CBS COPENHAGEN BUSINESS SCHOOL
HANDELSHØJSKOLEN

Algorithmen und Verbraucher

Reisch, Lucia A.; Bietz, Sabine; Micklitz, Hans-W.

Document Version
Final published version

Publication date:
2020

License
Unspecified

Citation for published version (APA):
Reisch, L. A., Bietz, S., & Micklitz, H.-W. (2020). *Algorithmen und Verbraucher*. Zeppelin Universität. https://www.zu.de/forschung-themen/forschungszentren/konsum/news/algorithmen-verbraucher.php

Link to publication in CBS Research Portal

General rights
Copyright and moral rights for the publications made accessible in the public portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.

Take down policy
If you believe that this document breaches copyright please contact us (research.lib@cbs.dk) providing details, and we will remove access to the work immediately and investigate your claim.

Download date: 04. Jul. 2025

zeppelin universität

zwischen
Wirtschaft Kultur Politik

Algorithmen und Verbraucher

Eine Studie im Auftrag des Ministeriums für Ländlichen Raum und Verbraucherschutz (MLR) Baden-Württemberg, Stuttgart

Prof. Dr. Lucia Reisch
Dipl. oec. soc. Sabine Bietz
Prof. Dr. Hans-W. Micklitz

Impressum

1. Auflage August 2020
Herausgeber: Forschungszentrum Verbraucher, Markt und Politik | CCMP

Zeppelin Universität gemeinnützige GmbH
Forschungszentrum Verbraucher, Markt und Politik
Am Seemooser Horn 20
D-88045 Friedrichshafen

Zitiervorschlag: Reisch, Lucia A., Bietz, Sabine & Micklitz Hans-W. (2020). Algorithmen und Verbraucher. Eine Studie im Auftrag des Ministeriums für Ländlichen Raum und Verbraucherschutz (MLR) Baden-Württemberg, Stuttgart. Friedrichshafen: Forschungszentrum Verbraucher, Markt und Politik | CCMP (Hrsg.).

Wir haben uns um geschlechterneutrale Sprache bemüht. Allerdings wird in dieser Studie aus Gründen der in deutschen Gesetzestexten üblichen Praxis (vor allem in den verbraucherrechtlichen Teilen) das generische Maskulinum verwendet. Weibliche und anderweitige Geschlechteridentitäten sind dabei ausdrücklich mitgemeint.

Titelfoto von ThisisEngineering RAEng via Unsplash

Inhalt

Abkürzungsverzeichnis

Allgemeine Geschäftsbedingungen ..... *AGB*
Allgemeines Gleichbehandlungsgesetz ..... *AGG*
Augmented Reality ..... *AR*
Baden-Württemberg ..... *BW*
Bundesamt für Sicherheit in der Informationstechnik ..... *BSI*
Bundesdatenschutzgesetz ..... *BDSG*
Bundesgerichtshof ..... *BGH*
Bundesministerium der Justiz und für Verbraucherschutz ..... *BMJV*
Bundesverfassungsgericht ..... *BVerfG*
Datenschutzgrundverordnung ..... *DSGVO*
EU-Richtlinie über unlautere Geschäftspraktiken ..... *UGP*
Europäische Union ..... *EU*
Europäischer Gerichtshof ..... *EuGH*
Forschungszentrum Verbraucher, Markt und Politik ..... *See* CCMP
Gesetz gegen Unlauteren Wettbewerb ..... *UWG*
Künstliche Intelligenz ..... *KI*
Maschinelles Lernen ..... *ML*
Preisangabenverordnung ..... *PAngV*
Quantified Self ..... *QS*
Rechtsdienstleistungsgesetz ..... *RDG*
Sachverständigenrat für Verbrauchfragen ..... *SVRV*
Schlichtungsstelle für den öffentlichen Personenverkehr ..... *SÖP*
Verbraucherzentrale ..... *VZ*
Versicherungsaufsichtsrecht ..... *VAG*
Virtual Reality ..... *VR*

Zu dieser Studie

Im Netz und zunehmend auch im stationären Einzelhandel hinterlassene Datenspuren machen Verbraucherinnen und Verbraucher zum gläsernen Konsumenten. Gleichzeitig fällen Computer – eigentlich: algorithmische Systeme – zunehmend Entscheidungen, die tief in unser Leben als Verbraucher und Bürger eingreifen. Datengetriebene Geschäftsmodelle, basierend auf Künstlicher Intelligenz (KI) und Maschinellem Lernen (ML), oft marktmächtiger Internetunternehmen führen zu nahezu ungebremster Sammlung, Speicherung und Auswertung personenspezifischer Daten. Verbraucher tappen laufend in die „Bequemlichkeitsfalle“ und nehmen für kleine Gewinne an Zeit und Bequemlichkeit langfristig erhebliche Datenrisiken in Kauf und vernachlässigen die Sicherheit beim Surfen und generell im Umgang mit „smarten“ Geräten, wie Chatbots und Sprachassistenten oder Smart Home Anwendungen. In Sozialen Netzwerken und über mobile Endgeräte wie Handys, aber auch Wearables zum Self-Tracking, hinterlassen Nutzer eine Vielfalt von Bewegungs-, Meinungs- und Interessendaten und geben auch ihr reales Beziehungsnetzwerk und Privatleben preis. Datenmissbrauch bis zum Identitätsdiebstahl und nahezu perfekte Profilierung zu Werbe- und politischen Meinungszwecken können eine Folge sein.

Telematiktarife und KI-basierte Verbraucher-Scores können Verbraucher preisliche Vorteile und Zugang zu Leistungen erbringen, haben jedoch eine Reihe von Risiken, die nicht alle Verbraucher kennen oder auch sehen wollen. Das gleiche gilt für dynamische und personalisierte Preise. Den meisten ist nicht bewusst, wie geschickt das Design von Websites beim Online-Shopping unser Nutzerverhalten durch sogenannte Dark Patterns manipuliert, etwa um Daten herauszugeben oder Zustimmung zu Allgemeinen Geschäftsbedingungen (AGB) zu erhalten. Die Möglichkeit der nahezu perfekten „Immersion“ durch Virtuelle und Erweiterte Realität (wie etwa bei den Google Glasses) lässt uns virtuelle Welten sehr real erscheinen und erleben; dies kann sowohl im Verbraucherinteresse genutzt (etwa bei der Verbraucher- oder Umweltbildung), aber auch zu Manipulationszwecken missbraucht werden.

Algorithmische Systeme sind aber zuerst einmal neutral. Und sie haben durchaus ein großes – und wie wir meinen, unterschätztes – Potential, im Interesse der Verbraucher eingesetzt zu werden. Wie wir im Rahmen des letztjährigen Verbraucherforschungsforum 2019 in Stuttgart zeigen konnten, gibt es im Bereich der Vrebraucherinformatik und des LegalTech vielversprechende Anfänge Algorithmen basierter Verbraucher-Informationssysteme. Beispiele sind KI-basierte Systeme, die verbrauchergerechte AGB oder „gute“ Datenschutzregeln eines Online-Shops in Form einer Ampel anzeigen. Sie sind sehr wertvoll für die Entscheidungsunterstützung, gerade wenn es um gewichtige Entscheidungen wie Kreditvergaben oder Behandlungsmethoden im Gesundheitsbereich geht. Denn sie sind (wenn sie gut und vorurteilsfrei trainiert wurden) unabhängig von Zufallseinflüssen („Noise“) und unbestechlich. Im Gesundheits- und Präventionsbereich wäre ohne Algorithmen auch keine Corona-App möglich, die trotz aller Datenschutzbedenken ein wichtiges Element der Pandemiekontrolle zu werden verspricht.

Die deutsche (und europäische) Daten- und Verbraucherpolitik ist auf dem Weg, sich nach und nach dieser Themen anzunehmen und den Einsatz von Algorithmen jeweils auf Sicherheit, Fairness und Verbrauchergerechtigkeit zu prüfen sowie Kriterien für eine „Ethische KI“ zu entwickeln. Die Datenethikkommission der Bundesregierung, die Enquetekommission „Künstliche Intelligenz“ des Bundestags, der Sachverständigenrat Verbraucherfragen des Bundesministeriums der Justiz und für Verbraucherschutz (BMJV), die Verbraucherkommission Baden-Württemberg sowie die Verbraucherzentralen und ihre Marktwächter Digitale Welt – um nur einige zu nennen – liefern Vorschläge für eine solche Ausgestaltung, die die Politik aber bislang noch nicht wirklich erreicht haben. Das vorliegende Booklet kann dies nicht umfänglich darstellen, fokussiert jedoch auf die jeweiligen Kernpunkte.

Zu dieser Studie

Die Verbraucherpolitik in Baden-Württemberg (BW) startete zum Verbrauchertag BW im Oktober 2019 die umfangreiche Informations- und Bildungskampagne „#seiunberechenbar - Verbraucher und Algorithmen“. Die Kampagne nutzt diverse Formate und Medien und hat eine umfassende Homepage erstellt mit Videoclips und Erklärtexten zu Themen rund um Algorithmen.

Das Forschungszentrum Verbraucher, Mark und Politik (CCMP) hat diese Kampagne von Anfang an begleitet. Das vorliegende Booklet greift einige der wichtigsten der vergangenen und laufenden Kampagnenthemen auf und unterfüttert sie mit Studien und Berichten aus Forschung und Praxis. Dabei geht es nicht um eine vollständige Literaturübersicht oder Rechtsanalyse. Vielmehr sollen in kampagnenadäquaten kompakten Themensteckbriefen die wichtigsten Fragen zum Thema jeweils beantwortet werden:

- Was steckt genau hinter dem jeweiligen Stichwort und welche Rolle spielen Algorithmen in der praktischen Anwendung? Was sind die Anwendungsfelder; gibt es bekannte Beispiele?
- Welche Chancen und welche Risiken gibt es für die Verbraucherinnen und Verbraucher? Welche sind schon jetzt nachweisbar, welche eher möglich, aber (noch) nicht relevant?
- Welche Herausforderungen stellen diese Algorithmen basierten Anwendungen an die Verbraucherpolitik als Daten- und Digitalpolitik? Welche verbraucherpolitischen Optionen werden diskutiert oder sind bereits in Vorbereitung?
- Welche rechtlichen Grundlagen liegen dem Thema zugrunde? Was ist rechtlich erlaubt, was nicht? Wie weit ist das Recht überhaupt auf die Herausforderungen der digitalen Welt eingestellt? Welche Regulierungsmaßnahmen sind in der Diskussion?
- Was können Verbraucherinnen und Verbraucher jetzt schon tun? Wie können sie ihre digitale Souveränität entfalten, damit sie die Vorteile der Algorithmen basierten Anwendung mitnehmen, die Nachteile aber begrenzen können?

An dieser Stelle sei auch ein wichtiger Hinweis zum Verbraucherrecht erlaubt: In nahezu allen hier relevanten Bereichen des Verbraucherrechts – dem Vertragsrecht, der AGB-Kontrolle, dem Lauterkeitsrecht, aber auch im Datenschutzrecht und bei der Regelung des e-Commerce und der Plattformen – ist die Europäische Union (EU) der Taktgeber. Soweit das Recht der EU Sachverhalte abschließend regelt (d.h. vollständig harmonisiert), liegt die Auslegungshoheit für die Interpretation des Unionsrechts bei dem Europäischen Gerichtshof. Deshalb reicht es nicht, allein auf die deutschen Regeln zu achten, mittels derer die Vorgaben des Unionsrechts umgesetzt werden.

Für das vorliegende E-Booklet haben wir 13 Themensteckbriefe erstellt. Die Liste ist jederzeit erweiterbar und neue Themen entstehen laufend. Die Texte sind bewusst so geschrieben, dass sie Verbraucherinnen und Verbraucher ansprechen – und kein Fachpublikum. Gleichzeitig basieren sie auf wissenschaftlichen Studien, die beispielhaft auch genannt werden.

Das Booklet ist das Ergebnis von Teamwork: Unser Dank geht an das (ehemalige und aktuelle) Team des CCMP an der Zeppelin Universität Friedrichshafen: Ass. Prof. Dr. Micha Kaiser, der uns im Bereich KI und Algorithmen beraten hat; Manuela Bernauer, M.A. und Tilman Knop, B.A., die hervorragende Recherchearbeit geleistet haben; und Noah Peters, B.A., der die finale Durchsicht und ansprechende Darstellung wie immer zuverlässig übernommen hat.

Friedrichshafen, Kopenhagen, Berlin, im August 2020

Lucia A. Reisch

Sabine Bietz

Hans-W. Micklitz

Chatbots und Sprachassistenten

Was sind Chatbots?

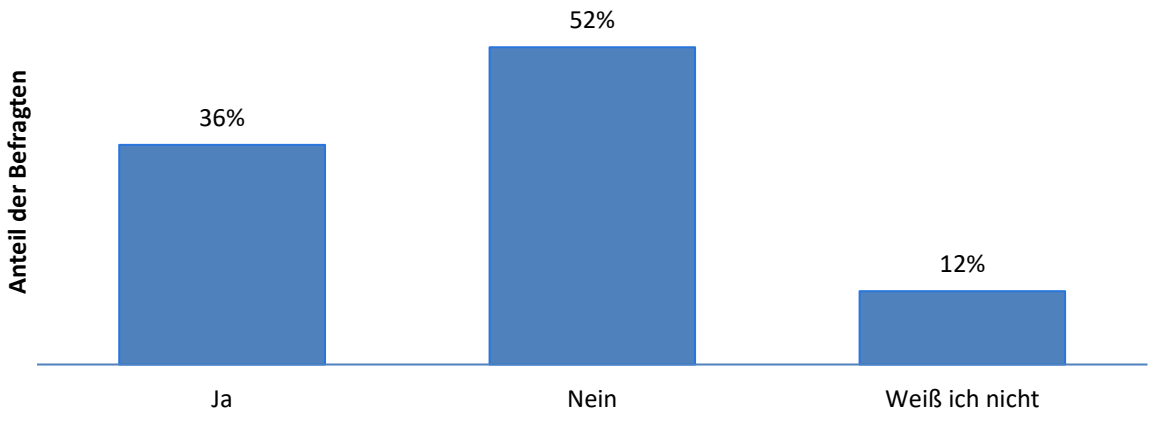
Das Wort ‚Bot' ist die Abkürzung für Roboter und meint „[...] Programme, die autonom mit Systemen oder Nutzern interagieren" (Hoffmann 2019, S. 19). Verbraucher treffen auf diese kleinen **Mini-Roboter** überall im Netz, häufig mit einer eigenen „Identität" – denn Menschen fällt es leichter, mit Personen zu kommunizieren als mit abstrakten Programmen. Der erste Chatbot war wohl das Programm ELIZA, das bereits 1966 am MIT entwickelt wurde und eine Psychotherapeutin nachahmt. Durch die rasanten Technologiesprünge der vergangenen Jahrzehnte ist die Entwicklung künstlicher Intelligenz erheblich vorangeschritten und damit die Anwendung, u.a. in Bots und vor allem Sprachassistenten.

Grundsätzlich ist ein Chatbot ein **Computersystem/-programm**, das die Kommunikation mit einem Menschen erlaubt, beispielsweise über einen Messenger Dienst, einen Browser oder eine App. Sie werden zumeist im Bereich der Kundenkommunikation eingesetzt, um Fragen in einem bestimmten thematischen Bereich zu beantworten. Diese **virtuellen Sprachassistenten** sind auf einer Datenbank aufgebaut, die Satzbausteine einordnen und verarbeiten kann, sowie eine entsprechende Reaktion auf die Frage bzw. inhaltlichen Input formuliert. Das Programm baut in der Regel auf einer Künstlichen Intelligenz (KI) auf, die sich durch gestellte Fragen und Antworten laufend weiterentwickelt.

Klassische Chatbots sind schriftliche **Messenger Applikationen**, die bereits in zahlreichen Bereichen von Unternehmen sowie zunehmend auch im öffentlichen Sektor verwendet werden. Häufig kommen diese Chat-Anwendungen bei einfachen Kundenanfragen zum Einsatz. Eine vergleichsweise neuere Entwicklung sind komplexere **Sprachassistenten**, die auch in natürlicher Sprache kommunizieren. Bekannte Beispiele für diese Kategorie sind der Google Assistant oder Amazons Alexa. Die Tech-Branche erwartet, dass die Anwendungsbreite und der Einfluss von Chatbots bald ähnlich groß sein wird wie die von Apps; die jetzige Verbreitung stellt wohl nur den Anfang einer bedeutenden technologischen Veränderung dar.

Hatten Sie schon einmal wissentlich Kontakt mit einem Chatbot?

Umfrage zur wissentlichen Nutzung von Chatbots in Deutschland 2019



Hinweise: Deutschland; 18.12.2019 bis 20.12.2019; 18-64 Jahre; 1.076 Online-Käufer
Quelle: idealo (2020, S. 18); verfügbar über Statista (ID 801513)

Anwendungsfelder

Verbraucherfreundliche Anwendungsfelder von Chatbots liegen u.a. in der öffentlichen Verwaltung und dort in der **Verbraucher- und Bürgerkommunikation**. So nutzt die Stadt Bonn einen Chatbot für einfache Anfragen (siehe Bild). Auch während der Corona-Pandemie finden Chatbots eine Anwendung. Im Rahmen des offiziellen Hackathon der Bundesregierung wurde im März 2020 auch der **Corona Legal Chatbot** ins Leben gerufen. Dieser sollte bei rechtlichen Fragen, die im Zusammenhang mit der Pandemie stehen, weiterhelfen (www.coronalegalchatbot.de[1]).

Auch Verbraucherzentralen können Chatbots für ihre Beratung nutzen. Verbraucher könnten vor dem eigentlichen Beratungstermin mit dem Chatbot kommunizieren und relevanten Daten für die Beratung bereitstellen. Hierdurch könnte die Beratungszeit verkürzt und die Beratungsleistung kosteneffizienter werden. Die Verbraucherzentale Hessen (23. April 2019) sieht solche nicht-menschlichen Berater als besonders hilfreich an: „Der **Verbraucherzentralen-Chatbot** wäre einer, der uns in besonderem Maß dabei hilft, diese kognitiven Vorurteile zu vermeiden. Sie könnten helfen, die Anzahl der Entscheidungen zu senken, die objektiv nicht in unserem Sinn gewesen wären." Besonders wenn es um Haftungsfragen geht, gibt es jedoch noch viele offene Fragen; ein großer Teil des Datenrechts ist noch in der Entwicklungsphase.

Herausforderungen

Wie alle auf Big Data beruhenden Anwendungen haben auch Chatbots erhebliche **Datenschutzrisiken**. Gleichzeitig kann ein Chatbot nur so gut sein, wie der zugrundeliegende **Algorithmus** und die für das Training verfügbaren **Daten**. Letztere sind meist unvollständig, ersterer abhängig von den Zielen und dem Können seiner Programmierer. Ein negatives Beispiel war ein Chatbot, der auf der Interaktion mit Twitter-Nutzern aufbaute. Da Nutzer diesem Chatbot absichtlich Fehlverhalten ‚anlernten', begann der Chatbot, andere Nutzer des Netzwerkes zu beleidigen. Dies zeigt, dass Chatbots zwar effektiv aus Interaktionen lernen können, diese jedoch gewisse Sicherheitsschranken benötigen, damit Missbrauch verhindert werden kann. Natürlich können Chatbots auch vorsätzlich dazu genutzt werden, unmoralische oder illegale Zwecke zu verfolgen, beispielsweise ohne Zustimmung persönliche Daten von Nutzern abzugreifen.

Für den Menschen ist eine Unterscheidung manchmal kaum ersichtlich, da die Programme mit einem eigenen Online-Profil mit ihrem digitalen Gegenüber interagieren, fast ganz so wie eine echte Person. Damit können sich Bots eine Glaubwürdigkeit erschleichen, die sie nicht immer haben. Je nach Einsatzgebiet kann dies zu mehr oder weniger problematischen Konsequenzen führen. Aus ethischen Gründen sollte es Nutzern deutlich sein, dass es sich beim Gesprächspartner um einen Roboter handelt.

Während Chatbots in der Regel nur passiv auf eine Anfrage reagieren, verbreiten sogenannte **Social Bots** Inhalte aktiv. Social Bots arbeiten von Accounts in Sozialen Netzwerken: sie teilen Postings, liken oder kommentieren. Das Risiko liegt vor allem darin, dass sie als vermeintliche (glaubwürdige)

[1] Zur Zeit der Studienabgabe nicht erreichbar, soll aber weitergeführt werden.

Individuen auf Social Media Plattformen agieren. Berüchtigt und für eine freiheitliche Demokratie gefährlich sind Hashtags oder gezielte Aussagen von Chatbots in Sozialen Medien, die die Einstellung von Bürgerinnen und Bürgern – und damit Wahlen – beeinflussen. In zahlreichen Beispielen wurden Social Bots benützt, um Gerüchten oder verschwörungstheoretischen Inhalten eine höhere Reichweite zu verschaffen. Andere Risiken bergen Bots, die es im Rahmen von Pandemien oder anderen Krisen darauf anlegen, die staatliche Kommunikation in Misskredit zu bringen und Bürger zu verwirren. Schließlich können Bots auch von Kriminellen missbraucht werden, etwa wenn ein Bot mit einem gestohlenen Profil Kontaktanfragen versendet, um das Vertrauen des Opfers zu erlangen. Bösartige Social Bots verschicken massenweise Links zu schadhaften Webseiten, um Viren zu verbreiten.

Für Verbraucher wird es immer schwieriger werden, die Interaktion mit Chatbots von denen mit Menschen zu unterscheiden. Gleichzeitig werden die Relevanz und Verbreitung von Bots in der Kundenkommunikation weiter zunehmen. Heute sind der Anwendung von Bots durch die Datenschutzgrundverordnung (DSGVO) erhebliche Grenzen gesetzt. Denn die Algorithmen der Bots sind auf (viele, zugängliche) Daten angewiesen. Wenn aufgrund einer strikten Datenschutzregelung bestimmte Daten nicht zum **Training** des Algorithmus eingesetzt werden dürfen, werden solche Variablen später auch nicht erkannt.

Auch die begrenzte Möglichkeit der **Datenspeicherung**, vor allem der Zugriff auf Daten, die außerhalb Europas lagern, ist zwar Schutz für Verbraucher, aber schränkt die Qualität von Bots ein: Bots bedürfen zur vollen Funktionalität oft riesiger „**Datenseen**“, oftmals von Drittanbietern wie Amazon oder Microsoft, die nicht unbedingt in Europa liegen. Ohne eine Möglichkeit zur Datenspeicherung funktioniert aber kein Bot. Dieses Dilemma gilt es, verbraucherfreundlich zu regeln.

Aus verbraucherrechtlicher Sicht ist zudem von Bedeutung, dass Unternehmer kognitive Einschränkungen auf Verbraucherseite (vor allem Biases und beschränkte Rationalität, die sich beispielsweise in Spontankäufen zeigen) zugunsten ihres wirtschaftlichen Gewinns grundsätzlich (aus)nutzen dürfen. Ein solcher Fall ist denkbar, wenn Assistenten eingesetzt werden, um Vertragsangelegenheiten des Verbrauchers zu erleichtern, dabei aber gleichzeitig eine Vielzahl unterschiedlicher Interessen vertreten, die dem Verbraucher nicht bekannt sind. Die Tatsache, dass die Verbraucher Geld für einen digitalen Assistenten zahlen (z.B. eingebettet in einen intelligenten Lautsprecher), kann sie zu der Annahme veranlassen, dass der Assistent ihre Interessen standardmäßig als vorrangig einstufen wird. Tatsächlich ist dies aber keineswegs immer der Fall; vielmehr wird die Funktion des Assistenten von unterschiedlichen und dem Nutzer unbekannten Interessen beeinflusst. Das Fehlen eines sichtbaren Rankings der Anliegen diverser Nutzer oder Newsfeeds hebt die (bereits vorgestellten) Probleme **personalisierter Suchergebnisse** auf eine neue Ebene. Es wird nämlich nicht deutlich, wer eigentlich welche Interessen verfolgt und wofür. Die Offenlegung der sogenannten Hauptmerkmale des Rankings hilft auch nicht wirklich weiter (siehe Steckbrief Personalisierte Preise).

Zwar delegieren Verbraucher derzeit (noch) nicht gesamte Entscheidungsprozesse an persönliche digitale Assistenten; dies bedeutet aber keineswegs, dass die Assistenten sich nicht auf den Verbraucher als Entscheidungsträger auswirken. Denn ihr Zweck liegt gerade darin, dass Verbraucher sich nicht die Mühe machen müssen, verfügbare Optionen zu identifizieren, zu vergleichen und zwischen diesen zu entscheiden. Stattdessen präsentieren die Algorithmen der Assistenten ihren Nutzern eine personalisierte Entscheidungsarchitektur oder treffen die zur Umsetzung des Sprachbefehls notwendigen Entscheidungen sogar selbst. Zentral für die Wahrung der **Entscheidungsautonomie** – und potenziell auch sogar für die **Stärkung** der Entscheidungsautonomie mithilfe von KI im Sinne von Entscheidungsunterstützung – sind die Transparenz und die Verständlichkeit. Die Nutzer müssen nachvollziehen können, nach welchen Kriterien und Interessen die Assistenten eine Option empfehlen.

Was können Verbraucher tun?

- die Seriosität des Bots und die genutzten Informationsquellen kritisch prüfen und bei Verdacht auf Betrug recherchieren
- Kontaktanfragen von unbekannten Personen in sozialen Netzwerken nicht annehmen
- im Kontakt mit Bots sparsam mit Daten umgehen und vor allem sensible Daten nicht preisgeben
- bei Sprachassistenten sollten datensparsame Einstellungen gewählt werden, das Mikrofon (und ggf. die Kamera) ausgeschaltet werden; bei vorübergehender Nichtnutzung vom Netz nehmen

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) schlägt für die Nutzung von Sprachassistenten folgende Maßnahmen vor:

- **Vermeidung von unberechtigten Zugriffen:** Der digitale Assistent sollte bei Abwesenheit deaktiviert oder ausgeschaltet werden. Falls möglich, sollten Sprachprofile für verschiedene Personen zur Interaktion mit dem Gerät eingerichtet werden.
- **Geeignete Platzierung des digitalen Assistenten:** Der digitale Assistent sollte an einem Ort platziert werden, an dem eine Nutzung nur durch Berechtigte möglich ist. Eine Position am offenen Fenster ist beispielsweise ungeeignet, wenn er ein smartes Türschloss steuern kann.
- **Sichern mit PIN oder Passwort:** Kritische Sprachbefehle und Bestellungen sollten immer erst nach Eingabe eines PIN-Codes oder Passwortes ausgeführt werden dürfen.
- **Prüfung der angefallenen Daten:** Durch regelmäßige Einsicht der gespeicherten Daten kann eine missbräuchliche Verwendung des digitalen Assistenten erkannt werden. Nach Bedarf können Daten gelöscht werden.
- **Datenschutzeinstellungen anpassen:** Datenschutzeinstellungen sollten kontrolliert und gemäß persönlicher Bedürfnisse verändert werden.
- **Nur vertrauenswürdige Erweiterungen:** Anwendungen zur Funktionserweiterung sollten nur aus vertrauenswürdigen Quellen bezogen werden.
- **Beschränkung auf notwendige Schnittstellen:** Der digitale Assistent sollte nur mit Geräten und Accounts verbunden werden, die für das Funktionieren des Systems unabdingbar sind. Manchmal ist das Anlegen eines neuen Accounts sinnvoll, um persönliche Daten abzusichern.

Quelle: https://www.bsi-fuer-buerger.de/BSIFB/DE/DigitaleGesellschaft/IoT/Digitale_Assistenten/Digitale_Assistenten_node.html

Verbraucherpolitische Forderungen

- Problemsensibilisierung: Hinweis, dass sensible Daten offengelegt werden können
- Kennzeichnungspflicht: Chatbots als solche kenntlich machen
- Transparenz und Informationspflicht: Offenlegen, welcher Entscheidungsmechanismus grundsätzlich dahintersteckt, welche Daten zugrunde gelegt werden und welche Daten gespeichert werden
- Institutionell: Verbraucherfreundliche Abwägung der Vor- und Nachteile (Nutzen und Kosten) des Schutzes der – für die Funktionalität der Bots notwendigen – Daten für Training und Arbeit der Bots.
- Speziell für Sprachassistenten fordert die Datenethikkommission (2019, S. 101) bindende technische Vorgaben und Transparenzpflichten:
  - bindende technische Vorgaben zur Implementierung von Datenschutz „by design“ und „by default“
  - grundsätzlich rein lokale Verarbeitung von Sprachdateien (und Löschbarkeit) und Beschränkung einer Datenweiterleitung an den Betreiber oder Dritte auf bereits in Maschinensprache übersetzte Befehle (z.B. eine Bestellung)
  - bindende technische Vorgaben zur Abschaltbarkeit von Mikrofon und Internetverbindung sowie Sichtbarmachung, ob das Mikrofon an- oder ausgeschaltet ist
  - dem Medium angemessene Ausgestaltung von Transparenzpflichten, indem die wichtigsten Offenlegungen in der jeweiligen Situation oder in regelmäßigen Abständen auch akustisch erfolgen

Was sagt das Verbraucherrecht?

Soweit über Chatbots und Sprachassistenten Daten gesammelt und ausgewertet werden sollen, gelten die üblichen **datenschutzrechtlichen Anforderungen**: Notwendig ist eine **Einwilligung**, und es stellen sich auch die bereits mehrfach angesprochenen Fragen zum **Dateneigentum** und zur **Datensicherheit** (Steckbrief Sicheres Surfen). Im Folgenden werden insbesondere Sprachassistenten oder Konversationsagenten betrachtet. Diese sind für Verbraucher in vielen Lebenslagen von hoher Bedeutung und auch besonders attraktiv; und sie haben bereits in die neueren Regeln des EU-Verbraucherrechts Eingang gefunden.

Lauterkeitsrecht

Die zweite Säule des Verbraucherrechts (neben dem Datenschutzrecht) ist das **Lauterkeitsrecht** (Gesetz gegen Unlauteren Wettbewerb, UWG). Es verbietet unlautere, irreführende und aggressive Geschäftspraktiken. Das Lauterkeitsrecht sanktioniert die irreführende Unterlassung bei fehlender Offenlegung der Produktbewertung (siehe Steckbrief Dark Patterns). Die diesbezügliche Reform des EU-Verbraucherrechts ist bislang zwar noch nicht in das deutsche Recht umgesetzt (erwartet wird sie Ende 2021); es zeichnet sich jedoch bereits die Richtung ab, in welche die Entwicklung gehen könnte. Der in der EU-Richtlinie über unlautere Geschäftspraktiken (Art. 2 lit. m UGP-RL) weit gefasste Begriff eines **Rankings**, der absichtlich technologisch neutral bleibt, legt nahe, dass Anbieter von Konversationsagenten verpflichtet werden könnten, die **Parameter offenzulegen**, die sie zur Produktbewertung verwenden. Tun sie es nicht, läge dann eine irreführende Unterlassung vor. Für Anbieter von Sprachassistenten erstreckt sich die Verpflichtung jedoch nur auf die **Hauptparameter** für das Ranking und nicht auf individuelle Informationen für jede einzelne Suchabfrage, was wahrscheinlich auch kaum praktikabel wäre. Weitere obligatorische Informationen können auf der Website eines Sprachassistentenanbieters bereitgestellt werden wie dies bei Suchmaschinenanbietern bereits der Fall ist.

Vertragsrecht

Vertragliche Informationspflichten beim Einsatz von Sprachassistenten

Insbesondere für Online-Verträge verlangt das Vertragsrecht (Art. 6 Abs. 1 lit. c VR-RL; Art. 246a Abs. 1 Nr. 2 EGBGB), dass Verbraucher vor Abschluss des Vertrages über die **Anschrift** des Ortes informiert werden, an dem der Unternehmer niedergelassen ist, ggf. auch seine Telefonnummer, Faxnummer und E-Mail-Adresse. Nach Ansicht des Europäischen Gerichtshofs (EuGH) (ECLI:EU:C:2019:165 – Amazon EU) ist der Unternehmer verpflichtet, jedem Verbraucher ein beliebiges Kommunikationsmittel zur Verfügung zu stellen, über das dieser schnell mit ihm in Kontakt treten und effizient mit ihm kommunizieren kann. Das muss aber nicht das Telefon sein. Mit der Anpassung des Verbraucherrechts an Online-Geschäfte (Art. 6 Abs. 1 lit. c VR-RL) können Chats als **zusätzliche** Variante der Kontaktaufnahme bereitgestellt werden. Doch muss dem Verbraucher die Möglichkeit erhalten bleiben, den Unternehmer per Post, per Telefon oder per E-Mail zu kontaktieren.

Die Informationspflichten des Verbraucherrechts (Art. 6 VR-RL) sind technologisch neutral. Dem Verbraucher können deshalb vor dem Abschluss eines Vertrages auch über einen Sprachassistenten eine Liste mit Informationen zu diesem Vertrag zur Verfügung gestellt werden. Aber sollte die ausführliche Liste der rechtlich vorgegebenen Informationen vor jedem eventuellen Kauf den Verbrauchern wirklich vom Assistenten vorgelesen werden? Eine solche Anforderung scheint wenig praktikabel. Die Verbraucherrecht-Richtlinie (Art. 8 Abs. 4 VR-RL; § 312d Abs. 1 BGB iVm Art. 246a Abs. 3 EGBGB) sieht daher ein **vereinfachtes Informationsregime** für Online-Verträge (wie auch bei Telefonvertrag) vor. Hier kann und muss Information nur räumlich oder zeitlich begrenzt zur Verfügung stehen (z.B. auf Displays und neuerdings auch bei Chats). Zu dieser vereinfachten Angabepflicht gehören Informationen über die wesentlichen Merkmale der Waren oder Dienstleistungen, die Identität des Unternehmers, den Gesamtpreis, das Widerrufsrecht, die Vertragslaufzeit und die

Bedingungen der Kündigung unbefristeter Verträge. Alle weiteren Informationen sind dem Verbraucher anderweitig, beispielsweise per E-Mail, zur Verfügung zu stellen.

