezogen werden, könnten sie durch abgeleitete Erkenntnisse mittelbare Diskriminierung bewirken. Die Intransparenz der Systeme würde es Betroffenen nahezu unmöglich machen, eine ungleiche Behandlung zu erkennen und anzufechten, da sie nicht wissen können, welche Werbung oder Angebote anderen Nutzer*innen angezeigt wird. Wenn zwei Personen mit objektiv vergleichbarer Qualifikation aufgrund ihrer unterschiedlichen Accountprofile systematisch verschiedene Chancen erhielten, würde dies den Grundsatz der Rechtsgleichheit aushöhlen.

2.2.2 Kulturbereich

Accountbasierte Recommender Systems auf Musik- und Kulturplattformen wie Spotify, SoundCloud oder Bandcamp könnten erhebliche grundrechtliche Risiken bergen, die weit über klassische Werbepraktiken hinausgingen. Besonders problematisch kann die mögliche Verletzung der Informationsfreiheit nach Art. 11 der EU-GRC sein: Wenn Empfehlungsalgorithmen ("Andere Leute, die das gehört haben, haben auch gehört") kontinuierlich ähnliche Inhalte basierend auf detaillierten Account-Profilen vorschlagen, entstünden möglicherweise personalisierte "Filter-Bubbles", die den freien Zugang zu vielfältigen kulturellen Inhalten unbeabsichtigt einschränken könnten. So werden account basierte Profile dabei nicht nur aktuelle Hörgewohnheiten berücksichtigen, sondern auch historische Daten, Playlists, gespeicherte Titel und soziale Interaktionen einbeziehen – bei Goodreads etwa Bewertungen von Leser*innen, bei Letterboxd Watchlists und Filmkritiken – was zu einer noch stärkeren Verfestigung bestehender Präferenzen führen könnte. Nutzer*innen werden in ihren kulturellen Gewohnheiten gehalten, anstatt mit der Breite des verfügbaren Angebots konfrontiert zu werden. Dies kann nicht nur das Recht auf Information beschneiden, sondern auch die Möglichkeit zur freien Meinungsbildung beeinträchtigen, da kulturelle Inhalte oft implizit politische oder gesellschaftliche Botschaften transportieren.

Die Account- basierte Personalisierung könnte besonders bei Kulturnachrichten und politisch motivierten Inhalten problematisch werden. Wenn Anbieter aufgrund detaillierter Nutzer*innenprofile gezielt bestimmte Nachrichten über Künstler*innen, Musikszenen oder kulturpolitische Themen ausspielen, könnte dies demokratische Meinungsbildungsprozesse verzerren und die in Art. 2 EUV verankerte Werte der Demokratie und Rechtsstaatlichkeit gefährden. Politische Beeinflussung durch Politikinfluencer, die

über Musik-, Film- und Literaturkanäle ihre Botschaften verbreiteten, wäre durch accountbasierte Targeting besonders effektiv, da sie an individuelle kulturelle Präferenzen anknüpfen und so authentischer wirkt. Die personalisierte Ansprache basierend auf Musikgeschmack, Filmvorlieben oder Literaturinteressen könnte politische Manipulationsversuche subtiler und schwerer erkennbar machen.

Die manipulative Dimension accountbasierter Empfehlungen könnte Art. 38 der EU-GRC (Verbraucherschutz) tangieren, wenn Algorithmen darauf programmiert wären, Engagement zu maximieren und Nutzer*innen zum Kauf von Musik, Büchern, Filmen, Premium-Abonnements oder Merchandise anzuregen. Dabei könnten psychologische Mechanismen ausgenutzt werden, etwa durch zeitlich begrenzte Angebote, personalisierte Buchempfehlungen oder emotionale Beeinflussung durch gezielt ausgewählte Inhalte, basierend auf detaillierten Accountanalysen. Diese Praktiken könnten Nutzer*innen ungewollt zu Datenobjekten reduzieren und ihre Entscheidungsautonomie untergraben, was grundlegende Prinzipien der Menschenwürde (Art. 1) verletzen würde.

Accountbasierte Recommender Systems könnten Auswirkungen auf die Kunst- und Wissenschaftsfreiheit nach Art. 13 der Charta haben, da sie ein zentrales Element bei Plattformen wie Spotify, Apple Music oder SoundCloud sind. Sie bestimmen welche kulturellen Inhalte überhaupt sichtbar werden und welche in der digitalen Unsichtbarkeit verschwinden. Kleinere, experimentelle oder nicht-kommerzielle Künstler*innen, Independent-Autor*innen oder Art-House-Filme hätten strukturell schlechtere Chancen, wahrgenommen zu werden, wenn Empfehlungslogiken hauptsächlich bereits in Accounthistorien erfolgreiche oder ähnliche Inhalte bevorzugten. Dies könnte zu einer unbeabsichtigten Homogenisierung der Kulturlandschaft führen und sowohl die Freiheit der Kunstschaffenden beschneiden, neue Zielgruppen zu erreichen, als auch das Recht der Rezipienten auf kulturelle Vielfalt und Teilhabe zu beeinträchtigen. Die accountbasierte Logik könnte dabei besonders problematisch sein, da sie nicht nur momentane Präferenzen, sondern langfristige kulturelle Gewohnheiten verstärken und damit kulturelle Offenheit und Experimentierfreude systematisch reduzieren könnten.

Weitere Risiken würden sich aus der Verletzung des Rechts auf Privatsphäre (Art. 7) und Datenschutz (Art. 8) ergeben, wenn detaillierte, langfristige Kultur- und Konsumprofile erstellt werden – etwa durch die Analyse von Hörverhalten auf Spotify, Lesepräferenzen auf Kindle oder Streaming-Gewohnheiten auf Netflix – ohne dass Nutzer*innen ausreichend über die Tragweite dieser Profilbildung informiert sind oder wirksame Kontrollmöglichkeiten wahrnehmen können. Diskriminierungsrisiken nach Art. 21 könnten entstehen, wenn bestimmte demographische oder sozioökonomische Gruppen aufgrund ihrer Account-Daten unterschiedlich behandelt oder ihnen verschiedene kulturelle Inhalte vorgespielt werden.

2.2.3 Nachrichtenbereich

Re-Targeting-Mechanismen in digitalen Nachrichtenportalen könnten Risiken für die in der EU-Grundrechtecharta verankerten Rechte bergen, insbesondere für die Informationsfreiheit nach Art. 11. Wenn basierend auf dem bisherigen Nutzer*innenverhalten entschieden würde, welche Nachrichten und Perspektiven Nutzer*innen präsentiert werden, könnte dies zu einer unbeabsichtigten Verengung des Informationsspektrums führen. Statt eines breiten, pluralistischen Meinungsbildes erhielten Nutzer*innen zunehmend nur noch solche Inhalte, die ihre bestehenden Überzeugungen bestätigten. Diese durch die Logik von Empfehlungssystemen entstehende Filterung könnte das Grundrecht auf freien Zugang zu Informationen untergraben, da sie eine umfassende und ausgewogene Meinungsbildung verhinderte und damit die Grundlage demokratischer Teilhabe schwächte.

Besonders problematisch wäre die potenzielle Verletzung von Art. 10 (Schutz der inneren Überzeugungen) und Art. 21 (Diskriminierungsverbot). Es könnten detaillierte Profile über politische Einstellungen, weltanschauliche Präferenzen und soziale Merkmale erstellt werden, die von Datenverarbeitenden einem

oder mehreren Endgeräten zugeordnet würden, ohne dass Nutzer*innen explizit zustimmen oder überhaupt wüssten, welche Schlüsse über sie gezogen würden. Die Auswahl könnte dabei ungewollt diskriminierende Effekte entfalten, wenn bestimmte gesellschaftliche Gruppen durch die Logik der Systeme von bestimmten Informationen ausgeschlossen oder mit einseitigen Darstellungen konfrontiert würden.

Ein weiteres Grundrechtsrisiko läge in der potentiellen Verletzung der Menschenwürde (Art. 1) und des Rechts auf Privatleben (Art. 7). Die kontinuierliche Analyse des Informationsverhaltens könnte zu einer reduktionistischen Betrachtung der Nutzer*innen als vorhersagbare Datenpunkte führen, was ihre Autonomie und Würde als freie Meinungsbildner*innen beeinträchtigen könnte. Das Recht auf Privatleben wäre bedroht, wenn Account-Profilen Rückschlüsse auf intime Überzeugungen und Weltanschauungen zugeordnet würden.

2.2.4 Gesundheitsbereich

Accountbasierte Recommender Systems in Gesundheits- und Fitness-Apps könnten weitreichende Grundrechtsrisiken bergen, da sie auf expliziter Nutzer*innenregistrierung und damit auf umfangreicher Dateneingabe durch Nutzer*innen und eindeutiger Zuordenbarkeit basieren. Bei der bewussten Erstellung eines Accounts können Nutzer*innen Informationen eingeben, die Rückschlüsse auf Demografie und Interessen geben könnten. Bei dieser Art der Datenverarbeitung könnten nicht nur Gesundheits- und Fitnessdaten, sondern auch scheinbar unverbundene Informationen wie Musikpräferenzen einfließen, wenn z.B. ein Musikstreaming Dienst mit einer App verknüpft wird. Auch ist es denkbar, dass soziale Kontakte Empfehlungen beeinflussen könnten, wenn Social Media Accounts verknüpft werden. Weiter könnten auch Konsumgewohnheiten, die aus Cross-Plattform-Tracking stammen, in Empfehlungen einfließen. Diese Informationen könnten nicht nur genutzt werden, um Empfehlungen auszuspielen, sondern auch um daraus Rückschlüsse auf Gesundheitszustand, Lebensstil oder persönliche Eigenschaften zu ziehen.

