Hintergrundpapier

23.10.2025

Hintergrundpapier zu Tracking und Datenverarbeitung der Digitalen Wirtschaft

Executive Summary

Dieses Dokument dient der sachlichen Aufklärung über Tracking- und Datenverarbeitung in der Digitalen Wirtschaft und soll die politische Debatte rund um den geplanten Digital Fairness Act auf eine faktenbasierte Grundlage stellen.

Ziel ist es, technische Fehlannahmen zu korrigieren, die tatsächlichen technischen Abläufe zu erklären und die Rolle von Tracking als zentrale Infrastruktur für nutzerorientierte digitale Angebote, Medienvielfalt und wirtschaftliche Wettbewerbsfähigkeit zu erläutern. Denn Tracking ist kein Selbstzweck, sondern ein essenzielles Instrument für die Sicherheit und zur Finanzierung, Optimierung und Personalisierung Digitaler Dienste und Angebote.

Unter Tracking verstehen wir die datengestützte Erhebung und Analyse von Nutzungsinformationen, um digitale Angebote für Verbraucher*innen relevanter, sicherer und effizienter zu machen. Es ermöglicht u. a. die Messung von Reichweiten und Werbewirkung, die Betrugsprävention, die Verbesserung der User Experience sowie die Ausspielung kontext- oder interessenbasierter Inhalte. Personalisierung ist heutzutage die Erwartungshaltung der Nutzer*innen – nicht die Ausnahme.

Die Digitale Wirtschaft ist ein hochvernetztes Ökosystem aus Digitalen Diensten, Publishern, Advertisern, Technologieanbietern und Intermediären. Insbesondere das offene, interoperable Internetist auf effiziente, datengestützte Werbe- und Messmechanismen angewiesen, um Vielfalt, Innovation und europäische Wettbewerbsfähigkeit sicherzustellen. Technische Standards wie das Transparency & Consent Framework gewährleisten dabei Datenschutz und Nutzerkontrolle bereits heute.

Die politische Diskussion ist aktuell häufig geprägt von der Sorge vor manipulativen oder unethischen Praktiken. Dieses Dokument stellt klar: Es existieren weder technologische Verfahren für eine kontinuierliche Emotionsauswertung im Alltag der Werbung, noch werden individuelle Vulnerabilitäten gezielt ausgenutzt. Profilbildung in besonders sensiblen Bereichen ist durch bestehendes Recht (insb. DSGVO, DSA) bereits ausgeschlossen und wird von der Branche nicht praktiziert.

Vor diesem Hintergrund plädieren wir für einen Fokus auf klare Begriffsdefinitionen, kohärente Durchsetzung bestehender Regeln und den Erhalt innovationsgerechter Rahmenbedingungen. Ein Digital Fairness Act kann nur dann wirksam und verhältnismäßig sein, wenn er Doppelregulierung vermeidet, technische Realitäten berücksichtigt und ein wettbewerbsfähiges offenes Internet in Europa sichert.

Kontakt

Daphne van Doorn | Head of EU Affairs | vanDoorn@bvdw.org

Philipp Hagen | Director Legal Affairs & Data Privacy | Hagen@bvdw.org

Hintergrundpapier

1. Inhaltsverzeichnis

Hintergrundpapier

Hintergrundpapier

1. Wofür ist das Dokument gedacht?

Dieses Dokument dient der fachlichen Aufklärung über Methoden und Zwecke von Tracking und Datenverarbeitung in der Digitalen Wirtschaft. Es soll einen Beitrag zur sachlichen Einordnung der politischen Debatte rund um den geplanten Digital Fairness Act leisten, insbesondere im Hinblick auf die Funktion und Notwendigkeit von datenbasierten Geschäftsmodellen im Bereich Online-Werbung und Inhalts-Personalisierung.

Ziel ist es, eine fundierte Faktenbasis zu schaffen, auf deren Grundlage Chancen, Risiken und mögliche Regulierungsansätze objektiv bewertet werden können. Gerade in einem Umfeld, in dem Diskussionen oftmals verkürzt geführt werden, möchten wir Transparenz über technische Abläufe, wirtschaftliche Zusammenhänge und bestehende Schutzmechanismen herstellen.

Das Dokument richtet sich an Entscheidungsträger*innen der Politik und Behörden, der Fachöffentlichkeit sowie an interessierte Stakeholder, die sich ein vertieftes Verständnis der technischen Grundlagen wünschen, um die Debatte differenziert und faktenorientiert führen zu können.

2. Über die Digitale Wirtschaft

Die Digitale Wirtschaft ist ein zentraler Treiber für Innovation, Wertschöpfung und Wettbewerbsfähigkeit in Deutschland und Europa. Sie umfasst nicht nur Plattformen und Technologieanbieter, sondern auch ein breit vernetztes Ökosystem aus Medienhäusern, Digitalen Diensten, Werbungtreibenden, Agenturen, Start-ups sowie Daten- und Infrastrukturprovidern. Digitale Angebote und datenbasierte Geschäftsmodelle sind heute nicht mehr nur Bestandteil einzelner Branchen, sondern strukturprägend für nahezu alle Wirtschaftsbereiche von Handel über Mobilität bis Bildung, Kultur oder Gesundheit.

Ein entscheidender Bestandteil dieses Ökosystems ist digitale Werbung. Sie ermögicht es Unternehmen, Nutzer*innen zielgerichtet zu erreichen und Geschäftsmodelle (insbesondere im offenen Internet) zu finanzieren. Tracking und datenbasierte Analyseverfahren kommen dabei vor allem zum Einsatz, um digitale Angebote zu verbessern, Nutzerinteressen besser zu verstehen, Werbeleistungen messbar zu machen und Betrug zu verhindern. Sie bilden die Grundlage für personalisierte Angebote und damit für die heutige Erwartungshaltung der Nutzer*innen, relevante und inspirierende Inhalte zu erhalten.

Dabei ist zwischen dem offenen (open) und dem geschlossenen (closed) Web zu unterscheiden. Im offenen Web erfolgt der Werbehandel über Standards, mit hoher Transparenz und Wettbewerb durch eine Vielzahl unabhängiger Publisher und Technologieanbieter. Im geschlossenen Web („Walled Gardens“) bündeln große Plattformen Daten, Werbeinventar und Ausspielung vollständig innerhalb eines proprietären Systems. Während geschlossene Ökosysteme hohe Reichweiten bieten und in ihrem System koordiniert vorgehen können, ist auch das offene Web essenziell für wirtschaftliche Vielfalt, Innovationskraft und die Unabhängigkeit europäischer Unternehmen.

Die Digitale Wirtschaft ist heute hochgradig arbeitsteilig organisiert. Intermediäre wie SSPs (Supply-Side-Plattformen), DSPs (Demand-Side-Plattformen), Ad Exchanges oder Consent-Management-Plattformen übernehmen spezialisierte Rollen, um Werbeflächen effizient zu vermarkten, rechtliche Anforderungen umzusetzen und den Wettbewerb zu stärken. Diese technologische Infrastruktur ermöglicht europäischen Unternehmen den Zugang zu regionalen oder globalen Märkten, unabhängig davon, ob sie selbst über große Plattformmacht verfügen.

Ziel des BVDW ist es, eine innovationsfreundliche und verantwortungsvolle Regulierung zu fördern, die Vertrauen schafft und gleichzeitig die Wettbewerbsfähigkeit europäischer Unternehmen sichert. Dazu gehört, bestehende Rechtsrahmen besser durchzusetzen, anstatt neue Hürden aufzubauen, und die Chancen datengestützter Wertschöpfung, wie auch durch Personalisierung oder neue technologische Entwicklungen im Sinne von Wirtschaft, Verbraucher*innen, Politik und Gesellschaft zu ermöglichen.

3. Was verstehen wir unter „Tracking“?

In der digitalen Wirtschaft bezeichnet Tracking das systematische Sammeln, Aggregieren und Verarbeiten von Daten über das Verhalten von Nutzer*innen im Internet. Neben dem Anwendungsfall der Werbung kommt Tracking unter anderem im Rahmen von Personalisierung von Inhalten und Services (Recommender Systeme wie z. B. auf e-Commerce-Seiten, Streamingseiten, Nachrichtenseiten, etc.) zur Anwendung.