Verantwortung für die Bereitstellung von Information

Nicht ohne weiteres ersichtlich ist, wer für die **Bereitstellung von Informationen** verantwortlich sein soll, wenn Produkte den Verbrauchern von **Dritten** angeboten werden. In ihrem Leitfaden zur VR-RL hat die Europäische Kommission darauf hingewiesen, dass der Begriff des Unternehmers in Art. 2 Nr. 2 VR-RL nicht nur die Person umfasst, die direkt mit dem Verbraucher einen Vertrag abschließt, sondern auch eine andere Person, die in ihrem Namen oder Auftrag handelt. Insofern können auch Sprachassistenten-Anbieter mit der Übermittlung beauftragt werden. Die jüngsten Entwicklungen auf EU-Ebene zeigen jedoch keine klare Linie, wie mit Sprachassistenten umzugehen ist. Einerseits scheinen die im Rahmen der Strategie für einen digitalen Binnenmarkt erlassenen Rechtsakte den Herausforderungen der Sprachassistenten Rechnung zu tragen. Auf der anderen Seite schreiben die Änderungen zur VR-RL den Anbietern von Online-Marktplätzen ausdrücklich vor, die Verbraucher über die Hauptparameter zur Festlegung des Rankings der Angebote, die dem Verbraucher als Ergebnis seiner Suchanfrage auf dem Online-Marktplatz präsentiert werden, zu informieren und zwar in einem bestimmten Bereich der Online-Benutzeroberfläche, der von der Seite, auf der die Angebote angezeigt werden, unmittelbar und leicht zugänglich ist.

Belege und weiterführende Literatur

Bird, J. J., Ekárt, A., & Faria, D. R. (2018). Learning from Interaction: An Intelligent Networked-Based Human-Bot and Bot-Bot Chatbot System. In A. Lotfi, H. Bouchachia, A. Gegov, C. Langensiepen, & M. McGinnity (Hrsg.), *Advances in Computational Intelligence Systems* (Vol. 840, S. 179–190). Vorgestellt beim UK Workshop on Computational Intelligence, Cham: Springer International Publishing. https://doi.org/10.1007/978-3-319-97982-3_15

Bundesamt für Sicherheit in der Informationstechnik (BSI). (2020a). Digitale Assistenten. *BSI für Bürger*. https://www.bsi-fuer-buerger.de/BSIFB/DE/DigitaleGesellschaft/IoT/Digitale_Assistenten/Digitale_Assistenten_node.html. Abgerufen 3. Juli 2020

Bundesamt für Sicherheit in der Informationstechnik (BSI). (2020b). Social Bots und Chat Bots: Kleine Mini-Roboter mit eigener Identität im Netz. *BSI für Bürger*. https://www.bsi-fuer-buerger.de/BSIFB/DE/DigitaleGesellschaft/SozialeNetze/Bots/bots_node.html. Abgerufen 6. August 2020

Bundesamt für Sicherheit in der Informationstechnik (BSI). (2020c). Wer antwortet mir? Wissenswertes rund um das Thema Bots. *BSI für Bürger*. https://www.bsi-fuer-buerger.de/BSIFB/DE/Service/Aktuell/Informationen/Artikel/Bots_20092017.html. Abgerufen 3. Juli 2020

Datenethikkommission der Bundesregierung. (2019). *Gutachten der Datenethikkommission der Bundesregierung*. Berlin: Bundesministerium des Innern, für Bau und Heimat. https://www.bmjv.de/SharedDocs/Downloads/DE/Themen/Fokusthemen/Gutachten_DEK_DE.pdf?__blob=publicationFile&v=2. Abgerufen 1. Juni 2020

Europäische Kommission. (2014). *LEITFADEN DER GD JUSTIZ zur Auslegung der Verbraucherrechte-Richtlinie 2011/83*.

Hoffmann, A. (2019). *Chatbots: Einführung in die Zukunft von Marketing, PR und CRM*. Haar bei München: Franzis Verlag.

idealo. (2020). *E-Commerce Trends 2020*. Berlin: idealo internet GmbH. https://www.idealo.de/unternehmen/wp-content/uploads/sites/33/2020/01/2020-01-16_idealo_E-Commerce-Trends-2020_Whitepaper.pdf

Micklitz, H.-W., Namyslowska, M., & Jablonowska, A. (2020 im Erscheinen). § 6 KI und Verbraucherrecht. In M. Ebers, C. Heinze, T. Krügel, & B. Steinrötter (Hrsg.), *Künstliche Intelligenz und Robotik* (1. Aufl.). München: C. H. Beck.

Verbraucherzentrale Hessen. (23. April 2019). Reden mit Robotern: KI-Experte Stefan Holtel im Interview mit Feature. *Verbraucherzentrale Hessen*. https://www.verbraucherzentrale-hessen.de/feature/chatbots-reden-mit-robotern-ki-experte-stefan-holtel-im-interview-35650. Abgerufen 6. August 2020

Volkmann, H. (27. März 2020). #WirVsVirus – Hacken im Auftrag der Bundesregierung. *legal-tech.de*. https://www.legal-tech.de/wirvsvirus-hacken-im-auftrag-der-bundesregierung/. Abgerufen 10. Juni 2020.

Dark Patterns

Was sind Dark Patterns?

Der Begriff „Dark Patterns“ („Dunkle Muster“) bezeichnet im Bereich der Software-Entwicklung und des Interface-Designs **unfaire Techniken und Tricks**, die Verbraucherinnen und Verbraucher beim Nutzen von Webseiten und Apps irreführen und sie dazu verleiten, ungewollte Einwilligungen zu geben oder ungewollte Handlungen durchzuführen – etwa Produktzusätze wie Versicherungen abzuschließen (z.B. Bogenstahl 2019). Erlernte Verhaltensmuster werden durch raffiniert platzierte Buttons oder Drop-Down-Menüs gezielt manipuliert. Schnelles Durchscrollen und Überfliegen von Webseiten oder Apps führt dann oft zu falschen Annahmen. Ein falsch gesetztes Häkchen, eine in einem Drop-Down-Menü versteckte Option oder einfach sehr klein gedruckte Informationen ermöglichen ungewollte Newsletter-Abonnements, kostenpflichtige Registrierungen oder heimlich in den Warenkorb geschmuggelte Waren und Dienstleistungen. Geprägt hat den Begriff der Webdesigner Harry Brignull. Auf der Webseite www.darkpatterns.org und dem Twitteraccount @darkpatterns werden entsprechende Praktiken gesammelt; eine digitale „Hall of Shame“ stellt Beispiele solcher manipulativen Dark Patterns aus der ganzen Welt an den digitalen Pranger.

Dark Patterns werden auch genutzt, um möglichst viele personenbezogene Daten von Verbraucherinnen und Verbrauchern zu sammeln. Die neue Datenschutz-Grundverordnung der EU verlangt zwar in den meisten Fällen eine explizite Zustimmung von Benutzerinnen und Benutzern, wenn deren persönliche Daten verarbeitet werden. Ein geschickt gewähltes **Interface-Design** mit Dark Patterns begünstigt jedoch die Einwilligung in vielen Fällen. Zum Beispiel benötigt es mindestens die doppelte Anzahl von Klicks, um die Datenverarbeitung abzulehnen; oder es wird suggeriert, dass man nicht die volle Leistung erhält; oder die Ablehnungs-Option muss bewusst auf der Webseite durch Scrollen oder über Menüs gesucht werden, wohingegen die Zustimmungsoption die naheliegende ist. Dark Patterns werden auch als eine gezielt eingesetzte Form von sogenannten „**Sludges**“ bezeichnet (Sunstein 2020), also Nudges (kleine, freundliche Stupser, Thaler & Sunstein 2008), die Verbraucher benachteiligen statt zu unterstützen (manchmal auch **Dark Nudges** genannt, Überblick bei Reisch 2020).

Typen und Beispiele

Trick Questions (Trickfragen)	Beim Ausfüllen von Formularen werden zweideutige Fragen gestellt, um Antworten zu bekommen, die die Nutzer eigentlich nicht beabsichtigt hatten.
Sneak into Basket (In den Einkaufskorb schmuggeln)	Während eines Einkaufs im Internet werden zusätzliche Artikel in den Warenkorb gelegt, oft durch voreingestellte Optionen auf vorherigen Seiten.
Roach Motel (Rattenfalle)	Es ist sehr leicht, zum Beispiel Premium-Abonnements abzuschließen; diese wieder zu kündigen, ist erheblich schwieriger gemacht.
Privacy Zuckering (Abgreifen persönlicher Daten)	Diese nach dem Facebook-Gründer Mark Zuckerberg benannte Datenabsauge-Technik beschreibt, dass man dazu verleitet wird, mehr persönliche Informationen öffentlich zu teilen als man eigentlich beabsichtigt hatte.
Price Comparison Prevention (Verhindern von Preisvergleichen)	Ein Händler erschwert den Preisvergleich zwischen Artikeln; fundierte Entscheidungen können nicht getroffen werden.
Misdirection (Irreführung)	Das Design lenkt die Aufmerksamkeit gezielt auf eine Sache, um von anderen Informationen (beispielsweise Pflichtinformationen) abzulenken.
Hidden Costs (Versteckte Kosten)	Erst im letzten Schritt des Bestellvorgangs werden unerwartete Kosten wie Versandpauschalen, Steuern oder Gebühren angezeigt. Dieser Praxis sind mittlerweile enge rechtliche Schranken gesetzt worden.

Bait and Switch (Anlocken und Überraschen)	Während der Erledigung eines bestimmten Vorgangs passiert plötzlich etwas völlig anderes, Nutzer sind überrascht und reagieren spontan.
Disguised Ads (getarnte Werbung)	Werbeanzeigen sind als Navigationspunkte oder andere Inhalte getarnt.
Forced Continuity (untergeschobener Kauf)	Eine kostenlose Testversion geht direkt in kostenpflichtige Leistungen über; dabei wird die Kreditkarte stillschweigend und ohne Vorwarnung belastet.
Confirmshaming (Bestätigung aus schlechtem Gewissen)	Die Möglichkeit zur Ablehnung wird so formuliert, dass Verbraucherinnen und Verbraucher Schuldgefühle bekommen, wenn sie tatsächlich ablehnen.
Friend Spam (Freunde Spam)	Unter einem Vorwand werden Email- oder Social Media-Zugänge abgefragt; dann werden im Namen des Nutzers Spam-Mails an diese Kontakte gesendet.

Quellen: Bogenstahl (2019); Mathur et al. (2019)

Verbreitung und Relevanz

Dark Patterns sind kein individuelles, sondern ein Massenphänomen (Mathur et al. 2019). Die norwegische Verbraucherschutzorganisation NCC wirft aufgrund einer eigenen Studie Google, Facebook und in kleinerem Ausmaß auch Microsoft vor, Nutzerinnen und Nutzer durch Dark Patterns zum Akzeptieren fragwürdiger Datenschutzbedingungen zu verleiten. Eine Studie der Verbraucherzentrale Hessen (4. August 2020) bei 20 großen Online-Shops (darunter Apple, H&M und Media Markt) zeigte, dass die Hälfte der Shops geltendes Recht missachtet und unübersichtliche Voreinstellungen nutzt, welche die gesamte Cookie-Auswahl aktivieren.

Dark Patterns werden vor allem im E-Commerce eingesetzt, und dort vor allem bei Dienstleistungen und Produkten, die in der Regel online gebucht / gekauft werden. Das Flugunternehmen Ryanair bot z.B. mit der Flugbuchung eine Reiseversicherung an, die allerdings nicht über eine einfache Ja/Nein Möglichkeit auszuwählen war. Über ein Drop-Down-Menü konnte zunächst nur das Land für die Versicherung gewählt werden. Erst zwischen den Länderoptionen versteckte sich auch die Möglichkeit, „keine Versicherung abschließen“. Konsumenten, die aufgrund der Corona-Pandemie Reisen stornieren mussten, wurden häufig durch solche Dark Patterns davon abgehalten. Verbraucher- und Datenschützer sowie die „Netzgemeinde“ verurteilen die Praxis des Dark Patterns als unethisch und ausbeuterisch.

Herausforderungen

- Aufgrund von Dark Patterns werden Einwilligungen gegeben und Handlungen vollzogen, die von Verbraucherinnen und Verbrauchern nicht intendiert waren.
- Das Recht auf Auskunft, Berichtigung und Löschung der Daten ist oft nur sehr schwer oder gar nicht wahrzunehmen.
- Unternehmen können auf der Grundlage persönlicher Daten ausgefeilte Nutzerprofile erstellen. Kategorisierung von Konsumentinnen und Konsumenten, gezielte Werbung, um Konsumbedürfnisse zu wecken, personalisierte Preise oder die Entscheidung über Vertragskonditionen werden aufgrund der Nutzerprofile vorgenommen. Diskriminierung und Manipulation sind möglich.
- Verletzung von Persönlichkeitsrechten.

Verbraucherpolitische Forderungen

- Öffentliches Problembewusstsein für manipulative Designtechniken schaffen.
- Explizite Einwilligung der Nutzer in die Datenverarbeitung (nicht versteckt in AGBs).
- Transparenz und aus Verbrauchersicht verständliche und nachvollziehbare Datenverarbeitungen mit echten Wahl- und Interventionsmöglichkeiten der Nutzenden.

- Keine Benachteiligung von datenschutzbewussten Verbraucherinnen und Verbrauchern; das Produkt muss auch ohne Herausgabe nicht-relevanter Daten erhältlich sein.
- „Sludge Audits“ durch verbraucherpolitische Institutionen (d.h. systematische Untersuchung von Angeboten auf solche „Dark Nudges“ oder „Sludges“, ggf. Abmahnung)
- Corporate Digital Responsibility als Teil guter Unternehmensführung etablieren (Thorun et al. 2018).

Was können Verbraucher tun?

- Cookie-Voreinstellungen genau anschauen: Viele Webseiten haben die Zustimmung zur Speicherung von Cookies voreingestellt; dabei ist dies ausdrücklich verboten. Zustimmungsbuttons sind meist prominent platziert und farblich gestaltet; ein unscheinbarer Button regelt dagegen die selbstgewählte, reduzierte Auswahl an erlaubten Cookies.
- Datenvermeidung und Datensparsamkeit: Grundsätzlich der Nutzung und Übermittlung von Daten zum Zweck der Werbung, Markt- oder Meinungsforschung und Drittanbieter-Cookies widersprechen (was auch bedeutet: Ausnahmen machen für seriöse Anbieter).
- Datenschutzbestimmungen lesen, zumindest bei wiederholt aufgesuchten Anbietern (auch das Kleingedruckte).
- Information über die besonders drastische Dark Patterns einholen und die jeweiligen Anbieter boykottieren.
- Nicht mit dem Smartphone, sondern mit einem PC o.ä. einkaufen, denn bei Handys ist die Aufmerksamkeitsschwelle aufgrund des kleinen Displays geringer als bei einem großen Bildschirm.

Was sagt das Verbraucherrecht?

Das Verbraucherrecht ist grundsätzlich nur sehr bedingt in der Lage, die Verbraucher vor der Ausnutzung von Verhaltensanomalien angemessen zu schützen. Die zuständigen Kontrollinstanzen, ob Datenschutzbehörden oder Gerichte, liefern bislang wenig Anhaltspunkte. Soweit von Verbraucherseite Verfahren angestrengt wurden, stehen die Ergebnisse aus. Gleichzeitigt zeigen sie das Spektrum der Probleme auf, die sich in der Praxis der Einwilligung und auch bei der Durchsetzung des Rechts mit Hilfe der Datenschutzbehörden stellen (BEUC 2020). Die Diskussion ist deshalb in weiten Teilen immer noch akademischer Natur. Dementsprechend weit liegen die Positionen auseinander.

Datenschutzrecht

Dreh- und Angelpunkt des **Datenschutzrechts** für die zur Entwicklung von Dark Patterns benötigten Daten ist die **Einwilligung** des Verbrauchers in Art. 4 Nr. 11 Datenschutzgrundverordnung (DSGVO). Die Wirksamkeit der Einwilligung ist an drei Voraussetzungen geknüpft: **Freiwilligkeit, Informiertheit** und **Unmissverständlichkeit**. Soweit ersichtlich, setzt der Europäische Datenschutzausschuss (d.h. das Gremium der nationalen Datenschutzbeauftragen und des Europäischen Datenschutzbeauftragten) vor allem bei der Unmissverständlichkeit an. Gefordert wird eine „bewusste Handlung“ ohne „Zweifel an der Zustimmungsabsicht“, die Sicherstellung der „warnenden Absicht“ der Einwilligung, die mit der „Müdigkeit gegenüber dem Anklicken“ abnimmt (Europäischer Datenschutzausschuss, 18 Rdnr. 87). Wie diese Anforderungen umgesetzt werden sollen, bleibt den Unternehmen überlassen. Der EuGH hat in seiner Entscheidung „Planet49“ (EuGH C-673/17 = NJW 2019, 3433) betont, dass klare und umfassende Informationen den Nutzer in die Lage versetzen müssen, die „Konsequenzen einer … Einwilligung leicht zu bestimmen“. Mit dieser Maxime lässt sich den Dark Patterns aber nicht beikommen.

Die Einwilligung ist nicht die einzige Möglichkeit des Unternehmens, legal personenbezogene Daten des Verbrauchers zu sammeln. Die Datenschutzgrundverordnung (Art. 6 Abs. 1 b)-f) DSGVO, eigene

Hervorhebung) enthält eine lange Liste von **Ausnahmen**, die in den Unternehmen in der Praxis einen großen Spielraum einräumen, auch ohne Einwilligung des Verbrauchers Daten zu erheben und zu verarbeiten, nämlich: zur „**Erfüllung eines Vertrags**, dessen Vertragspartei die betroffene Person ist, oder zur **Durchführung vorvertraglicher Maßnahmen**, die auf Anfrage der betroffenen Person erfolgt, zur Erfüllung einer rechtlichen Verpflichtung erforderlich, der der Verantwortliche unterliegt; zur **Wahrung der berechtigten Interessen des Verantwortlichen** oder eines Dritten, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen, insbesondere dann, wenn es sich bei der betroffenen Person um ein Kind handelt". Wann diese Grenzen überschritten werden, ist bislang unklar. Doch kommt die DSGVO den Interessen der Unternehmen weit entgegen, wenn es im 47. Erwägungsgrund heißt: „Die Verarbeitung personenbezogener Daten zum Zwecke der Direktwerbung kann als eine einem berechtigten Interesse dienende Verarbeitung betrachtet werden". Strengere Sonderregeln gelten bislang nur für die Erhebung und Verarbeitung gesundheitsbezogener Daten (Steckbrief Telematiktarife).

Konkrete rechtliche Vorgaben, die **Voreinstellungen zu Lasten der Verbraucher untersagen**, gibt es bislang nur wenige: Art 22 Verbraucherrechts-Richtlinie verbietet Voreinstellungen für Extrazahlungen, die über den Preis für die Hauptleistung hinausgehen. Nach Auffassung des EuGH ist der Vertrieb von Sim-Karten mit einer kostenträchtigen Voreinstellung für Internet und Mail-Box Dienste im Sinne des Anhang I Nr. 29 der Richtlinie 2005/29 über unlautere Geschäftspraktiken (ECLI:C:2018:710) verboten. Dieselbe Richtlinie verbietet (in Nr. 6 des Anhangs) „Bait and Switch" Techniken. Art. 25 II DSGVO untersagt datenschutzunfreundliche Voreinstellungen. Jedenfalls kann durch bloßes Scrollen bzw. Bewegungen mit der Maus keine Einwilligung fingiert werden. Darüberhinausgehende Vorgaben müssen erst noch definiert werden. Der Europäische Datenschussausschuss hat im November 2019 seine „Guidelines" vorgelegt. Diese präzisieren die Anforderungen an die datenerhebenden und datenverarbeitenden Unternehmen. Sie enthalten jedoch keine Verbotslisten, was aus der Sicht des Verbraucherrechts wünschenswert wäre.

Lauterkeitsrecht

Die sogenannte **Omnibus-Richtlinie** der Europäischen Union begründet ein eigenes Klagerecht der Verbraucher gegen unlautere Geschäftspraktiken einschließlich Ersatz des dem Verbraucher entstandenen Schadens sowie gegebenenfalls Preisminderung oder Beendigung des Vertrags. Die nähere Ausgestaltung des individuellen Klagerechts hat der deutsche Gesetzgeber bis Ende 2021 sicherzustellen. Soweit Dark Patterns mit Hilfe der individuell gesammelten Daten personalisiert werden, könnte ein solch individueller Klageanspruch zur Aufdeckung von Dark Patterns beitragen.

Gegenüber der Einbeziehung von Erkenntnissen der Konsumforschung über das Nutzerverhalten in die rechtliche Bewertung ist das Lauterkeitsrecht offener als das Datenschutzrecht, jedenfalls in der gerichtlichen Praxis (Schebesta & Purnhagen 2019). Das rührt daher, dass die Gerichte bei der Entscheidung, ob eine bestimmte Werbepraxis rechtswidrig ist, sich mit den möglichen Wirkungen auf das Verhalten der Verbraucher auseinandersetzen müssen. Art 8 der EU-Richtlinie über unlautere Geschäftspraktiken (UGP Richtlinie) (/§ 4 a UWG) untersagen Belästigung, Nötigung und unzulässige Beeinflussung als aggressive Geschäftspraktiken. Die im Gesetz verlangte Machtposition liegt in dem detaillierten Wissen des Unternehmens über die Präferenzen des Verbrauchers. Dieses Wissen wird gegenüber dem Verbraucher nicht offengelegt. Genau deshalb haben Dark Patterns das Potenzial, die Entscheidungs- und Verhaltensautonomie erheblich zu beinträchtigen. Die klagebefugten Verbraucherverbände können im Wege der **Unterlassungsklage** gegen Dark Patterns vorgehen, um mit Hilfe der Gerichte eine Konkretisierung der Rechtslage herbeizuführen.

Belege und weiterführende Literatur

BEUC. (2020). *The long and winding road. Two years of the GDPR: A cross-border data protection enforcement case from a consumer perspective* (Nr. BEUC-X-2020-074-05/08/2020). Brüssel: Der Europäische

Verbraucherverband. https://www.beuc.eu/publications/beuc-x-2020-074_two_years_of_the_gdpr_a_cross-border_data_protection_enforcement_case_from_a_consumer_perspective.pdf

Bogenstahl, C. (2019). *Dark Patterns –Mechanismen (be)trügerischen Internetdesigns* (Themenkurzprofil Nr. 30). Berlin: Büro für Technikfolgen-Abschätzung beim Deutschen Bundestag (TAB). https://www.tab-beim-bundestag.de/de/pdf/publikationen/themenprofile/Themenkurzprofil-030.pdf

Europäischer Datenschutzausschuss. (2019). *Guidelines 4/2019 on article 25 data protection by design and by default* (Guidelines Nr. 4/2019). Europäischer Datenschutzausschuss. https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_201904_dataprotection_by_design_and_by_default.pdf

Europäischer Datenschutzausschuss. (2020). *Guidelines 05/2020 on consent under Regulation 2016/679* (Guidelines Nr. 05/2020). Europäischer Datenschutzausschuss. https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202005_consent_en.pdf

Mathur, A., Acar, G., Friedman, M. J., Lucherini, E., Mayer, J., Chetty, M., & Narayanan, A. (2019). Dark patterns at scale: Findings from a crawl of 11K shopping websites. In *Proceedings ACM Human-Computer Interaction* (Vol. 3, CSCW, Artikel 81). https://doi.org/10.1145/3359183

Micklitz, H.-W., Namyslowska, M., & Jablonowska, A. (2020 im Erscheinen). § 6 KI und Verbraucherrecht. In M. Ebers, C. Heinze, T. Krügel, & B. Steinrötter (Hrsg.), *Künstliche Intelligenz und Robotik* (1. Aufl.). München: C. H. Beck.

Norwegian Consumer Council. (2018). *Deceived by design: How tech companies use dark patterns to discourage us from exercising our rights to privacy*. Norwegian Consumer Council. https://fil.forbrukerradet.no/wp-content/uploads/2018/06/2018-06-27-deceived-by-design-final.pdf

Reisch, L. A. (2020). Nudging hell und dunkel: Regeln für digitales Nudging. *Wirtschaftsdienst*, *100*(2), 87–91. https://doi.org/10.1007/s10273-020-2573-y

Rieger, S., & Sinders, C. (2020). *Dark Patterns: Design mit gesellschaftlichen Nebenwirkungen*. Berlin: Stiftung Neue Verantwortung. https://www.stiftung-nv.de/sites/default/files/dark.patterns.pdf

Schebesta, H., & Purnhagen, K. P. (2019). An average consumer concept of bits and pieces : Empirical evidence on the Court of Justice of the European Union's concept of the average consumer in the UCPD. In L. de Almeida, M. C. Gamito, M. Durovic, & K. P. Purnhagen (Hrsg.), *The Transformation of Economic Law: Essays in Honour of Hans-W. Micklitz* (1. Aufl., S. 13–28). Oxford: Hart Publishing. https://doi.org/10.5040/9781509932610.ch-002

Sunstein, C. R. (2020). Sludge audits. *Behavioural Public Policy*, 1–20. https://doi.org/10.1017/bpp.2019.32

Thaler, R. & Sunstein, C. R. (2008). *Nudge: Improving decisions about health, wealth, and happiness*. New Haven, CT: Yale University Press.

Thorun, C., Kettner, S. E., & Merck, J. (2018). Ethik in der Digitalisierung. Der Bedarf für eine Corporate Digital Responsibility. *WISO Direkt*, *17*, 1–4.

Verbraucherzentrale Hessen. (4. August 2020). Reingewilligt. *Verbraucherzentrale Hessen*. https://www.verbraucherzentrale-hessen.de/pressemeldungen/digitale-welt/reingewilligt-50288. Abgerufen 14. August 2020

Weinzierl, Q. (2020). Dark Patterns als Herausforderung für das Recht. Rechtlicher Schutz vor der Ausnutzung von Verhaltensanomalien. *Neue Zeitschrift für Verwaltungsrecht– Extra*, *39*(15), 1–11.

Dynamische Preise

Was sind dynamische Preise?

Bei einer dynamischen Preisstrategie ändern sich Preise kurzfristig im **Zeitablauf**: An unterschiedlichen Tagen oder zu unterschiedlichen Tageszeiten werden Waren oder Dienstleistungen im E-Commerce zu unterschiedlichen Preisen angeboten. Grundlage für die Schwankungen sind entsprechende lernende Algorithmen und Künstliche Intelligenz. Die Preise sind dabei für alle Verbraucherinnen und Verbraucher zu einem bestimmten Zeitpunkt gleich (Dautzenberg et al. 2018; Spann & Skiera 2020).

Dynamische oder schwankende Preise sind zu unterscheiden von einer **individualisierten** Preisgestaltung, bei welcher der Preis aufgrund von kunden- oder mengenindividuellen Entscheidungsparametern variiert (beispielsweise Einzelstücke für Stammkunden), sowie von **personalisierten** Preisen (siehe Steckbrief Personalisierte Preise) bei welchen es sich um unterschiedliche Preise für das gleiche Produkt zur gleichen Zeit handelt, abhängig von der Person des Käufers oder der Käuferin.

Verbreitung und Beispiele

Was seit Jahrzehnten von Tankstellen bekannt ist, ist heute auch im Online-Handel fest etabliert. Dabei ist das Ausmaß der Preisschwankungen sowohl in Häufigkeit als auch Volatilität unterschiedlich: Die „Marktwächter Digitale Welt“ der Verbraucherzentrale (VZ) Brandenburg (Dautzenberg et al. 2018) stießen bei einer Untersuchung dynamischer Preise in einem Untersuchungszeitraum von fünf Wochen bei 37% der Preise auf Schwankungen, wobei die meisten Preise sich nur wenige Male änderten, einige wenige jedoch bis zu 32 Mal. Die Höhe der Schwankungen reichte von wenigen Prozenten bis zu gewaltigen Preisunterschieden, beispielweise 220 EUR Preisunterschied bei einem Handy je nach Tageszeit. Die Bundesregierung (Deutscher Bundestag 2019) schätzt aufgrund publizierter Studien, dass die Schwankungen der Onlinepreise zwischen 40 bis 60 Prozent liegen. Laut Managementberatung PwC (August 2019) haben 39 Prozent der Unternehmen fluktuierende Preise – über die Hälfte mit Anpassungen bis zehn Prozent, weitere 30 Prozent der Anbieter um 25 Prozent. Gemäß einer eigenen Umfrage hält „die Mehrheit der Deutschen … dynamische Preise für vertretbar, sofern sich diese nicht ständig ändern. Am größten ist die Akzeptanz in der Altersgruppe der 18- bis 40-Jährigen, die regelmäßig online shoppt und schwankende Preise aus dem E-Commerce längst gewohnt ist.“ (ibid.).

Für die Unternehmen liegen die Vorteile von dynamischen Preisen darin, dass sie schnell auf Wettbewerber reagieren können. Ebenso kann auf eine schwankende Nachfrage, beispielsweise für saisonale oder zeitsensitive Produkte, reagiert werden, ungewollte Lagerbestände oder Überkapazitäten können abgebaut werden; die Zahlungsbereitschaft der Konsumenten wird voll ausgenutzt, die „Konsumentenrente“ abgeschöpft. In der Regel sind die zeitlichen Preissetzungen vom Konsumenten nicht vorhersehbar, was zu einer erheblichen Verunsicherung und auch Verärgerung führen kann. Verbraucherinnen und Verbraucher sehen laut Erhebungen der Verbraucherzentralen dynamische Preise daher eher kritisch (Dautzenberg et al. 2018). Vor allem der Wegfall eines gültigen **Referenzpreises** wird als Nachteil betrachtet sowie die **fehlende Preistransparenz**, die während des Such- und Kaufprozesses zu einem erheblichen Mehraufwand führen kann. Außerdem empfinden viele Verbraucherinnen und Verbraucher dynamische Preise als **unfair**, auch wenn sie selbst persönlich von niedrigeren Preisen profitieren können. Händler tragen daher das Risiko, dass Kundinnen und Kunden ihr Vertrauen verlieren und die Wahrscheinlichkeit eines Wiedereinkaufes sinkt.

Herausforderungen

- Die hohe Dynamik der Preisgestaltung im Internet macht es Verbraucherinnen und Verbrauchern schwer, abzuschätzen, welcher Preis tatsächlich den Wert des Produktes darstellt. Dies kann ggf. der Funktionsfähigkeit von Märkten schaden. Ähnliches ist auch bei den Spritpreisen zu beobachten, weshalb das Bundeskartellamt (die Markttransparenzstelle für Kraftstoffe) selbst erhobene Preisdaten der Tankstellen an Verbraucher-Informationsdienste (Apps) weitergibt, um so die Markttransparenz zu erhöhen.
- Die mangelnde Flexibilität von Konsumenten könnte ausgenutzt werden, etwa wenn sie zeitlich nicht flexibel sind aufgrund von Berufstätigkeit und zu den systematisch „teuren Zeiten" einkaufen müssen. Dies gilt vor allem bei dynamischen Preisen im stationären Einzelhandel, die zunehmend eingeführt werden.
- Die Verbraucherpreisstatistik steht vor der Herausforderung, die Preisentwicklung weiterhin repräsentativ zu erfassen, beispielsweise für den deutschen Verbraucherpreisindex, eine wichtige Kenngröße der Wirtschaftspolitik (Blaudow & Burg 2018).

Verbraucherpolitische Forderungen

- Um die Möglichkeit von Preisvergleichen und einer preislichen Orientierung zu ermöglichen, sollte ein Referenzpreis angegeben werden (beispielsweise im E-Commerce durch Angaben, die erscheinen, wenn man die Maus über die Preisangabe zieht, sog. „mouse-over" Angaben).
- Der Aufwand, das günstigste Angebot zu finden, steigt; dies kann sozial ungerecht sein und muss zumindest debattiert werden.
- Aktive Information und Erklärung der Anbieter, welche Preise dynamisch sind und was dies bedeutet.
- Eine gute Wettbewerbspolitik, die Monopolbildung vermeidet; dynamische Preise werden zum marktwirtschaftlichen Problem, wenn wenig Wettbewerb herrscht.

Was können Verbraucher tun?

- Kontinuierliches Beobachten und Vergleichen von Preisen über einen längeren Zeitraum, auch zu unterschiedlichen Tageszeiten, um Referenzpreise und günstige Zeitpunkte zu lernen.
- Extreme Schwankungen den Marktwächtern der Verbraucherzentralen melden.
- Grundsätzlich Browserverlauf und Cookies löschen. Nicht als eingeloggter Nutzer suchen, sondern erst einloggen, wenn das Produkt gekauft wird. Wenn möglich mit verschiedenen Endgeräten stöbern.

Was sagt das Verbraucherrecht?

Vertragsrecht

Dynamische Preise sind nicht verboten. Gewerbetreibende können ihre Preise grundsätzlich beliebig festsetzen (Rott 2019). Anders als bei personalisierten Preisen werden die Unternehmer in der neu gefassten Verbraucherrechts-Richtlinie nicht verpflichtet, dem Verbraucher dynamisierte Preise anzuzeigen. Das ist im 45. Erwägungsgrund ausdrücklich klarstellt.

Kartellrecht

Grenzen der dynamischen Preisfestsetzung ergeben sich aus dem Kartellrecht, ohne dass es jedoch eine etablierte Kontrollpraxis gäbe. Besonders relevant ist der Einsatz von dynamischen Preisanpassungsalgorithmen, wenn sich dahinter eine Preisabsprache oder ein aufeinander abgestimmtes Verhalten verbirgt (§ 1 GWB und Art. 101, AEUV - Vertrag über die Arbeitsweise der Europäischen Union). Ezrachi und Stucke (2017) haben drei problematische Szenarien ausgearbeitet: Preisalgorithmen werden eingesetzt, um eine zuvor getroffene Preisabsprache durchzusetzen;

Konkurrenten setzen Preisalgorithmen und Datensätze desselben Drittanbieters ein, konkurrierende Anbieter greifen auf eigene Algorithmen zurück, ohne dass nachgewiesen werden kann, dass die relevanten Informationen von einem gemeinsamen Drittanbieter gesammelt, gebündelt und verglichen werden (vgl. Ebers 2020).

