Internationaler Arbeitskreis für
Datenschutz in der Technologie

Arbeitspapier zu den Risiken im Zusammenhang mit dem Tracking- und Targeting-Ökosystem im digitalen Werbemarkt

Schriftliches Verfahren vor der 67. (virtuellen) Sitzung am 24. April 2021

Einführung

1. Die Funktionsweise des modernen Internets macht es nahezu unmöglich, anonym online zu sein. Die meisten Webseiten und Apps betten Technologien ein - manchmal ohne sie vollständig zu verstehen -, die direkt oder indirekt identifizierte oder ausgewählte Nutzer*innen über Webseiten, Apps und Geräte hinweg verfolgen, sogar in ihrem „Offline-Leben", Profile von ihnen erstellen und Informationen an verschiedene Dritte und Plattformen liefern, die Daten und Dienste zur gezielten Nutzer*innenansprache verkaufen.

2. So werden personenbezogene Daten über weit verzweigte Datensammelnetzwerke zusammengetragen, zu denen auch große Plattformbetreiber*innen gehören.[1] Durch den Verkauf von Werbeflächen auf ihren Webseiten mittels Echtzeit-Auktionen (auch bekannt als Real-Time-Bidding oder RTB), die Integration von Social-Plug-ins und Share-Buttons sowie die Nutzung von Software Development Toolkits (SDKs), Analyse- und Messtools werden Webseitenbetreiber*innen und App-Anbieter*innen zu Datenlieferant*innen für die Online-Werbe-Lieferketten. Damit helfen sie, die Datenprofile von Plattformen, Datenhändlern und –maklern (sog. Broker) sowie Ad-Tech-Unternehmen anzureichern.

3. Während Endnutzer*innen einen Teil des Trackings in ihren Geräten, Browsern oder Apps erkennen können, arbeiten viele Tracking-Technologien „hinter den Kulissen". Diese Praktiken werden meist erst nach entsprechenden Untersuchungen aufgedeckt. Die Undurchsichtigkeit, die dieses Daten-Ökosystem kennzeichnet, wird durch die Tatsache verschärft, dass viele der beteiligten Unternehmen ihr Angebot nicht unmittelbar an Endnutzer*innen richten; die meisten Menschen haben noch nie von ihnen gehört. Und selbst wenn, gibt es nur wenige Informationen darüber, woher die Daten stammen und mit wem sie geteilt werden.[2] Dies hat Auswirkungen auf die Ausübung von Rechten und die Möglichkeit, Kontrolle auszuüben, z. B. durch die Erteilung einer informierten Einwilligung oder durch die Einreichung von Anträgen auf Auskunft oder Löschung.

4. Der Detailgrad der verarbeiteten Informationen variiert: Dies beginnt bei der bloßen Zählung der individualisierten Besuche auf einer bestimmten Webseite oder Informationen über Webseiten, die der/die Nutzer*in vorher und nachher besucht hat. Darüber hinaus können sie detaillierte Aufzeichnungen über die Teile einer Webseite, die der/die Nutzer*in ansieht, angeklickte Inhalte, Mausbewegungen, Lesedauer, Tippverlauf und Tastenanschlagdynamik, Interaktion mit der App usw. umfassen. Diese Daten werden typischerweise mit dauerhaften und vorübergehenden eindeutigen Kennungen verknüpft. Die mit der Kennung verknüpften Informationen können dann

---

[1] ICO, Update report into adtech and real-time bidding, 20 June 2019, https://ico.org.uk/media/about-the-ico/documents/2615156/adtech-real-time-bidding-report-201906.pdf.

[2] https://privacyinternational.org/advocacy/2434/why-weve-filed-complaints-against-companies-most-people-have- never-heard-and-what.

mit demografischen Daten und abgeleiteten Daten über Nutzer*innen verknüpft werden, die auf Datenanalysen und gesammelten oder erworbenen Daten aus anderen Quellen basieren.

Umfang

5. Das 2013 von der IWGDPT veröffentlichte Arbeitspapier zu Web-Tracking und Datenschutz[3] beschrieb die gängigen Methoden zum Sammeln, Analysieren und Verarbeiten von Daten bezüglich der Nutzung von Diensten der Informationsgesellschaft mit Computern, Tablets, Smartphones und zunehmend auch anderen „intelligenten" und verbundenen Geräten. Einige Tracking-Aktivitäten werden zu Sicherheits- und Messzwecken durchgeführt. Die überwiegende Mehrheit dieser Technologien zielt jedoch darauf ab, Nutzer*innendaten von verschiedenen Webseiten, Apps, Geräten und darüber hinaus zu verknüpfen, um Verhaltensmuster zu erkennen, um Endnutzer*innen Eigenschaften oder Merkmale zuzuordnen oder diese abzuleiten und um diese Daten zu umfassenden digitalen Profilen zusammenzustellen, die zur Personalisierung von Werbung und Diensten verwendet werden, in einigen Fällen auch zur Manipulation der Nutzer*innen.