Die Informationsfreiheit (Art. 11) könnte durch die accountbasierten Empfehlungsdienste eingeschränkt werden, da diese eine noch personalisiertere, aber damit auch restriktivere Informationsfilterung ermöglichen würden. Anders als bei anonymen Systemen könnten hier langfristige Profile entstehen, die zu verfestigten Ansichten bei Nutzer*innen führen könnten. Außerdem könnten Nutzer*innen potentiell bestimmte Gesundheitsinformationen, Behandlungsansätze oder Präventionsmaßnahmen nicht ausgespielt bekommen, basierend auf Annahmen zu Präferenzen, Bildungsniveau oder ihrer sozioökonomische Situation.

Das Diskriminierungsrisiko (Art. 21) würde sich durch die Möglichkeit verstärken, aus vermeintlich harmlosen Accountdaten sensible Informationen abzuleiten und diese für diskriminierende Empfehlungen zu nutzen. Musikvorlieben und soziale Kontakte aus verknüpften Diensten oder Spracheinstellungen könnten zur Ableitung der sexuellen Orientierung, ethnischen Herkunft oder religiösen Überzeugung verwendet werden, was zu einer gezielten Vorenthaltung oder Bevorzugung bestimmter Gesundheitsangebote führen könnte. Diese Schlussfolgerung persönlicher Eigenschaften wie auch religiöse oder weltanschauliche Präferenzen, die sich aus dem Nutzungsverhalten erschließen lassen, könnte zu entsprechend gefilterten Gesundheitsinformationen führen, wodurch das Recht auf Unversehrtheit (Art. 3) tangiert sein könnte.

Weitere fehlerhafte Empfehlungen bei accountbasierten Systemen könnten zudem besonders gravierende Auswirkungen auf das Recht auf körperliche und geistige Unversehrtheit (Art. 3) haben, da sie auf umfangreichen Datengrundlagen basieren und damit als vertrauenswürdiger wahrgenommen werden könnten. Fehlschlüsse aus der Kombination verschiedener Datenquellen könnten zu inadäquaten

Gesundheitsempfehlungen führen, die aufgrund der scheinbaren Personalisierung befolgt werden würden.

Die Manipulationsgefahr (Art. 38 Verbraucherschutz) könnte sich durch die tieferen Einblicke in persönliche Verhaltensweisen und Präferenzen erheblich verstärken. Recommender Systems könnten unabsichtlich auf emotionale Schwachstellen oder Gesundheitsängste zielen und Nutzer*innen dazu ermutigen, überflüssige Leistungen anzunehmen. Die langfristige Erfassung des Nutzungsverhaltens würde es zudem ermöglichen, optimale Zeitpunkte für manipulative Angebote zu identifizieren.

IT-Sicherheitsrisiken würden bei accountbasierten Systemen ein noch größeres Bedrohungspotenzial für das Recht auf Achtung des Privat- und Familienlebens (Art. 7) darstellen, da die Datenbestände umfangreicher und eindeutig zuordenbar wären. Ein Datenleck könnte nicht nur aktuelle Gesundheitsinformationen preisgeben, sondern auch historische Verhaltensmuster, soziale Kontakte und persönliche Präferenzen offenlegen. Diese "Downstream-Risiken" könnten zu schwerwiegender Diskriminierung führen und die besonderen Schutzrechte vulnerabler Gruppen nach Art. 21 (Nichtdiskriminierung), 23 (Gleichstellung der Geschlechter), 24 (Kinderrechte), 25 (Rechte älterer Menschen) und 26 (Integration von Menschen mit Behinderung) verletzen.

Zusätzlich könnten accountbasierte Recommender Systems das Recht auf Gedanken-, Gewissens- und Religionsfreiheit (Art. 10) durch die permanente Überwachung und Beeinflussung von Überzeugungen und Werthaltungen bedrohen. Die kontinuierliche Profilbildung und personalisierte Nutzung eines Dienstes könnte zu einer schleichenden Verhaltensmodifikation führen. Ferner könnte das Recht auf Bildung (Art. 14) beeinträchtigt werden, wenn Gesundheitsbildung und -aufklärung basierend auf vermeintlichen Fähigkeiten oder Interessenslagen empfohlen wird, was außerdem die Autonomie der Meinungsbildung untergräbe.

2.3 Recommender Systems auf Basis von Profilen

In diesem Kapitel sollen die potentiellen Risiken von Recommender Systems auf Basis von Profilen besprochen werden. Profile sind von Accounts dadurch zu unterscheiden, dass sie von den Datenverarbeitenden und nicht von den Nutzer*innen angelegt und bearbeitet werden. Profile können Interessen enthalten und müssen nicht zwingend einer Person eindeutig zuordenbar sein. Sie sind eher einem Endgerät oder einem Internetzugang auf Grund von Wiedererkennungsmerkmalen zuzuordnen, wie einem Browserfingerprint, Cookies oder anderen Trackingtechnologien.

2.3.1 Werbung

Bei der Ausspielung von Werbung auf Grundlage von Profilen sind ähnliche Risiken denkbar, wie bei der Ausspielung auf Basis von Re-Targeting. Anders als beim Re-Targeting geht es aber nicht darum, gezielt Vorschläge zu wiederholen, sondern Interessen in Kategorien zu erfassen, um so passende Werbung anzeigen zu können.

Das Gefühl, dass in die Privatsphäre eingedrungen wird (Art. 7 EU-GRC), das Risiko, dass ungewollt Produkte gekauft werden (Art. 17 EU-GRC) oder das Risiko einer Ungleichbehandlung (Art. 20 EU-GRC) könnten aber weiterhin bestehen (von Grafenstein, 2025, S. 13)

2.3.2 Kulturbereich

Profilbasierte Recommender Systems im Kunst- und Kulturbereich könnten erhebliche grundrechtliche Risiken bergen, da einige Musikstreamingdienste und Kulturplattformen ausschließlich über solche Profilsysteme funktionieren. Anders als bei accountbasierten Systemen entstehen hier Profile durch die Verknüpfung von Daten verschiedener Endgeräte und Nutzungssessions, ohne dass Nutzer*innen

notwendigerweise explizite Accounts anlegen müssen. Dies könnte besonders problematisch für die Informationsfreiheit nach Art. 11 der EU-Grundrechtecharta sein. Das Finden und Verbreiten von kulturellen Inhalten kann systematisch eingeschränkt werden, wenn profilbasierte Vorschläge bestimmte Kunstformen oder kulturelle Ausdrucksweisen weniger sichtbar machen. Gleichzeitig könnte das Aufdrängen von Inhalten, wie bei Instagram beobachtbar, dazu führen, dass Nutzer*innen gezielt gesuchte kulturelle Inhalte nicht mehr wiederfinden, obwohl diese einmal verfügbar waren.

Die Erinnerung an noch nicht vollständig konsumierte Inhalte, kann die freie Entscheidung über Informationsaufnahme beeinträchtigen und Nutzer*innen in ungewollte Konsummuster kultureller Inhalte drängen. Da Profile über verschiedene Kontexte hinweg verknüpft werden, besteht das Risiko einer intransparenten Form der Kuration der Inhalte, die die Möglichkeit aufweist, das Recht auf informationelle Selbstbestimmung zu untergraben.

Diskriminierungsrisiken in Bezug auf Art. 21 (Nichtdiskriminierung) könnten sich ergeben, wenn profilbasierte Systeme bestimmte Personengruppen systematisch von kulturellen Informationen ausschließen oder ihnen unterschiedliche Inhalte vorspielen. Da Profile und ihre Verknüpfung mit Endgeräten oft auf indirekten Datenspuren und statistischen Korrelationen beruhen, könnten unbewusste Verzerrungen entstehen, die bestimmte demographische, sozioökonomische oder kulturelle Gruppen benachteiligten. Dies wäre besonders problematisch, wenn dadurch der Zugang zu bildungsrelevanten kulturellen Inhalten, subkulturellen Szenen oder künstlerischen Ausdrucksformen eingeschränkt würde.

Die gezielte Ausspielung kultureller Inhalte an bestimmte Personengruppen basierend auf Profildaten könnte Art. 10 (Gedanken-, Gewissens- und Religionsfreiheit) verletzen, insbesondere wenn dabei weltanschauliche oder religiöse Überzeugungen durch kulturelle Inhalte beeinflusst werden sollten. Profilbasierte Systeme könnten beispielsweise Musik, Literatur oder andere Kunstformen mit bestimmten ideologischen Inhalten gezielt an passende Nutzer*innen ausspielen, ohne dass diese um diese Einflussnahme wüssten. Die Subtilität kultureller Beeinflussung könnte dabei problematisch sein, da weltanschauliche Botschaften oft implizit in künstlerischen Werken transportiert werden.