Lauterkeitsrecht

Eine Eindämmung dynamischer Preise ist unter Umständen auch über das Lauterkeitsrecht möglich. Potenziell irreführende Handlungen können sich auf das Wissen stützen, das durch die Verwendung von KI generiert wird. Wenn ein Gewerbetreibender bspw. durch den Einsatz von KI herausfindet, dass dem Verbraucher die Zeit für den Kauf eines Flugtickets ausgeht, und fälschlicherweise behauptet, dass nur noch wenige Tickets verfügbar sind, könnte dies gegen das Lauterkeitsrecht (Art. 6 Abs. 1 lit. a und Nr. 7 des Anhangs I UGP-RL verstoßen; Leitlinien der EU-Kommission). Eine weitere Herausforderung stellen irreführende Rabattansprüche dar, die durch die wachsende Verbreitung personalisierter und dynamischer Preise noch komplizierter werden.

Belege und weiterführende Literatur

Blaudow, C., & Burg, F. (2018). Dynamische Preissetzung als Herausforderung für die Verbraucherpreisstatistik. *Statistisches Bundesamt WISTA*, (2), 11–22.

Dautzenberg, K., Gaßmann, C., Groß, B., Müller, F., Neukamp, D., Schmidtke, L., & Bodenstein, U. (2018). *Dynamische Preisdifferenzierung im deutschen Online-Handel* (Eine Untersuchung der Verbraucherzentralen). Potsdam: Verbraucherzentrale Brandenburg. https://www.vzbv.de/sites/default/files/downloads/2020/01/29/marktwaechter-untersuchung-individualisierte-preisdifferenzierung.pdf

Deutscher Bundestag. (2019). *Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Thomas L. Kemmerich, Michael Theurer, Reinhard Houben, weiterer Abgeordneter und der Fraktion der FDP – Drucksache 19/8654 – Auswirkungen von dynamischen und personalisierten Preisen* (Drucksache Nr. 19/9772). Berlin: Deutscher Bundestag. http://dipbt.bundestag.de/doc/btd/19/097/1909772.pdf

Ebers, M. (2020 im Erscheinen). § 3 Regulierung von KI und Robotik. In M. Ebers, C. Heinze, T. Krügel, & B. Steinrötter (Hrsg.), *Künstliche Intelligenz und Robotik* (1. Aufl.). München: C. H. Beck.

Europäische Kommission. (2016). *Leitlinien zur Umsetzung/Anwendung der Richtlinie 2005/29/EG über unlautere Geschäftspraktiken* (Nr. SWD(2016) 163 final). Brüssel: Europäische Kommission. https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A52016SC0163

Ezrachi, A., & Stucke, M. E. (2017). Artificial intelligence and collusion. When computers inhibit competition. *University of Illinois Law Review*, *2017*(5), 1775–1810.

Genth, S., Schleusener, M., Kenning, P., Pohst, M., Remmel, J., Weber, B., et al. (2016). Dynamische Preissetzung — Wer profitiert? *Wirtschaftsdienst*, *96*(12), 863–882. https://doi.org/10.1007/s10273-016-2065-2

Krämer, A. (2020). Dynamische und individuelle Preise aus Unternehmens- und Verbrauchersicht. In R. Kalka & A. Krämer (Hrsg.), *Preiskommunikation: Strategische Herausforderungen und innovative Anwendungsfelder* (S. 89–106). Wiesbaden: Springer Fachmedien Wiesbaden. https://doi.org/10.1007/978-3-658-28028-4_5

Micklitz, H.-W., Namyslowska, M., & Jablonowska, A. (2020 im Erscheinen). § 6 KI und Verbraucherrecht. In M. Ebers, C. Heinze, T. Krügel, & B. Steinrötter (Hrsg.), *Künstliche Intelligenz und Robotik* (1. Aufl.). München: C. H. Beck.

PwC. (August 2019). Sales Radar: Dynamic Pricing. *PwC*. https://www.pwc.de/de/managementberatung/sales-radar-dynamic-pricing.html. Abgerufen 3. August 2020.

Reisch, L. A., Büchel, D., Joost, G., & Zander-Hayat, H. (2016). *Digitale Welt und Handel. Verbraucher im personalisierten Online-Handel* (Veröffentlichungen des Sachverständigenrats für Verbraucherfragen). Berlin: Sachverständigenrat für Verbraucherfragen beim Bundesministerium der Justiz und für Verbraucherschutz. https://www.bmjv.de/SharedDocs/Downloads/DE/News/Artikel/01192016_Digitale_Welt_und_Handel.pdf?__blob=publicationFile&v=2

Rott, P. (2019). Dynamische und personalisierte Preise zwischen Vertragsfreiheit und Willkür. In C. Ochs, M. Friedewald, T. Hess, & J. Lamla (Hrsg.), *Die Zukunft der Datenökonomie: Zwischen Geschäftsmodell, Kollektivgut und Verbraucherschutz* (S. 285–305). Wiesbaden: Springer Fachmedien Wiesbaden. https://doi.org/10.1007/978-3-658-27511-2_13

Schleusener, M. (2016). Dynamisch und personalisiert: Wie entwickelt sich die Preissetzung im Online-Handel? *Wirtschaftsdienst*, *96*(12), 868–871. https://doi.org/10.1007/s10273-016-2065-2

Spann, M., & Skiera, B. (2020). *Dynamic pricing in a digitized world* (Discussion Paper Nr. 248). München, Berlin: Collaborative Research Center Transregio 190. https://rationality-and-competition.de/wp-content/uploads/2020/06/248.pdf

Verbraucherzentrale Bremen. (4. Februar 2020). Unterschiedliche Preise im Netz. *Verbraucherzentrale Bremen*. https://www.verbraucherzentrale.de/en/node/28618. Abgerufen 10. Juni 2020

Ethikregeln für Künstliche Intelligenz (KI) – Label für Ethische KI

Was bedeutet „ethische KI“?

Im Leben von Verbraucherinnen und Verbrauchern spielen KI und **algorithmische Systeme** (oder kurz: Algorithmen) eine immer größere Rolle. In vielen technischen Geräten und elektronischer Kommunikation stecken Algorithmen: das Navigationssystem, das den kürzesten Weg zur Arbeit vorschlägt, die Rechtschreibprüfung in Textverarbeitungsprogrammen, die Partnervorschläge beim Online-Dating und die personalisiert angebotene Werbung auf Facebook sind nur einige Beispiele für Algorithmen in unserem Alltag. Alle in diesem Booklet zusammengestellten Themen und Anwendungen basieren auf KI und Algorithmen.

Mit zunehmendem Einsatz von algorithmischen Systemen und KI hat auch die Diskussion über persönliche und gesellschaftliche Auswirkungen zugenommen. Die Bundesregierung hat zur Stärkung ihrer Strategie Künstliche Intelligenz (Bundesregierung 2018) eine Datenethikkommission (2019) eingesetzt, die neben Datenschutz und -sicherheit die KI-basierten algorithmischen Systeme in den Mittelpunkt gestellt hat. Die Ethikkommission hat klare Vorschläge gemacht, wie eine so tiefwirkende Technologie, die auch in sensiblen Lebensbereichen zum Einsatz kommt, ethisch, rechtlich, kulturell und institutionell eingebettet werden könnte, „so dass gesellschaftliche Grundwerte und individuelle Grundrechte gewahrt werden“ (Bundesregierung 2018, S. 4). Letztlich ist es eine politische Aufgabe, mit allen Akteuren gemeinsam dafür zu sorgen, dass algorithmische Systeme zum **Wohle der Gesellschaft** gestaltet werden.

Die Datenethikkommission (2019, S. 17-18) formuliert acht grundsätzliche Anforderungen an Algorithmische Systeme:

1. menschenzentriertes Design (die Maschine dient dem Menschen, nicht andersherum)
2. Vereinbarkeit mit gesellschaftlichen Grundwerten (u.a. demokratische Willensbildung, digitale Souveränität)
3. Nachhaltigkeit (u.a. gesellschaftliche Teilhabe, Umweltschutz)
4. Qualität und Leistungsfähigkeit (Zuverlässigkeit)
5. Robustheit und Sicherheit (nach außen gegen Hacker und nach innen)
6. Minimierung von Verzerrungen und Diskriminierung (keine Biases, keine eingebaute oder antrainierte Diskriminierung)
7. Transparenz, Erklärbarkeit, Nachvollziehbarkeit (Informationen zur Algorithmenkontrolle und ggf. Wahrnehmung von Rechten)
8. Klare Rechenschaftsstrukturen (Verantwortung, ggf. Haftung)

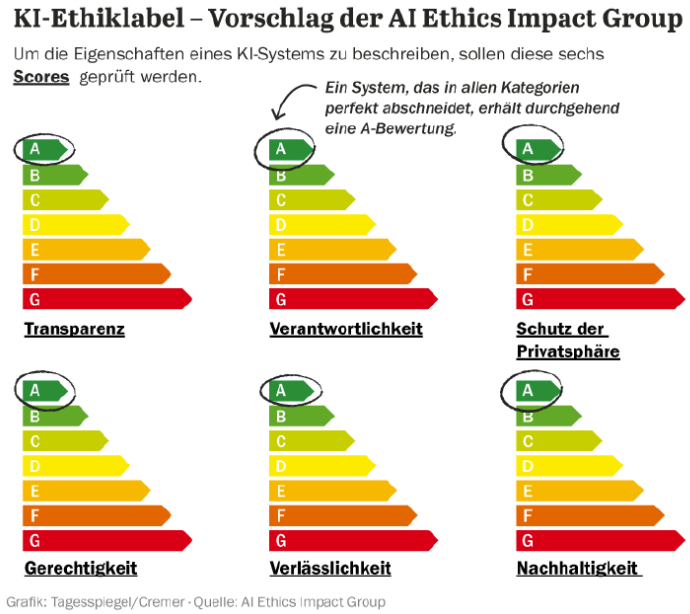
Praktische Hinweise, wie solche Anforderungen umgesetzt werden können, hat iRights.Lab gemeinsam mit der Bertelsmann Stiftung entwickelt. Im Kern stehen neun **Algo.Rules** (https://algorules.org/de/startseite, 2020), die bereits bei der Entwicklung mitgedacht und eingebaut werden sollten: Kompetenz aufbauen, Verantwortung definieren, Ziele und erwartete Wirkung dokumentieren, Sicherheit gewährleisten, Kennzeichnung durchführen, Nachvollziehbarkeit sicherstellen, Beherrschbarkeit absichern, Wirkung überprüfen, Beschwerden ermöglichen. Dabei werden diese Regeln gemeinsam mit der Zivilgesellschaft und allen interessierten Akteuren ständig weiterentwickelt und verfeinert. Speziell für Verbraucher ohne besonderes Technikinteresse ist der Vorschlag eines **Labels für vertrauenswürdige KI** wegweisend (https://irights-lab.de/kiethiklabel/), und wird auch von anderen Akteuren ins Spiel gebracht (siehe unten).

Die demokratieverträgliche und verbraucherfreundliche Einbettung der Algorithmen in Regeln kann jedoch nur begrenzt eine nationale Aufgabe sein; vielmehr ist diese auf europäischer und ggf. supranationaler Ebene zu gestalten. Die EU-Kommission hat daher u.a. eine unabhängige Hochrangige Expertengruppe für Künstliche Intelligenz (HEG-KI 2018) eingesetzt, die „**Ethik-Leitlinien für eine vertrauenswürdige KI**“ erarbeitet hat. Danach soll KI „ethisch, robust und rechtmäßig“ sein (ebenda).

All diese Leitlinien unterscheiden sich zwar in Schwerpunkt und Detail; letztlich geht es aber immer darum, die Beziehung zwischen **Mensch und Maschine** zu regeln, wenn Handlungen und Entscheidungen zunehmend auf algorithmische Systeme verlagert werden. Dabei kann man drei Stufen unterscheiden: Entscheidungen, die auf Algorithmen basieren und diese dadurch eher verbessern; Entscheidungen, die durch Algorithmen stark beeinflusst werden; sowie solche, die menschliche Entscheidungen ersetzen. Es liegt auf der Hand, dass hier unterschiedliche Anforderungen gestellt werden. Die Datenethikkommission (2019, S. 18-19) schlägt daher vor, die Regelung von Algorithmen vor allem an der Frage festzumachen, wie hoch das **Risiko eines Schadens** ist, den KI anrichten kann, wie potentiell kritisch der Einsatz also ist. Ist die mögliche Schädigung unvertretbar, sollte der KI-Einsatz verboten werden; sind die Risiken aber gering, bedarf es keiner besonderen Regulierung. Diese Eischätzung kann natürlich nicht der Verbraucher treffen.

KI-Ethiklabel

Der Vorschlag eines Verbraucherlabels für „ethische KI“, stößt zunehmend auf Interesse. Auch die Europäische Kommission (2020) schlägt in ihrem Weißbuch zur künstlichen Intelligenz ein Label als eine Möglichkeit einer **freiwilligen Kennzeichnung für KI-Anwendungen ohne hohes Risiko** vor. In Anlehnung an Design und Optik des europäischen Energieeffizienzlabels, das sich (mehrfach verbessert) für Verbraucher als nützliches Informationsinstrument erwiesen hat, hat ein Konsortium aus Industrie, Wissenschaft und Stiftungen (**AI Ethics Impact Group**, Hallensleben & Hustedt 2020) einen Vorschlag für ein KI-Ethiklabel entwickelt. Das KI-Ethiklabel erfasst sechs zentrale Werte oder Scores: Transparenz, Verantwortlichkeit, Schutz der Privatsphäre, Gerechtigkeit, Verlässlichkeit und Nachhaltigkeit. Das Label macht eine Einstufung in Gruppen von A bis G möglich.



Quelle: Hallensleben & Hustedt (2020)

Welche Einstufung die jeweils richtige ist bzw. welche Anforderungen an einen Algorithmus notwendig sind, damit die Hard- oder Software eine bestimmte Stufe auf den Scores (A-G) erreicht, kann durch die sogenannte WKIO-Methode (Wert, Kriterium, Indikator, Observable, d.h. Messwert) bestimmt werden. Die sechs Scores werden jeweils mit Kriterien, Indikatoren, und Messgrößen konkretisiert die zur Einstufung führen (Hustedt & Fetic, 2. April 2020).

Noch ist das Label nicht auf dem Markt. Es hat aber grundsätzlich das Potential, Nutzern eine einfache und verlässliche Entscheidungsgrundlage an die Hand zu geben und damit die individuelle Risikoabwägung zu ermöglichen. Gleichzeitig macht es „Ethik“ als Wettbewerbsfaktor für Märkte sichtbar und kann so Unternehmen zur Entwicklung verbrauchergerechter algorithmischer Systeme

ermuntern. Diese Doppelwirkung von Labels könnte man sich in diesem neuen, so wichtigen Markt zunutze machen. Labels vermitteln ihre Aussage offensichtlich deutlicher als seitenlange Informationsbroschüren. Ein „Informations-Dschungel“ sorgt schnell für Wegschauen und Informationsvermeidung, wohingegen Labels eingängig sind und niedrigschwellige Information bieten.

Was sagt das Verbraucherrecht?

Ethik und Verbraucherrecht

Ethische Maßstäbe leiten das Recht an. Sie formulieren Grundsätze – so wie die der Datenethikkommission – die in das Recht übersetzt werden müssen. Praktische Bedeutung erlangen sie im Wege der Konkretisierung der rechtlichen Rahmenbedingungen ökonomischen und politischen Handelns. Aus Verbrauchersicht von herausragender Bedeutung sind die vielfältigen Angriffe algorithmisch gesteuerter Techniken und Geräte auf die **Entscheidungsautonomie**. Das Verbraucherrecht wird vom Informationsparadigma beherrscht. 30 Jahre Verbraucherrecht haben zu umfassenden Informationspflichten geführt, die sämtlich einem Ziel dienen: die Autonomie der Verbraucher zu erhalten und zu stärken. Soweit empirische Erkenntnisse über den Einsatz von Algorithmen in der Wirtschaft überhaupt existieren, zeigen sie überdeutlich die strukturellen Defizite dieses Regulierungsansatzes. Jeden Tag willigen wir ein, Daten von uns zu speichern und zu verarbeiten, ohne dass wir überhaupt wissen *können*, was mit diesen Daten geschieht. Die bisherigen Regelungen des Datenschutzrechts, aber auch des AGB-Rechts, des Lauterkeitsrechts oder allgemeiner des Verbraucherinformationsrechts zeigen sich den Herausforderungen der Digitalisierung kaum gewachsen.

Ethikrichtlinien und Empfehlungen

Deutschland ebenso wie andere Staaten, die Organe der EU, die internationalen Organisationen wie die OECD, die Vereinten Nationen und schließlich die Selbstregulierung auf nationaler und internationaler Ebene haben vielfältige Ethikrichtlinien und Empfehlungen erarbeitet und zur Anwendung empfohlen. Oben sind einige Beispiele skizziert. Auch an einschlägigen Kommissionen auf nationaler, europäischer und internationaler Ebene besteht kein Mangel (Übersicht bei Ebers 2020). Diese Richtlinien und Empfehlungen überschneiden sich in ihren Inhalten, was nicht heißen soll, dass nicht beträchtliche Unterschiede zwischen den Ländern, innerhalb der Organe der EU; in den internationalen Organisationen und selbst innerhalb der Selbstregulierung der Wirtschaft bestehen. Aus Verbrauchersicht allein entscheidend ist, welche **Kontrollmechanismen** diese Richtlinien und Empfehlungen vorsehen, wie ihre Einhaltung überwacht wird und von wem, schließlich ob die Ergebnisse öffentlich gemacht werden. Die Erfahrungen im Umgang mit unverbindlichen Regeln stimmen eher skeptisch. Richtlinien und Empfehlungen mögen geeignet sein, die gröbsten Missbräuche zu beseitigen, doch darum geht es in der Datenethik nicht allein. Die sehr grundsätzlichen Fragen der Mensch-Technik und Mensch-Maschine Beziehung harren einer regulatorischen Antwort.

Rechtspolitische Vorschläge

Der Sachverständigenrat für Verbrauchfragen (SVRV) hat 2016 ein **Gutachten zum Verbraucherrecht 2.0** vorgelegt, das zentrale Forderungen formuliert. Im Zentrum steht die Forderung, schon bei der Entwicklung von Algorithmen zentrale Vorgaben des Rechts zu berücksichtigen. Der SVRV empfiehlt,

> dass durch rechtliche Vorgaben sichergestellt werden muss, dass Algorithmen die Vorgaben des Verbraucherrechts, des Datenschutzrechts, des Anti-Diskriminierungsrechts und der digitalen Sicherheit berücksichtigen. Die zugrundeliegenden Parameter sind bei Algorithmen mit direktem Verbraucherkontakt transparent zu machen. Auch bei selbst-lernenden Algorithmen muss die rechtliche Verantwortlichkeit zuzuordnen sein und geltende Regelungen zum Konsumentenschutz müssen gewahrt bleiben;

- dass Algorithmen durch standardisierte Offenlegungspflichten einem Kreis von Experten der Digitalagentur offengelegt werden, die per Stichprobe die rechtliche Unbedenklichkeit überprüfen. Hierzu sind standardisierte Verfahren des Software Engineering zu entwickeln;
- daneben die Unternehmen zur Ausarbeitung eines Code of Conduct über die Verwendung von personenbezogenen Daten, künstlich intelligenter Systeme und der Big Data-Analyse aufzufordern.

Generalklauseln im Recht

Solange der Gesetzgeber nicht handelt, auf welcher Ebene auch immer, bleibt es letztendlich den Gerichten überlassen, die politisch formulierten ethischen Bedenken in das existierende Recht zu integrieren, soweit das überhaupt möglich ist. Wenn überhaupt geschieht dies über Generalklauseln, die sich im Datenschutzrecht wie auch im Verbraucherrecht finden. An Hand von Treu und Glauben, von Fairness, von Transparenz und den guten Sitten müssen Gerichte situativ beurteilen, ob bestimmte kommerzielle Praktiken und Allgemeine Geschäftsbedingungen mit dem Datenschutzrecht, dem Lauterkeitsrecht oder dem AGB-Recht vereinbar sind.

Belege und weiterführende Literatur

Bundesregierung. (2018). Nationale Strategie für Künstliche Intelligenz. https://www.ki-strategie-deutschland.de/home.html. Abgerufen 14. August 2020

Datenethikkommission der Bundesregierung. (2019). *Gutachten der Datenethikkommission der Bundesregierung*. Berlin: Bundesministerium des Innern, für Bau und Heimat. https://www.bmjv.de/SharedDocs/Downloads/DE/Themen/Fokusthemen/Gutachten_DEK_DE.pdf?__blob=publicationFile&v=2. Abgerufen 1. Juni 2020

Ebers, M. (2020 im Erscheinen). § 3 Regulierung von KI und Robotik. In M. Ebers, C. Heinze, T. Krügel, & B. Steinrötter (Hrsg.), *Künstliche Intelligenz und Robotik* (1. Aufl.). München: C. H. Beck.

Europäische Kommission. (2020). *Weissbuch zur Künstlichen Intelligenz –ein europäisches Konzept für Exzellenz und Vertrauen* (Nr. COM(2020) 65 final). Brüssel: Europäische Kommission. https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_de.pdf

Hallensleben, S., & Hustedt, C. (2020). *From principles to practice: An interdisciplinary framework to operationalise AI ethics*. Gütersloh: Bertelsmann Stiftung. https://www.bertelsmann-stiftung.de/fileadmin/files/BSt/Publikationen/GrauePublikationen/WKIO_2020_final.pdf

Hochrangige Expertengruppe für künstliche Intelligenz. (2019). *Ethik-Leitlinien für eine vertrauenswürdige KI*. Brüssel: Europäische Kommission. https://doi.org/10.2759/22710

Hustedt, C., & Fetic, L. (2. April 2020). From principles to practice: Wie wir KI-Ethik messbar machen können. *Algorithmenethik*. https://algorithmenethik.de/2020/04/02/from-principles-to-practice-wie-wir-ki-ethik-messbar-machen-koennen/. Abgerufen 14. August 2020

iRights.Lab. (2. April 2020). Ethik auf den ersten Blick: Das KI-Ethik-Label. Ein KI-Ethik-Label als Entscheidungshilfe für ethische KI-Systeme. https://irights-lab.de/kiethiklabel/. Abgerufen 14. August 2020

Levina, O. (14. Januar 2020). Künstliche Intelligenz und Ethik. *Informatik Aktuell*. https://www.informatik-aktuell.de/betrieb/kuenstliche-intelligenz/kuenstliche-intelligenz-und-ethik.html, https://www.informatik-aktuell.de/betrieb/kuenstliche-intelligenz/kuenstliche-intelligenz-und-ethik.html. Abgerufen 14. August 2020

Micklitz, H.-W., Namyslowska, M., & Jablonowska, A. (2020 im Erscheinen). § 6 KI und Verbraucherrecht. In M. Ebers, C. Heinze, T. Krügel, & B. Steinrötter (Hrsg.), *Künstliche Intelligenz und Robotik* (1. Aufl.). München: C. H. Beck.

Sachverständigenrat für Verbraucherfragen. (2016). *Verbraucherrecht 2.0. Verbraucher in der digitalen Welt* (Gutachten des Sachverständigenrats für Verbraucherfragen). Berlin: Sachverständigenrat für Verbraucherfragen beim Bundesministerium der Justiz und für Verbraucherschutz. https://www.svr-verbraucherfragen.de/wp-content/uploads/Gutachten_SVRV-.pdf

Schwintowski, H.-P. (2017). Big Data – Rechtliche Rahmenbedingungen müssen grundlegend verbessert werden. *Verbraucher und Recht*, (12), 455–463.

Informationsseiten

https://irights-lab.de/kiethiklabel/

https://algorithmenethik.de/

https://algorules.org/de/startseite

Identitätsdiebstahl

Was ist digitaler Identitätsdiebstahl?

Bei dieser Form der Cyberkriminalität missbrauchen Kriminelle im Internet gestohlene personenbezogene Daten und Fotos. Genau genommen, handelt es sich um Identitäts**missbrauch** und nicht „-diebstahl“. Die direkte Übersetzung des englischsprachigen Begriffes „identity theft“ hat sich aber auch bei uns eingebürgert, denn in den USA steht dieses Problem schon seit Jahrzehnten ganz oben auf der Agenda der Verbraucherschützer.

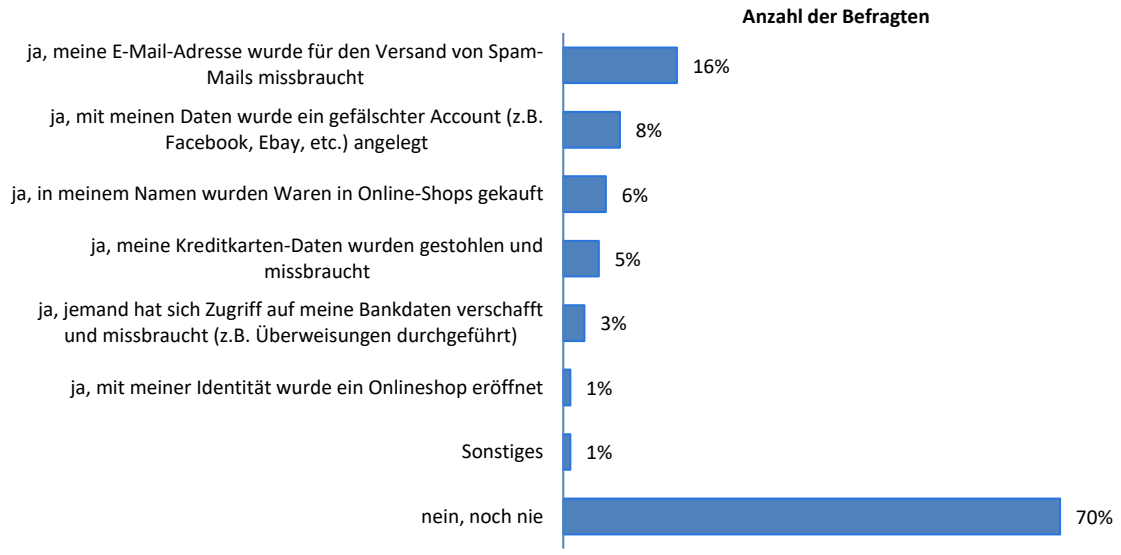
Mit der **digitalen Identität** der bestohlenen Person können finanzielle Vorteile erzielt, Straftaten begangen und Rufschädigung oder Mobbing betrieben werden. Zur digitalen Identität gehören die personenbezogenen Daten der Nutzer sowie alle Arten von Nutzer-Accounts – und damit auch der Zugang zu E-Government Daten, E-Commerce und sämtlicher Kommunikation. Mit den echten oder gefälschten **Nutzerprofilen** werden kompromittierende Inhalte geteilt; oder es werden Notfallsituationen vorgetäuscht und um Unterstützung gebeten. Im Namen anderer können so online und offline Straftaten begangen werden, wie der Kauf von Drogen und illegalen Waffen oder die Unterstützung terroristischer Netzwerke. Hierher gehören auch die sogenannte „Deep Fakes“ (siehe Virtuelle und Erweiterte Realität).

Für kleinere Betrügereien sind sogar nur wenige Daten notwendig: Mit dem Namen und dem Geburtsdatum einer Person kann man im Online-Handel Waren bestellen und an abweichende Lieferadressen, wie z.B. eine Paketstation, liefern lassen. Die angeblichen Käufer erhalten dann Rechnungen und Mahnungen über Waren, die sie nicht bestellt und nicht erhalten haben. Weitere Facetten sind Mobilfunkverträge, die im Namen der bestohlenen Person abgeschlossen werden oder Kontoeröffnungen, mit denen Kreditkarten bestellt und dann überzogen werden.

Verbreitung

Für 2018 zeigt eine repräsentative Befragung (Statista 2019), dass bereits 30% der Befragten in Deutschland auf verschiedene Weise Opfer von Daten- und Identitätsmissbrauch geworden sind.

Waren Sie schon einmal von Identitätsdiebstahl betroffen, hat also schon einmal jemand Ihre persönlichen Daten missbräuchlich genutzt und Ihnen Schaden zugefügt?



Hinweise: Deutschland; 08. bis 14.08.2018; ab 18 Jahre; 1025 Befragte; Mehrfachnennungen waren möglich.
Quelle: Statista (2019), verfügbar über Statista (ID 953397)

Nach einer Eurobarometer-Umfrage (Europäische Kommission 2018) haben etwa ein Drittel der Deutschen (33%) bereits betrügerische Emails erhalten und 38% haben auf ihren Geräten Schadsoftware entdeckt. Etwas seltener wurde der Account Sozialer Netzwerke gehackt (8%), und direkt von Identitätsdiebstahl betroffen waren demnach „nur“ 5% der Befragten. Auch wenn das digitale Abgreifen von Daten für viele Bürgerinnen und Bürger wenig fassbar ist, sind doch viele verunsichert. 55% der Deutschen geben in der Eurobarometerumfrage (2018) an, sie hätten (große) Angst vor einem Identitätsdiebstahl. In den USA ist das Problem schon deutlich länger akut und stärker verbreitet. Aber auch in Deutschland steigen die Betrugszahlen. Das BSI warnte bereits 2018, Identitätsdiebstähle erreichten immer neue Größenordnungen und auf dem IT-Schwarzmarkt würden Milliarden erbeuteter digitaler Identitäten gehandelt.

Quelle: Zindler & Bolz (2019, S. 4).

Eine der bekanntesten Methoden für den Diebstahl digitaler Identitäten ist das so genannte **Phishing**. Das aus den Worten Passwort und Fishing zusammengesetzte Wort beschreibt das Abfischen von Passwörtern und Zugangsdaten. Hierbei werden Spam-Mails im Namen seriöser Banken oder Internetanbieter versendet. Die Mails fordern dazu auf, über einen Link eine Webseite zu besuchen und dort persönliche Daten zu aktualisieren oder wegen eines Sicherheitsvorfalls das Passwort zu ändern. Sowohl die Phishing-Mail als auch die dazugehörige Webseite sind dabei heute meist sehr professionell gestaltet und nur schwer von originalen Mails, z.B. der Sparkasse oder Amazon, zu unterscheiden. Durch die große Masse der versendeten Spam-Mails können Betrüger davon ausgehen, tatsächlich einige Kunden zu erreichen, welche dann die genannten Schritte ausführen.

Posts in sozialen Netzwerken können auf gefälschte Webseiten führen, hier meist von bekannten Markenanbietern. Auch über Mails oder Webseiten wird Schadsoftware verbreitet, die unbemerkt vom Benutzer auf seinen Geräten installiert wurde und als Hintergrundprogramm Online-Eingaben mitliest, speichert und an die Täter übermittelt. Über gefälschte Job-Inserate werden Bewerberinnen und Bewerber dazu aufgefordert, sich per Video-Ident-Verfahren zu identifizieren. Dabei eröffnen sie aber unbewusst ein Konto, welches dann für kriminelle Zwecke, z.B. Fakeshops, missbraucht werden kann. Das Bundeskriminalamt BKA warnt zudem vor dem sogenannten „War-driving“. Dabei suchen die Täter aktiv nach ungeschützten WLAN-Netzwerken, um die Daten aller am WLAN-Router angeschlossenen Computer abgreifen zu können.

Herausforderungen

> Betroffene bemerken den Identitätsdiebstahl meist nicht sofort; wenn sie davon erfahren, ist meist schon Schaden an verschiedenen Stellen entstanden. Alle Unternehmen, Banken und

Auskunfteien müssen über den Diebstahl benachrichtigt werden. Jede Forderung muss bei der Polizei angezeigt werden. Nur so können die Forderungen der Gläubiger zurückgewiesen werden.

- Wenn die Forderungsschreiben der getäuschten Firmen ignoriert werden, besteht das Risiko, dass falsche Daten bei Auskunfteien eingetragen werden, welche die Kreditwürdigkeit auf lange Zeit belasten. Falsche Daten sollten deshalb überall gelöscht werden, auch wenn das mühsam ist (siehe Verbraucher-Scoring).
- Dass Nutzer durchaus viel für die Sicherheit ihrer digitalen Identität tun können, zeigt sich an den in den letzten Jahren rückläufigen Zahlen im Bereich des Phishings im Online-Banking. Entsprechende TAN-Verfahren und doppelte Identifizierung sind zwar etwas zeitaufwendiger, steigern jedoch die Sicherheit enorm. Das Thema Identitätsdiebstahl und wie man ihn vermeidet wird noch zu wenig aktiv kommuniziert. Denkbar wäre auch, dass Anbieter Sicherheitsoptionen qua Voreinstellung als Standard einrichten.

Das können Verbraucher tun

- Auf Phishing-Mails achten. Betrügerische Emails können anhand einiger Merkmale erkannt werden: gefälschte Absender-Adresse; Aufforderung zur Eingabe vertraulicher Informationen; vorgetäuschter dringender Handlungsbedarf oder Androhungen; Links zu anderen Webseiten; unpersönliche Anrede und sprachliche Ungenauigkeiten.
- Auf Phishing-Webseiten achten: Die Abkürzung "https://" im Internetadressfeld des Browsers bedeutet heute nicht mehr, dass die Adresse für eine gesicherte Verbindung und folglich für eine vertrauenswürdige Website steht. Die Internetadresse enthält zwar den Namen der angegebenen Institution, aber nur in Verbindung mit merkwürdigen Zahlen oder Buchstabenkombinationen.
- Auf die Verwendung möglichst neutraler Passwörter achten. Vermeidung von Single-Sign-Ons, d.h. sich mit den Zugangsdaten sozialer Netzwerke oder einem Amazon-Konto bei weiteren Webseiten anmelden. Wo es möglich ist, sollte eine Zwei-Faktor-Authentisierung genutzt werden. Für jeden Zugang und jede Webseite ein eigenes Passwort benutzen. Verwenden unterschiedlicher Nutzernamen und wenn möglich unterschiedliche Email-Adressen für verschiedene Zugänge.
- Niemals persönliche Informationen wie Passwörter oder Zugangsdaten über Emails preisgeben. Sich immer fragen: Braucht der Shop oder das Portal meine Identität wirklich und wenn ja, wozu?
- Regelmäßige Kontrolle des Bankkontos, nur so kann schnell auf unbefugte Abbuchungen reagiert werden. Im Ernstfall schnell handeln: Die Bank informieren und betroffenen Konten und Karten sperren lassen. Strafanzeige bei der Polizei stellen.
- Einige Auskunfteien und Online-Banken bieten kostengünstige Sicherheits-Apps für Verbraucherinnen und Verbraucher an (B2C Produkte wie „IdentSafe“), die speziell Identitätsmissbrauch verhindern sollen. Nutzt jemand die eigene Identität, wird man umgehend benachrichtigt und der Missbrauch angezeigt. Auskunfteien speichern auch teilweise Daten über gestohlene Identitäten, um weiteren Missbrauch zu verhindern.