6. Die Tracking-Technologien und die Dimensionen der in Big-Data-Datenbanken gesammelten Daten haben sich seit 2013 ganz erheblich weiterentwickelt und erweitert, insbesondere mit der Möglichkeit, Nutzer*innen über mehrere Geräte hinweg zu verfolgen und unter Berücksichtigung der Vielzahl von Anwendungen und Webseiten, die Daten mit Dritten teilen. Was noch als Vision oder mögliche Entwicklung formuliert wurde[4], ist Realität geworden. Der Online-Werbemarkt hat dabei eine systematische Weiterentwicklung durchlaufen. Es hat sich eine Vielzahl von Strukturen des Trackings und Targetings von Nutzer*innen mit verschiedenen Akteuren etabliert, von denen einige aufgrund ihrer Marktmacht sehr mächtig sind. Dieses Papier skizziert Bedenken hinsichtlich der Privatsphäre und des Datenschutzes in Bezug auf dieses Tracking-, Profiling- und Targeting-Ökosystem, das auch über die digitale Werbung hinaus genutzt werden kann, um den Meinungsbildungsprozess zu manipulieren. Es bestehen erhebliche Sorgen hinsichtlich der Folgen dieses Ökosystems für die Demokratie.[5] Das Papier gibt auch Empfehlungen an Gesetzgeber, Regulierungsbehörden, Behörden und die beteiligten Unternehmen.

Tracking- und Targeting-Ökosystem

7. Der digitale Werbemarkt besteht aus einer Vielzahl von unterschiedlichen Akteuren: Ziel ist es, dass die Werbetreibenden die passenden Kund*innen mit relevanter und ansprechender Werbung zum richtigen Zeitpunkt erreichen, was wiederum den Veröffentlichenden helfen soll, ihre Kreativität und Inhalte zu monetarisieren. Zwischen diesen drei Akteuren sind viele Dienstleister unterschiedlicher Art involviert, die Daten aus verschiedenen Quellen sammeln, analysieren, miteinander verknüpfen, persönliche Profile erstellen und/oder sie anderen Akteuren zur Verfügung stellen[6]. Obwohl auch Zweifel an der Wirksamkeit geäußert wurden[7], hat sich die individuelle, zielgerichtete Werbung als das dominierende Konzept entwickelt, um die gewünschte Zielgruppe zu erreichen.

---

3 IWGDPT, „Working Paper on Web Tracking and Privacy: Respect for context, transparency and control remains essential", 53. Sitzung, 15.-16. April 2013, Prag (Tschechische Republik).

4 IWGDPT, „Working Paper on Web Tracking and Privacy: Respect for context, transparency and control remains essential", 53. Sitzung, 15.-16. April 2013, Prag (Tschechische Republik), Abs 7.

5 Siehe https://ico.org.uk/media/action-weve-taken/2259369/democracy-disrupted-110718.pdf und https://privacyinternational.org/long-read/2850/data-exploitation-and-democratic-societies.

6 Für einen Überblick vgl. auch Forbrukerrådet (Norwegischer Verbraucherrat), Out of control, How consumers are exploited by the online advertising industry,, 14. Januar 2020, https://www.forbrukerradet.no/undersokelse/no-undersokelsekategori/report-out-of-control/, Kapitel 2.2, S. 13.

7 https://weis2019.econinfosec.org/wp-content/uploads/sites/6/2019/05/WEIS_2019_paper_38.pdf.

8. Das digitale Werbe-Ökosystem beinhaltet die Verarbeitung persönlicher Daten von Milliarden Personen. Nutzer*innendaten werden auf vielfältige Weise gesammelt, generiert, geteilt und verarbeitet, wobei eine Reihe von Tacking-Technologien[8] wie Cookies, Web Beacons, Device Fingerprinting, Tags und SDKs zum Einsatz kommen, um Kund*innen auf der Grundlage von besuchten Seiten, angeklickten Links und gekauften Produkten zu segmentieren/klassifizieren.

9. Mit den verschiedenen elektronischen Werkzeugen können Nutzer*innen Profile erstellt werden. Sie verfolgen nicht nur die Nutzer*innen, sondern können auch alle gesammelten Daten für weiteres Data Mining verwenden, um herauszufinden, was über die Vorlieben diese Nutzer*innen und ihr zukünftiges Verhalten abgeleitet werden kann. Diese Profile werden verwendet, um Menschen auf verschiedene Weise anzusprechen, z. B. um Werbung, Inhalte und Nachrichten auf ihre angenommenen spezifischen Interessen zuzuschneiden. Social-Media-Anbieter*innen und Online-Plattformen können die besagten elektronischen Tools in ihre Umgebungen und in die Webseiten und Apps von Drittanbieter*innen einbinden, die an Interaktion mit dem Publikum und dessen (Ein)Bindung interessiert sind.