Kommerzielle Manipulationsrisiken könnten Art. 17 (Eigentumsschutz) und Art. 38 (Verbraucherschutz) tangieren, wenn profilbasierte Empfehlungen systematisch zu materiellen Schäden führen. "BookTok"-ähnliche Phänomene, bei denen Empfehlungssysteme aufgrund von Profildaten gezielt zum Bücherkauf oder Abonnement-Abschlüssen animierten, könnten besonders bei vulnerablen Gruppen zu unüberlegten Ausgaben führen. Die profilbasierte Ansprache könnte auf statistischen Vorhersagen über Kaufbereitschaft beruhen und psychologische Schwächen ausnutzen, ohne dass Nutzer*innen die Grundlage dieser Personalisierung durchschauen könnten.

Weitere Risiken könnten die Kunst- und Wissenschaftsfreiheit (Art. 13) betreffen, wenn profilbasierte Empfehlungen zu einer Homogenisierung des kulturellen Angebots führten und experimentelle oder nicht-mainstream-konforme Kunstformen systematisch benachteiligten. Eine Beeinträchtigung des Datenschutzes (Art. 8) und der Privatsphäre (Art. 7) wären durch die intransparente Profilbildung über verschiedene Endgeräte und Kontexte tangiert.

2.3.3 Nachrichtenbereich

Profilbasierte Empfehlungssysteme in digitalen Nachrichtenportalen könnten Risiken für die EU-Grundrechtecharta darstellen, da sie detaillierte individuelle Profile erstellen und auf dieser Basis hochgradig personalisierte Informationsumgebungen schaffen würden. Diese Systeme könnten durch die kontinuierliche Analyse von Nutzungsverhalten, Präferenzen und demografischen Merkmalen individuelle "Informationsblasen" konstruieren, die das Grundrecht auf Informationsfreiheit nach Art. 11 fundamental bedrohen könnten. Jede*r Nutzer*in erhielte eine einzigartige, aber möglicherweise stark begrenzte

Auswahl an Nachrichten, die auf algorithmischen Annahmen über die vermuteten Interessen und Überzeugungen basieren würde. Dies könnte zu einer radikalen Fragmentierung der gemeinsamen Informationsbasis führen, die für demokratische Gesellschaften essentiell wäre.

Die Verletzung des Diskriminierungsschutzes nach Art. 21 wäre bei profilbasierten Systemen ausgeprägt, da diese systematische Vorenthaltung oder gezielte Ausspielung von Informationen an bestimmte Personengruppen ermöglichen könnte. Aufgrund der Empfehlungslogiken könnten Kategorien entstehen, die den Grad an politischem Interesse oder den Bildungsgrad der Nutzer*innen vermeintlich widerspiegeln und entsprechend unterschiedliche Informationsqualitäten ausspielen. So könnten beispielsweise Nutzer*innen mit niedrigerem formalen Bildungsgrad systematisch von komplexer politischer Berichterstattung ausgeschlossen werden.

Besonders problematisch wäre die Gefährdung des Schutzes innerer Überzeugungen nach Art. 10 durch gezielte Beeinflussung. Profilbasierte Systeme könnten nicht nur Filterblasen schaffen, sondern aktiv versuchen, Weltanschauungen zu formen oder zu bestärken. Wenn Empfehlungslogiken so aufgebaut sind, dass häufig Ähnliches vorgeschlagen wird, könnte das dazu führen, dass politische oder soziale Ansichten verstärkt würden. Dies könnte zu einer subtilen, aber wirksamen Manipulation der Meinungsbildung führen, ohne dass Nutzer*innen sich dieser Beeinflussung bewusst wären.

Profilbasierte Systeme könnten zudem das Recht auf Privatleben nach Art. 7 verletzen, indem sie aus scheinbar harmlosen Interaktionen tiefgreifende Rückschlüsse auf politische Einstellungen, religiöse Überzeugungen oder sexuelle Orientierung ziehen würden.

Individualisierte Filterblasen und Echokammern könnten eine Bedrohung für das Demokratieprinzip darstellen, wenn dadurch Ambiguität und Meinungspluralismus nicht mehr als gemeinsame Grundlage betrachtet werden.

2.3.4 Gesundheitsbereich

Profilbasierte Recommender Systems in Gesundheits- und Fitness-Apps könnten durch ihre gerätezentrierte und nutzungsbasierte Logik spezifische Grundrechtsrisiken bergen, die sich von accountbasierten Systemen unterscheiden. Da diese Profile aus der passiven Beobachtung des Nutzungsverhaltens über verschiedene Endgeräte hinweg entstehen würden, könnten sie besonders anfällig für Fehlinterpretationen und ungewollte Diskriminierung sein.

Das Recht auf körperliche und geistige Unversehrtheit (Art. 3) könnte durch fehlerhafte Empfehlungen gefährdet werden, die aus unvollständigen oder missinterpretierten Profildaten resultieren würden. Da profilbasierte Systeme auf statistischen Wahrscheinlichkeiten und Verhaltensmustern basieren würden, könnten sie falsche Rückschlüsse auf den Gesundheitszustand ziehen. Es könnte beispielsweise aus unregelmäßigen Schlafmustern oder veränderten Aktivitätslevels vorschnell auf bestimmte Gesundheitsprobleme schließen und entsprechend ungeeignete Empfehlungen ausspielen, die bei Befolgung gesundheitliche Schäden verursachen könnten.

Diskriminierungsrisiken (Art. 21, 23, 24, 25, 26) könnten entstehen, wenn die Profilbildung ungewollt bestimmte Gruppen benachteiligt. Recommender Systems könnten aus Nutzungsmustern demografische Eigenschaften ableiten und entsprechend unterschiedliche Gesundheitsinformationen oder -empfehlungen bereitstellen. Ältere Nutzer*innen (Art. 25) könnten aufgrund geringerer Interaktionsgeschwindigkeiten mit Online-Diensten automatisch vereinfachte oder weniger umfassende Informationen erhalten oder Kinder und Jugendliche (Art. 24) möglicherweise von wichtigen Präventionsinformationen ausgeschlossen würden, wenn ihr Alter aus dem Nutzungsverhalten falsch eingeschätzt wird. Menschen mit

Behinderungen (Art. 26) könnten durch abweichende Interaktionsmuster als "weniger interessiert" oder "weniger fähig" klassifiziert und entsprechend mit reduzierten Informationsangeboten versorgt werden.

Die Gleichstellung der Geschlechter (Art. 23) könnte durch unbewusste Verzerrungen beeinträchtigt werden, wenn Recommender Systems aus Aktivitätsmustern oder App-Nutzungsverhalten auf das Geschlecht schließen und geschlechtsspezifisch unterschiedliche Gesundheitsinformationen bereitstellen würden. Dies könnte zu einer Verfestigung tradierter Rollenbilder führen, bei der beispielsweise Frauen automatisch mehr Informationen zu Reproduktionsgesundheit angezeigt würden, unabhängig von den tatsächlichen individuellen Bedürfnissen.

IT-Sicherheitsrisiken würden das Recht auf Achtung des Privat- und Familienlebens (Art. 7) bedrohen, da profilbasierte Systeme umfangreiche Verhaltensdaten über verschiedene Endgeräte hinweg sammeln würden. Ein Sicherheitsverstoß könnte nicht nur individuelle Gesundheitsdaten preisgeben, sondern auch Rückschlüsse auf Familienmitglieder und Haushaltsstrukturen ermöglichen. Die geräteübergreifende Profildarstellung könnte private Gewohnheiten, Tagesabläufe und Lebensumstände offenlegen, die weit über die ursprünglich in Gesundheits-Apps eingegebenen Informationen hinausgehen würden.

Der Ausschluss vom Zugang zu Gesundheits-, Pflege- und Sozialleistungen (Art. 34, 35) könnte entstehen, wenn profilbasierte Algorithmen Nutzer*innen fälschlicherweise als "ungeeignet" oder "nicht bedürftig" für bestimmte Angebote einstufen würden. Da diese Systeme auf Verhaltensmustern basieren würden, könnten sie Menschen mit unkonventionellen Lebensrhythmen, seltenen Erkrankungen oder besonderen Lebensumständen systematisch übersehen oder falsch kategorisieren, wodurch ihnen wichtige Gesundheitsinformationen oder Zugang zu Unterstützungsleistungen verwehrt bliebe.

Manipulationsrisiken (Art. 38 Verbraucherschutz) könnten sich durch die kontinuierliche Verhaltensbeobachtung verstärken, da profilbasierte Systeme emotionale oder gesundheitliche Schwachstellen aus Nutzungsmustern ableiten könnten. Es könnten Phasen erhöhter Gesundheitsangst oder Unsicherheit erkannt und diese Zeitpunkte für die Bewerbung kostenpflichtiger Gesundheitsprodukte oder -dienstleistungen genutzt werden. Dies muss nicht unbedingt eine bewusste Geschäftsstrategie sein, sondern könnte als Ergebnis der Optimierung auf Engagement-Metriken entstehen.