Was sagt das Verbraucherrecht?

Strafrecht

Es gibt kein Verbraucher-Strafrecht, also keine Regeln, die rechtswidriges und schuldhaftes Verhalten eines Unternehmens gegenüber dem Verbraucher unter Strafe stellen. Deshalb ist der Identitätsdiebstahl an den allgemeinen Regeln des Strafrechts zu messen.

Einen eigenständigen Tatbestand für den Identitätsdiebstahl gibt es nicht. Schon der Begriff ist rechtlich nicht richtig, weil ein Diebstahl die Wegnahme einer fremden Sache voraussetzt. Am nächsten kommt dem Sachverhalt (nach §238 Strafgesetzbuch) die sogenannte **Nachstellung**. Danach wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft, wer einer anderen Person in einer Weise unbefugt nachstellt, die geeignet ist, deren Lebensgestaltung schwerwiegend zu beeinträchtigen, indem er beharrlich… unter missbräuchlicher Verwendung von personenbezogenen Daten dieser Person Bestellungen von Waren oder Dienstleistungen für sie aufgibt. Typischerweise dient der Identitätsdiebstahl in der Praxis der Vorbereitung eines **Kreditbetrugs**. Das Bundesamt für Sicherheit in der Informationstechnik, die Verbraucherzentrale Bundesverband und die Verbraucherzentralen der Bundesländer bieten Hilfestellung an (etwa VIS Bayern https://www.vis.bayern.de/daten_medien/datenschutz/identitaetsdiebstahl.htm).

Datenschutzrecht

Nach Art. 33 DSGVO hat der ‚Verantwortliche' im Falle einer Verletzung des Schutzes personenbezogener Daten, also vor allem eines Identitätsdiebstahls, der zuständigen Aufsichtsbehörde unverzüglich und möglichst binnen 72 Stunden zu melden, es sei denn, dass die Verletzung des Schutzes personenbezogener Daten voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt. Erfolgt diese Meldung nicht binnen 72 Stunden, so ist ihr eine Begründung für die Verzögerung beizufügen. Verantwortlich im Sinne des Art. 4 Nr. 7 DSGVO ist die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet. Das Bundesdatenschutzgesetz (BDSG) hat in § Nr. 7 diese Anforderungen weiter konkretisiert.

Belege und weiterführende Literatur

Bundesamt für Sicherheit in der Informationstechnik (BSI). (2018). *Die Lage der IT-Sicherheit in Deutschland 2018*. Bonn: Bundesamt für Sicherheit in der Informationstechnik (BSI). https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/it-digitalpolitik/bsi-lagebericht-2018.pdf?__blob=publicationFile&v=3

Bundesamt für Sicherheit in der Informationstechnik (BSI). (o.J.-a). Identitätsdiebstahl. *BSI für Bürger*. https://www.bsi-fuer-buerger.de/BSIFB/DE/Risiken/ID-Diebstahl/id-diebstahl_node.html. Abgerufen 14. August 2020

Bundesamt für Sicherheit in der Informationstechnik (BSI). (o.J.-b). Passwortdiebstahl durch Phishing. *BSI für Bürger*. https://www.bsi-fuer-buerger.de/BSIFB/DE/Risiken/SpamPhishingCo/Phishing/phishing_node.html. Abgerufen 14. August 2020

Bundesamt für Sicherheit in der Informationstechnik (BSI). (o.J.-c). Schutzmaßnahmen. *BSI für Bürger*. https://www.bsi-fuer-buerger.de/BSIFB/DE/Risiken/ID-Diebstahl/Schutzmassnahmen/id-dieb_schutz_node.html. Abgerufen 14. August 2020

Bundesamt für Sicherheit in der Informationstechnik (BSI). (o.J.-d). Spam, Phishing & Co. *BSI für Bürger*. https://www.bsi-fuer-buerger.de/BSIFB/DE/Risiken/SpamPhishingCo/spamPhishingCo_node.html. Abgerufen 14. August 2020

Bundeskriminalamt (BKA). (2019). *Cybercrime. Bundeslagebild 2018*. Wiesbaden: Bundeskriminalamt. https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrimeBundeslagebild2018.pdf?__blob=publicationFile&v=3

Europäische Kommission. (2019). *Special Eurobarometer 480. Europeans' attitudes towards Internet security*. Brüssel: Europäische Kommission. https://ec.europa.eu/commfrontoffice/publicopinion/index.cfm/ResultDoc/download/DocumentKy/85494

Statista. (2019). *Statista Umfrage Cybersecurity & Cloud 2018*. Hamburg: Statista. https://de.statista.com/prognosen/953397/umfrage-in-deutschland-zu-personen-die-opfer-eines-identitaetsdiebstahls-geworden-sind

Verbraucherzentrale Baden-Württemberg. (31. Juli 2018). Neue Betrugsmasche: Identitätsdiebstahl bei der Jobsuche. *Verbraucherzentrale Baden-Württemberg*. https://www.verbraucherzentrale.de/aktuelle-meldungen/digitale-welt/neue-betrugsmasche-identitaetsdiebstahl-bei-der-jobsuche-28475. Abgerufen 14. August 2020

Verbraucherzentrale Bayern. (12. März 2019). Weltverbrauchertag 2019: Identitätsdiebstahl - die Gefahr im Internet. *Verbraucherzentrale Bayern*. https://www.verbraucherzentrale-bayern.de/pressemeldungen/digitale-welt/phishingradar/weltverbrauchertag-2019-identitaetsdiebstahl-die-gefahr-im-internet-34656. Abgerufen 14. August 2020

Zindler, A., & Bolz, C. (2019). *Digitalbarometer: Bürgerbefragung zur Cyber-Sicherheit* (Kurzbericht zu den Umfrageergebnissen der Polizeilichen Kriminalprävention der Länder und des Bundes (ProPK) und des Bundesamts für Sicherheit in der Informationstechnik (BSI)). Bonn: Bundesamt für Sicherheit in der Informationstechnik (BSI) und Polizeiliche Kriminalprävention der Länder und des Bundes (ProPK). https://www.polizei-beratung.de/fileadmin/Dokumente/Digitalbarometer-Cyber-Sicherheit-Befragung-BSI-ProPK.pdf

Informationsseiten

https://www.klicksafe.de/themen/rechtsfragen-im-netz/irights/identitaetsdiebstahl-im-internet/

https://www.bka.de/DE/UnsereAufgaben/Deliktsbereiche/Cybercrime/cybercrime_node.html

https://www.bsi-fuer-buerger.de/

Legal Tech

Was ist Legal Tech?

Mit „Legal Tech“, der Abkürzung für **Legal Technology**, werden Software und Online-Dienste bezeichnet, die juristische Prozesse unterstützen oder **automatisierte Rechtsdienstleistungen** erbringen. Mithilfe von Algorithmen werden bestimmten Tatbeständen die entsprechenden Rechtsfolgen zugeordnet. Legal Tech kann Verbraucherinnen und Verbraucher bei der Anspruchsdurchsetzung effektiv und einfach unterstützen. Vor allem bei geringen Schadenssummen (sogenannten Streuschäden) überlegen die geschädigten Personen oft, ob es sich überhaupt lohnt, die Zeit einzusetzen, um eigene Ansprüche einzufordern. Manche Unternehmen rechnen mit diesem „rationalen Desinteresse“ ihrer Kundschaft und legen ihre Angebote genau darauf aus. Legal Tech Portale wie flugrechte.de schaffen einen niedrigschwelligen Zugang zu Gericht und helfen damit Verbrauchern, ihre Ansprüche niedrigschwellig und mit geringen Kosten (z. B. Ausfüllen eines Online Formulars) durchzusetzen.

Solange die Voraussetzungen und die Folgen klar geregelt sind, können Legal-Tech-Anwendungen **klare Vorteile** für Verbraucherinnen und Verbraucher sein. Besonders interessant sind solche neuen KI-basierten Legal Tech-Anwendungen der Verbraucherinformatik, die vor allem eine **Informations-** und **Transparenzfunktion** für Verbraucher haben (Reisch et al. 2019). Eine entsprechende Software kann beispielsweise die Verbraucherfreundlichkeit von AGB in Sekunden „scannen“ und bewerten; oder sie kann blitzschnell erkennen, ob im Kleingedruckten bestehende Datenschutzrichtlinien eingehalten werden. Ein Ampelsystem zeigt den Verbrauchern unmittelbar am Bildschirm, ob es ratsam ist, einen Online-Kauf abzuschließen oder nicht. Dies sind angesichts des enormen Informationsnachteils, den Verbraucher gerade im undurchsichtigen Online-Handel haben, sehr große Vorteile.

Anwendungsbereiche

Die Breite der Anwendungen ist weit und reicht von simpler Dokumentenverwaltung bis zu Chatbots, die mit Hilfe von KI ganze Fälle bearbeiten können. Für Verbraucher relevant sind Anbieter mit Geschäftsmodellen für private Rechtsdienstleistungen (B2C) sowie Streitschlichtung (Kind et al. 2019). Ein bekanntes Beispiel verbrauchernaher Legal-Tech-Lösungen ist die Fluggastentschädigung, wo die Tatbestände und Folgen durch EU-Recht klar geregelt sind: Eine bestimmte Verspätung zieht eine bestimmte Entschädigung nach sich. Um diese Ansprüche durchzusetzen, können sich Verbraucherinnen und Verbraucher an Legal-Tech-Portale wenden und ihre Forderungen an sie abtreten. Diese setzen die Forderungen gegenüber der Fluggesellschaft durch und verlangen dafür eine Provision, je nach Anbieter zwischen 23 und 36% der gezahlten Entschädigung (Stiftung Warentest 16. Juni 2020). Aus Verbrauchersicht sind die Anwendungen vor allem deshalb attraktiv, da nur im Erfolgsfall gezahlt werden muss. Weitere bekannte Einsatzbereiche sind Schadensersatzzahlungen wie nach dem VW-Dieselskandal, Hilfe bei unzulässigen Mieterhöhungen oder für die Überprüfung von Bußgeld- und Hartz-IV-Bescheiden. Zurecht befürchten Verbraucher lange Prozesse und hohe Anwaltskosten; entsprechende seriöse Legal Tech-Portale bieten eine effiziente Alternative. Ein ganz neuer und vielversprechender Anwendungsbereich findet sich im Bereich der **Verbraucherinformatik**, bei der Apps für den unmittelbaren Einsatz beim Online-Einkauf entwickelt werden (Reisch et al. 2019).

Was sagt das Verbraucherrecht?

Rechtsdienstleistungsgesetz

Wer Rechtsdienstleistungen erbringen darf, ist im Rechtsdienstleistungsgesetz (RDG) geregelt. Um diese Dienstleistungen zu erbringen, erfordert es eine Erlaubnis, über die zugelassene Anwälte

verfügen. Das anwaltliche Berufsrecht (§ 4 a Rechtsanwaltsvergütungsgesetz) stellt hohe Anforderungen an die Vereinbarung von **Erfolgshonoraren**. Die Übernahme von Prozesskosten durch den Anwalt ist verboten. Lange Zeit sah es so aus, als ob **gewerbliche Prozessfinanzierer** in diese Lücke springen können. Doch hat der Bundesgerichtshof (BGH) diesem in Österreich und in der Schweiz legalen Ansinnen einen rechtlichen Riegel vorgeschoben: Am 13.9.2018 hat der BGH (ZR I 26/17) die Gewinnabschöpfungsklage eines Verbraucherverbands, die von einem gewerblichen Prozessfinanzierer finanziert wurde, dem eine Vergütung in Form eines Anteils am abgeschöpften Gewinn zugesagt wurde, als unzulässig behandelt, weil sie dem Verbot unzulässiger Rechtsausübung aus § 242 BGB widerspreche.

Inkassodienstleister

Die begrenzten Möglichkeiten der Vereinbarung eines Erfolgshonorars, verknüpft mit dem Verbot der gewerblichen Prozessfinanzierung, hat zumindest indirekt das Geschäftsmodell der Legal-Tech-Unternehmen befördert. Diese bieten ihre Leistungen nicht als anwaltliche Beratung an, sondern als Hilfestellung in der Beitreibung einer Forderung, als **Inkassodienstleiste**r. Aus der Sicht von **Anwälten** werden von Legal Tech-Unternehmen jedoch Anwaltsleistungen erbracht, und die Einschränkungen des anwaltlichen Berufsrechts werden auf dem Umweg über die Inkassoleistung umgangen. Die Legal-Tech-Unternehmen sehen sich gar nicht als Konkurrenz zu Anwälten. Sie argumentieren, dass sie lediglich einen niederschwelligen Zugang zum Recht ermöglichen, und zwar in solchen Bereichen, in welchen Verbraucherinnen und Verbraucher wegen „rationalen Desinteresses“ ihr Recht sonst gar nicht wahrnehmen würden (also überwiegend bei Massengeschäften und Streuschäden). Anwälte sehen dagegen ihre Geschäftsgrundlage bedroht.

Im Dezember 2019 hat der BGH eine wegweisende Entscheidung getroffen (Urteil vom 27.11. 2019-VII ZR 285/17), die das Verhältnis zwischen Inkassodienstleistern und Anwälten neu ordnet. Danach erbringt das von einem **Inkassodienstleister** betriebene Legal-Tech-Portal ”wenigermiete.de” **keine unerlaubten Rechtsdienstleistungen** im Sinne des RDG, diese seien vielmehr durch die Inkassolizenz gedeckt. Damit dürfen Legal-Tech-Unternehmen ihre Leistungen als Inkassodienstleister anbieten und könnten so in Konkurrenz zu Anwälten treten. Anwälte dürfen dieses Geschäftsmodell dagegen weiterhin nicht anbieten, weil das anwaltliche Berufsrecht Erfolgshonorare ausschließt. Für Verbraucherinnen und Verbraucher bedeutet das, dass die Abtretung von Forderungen an Legal Tech-Unternehmen wirksam und zulässig ist. Allerdings hat der BGH den Legal Tech-Unternehmen keinen umfassenden Freibrief erteilt, sondern die Zulässigkeit an **Bedingungen** geknüpft: So verlangt der BGH stets eine am Schutzzweck des Rechtsdienstleistungsgesetzes orientierte Würdigung der Umstände des Einzelfalls einschließlich einer Auslegung der hinsichtlich der Forderungseinziehung getroffenen Vereinbarungen. Überschreitet ein registrierter Inkassodienstleister seine Inkassodienstleistungsbefugnis (nach § 10 Abs. 1 Satz 1 Nr. 1 RDG), kann darin ein Verstoß gegen § 3 RDG liegen. Die zwischen dem Inkassodienstleister und dessen Auftraggeber getroffene Inkassovereinbarung einschließlich einer erfolgten Forderungsabtretung wäre dann **nichtig**. Es scheint, dass sich auf untergerichtlicher Ebene Widerstand regt, so dass letztlich nur der Gesetzgeber Klarheit schaffen kann.

Grenzen von LegalTech

Allerdings ist es im Sinne des Mandanten- und Verbraucherschutzes keineswegs immer sinnvoll, sich bei Rechtsdienstleistungen allein auf die Algorithmen des LegalTech zu verlassen. Der **Schutz von Mandanteninteressen** fehlt bei Legal-Tech-Anwendungen, während er bei einer anwaltlichen Rechtsberatung durchgängig gewährleistet ist. Legal Tech Unternehmen sind dort hilfreich, wo das Gesetz eindeutige und nicht interpretierbare Maßstäbe formuliert. Bestes Beispiel dafür ist die **Fluggastrechte-Verordnung**, die Entschädigungsleistungen bei Verspätung oder Stornierung statuiert. Die Stiftung Warentest nennt in einem Vergleich verschiedener Fluggastentschädigungsdienste als Vorteil einen vergleichsweise geringen Aufwand. Ein gewichtiger Nachteil ist jedoch, dass die Entschädigung teilweise bis zu einem Jahr auf sich warten lässt, da die Entschädigung erst eingeklagt

werden muss. Im Erfolgsfall muss eine Provision gezahlt werden, die meist nur als **undurchsichtige Preisspanne** und oft nur als Nettopreise kommuniziert werden. Für Verbraucher bleibt immer die Möglichkeit, sich an die Schlichtungsstelle für den öffentlichen Personenverkehr (SÖP) zu wenden, die keine Kosten berechnet.

Neue Einsatzmöglichkeiten

Die Einsatzmöglichkeiten von Legal Tech zugunsten der Verbraucher stehen erst am Anfang. Besonders zukunftsträchtig sind **Massenverfahren**, wie etwa „Dieselgate". Ob und in welchem Umfang die involvierten Anwälte und Verbraucherverbände Legal Tech einsetzen, ist eine empirische Frage, die aktuell intensiv diskutiert wird (u.a. beim Verbraucherforschungsforum Baden-Württemberg im September 2020). Zuzustimmen ist Meller-Hannich (2020) wenn sie zusammenfasst: „Der gesetzliche Rahmen von Legal Tech ist noch nicht so ausgeprägt, dass für die Verbraucher_innen ein rechtssicheres Modell qualifizierter Rechtsberatung, für die Legal Tech-Anbieter ein innovatives Geschäftsmodell und für die Anwält_innen eine gewinnversprechende Vertretung auch von gebündelten kleineren Mandaten möglich ist."

Solange Institutionen der Zivilgesellschaft nicht mit dem RDG in Konflikt geraten, können sie mit Hilfe von **Big Data Analytics** Verbrauchern bei der Durchsetzung ihrer Rechte auch effektiv zur Seite stehen. Die Verbraucherinformatik entwickelt laufend vielversprechende Tools. So bietet beispielsweise **„Claudette"** (http://claudette.eui.eu/) Verbrauchern die Möglichkeit, die AGB und die Datenschutzpolitik von Anbietern auf ihre Vereinbarkeit mit den Vorgaben des Unionsrechts, der Richtlinie 93/13 missbräuchliche Vertragsklauseln und der DSGVO zu überprüfen. Claudette gibt einen **Hinweis** darauf, welche Klauseln möglicherweise rechtswidrig, problematisch oder legal sind; eine abschließende rechtliche Bewertung ist damit jedoch nicht verbunden.

Belege und weiterführende Literatur

Kind, S., Ferdinand, J.-P., & Priesack, K. (2019). *Legal Tech – Potenziale und Wirkungen* (Arbeitsbericht Nr. 185). Berlin: Büro für Technikfolgen-Abschätzung beim Deutschen Bundestag (TAB). https://www.tab-beim-bundestag.de/de/pdf/publikationen/berichte/TAB-Arbeitsbericht-ab185.pdf

Lippi, M., Contissa, G., Jablonowska, A., Lagioia, F., Micklitz, H.-W., Palka, P., et al. (2020). The Force Awakens: Artificial intelligence for consumer law. *Journal of Artificial Intelligence Research*, *67*, 169–190. https://doi.org/10.1613/jair.1.11519

Lorenz, P. (27. November 2019). Darum billigt der BGH wenigermiete.de. „Die Entwicklung neuer Berufsbilder erlauben." *Legal Tribune Online*. https://www.lto.de/recht/juristen/b/bgh-viii-zr-285-18-legal-tech-wenigermiete-de-inkassodienstleistung-weite-auslegung-abtretung-wirksam-rechtsdienstleistungsgesetz/. Abgerufen 15. August 2020

Meller-Hannich, C. (2020). Legal Tech Portale zur Durchsetzung von Verbraucherrechten. *WISO Direkt*, (01), 1–4.

Reisch, L. A., Thorun, C., & Micklitz, H.-W. (Hrsg.). (2019). *Künstliche Intelligenz und Verbraucherpolitik: Chancen der Verbraucherinformatik* (Verbraucherforschungsforum Baden-Württemberg 2019). Friedrichshafen: Forschungszentrum Verbraucher, Markt und Politik. https://www.zu.de/forschung-themen/forschungszentren/konsum/assets/pdf/Verbraucherforschungsforum-Report-2019.pdf

Rott, P. (2018). Rechtsdurchsetzung durch Legal Tech-Inkasso am Beispiel der Mietpreisbremse – Nutzen oder Gefahr für Verbraucher? *Verbraucher und Recht*, (12), 443–447.

Stiftung Warentest. (16. Juni 2020). Fluggastrechte – Der Weg zur Entschädigung. *test.de*. https://www.test.de/Fluggastrechte-Der-Weg-zur-Entschaedigung-4667375-0/. Abgerufen 15. August 2020

Verbraucherzentrale Hessen. (26. März 2020). Legal Tech – Warten auf den Code. *Verbraucherzentrale Hessen*. https://www.verbraucherzentrale-hessen.de/vertraege-reklamation/kundenrechte/podcast-legal-tech-warten-auf-den-code-45357. Abgerufen 15. August 2020

Werthmann, B. (2020 im Erscheinen). § 22: Legal Tech. In M. Ebers, C. Heinze, T. Krügel, & B. Steinrötter (Hrsg.), *Künstliche Intelligenz und Robotik* (1. Aufl.). München: C. H. Beck.

Informationsseiten

http://claudette.eui.eu/

https://www.haufe.de/thema/legal-tech/.

https://www.verbraucherzentrale.de/inkasso-check

https://www.verbraucherzentrale.de/wissen/reise-mobilitaet/unterwegs-sein/flugaerger-mit-app-kostenlos-entschaedigung-berechnen-40119

Personalisierte Preise

Was sind personalisierte Preise?

Ein Unternehmen bietet zwei verschiedenen Konsumenten zum gleichen Zeitpunkt das gleiche Produkt zu zwei unterschiedlichen Preisen an. Diese Strategie der **personalisierten Preise** basiert auf den Informationen, welche das Unternehmen über das Verhalten des jeweiligen Konsumenten gesammelt hat. Mithilfe dieser Informationen erfolgt eine Abschätzung der Zahlungsbereitschaft und des Kaufverhaltens. Verbraucherinnen und Verbraucher können so – auf Einzel- oder Gruppenbasis – verschiedenen Preisen individuell zugeordnet werden, die von Algorithmen automatisiert festgelegt werden. Je mehr Informationen berücksichtigt werden, desto ausdifferenzierter können die Preise personalisiert werden. Dabei werden Daten gesammelt, die Verbraucher freiwillig, z.B. durch Ausfüllen eines Online-Formulars, zur Verfügung stellen. Genutzt werden zudem vom Unternehmen beobachtbare Daten, etwa durch das Surfverhalten und die Installation von Cookies, sowie weitere, aus diesen Informationen abgeleitete Daten, die durch Datenanalyse oder maschinelles Lernen generiert werden. Weiter schließen Unternehmen durch das verwendete Endgerät, den Browser oder das Betriebssystem sowie über die IP-Adresse, bzw. Postleitzahl, Alter und Geschlecht auf die Kaufkraft und die Präferenzen der Konsumenten (Zander-Hayat et al. 2016).

Online erfasste personenbezogene Daten

Freiwillige Daten	Beobachtbare Daten	Abgeleitete Daten
Name, Telefonnummer, Email-Adresse, Geburtstag, Lieferadresse, Antworten auf Fragebögen, Beruf, Schulabschluss.	IP Adresse, Betriebssystem, letzte Käufe, besuchte Webseiten, Klicks, Wohnort, Browserverlauf, „Likes“ in sozialen Netzwerken.	Einkommen, allgemeiner Gesundheitszustand, Risikofaktor, Reaktion auf Werbung, Kundenbindung, politische Einstellung, Hobbys.

Von den personalisierten Preisen zu unterscheiden sind **dynamische Preise**, die sich im Zeitverlauf ändern, aber für alle Kunden gleichermaßen zu einem bestimmten Zeitpunkt gelten. Die Preise schwanken basierend auf Lagerbeständen, Kapazitätsengpässen, der Beliebtheit eines Produktes oder den Preisen der Konkurrenz (siehe Dynamische Preise).

Verbreitung

2018 wurden personalisierte Preise noch von wenigen Händlern, bzw. Anbietern und nur bei bestimmten Warengruppen verwendet (Dautzenberg et al. 2018; Reisch et al. 2016); sie werden jedoch zunehmend in „smart pricing“ Strategien von Unternehmen eingesetzt, denn sie sind für die Unternehmen attraktiv und grundsätzlich erlaubt, auch wenn sie in Deutschland höchst umstritten sind. Auch wenn momentan die Kosten der Personalisierung für die Unternehmen einen breitflächigen Einsatz noch nicht nahelegen, so spricht doch alles dafür, dass sich dies mit technologischem Fortschritt der Big-Data-Anwendungen schnell ändert. Es gibt heute zahllose Anbieter, die KI-basierte, auch personalisierte „smart pricing“-Strategien anbieten. Neue Marketingtrends wie das „Mobile Couponing“ (Winkler 2020) und vergleichbare personalisierte Preisstrategien sind stark im Trend.

Nach aktuellem Stand werden individualisierte Preise aufgrund von Personenvariablen von der überwiegenden Mehrheit der Verbraucher eher abgelehnt (u.a. Thorun & Diehl 2016; Tillmann & Vogt 2018), viel stärker als dynamische Preise. Verbraucher finden solche Preise unfair. Sie fürchten um die Verletzung von Persönlichkeitsrechten, das massive Sammeln und Speichern von Daten weitgehend ohne Kontrolle sowie die fehlende Preistransparenz.

Herausforderungen

- Unternehmen können auf der Basis gesammelter Daten die Preise nicht nur effektiver personalisieren, es geschieht auch ohne das Bewusstsein und die Zustimmung der Verbraucher, die möglicherweise nicht wissen, dass die Unternehmen detaillierte Profile über sie führen.
- Sich schnell ändernde Preise, Standortdifferenzierungen, unterschiedliche Darstellungen auf verschiedenen Endgeräten oder Versandkosten als Preisschraube sind für Verbraucherinnen und Verbraucher oft schwer zu durchschauen. Verbraucher können nicht erkennen, auf Basis welcher Kriterien persönliche Preise berechnet werden. Meistens wissen sie nicht einmal, dass Preise personenbasiert gesetzt werden.
- Die Komplexität der Auswahlentscheidung und die Suchkosten für Verbraucher werden erhöht. Das Vertrauen in einen „fairen Preis“ kann sinken. Es sind nicht mehr nur die bekannten (und nachvollziehbaren) Produktpreise (wie Flugtickets) im Internet, sondern durch die Digitalisierung im Einzelhandel werden flexible Preise auch im stationären Laden zunehmend eingesetzt, Festpreise werden seltener. Entsprechende Daten werden in Kundenprofilen gesammelt und gespeichert.
- Durch die auf Algorithmen beruhende Preisdifferenzierung kann es zu einer Ungleichbehandlung (Diskriminierung) bestimmter Bevölkerungsgruppen kommen, z. B. aufgrund ethnischer Herkunft, Wohnort, besuchten Orten, Religion oder sexueller Orientierung.
- Notlagen könnten ausgenutzt werden, indem Waren, auf die Verbraucher dringend angewiesen sind (z.B. Arzneimittel), teurer angeboten werden.
- Das heutige Verbraucherrecht ist den Herausforderungen des Big-Data-Zeitalters nicht mehr gewachsen und kann die marktwirtschaftlich notwendige Preistransparenz nicht mehr herstellen (Tillmann & Vogt 2018). Erste Ansätze zur Korrektur sind gleichwohl erkennbar.

Verbraucherpolitische Forderungen

- Explizite Abfrage der Einwilligung in die Datensammlung und -verarbeitung.
- Änderungen der Voreinstellungen, um die Transparenz zu erhöhen.
- Informationen über eine personalisierte Preisbildung beim Kauf, ggf. explizite Kennzeichnungspflicht in die Preisangabenverordnung (PAngV) einführen.
- Die Kriterien, die für die Berechnung des Algorithmus entscheidend sind, sollten offengelegt werden.
- Um die Möglichkeit von Preisvergleichen und einer preislichen Orientierung zu ermöglichen, sollte ein Referenzpreis angegeben werden.
- Keine Benachteiligung von datenschutzbewussten Verbrauchern.
- Konkretisierung und Erweiterung des Art. 22 Datenschutzgrundverordnung.

Was können Verbraucher tun?

- Erfahrungen sammeln, wann und von welchem Endgerät die Preise am günstigsten sind. Für Online-Einkäufe kein teures Apple-Gerät nutzen, sondern einen billigen PC oder Notebook.
- Prüfen, ob Kundenkarten wirklich einen reellen Nutzen bringen, denn der Preis dafür ist die vollständige Transparenz als Kunde.
- Virtuelle private Netzwerke (VPN) nutzen, um Ländereinstellungen zu ändern und damit ortsbasierte Preisaufschläge zu umgehen.
- Waren erst in den Warenkorb ablegen, warten, und erst kaufen, wenn der Preis gesunken ist.
- Daten grundsätzlich sparsam herausgeben. Nutzen von Privatsphäre-Einstellungen.
- Datenschutzbestimmungen genau lesen. Profiling ist nur zulässig, wenn die explizite Zustimmung erfolgt ist (die allerdings oft untergeschoben wird, siehe Dark Patterns)
- Cookies nur temporär erlauben, nur Funktionscookies akzeptieren, regelmäßig löschen.

Was sagt das Verbraucherrecht?

Verbraucherinformation

Personalisierte Preise sind grundsätzlich erlaubt. Es gilt die Wettbewerbs- und Preisgestaltungsfreiheit: Händler handeln nicht unlauter, wenn sie Kunden personalisiert unterschiedliche Preise anbieten, solange sie die Verbraucher angemessen über die Preise und die Art der Preisberechnung informieren. Die durch den „**New Deal for Consumers**" geänderte **Verbraucherrechte-RL** 2011/83/EU verpflichtet den Unternehmer (in Art. 6 lit e), den Verbraucher gegebenenfalls darauf hinzuweisen, dass der Preis auf der Grundlage einer **automatisierten Entscheidungsfindung** personalisiert worden ist. Diese Verpflichtung ist bis Ende 2021 in deutsches Recht umzusetzen. Jenseits dieser Regelung herrscht rechtliche Ungewissheit, weil es an Gerichtsurteilen und gesicherter Praxis der Kartell- und Datenschutzbehörden fehlt.

Die genannte Informationsverpflichtung besagt nicht, dass der Unternehmer auch die Parameter offenlegen muss, die hinter der Personalisierung stehen. Art. 246a EGBGB, der den Umfang der Informationsverpflichtung für den Online-Handel detailliert regelt, hilft nicht weiter. Art. 5 Abs. 2 P2B-VO 2019/1150 zur Förderung von Fairness und Transparenz für gewerbliche Nutzer von Online-Vermittlungsdiensten verpflichtet die Anbieter von Online-Suchmaschinen, die Hauptparameter, die einzeln oder gemeinsam für die **Festlegung des Rankings** am wichtigsten sind, und die relative Gewichtung dieser Hauptparameter darzulegen. Personalisierte Preise werden von dieser Regel nicht erfasst.

AGB-Kontrolle

Personalisierte Preise unterliegen prinzipiell nicht der AGB-Kontrolle. Wenn überhaupt, so greift die AGB-Kontrolle nur bei Intransparenz der Preisgestaltung, also etwa wenn Nebenkosten in AGBs verborgen werden. Hier liegt die Intransparenz in der Art und Weise, wie der personalisierte Preis berechnet wird. Doch folgt aus einer möglichen Intransparenz nicht notwendig eine Aufklärungspflicht. Insofern ist die Transparenzkontrolle von personalisierten Preisen ein stumpfes Schwert. Dagegen werden personalisierte Vertragsbedingungen von § 310 Abs. 3 Nr. 2 BGB erfasst. Hier kommt das gesamte Instrumentarium zur Kontrolle von unfairen AGBs zur Geltung.

Kartellrecht

Theoretisch können personalisierte Preise zu einer Diskriminierung der Verbraucher führen, wenn sie von marktbeherrschenden Unternehmen eingesetzt werden. § 19 Abs. 1 und Abs. 2 Nr. 1 und 3 des GWB (Kartellrechts) formuliert jedoch hohe Hürden. Bislang spielt die personalisierte Preiskontrolle gegenüber Endverbrauchern in der Praxis keine Rolle.

Datenschutz

Nicht erlaubt ist (laut Art. 22 DSGVO) das Profiling. Verboten ist eine automatisierte Entscheidung mit rechtlicher oder vergleichbarer Wirkung für das Datensubjekt. Das Profiling liegt typischerweise im Vorfeld. Insofern ist nicht klar, ob Art. 22 DSGVO überhaupt anwendbar ist. (Rott, 2019). Hinzu kommt ein weiteres. Art. 22 DSGVO adressiert nicht die automatisierte Verarbeitung durch KI an sich. Das Verbot nach Art. 22 Abs. 1 DSGVO greift nur, soweit automatisiert eine Entscheidung oder Maßnahme getroffen wird. Der zu einer Entscheidung führende Verarbeitungsprozess ist ebenso wenig abgedeckt, wie bloße Unterstützungs- und Vorbereitungshandlungen. Genau darum dürfte es sich aber bei der Aufforderung an den Verbraucher, zu einem bestimmten personalisierten Preis zu kaufen, handeln. Art. 22 DSGVO verlangt eine Außenwirkung der Ergebnisse des Verarbeitungsprozesses. Daran fehlt es aber bei der bloßen Aufforderung.

Sobald ein Kunde der Datenschutzerklärung eines Händlers zugestimmt hat, in der etwas anderes steht, läuft das Verbot des Profiling leer (zu den Voraussetzungen der Einwilligung Steckbrief Dark Patterns). Ob die geplante E-Privacy Verordnung der EU dies ändern wird, ist derzeit völlig ungewiss (Hofmann & Freiling 2020).