Tracking verstehen wir als die datengestützte Erhebung und Verarbeitung von Nutzungsinformationen über digitale Angebote hinweg, um das Verhalten, die Interessen und Interaktionen von Nutzer*innen besser nachvollziehen zu können. Dazu zählen etwa Informationen über Seitenaufrufe, Interaktionsverläufe, genutzte Geräte oder wiederkehrende Besuche. Tracking bedeutet dabei nicht automatisch personenbezogene Profilbildung, sondern umfasst unterschiedliche technische Verfahren von Reichweiten- und Performance-Messung über Session-Analysen bis hin zu pseudonymisierten oder aggregierten Nutzungsdaten.

Eingesetzt wird Tracking vor allem, um digitale Angebote nutzerfreundlicher, sicherer und relevanter zu gestalten. Es ermöglicht die Optimierung des Nutzererlebnisses (User Experience) und die Messung von Kampagnenwirksamkeit in der Werbung. Zudem hilft es auch bei der Betrugsprävention sowie der Ausspielung kontext- oder interessenbasierter Inhalte und Werbung. Ziel ist es, Nutzer*innen Informationen bereitzustellen, die möglichst passgenau und hilfreich sind, und gleichzeitig Unternehmen in die Lage zu versetzen, digitale Geschäftsmodelle wirtschaftlich und wettbewerbsfähig zu betreiben.

4. Akteure der Digitalen Wirtschaft

a. Akteure im Kontext von Werbung

- *Advertiser*

Advertiser (Werbungtreibende) umfassen alle Unternehmen und Organisationen, die ihre Produkte, Marken oder Dienstleistungen digital bewerben möchten. Dazu gehören sowohl international operierende Konzerne als auch kleine und mittlere Unternehmen sowie innovative Start-ups. Ihr Ziel ist es, die richtigen Zielgruppen effizient anzusprechen, Markenbekanntheit zu steigern und langfristige Kundenbeziehungen aufzubauen. Dabei steht im Mittelpunkt, Marketingbudgets bestmöglich einzusetzen, Streuverluste zu minimieren und Werbemaßnahmen gezielt zu steuern, sodass sie die richtige Zielgruppe zur richtigen Zeit erreichen.

- *Publisher*

Publisher sind Anbieter digitaler Inhalte und Dienste, darunter Nachrichtenseiten, soziale Netzwerke, Video-Plattformen, mobile Apps sowie kleinere Spezialseiten und Blogs. Ihre primäre Aufgabe im Werbeökosystem besteht darin, Inhalte bereitzustellen, mit denen sie Nutzer gewinnen können. Publisher sorgen damit für die notwendige Reichweite und attraktive Umfelder, die Advertiser für ihre Werbekampagnen benötigen.

- *Intermediäre*

Intermediäre umfassen eine Vielzahl von Dienstleistern, Plattformen und Technologieanbietern, die im digitalen Werbemarkt zwischen Advertisern und Publishern vermitteln. Hierzu zählen unter anderem Werbeagenturen, Demand-Side-Plattformen (DSP), Supply-Side-Plattformen (SSP), Ad Exchanges sowie spezialisierte Anbieter für Datenmanagement-Plattformen (DMP), Consumer Data Platforms (CDP) und Consent-Management-Lösungen. Weiterführendes und ergänzendes Material hierzu ist auf Nachfrage vorhanden.

  - DSPs (Demand-Side-Plattformen) ermöglichen Werbetreibenden, Werbeflächen automatisiert zu kaufen und Kampagnen auf Basis definierter Zielgruppen- und Kampagnenkriterien auszuspielen.

- SSPs (Supply-Side-Plattformen) bündeln das Inventar von Publishern, optimieren die Ausspielung und stellen es dem automatisierten Handel zur Verfügung.
- Ad Exchanges verbinden Angebot und Nachfrage in Echtzeit und ermöglichen programmatischen Handel.
- Ad Networks bündeln Werbeflächen kleinerer Publisher und vertreiben sie gebündelt an Advertiser oder DSPs.
- Adserver liefern Anzeigen technisch aus, zählen Impressionen, Klicks und andere Kennzahlen und unterstützen Kampagnensteuerung und Reporting.
- Measurement & Analytics Anbieter erstellen Kampagnenanalysen und Attribution-Modelle, um Werbeleistung messbar zu machen und Optimierungen zu ermöglichen.
- DMPs / CDPs verarbeiten und segmentieren Daten, damit Targeting, Personalisierung und Kampagnensteuerung datenschutzkonform erfolgen. Zentrale und dezentrale Data Clean Rooms sind Umgebungen, die hierfür als Tool eingesetzt werden können, um Daten datenschutzkonform abzugleichen.
- CMPs (Consent-Management-Plattformen) sichern die Einhaltung von Nutzerzustimmungen und Datenschutzvorgaben.
- Ad Verification / Brand Safety Anbieter überwachen die korrekte Ausspielung von Werbung in markensicheren Umfeldern und verhindern Betrug oder problematische Platzierungen.
- Content Recommendation / Personalization Engines sorgen dafür, dass Inhalte und Werbung auf Basis von Nutzerinteressen personalisiert werden, um Relevanz und Nutzerzufriedenheit zu erhöhen.

Die zentrale Funktion der Intermediäre ist die effiziente, datenbasierte Vermittlung zwischen Angebot (Publisher) und Nachfrage (Advertiser). Sie sorgen dafür, dass digitale Werbung automatisiert und skalierbar abgewickelt werden kann. Zu den wesentlichen Vorteilen gehört, dass Advertiser innerhalb weniger Millisekunden die richtigen Werbeplätze identifizieren und buchen können, während Publisher ihr Inventar optimal monetarisieren können.

Daten spielen dabei eine essenzielle Rolle: Intermediäre benötigen Datensätze, um sicherzustellen, dass Anzeigen zum richtigen Zeitpunkt, im richtigen Kontext und an die richtigen Zielgruppen ausgespielt werden. Sie ermöglichen zudem eine präzise Erfolgsmessung und tragen damit wesentlich zur Transparenz und Optimierung digitaler Werbeprozesse bei.

- *Plattformübergreifende Ökosysteme*

Große Plattformen bieten Werbeflächen, Nutzerdaten und Targeting innerhalb geschlossener Systeme an. Sie ermöglichen größere Reichweiten und datenbasierte Kampagnensteuerung, sind aber weniger interoperabel als das offene Web.

- *Potenzielle Kunden / Verbraucher*innen*

Verbraucher*innen erwarten heute zunehmend personalisierte Angebote, die möglichst auf ihre individuellen Interessen zugeschnitten sind, und wünschen sich gleichzeitig Inspiration in ihren digitalen Interaktionen. Personalisierte Inhalte, Angebote, Dienste und Werbung werden mittlerweile als „normal“ wahrgenommen. Hierzu hat der BVDW zusammen mit Kantar Media auch eine aktuelle Studie veröffentlicht, worin Verbraucher*innen zu Personalisierung in der Digitalen Welt befragt wurden. Dieser Trend, der durch Generative KI zusätzlich verstärkt wird. Die Erfüllung dieser sich wandelnden Erwartungen ist daher entscheidend, damit europäische Unternehmen wettbewerbsfähig und zukunftsfähig bleiben.

b. Akteure im Kontext der Personalisierung von Inhalten

Dazu zählen insbesondere digitale Plattformen, Digital-Unternehmen und Dienste, die Inhalte oder Funktionen personalisieren etwa Streaming- und Video-Plattformen, Musik- und Audio-Plattformen, e--Commerce-Plattformen und Unternehmen, Nachrichten-, Wetter- und Informationsplattformen, Soziale Netzwerke und Community-Plattformen, Navigations- und Mobilitätsdienste, Lernplattformen und Bildungsdienste und Mobile Apps und digitale Services.