2.4 Recommender Systems auf Basis von Kohorten

2.4.1 Werbung

Bei der Personalisierung von Werbung auf Basis von Kohorten sind ähnliche Grundrechtsrisiken wie bei den vorherigen beiden Datenverarbeitungsweisen denkbar (Art. 7, 17 & 20 EU-GRC). Dadurch, dass die Datenbasis hier gröber ist als bei den vorangegangenen Verarbeitungsweisen, ist auch vorstellbar, dass sich die potentiellen Risiken minimieren. Dies hängt damit zusammen, dass die Empfehlungen auf Grundlage statistischer Wahrscheinlichkeiten ausgegeben werden und nicht mehr Profilen oder Accounts mit eindeutigen Interessen zuzuordnen sind. Durch die Ungenauigkeit könnte es aber wiederum zu unpassenden oder unsensiblen Empfehlungen kommen.

2.4.2 Kulturbereich

Kohortenbasierte Recommender Systems auf Musik- und Kulturplattformen bergen grundrechtliche Risiken, die aus der gruppenbezogenen Inhaltskuration resultieren. In solchen Systemen werden Nutzer*innen in demografische, verhaltensbasierte oder interessensspezifische Kohorten eingeteilt und erhalten Empfehlungen basierend auf den Präferenzen ihrer jeweiligen Gruppe. Problematisch wäre hier die mögliche Verletzung der Informationsfreiheit nach Art. 11 der EU-Grundrechtecharta: Wenn Recommender Systems kulturelle Inhalte primär basierend auf Kohortenzugehörigkeit ausspielen,

entstünden systematische Informationsbarrieren zwischen verschiedenen gesellschaftlichen Gruppen. Das Auffinden und Verbreiten von Inhalten könnte eingeschränkt werden, wenn bestimmte kulturelle Ausdrucksformen nur innerhalb spezifischer Kohorten zirkulieren, während andere Gruppen systematisch davon ausgeschlossen blieben.

Die kohortenbasierte Logik könnte zu einer problematischen Segmentierung des kulturellen Raums führen, bei der verschiedene gesellschaftliche Gruppen in separaten Informations- und Kulturräumen gebündelt wären. Musiknachrichten, gesellschaftskritische Filmrezensionen oder politische Botschaften von Autor*innen würden nur innerhalb bestimmter Kohorten verbreitet werden, was demokratische Meinungsbildungsprozesse fragmentiere und die in Art. 2 EU-GRC verankerte Werte der Demokratie und Rechtsstaatlichkeit gefährden könnte.

Schwerwiegende Diskriminierungsrisiken könnten sich aus Art. 21 (Nichtdiskriminierung) ergeben, wenn die Kohortenbildung auf demografischen Merkmalen wie Alter, Geschlecht, ethnischer Herkunft oder sozioökonomischem Status beruht. Bestimmte kulturelle Inhalte, die soziale Teilhabe fördern oder Zugang zu Bildung erleichtern, könnten systematisch nur bestimmten Kohorten zugänglich gemacht werden, was zu struktureller Benachteiligung führen könnte. Die Zuordnung zu Kohorten könnte Stereotypisierung verstärken und bestehende soziale Ungleichheiten perpetuieren.

Die gezielte Ausspielung an bestimmte Kohorten könnte Art. 10 (Gedanken-, Gewissens- und Religionsfreiheit) verletzen, wenn weltanschaulich geprägte kulturelle Inhalte gezielt an empfängliche eingeschätzte Gruppen ausgespielt würden. So wäre eine gruppenbezogene weltanschauliche Manipulation durch Kohorten möglich, die als Proxy für ideologische Vulnerabilität missbraucht würde. Religiöse Musik, politische Liedtexte, ideologisch gefärbte Literatur oder Filme mit weltanschaulichen Bezügen könnten kohortenspezifisch distribuiert werden, um Überzeugungen zu beeinflussen, ohne dass Nutzer*innen von dieser Form der Manipulation wüssten.

Kommerzielle Manipulationsrisiken könnten Art. 17 (Eigentumsschutz) und Art. 38 (Verbraucherschutz) tangieren, wenn kohortenbasierte Empfehlungen systematisch zu materiellen Schäden führen. Empfehlungsmechanismen auf Goodreads oder Letterboxd könnten Gruppendynamiken ausnutzen, um gezielt bestimmte Kohorten zu Abonnementabschlüssen oder Kaufentscheidungen zu bewegen. Besonders jüngere Nutzer*innen-Gruppen wären hier anfällig, da sozialer Druck und Trends innerhalb der Kohorten verstärkt werden könnten.

Die Kunst- und Wissenschaftsfreiheit nach Art. 13 könnte beeinflusst werden, wenn kohortenbasierte Systeme als zentrales Element auf Plattformen wie SoundCloud oder Bandcamp zu einer Fragmentierung der Kulturlandschaft führten. Künstler*innen könnten sich gezwungen fühlen, ihre Werke stärker an spezifische Kohortenerwartungen anzupassen, um Sichtbarkeit zu erlangen. Experimentelle, interdisziplinäre oder kohortenübergreifende Kunstformen würden systematisch benachteiligt sein, da sie nicht in die algorithmischen Kategorisierungen passen. Dies könnte eine Homogenisierung innerhalb der Kohorten und zugleich eine Fragmentierung zwischen den Gruppen begünstigen.

Weitere Risiken könnten sich aus der Verletzung des Rechts auf Privatsphäre (Art. 7) und Datenschutz (Art. 8) ergeben, wenn die Kohortenbildung auf sensiblen persönlichen Daten beruhte, ohne dass Nutzer*innen ausreichend über die Grundlagen ihrer Gruppenzuordnung informiert wären. Schließlich könnte die Menschenwürde (Art. 1) verletzt werden, wenn Nutzer*innen auf ihre Kohortenzugehörigkeit reduziert und ihre Individualität im kulturellen Raum ignoriert würde.

2.4.3 Nachrichtenbereich

Kohortenbasierte Empfehlungssysteme in digitalen Nachrichtenportalen könnten besonders problematische

Risiken für die EU-Grundrechtecharta schaffen, da sie Nutzer*innen in Gruppen mit ähnlichen Merkmalen oder Verhaltensmustern kategorisieren würden. Diese Systeme würden davon ausgehen, dass Personen innerhalb derselben Kohorte ähnliche Informationsbedürfnisse und Präferenzen hätten, was zu einer systematischen Vereinheitlichung der Informationsversorgung ganzer Bevölkerungsgruppen führen könnte. Dies könnte das Grundrecht auf Informationsfreiheit nach Art. 11 erheblich beeinträchtigen, da individuelle Nutzer*innen nicht mehr als autonome Informationssucher*innen behandelt, sondern als Mitglieder vordefinierter Gruppen betrachtet würden, wodurch ihre Chance auf ein vollständiges und vielfältiges Informationsspektrum reduziert werden könnte.

Ebenfalls problematisch wären die Risiken für den Diskriminierungsschutz nach Art. 21. Kohortenbasierte Systeme könnten unbeabsichtigt diskriminierende Profildbildungen verstärken, wenn sie Nutzer*innen basierend auf impliziten Merkmalen wie Alter, Geschlecht, sozioökonomischem Status oder geografischer Herkunft clustern würden. Recommender Systems könnten dabei Annahmen über die Informationsbedürfnisse bestimmter Gruppen treffen, die auf Stereotypen oder historischen Datenverzerrungen basieren. So könnten beispielsweise jüngere Kohorten überwiegend mit Entertainment-News versorgt werden, während ältere Kohorten vorrangig traditionelle politische Berichterstattung angeboten bekämen, wodurch beiden Gruppen wichtige Perspektiven und Informationsbereiche vorenthalten blieben.

Die Gefährdung des Schutzes innerer Überzeugungen nach Art. 10 wäre bei kohortenbasierten Systemen besonders ausgeprägt, da diese Weltanschauungen nicht nur individuell, sondern gruppenweise beeinflusst werden könnten. Wenn Algorithmen davon ausgingen, dass alle Mitglieder einer Kohorte ähnliche politische oder weltanschauliche Präferenzen hätten, könnte dies zu einer Homogenisierung der Meinungen innerhalb dieser Gruppen führen. Abweichende Stimmen oder sich wandelnde Überzeugungen einzelner Nutzer*innen würden möglicherweise nicht erkannt oder berücksichtigt, was zu einer Erstarrung der Meinungslandschaft führen könnte.

Ein spezifisches Risiko läge in der Entstehung intersektionaler Diskriminierung, bei der Nutzer*innen aufgrund mehrerer Gruppenzugehörigkeiten besonders einseitige Informationsversorgung erhalten könnten. So könnten beispielsweise junge Frauen in ländlichen Gebieten eine völlig andere Nachrichtenauswahl erhalten als ältere Männer in städtischen Räumen, wodurch gesellschaftsweite Debatten fragmentiert und der demokratische Diskurs geschwächt werden könnte.

Kohortenbasierte Systeme könnten zudem zu einer problematischen Verstärkung gesellschaftlicher Spaltungen führen. Indem sie ähnliche Nutzer*innen zusammenfassen und ihnen ähnliche Inhalte anbieten würden, könnten sie bestehende soziale, politische oder kulturelle Gräben vertiefen.