Belege und weiterführende Literatur

Dautzenberg, K., Gaßmann, C., Groß, B., Müller, F., Neukamp, D., Schmidtke, L., & Bodenstein, U. (2018). *Individualisierte Preisdifferenzierung im deutschen Online-Handel* (Eine Untersuchung der Verbraucherzentralen). Potsdam: Verbraucherzentrale Brandenburg. https://www.verbraucherzentrale.de/sites/default/files/2019-09/marktwaechter-untersuchung-individualisierte-preisdifferenzierung.pdf

Deutscher Bundestag. (2019). *Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Thomas L. Kemmerich, Michael Theurer, Reinhard Houben, weiterer Abgeordneter und der Fraktion der FDP – Drucksache 19/8654 – Auswirkungen von dynamischen und personalisierten Preisen* (Drucksache Nr. 19/9772). Berlin: Deutscher Bundestag. http://dipbt.bundestag.de/doc/btd/19/097/1909772.pdf

Hofmann, F., & Freiling, F. (2020). Personalisierte Preise und das Datenschutzrecht: Anforderungen an die datenschutzrechtliche Einwilligung. *Zeitschrift für Datenschutz*, *10*(7), 331–335.

Krämer, A., Kalka, R., & Ziehe, N. (2016). Personalisiertes und dynamisches Pricing aus Einzelhandels- und Verbrauchersicht. *Marketing Review St Gallen*, *34*(6), 29–37.

Micklitz, H.-W., Namyslowska, M., & Jablonowska, A. (2020 im Erscheinen). § 6 KI und Verbraucherrecht. In M. Ebers, C. Heinze, T. Krügel, & B. Steinrötter (Hrsg.), *Künstliche Intelligenz und Robotik* (1. Aufl.). München: C. H. Beck.

Reisch, L. A., Büchel, D., Joost, G., & Zander-Hayat, H. (2016). *Digitale Welt und Handel. Verbraucher im personalisierten Online-Handel* (Veröffentlichungen des Sachverständigenrats für Verbraucherfragen). Berlin: Sachverständigenrat für Verbraucherfragen beim Bundesministerium der Justiz und für Verbraucherschutz. https://www.bmjv.de/SharedDocs/Downloads/DE/News/Artikel/01192016_Digitale_Welt_und_Handel.pdf?__blob=publicationFile&v=2

Rott, P. (2019). Dynamische und personalisierte Preise zwischen Vertragsfreiheit und Willkür. In C. Ochs, M. Friedewald, T. Hess, & J. Lamla (Hrsg.), *Die Zukunft der Datenökonomie: Zwischen Geschäftsmodell, Kollektivgut und Verbraucherschutz* (S. 285–305). Wiesbaden: Springer Fachmedien Wiesbaden. https://doi.org/10.1007/978-3-658-27511-2_13

Schwaiger, M., & Hufnagel, G. (2018). *Gutachten zum Thema „Handel und elektronische Bezahlsysteme“* (ABIDA Gutachten Nr. 2017_58_B). München: Ludwig-Maximilians-Universität München, Institut für Marktorientierte Unternehmensführung. https://www.abida.de/sites/default/files/Gutachten_Handel_Bezahlsysteme.pdf

Thorun, C., & Diels, J. (2016). *Was Verbraucherinnen und Verbraucher in NRW über individualisierte Preise im Online-Handel denken* (Abschlussbericht Aktenzeichen: I-4-2.1-15/085). Berlin: ConPolicy Institut für Verbraucherpolitik. https://docplayer.org/54455832-Was-verbraucherinnen-und-verbraucher-in-nrw-ueber-individualisierte-preise-im-online-handel-denken.html

Tillmann, T. J., & Vogt, V. (2018). *Personalisierte Preise – Diskriminierung 2.0?* (ABIDA-Dossier). Münster: Institut für Informations-, Telekommunikations und Medienrecht (ITM) Westfälische Wilhelms-Universität Münster. https://www.abida.de/sites/default/files/22_Dossier_Personalisierte%20Preise_Online.pdf

Winkler, T. (2020). *Mobile Couponing im stationären Einzelhandel: Analyse erfolgversprechender Gestaltungsansätze und ihrer Problembereiche*. Melle: youneo projects flick und weber GBR.

Zander-Hayat, H., Reisch, L. A., & Steffen, C. (2016). Personalisierte Preise: Eine verbraucherpolitische Einordnung. *Verbraucher und Recht*, *31*(11), 403–409.

Self-Tracking

Was bedeutet Self-Tracking („Selbstvermessung“)?

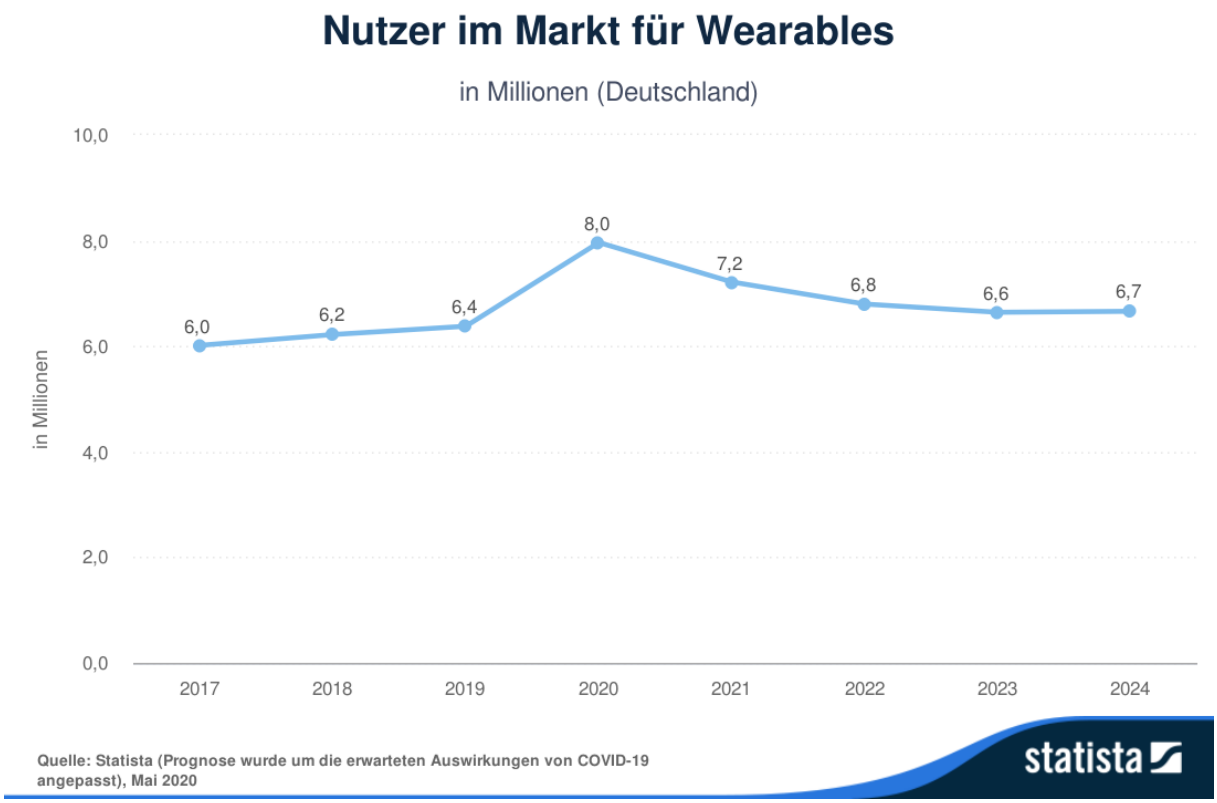
Selbstvermessung oder Self-Tracking ist ein Trend im Feld der **personalisierten Gesundheit** (SCNAT 2019). Sie zielt darauf ab, mit Hilfe von Hard- und Software eigene (biologische, physische, verhaltensbasierte und umweltbezogene) Daten möglichst umfassend und genau zu erheben und zu steuern, vor allem im Fitness-, Wellness- und Gesundheitsbereich. Anhand der gesammelten Daten können durch **prädiktive Algorithmen** Vorhersagen bezüglich des zukünftigen Gesundheitszustandes gemacht und Hinweise auf Optimierungsmöglichkeiten gegeben werden. Ziel ist, die eigene Gesundheit, das eigene Wohlbefinden und die Leistungsfähigkeit zu optimieren. Heute gibt es mehr als 100.000 Gesundheits-Apps, circa die Hälfte der Smart-Phone Nutzer nutzen mindestens eine davon. Klassische Anwendungsbereiche sind Kalorien-Zähler, Schrittzähler, Schlafrhythmus-Coaches oder Fitness-Apps. Handys haben eine Reihe von standardmäßigen Apps, zudem sind viele Arten von Fitnessarmbändern und sonstigen „smarten“ **Wearables** (also: bequem am Körper tragbare mobile Messgeräte) auf dem Markt. Die Daten werden entweder selbst in eine App eingetragen, die beispielsweise den Verlauf des täglichen subjektiven Wohlbefindens abbildet, oder aber automatisch über Wearables oder das Smartphone erfasst.

Der Trend, sein Verhalten exakt zu vermessen um sein (physisches) Selbst zu optimieren, wird als „**Quantified Self**“ (QS) bezeichnet (Meidert 2018). Die QS-Bewegung geht auf die beiden Wired-Autoren Gary Wolf und Kevin Kelly zurück, der gleichnamige Internet Blog „quantifiedself.com“ verbindet das mittlerweile globale Netzwerk, das auch in Deutschland aktiv ist. Die enorme Menge der Daten, die bei der Selbstvermessung entsteht, weckt auch bei Akteuren aus dem Gesundheitsbereich und der Wirtschaft Hoffnung auf Profit. Wie sinnvoll der Einsatz von Self-Tracking ist, ist letztlich abhängig von den Erwartungen der Nutzer und dem Einsatzbereich. So versuchen Freizeit- und Leistungssportler, ihr Training und ihre Ernährung auf ein bestimmtes Trainingsziel abzustimmen, um bestmögliche Ergebnisse zu erzielen. Chronisch kranke Menschen kontrollieren damit bestimmte Gesundheitswerte, wie bspw. die Blutzuckerwerte bei einer Diabetes-Erkrankung, und verbessern ihre Köperwahrnehmung und damit u.U. die Wirksamkeit der Therapie (ibid.). Prädiktive Algorithmen in der Medizin sind in der Lage, Krankheitsrisiken vorherzusagen und entsprechende Präventionsvorschläge zu machen (Scherenberg 2019). Auch das betriebliche Gesundheitswesen hat Apps als Motivationsvehikel entdeckt. Es gibt aber auch Anwender ohne spezifische Diagnose, die diverse Tracking-Apps aus Neugierde oder zur allgemeinen Selbstoptimierung nutzten.

Verbreitung und Wirkung

Einige Studien zeigen, dass dem QS zu gelingen scheint, woran viele Gesundheitsförderungs- und Präventionskampagnen oft scheitern, nämlich der Sprung vom Wissen zu konkreten Verhaltensänderungen. So hat Roediger (2015) gezeigt, dass schon das „Tracking“ an sich Verhaltensänderungen auslösen kann. Besonders im gesundheitlichen Bereich kann die Selbstüberwachung bspw. die Gewichtsabnahme oder das Halten eines bestimmten Gewichts unterstützen. Dabei nutzen erfolgreiche Apps häufig spielerische Aspekte, helfen bei einer konkreten Zielsetzung und führen zu einem direkten Feedback. Viele Anwendungen arbeiten mit „digitalen Nudges“ (d.h. Stupser, Thaler & Sunstein 2008) wie einfachen Feedbacks über Erfolge und Misserfolge verbunden mit kleinen Belohnungen; aber auch Erinnerungen oder (mit anderen geteilte) Selbstverpflichtungen können motivierende Elemente solcher Tracking-Apps sein. Eine Rolle spielt auch die unmittelbare und zeitgenaue Verfügbarkeit und Sichtbarkeit der eigenen Gesundheit in Zahlen, Grafiken und Bildern, sowohl als Feedback als auch Erinnerung an Ziele. In der Forschung hat sich weltweit ein eigener Forschungsbereich etabliert, der die Wirkung des „e-nudging“ im Gesundheitsbereich untersucht.

Verbreitung und Prognose von Wearables



Quelle: Statista (2020). Wearables. https://de.statista.com/outlook/319/137/wearables/deutschland.

Herausforderungen

Ob und wie weit insbesondere Gesundheits-Tracking-Produkte wirksam sind, ist von vielen persönlichen und technischen Variablen abhängig (Klingel 2019). Wearables and Tracker erheben Daten unterschiedlicher Qualität. Manche Wearables können selbst bei korrekter Nutzung ungenau sein (Stiftung Warentest 2020). Zusätzlich wird die Datenqualität verschlechtert, wenn die Wearables nur zu bestimmten Zeiten getragen werden, was Selektionseffekte ergibt, die zu unerkannten Abweichungen führen können. **Gesundheitsrisiken** können beispielsweise dann auftreten, wenn Apps nicht-evidenzbasierte Methoden empfehlen oder kontraindizierte Handlungsempfehlungen geben. Auch negative psychologische Folgen – wie ein gestörtes Körperbild, Suchtverhalten und gesteigerte soziale Erwartungen bzgl. Selbstoptimierung – werden diskutiert, sind bislang jedoch noch wenig untersucht.

Die bisherige sozialwissenschaftliche Literatur hat sich vor allem mit den **gesellschaftlichen** und **ethischen Folgen** von Self-Tracking-Apps befasst (Meidert et al. 2018). Von Anfang an gab es eine gesellschaftskritische Perspektive auf die Selbstvermessung und -optimierung („self-logging“), die den versprochenen Nutzen und die echten Kosten und oft unerkannten (psychischen) Risiken für die Nutzer sowie die Folgen für die Gesellschaft thematisiert (u.a. Selke 2016). Die Selbstvermessung präferiert individuelle sportliche Aktivitäten, die der Fitness dienen; der ebenfalls gesundheitsdienliche Gemeinschaftssport lässt sich aber nicht so einfach vermessen. Hinzu kommen die enormen **Datenschutzrisiken.** Die Verarbeitung, Übertragung und Speicherung der notwendigen großen Datenmengen ist eine Herausforderung für die Datensicherheit. Nicht zuletzt wird die Frage aufgeworfen, wem diese nutzergenerierten Daten gehören - dem Nutzer selbst oder dem Anbieter der App oder des Wearables und damit wer letztendlich verantwortlich im Sinne des Datenschutzes ist.

Insgesamt sind QS-Produkte eher unübersichtlich, und es mangelt systematisch an Transparenz in Sachen Datenqualität, -schutz und -sicherheit. Einige Anbieter wurden bereits von Marktwächterexperten abgemahnt, weil sie die Datenschutzbestimmungen in vielfältiger Hinsicht nicht eingehalten haben. So fehlt überwiegend die Einholung einer ausdrücklichen Einwilligung für die Erhebung und Verarbeitung von Gesundheitsdaten, eine genaue Konkretisierung der erhobenen Daten, des Nutzungszwecks und der Hinweis, an wen die Daten weitergeleitet werden (Moll et al. 2017; Verbraucherzentrale 9. Juni 2017). Bis heute gibt es noch keine umfassende und gleichzeitig valide Orientierungshilfe zur Einschätzung der Vertrauenswürdigkeit von Gesundheits-Apps – etwas, das Nutzern sehr helfen würde.

Was können Verbraucher tun?

- Sich informieren, wer für die App (oder das Wearable) verantwortlich zeichnet, welche Funktionalitäten sie beinhalten, ob sie dem persönlichen Einsatzzweck entspricht und für die richtige Zielgruppe entwickelt wurde
- sich darauf einstellen, dass personenbezogene Körperdaten erhoben werden, die sehr sensibel sind und für andere Zwecke (z.B. Versicherungen, siehe Stichwort Telematiktarife) genutzt, aber auch missbraucht werden können
- auf Datensicherheit achten und ein datensicheres Gerät kaufen bzw. eine hochqualitative und sichere App nutzen; Datenschutzbestimmungen lesen und vergleichende Warentests nutzen
- sich nicht von den Daten psychisch abhängig machen, sondern weiterhin in sich „hineinhören“
- alle per Voreinstellung auf den meisten Smart-Phones datensammelnde Gesundheits-Tracking-Apps auf persönliche Nutzen und Nutzung prüfen, ggf. abstellen oder ganz löschen

Verbraucherpolitische Forderungen

- Anpassung der Datenschutzbestimmungen
- Informationen der Anbieter, wie genau die Daten genutzt werden, wofür und an wen sie weitergeleitet werden
- Kontrolle der eigenen Daten muss gewährleistet sein, vollständige Datenschutzbestimmungen in leicht verständlicher Sprache

Was sagt das Verbraucherrecht?

Datenschutzrecht

Die über Wearables gesammelten Daten beziehen sich in der Regel auf die körperliche und geistige Gesundheit einer natürlichen Person (§ 4 Nr. 15 DSGVO). Deshalb gelten für die Beurteilung der datenschutzrechtlichen Zulässigkeit nicht nur die Standardanforderungen – nämlich: Einwilligung (Art. 6 Abs. 1 lit. a DSGVO), Vertragserfüllung (Art. 6 Abs. 1 lit. b DSGVO) oder Interessenabwägung (Art. 6 Abs. 1 lit. f DSGVO) – sondern auch die des Art. 9 DSGVO, der besondere Anforderungen für die Erhebung und Verarbeitung von **Gesundheitsdaten** formuliert. Danach ist im Grundsatz immer eine **ausdrückliche Einwilligung** erforderlich, nur ausnahmsweise können Gesundheitsdaten auch ohne Einwilligung erhoben werden, etwa zu medizinischen Zwecken. (Deutschland hat in §22 BDSG Abs. 1 Nr. 1 a)-d) diese Anforderungen weiter konkretisiert). Wearables werden aber in aller Regel nicht zu medizinischen Zwecken getragen, es sei denn das Tragen und Auswerten ist ärztlich veranlasst. Ebenso wenig können sich die Anbieter darauf berufen, die Erhebung diene lebenswichtigen Interessen des Trägers (Moll et al. 2017).

Verantwortung für die Sicherstellung des Datenschutzes

Schwierig ist die Frage, wer für die Sicherstellung des **Datenschutzes** verantwortlich (und damit haftbar) ist. Hier kommen eine Mehrzahl von Akteuren in Betracht, je nach Vertragslage. Sofern der Verkäufer der Hardware und der Anbieter der Software in einer Rechtsperson zusammenfallen, gibt

es nur *eine* datenschutzrechtlich verantwortliche Stelle. Bietet ein Drittanbieter Software an (z.B. eine App) kann entweder eine jeweilige Einzelverantwortlichkeit der drei vorliegen oder die gemeinsame Verantwortlichkeit (Art. 26 DS-GVO; Art. 28 DS-GVO). Für die Nutzer ist es deshalb schwer erkennbar, wer der Verantwortliche im Sinne des Gesetzes ist. Genau gegen diesen richten sich aber seine Informations- und Auskunftsrechte. Der EuGH ist durch sein weites Verständnis der „gemeinsamen Verantwortlichkeit" den Interessen der Verbraucher sehr entgegen gekommen (Steckbrief Soziale Netzwerke). Er hat entschieden, dass bei der Zuordnung datenschutzrechtlicher Verantwortlichkeit auf die wirtschaftliche Interessenlage und das „Eigeninteresse" der Beteiligten an der Verarbeitung zu achten ist. Diese Sichtweise legt die Möglichkeit gemeinsamer Verantwortlichkeit nahe. Das gilt sogar dann, wenn der Wearable-Hersteller nur einen sehr beschränkten Zugriff auf die vom App-Anbieter erhobenen, personenbezogenen Daten erhält (Krügel & Pfeiffenbring 2020). Den Verbrauchern stehen damit gleich mehrere Verantwortliche zur Verfügung, die sie zur Rechenschaft ziehen können.

Umgekehrt taucht auch bei Wearables die Frage auf, wem die **Daten gehören**. Mancher Verbraucher mag das Eigentum an seinen Daten reklamieren (siehe Steckbrief Virtuelle Realität). Trotz einiger Stimmen in der Literatur (Fezer 2018) sieht es nicht danach aus, dass die Politik und/oder die Gerichte bereit wären, einen solchen Schritt zu gehen.

Belege und weiterführende Literatur

Adam, L., & Micklitz, H.-W. (2016). *Information, Beratung und Vermittlung in der digitalen Welt* (SVRV Working Paper Nr. 6). Berlin: Sachverständigenrat für Verbraucherfragen beim Bundesministerium der Justiz und für Verbraucherschutz. https://www.svr-verbraucherfragen.de/wp-content/uploads/SVRV_WP06_Information_Beratung_Vermittlung.pdf

Ballhaus, W., Song, B., Meyer, F.-A., Ohrtmann, J.-P., & Dressel, C. (2015). *Wearables: Die tragbare Zukunft kommt näher*. PricewaterhouseCoopers AG Wirtschaftsprüfungsgesellschaft (PwC). https://www.pwc.de/de/technologie-medien-und-telekommunikation/assets/pwc-media-trend-outlook_wearables.pdf

Fezer, K.-H. (2018). *Repräsentatives Dateneigentum. Ein zivilgesellschaftliches Bürgerrecht* (Studie im Auftrag der Konrad-Adenauer-Stiftung e. V. zum Thema „Einführung eines besonderen Rechts an Daten"). Sankt Augustin, Berlin: Konrad-Adenauer-Stiftung e.V. https://www.kas.de/documents/252038/253252/7_dokument_dok_pdf_52161_1.pdf/f828a351-a2f6-11c1-b720-1aa08eaccff9?version=1.0&t=1539647605952

Klingel, A. (2019). *Gesund dank Algorithmen? Chancen und Herausforderungen von Gesundheits-Apps für Patient:innen*. Berlin, Gütersloh: Stiftung Neue Verantwortung und Bertelsmann Stiftung. https://www.bertelsmann-stiftung.de/fileadmin/files/BSt/Publikationen/GrauePublikationen/Impulspapier_Gesund-Dank-Algorithmen.pdf

Krügel, T., & Pfeiffenbring, J. (2020 im Erscheinen). § 11: Datenschutzrechtliche Herausforderungen von KI und Robotik. In M. Ebers, C. Heinze, T. Krügel, & B. Steinrötter (Hrsg.), *Künstliche Intelligenz und Robotik* (1. Aufl.). München: C. H. Beck.

Moll, R., Schulze, A., Rusch-Rodosthenous, M., Kunke, C., & Scheibel, L. (2017). *Wearables, Fitness-Apps und der Datenschutz: Alles unter Kontrolle?* (Eine Untersuchung der Verbraucherzentralen). Düsseldorf: Verbraucherzentrale NRW. https://www.verbraucherzentrale.de/sites/default/files/2019-09/mw-untersuchung_wearables_0.pdf

Meidert, U., Scheermesser, M., Prieur, Y., Hegyi, S., Stockinger, K., Eyyi, G., et al. (2018). *Quantified Self - Schnittstelle zwischen Lifestyle und Medizin*. Zürich: vdf Hochschulverlag. https://doi.org/10.3218/3892-7

Roediger, A. (2015). mHealth – unterwegs zu Gesundheitskompetenz 2.0. In Schweizerische Akademie der Medizinischen Wissenschaften (Hrsg.), *Gesundheitskompetenz in der Schweiz – Stand und Perspektiven* (1. Aufl., *10*(4), S. 72–74). Bern: Schweizerische Akademie der Medizinischen Wissenschaften. www.akademien-schweiz.ch/dms/publikationen/10/report1004.pdf

Scherenberg, V. (2019). Prävention via Lifelogging – Möglichkeiten und Grenzen der digitalen Selbstvermessung. In M. A. Pfannstiel, P. Da-Cruz, & H. Mehlich (Hrsg.), *Digitale Transformation von Dienstleistungen im Gesundheitswesen VI: Impulse für die Forschung* (S. 475–486). Wiesbaden: Springer Fachmedien Wiesbaden. https://doi.org/10.1007/978-3-658-25461-2_24

Selke, S. (Hrsg.). (2016). *Lifelogging. Digital self-tracking and Lifelogging - between disruptive technology and cultural transformation* (1. Aufl.). Wiesbaden: VS Verlag für Sozialwissenschaften. https://doi.org/10.1007/978-3-658-13137-1

Stiftung Warentest. (2. Juli 2020). Smartwatches und Fitnesstracker im Test. Nur 3 von 25 sind gut. Test, 02.07.2020. *test.de*. Stiftung Warentest. https://www.test.de/Smartwatch-Fitnessarmband-Laufuhr-Wearables-Test-5254021-0/. Abgerufen 5. Juli 2020

Swiss Academy of Sciences (SCNAT). (2019). *Themenportal „Personalisierte Gesundheit"*. Bern: Swiss Academy of Sciences (SCNAT). https://naturwissenschaften.ch/uuid/b92d9be9-5ee9-5b6a-9588-e54736b6b50a?r=20200527115808_1565136497_3011205d-3bd0-5cb8-8b29-9492f0ee23df

Thaler, R. & Sunstein, C. R. (2008). *Nudge: Improving decisions about health, wealth, and happiness*. New Haven, CT: Yale University Press.

Verbraucherzentrale. (9. Juni 2017). Unsportlich: Datenschutz-Mängel bei Wearables und Fitness-Apps. *Verbraucherzentrale.de*. https://www.verbraucherzentrale.de/aktuelle-meldungen/digitale-welt/unsportlich-datenschutzmaengel-bei-wearables-und-fitnessapps-13659. Abgerufen 15. August 2020

Wolf, G. (2010). *The quantified self*. Cannes: TED. https://www.ted.com/talks/gary_wolf_the_quantified_self. Abgerufen 9. Juli 2020

Informationsseiten

https://quantifiedself.com/

http://www.charismha.de/

Sicheres Surfen im Internet

Problemlage

Online-Einkaufen, Bankgeschäfte im Internet, Kommunikation über Emails oder Soziale Medien, Videobotschaften und virtuelle Treffen mit Familie und Freunden, Online-Meetings mit Kollegen, schnelle Faktensuche, Online-Tageszeitungen und Fernsehen – das Internet und die Nutzung von Apps auf mobilen Endgeräten ist das neue Normal. Spätestens seit der Corona Pandemie haben auch bislang zurückhaltende Bevölkerungsgruppen wie Senioren die fast unbegrenzten Möglichkeiten, Bequemlichkeiten und sonstige Vorteile, die ein vernetztes Leben bietet, entdeckt. Die vielfältigen Risiken – vor allem die mangelnde **Datensicherheit** und die verbreitete **KI-basierte Überwachung und Propaganda** auf Grundlage von **Profilbildungen** – sind zwar im Prinzip bekannt. Die meisten haben davon gehört, dass Daten mithilfe von Big-Data-Analysemethoden ausgewertet werden, um Verhaltensmuster, Eigenschaften, Neigungen, Interessen und sogar vollständige **Persönlichkeitsprofile** von Personen zu erstellen (siehe Verbraucher-Scoring). Auch ist weitgehend bekannt, dass man im Netz mit persönlichen Daten teuer „bezahlt“, und dass diese Geschäftsmodelle Grundlage der vermeintlichen „Kostenloskultur“ sind (Sunyaev 2019). Verbraucher trappen jedoch regelmäßig in die Bequemlichkeits- und Aufmerksamkeitsfalle und geben für wenig kurzfristigen Nutzen zu viele Daten preis.

Dabei mangelt es nicht an Bemühungen, die digitalen Fähigkeiten der Verbraucherinnen und Verbraucher zu erhöhen und sie für Sicherheitsrisiken zu sensibilisieren. Die aktuelle Kampagne des Verbraucherministeriums Baden-Württemberg „#seiunberechenbar“ gehört hier dazu. Auch stellt sich die Verbraucherpolitik den Herausforderungen der digitalen Welt und ist dabei, eine verbrauchergerechte Digital- und Datenpolitik zu entwickeln (SVRV 2016). Die Herausforderungen, die sich rasant entwickelnden KI-basierten Anwendungen verbraucher- und bürgergerecht zu regulieren und gestalten, sind jedoch groß. Die Regulierung ist traditionell langsam, und der Weg zu einer „verantwortungsvollen und gemeinwohlorientierten Entwicklung und -nutzung von KI“, den die Bundesregierung im Rahmen ihrer Strategie Künstliche Intelligenz (2018) fordert, ist weit (siehe Ethische KI).

Grundsätzlich gilt: Je mehr persönliche Daten im Umlauf sind, desto größer ist die Gefahr, Unternehmen nicht nur die immer umfangreichere Profilbildung zu ermöglichen (siehe auch: Personalisierte Preise), sondern auch Opfer von Betrügereien und Straftaten wie Identitätsdiebstahl zu werden. Sind die Daten erst einmal im Umlauf, ist es langwierig und manchmal auch erfolglos, sie wieder zu löschen oder auch nur zu korrigieren. Ebenso gefährdet sind Verbraucherinnen und Verbraucher in ihrer Rolle als (Konsumenten-)Bürger, wenn politische Propaganda und falsche Nachrichten Gesellschaft und Demokratie unterhöhlen, polarisieren und in eine Parallelwelt alternativer Fakten führen. Auch hier spielt die exakte Profilbildung und personalisierte Ansprache – ermöglicht durch Algorithmen und maschinelles Lernen als Methoden der Big Data Analytics – eine entscheidende Rolle.

Jegliche Kommunikation im Internet hinterlässt Spuren, die ausgewertet werden können. Die IP-Adressen von Computern im Internet können dem jeweiligen Nutzer zugeordnet werden. Nach jedem Besuch von Webseiten werden **Cookies** (vom Websitenbetreiber sowie von Dritten) auf dem Rechner gespeichert, durch die es möglich ist, das Surfverhalten auf diesem Computer nachzuvollziehen. Mit weiteren Daten wie Namen, Geburtsdatum, persönlichen Interessen etc., lassen sich dann umfangreiche Verbraucherprofile erstellen. Besondere Risiken ergeben sich aus dem Umgang mit **persönlichen Daten**. Adresshändler sammeln diese und verkaufen sie meist für Werbezwecke. Über die persönlichen Daten können individuelle Profile von Verbraucherinnen und Verbrauchern angelegt werden, über welche personalisierte Werbung (kommerzielle und politische) verbreitet wird oder personalisierte Preise angeboten werden können. Sie werden für **Verbraucher-Scorings** eingesetzt

(Steckbrief Verbraucher-Scoring), um die Kreditwürdigkeit oder Preisbereitschaft von Personen einzuschätzen, werden aber auch für Betrügereien und Straftaten genutzt.

Weitere Möglichkeiten für das Datensammeln bieten sich durch Kundenkarten, für welche bereits bei der Antragsstellung neben Namen und Adresse Angaben zu Interessen, Familienstand, Haushaltsgröße, Beruf und Einkommensklasse gemacht werden müssen. Auch Preisausschreiben dienen hauptsächlich dazu, Daten abzufragen. Von Interesse ist hier oft das Geburtsdatum, da es eine eindeutige Identifikation möglich macht. Über die Benachrichtigungen von vermeintlichen Gewinnen wird die Bankverbindung erfragt. Bankdaten sollten nicht leichtfertig weitergeleitet werden, da gerade der Missbrauch mit diesen Daten zu den häufigsten Betrugsfällen im Internet gehört. Kriminelle ziehen kleinere Geldbeträge ein, die oft unbemerkt bleiben, da die Abbuchungen nicht immer sorgfältig geprüft werden. Auch über die Nutzung von Apps werden oft persönliche Daten preisgegeben, da die Dienste bei mobilen Geräten auf Daten wie das Adressbuch oder den Standort zugreifen, obwohl diese für die Anwendung völlig unerheblich sind. Ein bekanntes Beispiel ist die Taschenlampen-App, die bei Nutzung Daten im Hintergrund abzieht.

Dabei sind Algorithmen und KI keineswegs per se problematisch, sondern erst einmal neutral. Entsprechend eingesetzt können sie – wie viele gute Beispiele der **Consumer Informatics** und **Consumer Legal Tech zeigen** (siehe dort beispielsweise die Verbraucher-App „Claudette“) – viel zum Wohl der Verbraucher beitragen.

Verbraucherpolitische Forderungen

Der Sachverständigenrat für Verbraucherfragen hat bereits 2016 folgende Vorgaben für eine verbraucherbezogene Netzpolitik im Online-Handel vorgeschlagen, bei der die **Sicherheit der Daten** im Mittelpunkt steht (Reisch et al. 2016, S. 3-4):

> „Starker regulativer Rahmen – keine Individualisierung der Verantwortung
> Einfachheit und Entlastung der Verbraucher – nicht Entmündigung
> Kompetenz schaffen und Verbraucher stärken – aber nicht überfordern
> Transparenz erhöhen – nicht mehr, aber qualitativ bessere Information
> Gesicherter Zugang für alle – mehr Wettbewerb im Netz
> Gemeinsame Verantwortung – auch die Gesellschaft ist gefordert.“

Mittlerweile haben einige Kommissionen, Initiativen und Praxisprojekte diese Forderungen konkretisiert, etwa die Datenethikkommission der Bundesregierung (2019). Auch die aktuelle Diskussion um ein neues, umfassendes **Datenrecht** ist ein Versuch, die Sicherheit und Verbraucherfreundlichkeit des Internet zu erhöhen und echte digitale Souveränität erst zu ermöglichen.

Was können Verbraucher tun?

Häufig ist die sicherere Alternative weniger bequem, erfordert eigenen Einsatz und Wissen oder macht die Bedienung etwas umständlicher. Verbraucher sollten die kleinen Bequemlichkeitsgewinne jedoch mit den großen Gefahren abwägen und regelmäßig etwas Zeit in ein persönliches Datenmanagement investieren. Verbraucherzentralen und Netzaktivisten empfehlen:

> Nur solche Daten angeben, die für das Zustandekommen des jeweiligen Vertrages notwendig sind; genau prüfen, ob der Zweck präzise und eindeutig umrissen ist.
> Überlegen, welche Informationen in sozialen Netzwerken geteilt werden sollen und die Empfänger einschränken.
> Über eine VPN-Verbindung (Virtuelles Privates Netzwerk) ist anonymes Surfen ohne Zuordnung der IP-Adresse sowie die verschlüsselte Übertragung von Daten möglich.