10. Online-Publisher verwenden Tracking-Code von verschiedenen Unternehmen, darunter nicht nur die bekannten wie Google und Facebook, sondern auch eine Vielzahl weitgehend unbekannter großer und kleiner Unternehmen, um Werbung gezielt zu platzieren. Wenn der Code eines Unternehmens auf vielen verschiedenen Webseiten eingebettet ist, kann es detaillierte Profile über Einzelpersonen erstellen, während sie sich im Web und in Apps bewegen, indem es ihnen eindeutige Kennungen zuweist. So können Nutzer*innen wiedererkannt werden. Nicht nur große Unternehmen, sondern auch Unternehmensnetzwerke sind in der Lage, durch den Austausch von Informationen solche umfassenden Profile zu erstellen.

11. Sogar ein großes Ausmaß an Offline-Aktivitäten wird verfolgt und in das Werbe-Ökosystem einbezogen. So werden beispielsweise Daten gesammelt, wenn Verbraucher in einem Geschäft Produkte mit einer Kundenkarte kaufen oder mit einer Kredit- oder EC-Karte bezahlen. Darüber hinaus verfolgen viele Apps permanent den Standort des Geräts - im Falle von Smartphones ist dies gleichbedeutend mit dem Standort des/der Nutzer*in - und erstellen so ein detailliertes Profil der physischen Bewegung des/der Nutzer*in. Da diese Daten nicht nur von einem einzigen Unternehmen gesammelt, sondern auch auf einem Markt verkauft werden, können Daten aus verschiedenen Quellen leicht miteinander verknüpft werden, um ein Profil abzurunden.

12. Der weltweite Umsatz des digitalen Werbemarktes wuchs 2019 um 15,9 % auf 124,6 Milliarden US-Dollar, so der IAB [9] Internet Advertising Revenue Report[10] von PwC, der im Mai 2020 veröffentlicht wurde. Der IAB-Bericht identifiziert zwei Hauptfaktoren, die das Wachstum vorantreiben: Selbstbedienungsplattformen, die es kleinen Unternehmen ermöglichen, einfach im Internet zu werben, und der Aufstieg von Online-Startups, die diese Selbstbedienungsplattformen nutzen, um Produkte direkt an Verbraucher zu verkaufen.

Personenbezogene Daten in diesem Kontext

13. Datenschutzgrundsätze gelten für alle Informationen, die eine identifizierte oder identifizierbare natürliche Person betreffen. Wenn Nutzer*innen Webseiten besuchen oder Apps installieren, die Schnipsel von relevantem Code von Drittanbieter*innen eingebettet haben, sammelt dieser Code Daten aus der Sitzung und verknüpft sie mit einer (normalerweise eindeutigen) Kennung (auch möglich durch Geräte-Fingerabdruck usw.).[11] Da derselbe Code eines/einer Drittanbieter*in

8 https://privacyinternational.org/explainer/2976/how-do-tracking-companies-know-what-you-did-last-summer.

9 Interactive Advertising Bureau, https://www.iab.com.

10 https://www.iab.com/wp-content/uploads/2020/05/FY19-IAB-Internet-Ad-Revenue-Report_Final.pdf.

11 Reuben Binns / Elettra Bietti, Acquisitions in the third party tracking industry: competition and data protection aspects, https://osf.io/preprints/lawarxiv/fe8u7/download , Abs. 1.1.

typischerweise auf mehreren verschiedenen Webseiten oder Apps eingebettet ist,[12] ermöglicht die eindeutige Kennung die Zusammenführung von Daten über diese Webseiten, Apps oder Geräte hinweg. Daraus ergeben sich einzelne Verhaltensprofile, die alle Arten von Informationen enthalten, die mit Hilfe der Kennung gesammelt und zusammengeführt werden. Da diese Profile sehr spezifische Informationen enthalten, können sie sogar zwischen verschiedenen Unternehmen oder Netzwerken, die unterschiedliche Kennungen verwenden, zusammengeführt werden.[13] Diese Daten müssen als personenbezogene Daten angesehen werden. Der Bezug zu einer Person kann sich aus den Umständen oder dem Kontext ergeben, in dem die Informationen verarbeitet werden. Es ist nicht relevant, dass Namen aus der realen Welt möglicherweise nicht mit den Daten verbunden sind, wenn es um den Personenbezug geht. Wenn sich - wie bei vielen Menschen - große Teile des Lebens in der Online-Welt abspielen, ist es relevant, ob Personen über Online-Kennungen identifiziert oder angesprochen werden können. Um festzustellen, ob eine natürliche Person identifizierbar ist, reicht es aus, wenn die Person herausgegriffen, von anderen unterscheidbar und eindeutig adressierbar gemacht wird. Genau das ist Ziel und Zweck des Targeting-Ökosystems.

14. Es kann zu leichten Ungenauigkeiten kommen, da Geräte oder Browser von mehr als einer Person genutzt werden können. In Zeiten hochindividualisierter Geräte, insbesondere von Smartphones, nehmen die Fälle der gemeinsamen Nutzung jedoch stetig ab. Unabhängig davon ist es bei ausgefeilten Profilen möglich, Nutzer*innen anhand ihres tatsächlichen Surfverhaltens zu individualisieren (Browser-Historie; Nutzer*innenverhalten auf einer Webseite, Anmeldung bei bestimmten Konten usw.).