Darüber hinaus bestünde das Risiko einer Perpetuierung historischer Ungleichheiten. Wenn kohortenbasierte Systeme auf historischen Daten trainiert würden, könnten sie vergangene Diskriminierungsmuster in die Zukunft übertragen und dabei marginalisierte Gruppen weiterhin benachteiligen. So könnten beispielsweise bestimmte ethnische oder soziale Gruppen systematisch von hochwertiger politischer Berichterstattung ausgeschlossen werden, weil historische Daten suggerierten, dass diese Gruppen weniger Interesse an politischen Inhalten hätten.

Ein weiteres Grundrechtsrisiko läge in der Verletzung der Menschenwürde nach Art. 1 durch die Reduzierung individueller Komplexität auf Gruppenzugehörigkeiten. Menschen würden nicht mehr als einzigartige Individuen mit vielfältigen Interessen und sich wandelnden Präferenzen behandelt, sondern als austauschbare Mitglieder statistischer Kategorien. Dies könnte ihre Autonomie und Würde als freie Meinungsbildner*innen fundamental beeinträchtigen.

Die daraus entstehenden gruppenspezifischen Echokammern und Filterblasen würden eine besonders ernsthafte Gefährdung für das Demokratieprinzip darstellen. Demokratie setzt voraus, dass verschiedene gesellschaftliche Gruppen trotz ihrer Unterschiede auf einer gemeinsamen Faktenbasis diskutieren können. Kohortenbasierte Empfehlungssysteme könnten jedoch dazu führen, dass nicht nur Individuen, sondern ganze Bevölkerungsgruppen in isolierten Informationsräumen leben, wodurch gesellschaftlicher Zusammenhalt und demokratische Kompromissfindung fundamental erschwert würden.

2.4.4 Gesundheitsbereich

Kohortenbasierte Recommender Systems in Gesundheits- und Fitness-Apps könnten durch ihre Gruppenzuordnungslogik besondere Grundrechtsrisiken schaffen, die aus der Kategorisierung von Nutzer*innen in vermeintlich ähnliche Gruppen resultieren könnten. Die scheinbare Anonymität der Kohortenbildung könnte zu subtilen Manipulations- und Diskriminierungseffekten führen.

Manipulationsrisiken (Art. 38 Verbraucherschutz) könnten entstehen, wenn kohortenbasierte Empfehlungen auf vulnerable Gruppen gerichtet sind und diese ausgenutzt würden. Das System könnte beispielsweise Menschen mit chronischen Schmerzen, Angststörungen oder seltenen Erkrankungen in Kohorten zusammenfassen und diesen gezielt teure oder unerprobte Behandlungsalternativen empfehlen, da diese Gruppen aufgrund ihrer Verzweiflung oder ihres Leidensdrucks statistisch eher empfänglich für vermeintliche "Lösungen" wären. Die Kohortenzugehörigkeit könnte dabei als Rechtfertigung für die gezielte Ansprache dienen, ohne dass die individuelle Situation der Betroffenen angemessen berücksichtigt würde.

Der Ausschluss vom Zugang zu Gesundheits-, Pflege- und Sozialleistungen (Art. 34, 35) könnte durch eine rigide Kohortenzuordnung verstärkt werden. Wenn Menschen aufgrund ihrer Symptome oder Verhaltensweisen bestimmten Kohorten zugewiesen werden, könnten sie gleichzeitig von anderen, möglicherweise relevanteren Informationen oder Unterstützungsangeboten ausgeschlossen werden. Eine Person mit Rückenschmerzen könnte beispielsweise ausschließlich orthopädische Empfehlungen erhalten, obwohl die Beschwerden psychosomatische Ursachen haben könnten, für die ganz andere Behandlungsansätze und Sozialleistungen verfügbar wären. Die Kohortenzugehörigkeit würde zu einer einschränkenden Kategorienbildung führen, die den Zugang zu passender Versorgung erschweren könnte.

Weitere Diskriminierungsrisiken könnten sich durch die Kohortenbildung in mehrfacher Hinsicht manifestieren. Das Recht auf Achtung des Privat- und Familienlebens (Art. 7) könnte verletzt werden, wenn aus der Kohortenzugehörigkeit Rückschlüsse auf intime Lebensbereiche wie die sexuelle Orientierung gezogen würden. Beispielsweise könnten Menschen aufgrund bestimmter Suchanfragen zu Symptomen in Kohorten eingeteilt werden, die indirekt auf LGBTQ+-Zugehörigkeit hindeuten, und diese Informationen ungewollt preisgeben oder für weitere Kategorisierungen nutzen.

Das allgemeine Diskriminierungsverbot (Art. 21) könnte durch kohortenbasierte Systeme unterlaufen werden, wenn sie Menschen mit ähnlichen Gesundheitsproblemen ähnliche, möglicherweise eingeschränkte Informationen und Optionen anbieten würden, ohne die dahinterliegenden strukturellen Ursachen zu berücksichtigen.

Die Gleichstellung der Geschlechter (Art. 23) könnte durch geschlechtsspezifische Stereotypisierung beeinträchtigt werden. Personen könnten aufgrund ihrer Geschlechtsidentität trotz identischer Symptome in unterschiedliche Kohorten eingeteilt werden und entsprechend verschiedene Behandlungsempfehlungen ausgespielt bekommen, die gesellschaftliche Vorurteile widerspiegeln. Frauen könnten bei Herzproblemen eher psychosomatische Behandlungen empfohlen werden, während Männern bei denselben Symptomen

schneller kardiologische Untersuchungen vorgeschlagen bekämen.

Kinderrechte (Art. 24) könnten gefährdet werden, wenn kohortenbasierte Systeme Minderjährige aufgrund ihrer Altersgruppe automatisch in restriktive Informationskohorten einordnen würden, die ihnen wichtige gesundheitliche Aufklärung vorenthalten, beispielsweise zur sexuellen Aufklärung. Gleichzeitig könnten die Rechte älterer Menschen (Art. 25) verletzt werden, wenn diese aufgrund ihres Alters in Gruppen mit reduzierten Behandlungsoptionen kategorisiert würden, basierend auf der Annahme, dass bestimmte Therapien für ihre Altersgruppe nicht geeignet seien. Menschen mit Behinderungen (Art. 26) könnten in separate Kohorten mit eingeschränkten Informationsangeboten einsortiert werden, die ihre individuellen Fähigkeiten und Bedürfnisse nicht angemessen berücksichtigen würden.

Fehlerhafte Ergebnisse könnten das Recht auf körperliche und geistige Unversehrtheit (Art. 3) gefährden, wenn die Kohortenzuordnung auf fehlerhaften Annahmen über Gruppenzugehörigkeiten basieren würde. Ein System könnte Menschen mit ähnlichen Symptomen in dieselbe Kohorte einordnen, obwohl die zugrundeliegenden Ursachen völlig unterschiedlich sind, und entsprechend ungeeignete oder sogar schädliche Behandlungsempfehlungen ausspielen. Die scheinbare Validierung durch „andere mit denselben Beschwerden“ könnte Nutzer*innen dazu verleiten, inadäquate Therapieansätze zu verfolgen, die ihrer individuellen Situation nicht entsprechen.

2.5 Recommender Systems auf Basis von Kontexten

2.5.1 Werbung

Für Recommender Systems auf Basis von Kontexten wird vermutet, dass keine Grundrechtsrisiken für Nutzer*innen bestehen, da keine personenbezogenen Daten verarbeitet werden. Dies bedeutet aber nicht, dass sie nicht problematisch sein könnten, da eine Empfehlung aufgrund des sehr groben Kontexts des Inhalts ungenau und unsensibel gegenüber Diskriminierung und persönlichen Triggerpunkten sein kann (von Grafenstein, 2025, S. 14f).

2.5.2 Kulturbereich

Kontextbasierte Recommender Systems auf Musik- und Kulturplattformen wie SoundCloud, Bandcamp, Goodreads oder Letterboxd könnten erhebliche grundrechtliche Risiken bergen, die aus der situativen Inhaltskuration resultieren. Solche Systeme empfehlen, basierend auf dem unmittelbaren Nutzungskontext, etwa abhängig von der soeben gehörten Musik, einem aktuell gelesenen Buch oder den zuletzt bewerteten Filmen. Ein typisches Beispiel wäre eine Literaturplattform, die nach dem Lesen mehrerer Romane eines Genres fast ausschließlich ähnliche Werke empfiehlt, oder ein Musikdienst, der sich ausschließlich an dem gerade gehörten Stil orientiert. Besonders problematisch könnte die Verletzung der Informationsfreiheit nach Art. 11 der EU-Grundrechtecharta sein: Wenn die Auswahl und Gewichtung kultureller Inhalte nach bisherigen Lese-, Hör- oder Sehgewohnheiten erfolgt, könnten Nutzer*innen nur noch basierend auf momentanen Aufmerksamkeits-Mustern Inhalte präsentiert bekommen, anstatt einen Zugang zu einer breiten kulturellen Vielfalt zu erhalten.