- Über Einstellungen des Internetbrowsers wie zum Beispiel „privater Modus“, „Verlauf löschen“ oder „Cookies nicht für Drittanbieter zulassen“ wird die Speicherung von Informationen über das Verhalten im Web vermindert.
- Cookie-Einstellungen im Browser überprüfen und Cookies regelmäßig löschen. Cookies deaktivieren und nur Ausnahmen zulassen, wenn sie nützlich und wichtig sind.
- Sich informieren, auf welche Daten Apps zugreifen und die Privatsphäre- und Datenschutzeinstellungen anpassen.
- Auf versteckte Erklärungen in den AGBs achten.
- Benachrichtigungen über vermeintliche Gewinne ignorieren.
- Bei Unternehmen nachfragen, wenn Unklarheit über die gespeicherten Daten herrscht.
- Aktiv das Löschen von Daten verlangen, wenn sie für den Zweck, für den sie erhoben wurden, nicht mehr benötigt werden.

Was sagt das Verbraucherrecht?

Relevant für die verbraucherpolitische Förderung des sicheren Surfens im Internet sind in erster Linie das Datenschutzrecht, das Vertragsrecht sowie die EU-Richtlinie zu Digitalen Inhalten.

Datenschutzrecht

Informierte Einwilligung und Grundsatz der Datensparsamkeit

Dreh- und Angelpunkt in der Datensicherheit sind die Voraussetzungen, unter denen Unternehmen die persönlichen Daten der Verbraucher sammeln und verarbeitet dürfen. Nach **Datenschutzrecht** ist hierzu die **Einwilligung** des Verbrauchers notwendig, es sei denn, es handelt sich um von der DSGVO legalisierte Formen der Datenerhebung und Verarbeitung, die auch ohne Einwilligung erfolgen können (Steckbrief Dark Patterns). Oberstes Prinzip ist die **Datensparsamkeit** und **-minimierung** (Art. 5 Abs. 1 lit c DSGVO). Eines der großen bislang völlig ungelösten Probleme der Datensicherheit ist, dass Verbraucher in aller Regel nicht übersehen können, in welche Anwendungen und Bedingungen sie im Einzelnen einwilligen. ‚Wie können betroffene Personen überhaupt in die Verarbeitung ihrer Daten einwilligen, wenn sogar das Unternehmen zum Zeitpunkt der Datenerhebung noch nicht weiß, zu welchen Zwecken die Daten weiterverwendet werden? Wie lassen sich Profiling, Dark Patterns und algorithmische Manipulation mit dem **Recht auf informationelle Selbstbestimmung** und dem datenschutzrechtlichen Prinzip der informierten Einwilligung in Einklang bringen?‘ (Ebers 2020, § 3 Rdnr. 89). Stellt man die Wirklichkeit der Verbraucher den hehren Worten des Bundesverfassungsgerichts im fast vier Jahrzehnte alten Volkszählungsurteil gegenüber, offenbart sich das ganze Dilemma (BVerfGE 65, 1 (33) Rn. 146): „Wer nicht mit hinreichender Sicherheit überschauen kann, welche ihn betreffenden Informationen in bestimmten Bereichen seiner sozialen Umwelt bekannt sind, und wer das Wissen möglicher Kommunikationspartner nicht einigermaßen abzuschätzen vermag, […] [kann] in seiner Freiheit wesentlich gehemmt sein, aus eigener Selbstbestimmung zu planen oder zu entscheiden. Mit dem Recht auf informationelle Selbstbestimmung wären eine Gesellschaftsordnung und eine diese ermöglichende Rechtsordnung nicht vereinbar, in der Bürger nicht mehr wissen, wer was bei welcher Gelegenheit über sie weiß“. Die Rechtswirklichkeit ist 37 Jahre später immer noch weit von diesem Anspruch entfernt.

Pflichten der verantwortlichen Unternehmen und Aufgaben der Datenschutzbehörden

Die Datenschutzgrundverordnung (DSGVO) in Verbindung mit dem Bundesdatenschutzgesetz (BDSG) bietet eine Reihe von Ansatzpunkten, die der Datensicherheit dienen sollen. Adressat dieser Regeln sind die **verantwortlichen Unternehmen**. Ob diese Regeln eingehalten werden, überprüfen die Datenschutzbehörden. Folgende Regeln sind vorgesehen (Krügel & Pfeiffenbring 2020):

- Soweit Versicherungen von der in § 37 Abs. 2 BDSG geschaffenen Möglichkeit Gebrauch machen, in der Entscheidung ausschließlich auf Algorithmen zu vertrauen, müssen sie dem Verbraucher ein Recht auf Überprüfung dieser Entscheidung durch einen **Menschen** gewähren.

- Art 25 DSGVO formuliert Anforderungen an die Datensicherheit durch Technikgestaltung (privacy by design; privacy by default) und **datenschutzfreundliche Voreinstellungen** (Steckbrief Dark Patterns).
- Art. 32 DSGVO verlangt, „geeignete technische und organisatorische Maßnahmen“ zu treffen, „um ein dem Risiko **angemessenes Schutzniveau** zu gewährleisten“: durch Pseudonymisierung und Verschlüsselung personenbezogener Daten (Art. 32 Abs. 1 lit. a DSGVO), durch Sicherstellung der Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste (Art. 32 Abs. 1 lit. b DSGVO), durch die Gewährleistung der Verfügbarkeit und Wiederherstellbarkeit bei einem physisch oder technischen Zwischenfall (Art. 32 Abs. 1 lit. c DSGVO), durch Verfahren, die eine regelmäßige Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen ermöglichen (Art. 32 Abs. 1 lit. d DSGVO).
- Art. 35 Abs. 1 DSGVO fordert eine **Datenschutzfolgenabschätzung**, wenn die Verarbeitung „aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge“ hat. Das Recht vermutet ein hohes Risiko dort, wo es sich um personenbezogene Daten und automatisierte Verarbeitung mit ggf. rechtswirksamen Konsequenzen handelt.

Vertragsrecht

Aufklärungspflichten

Bislang ist ungelöst, inwieweit ein Unternehmen den Verbrauchern gegenüber **vertraglich** verpflichtet ist, die Daten offenzulegen, die es über sie gesammelt hat (zum Recht auf Auskunft und Information siehe Steckbrief Verbraucher-Scoring). Bislang konzentriert sich die Diskussion im Wesentlichen auf die im Datenschutzrecht formulierten **gesetzlichen** Verpflichtungen. Spindler & Seidel (2018) haben unter dem Stichwort „Wissenszurechnung“ eine griffige Regel formuliert, die in der Diskussion um die Verantwortlichkeiten der Unternehmen eine neue Seite aufschlägt: „Wer Daten besitzt und diese verarbeitet, darf diese nicht nur zu Werbezwecken nutzen, sondern muss sie auch zum **Schutz seiner Kunden** einsetzen.“ Aus dieser Treuepflichten könnten dem Unternehmer Aufklärungspflichten erwachsen; er müsste dem Verbraucher mitteilen, welche Daten er besitzt. Tut er das nicht, kämen Schadensersatzansprüche in Betracht. Doch fehlt es bislang an einer gerichtlichen Praxis.

Pflicht zur Information über verfügbare Software Updates

Die **EU Richtlinie über Digitale Inhalte** (RL 770/2019) formuliert (in Art. 8 Abs. 2) Anforderungen an Software Updates: Der Unternehmer muss sicherstellen, dass der Verbraucher über Aktualisierungen – einschließlich Sicherheitsaktualisierungen, die für den Erhalt der Vertragsmäßigkeit der digitalen Inhalte und digitalen Dienstleistungen erforderlich sind – informiert wird. Entsprechende Updates müssen bereitgestellt werden „während des Zeitraums, in dem die digitalen Inhalte oder digitalen Dienstleistungen im Rahmen des Vertrags bereitzustellen sind oder den der Verbraucher aufgrund der Art und des Zwecks der digitalen Inhalte vernünftigerweise erwarten kann“. Ob aus der Verletzung dieser Pflicht Schadensersatzansprüche formuliert werden können, hängt von der – noch ausstehenden – Umsetzung in das deutsche Recht ab, was bis Ende 2021 erwartet wird.

Belege und weiterführende Literatur

Bundesamt für Sicherheit in der Informationstechnik (BSI). (2019). *Surfen, aber sicher!* (Broschüre). Bonn: Bundesamt für Sicherheit in der Informationstechnik (BSI). https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSIFB/Broschueren/Brosch_A6_Surfen_aber_sicher.pdf;jsessionid=17FBAD8350B7A757DEE9C02B2AA23521.1_cid503?__blob=publicationFile&v=7

Bundesregierung. (2018). Nationale Strategie für Künstliche Intelligenz. https://www.ki-strategie-deutschland.de/home.html. Abgerufen 14. August 2020

Ebers, M. (2020 im Erscheinen). § 3 Regulierung von KI und Robotik. In M. Ebers, C. Heinze, T. Krügel, & B. Steinrötter (Hrsg.), *Künstliche Intelligenz und Robotik* (1. Aufl.). München: C. H. Beck.

Niedermann, A. (2019). *Freiwillige und informierte Einwilligung? Die Nutzerperspektive* (Eine Untersuchung im Auftrag des FOCUS MAGAZIN VERLAG GMBH). Institut für Demoskopie Allensbach. https://www.ifd-allensbach.de/fileadmin/IfD/sonstige_pdfs/FOCUS_deutsch.pdf

Krügel, T., & Pfeiffenbring, J. (2020 im Erscheinen). § 11: Datenschutzrechtliche Herausforderungen von KI und Robotik. In M. Ebers, C. Heinze, T. Krügel, & B. Steinrötter (Hrsg.), *Künstliche Intelligenz und Robotik* (1. Aufl.). München: C. H. Beck.

Reisch, L. A., Büchel, D., Joost, G., & Zander-Haya, H. (2016). *Digitale Welt und Handel. Verbraucher im personalisierten Online-Handel* (Veröffentlichungen des Sachverständigenrats für Verbraucherfragen). Berlin: Sachverständigenrat für Verbraucherfragen beim Bundesministerium der Justiz und für Verbraucherschutz. https://www.bmjv.de/SharedDocs/Downloads/DE/News/Artikel/01192016_Digitale_Welt_und_Handel.pdf?__blob=publicationFile&v=2

Sachverständigenrat für Verbraucherfragen (SVRV). (2016). *Verbraucherrecht 2.0. Verbraucher in der digitalen Welt* (Gutachten des Sachverständigenrats für Verbraucherfragen). Berlin: Sachverständigenrat für Verbraucherfragen beim Bundesministerium der Justiz und für Verbraucherschutz. https://www.svr-verbraucherfragen.de/wp-content/uploads/Gutachten_SVRV-.pdf

Spindler, G., & Seidl, A. (2018). Die zivilrechtlichen Konsequenzen von Big Data für die Wissenszurechnung und Aufklärungspflichten. *Neue Juristische Wochenschrift*, *71*(30), 2153–2157.

Sunyaev, A. (2019). *Verbraucherdaten als Gegenleistung: Der ökonomische Wert von Kundendaten* (Studie im Auftrag des BMJV, Bundesministerium der Justiz und für Verbraucherschutz Aktenzeichen 123-02.05-20.0216/16-I-D). Kassel: Wissenschaftliches Zentrum für Informationstechnik-Gestaltung, Universität Kassel. https://www.bmjv.de/SharedDocs/Downloads/DE/Service/Fachpublikationen/Abschlussbericht_Verbraucherdaten.pdf?__blob=publicationFile&v=1

Verbraucherzentrale. (4. Oktober 2016). Kundenkarten: Wenig Rabatt für viel Information. *Verbraucherzentrale.de*. https://www.verbraucherzentrale.de/wissen/vertraege-reklamation/werbung/kundenkarten-wenig-rabatt-fuer-viel-information-13862. Abgerufen 15. August 2020

Verbraucherzentrale. (7. April 2020). So können Apps wie Facebook auf Telefon-Daten zugreifen. *Verbraucherzentrale.de*. https://www.verbraucherzentrale.de/wissen/digitale-welt/soziale-netzwerke/so-koennen-apps-wie-facebook-auf-telefondaten-zugreifen-24683. Abgerufen 15. August 2020

Informationsseiten/Kampagnen

https://mlr.baden-wuerttemberg.de/de/unsere-themen/verbraucherschutz/algorithmen/

https://www.klicksafe.de/

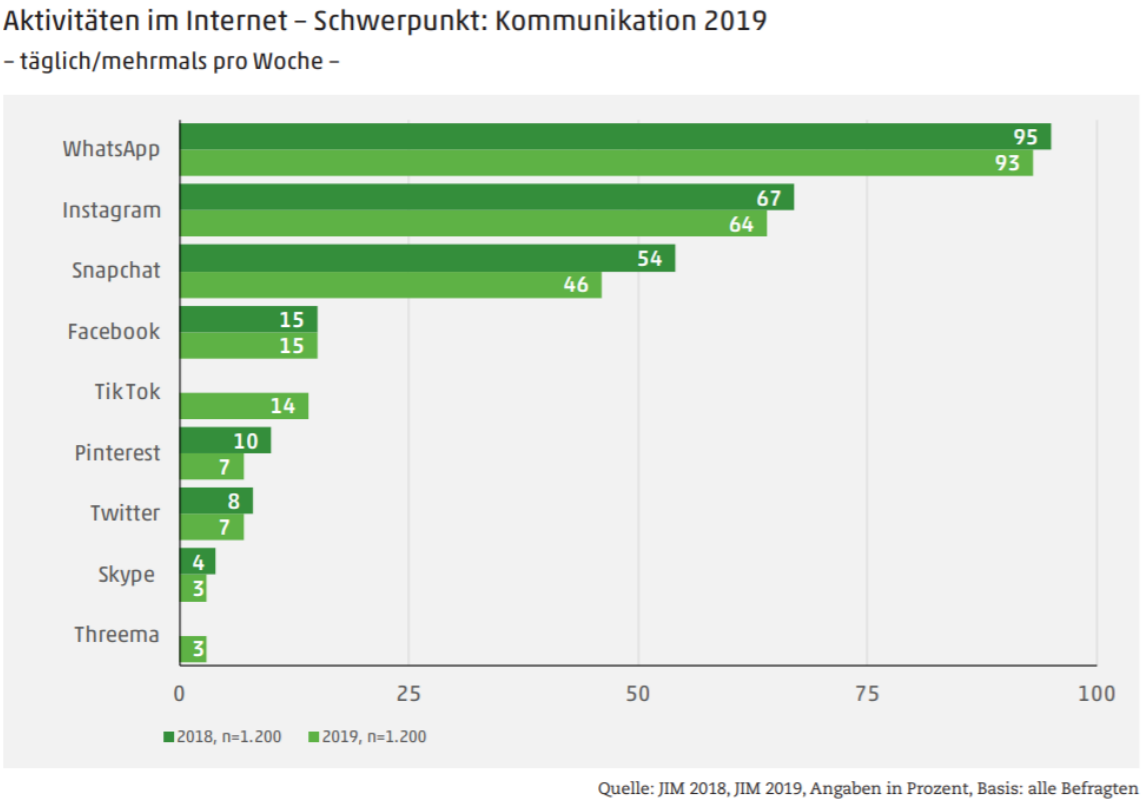
https://www.schau-hin.info/surfen

https://www.sicher-im-netz.de/browser-co-sicher-unterwegs-im-netz

Soziale Netzwerke

Was sind Soziale Netzwerke?

Viele Verbraucherinnen und Verbraucher sind in mehrere Soziale Netzwerke eingebunden. Auf Plattformen wie Facebook, Instagram, Snapchat, TikTok, Google+, Youtube, Pinterest, Twitter oder Karrierenetzwerken wie LinkedIn und XING entstehen virtuelle Gemeinschaften zu bestimmten Themen, gemeinsamen Interessen oder zum allgemeinen Austausch. Voraussetzung ist das Einrichten eines Nutzerprofils, das neben Angaben zur Person auch Informationen über Interessen, Familienstatus oder den beruflichen Werdegang enthalten kann. Die Kommunikation untereinander erfolgt auf Pinnwänden oder in Nachrichten- und Chat-Foren. Es werden Privatfotos, politische Meinungen, Tipps sowie Informationen zum Job- oder Beziehungsstatus geteilt, in beruflichen Netzwerken auch Arbeitsergebnisse oder Neuigkeiten.



Quelle: Feierabend et al. (2020, S. 30).

Soziale Netzwerke bilden reale Beziehungsnetzwerke aber nicht nur digital ab, sondern **gewichten die Kontakte** auch mit Hilfe von Algorithmen nach Häufigkeit und Bedeutung. Welche Posts man sieht und was man zum Lesen angeboten bekommt, entscheiden lernende Algorithmen. Soziale Netzwerke funktionieren über die Selbstdarstellung ihrer Nutzerinnen und Nutzer und deren Vernetzung über Freundeslisten. Sie erlauben, eine gewünschte soziale oder auch berufliche Ideal-Identität zu kreieren und darzustellen, bestimmte ausgewählte Informationen und Werbung für sich selbst oder andere zu veröffentlichen und zu bewerten. Allerdings sind diese Daten auch Grundlage für **datenbasierte Geschäftsmodelle** und Big Data Anwendungen.

Soziale Netzwerke bergen eine ganze Reihe von rechtlichen, ökonomischen, sozialen und auch psychischen Risiken. Diese reichen von Profiling und Verbraucher-Scoring (siehe Verbraucher-Scoring) über Manipulation und Identitätsmissbrauch (siehe Identitätsdiebstahl) bis zu Internetsucht und Cybermobbing. In einer aktuellen Studie mit Jugendlichen in Deutschland gaben fast 13 Prozent an,

bereits Opfer von Cybermobbing-Attacken gewesen zu sein, bei den 14- bis 16-Jährigen war es fast jeder Vierte (Leest & Schneider 2017); und 2,6 Prozent der Teenager erfüllen die Kriterien einer Sucht nach Sozialen Medien (DAK Gesundheit 2018). Dies liegt nicht zuletzt an den Dark Patterns (siehe Dark Patterns), deren Design viele kleine soziale Belohnungen vorsieht und daher die Nutzung fast unwiderstehlich macht. Der Blick ins soziale Netzwerk belebt und beruhigt, lenkt ab und kompensiert, ist ein ortsunabhängiger aktivierender Zeitvertreib und Likes, Shares und „Freunde" sorgen für ständigen Nachschub an stimmungsaufhellenden Glückshormonen. Allerdings werden Soziale Netzwerke – vor allem bildintensive wie Facebook und Instagram – auch für die wachsende Zahl an diagnostizierten Depressionen mitverantwortlich gemacht, wie eine US-amerikanische Studie mit 4000 Jugendlichen nahelegt (Boers et al. 2019). Der Hauptgrund wird darin gesehen, dass die Jugendlichen im permanenten Vergleich zueinanderstehen und notgedrungen täglich viele kleine „Niederlagen" und Selbstwertdämpfer erleiden.

Herausforderungen

- Trotz der geltenden **Datenschutzgrundverordnung** (DSGVO), die mehr Kontrolle über eigene Daten verspricht, ist es Verbraucherinnen und Verbrauchern kaum möglich, die Verarbeitung, Nutzung und Speicherung der eigenen Daten in Sozialen Netzwerken nachzuvollziehen (Moll et al 2018). Auch die von der DSGVO vorgesehene datenschutzfreundliche Voreinstellung (**privacy by default**) wird meist nicht oder nicht vollständig umgesetzt. So ist bei den meisten Diensten voreingestellt, dass die Beiträge öffentlich und nicht nur für ausgewählte Kontakte sichtbar sind.
- Die **Einstellungen** zum Schutz der Privatsphäre und Zustimmungen zu Werbezwecken sind nicht nutzerfreundlich gestaltet, sondern erfordern eine zeitintensive Auseinandersetzung. Auch werden meist mehr Daten erhoben, als für den eigentlichen Zweck nötig wären. Werden jedoch keine erhöhten Privatsphäre- oder Sicherheitseinstellungen vorgenommen, sind Beiträge im gesamten Netzwerk und auch darüber hinaus sichtbar. Nachteile können sich hier ergeben, wenn sich Unternehmen bei der Arbeitssuche vorab über Bewerberinnen und Bewerber informieren. Über geteilte Urlaubszeiten lassen sich von Kriminellen leerstehende Häuser und Wohnungen ausspionieren.
- Anhand der Daten können detaillierte **Verbraucherprofile** erstellt werden, welche das individuelle Surf- und Nutzungsverhalten auswerten und Auskunft über Lebensumstände, persönliche Vorlieben und finanzielle Situation geben. Das ermöglicht beispielweise personalisierte Werbung oder auch **personalisierte Preise** (siehe Steckbrief Personalisierte Preise), die ein großer Teil der Verbraucher ablehnt.
- Über so genanntes **Phishing** können Nutzername und Passwort abgefangen werden. Betrüger haben so Zugang zum jeweiligen Account, können Daten einsehen und ändern sowie Nachrichten verschicken und chatten. Auch über gehackte Accounts kann ein solcher **Identitätsmissbrauch** erfolgen. Über die Freundesliste wird dabei beispielsweise die Nachricht über eine fingierte Notsituation verbreitet und um finanzielle Hilfe gebeten.
- Betrüger verschicken als Nachricht eines Sozialen Netzwerks getarnte Emails, welche Links zu manipulierten Webseiten enthalten. Über diese Webseiten wird dann **Schadsoftware** übertragen. Von einigen Sozialen Netzwerken angebotene Zusatz-Anwendungen, wie Mini-Spiele o.ä. stammen von Drittanbietern, deren Sicherheitsstandards nicht denen des Sozialen Netzwerks entsprechen und so Schadprogramme verbreiten können.
- In Sozialen Netzwerken erhält **Mobbing** eine neue Qualität: Beschimpfungen, Bloßstellungen und Ausgrenzungen erfolgen anonym und setzen andere oft unter Druck. Zudem können über falsche Profile Personen anonym ausgespäht und gestalkt werden oder Kinder und Jugendliche werden sexuell belästigt. Ebenso können Profile im Namen einer Person erstellt werden, auf denen falsche Informationen und Behauptungen verbreitet werden. Die betreffenden Personen erfahren oft erst sehr spät davon.

- Wenn Soziale Netzwerke auf mobilen Endgeräten über Apps genutzt werden, können sensible Daten wie Adressbuch, Fotos, Videos oder Standortangaben abgegriffen werden, die auf dem Mobilgerät vorhanden sind.
- Ein Zugang zu Webseiten oder Internetshops über beispielweise ein Facebook-, Google- oder Amazon-Konto („Single Sign-on“) ist mit einigen Daten-Risiken verbunden. Der Vorteil liegt wie meist in der Bequemlichkeit, da keine aufwändige Neuregistrierung und kein neues Passwort nötig sind. Fällt das Passwort aber über Phishing oder eine Hackerattacke an Unbefugte, erhalten sie Zugang zu allen Konten mit der entsprechenden Login-Möglichkeit. Noch höher ist das Risiko, falls ein Anbieter die Login-Daten nicht verschlüsselt speichert. Zudem können individuelle Verbraucherprofile mit Informationen zu Verhalten und Nutzung über etliche Internetseiten hinweg ergänzt werden.
- Zudem ist zu bedenken, dass einmal ins Internet gestellte Daten durch Suchmaschinen aufgefunden werden können. Stehen die Daten im Netz, können sie von jedem kopiert und weiterverbreitet werden. Daten können nur sehr schwer aus dem Internet gelöscht werden. Und selbst das neue **Recht auf Vergessen** gilt nur begrenzt.

Was können Verbraucher tun?

- Datenvermeidung und Datensparsamkeit.
- Sich über Nutzungs- und Datenschutzbestimmungen informieren, auch wenn es lästig ist.
- Auf hohe Privatsphäre- und Sicherheitseinstellungen achten und regelmäßig aktualisieren.
- Widerruf der Einwilligung zur Nutzung der Daten, wenn der Dienst nicht mehr verwendet wird.
- Der Nutzung und Übermittlung von Daten zum Zweck der Werbung, Markt- oder Meinungsforschung grundsätzlich widersprechen.
- Nutzungsrechte eingestellter Bilder, Texte und Informationen überprüfen, keine weitreichenden Rechte für den Seitenbetreiber einräumen und der Verwendung und Weitergabe seiner Daten widersprechen.
- Kontaktanfragen stets auf Echtheit des Absenders hinterfragen.
- Über das Betriebssystem Berechtigungen für Apps einschränken, alternativ soziale Netzwerke über einen Internetbrowser nutzen.
- Sichere Passwörter verwenden. Passwörter schützen.
- Cookies auf dem Endgerät löschen; dies erschwert es, Nutzerverhalten nachzuvollziehen.
- Radikal, aber wirksam: aus Sozialen Netzwerken austreten, Facebook & Co. löschen und andere Kommunikations- und Informationskanäle sorgfältig auswählen.

Was sagt das Verbraucherrecht?

Soziale Netzwerke bewegen sich an der noch wenig beleuchteten Schnittstelle von Datenschutz-, Verbraucher- und Medienrecht.

Datenschutzrecht

Die Daten der Nutzer sind die Ressourcen, auf denen alle Sozialen Netzwerke aufbauen. Einmal geht es also darum, unter welchen Bedingungen die sozialen **Netzwerke Daten sammeln** dürfen. (Die Voraussetzungen an die Einwilligung und die zulässigen Grenzen der Datensammlung werden im Steckbrief Dark Patterns erörtert.)

Vor allem die Nutzung der von den Sozialen Netzwerken und dort auch von Dritten gesammelten Daten für Werbezwecke hat die Frage aufgeworfen, wer die **„für die Datenverarbeitung Verantwortliche Person oder Stelle“** ist, die der Gesetzgeber vorsieht. Der Verbraucher muss wissen, gegen wen er sich wenden muss und gegen wen er seine Recht durchsetzen kann. Nach der Datenschutzgrundverordnung (Art. 4 Nr. 7 1. Hs. DSGVO) ist verantwortlich jede „natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen

über die **Zwecke und Mittel der Verarbeitung** von personenbezogen Daten entscheidet“. Für den Verbraucher ist aber genau das nicht leicht zu erkennen, weil insbesondere an der Verarbeitung der Daten mehrere Personen beteiligt sein können. In gleich vier Entscheidungen hat der EuGH die Anforderungen an die Verantwortungsverteilung präzisiert (EuGH Urt. v. 29. 7. 2019 – C-40/17, ECLI:EU:C:2019:629 – Fashion ID; EuGH Urt. v. 10. 7. 2018 – C-25/ 17, ECLI:EU:C:2018:551 – Zeugen Jehovas; EuGH Urt. v.5.6.2018 – C-210/16, ECLI:EU:C:2018:388 – Fanpage; EuGH Urt. v. 13.5.2014 – C-131/12, ECLI:EU:C:2014:317 – Google Spain). In zwei Verfahren ging es um eine internetbezogene Datenverarbeitung durch Verwendung von sogenannten Tracking-Technologien, sodann um die Nutzung von Fanpages auf Facebook, und zuletzt um einen Webseitenbetreiber, der für seine Webseite das Social Plug-in „Gefällt mir“ von Facebook integriert hatte.

Grundsätzlich formuliert der EuGH darin aus Verbrauchersicht eher erfreulich niedrige Voraussetzungen an das Vorliegen gemeinsamer Verantwortlichkeit. Damit stehen dem Verbraucher gleich mehrere Verantwortliche gegenüber, an die er sich wenden kann. Nicht jeder der Beteiligten muss direkten Zugang zu den betroffenen personenbezogenen Daten haben, es reicht aus, wenn weitere Beteiligte von der Verarbeitung profitieren. Jeder, der aus Eigeninteresse auf die Verarbeitung personenbezogener Daten Einfluss nimmt und dadurch an der Entscheidung über die Zwecke und Mittel dieser Verarbeitung mitwirkt, kann nach Ansicht des EuGH als Verantwortlicher gelten (Rammos 2020, § 25, Rdnr. 79 ff).

Kartellrechtliche Kontrolle von Nutzungsbedingungen

In der digitalen Wirtschaft rückt das Datenschutzrecht mit dem Verbraucherrecht (einschließlich des Lauterkeitsrechts des UWG) immer näher zusammen. Bereits jetzt untersuchen Verbraucher- und Datenschutzbehörden sowie Nichtregierungsorganisationen die Datenpraktiken verschiedener Online-Händler anhand der Lauterkeits- und Datenschutz-Regeln. Ob dies zu einer direkteren Verknüpfung zwischen UWG und DSGVO führt und damit den Umfang der den Verbrauchern zur Verfügung stehenden Rechtsmittel erweitern könnte, steht noch offen. Ein solch integrierter Ansatz wurde kürzlich vom **Bundeskartellamt** in Bezug auf **Facebook** angewandt: Facebook verwendet Nutzungsbedingungen, die auch die Verarbeitung und Verwendung von Nutzerdaten vorsehen, die bei einer von der Facebook-Plattform unabhängigen Internetnutzung erfasst werden. Im Klartext: Private Facebook-Nutzer müssen bei der Anmeldung den Nutzungsbedingungen von Facebook zustimmen, um das Soziale Netzwerk nutzen zu können. Hiermit wird auch eine Einwilligung des Nutzers verlangt, für die Verwendung personenbezogener Daten, welche aus der Nutzung anderer konzerneigener Dienste (z.B. WhatsApp und Instagram) entstehen oder durch den Aufruf von Drittseiten (Off-Facebook Daten).

Das Bundeskartellamt hatte Facebook untersagt, solche Daten ohne weitere Einwilligung der privaten Nutzer zu verarbeiten (BKartA Beschl. v. 6.2.2019 – B6–22/16). Der Kartellsenat des Bundesgerichtshofs hat am 23.6.2020 im Eilverfahren entschieden, dass **dieses Verbot vom Bundeskartellamt vorläufig durchgesetzt** werden darf **(**KVR 69/19 - Beschluss vom 23. Juni 2020). Diese Eilentscheidung lässt erwarten, dass der BGH das Verbot in der noch ausstehenden endgültigen Entscheidung bestätigen wird. Die Kontrolle missbräuchlicher Datenschutzpraktiken könnte damit auch über das Kartellrecht erfolgen, sofern das Unternehmen über eine marktbeherrschende Stellung verfügt.

Medienrecht

Der Einsatz von Algorithmen und KI-Systemen in Sozialen Netzwerken wirft angesichts der vielfältigen (häufig unbemerkten) Möglichkeiten der Einflussnahme auf Informationswahrnehmung, Meinungsbildung und -äußerung durch Auswahl und Filterung von Informationen, Social Bots, Deep Fakes und Fake News allerdings die Frage auf, wie in einer algorithmisch gesteuerten Gesellschaft **Meinungsbildungsfreiheit** und **Medienpluralität** aufrechterhalten werden können. Beide sind tragende Säulen demokratischer Gesellschaften (Ebers 2020). Das geltenden Recht bietet bislang nur wenige Anhaltspunkte und ist selbst für Juristen von einer verwirrenden Komplexität. Neben dem

Unionsrecht, dem Grundgesetz, Bundesgesetzen sind auch die landesrechtlichen Regeln zu beachten. Schließlich garantiert das Grundgesetz den Ländern die Kompetenz in Rundfunk und Fernsehen. Der novellierte Medienstaatsvertrag regelt die Zusammenarbeit der Länder und erstmals auch die Anbieter von Telemedien, wie es in der Rechtssprache heißt. Dazu gehören: Soziale Medien und Blogs, Chatrooms, Spiele-Apps, Informationsdienste, Webportale und private Websites, Webshops, Online-Auktionshäuser, Suchmaschinen, Webmail-Dienste, Podcast, Dating-Communities. Sie sind (nach § 18 Abs. 3) Medienstaatsvertrag verpflichtet, bei mittels eines Computerprogramms automatisiert erstellten Inhalten oder Mitteilungen den Umstand der Automatisierung (also Social Bots) kenntlich zu machen, sofern das hierfür verwandte Nutzerkonto seinem äußeren Erscheinungsbild nach für die Nutzung durch natürliche Personen bereitgestellt wurde. Dem Inhalt oder der Mitteilung ist der Hinweis gut lesbar bei- oder voranzustellen, dass dieser oder diese unter Einsatz eines das Nutzerkonto steuernden Computerprogrammes automatisiert erstellt und versandt wurde.

Wie der novellierte Staatsvertrag deutlich macht, steht die rechtspolitische Diskussion erst am Anfang (vgl. Berberich & Conrad, 2020). Bei der Suche nach den geeigneten Lösungen ist vor allem eines wichtig: Die sozialen Netzwerke **überschreiten** mit den hoch effektiven Möglichkeiten der Einflussnahme auf die Meinungsbildung und -äußerung (und damit auf das Wahlverhalten) den **rein wirtschaftlichen Kontext** ihrer Tätigkeit. Sie sind eben nicht „nur“ Plattformen, sondern auch für die Inhalte mitverantwortlich. Das ist insofern zentral, weil die Europäische Union bislang in der Regulierung des **E-commerce** und der **Plattformregulierung**, kurz all dem, was heute unter digitaler Wirtschaft verstanden wird, der Taktgeber ist. Die Europäische Union hat aber keine Gesetzgebungskompetenz, wenn es um den politischen Raum geht. Hier sind allein die Mitgliedstaaten bzw. in Deutschland die Bundesländer verantwortlich.

Belege und weiterführende Literatur

Berberich, M., & Conrad, A. (2020 im Erscheinen). § 30: Plattformen und KI. In M. Ebers, C. Heinze, T. Krügel, & B. Steinrötter (Hrsg.), *Künstliche Intelligenz und Robotik* (1. Aufl.). München: C. H. Beck.

Boers, E., Afzali, M. H., Newton, N., & Conrod, P. (2019). Association of screen time and depression in adolescence. *JAMA Pediatrics*, *173*(9), 853–859. https://doi.org/10.1001/jamapediatrics.2019.1759

Bundesamt für Sicherheit in der Informationstechnik (BSI). (2019). *Soziale Netzwerke* (Broschüre). Bonn: Bundesamt für Sicherheit in der Informationstechnik (BSI). https://www.bsi-fuer-buerger.de/SharedDocs/Downloads/DE/BSIFB/Broschueren/Brosch_A6_Soziale_Netzwerke.pdf?__blob=publicationFile&v=7

DAK-Gesundheit. (2018). *WhatsApp, Instagram und Co. – so süchtig macht Social Media* (DAK-Studie: Befragung von Kindern und Jugendlichen zwischen 12 und 17 Jahren). Hamburg: DAK-Gesundheit. https://www.schau-hin.info/fileadmin/content/Downloads/Sonstiges/dak-studie-sucht-nach-sozialen-medien.pdf

Ebers, M. (2020 im Erscheinen). § 3 Regulierung von KI und Robotik. In M. Ebers, C. Heinze, T. Krügel, & B. Steinrötter (Hrsg.), *Künstliche Intelligenz und Robotik* (1. Aufl.). München: C. H. Beck.