Diese Akteure nutzen Tracking, um das Nutzerverhalten auszuwerten und darauf aufbauend personalisierte Empfehlungen, Inhalte, Interface-Anpassungen oder Benachrichtigungen anzubieten. Ziel ist es, Relevanz und Nutzerbindung zu erhöhen durch maßgeschneiderte Serviceangebote, Inhalte oder Funktionen.

5. Liste von Tracking- & Personalisierungsmethoden

Im Folgenden geben wir einen Überblick über die wichtigsten Tracking- und Personalisierungsmethoden, die heute in der digitalen Wirtschaft zum Einsatz kommen. Diese reichen von klassischen Cookies bis hin zu modernen Privacy-APIs. Jede Technik hat spezifische Funktionen, Stärken und Schwächen. Diese Liste erhebt keinen Anspruch auf Vollständigkeit, da sie fortlaufend weiterentwickelt wird.

- *Cookie-Tracking*

HTTP-Cookies sind kleine Textdateien, die bei Bedarf vom Anbieter im Browser gespeichert werden. Sie werden jedoch nicht auf jeder Website automatisch gesetzt. Cookies kommen nur zum Einsatz, wenn bestimmte Funktionen dies erfordern, etwa für Nutzeridentifikation, Targeting, Speicherung von Privatsphäre-Einstellungen (wie unter anderem Einwilligungen), Conversion-Tracking (Zuordnung von Verkäufen zu Werbeklicks), Erfolgsmessung von Kampagnen oder zur Betrugsprävention. Cookies können auch seitenübergreifendes Tracking (Cross-Site) ermöglichen. Sie sind damit sowohl ein optionales als auch ein zweckgebundenes Werkzeug.

First-Party-Cookies

- Besucht man eine Website, kann diese eine eindeutige ID im Browser ablegen (First-Party-Cookie). Bei jedem Folgebesuch wird die ID mitgeschickt, sodass der Nutzer wiedererkannt wird. Dies dient der Personalisierung von Inhalten, der Messung von Nutzungsverhalten und der gezielten Ausspielung von Werbung. Technisch wird dies erreicht, indem der Browser die Cookie-Information bei jeder Anfrage an genau diese Domain automatisch mitsendet.
- First-Party-Cookies werden direkt von der besuchten Domain gesetzt und sind daher vor allem für Funktionen wie Login, Warenkorb, Spracheinstellungen oder Analyse des eigenen Traffics wichtig.
- Sie ermöglichen in erster Linie das Nachvollziehen von Nutzerinteraktionen innerhalb derselben Website und dienen der Optimierung von Nutzererlebnis und Angebotsgestaltung.

Third-Party-Cookies

- Drittanbieter-Cookies funktionieren ähnlich, stammen aber von externen Domains (z. B. einem Werbenetzwerk, Analyse- oder Social-Media-Anbieter).
- Sie ermöglichen seitenübergreifendes Tracking (Cross-Site), da dieselbe externe Domain auf vielen verschiedenen Websites eingebunden sein kann. So lassen sich Aktivitäten und Interessen von Nutzer*innen über mehrere Seiten hinweg beobachten und für Werbung, Reichweitenmessung oder Profilbildung nutzen.
- Technisch wird dies dadurch erreicht, dass beim Laden der Website Inhalte von Drittanbietern (z. B. Werbebanner oder Tracking-Pixel) nachgeladen werden, die ihrerseits ein

Cookie im Browser platzieren. Der Browser sendet dieses Cookie anschließend bei jedem erneuten Kontakt mit dieser Dritt-Domain mit.

- *Server-Side-Tracking*

Hierbei werden Tracking-Aktionen nicht vom Nutzerbrowser direkt an Drittserver gemeldet, sondern der Website-Betreiber leitet die Daten vom eigenen Server aus weiter. Beispielsweise kann ein Pixel auf der Seite nicht mehr einen Aufruf zu einem externen Ad-Server durchführen, sondern sendet einen Request an den eigenen Server, welcher dann serverseitig den Drittanbieter informiert. Ein Whitepaper zu dem Thema ist bei Bedarf vorhanden.

- *IP-Adressen und Geolokalisierung*

Jede Internetverbindung hat eine IP-Adresse, die Rückschlüsse auf den ungefähren Standort (Land, Stadt, Anbieter) zulässt. IP-Adressen werden oft automatisch erfasst und dienen z. B. dazu, Werbeinhalte regional anzupassen (Stichwort Geotargeting) oder Betrugsfälle (auffällige ausländische Zugriffe) zu erkennen. Eine IP allein ist kein perfektes Identifier, da sie sich ändern kann und ggf. mehreren Nutzern zugewiesen ist, liefert aber wichtige Kontextdaten.

- *Tracking-Pixel und Tags*

Hierbei handelt es sich um 1×1 Pixel-Bilder oder Skripte, die in Webseiten eingebunden sind. Wird die Seite geladen, wird auch dieser Pixel vom Server des Anbieters geladen, wodurch dieser einen Seitenaufruf registrieren kann. Tracking-Pixel liefern so z. B. Zählstatistiken, welche Artikel wie oft gelesen wurden (ein bekanntes Beispiel sind VG-Wort-Pixel zur Autorenvergütung) oder ob eine E-Mail geöffnet wurde. In der Werbung dienen Pixel und sogenannte Tags vor allem der Messung (View-Tracking von Anzeigen, Zählung von Ad-Impressions) und dem Retargeting (ein Pixel auf der Bestellbestätigungsseite kann an ein Werbenetzwerk melden, dass der Nutzer Kunde wurde).

- *Mobile Advertising IDs*

In mobilen Apps erfolgt das Tracking nicht über Browser-Cookies, sondern über dedizierte Werbe-Identifikatoren des Betriebssystems. Auf Android-Geräten gibt es z. B. die Google Advertising ID (GAID), auf Apple-Geräten den Identifier for Advertisers (IDFA). Diese IDs sind pro Gerät eindeutig und können von Apps (mit entsprechender Berechtigung) ausgelesen werden. Sie ermöglichen über verschiedene Apps hinweg eine Wiedererkennung des Nutzers für Werbezwecke. Nutzer können diese IDs allerdings zurücksetzen oder das Tracking einschränken. Mobile Ad-IDs (MAIDs) werden für App-übergreifendes Frequenz-Capping, Attribution von App-Installationen oder Cross-App-Profile genutzt.

- *Fingerprinting (Geräte-Fingerabdruck)*

Fingerprinting bezeichnet eine Sammlung von Gerätedaten, um einen Nutzer auch ohne Cookies wiederzuerkennen. Hierbei werden Skripte im Browser ausgeführt, die Merkmale auslesen: z. B. Bildschirmauflösung, installierte Schriftarten, Browser-Version, Betriebssystem, Sprache, Zeitzone, aktivierte Plugins oder auch die Eigenschaften von HTML5-Canvas-Elementen. Aus diesen vielen Datenpunkten wird ein quasi eindeutiger Fingerabdruck des Geräts berechnet. Studien zeigen, dass 80–90 % der Browser-Fingerprints einmalig sind. Die meisten Nutzer*innen lassen sich so also individuell identifizieren. Beispielsweise nutzen Banken, Shops und e-Commerce diese Geräte-Fingerabdrücke, um verdächtige Logins oder Transaktionen zu erkennen (Betrugsabwehr). In Zeiten von KI nehmen betrügerische Angriffe zu und erfolgen zunehmend automatisiert, sodass es immer wichtiger wird, mit den technischen Fortschritten der Angreifer mitzuhalten. Der Einsatz von KI zur Mustererkennung und Betrugsprävention wird daher zunehmend notwendig.

- *Local Storage / IndexedDB:*

Dabei handelt es sich um browserinterne Speichertechniken, die webseitenübergreifend persistent sein können. Local Storage ist nützlich, um z. B. Consent-Entscheidungen oder Nutzerpräferenzen zu speichern.

- *Click-Tracking und URL-Parameter*

Eine simple, aber effektive Methode ist das Anhängen von Identifiers in URLs, wenn der Nutzer auf einen Link klickt. Beispiele sind UTM-Parameter (utm_source, utm_campaign etc.), die zu Analysezwecken genutzt werden. Große Plattformen wie Meta oder Google hängen teils eigene IDs an externe Links an (z. B. fbclid, gclid), um später erkennen zu können, welcher Klick zu welcher Aktion führte. Klick-Tracking ist hilfreich für die Attribution (Zuordnung von Werbeausgaben zu Ergebnissen) und funktioniert auch ohne Cookies. In der Praxis dienen URL-Parameter primär Analyse- und Kampagnenzwecken.