Die kontextbasierte Logik könnte zu einer problematischen Verengung des kulturellen Horizonts führen, bei der Nutzer*innen in momentanen Interessen Schleifen gefangen wären. Das Auffinden und Verbreiten neuer Inhalte wird systematisch eingeschränkt, wenn Recommender Systems nur noch kontextuell „passende“ Empfehlungen ausspielen. Musiknachrichten, gesellschaftskritische Essays oder filmische Kommentare können nur dann sichtbar werden, wenn sie in den aktuellen Nutzungskontext passen, was die demokratische Meinungsbildung fragmentieren könnte. Politische oder weltanschauliche Einflussnahme wäre durch kontextbasiertes Targeting eher subtil, da Botschaften im scheinbar passenden

kulturellen Rahmen als authentisch und ungefiltert wahrgenommen würden.

Folgenreiche Auswirkungen könnte es auf die Berufsfreiheit nach Art. 15 und die unternehmerische Freiheit nach Art. 16 geben, insbesondere bei der Ausübung von Kunst als Beruf. Kulturschaffende wären möglicherweise darauf angewiesen, ihre Werke kontextuell „optimiert“ zu gestalten, um in den momentanen Recommender Logiken sichtbar zu bleiben und ihre ökonomischen Ziele zu erreichen. So könnte beispielsweise ein*e Musiker*in auf Bandcamp gezwungen sein, ihre experimentellen Werke an gängige Kontextmuster anzupassen, um überhaupt wahrgenommen zu werden. Dies könnte die künstlerische Ausdrucksfreiheit erheblich einschränken und zu einer Ökonomisierung kreativer Prozesse führen, bei der vor allem „algorithmuskompatible“ Kunst wirtschaftlich überlebensfähig wäre.

Die Kunst- und Wissenschaftsfreiheit nach Art. 13 könnte betroffen sein, wenn kontextbasierte Systeme als zentrales Element auf Plattformen wie Goodreads oder Letterboxd zu einer Trivialisierung kultureller Inhalte führen. Komplexe, vielschichtige oder kontextübergreifende Kunstwerke könnten systematisch benachteiligt sein, da sie nicht in die momentanen Aufmerksamkeitsmuster passen. Die kontextuelle Logik könnte dabei besonders problematisch für experimentelle oder avantgardistische Kunst sein, die oft bewusst Erwartungen durchbricht und neue Kontexte schafft. Kulturelle Bildung und tiefgreifende künstlerische Auseinandersetzung könnten zugunsten oberflächlicher, kontextkonformer Inhalte verdrängt werden.

Kommerzielle Manipulationsrisiken könnten Art. 38 (Verbraucherschutz) betreffen, wenn kontextbasierte Empfehlungen momentane Stimmungen oder Situationen ausnutzen, um Nutzer*innen zu Käufen oder Abonnementabschlüssen zu bewegen. Empfehlungsmechanismen auf Literatur- oder Filmplattformen könnten besonders effektiv sein, wenn sie an den unmittelbaren emotionalen oder situativen Kontext der Nutzer*innen anknüpfen. Die Spontaneität solcher Empfehlungen könnte rationale Kaufentscheidungen untergraben und zu impulsiven Ausgaben führen.

Weitere Risiken könnten die Menschenwürde (Art. 1) betreffen, wenn Nutzer*innen durch kontextbasierte Manipulation zu bloßen Reaktionsobjekten auf situative Reize reduziert werden. Diskriminierungsrisiken nach Art. 21 könnten entstehen, wenn bestimmte Kontexte systematisch mit bestimmten demografischen Gruppen assoziiert und entsprechend unterschiedlich behandelt werden würden. Die Privatsphäre (Art. 7) könnte durch die intensive Überwachung momentaner Nutzungskontexte verletzt sein, insbesondere wenn dabei sensible Rückschlüsse auf emotionale Zustände oder persönliche Situationen gezogen würden.

2.5.3 Nachrichtenbereich

Kontextbasierte Empfehlungssysteme in digitalen Nachrichtenportalen könnten durch ihre Fokussierung auf situative Faktoren spezifische Risiken für die EU-Grundrechtecharta bergen. Diese Systeme würden Inhalte basierend auf Verhaltensmustern wie Klicks, Lesezeiten oder Scrollverhalten auswählen und gewichten, was zu einer schleichenden Beeinflussung der Informationswahrnehmung führen könnte. Wenn Recommender Systems bevorzugt Artikel empfehlen, mit denen Nutzer*innen in der Vergangenheit längere Zeit interagiert haben, könnte dies unbeabsichtigt zu einer Verstärkung bestimmter Themenpräferenzen führen und andere wichtige Informationsbereiche vernachlässigen. Dies könnte das Grundrecht auf Informationsfreiheit (Art. 11) beeinträchtigen, da Nutzer*innen möglicherweise nicht mehr Zugang zu einem vollständigen Spektrum relevanter Nachrichten erhielten.

Besonders problematisch wäre die potenzielle Verletzung des Schutzes innerer Überzeugungen nach Art. 10. Kontextbasierte Systeme könnten durch die kontinuierliche Analyse von Interaktionsmustern subtile Rückschlüsse auf weltanschauliche Präferenzen ziehen und entsprechend angepasste Inhalte liefern. Diese algorithmische Suggestion könnte unbeabsichtigt Weltanschauungen beeinflussen, indem sie bestimmte Denkrichtungen verstärken und andere marginalisieren würde. Den Nutzer*innen wäre dabei

möglicherweise nicht bewusst, dass ihre Informationslandschaft durch vergangenes Verhalten geprägt wird.

Die ortsbezogene Kontextualisierung von Nachrichten könnte zusätzliche Grundrechtsrisiken schaffen. Wenn Systeme Inhalte basierend auf Standortdaten, lokalen Ereignissen oder regionalen Präferenzen auswählen würden, könnte dies zu einer geografischen Fragmentierung der Informationslandschaft führen. Nutzer*innen erhielten möglicherweise überwiegend lokale oder regional gefärbte Perspektiven zu nationalen oder internationalen Themen, was ihre Fähigkeit zur umfassenden politischen Meinungsbildung beeinträchtigen könnte. Dies könnte besonders in strukturschwachen oder politisch polarisierten Regionen problematisch werden, wo eine einseitige Berichterstattung verstärkt werden könnte.

Die ereignisbezogene Kontextualisierung, wie beispielsweise eine prominente Anzeige relevanter Inhalte bei Extremwetter oder sportbezogener News während Großereignissen, könnte zu einer Verzerrung der Nachrichtenagenda führen. Wichtige politische, soziale oder wirtschaftliche Entwicklungen könnten in den Hintergrund gedrängt werden, wenn sie nicht zum aktuellen Kontext passen. Dies könnte die demokratische Funktion der Medien als "Watchdog" untergraben und zu einer partiell uninformierten öffentlichen Debatte führen.

Darüber hinaus bestünde das Risiko einer zeitlichen Diskriminierung im Sinne von Art. 21. Kontextbasierte Systeme könnten unterschiedliche Nutzer*innengruppen systematisch unterschiedlich behandeln, beispielsweise könnten Berufstätige zu bestimmten Tageszeiten andere Inhalte erhalten als andere Bevölkerungsgruppen. Dies könnte zu ungleichen Informationschancen führen und bestimmte gesellschaftliche Gruppen von wichtigen Debatten ausschließen.

Ein weiteres Risiko läge in der Entstehung temporärer Filterblasen durch ereignisbasierte Empfehlungen. Während einer Krise oder eines Großereignisses könnten Nutzer*innen überwiegend mit Inhalten zu diesem spezifischen Thema versorgt werden, wodurch andere wichtige gesellschaftliche Entwicklungen aus dem Blickfeld gerieten. Dies könnte zu einer Tunnelblick-Mentalität führen und die Fähigkeit zur ganzheitlichen gesellschaftlichen Wahrnehmung beeinträchtigen.

Schließlich könnte die Abhängigkeit von Verhaltensdaten zu einer problematischen Selbstverstärkung führen: Nutzer*innen, die aufgrund ihrer Kontextfaktoren bestimmte Inhalte konsumieren, würden zunehmend ähnliche Inhalte empfohlen bekommen, was ihre Informationsvielfalt kontinuierlich reduzieren und ihre autonome Meinungsbildung einschränken könnte. Dies könnte langfristig zu einer Verhärtung gesellschaftlicher Positionen und einer Abnahme des demokratischen Diskurses führen.

2.5.4 Gesundheitsbereich

Kontextbasierte Recommender Systems in Gesundheits- und Fitness-Apps könnten durch ihre situative Empfehlungslogik spezifische Grundrechtsrisiken schaffen, die aus der Verknüpfung aktueller Nutzer*innenaktivitäten mit vermeintlich passenden Folgeangeboten resultieren würden. Die Logik der Empfehlungen könnte auf der Annahme basieren, dass bestimmte Gesundheitssituationen oder Suchanfragen unmittelbar verwandte Bedürfnisse auslösen würden, und entsprechend Empfehlungen ausspielen nach dem Prinzip "da Sie gerade nach X gesucht haben, könnten Sie auch Y benötigen". Die zeitliche und inhaltliche Nähe der Empfehlungen könnte jedoch zu problematischer Beeinflussung führen, da Nutzer*innen in akuten Gesundheitssituationen besonders empfänglich für schnelle Lösungsangebote wären.