Profiling

15. Profiling ist das Herzstück des digitalen Werbeökosystems. Verschiedene und scheinbar harmlose Daten können kombiniert werden, um ein aussagekräftiges, umfassendes Profil einer Person zu erstellen.[14] Fortschritte in der Datenanalyse sowie beim maschinellen Lernen haben es möglich gemacht, aus immer mehr Quellen von Daten, die in keiner Weise sensibel sind, sensible Daten abzuleiten und vorherzusagen. So hat sich zum Beispiel herausgestellt, dass von Nutzer*innen auf Facebook geteilte Inhalte ein Indikator für das zukünftige Auftreten von Depressionen sind.[15] Dieselben Techniken haben es einfacher gemacht, einzelne Individuen aufgrund von Daten über ihr Verhalten über Geräte, Dienste und sogar im öffentlichen Raum zu identifizieren.[16] Solche Profile erlauben es, aus den Daten hochsensible Details abzuleiten, die zutreffend oder nicht zutreffend sein können und die auf eine Art und Weise ungenau sein können, dass bestimmte Gruppen von Menschen systematisch falsch charakterisiert oder falsch klassifiziert werden. Solche Analysen bedeuten, dass das Ergebnis der Datenanalyse größer ist als die Summe ihrer Teile: Selbst scheinbar harmlose Daten können zusammen verwendet werden, um Einblicke und Rückschlüsse auf sensible Details im Leben einer Person zu erhalten.

16. Da Profiling ohne weiteres Zutun von Personen erfolgen kann, wissen diese in der Regel nicht, ob diese Profile zutreffend sind, für welche Zwecke sie verwendet werden und welche Folgen eine solche Verwendung hat. In vielen Fällen weiß oder bemerkt ein*e Internetnutzer*in nicht einmal, dass die angezeigte Werbung oder der Inhalt auf der Grundlage ihres bzw. seines individuellen

12 Reuben Binns / Elettra Bietti, Acquisitions in the third party tracking industry: competition and data protection aspects, https://osf.io/preprints/lawarxiv/fe8u7/download , Abs. 1.1.

13 Forbrukerrådet (Norwegischer Verbraucherrat), Out of control, How consumers are exploited by the online advertising industry,, https://www.forbrukerradet.no/undersokelse/no-undersokelsekategori/report-out-of-control/, Kapitel 2.5, S. 25.

14 https://privacyinternational.org/feature/1721/snapshot-corporate-profiling and https://privacyinternational.org/report/1718/data-power-profiling-and-automated-decision-making-gdpr.

15 https://www.pnas.org/content/115/44/11203.

16 De Montjoye, Y.-A./ Hidalgo, C.A./ Verleysen, M. & Blondel, V.D., Unique in the Crowd: The privacy bounds of human mobility, Nature srep. 3, 1376; DOI:10.1038/srep01376 (2013).

Profils zusammengestellt wurde. Dieses fehlende Bewusstsein verhindert, dass Einzelne ihre Rechte in Bezug auf Datenschutz und Privatsphäre wahrnehmen können.

17. Wie oben dargestellt, beinhaltet dieses Profiling die Verarbeitung von personenbezogenen Daten. Daher müssen die Datenschutzbestimmungen zum Profiling - soweit vorhanden - berücksichtigt werden.

Bedenken hinsichtlich Privatsphäre und Datenschutz

18. Das Ökosystem von Tracking und Targeting, wie es derzeit funktioniert, wurde über nationale Grenzen hinweg entwickelt, obwohl es in einigen wichtigen Rechtsordnungen klare Datenschutzbestimmungen gibt. Die Europäische Union zum Beispiel führte 1995 ihre erste Datenschutzgesetzgebung ein, die Datenschutzrichtlinie [17]. Sie enthielt bereits das Prinzip des „Privacy by Design" [Datenschutz durch Technikgestaltung][18], das Erfordernis einer spezifizierten Rechtsgrundlage für jede Verarbeitung personenbezogener Daten [19] und Vorschriften zur Transparenz des Verarbeitungsprozesses [20]. Die im Folgenden aufgeworfenen, wichtigsten Fragen hätten also schon zu Beginn dieser Entwicklungen bekannt sein und berücksichtigt werden müssen.

19. Ungeachtet der Komplexität des Ökosystems und möglicher Schwierigkeiten bei der praktischen Durchführbarkeit liegt es in der Verantwortung jedes Verantwortlichen und jedes Auftragsverarbeiters, der an diesem Ökosystem beteiligt ist, alle geltenden gesetzlichen Vorschriften vollständig einzuhalten. Geschäftsmodelle müssen so entwickelt werden, dass sie den rechtlichen Rahmen respektieren, in den sie implementiert werden sollen.