Feierabend, S., Rathgeb, T., & Reutter, T. (2020). *JIM-Studie 2019. Jugend, Information, Medien* (Basisuntersuchungzum Medienumgang 12- bis 19-Jähriger). Stuttgart: Medienpädagogischer Forschungs-verbund Südwest (mpfs). https://www.mpfs.de/fileadmin/files/Studien/JIM/2019/JIM_2019.pdf

Krügel, T., & Pfeiffenbring, J. (2020 im Erscheinen). § 11: Datenschutzrechtliche Herausforderungen von KI und Robotik. In M. Ebers, C. Heinze, T. Krügel, & B. Steinrötter (Hrsg.), *Künstliche Intelligenz und Robotik* (1. Aufl.). München: C. H. Beck.

Leest, U., & Schneider, C. (2017). *Cyberlife II Spannungsfeld zwischen Faszination und Gefahr Cybermobbing bei Schülerinnen und Schülern* (Zweite empirische Bestandsaufnahme bei Eltern, Lehrkräften und Schülern/innen in Deutschland (Folgestudie von 2013)). Karlsruhe: Bündnis gegen Cybermobbing e.V. https://www.schau-hin.info/fileadmin/content/Downloads/Sonstiges/Buendnis_gegen_Cybermobbing_Studie_2017.pdf

Micklitz, H.-W., Namyslowska, M., & Jablonowska, A. (2020 im Erscheinen). § 6 KI und Verbraucherrecht. In M. Ebers, C. Heinze, T. Krügel, & B. Steinrötter (Hrsg.), *Künstliche Intelligenz und Robotik* (1. Aufl.). München: C. H. Beck.

Moll, R., Horn, M., Scheibel, L., & Rusch-Rodosthenous, M. (2018). *Soziale Medien und die EU-Datenschutzgrundverordnung – Teil I. Informationspflichten und datenschutzfreundliche Voreinstellungen* (Eine Untersuchung der Verbraucherzentralen). Düsseldorf: Verbraucherzentrale NRW. https://www.verbraucherzentrale.de/sites/default/files/2019-11/bericht_soziale_medien_dsgvo_i.pdf

Rammos, T. (2020 im Erscheinen). § 25: Smart Devices & Wearables. In M. Ebers, C. Heinze, T. Krügel, & B. Steinrötter (Hrsg.), *Künstliche Intelligenz und Robotik* (1. Aufl.). München: C. H. Beck.

Verbraucherzentrale. (24. Mai 2018). Sicheres Surfen in sozialen Netzwerken: Mit persönlichen Daten und Reizen geizen. *Verbraucherzentrale.de*. https://www.verbraucherzentrale.de/wissen/digitale-welt/soziale-netzwerke/sicheres-surfen-in-sozialen-netzwerken-mit-persoenlichen-daten-und-reizen-geizen-10620. Abgerufen 15. August 2020

Verbraucherzentrale. (16. Januar 2019). Soziale Medien: Verstöße gegen die DSGVO. *Verbraucherzentrale.de*. https://www.verbraucherzentrale.de/aktuelle-meldungen/digitale-welt/soziale-medien-verstoesse-gegen-die-dsgvo-30411. Abgerufen 15. August 2020

Verbraucherzentrale. (21. April 2020). So verbieten Sie Apps bei Facebook den Zugriff auf Ihre Daten. *Verbraucherzentrale.de*. https://www.verbraucherzentrale.de/wissen/digitale-welt/soziale-netzwerke/so-verbieten-sie-apps-bei-facebook-den-zugriff-auf-ihre-daten-24601. Abgerufen 15. August 2020

Informationsseiten

https://mlr.baden-wuerttemberg.de/de/unsere-themen/verbraucherschutz/algorithmen/social-media/

https://www.bsi-fuer-buerger.de/BSIFB/DE/DigitaleGesellschaft/SozialeNetze/sozialeNetze_node.html

https://www.verbraucherportal-bw.de/,Lde/Startseite/Verbraucherschutz/Verantwortungsvolle+Nutzung+sozialer+Netzwerke

https://www.verbraucherzentrale.de/wissen/digitale-welt/soziale-netzwerke

https://www.schau-hin.info/soziale-netzwerke

Telematiktarife

Was sind Telematiktarife?

Der Begriff Telematik setzt sich zusammen aus Telekommunikation und Informatik und beschreibt die Möglichkeit von **Versicherungsunternehmen**, ihren Kunden Tarife aufgrund ihres eigenen Verhaltens – etwa des Fahrverhaltens oder des Gesundheitsverhaltens – anzubieten und damit eine günstigere Prämie zu verlangen. Eingesetzt werden solche Tarife in Deutschland bislang fast ausschließlich bei Kfz-Versicherungen – sogenannte „**Pay as you drive"-Tarife.** Auch im Gesundheitsbereich **(„Pay as you live"** oder **PAYL-Tarife**) gibt es vergleichbare Ansätze der Tarifierung von Krankenversicherungen (Weichert 2018). Allerdings setzt das Gesetz diesen (noch) enge Grenzen und macht sie (noch) eher unattraktiv (siehe unten). Gleichwohl ist es wahrscheinlich, dass durch die hohe Verbreitung und Akzeptanz von sogenannten **Wearables** (Fitnessarmbänder, Smart Watches u.ä.), die eine große Bandbreite an Gesundheitsdaten erfassen und zur Weiterverarbeitung übertragen, auch hier Telematiktarife verstärkt angeboten werden (Selke & Betz 2019);

Im KfZ-Bereich werden mithilfe einer Telematik-Box, oder alternativ auch über eine App auf dem Smartphone, laufend digitale Fahrtdaten gesammelt und direkt an die Kfz-Versicherung übertragen. Das individuelle, prämienbestimmende Risiko wird mit Hilfe von **Algorithmen** durch einen Dienstleister ermittelt. Telematiktarife werden also nicht wie klassische Tarife nur über den Fahrzeughalter und den Fahrzeugtyp berechnet, sondern auch basierend auf dem konkreten Fahrverhalten, das in einen **Score** eingeht (SVRV 2018). Aufgrund verschiedener Parameter, die für ein Score-Modell herangezogen werden, soll die Wahrscheinlichkeit und die Häufigkeit eines Schadens vorausgesagt werden. Die Scores der Versicherungsunternehmen unterscheiden sich dabei sowohl nach Kriterien, die zur Berechnung herangezogen werden, sowie deren Gewichtung. Die Verbraucherzentrale Bayern listet folgende Daten auf, die erhoben werden: Da überhöhte *Geschwindigkeit* häufiger zu Unfällen führt, wird eine angepasste Geschwindigkeit belohnt; plötzliches *Bremsen* erhöht die Gefahr von Auffahrunfällen und deutet nicht auf eine vorausschauende Fahrweise hin; schnelle und starke *Beschleunigung* wirken sich negativ auf den Tarif aus; *Fahrverhalten in Kurven, d.h.* ruhige Lenkbewegungen und gute Kurvenlage, wirken sich günstig auf den Tarif aus; *Fahrzeiten und -orte:* Da bei schlechten Sichtverhältnissen in der Nacht die Unfallwahrscheinlichkeit steigt, sowie bei Fahrten im dichten Berufsverkehr, wirken sich häufige Fahrten in der Nacht und in der Stadt negativ aus.

Netzwerk	Ökonomischer Nutzen	Technischer Nutzen	Datenbezogener Nutzen
Versicherer	- Differenzierte Leistungsbereitstellung und Erlösgenerierung durch KI-basierte Risikoeinstufung - Weniger Schadensfälle	- Zugang zu KI-basiertem Scoring des Fahrstils	- Zugang zu datenbasiertem Score des Fahrstils
KI-Dienstleister	- Neuer Kunde für bestehende Technologie und Infrastruktur	- Anwendung und kontextspezifische Anpassung der eigenen, skalierbaren KI-Technologie	- Zugang zu Telemetriedaten zum Training der eigenen Software
Versicherungsnehmer	- Günstige, faire Policengestaltung für sicherheitsbewusste Versicherungsnehmer	- Funktionserweiterung des eigenen PKW um KI-basierte Unfallmeldung on Edge	- Datenbasiertes Feedback zum Fahrverhalten

Quelle: Lernende Systeme – Die Plattform für Künstliche Intelligenz (2020, S. 22-23).

Versicherte, die vorausschauend und aufmerksam fahren und dazu bereit sind, ihr Fahrverhalten an die Versicherung zu übermitteln, können für ihre rücksichtsvolle und defensive Fahrweise Nachlasse auf die Versicherungsprämie erhalten. Dies kann sich insgesamt positiv auf die Verkehrssicherheit auswirken. Durch den laufenden Datenabfluss ermöglichen solche Tarife dem

Versicherungsunternehmen aber auch, ihre Kunden auf diese Weise zu überwachen, Bewegungsprofile zu erstellen und Risiken abzubilden und zu speichern.

Verbreitung

In Deutschland bieten derzeit elf Versicherungsunternehmen 15 Telematiktarife in der **Kfz-Haftpflichtversicherung** an. Allerdings sind dies keine eigenständigen Tarife, sondern ausschließlich zusätzliche Angebotsoptionen, wie ein „Carfinder“ oder ein „Unfallkartenschreiber“. Stand heute bietet kein Unternehmen in Deutschland ausschließlich Telematiktarife an. Insgesamt sind Scoring-Verfahren im Bereich von Kfz-Versicherungen noch nicht so weit verbreitet wie man aufgrund der öffentlichen Diskussion vermuten könnte. Dies zeigt, dass das Missbrauchspotential für beachtlich gesehen wird und die Rechtslage noch nicht geklärt ist.

Die **Krankenversicherungen** bieten bis heute noch keine echten Telematiktarife an; allerdings gibt es erste Ansätze in Form von Zusatzangeboten. Vier der elf größten gesetzlichen Krankenkassen (Techniker und drei AOKs) boten im November 2019 PAYL Elemente in Bonusprogrammen an; bei den Privaten ist es hauptsächlich die Generali, die ein entsprechendes verhaltensbasiertes Bonus-Programm als Zusatzleistung anbietet (Selke & Betz 2019; SVRV 2018).

Herausforderungen

Durch die Übertragung der Fahrtdaten soll der Fahrstil der Versicherten ausgewertet und verbessert werden. Telematiktarife sollen damit insgesamt zu mehr Sicherheit im Straßenverkehr beitragen und erwünschtes Verhalten belohnen. Tatsächlich werden aber nicht nur der Fahrstil, sondern auch Daten zu den Fahrzeiten oder Orten, wie die Tageszeit und die Dauer einer Fahrt oder die Bevölkerungsdichte und der Straßentyp ausgewertet. Der Score wird also nicht ausschließlich vom Fahrverhalten beeinflusst, sondern auch von Variablen, auf welche Kunden keinen direkten Einfluss haben. Aus Verbrauchersicht ist es problematisch, dass hier keine Möglichkeit besteht, auf den gesamten Score Einfluss zu nehmen. Daten- und Verbraucherschützer bezeichnen dies als **Diskriminierung**.

Datenschutz ist ein ernstes Problem. Versicherungsunternehmen speichern und verarbeiten eine große Anzahl sensibler Verkehrsdaten von Verbrauchern. Auf der Grundlage dieser Daten kann nicht nur das Fahrverhalten überwacht werden, es können auch individuelle **Bewegungs- und Verhaltensprofile** erstellt werden; durch die gespeicherten Adressen und Zeiten kann auf große Teile des Privatlebens geschlossen werden. Dies ist wiederum für die personalisierte Werbung interessant, die sowohl Ergebnisse von Suchmaschinen entsprechend anzeigen als auch algorithmenbasierte **personalisierte Preise** anbieten kann (siehe Personalisierte Preise). Im Schadensfall könnten die Daten auch gegen die Versicherten verwendet werden.

Durch die eingesetzte Technik und den gestiegenen Verwaltungsaufwand entstehen hohe **Kosten** für Unternehmen und Verbraucher. Kosten oder Miete für eine GPS-Blackbox können unter Umständen die Ersparnis bei der Versicherungsprämie übersteigen. Alternativ können Daten über eine App gesichert werden. Auch hier sind zusätzliche Kosten möglich, z.B. durch weitere verpflichtende Versicherungsverträge oder die Beanspruchung von Datenvolumen. Es muss zudem daran gedacht werden, die Datenerfassung bei Fahrten als Beifahrer oder mit öffentlichen Verkehrsmitteln zu unterbrechen. Die in der Werbung versprochenen Rabatte der Telematiktarife stellen meist einen optimalen Wert dar, der durch häufiges Fahren in der Nacht oder im Berufsverkehr bereits nicht erreichbar ist.

Bei einer Zunahme von Telematiktarifen besteht die Gefahr, dass Risikomerkmale zunehmend individualisiert werden. Unverschuldet hohe Risiken müssen sehr teuer bezahlt werden oder werden im schlimmsten Fall nicht mehr versichert. Die Idee der Versicherung als **Solidargemeinschaf**t wird dadurch ausgehöhlt.

Auch verändert sich die Rolle der Versicherungsunternehmen. Sie sehen sich selbst nicht mehr nur in der Rolle eines Dienstleisters, der ein bestimmtes Risiko übernimmt und abdeckt, sondern als Berater an der Seite des Verbrauchers. Versicherungen wollen Hilfestellung anbieten im Umgang mit dem Risiko Auto oder Krankheit, so jedenfalls ihr Selbstverständnis. Grundsätzlich stellt sich die Frage, ob und inwieweit diese neue Beraterrolle von den bestehenden Gesetzen abgedeckt ist und ob den Versicherungsunternehmen aus dieser Beraterrolle treuhänderische Pflichten vor allem im Umgang mit den Daten erwachsen.

Verbraucherpolitische Forderungen

Der Sachverständigenrat Verbraucherfragen (2018) hat ein Gutachten u.a. zu Telematiktarifen und entsprechenden Scores vorlegt und folgende Forderungen formuliert:

- Scoring für Verbraucher verständlich machen
- Gesetzliche Garantie für Telematik-freie Optionen
- Diskriminierung prüfen und offenlegen
- Score-Verfahren offenlegen und auf Verbrauchergerechtigkeit überprüfen
- Aufsicht über Score-Verfahren stärken und verbessern
- Verbesserung der Datenqualität
- Werden Daten zur personalisierten Risikoeinschätzung verwendet, so sollte dies an enge Voraussetzungen geknüpft werden.

Ebenso hat sich die Deutsche Verbraucherschutzkonferenz (2019) jüngst umfänglich mit Telematiktarifen auseinandergesetzt und schlägt folgende Maßnahmen vor:

- Untersuchung der wirtschaftlichen Vorteile von Telematik-Programmen und der tatsächlich gewährten Prämienermäßigungen beispielsweise durch den Marktwächter Finanzen
- regelmäßige Mitteilung der Zahl der Telematik-Verträge an die BaFin, erforderlichenfalls Einführung einer gesetzlichen Mitteilungspflicht
- Leitlinien zur Verhinderung von unangemessener Diskriminierung (u.a. Zugang zu Telematiktarifen auch für Personen mit ungünstiger Disposition)
- Gewährung von Prämienermäßigungen auch bei Ausscheiden im Folgejahr (z.B. bei Vertragsbeendigung, Erreichen der Altersgrenze)
- „Datenbezogene Spartentrennung“ und Ausschluss einer kommerziellen Drittverwertung
- Absicherung eines Anspruchs auf Sicherheits-Updates durch die Versicherer
- Pflicht zur Vorlage der Vertragsbedingungen an die BaFin.

Was können Verbraucher tun?

- Datenschutzbestimmungen vor Vertragsabschluss aufmerksam prüfen: Werden personenbezogene Daten ausreichend geschützt? Welche Daten müssen übermittelt werden? Wann werden Daten gelöscht? Gibt es personalisierte Werbung?
- Auf Datensicherheit der Endgeräte achten.
- Überprüfen, ob die Versicherung Daten an weitere Vertragspartner oder an die Polizei herausgibt.
- Genau überlegen, ob sich die Ersparnis im Vergleich zur Freigabe von individuellen Bewegungsprofilen wirklich lohnt.

Was sagt das Verbraucherrecht?

Aus Verbrauchersicht berühren Versicherungsverträge über die Kfz-Haftplicht und die Krankenversicherung unterschiedliche Rechtsfelder: das Versicherungsaufsichtsrecht, das Versicherungsvertragsrecht, das Allgemeine Gleichbehandlungsgesetz, das AGB-Recht und schließlich

den Datenschutz. Hinzukommt, dass die rechtlichen Anforderungen je nach Versicherungstyp variieren. Hilfreich und auch für den Laien verständlich ist der Abschlussbericht der Verbraucherschutzkonferenz.

Allgemeines Gleichbehandlungsgesetz (AGG)

Nach § 20 Abs. 2 AGG dürfen Kosten bei personenbezogenen Versicherungen im Zusammenhang mit Schwangerschaft und Mutterschaft nicht zu unterschiedlichen Prämien oder Leistungen führen. Die Berücksichtigung von **Religion, Behinderung, Alter oder sexueller Identität** setzt voraus, dass dies nachweisbar „auf anerkannten Prinzipien risikoadäquater Kalkulation beruht". Versicherungen müssen offenlegen können, wie der Algorithmus eine bestimmte Prämienhöhe errechnet hat. Nach Art. 22 DSGVO und § 37 BDSG darf das im Prinzip nicht im Wege einer **ausschließlich** automatisierten Entscheidung erfolgen. Deutschland hat von der Möglichkeit Gebrauch gemacht, die Versicherungen in Grenzen von diesem Verbot freizustellen (§ 37 Abs. BDSG) (siehe zum Recht auf Überprüfung durch einen Menschen Steckbrief Sicheres Surfen).

Versicherungsaufsichtsrecht (VAG)

Für die Aufsicht über die Versicherungsunternehmen ist die Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) zuständig. Hauptziel der Aufsicht ist nach § 294 VAG der Schutz der Versicherten. Nach § 4 Abs. 1a FinDAG ist die BaFin zum **Schutz der kollektiven Verbraucherinteressen** verpflichtet und kann insoweit auch bei Verstößen gegen verbraucherschützende Vorschriften außerhalb des Versicherungsrechts tätig werden. Wie weit diese Verpflichtung reicht, ist nicht genau geklärt. Jedenfalls ist die Bafin nicht zu einer AGB-Kontrolle verpflichtet.

Die Vertragsbedingungen müssen der BaFin jedoch bei Pflichtversicherungen (Kfz-Haftpflicht, Krankenversicherung) vorgelegt werden. Die Details sind oft in einer eigenständigen Vereinbarung mit einem Drittunternehmen geregelt, das das Telematikprogramm betreut, und damit vom eigentlichen Versicherungsvertrag entkoppelt. Die Vertragsbedingungen der Telematikprogramme werden der BaFin nicht automatisch vorgelegt. Ein aufsichtsrechtlicher Rahmen, der sicherstellt, dass aktuelle Daten zur Verbreitung von Telematiktarifen verfügbar sind, fehlt, so die Verbraucherschutzminister Konferenz (2019).

Versicherungsvertragsrecht

Kfz-Haftpflicht: Ein über das Allgemeine Gleichbehandlungsgesetz (AGG) hinausgehendes generelles Gleichbehandlungsgebot von Versicherungsverträgen im Bereich der Kfz-Versicherungen findet sich nur in § 177 VAG für Versicherungsvereine auf Gegenseitigkeit. Versicherungsnehmer haben keinen Anspruch darauf, Schadensfreiheitsrabatte oder sonstige Prämien bei Wechsel des Versicherers zu übertragen. Telematiktarife **binden die Versicherungsnehmer** deshalb an das Vertragsunternehmen.

Krankenversicherung: Bei privaten Krankenversicherungen kann die individuelle Tarifeinstufung durch den Versicherer nach Vertragsschluss nicht mehr geändert werden, da Wesensmerkmal der Krankenversicherung die Übernahme des Risikos unbekannter Gesundheitsverläufe ist. Eine prämienwirksame Anpassung **nach Vertragsschluss** in Abhängigkeit von gesundheitsfördernden Aktivitäten oder einer Veränderung des Gesundheitszustandes des Versicherten ist **ausgeschlossen**. Dieses Verbot gilt auch für Krankentagegeldversicherung oder Zusatzversicherungen. §§ 146 Abs. 2, 138 Abs. 2 VAG formulieren ein **Gebot der Gleichbehandlung** bei der Bemessung der Prämien und Leistungen sowie ein **Verbot günstigerer Prämien** im Neukundengeschäft. Dies ist vor allem für Bonusprogramme von Bedeutung, bei denen gesundheitsbewusstes Verhalten im Rahmen der Überschussverteilung und Beitragsrückerstattung belohnt werden soll. Nach Auffassung der Verbraucherschutzminister-Konferenz (2019) schließt das Gleichbehandlungsgebot die Einführung einer eigenen Tarifgruppe für Versicherte aus, die für die Bereitschaft zur laufenden, telematikgestützten Übermittlung gesundheitsbezogener Daten mit günstigeren Prämien belohnt würden.

Datenschutzrecht

Die Datenerhebung bzw. Verarbeitung ist an die Einwilligung des Verbrauchers geknüpft (siehe grundsätzlich zu den Voraussetzungen an die Einwilligung Steckbrief Dark Patterns). Bei Telematik-Tarifen muss für die Versicherungsnehmer zudem transparent sein, dass **personenbezogene Daten** erhoben und **Persönlichkeitsprofile** anhand des individuellen Fahrverhaltens gebildet werden. Individuelle Fahrzeugeinstellungen erlauben Rückschlüsse auf den Fahrzeugführer. Insofern handelt es sich bei den Fahrdaten, die für die Telematik-Optionen im Kfz-Bereich erhoben werden, um personenbezogene Daten. Das gilt jedenfalls dann, wenn eine Verknüpfung mit der Fahrzeugidentifikationsnummer oder dem Kfz-Kennzeichen vorliegt.

Gesundheitsbezogene Daten stehen nach Art. 9 DSGVO unter besonderem Schutz (siehe Steckbrief Self-Tracking). Bereits bei einer spürbaren Schlechterstellung von Versicherten, die sich nicht zur Teilnahme an einem mit Vergünstigungen verbundenen Telematikprogramm bereit erklären, könnten nach Auffassung der Verbraucherminister-Konferenz Zweifel an der Wirksamkeit der Einwilligung bestehen. Aus Art. 7 Abs. 4 und Art. 9 DSGVO lässt sich ein Wahlrecht zwischen einem Tarif mit und ohne Erfassung verhaltensbezogener Daten ableiten. Diese Auslegung bedarf der richterlichen Anerkennung.

Scoring

Telematiktarife unterliegen den in § 31 Abs. 1 Nr. 2 BDSG (n.F.) aufgestellten Anforderungen an das **Scoring** (siehe Steckbrief Verbraucher-Scoring). Nur solche Daten dürfen erhoben werden, die für die Durchführung des Versicherungsvertrages und die Prognose des zu ermittelnden Risikos relevant sind. Die Verbraucherschutzministerkonferenz (2019) verlangt den Nachweis eines Wirkzusammenhangs zwischen den Scoring- Kriterien und der Unfallhäufigkeit und -schwere. Da dieser Wirkzusammenhang bislang nicht mit konkreten Zahlen belegt werden kann (SVRV 2018), sind die angewandten Scoring-Verfahren datenschutzrechtlich möglicherweise unzulässig.

AGB-Recht

Die Allgemeinen Geschäftsbedingungen (AGB) der Versicherer regeln die Details des Versicherungsvertrages. Eine besondere Bedeutung kommt der Kontrolle der AGBs durch die klagebefugten Verbraucherschutzorganisationen zu. Ein wichtiger Ansatzpunkt wäre die Transparenzkontrolle. Intransparente AGBs sind rechtlich unwirksam. Der Teufel steckt im Detail. Es fehlt an Gerichtsurteilen, die klare Vorgaben an transparente Telematiktarife formulieren. Insbesondere ist umstritten, ob und inwieweit aus dem Transparenzgebot Aufklärungspflichten folgen, die die Versicherer aktiv in ihren AGBs umsetzen müssen.

Belege und weiterführende Literatur

Datenethikkommission der Bundesregierung. (2019). *Gutachten der Datenethikkommission der Bundesregierung*. Berlin: Bundesministerium des Innern, für Bau und Heimat. https://www.bmjv.de/SharedDocs/Downloads/DE/Themen/Fokusthemen/Gutachten_DEK_DE.pdf?__blob=publicationFile&v=2.

Deutsche Verbraucherschutzkonferenz. (2019). *Telematiktarife im Versicherungsbereich* (Abschlussbericht der Projektgruppe der Arbeitsgemeinschaft Wirtschaftlicher Verbraucherschutz). Deutsche Verbraucherschutzkonferenz. https://www.verbraucherschutzministerkonferenz.de/documents/anlage-1_1559131158.pdf

Ebert, I. (2020 im Erscheinen). § 16: KI und Versicherung. In M. Ebers, C. Heinze, T. Krügel, & B. Steinrötter (Hrsg.), *Künstliche Intelligenz und Robotik* (1. Aufl.). München: C. H. Beck.

Lernende Systeme – Die Plattform für Künstliche Intelligenz. (2020). *Von Daten zu Wertschöpfung. Potenziale von daten- und KI-basierten Wertschöpfungsnetzwerken*. München: Lernende Systeme – Die Plattform für Künstliche Intelligenz. https://www.acatech.de/wp-content/uploads/2020/07/PLS_Booklet_Datenoekosysteme.pdf

Sachverständigenrat für Verbraucherfragen (SVRV). (2018). *Verbrauchergerechtes Scoring* (Gutachten des Sachverständigenrats für Verbraucherfragen). Berlin: Sachverständigenrat für Verbraucherfragen beim

Bundesministerium der Justiz und für Verbraucherschutz. https://www.svr-verbraucherfragen.de/wp-content/uploads/SVRV_Verbrauchergerechtes_Scoring.pdf

Selke, S., & Betz, S. (2019). *PAYL als neuer gesundheitsökonomischer Trend* (Whitepaper im Kontext des Forschungsprojekts „Big Data und Boni: Pay-as-you-live-Tarife (PAYL) im Gesundheitswesen – Technologische Voraussetzungen und gesellschaftliche Folgen“). Stuttgart: Ministerium für Wissenschaft, Forschung und Kunst Baden-Württemberg (MWK BW).

Verbraucherzentrale Bayern. (5. Dezember 2019). Telematiktarife in der KFZ-Versicherung. *Das Bayerische Verbraucherportal*. https://www.vis.bayern.de/finanzen_versicherungen/versicherungen/kfztelematik.htm. Abgerufen 15. August 2020

Verbraucherzentrale Bayern. (11. August 2020). Telematik-Versicherung: Geld sparen möglich, aber es gibt Kehrseiten. *Verbraucherzentrale Bayern*. https://www.verbraucherzentrale.de/wissen/geld-versicherungen/weitere-versicherungen/telematikversicherung-geld-sparen-moeglich-aber-es-gibt-kehrseiten-38399. Abgerufen 15. August 2020

Weichert, T. (2018). *Big Data im Gesundheitsbereich* (ABIDA-Gutachten Nr. 01IS15016A-F). https://www.abida.de/sites/default/files/ABIDA%20Gutachten-Gesundheitsbereich.pdf

Verbraucher-Scoring

Was ist Verbraucher-Scoring?

Der Begriff Scoring bezeichnet ein mathematisch-statistisches Verfahren, mit welchem die Wahrscheinlichkeit eines bestimmten Verhaltens in der Zukunft - und damit letztlich die Bonität von (möglichen) Kundinnen und Kunden - berechnet wird. Für diese Berechnung werden vergangenes Verhalten sowie weitere Merkmale (wie Wohnort, Vermögen oder Geschlecht) und in manchen Fällen auch digitale Bewegungs- und Kommunikationsdaten analysiert. Aus diesen Daten errechnen Algorithmen einen **Score-Wert**. Dieser kann dann z.B. entscheidend sein, ob und zu welchen Konditionen beispielsweise ein Kredit gewährt wird. Auch beim Abschluss eines Mobilfunkvertrages oder bei der Zahlungsart bestellter Waren kann der Score-Wert eine Bedeutung haben. Bei einem schlechten Wert kann der Mobilfunkvertrag abgelehnt werden oder man erhält Warenlieferungen ausschließlich über Vorkasse anstatt auf Rechnung. Zunehmende Digitalisierung und neue KI-basierte Möglichkeiten der automatisierten Datenauswertung und maschinellen Mustererkennung erhöhen die Möglichkeiten, das Verhalten von Verbraucherinnen und Verbrauchern anhand von solchen Werten recht präzise einzuschätzen und in Risikogruppen einzuteilen. KI und Algorithmen haben das Verbraucher-Scoring zwar keineswegs „erfunden“, verhelfen ihm jedoch zu höherer Präzision bei niedrigeren Kosten; und sie bringen neue Risiken wie Datenschutz, systematische Diskriminierung und Falschbewertungen (SVRV 2018) mit sich.

Auskunfteien wie die SCHUFA haben sich auf **Bonitäts-Scoring** spezialisiert und geben Banken, Mobilfunkfirmen oder Onlinehändlern Auskunft zur Kreditwürdigkeit der Kunden. Aufgrund der Zuordnung zu einer Vergleichsgruppe mit identischen Merkmalen wird das erwartete Risiko von Verbraucherinnen und Verbrauchern errechnet. Für jede Gruppe ergibt sich am Ende ein bestimmtes Risiko. Durch Bonitäts-Scorings werden Kreditausfälle vermindert und Informationsasymmetrien abgebaut, was bei verbrauchergerechter Durchführung sowohl auf der Anbieter- als auch auf der Kundenseite Transparenz und Vertrauen schaffen sowie Kosten sparen kann. Während die SCHUFA neben Kontaktdaten überwiegend Positivmerkmale über die Vertragstreue (z. B. Anzahl der Bankkonten, Kreditkarten, Kredit- und Leasingverträge) speichert, sammeln andere Unternehmen der Branche eine Vielzahl von Daten über Beruf, Einkommen, Vermögen, den Familienstand sowie Negativdaten, vor allem nicht bezahlte Forderungen. Besonders kritisch wird das sogenannte **Geo-Scoring** betrachtet, in das Angaben über „gute“ oder weniger gute Wohngegenden einfließen. Diesem sind daher rechtlich enge Grenzen gesetzt.

Neben den Bonitäts-Scores werden auch in anderen Bereichen Scores eingesetzt. Bekannte Beispiele sind solche **Social Scores**, die das „soziale Wohlverhalten“ von Bürgerinnen und Bürgern bewerten und damit den Zugang zu staatlichen Leistungen regulieren (SVRV 2018). Angesichts der sinkenden Such- und Sammelkosten für Big Data, der sich rasant entwickelnden Technologie KI-basierter lernender Algorithmen und der Leichtfertigkeit, mit der Nutzer ihre Daten im Internet gegen etwas Zeit, Geld oder Bequemlichkeit teilen, nutzen Unternehmen zunehmend mehr oder weniger umfangreiche **Verhaltens-Scores**. In diese gehen auch Bewegungs-, Interessens- und Meinungsdaten ein, systematisch gesammelt auf Sozialen Netzwerken (siehe Stichwort Soziale Netzwerke), Suchmaschinen oder Online Shopping-Portalen. Beim **Social Scoring** werden Posts in sozialen Netzwerken oder die Freundesliste einbezogen, aber auch technische Informationen zum genutzten Gerät, die Uhrzeit einer Bestellung oder das Bewertungsprofil bei eBay können eine Rolle spielen. Social Scores und Datensammlung in Sozialen Netzwerken (siehe Soziale Netzwerke) war im ehemals datensensiblen Deutschland lange ein Tabu; zunehmend wird diese Art der Datensammlung,-auswertung und -verwendung jedoch als Geschäftsmodell von Start-ups eingesetzt und unter Beteiligung der Verbraucher von online Plattformen wie booking.com praktiziert.

Scoring wird aus Verbrauchersicht meist negativ wahrgenommen, weil es nach Überwachung aussieht und weil es manchen Verbrauchern u.U. den Zugang zu Produkten oder (bei der „Miet-Schufa“) zu einer Wohnung erschwert. Oft befinden sich diese zudem in prekären Lebenslagen. Für Verbraucherinnen und Verbraucher kann eine auf formalisierten Scoring-Werten getroffene automatisierte Entscheidung auf Basis von Algorithmen jedoch durchaus gerechter sein als eine persönliche, von einzelnen Entscheidern – und deren Einstellungen oder Vorurteilen – beeinflusste. In der Literatur spricht man neuerdings vom Potential der **„Noise“-Reduktion** durch Algorithmen, wobei mit „Noise“ (also „Rauschen“) die Zufälligkeit von Entscheidungen (beispielsweise eines Kreditsachbearbeiters einer Bank oder einer Ärztin bei der Diagnose) gemeint ist. Algorithmen kennen keine Vorurteile oder Zufälle – allerdings nur, soweit sie entsprechend sorgfältig entwickelt werden und mit vorurteilsfreien Datensätzen trainiert wurden (Kahneman et al. 2021). Entscheidend ist, dass wichtige Entscheidungen nicht ausschließlich automatisiert getroffen werden, sondern einem menschlichen Entscheider als unabhängige und unbestechliche Entscheidungsgrundlage dienen.

Verbreitung

Scoring ist in der Kreditwirtschaft schon lange Routine, um Auskunft über die Kundenbonität zu erhalten. Neben dem Bonitäts-Scoring aufgrund verschiedener Merkmale, wird auch verhaltensbasiertes Scoring eingesetzt, zum Beispiel im Rahmen von Telematiktarifen bei Kfz-Versicherungen (siehe Stichwort Telematiktarife). Andere Scores, vor allem Social Scores, sind in Deutschland noch wenig verbreitet und werden von datensensiblen Verbrauchern eher abgelehnt. Sobald jedoch persönliche Vorteile und Versprechen wie erhöhte Sicherheit vor Kriminalität zu erwarten sind, kann sich dies ändern.