Manipulationsrisiken (Art. 38 Verbraucherschutz) könnten vorhanden sein, da kontextbasierte Systeme Menschen in vulnerablen Momenten ansprechen würden. Wenn jemand nach Informationen zu Kopfschmerzen sucht, könnte das System unmittelbar kostenpflichtige Schmerzmittel,

Nahrungsergänzungsmittel oder alternative Heilmethoden bewerben, ohne dass dabei die Angemessenheit oder Notwendigkeit dieser Produkte geprüft würde. Die zeitliche Unmittelbarkeit der Empfehlung würde deren Glaubwürdigkeit erhöhen und Menschen dazu verleiten können, vorschnelle Kaufentscheidungen zu treffen, obwohl möglicherweise einfachere, kostenlose oder besser geeignete Lösungen verfügbar wären. Die Ausnutzung akuter Beschwerden für kommerzielle Zwecke würde dabei nicht aus böswilliger Absicht, sondern aus der Logik der Kontextrelevanz entstehen.

Das Recht auf Informationsfreiheit (Art. 11) könnte durch die kontextuelle Fokussierung beeinträchtigt werden, da die Informationsauswahl auf vermeintlich unmittelbar relevante Inhalte beschränkt wäre. Nutzer*innen könnten durch diese Logik von wichtigen, aber nicht offensichtlich zusammenhängenden Gesundheitsinformationen ferngehalten werden. Bei der Suche nach Hausmitteln gegen Kopfschmerzen könnte das System ausschließlich symptombezogene Empfehlungen ausspielen, aber wichtige Informationen über mögliche Grunderkrankungen, Präventionsmaßnahmen oder professionelle Behandlungsnotwendigkeiten ausblenden. Die kontextuelle Eingrenzung würde zu einer Einengung der Informationsversorgung führen, die das Verständnis für komplexere Gesundheitszusammenhänge außer Acht ließe.

Die kontextbasierte Verknüpfung könnte zudem zu einer problematischen Normalisierung von Selbstmedikation führen, wenn bei jeder Beschwerdesuche unmittelbar entsprechende Behandlungsoptionen vorgeschlagen würden, ohne dass dabei die Notwendigkeit einer professionellen Beratung oder Diagnose thematisiert würde. Dies könnte Menschen dazu ermutigen, ernsthafte Symptome zu bagatellisieren oder wichtige Warnsignale zu übersehen, da Empfehlungen durch ihre unmittelbaren "Lösungsangebote" den Eindruck erwecken würde, dass jedes Gesundheitsproblem durch einfache, direkt verfügbare Mittel behandelbar sei. Dies würde dann das Recht auf körperliche und geistige Unversehrtheit (Art. 3) gefährden. Denkbar ist auch, dass die Verknüpfung verschiedener Gesundheitsthemen zu medizinisch unsinnigen oder kontraproduktiven Empfehlungen führen könnte, beispielsweise wenn bei gleichzeitiger Suche nach Informationen zu verschiedenen Medikamenten Kombinationen vorgeschlagen würden, die zu gefährlichen Wechselwirkungen führen könnten. Die kontextuelle Logik würde dabei nicht die medizinische Sinnhaftigkeit, sondern lediglich die statistische Häufigkeit gemeinsamer Suchanfragen berücksichtigen.

2.6 Sonstige relevante Zwecke

Die häufigsten sonstigen Zwecke der Nutzungsdatenerhebung sind die Gewährleistung der IT-Sicherheit und die Erfassung statistischer Daten zur Verbesserung des Angebots. Da beides als ein berechtigtes Interesse der Betreiber*innen formuliert werden kann, gibt es für Nutzer*innen keine Möglichkeit, sich dieser Datenerhebung zu verweigern. Dies schließt jedoch Grundrechtsrisiken für Nutzer*innen nicht aus.

2.6.1. IT-Sicherheit

2.6.1.1. Werbung

Die für IT-Sicherheit erhobenen Daten könnten mit Werbesystemen kombiniert werden, da beide oft auf denselben technischen Infrastrukturen basieren. IP-Adressen, Geräteinformationen und Verhaltensmuster, die eigentlich der Betrugserkennung dienen, könnten für Werbeprofilbildung missbraucht werden. Dies würde gegen die Zweckbindung verstoßen und das Recht auf Datenschutz (Art. 8) untergraben.

2.6.1.2. Kultur

Die Protokollierung kultureller Nutzungsgewohnheiten könnte Profile über politische Einstellungen,

religiöse Überzeugungen oder sexuelle Orientierung ermöglichen. Welche Filme, Musik oder Literatur jemand konsumiert, verrät viel über eine Person. Dies tangiert die Kunstfreiheit (Art. 13) indirekt, da Nutzer*innen möglicherweise auf kontroverse oder nonkonforme Kulturangebote verzichten, wenn sie Überwachung befürchten. Auch das Recht auf Gedanken-, Gewissens- und Religionsfreiheit (Art. 10) könnte betroffen sein, wenn kulturelle Präferenzen auf weltanschauliche Überzeugungen schließen lassen.

2.6.1.3. Nachrichten

Zugriffsprotokolle auf Nachrichtenportale könnten zur Erstellung detaillierter Profile über politische Interessen, Meinungen und Informationsverhalten genutzt werden. Dies würde die Informationsfreiheit (Art. 11) gefährden, da Nutzer*innen kritische oder kontroverse Nachrichten meiden könnten, wenn ihre Zugriffe nachvollziehbar sind. Für Journalist*innen und deren Quellen entstünden besondere Risiken, wenn Zugriffsmuster Rückschlüsse auf Recherchen oder vertrauliche Kommunikation erlauben. In autoritären Kontexten oder bei staatlichem Zugriff auf Sicherheitsdaten könnten solche Informationen zur politischen Verfolgung genutzt werden. Auch die Pressefreiheit als Teil von Art. 11 wäre tangiert, wenn Mediennutzungsdaten die Anonymität von Leser*innen und Informant*innen gefährden.

2.6.1.4. Gesundheit

Im Bereich der Gesundheit könnte es sein, dass Zugriffsprotokolle auf Gesundheitsportale, medizinische Informationsseiten oder Telemedizin-Dienste sensible Gesundheitsdaten offenbaren, selbst wenn die eigentlichen medizinischen Inhalte geschützt sind. Die bloße Information, wann und wie oft jemand bestimmte Gesundheitsplattformen nutzt, könnte auf Erkrankungen hinweisen. Dies betrifft nicht nur Art. 8 (Datenschutz), sondern auch die Menschenwürde (Art. 1), da Gesundheitsinformationen zum Kernbereich privater Lebensgestaltung gehören. Bei unzureichender Sicherung dieser Zugriffsprotokolle bestünde zudem das Risiko von Diskriminierung durch Arbeitgeber oder Versicherungen.

2.6.2. Performance-Messung und Optimierung

2.6.2.1. Werbung

Die Zweckbindung nach Art. 5 Absatz 1 lit. b DSGVO legt fest, dass personenbezogene Daten nur für festgelegte Zwecke erhoben werden dürfen. Die Daten, die eine Website oder ein Dienst zur Verbesserung des Angebots erhebt, dürfen also nicht für die Ausspielung von Werbung genutzt werden. Sicherlich kann es aber Überschneidungen bei den Daten geben, die für verschiedene Zwecke erhoben wurden. So wie auch hier der Missbrauch und die Missachtung der Zweckbindung nicht ausgeschlossen oder kontrolliert werden kann, liegt es in der Verantwortung der Datenverarbeitenden, Daten nicht für andere Zwecke zu verarbeiten, aus denen sich die vorangegangenen Risiken ergeben könnten.

2.6.2.2. Kultur

Auch die systematische Erhebung von Nutzungsdaten zur Performance-Messung und Optimierung von Inhalten könnte die in der EU-GRC zugesicherten Rechte gefährden. Möglicherweise stünde die Kunstfreiheit nach Art. 13 unter Druck, wenn Reichweitenmessung als Maßstab für die Erstellung von Kunst und Nachrichten angelegt wird. Schaffende könnten ihre Werke dann zunehmend so gestalten, dass diese eher den Nutzenlogiken von Plattformen unterliegen, um beispielsweise möglichst lange Verweildauern auf Plattformen zu generieren und damit die Werbeeinnahmen zu maximieren. Dabei könnte das Risiko bestehen, dass die ursprüngliche künstlerische Vision verloren geht. Besonders prekär wäre diese Situation für Newcomer*innen, die auf Sichtbarkeit angewiesen sind und sich dem Druck der Anpassung an die Logiken der Vorschlagssysteme schwer widersetzen könnten.

2.6.2.3. Nachrichten

Ebenso betroffen wäre die Nachrichtenproduktion. Journalist*innen könnten bewusst oder unbewusst verleitet werden, Inhalte nach Engagement-Metriken statt nach journalistischer Relevanz auszurichten. Unlukrative, aber gesellschaftlich wichtige Nachrichten blieben womöglich ungeteilt oder würden gar nicht erst publiziert. Dies würde die Informationsfreiheit nach Art. 11 der Grundrechtecharta untergraben. Für Nutzer*innen bestünde das Risiko, einem zunehmenden Konformismus gegenüber Logiken ausgesetzt zu sein, in denen nur noch reichweitenoptimierte, aber inhaltlich unterkomplexe oder polarisierende Kultur- und Nachrichtenangebote präsent wären. Die Optimierung anhand von Performance-Messung könnte somit die Vielfalt künstlerischen Ausdrucks und den freien Informationszugang erheblich einschränken.