- *Authentifizierte Nutzer-IDs (Login-Tracking)*

Viele digitale Plattformen setzen auf eigene Login-Systeme. Wenn sich ein Nutzer anmeldet, kann sein Verhalten direkt mit seinem Account verknüpft werden. Der große Vorteil: Dieses Tracking ist geräteübergreifend möglich (da derselbe Account auf Smartphone und Laptop genutzt wird) und sehr präzise. Anbieter nutzen die Account-ID, um ein umfassendes Bild der Interessen zu erhalten. Die entsprechenden Daten verbleiben dabei vollständig innerhalb der Plattform und werden nicht direkt an externe Dritte weitergegeben, sondern lediglich in aggregierter oder anonymisierter Form über die von der Plattform kontrollierten Werbe- oder Reporting-Schnittstellen. Zur Einordnung: diese „Walled Gardens" bezeichnen in diesem Kontext geschlossene Plattform-Ökosysteme, in denen zentrale Infrastrukturelemente wie Login-IDs, Targeting- oder Messmechanismen ausschließlich unter der Kontrolle des jeweiligen Plattformbetreibers stehen.

- *Privacy Enhancing Browser-APIs*

Als Antwort auf strengere Datenschutzregeln und Diskussionen um Third-Party-Cookies arbeitet die Branche an neuen Lösungen, die zielgerichtete Werbung ohne individuelles Tracking ermöglichen sollen. Hierbei ermittelt der Browser lokal einige grobe Interessenskategorien des Nutzers (z. B. „Sport", „Reisen"), basierend auf dem Surfverhalten, und teilt diesen Themen-Tag mit Werbepartnern statt individueller IDs. Die Werbenden können dann z. B. sagen: zeige diese Anzeige allen, die das Thema „Auto" im Browser haben. Die spezifischen Webseiten, die der Nutzer besucht hat, werden nicht nach außen offenbart. Solche Ansätze zielen darauf ab, Gruppenprofiling statt Einzelprofiling zu betreiben.

- *Plattforminterne Personalisierung*

Plattformen wie YouTube, Instagram, TikTok etc. betreiben ein On-Platform-Tracking. Alle Aktivitäten (Like, Watch oder Scroll) werden erfasst, um z. B. den Feed zu personalisieren oder um passende Werbung innerhalb der Plattform auszuspielen. Technologisch kommen hier Machine-Learning-Algorithmen zum Einsatz, die anhand des Verhaltens ähnliche Inhalte empfehlen (Stichwort: Empfehlungssysteme).

- *Hash-Matching und CRM-Anwendung*

Unternehmen verfügen über Kundendaten (z. B. E-Mail-Adressen von Newsletter-Abonnenten oder Käuferlisten). Viele Werbeplattformen erlauben es, solche Datensätze bei vorliegendem Consent gehasht hochzuladen, um die entsprechenden Nutzer*innen online wiederzufinden. Gehasht bedeutet in diesem Kontext, dass die ursprünglichen Daten (z. B. E-Mail-Adressen) in einen nicht direkt lesbaren Code umgewandelt werden, bevor sie an die Plattform übermittelt werden. Beispielsweise kann ein Händler seine Kunden-E-Mails an eine Plattform liefern; die Plattform hasht seine User-E-Mails ebenso mit der gleichen Hash-Methode und erstellt eine

Schnittmenge (Custom Audience). So kann der Händler gezielt seine bestehenden Kunden mit Werbung ansprechen, ausschließen oder ähnliche Zielgruppen bilden (Lookalike Audience).

- *Geo-Location Targeting*

Geo-Location Targeting nutzt die geografische Position von Nutzer*innen, um Inhalte oder Werbung gezielt auszuspielen. Dies kann auf Basis von GPS-Daten, IP-Adresse, WLAN oder Mobilfunkmasten erfolgen. Werbende können so z. B. lokale Angebote, Standorte oder regionale Services nur den Nutzerinnen anzeigen, die sich in einem bestimmten Gebiet befinden. Technologisch kommen hier Geodaten-Services, Mobile SDKs oder Location-APIs zum Einsatz. Ansätze wie Geo-Fencing ermöglichen zudem die gezielte Ansprache von Nutzer*innen, die ein definiertes geografisches Gebiet betreten oder verlassen (wie z. B. ein 3-km-Radius um ein Fußballstadion).

- *Contextual Targeting*

Beim Contextual Targeting wird Werbung passend zum Inhalt einer Webseite, App oder eines Medienformats ausgespielt, ohne dass Nutzerinnen oder Nutzer persönlich identifiziert werden. Algorithmen analysieren Text, Bilder, Videos oder Metadaten, um thematisch passende Anzeigen auszuwählen (z. B. Reiseanzeigen auf einer Reiseblog-Seite). Der Fokus liegt auf dem Umfeld und Macro-Kontext, nicht auf individuellen Nutzerprofilen. Technologisch werden hierbei Natural-Language-Processing, Bild- und Videoklassifikation oder semantische Analysen eingesetzt, um relevante Zusammenhänge zwischen Inhalt und Anzeige zu erkennen. Contextual Targetting kann für manchen Zwecken passend sein. Allerdings berücksichtigt Contextual Targeting nur den Seiten- oder App-Inhalt, nicht das individuelle Nutzerverhalten. Dadurch ist die Ansprache oft weniger präzise, langfristige Nutzerprofile lassen sich nicht aufbauen, und für sehr spezifische Zielgruppen kann die Relevanz der Werbung eingeschränkt sein.

Contextual Targeting wird aktuell im Rahmen des BVDWs in einer der Working Groups weiter definiert.

- *Analyse / Abgleich von Daten über Data Clean Rooms*

Data Clean Rooms sind sichere, datenschutzkonforme Umgebungen, in denen Werbetreibende und Plattformen Daten abgleichen und analysieren können, ohne personenbezogene Informationen direkt auszutauschen. Sie ermöglichen diesen Abgleich, um Zielgruppen zu definieren, Kampagnen zu messen oder Insights zu gewinnen, ohne dass die Rohdaten des Herrschaftsbereichs des Verantwortlichen verlassen. Technologisch werden hierbei häufig verschlüsselte IDs, Aggregationen und anonymisierte Analysen genutzt, sodass keine Rückschlüsse auf einzelne Nutzer*innen möglich sind. Data Clean Rooms sind besonders relevant, um datenschutzkonforme Attribution, Zielgruppenanalyse und Kampagnenoptimierung auch ohne Third-Party-Cookies zu ermöglichen.

- *Ultraschall-Beacons (Cross-Device-Tracking)*

Eine eher exotische und nicht-verwendete Methode ist das Tracking per ultrahochfrequenter Schallsignale, um verschiedene Geräte ein und derselben Person zuzuordnen. Hierbei sendet z. B. ein TV-Spot oder ein Werbebanner auf dem Laptop ein für Menschen unhörbares Ultraschallmuster aus. Eine App auf dem Smartphone lauscht mit dem Mikrofon und erkennt dieses Signal, wodurch festgestellt werden kann, dass beide Geräte zum selben Nutzer gehören. So könnte man z. B. nachvollziehen, ob jemand nach dem Sehen eines TV-Spots auf dem Handy nach dem Produkt sucht. Aus Sicht der Werbewirtschaft spielt diese Technik keine Rolle. Sie wird weder als Standard eingesetzt noch verteidigt, da sie das Vertrauen der Nutzer massiv gefährden würde.

6. Zwecke und TCF

6.1. Zwecke

Die nachfolgenden Abschnitte geben einen Überblick über die verschiedenen Zwecke, für die Tracking- und Targeting-Technologien in der digitalen Werbung eingesetzt werden. Sie zeigen, wie Nutzungs- und Interaktionsdaten verwendet werden, um Werbung gezielt auszuspielen, Reichweiten zu messen, Inhalte zu personalisieren oder die Effektivität von Kampagnen zu optimieren.