Herausforderungen

- Verbraucherinnen und Verbraucher können das komplexe Scoring-Verfahren **nicht nachvollziehen**. Die Berechnung der Score-Werte beim Kredit-Scoring ist ein Geschäftsgeheimnis und wird von Auskunfteien den Kunden gegenüber nicht offengelegt (den Landesdatenschutzbeauftragten und der Bundesanstalt für Finanzdienstleistungen allerdings durchaus). Bekannt sind meist nur die Merkmale, die in die Berechnung einfließen: die Anzahl der Girokonten, Kreditkarten und Handyverträge sowie laufende Kredite, die Dauer der Kreditbeziehung, die Anzahl der Versandhandelskonten und Wohnungswechsel. Aber auch der Wohnort, der Beruf, Einkommen, Geschlecht, Alter, Familienstand, werden teilweise in die Entscheidung einbezogen. Die Gewichtung der Merkmale bleibt den Verbrauchern unbekannt.
- Scoring kann direkt **diskriminierend** sein, wenn zur Berechnung des Scores geschützte Merkmale wie das Geschlecht, die Rasse oder die ethnische Gruppenzugehörigkeit einbezogen werden, die zu einem schlechteren Score-Wert führen. Häufig wirkt eine Diskriminierung aber indirekt, über die Auswertung von nicht geschützten Merkmalen, wenn zum Beispiel über die Körpergröße, Freizeit- und Konsumgewohnheiten auf das Geschlecht geschlossen wird.
- In den Score-Wert gehen vor allem bei Social Scores **sachfremde** Informationen ein, z.B. Beiträge in sozialen Netzwerken zur Bewertung der Bonität.
- Einige der gespeicherten Daten sind **falsch**, unvollständig oder beruhen auf Schätzwerten. Beispielsweise wird aufgrund fehlender Daten über den Vornamen das Alter von Verbraucherinnen und Verbrauchern geschätzt. Dies ist kaum zu vermeiden, aber die Korrektur muss einfach und zuverlässig möglich sein.
- Aufgrund der wachsenden Datenmengen in Händen weniger marktbeherrschender Internetfirmen, der Möglichkeiten des KI-basierten maschinellen Lernens sowie dem wachsenden Datenhandel als lukratives Geschäftsmodell besteht heute die Möglichkeit, Daten aus verschiedensten Lebensbereichen konkreten Verbraucherinnen und Verbrauchern zuzuordnen und in einer Datenbank zu einem **Super Score** (wie in China) zu vereinen.

Verbraucherpolitische Forderungen

Der Sachverständigenrat Verbraucherfragen (2018) hat folgende Forderungen für ein verbrauchergerechtes Scoring aufgestellt:

- Für Verbraucherinnen und Verbraucher muss die Berechnung des Score-Wertes verständlich und in Grundzügen nachvollziehbar sein.
- Offenlegung der wesentlichen Merkmale, die der Berechnung zugrunde gelegt werden, sowie ihre Gewichtung; Angaben, wann und an welche Vertragspartner der Score-Wert weitergegeben wurde.
- Mögliche Diskriminierungen prüfen und überwachen.
- Informationsmaterial erstellen, welches das Scoring-Wissen und die Kompetenzen von Verbraucherinnen und Verbrauchern fördert.
- Möglichkeiten für Aufsichtsbehörden, das Score-Verfahren auf Verbrauchergerechtigkeit zu überprüfen. Die bisherige Überprüfung durch die Landesdatenschutzbehörden reicht nicht aus.
- Verbesserung der Qualität der zugrunde gelegten Daten.
- Den Einsatz von Super Scores – wie sie etwa in China zur Überwachung der Bürgerinnen und Bürger eingesetzt werden – verbieten und verhindern.

Was können Verbraucher tun?

- Regelmäßig einen Überblick über das eigene Daten-Profil verschaffen: Welche Daten werden zu welchem Zweck gespeichert, woher stammen sie und an wen werden sie weitergegeben? Einmal im Jahr kann eine unentgeltliche Auskunft von Firmen und Auskunfteien verlangt werden.
- Bonitäts-Scores regelmäßig abfragen und ggf. sowohl bei der Auskunftei und dem Unternehmen, das falsche Daten übermittelt hat, korrigieren lassen: Unrichtige Angaben, die die Berechnung der Kreditwürdigkeit beeinflussen, müssen von den Auskunfteien korrigiert werden und eine allgemein verständliche Darstellung, wie der eigene Score-Wert zustande kommt und welche Bedeutung er für die Entscheidung hat, kann verlangt werden. Bei Verdacht auf falschen Score-Wert die Ombudspersonen der Schufa, der Versicherungen oder die Experten der Verbraucherzentralen einschalten.
- Bonitäts-Scores aktiv managen: Bankkonten, Handyverträge und Darlehen bündeln, denn jeder weitere Kredit kann den Score-Wert verschlechtern.
- Datenvermeidung und Datensparsamkeit: Grundsätzlich im Internet nur die Einwilligung für solche Datenverarbeitungen erteilen, die beispielsweise für die Nutzung einer App erforderlich sind. Zurückhaltung mit persönlichen Daten in Sozialen Medien.

Was sagt das Verbraucherrecht?

Vorgaben im Bundesdatenschutzgesetz

Deutschland ist im europäischen Maßstab einen Sonderweg gegangen: Seit 2009 ist Scoring im **Bundesdatenschutzgesetz** geregelt. Nach der Verabschiedung der Datenschutzgrundverordnung wurde das Bundesdatenschutzgesetz novelliert. Die Regelung in § 31 BDSG blieb im Kern erhalten. Sie ist auf das Bonitäts-Scoring zugeschnitten, erfasst also darüber hinaus gehende Formen des Social Scoring nicht. Den Kern der Regelung bilden die Mindestanforderungen, die an das Scoring gestellt werden und die über die Anforderungen in der Datenschutzgrundverordnung hinausgehen. Das Gesetz verlangt nämlich, dass zur Berechnung des Wahrscheinlichkeitswerts **„wissenschaftlich anerkannte mathematisch-statistische Verfahren“** eingesetzt werden müssen und dass die genutzten Daten **nachweisbar** für die Berechnung der Wahrscheinlichkeit des bestimmten Verhaltens **erheblich** sind. Das sogenannte „**Geo-Scoring**“ ist nicht verboten, die Verwendung ist jedoch an bestimmte Voraussetzungen geknüpft. So dürfen für die Berechnung des Wahrscheinlichkeitswerts nicht

ausschließlich Anschriftendaten genutzt werden; und wenn diese genutzt werden, muss die betroffene Person vor Berechnung des Wahrscheinlichkeitswerts über die vorgesehene Nutzung dieser Daten unterrichtet werden. Diese Unterrichtung ist zu dokumentieren. Jeder Betroffene hat einen Anspruch auf eine kostenlose Sore-Wert Auskunft pro Jahr.

Kein Recht auf Offenlegung des Score-Wertes

Noch unter der alten, aber im wesentlichen identischen Rechtsgrundlage hatte eine Verbraucherin auf **Offenlegung des Score-Wertes** geklagt, um Kenntnis über die **Gewichtung** der verwandten Merkmale zu erhalten. Der BGH hat dieses Ansinnen abschlägig beschieden (BGH Urteil vom 28. Januar 2014 - VI ZR 156/13). Ein durch eine Bonitätsauskunft der SCHUFA Betroffener hat zwar einen Anspruch auf Auskunft darüber, welche personenbezogenen, insbesondere kreditrelevanten Daten dort gespeichert sind und in die den Kunden der Beklagten mitgeteilten Wahrscheinlichkeitswerte (Score-Werte) einfließen. Jedoch ist die Schufa nicht verpflichtet, die sogenannte Score-Formel, also die abstrakte Methode der Score-Wertberechnung, mitzuteilen. Zu den als Geschäftsgeheimnis geschützten Inhalten der Score-Formel zählen nach Auffassung des BGH die in die Score-Formel eingeflossenen allgemeinen Rechengrößen, wie etwa die herangezogenen statistischen Werte, die Gewichtung einzelner Berechnungselemente bei der Ermittlung des Wahrscheinlichkeitswerts sowie die Bildung etwaiger Vergleichsgruppen als Grundlage der Scorekarten. Die gegen das BGH-Urteil eingelegte Verfassungsbeschwerde hat das Bundesverfassungsgericht (BVerfG) nicht zur Entscheidung angenommen. Auch eine Gesetzgebungsinitiative der Opposition (BT-Drucks. 18/4864), die Rechtslage zugunsten der Verbraucher zu ändern, ist gescheitert. Hier sollten auch „die verwendeten Einzeldaten, die Gewichtung der verwendeten Daten, die verwendeten Vergleichsgruppen und die Zuordnung der betroffenen Personen zu den Vergleichsgruppen, die in die Berechnung des Wahrscheinlichkeitswerts einfließen“ der Auskunftspflicht unterfallen.

Datenschutzgrundverordnung

Die Datenschutzgrundverordnung befasst sich nur indirekt mit dem Scoring. Art. 4 Nr. 4 DSGVO stellt klar, dass auch das sogenannte **Profiling** in den Anwendungsbereich fällt, formuliert jedoch keinen rechtlichen Konsequenzen. Diese können sich, wenn überhaupt, nur aus Art. 22 DSGVO ergeben. Dieser gewährt dem Bürger das Recht, nicht einer ausschließlich auf einer automatisierten Verarbeitung – einschließlich Profiling – beruhenden Entscheidung unterworfen zu werden, die dem Bürger gegenüber rechtliche Wirkung entfaltet oder ihn/sie in ähnlicher Weise erheblich beeinträchtigt. Diese Regelung weckt die Hoffung, dass die Europäische Union über das deutsche Recht hinausgeht. Art. 22 DSGVO stellt jedoch auf die **Ausschließlichkeit** der automatisierten Verarbeitung. Daran wird es im Regelfall beim Boniäts-Scoring fehlen. Dort wo ein bestimmter Score *prima facie* für einen menschlichen Entscheider (etwa eine Kreditbearbeiterin einer Bank) beachtlich ist, wird dieser Entscheider mit einiger Häufigkeit auf die dem Score zugrunde gelegten Daten des Betroffenen zurückgreifen und sich sodann ein eigenes Urteil bilden. Dann aber ist der Anwendungsbereich von Art. 22 DSGVO nicht eröffnet.

Die Auslegung der Reichweite des Art. 22 DSGVO obliegt dem EuGH. Angesichts der Bereitschaft des Gerichts, durchaus im Sinne des Datenschutzes zu entscheiden – man denke nur an das vom Gericht formulierte „**Recht auf Vergessen**“ – ist nicht auszuschließen, dass der EuGH Art 4 und 22 DSGVO eine andere Stoßrichtung gibt. Der Grundgedanke des § 31 BDSG, auf die Wissenschaftlichkeit der Methode abzustellen, ließe sich auf die DSGVO übertragen. Der „deutsche“ Ansatz wird im 71. Erwägungsgrund als Soll-Regelung immerhin erwähnt, so dass der EuGH sich drauf beziehen könnte. Genauso gut möglich ist aber auch, dass der EuGH im Hinblick auf die vollständige Harmonisierung der DSGVO die Konformität des § 31 BDSG mit dem Unionsrecht anzweifelt. Dagegen spricht die Entstehungsgeschichte des Art. 22 DSGVO: Die Mitgliedstaaten konnten sich schlicht nicht einigen, ob und wie eine europäische Regelung des Scoring aussehen sollte.

Belege und weiterführende Literatur

Bayerisches Staatsministerium für Umwelt und Verbraucherschutz. (16. Mai 2018). Scoring - Häufige Fragen und Antworten. *Das Bayerische Verbraucherportal*. https://www.vis.bayern.de/daten_medien/datenschutz/scoring.htm. Abgerufen 15. August 2020

Domurath, I., & Neubeck, I. (2019). *Verbraucher-Scoring aus Sicht des Datenschutzrechts* (Veröffentlichungen des Sachverständigenrats für Verbraucherfragen). Berlin: Sachverständigenrat für Verbraucherfragen beim Bundesministerium der Justiz und für Verbraucherschutz. https://www.svr-verbraucherfragen.de/wp-content/uploads/WP_Verbraucher-Scoring_und_Datenschutzrecht.pdf

Kahneman, D., Sibony, O., & Sunstein, C. R. (2021 bevorstehend). *Noise* (1. Aufl.). William Collins.

Ministerium für Ländlichen Raum und Verbraucherschutz Baden-Württemberg. (2020). #seiunberechenbar ... bei Finanzierungen. *Baden-Württemberg.de*. https://mlr.baden-wuerttemberg.de/de/unsere-themen/verbraucherschutz/algorithmen/finanzierung/. Abgerufen 15. Juni 2020

Sachverständigenrat für Verbraucherfragen (SVRV). (2018). *Verbrauchergerechtes Scoring* (Gutachten des Sachverständigenrats für Verbraucherfragen). Berlin: Sachverständigenrat für Verbraucherfragen beim Bundesministerium der Justiz und für Verbraucherschutz. https://www.svr-verbraucherfragen.de/wp-content/uploads/SVRV_Verbrauchergerechtes_Scoring.pdf

Verbraucherportal Baden-Württemberg. (19. Juli 2018). Scoring durch Auskunfteien – Bedeutung und Zulässigkeit. *Verbraucherportal Baden-Württemberg*. https://www.verbraucherportal-bw.de/,Lde/Startseite/Verbraucherschutz/Scoring+durch+Auskunfteien. Abgerufen 15. August 2020

Verbraucherzentrale. (3. Juli 2018). Scoring mit Kundendaten: So verlangen Sie Auskunft bei Schufa & Co. *Verbraucherzentrale.de*. https://www.verbraucherzentrale.de/wissen/digitale-welt/datenschutz/scoring-mit-kundendaten-so-verlangen-sie-auskunft-bei-schufa-co-12756. Abgerufen 15. August 2020

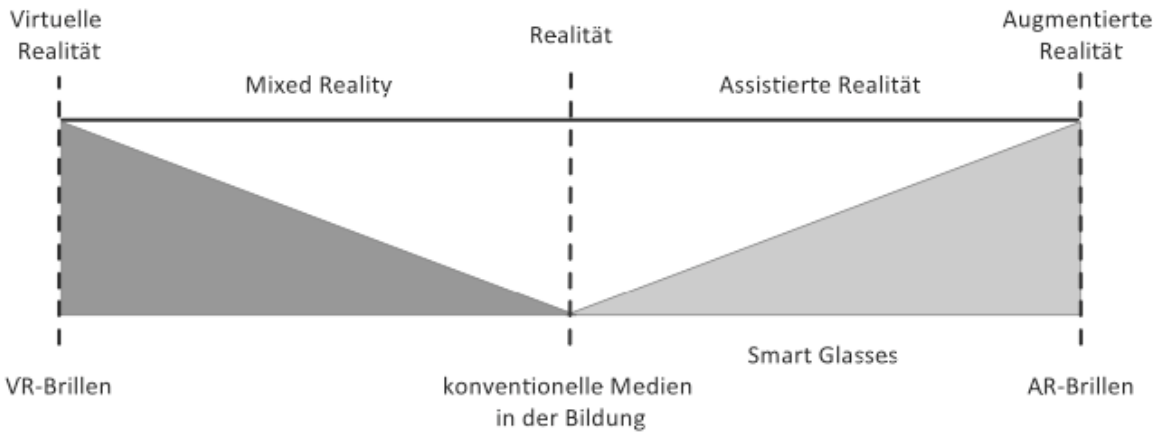
Verbraucherzentrale Hamburg. (o.J.). Was ist Scoring? *Verbraucherzentrale Hamburg*. https://www.vzhh.de/themen/finanzen/was-ist-scoring. Abgerufen 15. August 2020

Virtuelle und Erweiterte Realität

Was bedeutet „Virtual“ und „Augmented Reality“?

Virtual (virtuelle) (VR) und Augmented (erweiterte) Reality (AR) sind Ergebnis einer KI-basierten Technologie, bei der **computererzeugte Darstellungen von Bildern** künstliche oder veränderte Umgebungen unmittelbar erfahrbar machen. Bei der AR werden virtuelle und reale Räume vermischt und digital angereichert („erweitert“). Dies gelingt dann besonders gut, wenn die Technik in Brillen eingebaut, damit mobil und an die menschliche (Seh-)Wahrnehmung ideal angepasst ist. Dadurch können VRs eine bestimmte fiktive oder reale Umgebung vollständig abbilden, die sich auch beispielsweise unter Wasser oder im Weltall befinden kann. Durch die entsprechenden Brillen (sog. Head-Mounted Displays) kann das gezeigte Bild diese Umgebung interaktiv mit 360 Grad abbilden. Eine entsprechende Sensorik erfasst die Bewegungen des Kopfes und spiegelt diese in der digitalen Abbildung. Die in einer VR-Brille gezeigten Bilder sind für beide Augen leicht versetzt, so dass ein stereoskopischer Effekt entsteht. Bei ausreichender Prozessoren-Leistung haben Betrachter das Gefühl, in der VR präsent zu sein und in eine virtuelle Welt „einzutauchen“.

Bei der Augmented Reality wird die reale Umgebung mit virtuellen und computergenerierten Realitäten kombiniert, daher spricht man auch von **Mixed Reality** (Lampropoulos et al. 2020). Dabei werden zumeist Informationen oder virtuelle, dreidimensionale Elemente in das Sichtfeld des Benutzers eingeblendet. Diese wirken dann so, als wären sie in der realen Welt existent. Möbelstücke lassen sich probeweise in den eigenen vier Wänden platzieren und Kleidungsstücke anprobieren. Auch AR wird durch eine Brille erzeugt, die mit einer Kamera gleichzeitig die reale Umwelt filmt und abbildet, oder auch mit dem Smartphone. AR basiert zum Teil auf Bilderkennungsverfahren, die wiederum auf KI-Algorithmen aufgebaut sind. Bilderkennung basiert dabei in der Regel auf sogenannten Convolutional Neural Networks, ein Teilgebiet des Deep Learning bzw. des maschinellen Lernens.



Klassifikation von VR und AR (Quelle: Zobel et al. 2018, S. 28).

Anwendungen

Ein klassischer Einsatzbereich der VR für Endverbraucher sind Computerspiele, bei denen sich die Spieler in eine fiktive Welt begeben. Die erste marktreife Anwendung einer VR war der 1995 veröffentlichte „Virtual Boy“ von Nintendo, der jedoch an einer zu geringen Rechner-Kapazität der damaligen Computer scheiterte. VR findet heute in vielen Unterhaltungsmedien Anwendung. Bei (Sport-) Events haben die Zuschauer das Gefühl, dem Spiel inmitten von anderen Zuschauern/Teilnehmern zu folgen, vergleichbare Beispiele gibt es in der Kunst-, Musik- und Erotikbranche (Heuer 2020).

Jenseits des Unterhaltungswertes spielen VR und AR noch eine geringe, aber potentiell stark wachsende Rolle (Kind et al. 2019). Die wohl bekannteste Endnutzer-Anwendung der AR ist die Google Glass Brille, die Anfang 2012 auf den Markt kam, aber in Deutschland zu erheblichen Datenschutz-Diskussionen führte. Weniger problematisch sind Angebote wie bei Ikea, beispielsweise eine geplante Küche virtuell zu begehen oder Wohnungen einzurichten. Auch Navigations-Apps können mit AR deutlich verbessert werden; Bücher, Zeitschriften und Kataloge lassen sich mit AR-Inhalten erweitern (viele weitere Beispiele in: Kahlenborn et al. 2018). Im **Gesundheitsbereich** wird AR vielseitig eingesetzt, u.a. in der Krebsdiagnostik (Chen et al. 2019). In den Bereichen Fitness und der klinischen Rehabilitation gibt es virtuell unterstützte Laufbänder und Ergometer, im psychiatrischen und geriatrischen Bereich laufen vielversprechende Versuche. Gerade die AR eignet sich grundsätzlich, weil über die Stimme, mit Handgesten oder Steuerelementen wie Touchpads interagiert werden kann. Aufgrund der Ortunabhängigkeit werden AR-Anwendungen auch für **Lern- und Trainingszwecke** bei Militär oder in Unternehmen eingesetzt.

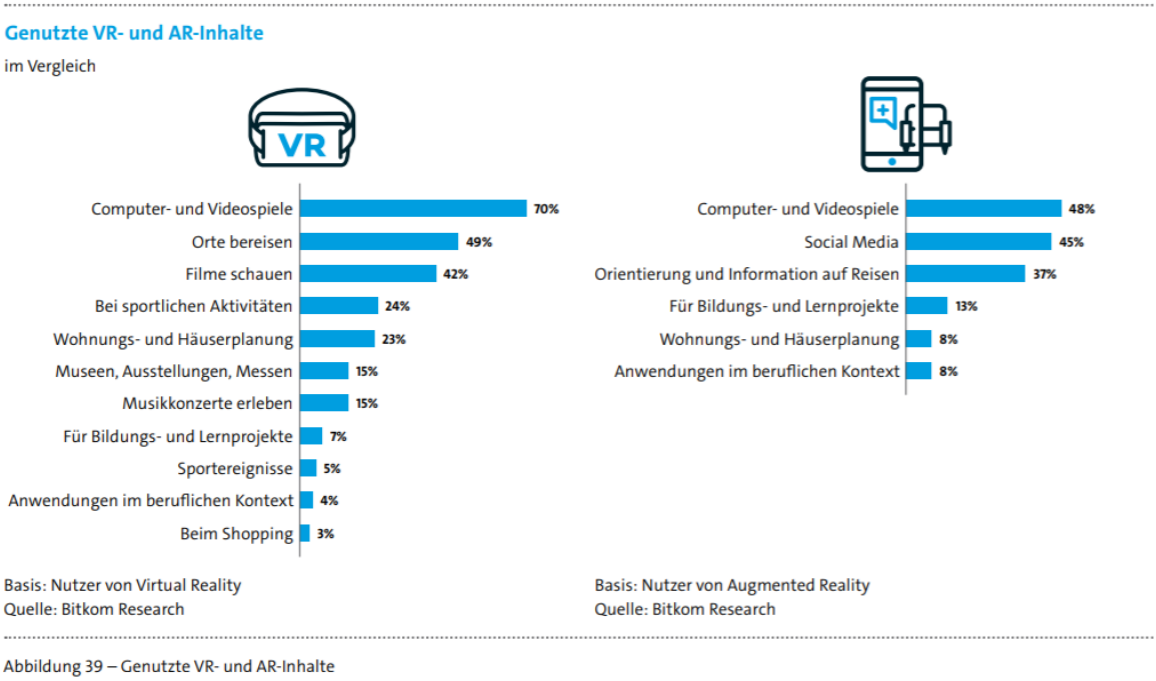


Abbildung 39 – Genutzte VR- und AR-Inhalte

Quelle: Klöß et al. (2019, S. 50).

Auch für die **Verbraucher- und Umweltarbeit** kann man sich vielversprechende Einsatzfelder der AR und MR vorstellen, da sie Empathie und Betroffenheit steigern können und gleichzeitig orts- und aufgabenspezifische Informationen vermitteln können. Beispiele sind die Assistenz im Alltag (Smartphone Apps mit Verbraucher- oder Umweltbezug), Einsatz in der Verbraucher- und Umweltbildung (Filme, Videospiele) sowie in der Produktberatung sowie in der Produktentwicklung mit Verbraucherpartizipation. Die Technik ist jedoch vergleichsweise teuer und daher hier noch kaum nicht-kommerziell genutzt. Die direkten und indirekten Umweltauswirkungen sind jedoch nicht zu vernachlässigen (Kahlenborn et al. 2018).

Herausforderungen

Auch wenn jenseits der Spielewelt Verbraucher bislang noch wenig mit VR und AR zu tun haben, wird davon ausgegangen, dass beide vermehrt unseren Alltag durchdringen werden. Da VR und AR datenbasiert agieren und ggf. große Datenmengen sammeln, bestehen wie bei allen KI-Anwendungen auch **Sicherheitsbedenken**, dass diese missbraucht werden könnten. Darüber hinaus bietet die Technologie die einzigartige Möglichkeit, Menschen gezielt zu **manipulieren** und Desinformation zu streuen. Dieses Risiko lässt sich anhand der hochprofessionellen Qualität von **Deep Fakes** (d.h. mit

Hilfe von KI bearbeitete oder gänzlich erstellte Videos) erahnen. Die emotionale Wahrnehmung und unmittelbare Erfahrbarkeit sind bei der VR und der AR deutlich intensiver als beispielsweise in einem Fernsehfilm oder einem klassischen Videospiel. Man denke nur an die in der Werbung eingesetzten Bilder, die auf das Lebensgefühl der Verbraucher zielen. Durch einen Hacking-Angriff könnten virtuelle und reale Situationen zur Unkenntlichkeit verschmolzen werden. Besonders im Bereich der AR, die in der Regel über eine Kamera und Sensorik verfügt, besteht die Gefahr, dass private Daten abgefangen und genutzt werden. Zudem können durch das ständige Senden von Standorten an den Hersteller der Spiele Bewegungsprofile erstellt werden.

Für eine verbrauchergerechte Regulierung in diesem Bereich spricht also vieles. Datenschutz, Datensicherheit, Nutzungsregeln von virtuellen Räumen u.a. sind noch weitgehend unterreguliert. Auf jeden Fall vergrößert sich der digitale Fußabdruck des Verbrauchers durch die Nutzung von VR und AR, allein schon dadurch, dass die Anwendung immer genau weiß, wo und wie lange ein Nutzer auf eine reale oder virtuelle Abbildung geschaut hat. Neben den Sicherheitsbedenken wird es neben erwünschten auch unerwünschte physische und psychischen Folgen geben. Diese sind noch weitgehend unbekannt und sollten auch im Verbraucherinteresse erforscht werden. Wie bei den sozialen Netzwerken auch verwischen sich im Einsatz von AR und VR die Grenzen zwischen dem wirtschaftlichen und dem politischen Verhalten der Verbraucher

Verbraucherpolitische Forderungen

- Datenschutz: Klarstellung durch den Gesetzgeber wünschenswert.
- Regelung, wenn urheberrechtlich geschützte Werke oder personenbezogene Daten von AR-Anwendungen erfasst werden (und ausgewertet werden).
- Datensicherheit gewährleisten.
- Schulung der Medienkompetenz von Kindern, Jugendlichen und Erwachsenen und eine grundlegende Aufklärung darüber, wie und durch wen Inhalte manipuliert werden können.

Was können Verbraucher tun?

- Informationen einholen, kritisch bleiben, Deep Fakes erkennen.
- Sichere Apps nutzen.
- Gesundheitliche Risiken bei starker Nutzung abklären.

Was sagt das Verbraucherrecht?

Strafrecht

Die mit dem Einsatz von AR und VR verbunden Rechtsfragen sind bislang wenig diskutiert. Wenn überhaupt dominiert in der Diskussion, inwieweit das **Strafrecht** geeignet ist, den Einsatz von **Deep Fakes** effektiv zu kontrollieren (dazu Steckbrief Identitätsdiebstahl). Das hängt auch damit zusammen, dass der praktische Einsatz von AR und VR jenseits von Computerspielen derzeit noch begrenzt ist. Dem Phänomen der Google Glass Brille am nächsten kommen Wearables, wenn Kleidungsstücke mit Kameras und Sensortechnik ausgerüstet werden (Rammos 2020).

Datenschutzrecht

Bislang richtet sich das Augenmerk vor allem auf die Auswirkungen von AR und VR im **Urheber**- und im **Datenschutzrecht**. Diskutiert werden die rechtlichen Konsequenzen des Einsatzes der Google Glass Brille **im öffentlichen Raum**. Die mit der Videoaufzeichnung verbundene Vervielfältigung wird allgemein nicht als Verletzung des § 16 Abs. 1 UrheberG angesehen. Eine Einwilligung der ‚gefilmten' Personen in die Datenerhebung und Verarbeitung ist praktisch undenkbar. Besondere Beachtung haben in Kfz eingebaute Dashcams gefunden, nicht zuletzt, weil mögliche Aufzeichnungen im Falle

eines Unfalls von herausragender Bedeutung sind. Rechtlich untersagt ist es, die Dashcams dauerhaft laufen zu lassen. Der anlassbezogene Einsatz ist dagegen möglich.

Wearables sind langfristig von besonderem Interesse, weil sie überall einsetzbar sind. Besonders problematisch ist es, wenn Wearables sensitive Daten sammeln. Bekanntlich verbietet Art. 9 DSGVO die Verarbeitung personenbezogener Daten, aus denen die Rasse, ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder auch die Gewerkschaftszugehörigkeit hervorgehen, sowie die Verarbeitung von genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person. Ist nun der Träger verantwortlich im Sinne des Datenschutzrechts, wenn er Wearables trägt (vgl. Identitätsdiebstahl)? Eine solche Rechtsauffassung würde den Kreis der Verantwortlichen über Gebühr ausweiten. Diskutiert wird deshalb, den Träger der Wearables als Verantwortlichen nur heranzuziehen, wenn er oder sie eine **Auswertungsabsicht** hat (Rammos 2020, Rdrn. 94 ff).

Urheberrecht

Urheberrechtlich ist die reine Sammlung von Daten über Wearables frei. Die gesammelten Daten könnten aber als eine Datenbank qualifiziert werden und damit Leistungsschutz nach dem Urheberrecht genießen. Aus der Sicht des Trägers der Wearables stellt sich die Frage, ob ihm oder ihr die Daten ‚gehören', aus der Sicht potenziell Betroffener, ob sie ein Recht auf Datenzugang haben. Die Diskussion ist noch sehr im Fluss (Rammos 2020, Rdnr. 111 ff).

Lauterkeitsrecht

Soweit AR und VR in der **Werbung** eingesetzt werden sollten, scheint das **Lauterkeitsrecht** am ehesten berufen, gegen die sich verwischenden Grenzen der realen Welt mit der virtuellen Welt vorzugehen. Das Lauterkeitsrecht verbietet die Irreführung durch Handeln, aber auch durch Unterlassen. Doch kennt das von der Union geschaffene Lauterkeitsrecht kein Informationsgebot, anders ausgedrückt, der Verbraucher hat im Lauterkeitsrecht keinen Anspruch auf die ‚Wahrheit'. Rechtlich sanktioniert wird nur die Irreführung. Lediglich in sehr eingeschränkten Grenzen lässt sich ein Informationsgebot formulieren, dass es Verbrauchern erlauben würde, AR und VR zu identifizieren. Das Verbraucherrecht vertraut durchgehend auf spezielle Informationspflichten. So könnte man sich vorstellen, dass Unternehmen, die VR und AR zum Einsatz bringen, diese kennzeichnen müssen. In der Vergangenheit haben sich jedoch gerade Kennzeichnungspflichten nur sehr begrenzt als ein taugliches Mittel des Verbraucherrechts erwiesen.

Belege und weiterführende Literatur

Chen, P.-H. C., Gadepalli, K., MacDonald, R., Liu, Y., Kadowaki, S., Nagpal, K., et al. (2019). An augmented reality microscope with real-time artificial intelligence integration for cancer diagnosis. *Nature Medicine*, *25*(9), 1453–1457. https://doi.org/10.1038/s41591-019-0539-7

Citron, D. K., & Chesney, R. (2019). Deep fakes: A looming challenge for privacy, democracy, and national security. *California Law Review*, *107*, 1753–1820. https://doi.org/10.15779/Z38RV0D15

Heuer, S. (2020). Virtual Reality: Schöne neue Welten. *brandeins*, *02/2020*. https://www.brandeins.de/magazine/brand-eins-wirtschaftsmagazin/2020/kommunikation/virtual-reality-schoene-neue-welten

Kahlenborn, W., Keppner, B., Uhle, C., Richter, S., & Jetzke, T. (2018). *Die Zukunft im Blick: Konsum 4.0: Wie die Digitalisierung den Konsum verändert* (Trendbericht zur Abschätzung der Umweltwirkungen). Dessau-Roßlau: Umweltbundesamt. https://www.umweltbundesamt.de/sites/default/files/medien/1410/publikationen/fachbroschuere_konsum_4.0_barrierefrei_190322.pdf

Kind, S., Ferdinand, J.-P., Jetzke, T., Richter, S., & Weide, S. (2019). *Virtual und Augmented Reality. Status quo, Herausforderungen und zukünftige Entwicklungen* (Arbeitsbericht Nr. 180). Berlin: Büro für Technikfolgen-Abschätzung beim Deutschen Bundestag (TAB). http://www.tab-beim-bundestag.de/de/pdf/publikationen/berichte/TAB-Arbeitsbericht-ab180.pdf

Klöß, S., Böhm, K., & Esser, R. (2019). *Zukunft der Consumer Technology – 2019. Marktentwicklung, Trends, Mediennutzung, Technologien, Geschäftsmodelle*. Berlin: Bitkom e. V. https://www.bitkom.org/sites/default/files/2019-09/190903_ct_studie_2019_online.pdf

Lampropoulos, G., Keramopoulos, E., & Diamantaras, K. (2020). Enhancing the functionality of augmented reality using deep learning, semantic web and knowledge graphs: A review. *Visual Informatics*, *4*(1), 32–42. https://doi.org/10.1016/j.visinf.2020.01.001

Rammos, T. (2020 im Erscheinen). § 25: Smart Devices & Wearables. In M. Ebers, C. Heinze, T. Krügel, & B. Steinrötter (Hrsg.), *Künstliche Intelligenz und Robotik* (1. Aufl.). München: C. H. Beck.

Wagener, A. (30. April 2020). Künstliche Intelligenz schafft alternative Realitäten. *Nerdwärts.de*. https://nerdwaerts.de/2020/04/kuenstliche-intelligenz-schafft-alternative-realitaeten/. Abgerufen 15. August 2020

Zobel, B., Werning, S., Berkemeier, L., & Thomas, O. (2018). Augmented- und Virtual-Reality-Technologien zur Digitalisierung der Aus- und Weiterbildung – Überblick, Klassifikation und Vergleich. In O. Thomas, D. Metzger, & H. Niegemann (Hrsg.), *Digitalisierung in der Aus- und Weiterbildung: Virtual und Augmented Reality für Industrie 4.0* (S. 20–34). Berlin, Heidelberg: Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-662-56551-3_2