Mangelnde Transparenz / Nachvollziehbarkeit

20. Den meisten Nutzer*innen wird verborgen bleiben, dass nicht nur die Webseitenbetreiber*innen oder App-Anbieter*innen selbst Tracking-Cookies auf ihren Endgeräten setzen, sondern dass eingebettete Technologien es Dritten ermöglichen, Tracking-Cookies zu setzen, Geräte-Fingerabdrücke zu sammeln, Inhalte über Pixel hochzuladen etc. Die Nutzer*innen haben oft keine ausreichenden Informationen darüber, welche Dritten an der Verarbeitung ihrer Daten beteiligt sind, welche Zwecke die Datenverarbeitung verfolgt, welche Arten von Daten gesammelt werden, wie ihr Verhalten kategorisiert wird und welche Folgen das Tracking für sie hat. Diese breite Streuung der Daten der Nutzer*innen ist nicht transparent. In vielen Fällen geht aus den Datenschutzrichtlinien und -erklärungen nicht klar hervor, wer an der Verarbeitung beteiligt ist und wofür die Daten verwendet werden.

21. Nichtsdestotrotz sind die für die Datenverarbeitung Verantwortlichen in vielen Rechtssystemen verpflichtet, gegenüber betroffenen Personen Transparenz über den Zweck und den Umfang der Datenverarbeitung herzustellen. Wenn ein*e Webseitenbetreiber*in oder App-Anbieter*innen personenbezogene Daten an Dritte weitergibt oder ihnen die Erhebung dieser Daten ermöglicht, ist der/die Webseitenbetreiber*in oder App-Anbieter*in oft die einzige Partei des Ökosystems, die mit dem/der Nutzer*in interagiert. Daher muss der/die Webseitenbetreiber*in oder App-Anbieter*in praktisch dafür verantwortlich sein, die Nutzer*innen über alle Prozesse zu informieren, denen ihre Daten unterworfen werden, auch wenn der/die Webseitenbetreiber*in oder App-Anbieter*in möglicherweise die gesamte Datenverarbeitung nicht selbst durchführt. Dessen ungeachtet ist jeder Akteur, der als Verantwortlicher personenbezogene Daten innerhalb des Ökosystems verarbeitet, selbst dafür verantwortlich, dass dem/der Nutzer*in ausreichende

17 Richtlinie 95/46/EG.

18 Erw. 46 der Richtlinie 95/46/EG.

19 Art. 7 der Richtlinie 95/46/EG.

20 Art. 10 - 12 der Richtlinie 95/46/EG.

Transparenz über den Umfang der Verarbeitung geboten wird. Viele Verantwortliche können dies nur erreichen, indem sie dem/der jeweiligen Webseitenbetreiber*in oder App-Anbieter*in klare und ausreichende Informationen zur Verfügung stellen.

22. In Anbetracht der Komplexität des aktuellen Ökosystems und der riesigen Anzahl seiner Teilnehmer*innen wird es kaum möglich sein, den Prozess so darzustellen, dass die Nutzer*innen tatsächlich verstehen können, was mit ihren Daten geschieht oder geschehen könnte. Dies gilt umso mehr, als die Daten nicht nur von einem einzelnen Akteur gesammelt und genutzt werden, sondern die gesammelten Daten oft durch Daten angereichert werden, die mit Vorhersage-Technologien abgeleitet und mit Datensätzen verknüpft werden, die von anderen Akteuren gesammelt und verkauft werden. Diese Datensätze werden nicht nur in der Online-Umgebung gesammelt, sondern auch das Offline-Verhalten wird stark verfolgt. Letztendlich ist es für eine*n Nutzer*in nahezu unmöglich zu wissen, geschweige denn zu kontrollieren, welche Datensätze über sie oder ihn in dem Ökosystem existieren und welche Akteure diese zu welchen Zwecken verarbeiten. Nichtsdestotrotz ist Transparenz gegenüber den Nutzer*innen eine rechtliche Verpflichtung und eine Voraussetzung für die Kontrolle durch die Nutzer*innen.

23. Herkömmliche Cookie-Banner sind oft nicht transparent und erfüllen nicht die Anforderungen an eine datenschutzrechtliche Einwilligung, wie sie in vielen Datenschutzgesetzen festgelegt sind. Außerdem suggeriert die Formulierung oft, dass der/die Nutzer*in eine Wahl hat, was bei vielen dieser Banner nicht der Fall ist. Im Gegenteil, es fehlt oft an der Wahlfreiheit. Noch immer enthalten viele Banner nur einen „OK"-Button, aber keine Ablehnungsmöglichkeit, oder eine Ablehnungsmöglichkeit, die so umständlich ist, dass der/die Nutzer*in es aufgibt, eine Wahl zu treffen. Andere Banner zielen darauf ab, die Illusion einer stillschweigenden Zustimmung zu schaffen, bei der der/die Nutzer*in weiter auf der Webseite surft. Selbst wenn es eine Wahlmöglichkeit gibt, sehen wir oft, dass die Informationen nicht ausreichen, um den Nutzer*innen eine Vorstellung von der Dimension des Ökosystems der Online-Werbung, in das ihre Daten eingespeist werden, und der sich für sie daraus ergebenden Konsequenzen zu geben.