Dabei wird deutlich, dass die erhobenen Daten nicht nur für klassische Werbezwecke genutzt werden, sondern auch zur Verbesserung der Nutzererfahrung, zur Betrugserkennung und zur datengestützten Produktentwicklung dienen. Dieses Kapitel erläutert die gängigen Methoden, die technischen Mechanismen dahinter und die unterschiedlichen Zielsetzungen im digitalen Werbeökosystem.

Das Transparency & Consent Framework (TCF) ist ein von der IAB Europe entwickelter Standard, der sicherstellt, dass Nutzer*innen transparent über Tracking- und Werbezwecke informiert werden und ihre Zustimmung datenschutzkonform erteilen oder ablehnen können. Es ermöglicht Publishern und Werbepartnern, Zustimmungen systematisch zu verarbeiten und damit digitale Werbung rechtskonform auszuspielen.

- *Ad-Targeting (gezielte Werbeansprache)*

Darunter versteht man das Ausliefern von Werbung an spezifische Zielgruppen anhand bestimmter Kriterien. Behavioral / Verhaltensbasiertes Targeting ist die Analyse des früheren Online-Verhaltens, durch z.B. besuchte Websites, Suchbegriffe, Klicks, sowie demografische Merkmale, um Interessen des Nutzers abzuleiten und entsprechende Anzeigen zu schalten.

Diese Targeting-Formen greifen auf die oben genannten Daten zurück. z. B. werden für behavioral Targeting Cookie-IDs oder Geräte-IDs genutzt, um über das Nutzungsverhalten Interessenprofile zu erstellen, oder es werden Account-Daten wie Altersangaben für demografisches Targeting herangezogen.

- *Conversion-Tracking / Attribution*

Erfasst wird hierbei, welche Werbung zu einer Conversion (einem definierten Erfolg, z. B. Kauf, Registrierung) geführt hat. Typischerweise wird beim Klick auf eine Anzeige ein Identifier (Cookie-ID oder spezifische Klick-ID) mitgegeben und auf der Zielseite bzw. beim Kaufabschluss ausgelesen, um die Conversion der ursprünglichen Anzeige zuzuordnen. Häufig kommen Tracking-Pixel oder Skripte zum Einsatz, die auf der Bestellbestätigungs-Seite feuern und den Erfolg an das Werbesystem melden (z. B. der Meta/Facebook-Pixel, der Website-Aktionen zur Erfolgsmessung an Facebook Ads meldet).

So kann die Attribution erfolgen, also die Zuordnung des Erfolgs zu einem Werbekanal oder einer Kampagne. Fortgeschrittene Attribution-Modelle verteilen den Weg des Users auf mehrere Touchpoints (z. B. wenn ein Nutzer über mehrere Anzeigenkontakte und Geräte hinweg konvertiert), dafür werden geräteübergreifende IDs oder Modelle der Identitätsauflösung eingesetzt, um Interaktionen einer Person über Cookies und Geräte hinweg zusammenzuführen.

- *Reichweitenmessung*

Die Reichweite einer Kampagne oder Website gibt an, wie viele eindeutige Nutzer erreicht wurden (Unique Users). Zur Messung werden eindeutige Identifier benötigt, um Mehrfachkontakte zu erkennen. Beispielsweise zählt ein Ad-Server die unique Cookie-IDs oder Geräte-IDs, die eine Anzeige gesehen haben, um daraus die Anzahl individueller Nutzer zu bestimmen. Über sog. Frequency Capping (siehe unten) wird dabei auch gezählt, wie oft derselbe Nutzer ein Ad gesehen hat – beides zusammen ergibt Reichweite und Frequenz einer Kampagne. Für cross-device Reichweitenmessung (ein Nutzer surft z. B. am Handy und Laptop) werden

Identitätsabgleiche genutzt, etwa Login-IDs (wenn der Nutzer auf beiden Geräten eingeloggt ist) oder probabilistische Modelle, die anhand von gemeinsamen Merkmalen (IP-Adresse, Gerätetyp, Uhrzeit) Nutzungen zusammenführen.

In Deutschland kommen zur Standardisierung oft gemeinsame Messverfahren zum Einsatz (z. B. IVW oder AGF), die mittels Tracking-Skripten oder Zählpixeln auf vielen Websites anonyme Nutzerkennungen erheben, um Überschneidungen zu berechnen. Moderne Web-Analytics-Tools bieten auch cookielose Reichweitenmessung an, die z. B. nur aggregierte Seitenaufrufe ohne individuenbezogene IDs zählen.

- *Personalisierung von Inhalten*

Neben Werbung werden die Daten auch genutzt, um Inhalte an den Nutzer anzupassen. Empfehlungssysteme (Recommender) etwa bei Streaming-Plattformen oder News-Seiten analysieren das Nutzungsverhalten, um personalisierte Vorschläge zu machen. So berücksichtigt Netflix z. B. "*deine Interaktionen mit unserem Dienst (wie deine bisherige Seh-Historie und Bewertungen anderer Titel)*" sowie "*weitere Signale wie Tageszeit, genutztes Gerät, Spracheinstellungen und wie lange du etwas geschaut hast*" für die Empfehlungen. Ähnlich wertet YouTube den Videoverlauf und Interaktionen (Likes, Watch-Time) aus, um den Feed zu personalisieren. Spotify analysiert Hör-Historie, übersprungene Songs und bevorzugte Genres, um kuratierte Playlists (Daily Mix, Discover Weekly) zusammenzustellen. Hierbei werden Profile pro Nutzer bzw. Gerät gebildet (über Login, Cookie oder Geräte-ID), um die Präferenzen zu speichern. Die Algorithmen vergleichen oft das Verhalten vieler Nutzer (Collaborative Filtering) und nutzen Inhalts-Metadaten, um relevante Inhalte individuell auszuspielen.

- *Frequency Capping*

Darunter versteht man die Begrenzung, wie oft derselbe Nutzer eine bestimmte Werbeanzeige sieht. Um dies umzusetzen, muss der Werbeserver einen wiederkehrenden Nutzer erkennen können. Im Web geschieht das meist über Cookies: beim ersten Ad-Kontakt wird der Person ein eindeutiger User-Key in einem Cookie zugeordnet, über den gezählt wird, wie viele Ad-Impressions dieser Nutzer erhalten hat. In Mobile Apps dienen die geräteseitigen Werbe-IDs (IDFA/GAID) als Identifier, die vom Ad-SDK ausgelesen und an das Ad-System gemeldet werden. So kann z. B. eingestellt werden, dass eine bestimmte Anzeige pro Nutzer in 24 Stunden erscheint – das System stellt nach Einblendungen an dieselbe ID die Auslieferung ein. Frequency Capping verhindert Ad-Fatigue (Werbemüdigkeit) und verbessert die Nutzererfahrung, indem zu hohe Wiederholungen vermieden werden.

- *Fraud Prevention / Bot Detection*

In der digitalen Werbung ist Betrugserkennung wichtig, um ungültige Impressionen oder Klicks (z. B. durch Bots, Skripte oder betrügerische Websites) herauszufiltern. Dazu werden technische Merkmale und Nutzungsdaten herangezogen, um auffällige Muster zu erkennen. Beispielsweise können Device-Fingerprints erstellt werden, um ein Gerät wiederzuerkennen und betrügerisches Verhalten aufzudecken (z. B. ein Gerät, das hunderte Ads pro Minute lädt). Es werden IP-Adressen überwacht (viele Klicks von derselben IP in kurzer Zeit), Verhaltensmetriken analysiert (unmenschlich gleichmäßige Mausbewegungen oder Scrollverhalten) und Blacklists verdächtiger Geräte-IDs oder User-Agents geführt.