2.6.2.2. Gesundheitsbereich

Datenerhebung zur Optimierung und Performance-Messung in Gesundheits- und Fitness-Apps könnte Grundrechtsrisiken schaffen, die aus der kontinuierlichen Überwachung und Bewertung menschlichen Verhaltens resultieren würden. Wenn diese Systeme darauf abzielen, die App-Performance, Nutzer*innenengagement und Geschäftsergebnisse zu optimieren, könnten Gesundheitsdaten zur Effizienzsteigerung instrumentalisiert werden. Die scheinbar technische Notwendigkeit der Performance-Optimierung könnte dabei Grundrechtsrisiken schaffen, ohne dass das Ziel der Datenverarbeitung erkennbar wäre.

Manipulationsrisiken (Art. 38 Verbraucherschutz) könnten entstehen, wenn die zur Performance-Messung gesammelten Daten dazu verwendet würden, Nutzungsverhalten zu analysieren und entsprechend manipulative Strategien zu entwickeln. Beispielsweise könnte analysiert werden, zu welchen Tageszeiten Menschen besonders empfänglich für Gesundheitsprodukte sind, welche emotionalen Zustände zu impulsiven Kaufentscheidungen führen oder welche Formulierungen bei bestimmten Gesundheitsproblemen am wirksamsten sind. Diese Erkenntnisse könnten dann zur Optimierung von Verkaufsstrategien genutzt werden, die auf psychologische Schwachstellen abzielen, ohne dass Nutzer*innen sich der Manipulation bewusst wären.

Das Recht auf Achtung des Privat- und Familienlebens (Art. 7) könnte durch IT-Sicherheitsrisiken bedroht werden, die aus der Datensammlung für Optimierungszwecke resultieren würden. Die erhobenen Daten, durch die sich Rückschlüsse auf Gesundheitsgewohnheiten, Tagesabläufe, emotionale Zustände und persönliche Schwächen ziehen ließe, könnten bei Sicherheitsverletzungen Schaden anrichten. Die Zweckentfremdung durch missbräuchliche Nutzungen könnte zu Diskriminierung, Erpressung oder sozialer Stigmatisierung führen, da die Optimierungsdaten intimere Einblicke in das Privatleben gewähren könnten als die ursprünglich für Gesundheitszwecke erhobenen Informationen.

Darüber hinaus könnte die Optimierung auf Engagement und Nutzungszeit zu einer problematischen Verstärkung gesundheitsschädlicher Verhaltensweisen führen. Wenn Systeme darauf optimiert würden, möglichst viel Zeit in der App zu verbringen, könnten sie unbeabsichtigt Angststörungen, Hypochondrie oder zwanghafte Selbstüberwachung fördern. Die Performance-Messung könnte zeigen, dass Menschen mit Gesundheitsängsten besonders lange und häufige Nutzungszeiten aufweisen, was dann zur weiteren Verstärkung dieser Verhaltensmuster genutzt werden könnte, ohne dass dies als Gesundheitsschädigung erkannt würde. Dies beträfe dann erneut Art. 3, das Recht auf körperliche und geistige Unversehrtheit.

3 ZUSAMMENFASSUNG UND AUSBLICK AUF SUBJEKTIVE RISIKEN

In der Betrachtung der verschiedenen Verarbeitungszwecke lassen sich einige Gemeinsamkeiten finden. Diese bestehen vor allem darin, dass für die verschiedenen Recommender Systems auf Basis von Re-Targeting, Accounts, Profilen und Kohorten größtenteils die gleichen Risiken denkbar sind. Da die Datenverarbeitungsweisen aber in ihrer Funktion und ihren Ergebnissen sukzessive gröber werden und weniger personenbezogene Daten verwenden, könnte es sein, dass sich auch die Qualität oder Intensität der Risiken minimiert. Wenn die Ergebnisse der Empfehlungssysteme unzutreffender werden, ist davon auszugehen, dass z.B. Kaufentscheidungen eher nicht getroffen werden, Personen sich nicht verfolgt fühlen oder eine Ungleichbehandlung seltener stattfindet.

Unabhängig davon, ob Re-Targeting, account-, profil-, kohorten- oder kontextbasierte Empfehlungen zum Einsatz kommen, drohen Manipulationsrisiken (Art. 38), die Beeinträchtigung der Informationsfreiheit sowie die Gefährdung der körperlichen Unversehrtheit durch fehlerhafte Empfehlungen (Art. 3). Ebenso ziehen sich IT-Sicherheitsrisiken und damit verbundene Privatsphäreverletzungen (Art. 7) als Querschnittsthema durch alle Verarbeitungszwecke beziehungsweise ihre Verarbeitungsweisen, wobei das Ausmaß mit dem Detailgrad der jeweiligen Methode variiert.

Die wesentlichen Unterschiede liegen in der Art und Tiefe der Grundrechtsbeeinträchtigung. Accountbasierte Systeme ermöglichen die umfassendste Personalisierung und schaffen daher die intensivsten Profile mit entsprechend höherem Diskriminierungspotenzial, während profilbasierte Ansätze durch ihre geräte- statt personenzentrierte Logik eher anfällig für Fehlinterpretationen sind. Kohortenbasierte Recommender Systems könnten die spezifische Gefahr der falschen Einordnung in Kategorien und der Reproduktion gesellschaftlicher Ungleichheiten bergen, da sie strukturelle Diskriminierungsmuster verfestigen können. Kontextbasierte Systeme unterscheiden sich fundamental durch ihre zeitliche Unmittelbarkeit, die Menschen in vulnerablen Momenten ansprechen könnte und gleichzeitig durch ihren begrenzten Fokus nur einen Tunnelblick an Informationen darstellt.

Eine Lücke in der Betrachtung, wie wir sie vorgenommen haben, ist die Kombination verschiedener Typen von Recommender Systems, die auch parallel eingesetzt werden könnten. Die Wechselwirkungen zwischen den verschiedenen Logiken könnten Grundrechtsrisiken potenzieren oder neue Gefährdungslagen schaffen, die sich nicht aus der isolierten Betrachtung einzelner Systeme ergeben. Zwar gilt das Prinzip der Zweckbindung, jedoch ist durch die Überschneidung der Zwecke und der erhobenen Daten und das Einwilligen in mehrere Verarbeitungszwecke eine Kombination theoretisch möglich. Des Weiteren fehlt eine systematische Analyse der zeitlichen Dimension. Während kurzfristige Manipulationseffekte im Vordergrund stehen, könnten auch langfristige Auswirkungen wie die graduelle Verhaltensmodifikation, die Normalisierung von Überwachung oder die gesellschaftliche Akzeptanzverschiebung bezüglich digitaler Angebote relevant sein oder werden. Schließlich ist die Frage der Reversibilität von Grundrechtseingriffen eine offene Frage: Einmal erstellte Profile, etablierte Diskriminierungsmuster oder verfestigte Sichtweisen lassen sich möglicherweise nicht einfach rückgängig machen, selbst wenn die Datenverarbeitung beendet wird.

Der Missbrauch und die Missachtung der Zweckbindung sind Aspekte, die sich nicht verhindern oder umfassend kontrollieren lassen. Diese Abwägung zwischen Risiken und Vorteilen wurde auch in unserer eingangs erwähnten Untersuchung zu subjektiven Risikomodellen von Expert*innen und Nutzer*innen deutlich. Schließlich muss auch mit einem gewissen Restrisiko gelebt werden, so wie in vielen Gesellschaftsbereichen. Regeln für den Straßenverkehr schließen Unfälle nicht aus, ebenso wie bei medizinischen Routineeingriffen immer mit Komplikationen gerechnet werden muss.

4 LITERATURVERZEICHNIS

Lancieri, Narrowing Data Protection's Enforcement Gap, MLR 2022, S. 31 ff.

Lukat, M., Sayman, V., Guagnin, D., & Pohle, J. (2025). Zwischen Bauchgefühl und Fachwissen: Risiken personalisierter Werbung im Internet. Eine Annäherung aus Sicht von Nutzer*innen und Expert*innen. In: HIIG Discussion Paper Series 2025-03. Alexander von Humboldt Institut für Internet und Gesellschaft, Berlin. DOI: 10.5281/zenodo.16651959

Margaritis, (2023). Online Behavioral Advertising as an Aggressive Commercial Practice, EuCML 2023, S. 244;

von Grafenstein, M. (2025). Rechtswissenschaftliche Studie zu verarbeitungszweckspezifischen Grundrechtsrisiken im Bereich von personalisierter Werbung und personalisierter Inhalte im Internet. In: HIIG Discussion Paper Series 2025-04. Alexander von Humboldt Institut für Internet und Gesellschaft, Berlin. DOI: 10.2139/ssrn.5375301