24. Während die meisten Cookies von den Nutzer*innen zumindest erkannt werden können, hinterlässt der Einsatz anderer Tracking-Mechanismen, wie z. B. Device Fingerprinting, kaum Spuren, die für den/die Nutzer*in nachvollziehbar wären. Den Nutzer*innen bleibt fast keine Möglichkeit, das Sammeln von Daten zu erkennen oder einzugreifen. Dennoch bieten viele Webseitenbetreiber*innen oder App-Anbieter*innen noch weniger Transparenz, wenn es um diese alternativen Tracking-Mechanismen geht.

25. Viele Webseitenbetreiber*innen behaupten, dass die verarbeiteten Daten pseudonym sind und nicht mit der einzelnen Person namentlich in Verbindung gebracht werden können, indem sie vorgeben, dass die Nutzer*innen nicht individuell identifiziert werden können. Aber auch ohne Verwendung von realen Namen werden andere Kennungen verwendet, um detaillierte, mit diesen Kennungen verknüpfte Profile zu erstellen, und um sie wiederum mit Werbung oder anderen Nachrichten anzusprechen, die auf den im Profil enthaltenen Informationen basieren. So werden z. B. gehashte E-Mails häufig als Profilkennungen verwendet, da sie es ermöglichen, auf einfache Weise externe und/oder Offline-Daten über die Nutzer*innen zu importieren, und sie werden auch als pseudonymisiert bezeichnet. Der prominente Hinweis auf die Pseudonymisierung ist daher für die Nutzer*innen eher irreführend.

26. Im Umfeld von Apps ist das Tracking noch intransparenter als auf Webseiten. Wenn überhaupt, erfolgt eine Benachrichtigung über die Datenschutzrichtlinien inklusive der Tracking-Tools, sobald die App installiert ist. Im Gegensatz zu Webseiten, die bei jedem Öffnen das sogenannte „Cookie-Banner" anzeigen, das den/die Nutzer*in an die Verarbeitungsweise erinnert, zeigen Apps diese Informationen nicht bei jedem Start. Außerdem passt die Textmenge nicht sehr gut zu einem Smartphone-Display. Dies muss bei der Gestaltung von Transparenz-Tools einer App berücksichtigt werden, z. B. durch Integration verschiedener Ebenen und Hervorhebung der wichtigsten Datenschutzthemen auf der ersten Ebene.

Fehlende Kontrolle/ Eingeschränkte Eingriffsmöglichkeiten / Verknüpfbarkeit

27. Ein großer Teil des täglichen Lebens hat sich heutzutage ins Internet verlagert, insbesondere viele Dienstleistungen, z. B. das Buchen von Flügen, das Lesen von Zeitungen, alle Arten von Einkäufen, Interaktionen mit Banken und Versicherungen, Ankündigungen von Veranstaltungen aller Art usw. Ein sinnvolles Surfen im Internet und die Nutzung dieser Dienste zwingt die Nutzer*innen, die Kontrolle über die Erhebung und Verarbeitung persönlicher Daten zu ihrem Online-Verhalten und den gesuchten Informationen/Inhalten abzugeben.

28. Nahezu alle diese Internetdienste sind mit Werkzeugen aus dem Tracking-Ökosystem ergänzt, die weit über das hinausgehen, was aus Funktions- und Sicherheitsgründen notwendig ist. Die meisten Nutzer*innen haben keine effektiven Möglichkeiten, die Sammlung von personenbezogenen Daten auf der Basis von Kennungen zu stoppen, wenn sie auf Webseiten und/oder Apps zugreifen und das Internet sinnvoll nutzen möchten:

29. In Bezug auf Webseiten gibt es Tools, die Cookies zumindest identifizieren und blockieren können. Diese Tools ermöglichen es dem/der Nutzer*in, einige Tracking-Aktivitäten zu verhindern. Sie können dem/der Nutzer*in jedoch keine vollständige Kontrolle darüber geben, welche persönlichen Daten gesammelt werden, da das Setzen von Cookies nicht die einzige Tracking-Technologie ist. Darüber hinaus machen es einige Webseitenbetreiber*innen zwingend erforderlich, Cookies, die dem Tracking dienen, auf dem Endgerät des/der Nutzer*in zu speichern, da sonst Inhalte oder Dienste nicht verfügbar sind.

30. Bei Apps haben die Nutzer*innen sogar noch weniger Möglichkeiten, in die Weitergabe von Daten an Plattformen oder andere Dritte einzugreifen.