Zusätzlich existieren brancheneinheitliche Fraud- und Bot-Listen, z. B. von der IAB Tech Lab oder der TAG-Initiative, deren bekannte Quellen zentral erfasst und automatisiert von der Auslieferung ausgeschlossen werden. Moderne Fraud-Detection-Systeme nutzen Machine Learning, um betrügerisches von echtem Verhalten zu unterscheiden. Wenn ein Muster als Bot erkannt wird, können weitere Anfragen von diesem User blockiert oder für die Abrechnung ausgeschlossen werden. Insgesamt helfen diese Maßnahmen, Werbebudgets vor ineffektiven Auslieferungen zu schützen und die Brand Safety zu erhöhen.

- *A/B-Testing und Produktentwicklung*

Webdienste und Apps verwenden Nutzerdaten auch, um neue Funktionen oder Designs zu testen. Bei einem A/B-Test wird die Nutzerbasis zufällig in Gruppen aufgeteilt (z. B. per Cookie-ID oder Benutzer-ID) und jede Gruppe sieht eine andere Variante einer Website oder App. Durch Tracking der Nutzungsmetriken (Klickrate, Conversion-Rate, Verweildauer etc.) pro Variante kann analysiert werden, welche Version besser performt. Hierfür werden dieselben Tracking-Daten genutzt: Eindeutige Nutzerkennungen stellen sicher, dass ein Nutzer konsistent nur eine Variante sieht, und Events aus dem Nutzungsverhalten zeigen Unterschiede im Engagement. Die Ergebnisse fließen in die Produktentwicklung ein – etwa entscheidet man sich für das Layout, das im Test bessere Werte erzielt hat. A/B-Tests erfordern also die Erhebung von Interaktionsdaten und oft die Verknüpfung mit Kunden-Daten (um z. B. Ergebnisse für bestimmte Segmente zu prüfen). Insgesamt ermöglichen solche Experimente eine datengesteuerte Optimierung von Produkten und Werbemitteln.

- *CRM-Onboarding / Zielgruppenabgleich*

Hierbei werden Offline-Kundendaten (aus dem CRM eines Werbungtreibenden) mit Online-Identifikatoren verknüpft, um bestehende Kunden oder definierte Zielgruppensegmente online anzusprechen. Ein Beispiel ist das Hochladen einer verschlüsselten Kundenliste (z. B. gehashte E-Mail-Adressen) zu einer Werbeplattform wie Facebook oder Google. Die Plattform führt dann einen Abgleich durch und erstellt eine Custom Audience aus den Nutzern, die sie in ihrer Datenbank zuordnen konnte. So kann ein Unternehmen seine z. B. im Laden gesammelten Kundenkontakte online mit Anzeigen erneut ansprechen (Retargeting auf Bestandskunden) oder ähnliche Zielgruppen finden lassen (Lookalike Audiences). Auch Geräte-IDs können zum Onboarding genutzt werden, z. B., um App-Nutzer in einem Werbenetzwerk wiederzufinden. Technisch werden dabei First-Party-Daten (E-Mail, Telefonnummer, Kundennummer) mittels Hashing anonymisiert an den Ad-Anbieter gegeben, der sie mit seinen Login-Datenbanken abgleicht.

6.2. Transparency and Consent Framework (TCF)

Im Rahmen des IAB Europe Transparency and Consent Framework (TCF) werden standardisierte Zwecke der Datenverarbeitung definiert, die es ermöglichen, Nutzer*innen transparent über Verarbeitungsaktivitäten aufzuklären und die spezifischen Rechtsgrundlagen rechtsgültig einzuholen und sicherzustellen, dass die Nutzer*innen kompetent und eigenständig entscheiden können. Für die Punkten 1 bis 11 werden z.B. Einwilligungen oder Widersprüche von Nutzer*innen eingeholt.

Nachfolgend werden diese Zwecke auf Deutsch erläutert:

1. **Informationen auf einem Gerät speichern und/oder abrufen.** Speicherung oder Zugriff auf Informationen wie Cookies, Gerätekennungen oder andere Daten auf dem Gerät der Nutzerin (z. B. zur Wiedererkennung bei späteren Besuchen).
2. **Begrenzte Daten verwenden, um Werbung auszuwählen.** Auswahl von Werbung auf Basis allgemeiner Informationen (z. B. Kontext der Seite oder grobe Standortdaten), ohne individuelle Profile zu nutzen.
3. **Profile zur personalisierten Werbung erstellen**. Aufbau detaillierter Nutzerprofile auf Grundlage des Surfverhaltens, um Vorlieben, Interessen und demografische Merkmale für gezielte Werbung abzuleiten.
4. **Personalisierte Werbung basierend auf einem Profil auswählen**. Auswahl von Werbeanzeigen anhand zuvor erstellter Nutzerprofile, um möglichst relevante Werbung anzuzeigen.
5. **Profile zur Personalisierung von Inhalten erstellen.** Erstellung von Profilen zur Anpassung redaktioneller oder redaktionell-ähnlicher Inhalte, etwa Empfehlungen bei Newsportalen oder Streamingdiensten.

6. **Personalisierte Inhalte basierend auf einem Profil auswählen.** Auswahl und Anzeige individualisierter Inhalte basierend auf bekannten Nutzerpräferenzen (z. B. empfohlene Artikel, Videos, Produkte).
7. **Leistung von Werbung messen.** Analyse der Effektivität einzelner Anzeigen, zum Beispiel wie viele Nutzer*innen sie gesehen, angeklickt oder daraufhin ein Produkt gekauft haben.
8. **Leistung von Inhalten messen.** Bewertung, wie gut Inhalte (z. B. Artikel, Videos, Produkte) bei Nutzer*innen ankommen, z. B. durch Verweildauer, Scrollverhalten oder Interaktionen.
9. **Zielgruppen anhand von Statistik oder Datenkombination verstehen.** Aggregierte Datenanalysen zur Gewinnung von Erkenntnissen über Nutzersegmente, z. B. typische Interessen, Altersstruktur oder Nutzungsmuster.
10. **Dienste entwickeln und verbessern**. Nutzung der gesammelten Daten, um digitale Produkte, Apps und Websites zu optimieren – z. B. durch A/B-Tests oder Nutzerfeedback.
11. **Begrenzte Daten verwenden, um Inhalte auszuwählen.** Nicht-personalisierte Auswahl von Inhalten basierend auf kontextuellen Informationen, etwa der Art der aufgerufenen Seite oder des Geräts.
12. **Sicherheit gewährleisten, Betrug verhindern und Fehler beheben.** Erkennung und Verhinderung betrügerischer oder fehlerhafter Nutzung, z. B. durch Bot-Erkennung, Schutz vor Missbrauch oder Debugging.
13. **Werbung und Inhalte ausliefern und präsentieren.** Technische Bereitstellung von Inhalten und Werbeanzeigen – einschließlich Ladezeit, Formatierung, Darstellung auf dem Endgerät.
14. **Datenschutzpräferenzen speichern und übermitteln.** Erfassung und Verwaltung der Einwilligungsentscheidungen der Nutzer*innen (z. B. über das Consent-Banner) und deren Weitergabe an beteiligte Anbieter.
15. **Daten mit anderen Datenquellen abgleichen und kombinieren.** Zusammenführung verschiedener Datenquellen, um ein vollständigeres Bild über Nutzerinteraktionen zu erhalten – z. B. CRM-Daten mit Online-Daten.
16. **Geräte über verschiedene Kontexte hinweg verknüpfen.** Identifikation und Zuordnung von Nutzer*innen über mehrere Geräte hinweg – z. B. wenn jemand am Smartphone klickt und später am Laptop kauft.
17. **Geräte anhand automatisch übertragener Merkmale identifizieren**. Wiedererkennung von Geräten über technische Merkmale wie Bildschirmauflösung, Browser-Version oder installierte Schriftarten (Device Fingerprinting).
18. **Präzise Geolokalisierungsdaten verwenden.** Nutzung genauer Standortdaten (z. B. via GPS) zur Lokalisierung des Nutzers – z. B. für standortbezogene Werbung oder Services.
19. **Geräteeigenschaften aktiv scannen, um sie zu identifizieren**. Aktive Erhebung technischer Daten vom Gerät (z. B. durch ein Skript), um individuelle Geräte eindeutig zu erkennen – meist zur Betrugserkennung oder Wiedererkennung.

7. Welche Daten werden aktuell verwendet?

In der Online-Werbung und bei personalisierten Diensten kommen vor allem die folgenden Datenarten zum Einsatz, je nach Funktion und Notwendigkeit. Oft werden mehrere Daten gleichzeitig verwendet, manche Daten weniger oder in sehr spezifischen Fällen:

Datenart	Beschreibung
Cookie-ID	Eindeutige Kennung in einem Browser-Cookie, dient zur Wiedererkennung eines Nutzers bzw. Browsers über verschiedene Seitenaufrufe und Websites hinweg. Wird oft von Werbenetzwerken gesetzt, um Nutzeraktivitäten seitenübergreifend zu verfolgen.
Geräte-ID	Gerätebezogene Kennung, insbesondere auf mobilen Geräten (z. B. Apples IDFA oder Googles Advertising ID). Damit können Nutzer geräteübergreifend identifiziert werden, sofern Apps oder Werbe-SDKs diese ID auslesen. Häufig genutzt für In-App-Tracking und mobile Werbung.
IP-Adresse	Numerische Netzwerkadresse des Nutzers. Sie ermöglicht eine grobe Standortbestimmung (Geolokation) und kann für Betrugserkennung oder zur Wiedererkennung von Besuchern verwendet werden. Allerdings teilen sich manchmal mehrere Nutzer eine IP (z. B. in Firmennetzwerken).
Geolokationsdaten	Standortdaten des Nutzers, entweder präzise (GPS-Daten, WLAN) oder approximativ (aus der IP-Adresse abgeleitet). Diese werden genutzt, um standortbezogene Inhalte oder Werbung auszuspielen (z. B. lokale Angebote in der Nähe des Nutzers).
Nutzungsverhalten	Daten über das Verhalten und die Interaktionen des Nutzers, z. B. besuchte Websites, angesehene Inhalte, Klicks, Suchanfragen, Kaufhistorie oder Verweildauer. Solche Verhaltensdaten dienen dazu, Interessenprofile zu erstellen (für personalisierte Empfehlungen oder zielgerichtete Anzeigen).
Account-Daten	Vom Nutzer bereitgestellte Profildaten in einem Account, z. B. Name, E-Mail, Alter, Geschlecht, Kundenhistorie oder Interessen. Diese Daten werden v. a. in Login-basierten Plattformen genutzt, um Werbung demografisch auszuspielen oder Inhalte zu personalisieren (z. B. personalisierte Empfehlungen, Begrüßung mit Namen).
Browser-/ Geräteeigenschaften	Technische Merkmale des genutzten Endgeräts und Browsers: z. B. Gerätetyp (Smartphone/Desktop), Betriebssystem, Browser-Version, Bildschirmauflösung, Spracheinstellung, installierte Plugins oder Schriftarten. Solche Informationen werden teils für die Geräte- bzw. Browsererkennung (Fingerprinting) genutzt oder um Inhalte technisch zu optimieren (z. B. mobile vs. Desktop-Version).
Segmente	Zusammengefasste Nutzergruppen mit ähnlichen Eigenschaften oder Verhaltensmustern, die von Werbungtreibenden oder Datenplattformen definiert werden. Segmente können z. B. Interessen (z. B. „Reiseinteressierte“), Demografie (z. B. „Männer 30–45“) oder Kaufabsichten (z. B. „Auto-Kauf in den nächsten 30 Tagen“) abbilden. Sie entstehen durch Clustering von Nutzerdaten aus verschiedenen

	Quellen (Onsite-Tracking, CRM, DMPs) und dienen zur gezielten Ansprache im Targeting. Segmente werden häufig von Data-Providern oder Adtech-Plattformen standardisiert und vermarktet. Eine Person kann gleichzeitig Teil mehrerer Segmente sein.
Klickpfad („Clickstream“) / Referrer-Daten	Die Abfolge von Seiten, die ein Nutzer innerhalb einer Session besucht (inkl. vorher besuchter Website, sog. Referrer). Diese Daten geben Aufschluss über die Nutzerintention und Navigationsmuster und werden für Attribution, Targeting und UX-Optimierung genutzt.
Session-Daten	Informationen, die nur für die Dauer einer Browsersitzung gespeichert werden, z. B. Session-ID, Login-Zustand oder Zwischenergebnisse von Formularen. Werden oft für Conversion-Tracking, Warenkörbe oder Login-basierte Anwendungen genutzt.
Zahlungs- und Transaktionsdaten	Daten zu Bestellungen, Käufen, Buchungen oder Zahlungen (z. B. Produktart, Warenkorbwert, Zahlungsart). Diese Daten fließen in die Bewertung von Kampagnen-Erfolg (ROI) ein und dienen zur Erstellung von Käufersegmenten für Targeting- und Retargeting-Zwecke.
Feedback- und Interaktionsdaten	Bewertungen, Kommentare, Support-Anfragen oder Feedback-Formulare. Diese qualitativen Daten ergänzen das quantitative Nutzerverhalten und können zur Verbesserung der Customer Experience sowie zur Bildung von Affinitätsgruppen herangezogen werden.
Kampagnen-IDs / Creative-IDs	Technische Marker zur Identifikation einzelner Werbemittel oder Kampagnen. Werden eingesetzt, um Klicks und Conversions gezielt auf bestimmte Creatives oder Kampagnen-Varianten zurückzuführen (z. B. A/B-Tests, Performance-Optimierung).
Consent-Daten	Informationen über die vom Nutzer erteilten Einwilligungen oder Widersprüche, gespeichert z. B. in TC-Strings oder über Consent Management Platforms (CMPs). Diese sind essenziell für die rechtmäßige Verarbeitung personenbezogener Daten im Werbe- und Analysekontext.

8. Welche Maßnahmen und Techniken sind essenziell?

Tracking und Datenverarbeitung sind in zahlreichen Bereichen der digitalen Wirtschaft unverzichtbar. Sie bilden die Grundlage vieler Innovationen, von Empfehlungsalgorithmen und Optimierung der Benutzerfreundlichkeit bis hin zur Betrugsprävention. Personalisierte digitale Werbung ist eine zentrale Anwendung dieser Datenflüsse und leistet einen zentralen Beitrag zur Refinanzierung frei zugänglicher Inhalte und digitaler Dienste. Sie ermöglicht es Unternehmen, insbesondere kleinen und mittelständischen Anbietern, ihre Angebote effizient zu finanzieren, gezielt auszuspielen und Nutzer*innen relevante Inhalte, statt irrelevanter Massenwerbung bereitzustellen. Gleichzeitig sind viele Innovationen, von Empfehlungslogiken über Benutzerfreundlichkeit bis hin zu Betrugsabwehr, ohne die zugrunde liegenden Datenflüsse und technischen Verfahren nicht denkbar.

Die nachfolgend genannten Maßnahmen und Techniken sind Beispiele für Praktiken, die aus Sicht der digitalen Wirtschaft unverzichtbar für den Betrieb, die Finanzierung und die kontinuierliche Optimierung digitaler Angebote sind. Die ausführliche Beschreibung der jeweiligen Maßnahmen und Techniken sind in Kapitel 5 und 6 vorhanden.