31. In dem Maße, in dem den Nutzer*innen durch die Möglichkeit, Privatsphäre-Einstellungen zu ändern, (wenig) Kontrolle über das Sammeln ihrer Daten gewährt wird, scheinen viele Unternehmen große Anstrengungen zu unternehmen, ihre Produkte so zu gestalten, dass die Nutzer*innen diese Maßnahmen nicht ergreifen. Dies kann bedeuten, dass das Tracking von Nutzer*innen die Standardeinstellung ist, dass die Einstellungen versteckt werden, dass die entsprechenden Schaltflächen so gestaltet werden, dass es unwahrscheinlich ist, dass sie angeklickt werden oder dass sie mit Einschränkungen der Funktionalität drohen. Im Gegensatz dazu sind Unternehmen aufgrund vieler gesetzlicher Regelungen an die Prinzipien Privacy by Design und Privacy by Default gebunden, was bedeutet, dass sie verpflichtet sind, datenschutzfreundliche Einstellungen standardmäßig zu implementieren.

Fehlende Datenminimierung

32. Das gesamte Ökosystem ist auf der Sammlung von möglichst vielen, möglichst detaillierten und möglichst personalisierten Daten aufgebaut und steht damit im direkten Widerspruch zum Prinzip der Datenminimierung. Der Erfolg vieler Unternehmen in diesem Ökosystem hängt direkt von der Masse an personenbezogenen Daten ab, die sie sammeln können. Diese Unternehmen behaupten, je mehr Daten sie verarbeiten, desto genauer seien die Vorhersagen und desto maßgeschneiderter und gezielter könne die Werbung/der Inhalt sein. Da die Unternehmen über einen Bietmechanismus gegeneinander antreten, ist es für sie entscheidend, so zielgerichtet wie möglich zu sein, was zu einem Anreiz führt, immer mehr Daten zu sammeln als der Mitbewerber. Wie heutzutage oft gesagt wird: Daten sind das neue Gold oder Öl.

Unterminierung des besonderen Schutzes sensibler Daten

33. Es ist wichtig zu beachten, dass die Datenverwertungspraktiken des Ökosystems auch spezielle Kategorien oder sensible personenbezogene Daten umfassen können, [21] wie z. B. Gesundheitsdaten, Daten über das Sexualleben oder die sexuelle Orientierung einer Person oder Daten, die politische Meinungen offenbaren. [22] Beispielsweise könnten Besuche auf gesundheitsbezogenen Webseiten oder Apps, insbesondere Versicherungs-Apps, im Falle von Tracking ein Bild über den Gesundheitszustand, Krankheiten und Therapien zeichnen. Gleichzeitig kann das Tracking auf bestimmten Webseiten und Apps Aufschluss über religiöse Überzeugungen oder sexuelle Vorlieben sowie über die wirtschaftlichen Verhältnisse oder politischen Ansichten des Nutzers oder der Nutzerin geben. Diese Datenkategorien sind in vielen Rechtsordnungen besonders geschützt und dürfen nur unter besonderen Rechtmäßigkeitsvoraussetzungen (z. B. ausdrückliche Einwilligung) verarbeitet werden, da bei der Verarbeitung dieser Daten hohe Diskriminierungs- und Manipulationsrisiken entstehen. Solche Anforderungen an die Rechtmäßigkeit sehen zumindest die Kenntnis des Kontexts, in dem die Daten verwendet werden, der Zwecke, für die sie verarbeitet werden, und der spezifischen Datentypen sowie die Möglichkeit des Eingriffs vor. Wenn Plattformen auf der Grundlage der Analyse dieser sensiblen Daten Zielgruppen auswählen, ohne diese Aktivitäten transparent zu machen und den betroffenen Personen Instrumente zum Eingreifen an die Hand zu geben, werden besondere gesetzlich vorgesehene Schutzmaßnahmen untergraben. Verwundbarkeiten von Einzelpersonen sind leicht zu erkennen und auszunutzen.

34. Im September 2019 veröffentlichte Privacy International eine Studie, die aufzeigt, wie beliebte Webseiten über Depressionen in Frankreich, Deutschland und Großbritannien Nutzer*innendaten mit Werbetreibenden, Datenmaklern und großen Tech-Unternehmen teilen, während einige Webseiten mit Depressionstests Antworten und Testergebnisse an Dritte weitergeben.[23] Eine weitere Untersuchung zeigte, dass Menstruations-Apps intime Details über das Sexualleben und die psychische Gesundheit der Nutzerinnen mit Facebook und/oder Dritten teilen. Dazu gehörten unter anderem Informationen darüber, ob Nutzerinnen ungeschützten Sex hatten, ob sie sich ängstlich oder depressiv fühlen usw.[24] In beiden Fällen wirft die Datensammelpraxis bestimmter Unternehmen die grundsätzliche Frage auf, ob solche sensiblen Daten möglicherweise auch zu Werbezwecken in die Profile der Nutzer*innen einfließen könnten.

35. Selbst wenn die gesammelten Daten zunächst nicht sensibel sind, können die Big-Data-Analyse und die Vorhersage bestimmter Verhaltensweisen äußerst sensible Daten ergeben, die für diskriminierende Zwecke verwendet werden können, ohne dass der/die Nutzer*in die Möglichkeit hat, Schutzmechanismen zu erkennen oder durchzusetzen.