8.1. Maßnahmen

1. **Reichweiten- und Kampagnenmessung.** Die Erfassung von Unique Users, Impressions und Conversions ist essenziell für die Erfolgskontrolle von Kampagnen und die effiziente Allokation von Werbebudgets, insbesondere im wettbewerbsintensiven digitalen Markt.
2. **Frequency Capping (Begrenzung der Werbewiederholung).** Dies ermöglicht es, Nutzer*innen vor übermäßiger Werbewiederholung zu schützen und Ad Fatigue zu vermeiden. Dies dient nicht nur der UX, sondern ist auch ein zentrales Steuerungsinstrument für Werbequalität und Nutzererlebnis.
3. **Betrugsprävention und Sicherheit (z. B. Fraud Prevention, Bot Detection, Invalid Traffic).** Der Einsatz technischer Merkmale (z. B. Device-Fingerprints, Verhaltensmuster) zur Erkennung von betrügerischen Zugriffen ist unverzichtbar für die Integrität von Werbesystemen und Schutz von Budgets und Nutzer*innen. Dabei kommen auch allgemeine Fraud-Listen zum Einsatz, z. B. vom IAB, die verdächtigen Geräte oder IPs ausschließen.
4. **Personalisierte Werbung.** Gezielt ausgespielte Werbung auf Basis von Interessen, Verhalten oder demografischen Merkmalen erhöht die Relevanz für Nutzer*innen, steigert die Effizienz von Marketingbudgets und trägt zur Refinanzierung digitaler Angebote bei.
5. **Content-Personalisierung.** Die Anpassung von redaktionellen Inhalten, Produktempfehlungen oder Nutzeroberflächen auf Basis des Nutzerverhaltens ist für viele Plattformen Teil der vertraglichen Leistungserbringung oder erfolgt auf Grundlage eines berechtigten Interesses, etwa zur Steigerung der Relevanz.
6. **Conversion-Tracking / Attribution.** Die Zuordnung von Werbekontakten zu konkreten Conversions (Kauf, Registrierung etc.) ist entscheidend für die Erfolgsmessung von Kampagnen.
7. **A/B-Testing und Produktoptimierung.** Der Einsatz von Trackingdaten für datenbasierte Weiterentwicklung von Diensten, z. B. durch Tests alternativer UX-Designs oder Features, ist unverzichtbar für Innovation und Wettbewerbsfähigkeit digitaler Produkte.
8. **Geotargeting / Kontextuelles Targeting.** Die Ausspielung von Inhalten oder Werbung basierend auf Standortdaten oder dem Seitenkontext erhöht die Relevanz für die Nutzer*innen und ist ein bewährtes Steuerungsinstrument im Marketing.
9. **Plattforminterne Empfehlungen / On-Platform-Personalisierung.** Innerhalb von Plattformen werden Nutzeraktivitäten analysiert, um Feeds, Empfehlungen oder Inhalte individuell anzupassen. Diese verbessern die Nutzererfahrung und Bindung an die Plattform.

8.2. Techniken

10. **Cross-Device-Tracking und Identitätsauflösung.** Die Zusammenführung von Interaktionen über mehrere Geräte hinweg ermöglicht konsistente Nutzerprofile, die sowohl für Werbeeffizienz als auch für personalisierte Services entscheidend sind.
11. **Consent-Verwaltung und -Übertragung (TCF / CMP-Systeme).** Ohne funktionierende Consent Management Systeme ist eine rechtskonforme Datenverarbeitung nicht möglich. Die Speicherung und Übermittlung von Einwilligungsentscheidungen (z. B. TCF-String) stellt eine technische Grundlage für viele weitere Prozesse dar.
12. **Data Clean Rooms.** Diese ermöglichen den datenschutzkonformen Abgleich und Analyse von First-Party- und ggf. Third-Party-Daten, um Erkenntnisse für Kampagnenoptimierung zu gewinnen, ohne persönliche Daten direkt weiterzugeben.

13. **ID-Partnerschaften.** Technische Lösungen wie Login-basierte IDs oder gemeinsame Identifikationssysteme (z. B. EU ID, ID5, Ramp ID) erlauben eine konsistente Zielgruppenansprache über Plattformen hinweg und sind wichtig für Reichweitenmessung, Conversion-Tracking und personalisierte Werbung.

9. Fakten zu Tracking und Personalisierung im Kontext des Digital Fairness Act

Im Rahmen des geplanten Digital Fairness Act diskutiert die EU politische Maßnahmen gegen unethische Techniken im Digitalmarketing. Vertrauen von Nutzer*innen ist für die Digitale Wirtschaft überlebensnotwendig. Ohne Vertrauen in die Produkte, Angebote und Information darüber, wie welche Daten verwendet werden, können digitale Geschäftsmodelle nicht florieren.

In der heutigen politischen Diskussion wird oft über die Ausnutzung von Schwächen (Vulnerabilität) oder emotionalen Zuständen von Verbraucher*innen für Kommerzialisierung gesprochen. Mit diesem technischen Fachpapier möchten wir unseren Beitrag zur Aufklärung über die Nutzung von Daten für Tracking leisten. Es dient als Gesprächsangebot und soll über die notwendige Differenzierung zwischen verantwortungsvoller Datenverarbeitung und tatsächlich problematischen Praktiken darstellen.

Die elementare Frage: „Was wird beim Tracking tatsächlich erfasst?“

Dieses Papier macht deutlich, welche Datenarten für Tracking und personalisierte Werbung aktuell genutzt werden – von technischem Identifier (wie Cookie-ID, Device-ID), grobe Nutzungsprofile, Account-Informationen, Standort, Surfverhalten und Segmentierung auf Basis offensichtlicher Interessen und vergangener Interaktionen.

Dieses Papier grenzt klar ab, dass die direkte Erfassung und Auswertung besonders sensibler Daten, wozu explizit auch emotionale Zustände zählen, bewusst ausgeschlossen ist, sowohl aus technischen (keine zuverlässige Messung ohne Explicitsignal, z.B. Gesundheitsdaten) als auch aus regulatorischen Gründen (Art. 9 DSGVO, Verbot der Profilierung auf Basis besonders geschützter Merkmale). Es gibt keine technische Infrastruktur oder Praxis, die eine Verfolgung individueller emotionaler Zustände, im Sinne einer kontinuierlichen Emotionsmessung oder -auswertung, im Alltag von Werbung oder Personalisierung zulässt. Weder werden psychologische Profile auf dieser Ebene erstellt, noch existieren Standardprozesse zur individuellen „Emotions- oder Vulnerabilitätserkennung“. Verfahren, die als besonders invasiv gelten (wie Ultraschalltracking zur Kontextkopplung oder psychometrisches Fingerprinting auf individueller Ebene), werden explizit nicht eingesetzt und von der Branche selbst abgelehnt.

Personalisierte, verhaltens- und interessenbasierte Werbung, wie sie in der digitalen Praxis üblich ist, basiert auf segmentierten Gruppenprofilen („Zielgruppen“, „Segments“), nicht auf individuellen Schwächen oder situativen Emotionen.

Das in der politischen Debatte immer wieder geforderte Verbot einer systemischen Emotionskontrolle oder gezielten Ausnutzung von Momentan-Schwächen durch Personalisierungs- und Werbesysteme basiert nicht auf einer realen, technischen Grundlage. In der aktuellen Praxis sind diese Risiken abstrakt und werden durch technische Begrenzungen ausgeschlossen. Die gezielte Ausnutzung emotionaler Zustände oder individueller Vulnerabilitäten findet in der digitalen Werbepraxis nicht statt. Personalisierung basiert auf Gruppenprofilen und offensichtlichen Nutzungsinteressen, nicht auf psychologischer Manipulation. Darüber hinaus sorgen auch die zahlreichen bestehende Datenschutz- und Verbraucherschutzregulierungen (insb. DSGVO, DSA) sowie Branchen-Selbstbeschränkungen dafür, dass bestimmte Praktiken ausgeschlossen sind.

Was jedoch verbessert werden muss, ist die Umsetzung und Durchsetzung des bestehenden Rechtsrahmens. Eine konsequente und faire Enforcement-Praxis gegenüber allen Marktteilnehmern würde nicht nur Verbraucher*innen besser schützen, sondern gleichzeitig Betrugsprävention stärken und ein echtes Level-Playing-Field für die Digitale Wirtschaft

sicherstellen. Darüber hinaus streben wir Rechtssicherheit und klare, praktikablen Leitlinien an, die sowohl für Behörden als auch für Unternehmen nachvollziehbar sind. Ziel ist es, ein gemeinsames Verständnis für legitime, innovationsgetriebene Geschäftspraktiken der Digitalen Wirtschaft zu schaffen und gleichzeitig Graubereiche zu minimieren, die zu Unsicherheiten oder ungleichen Wettbewerbsbedingungen führen könnten. Verantwortungsvolle Datenverarbeitung in Verbindung mit Rechtsklarheit im heutigen regulatorischen Framework ist die Grundlage, dass digitale Geschäftsmodelle nachhaltig, effizient und vertrauenswürdig für alle Beteiligten agieren können.