Automatisierte Entscheidungsfindung/Profilierung

36. Das Ökosystem von Tracking und Targeting ist als eine Reihe vollautomatisierter Prozesse konzipiert. Die Entscheidung, welcher Inhalt oder welche Werbung einer individuell anvisierten Person präsentiert wird, ist das Ergebnis der von Maschinen gesammelten, analysierten und angereicherten Daten des Nutzers oder der Nutzerin, wobei es vom jeweiligen Einzelfall abhängt, wie viele Daten verwendet werden und wie spezifisch der Inhalt auf den/die Nutzer*in abgestimmt ist. Der RTB- Prozess ist ein Modell der automatisierten Entscheidung.

---

21 Vgl. Datenschutz-Grundverordnung (EU) 2016/679 (DSGVO), Artikel 9.

22 UK Information Commissioner's Office (ICO, Datenschutzaufsichtsbehörde des Vereinigten Königreichs), ICO, - Update report into adtech and real-time bidding, 20 June 2019, https://ico.org.uk/media/about-the-ico/documents/2615156/adtech-real-time-bidding-report-201906.pdf.

23 https://privacyinternational.org/sites/default/files/2019-09/Your%20mental%20health%20for%20sale%20-%20Datenschutz%20International.pdf.

24 https://privacyinternational.org/long-read/3196/no-bodys-business-mine-how-menstruation-apps-are-sharing-your- Daten.

37. Obwohl gezielte Werbung oder Inhalte in den meisten Fällen keine unmittelbaren rechtlichen Folgen haben, haben sie reale Auswirkungen. Der Europäische Datenschutzausschuss stellt fest, dass die Entscheidung, gezielte Werbung auf der Grundlage von Profiling zu präsentieren, in den Anwendungsbereich von Artikel 22 DSGVO fallen könnte, da dies Einzelpersonen erheblich beeinträchtigen kann.[25] Ob dies zutrifft, hängt von den besonderen Merkmalen des Falles ab, einschließlich:
    - des eingreifenden Charakters des Profiling-Prozesses, wenn beispielsweise Personen über mehrere Websites, Geräte oder Dienste verfolgt werden;
    - der Erwartungen und Wünsche der betroffenen Personen;
    - der Art und Weise der Werbeanzeige und
    - der Ausnutzung von Schwachstellen der betroffenen Personen, an die sich die Anzeige richtet. [26]

    Das Ausmaß der Betroffenheit von Nutzer*innen wird umso bedeutsamer, wenn nicht nur Werbung, sondern auch Inhalte von Webseiten und Apps persönlich gestaltet sind. Es kann sehr intrusiv und diskriminierend sein, wenn Personen aufgrund ihres Profils bestimmte Jobangebote nicht angezeigt werden und es hat schwerwiegende Auswirkungen auf eine*n Nutzer*in, wenn die angezeigten Inhalte unbemerkt auf sein Profil abgestimmt werden, z. B. auf seine politischen Ansichten. Dies kann den/die Nutzer*in an einer ausgewogenen Information über politische oder andere gesellschaftliche Diskurse hindern. In manchen Fällen kann dieses System eine „Inhaltsblase“ erzeugen, die unser gemeinsames Verständnis von Ereignissen bedroht, das die Grundlage für eine funktionierende Demokratie ist.

38. Ungeachtet des spezifischen rechtlichen Rahmens für automatisierte Entscheidungen stellen diese Vorgänge eine Verarbeitung personenbezogener Daten dar und unterliegen als solche den allgemeinen Transparenzpflichten des jeweiligen Verantwortlichen. Außerdem sollten die Nutzer*innen die Möglichkeit haben, zu entscheiden, ob ein Profiling stattfinden soll oder nicht.

Fehlende Rechtmäßigkeit

39. Eine zentrale Anforderung der meisten Datenschutzregelungen ist, dass die Verarbeitung personenbezogener Daten eine Rechtsgrundlage oder Rechtfertigung haben muss. Eine zusätzliche Rechtfertigung ist oft für die Verarbeitung sensibler oder besonderer Kategorien personenbezogener Daten erforderlich. Dies gilt für jeden einzelnen Akteur im Ökosystem, der personenbezogene Daten als Verantwortlicher verarbeitet.

40. Die verschiedenen Akteure im Ökosystem der digitalen Werbung scheinen sich auf eine Reihe von Rechtsgrundlagen für die Verarbeitung ihrer personenbezogenen Daten zu stützen. Es ist jedoch oft nicht klar, auf welche Rechtsgrundlage für welchen Verarbeitungsvorgang zurückgegriffen wird und wenn ja, ob der rechtliche Standard erfüllt ist.

41. Das berechtigte Interesse kann in einer Reihe von Rechtsrahmen eine Grundlage für die Verarbeitung personenbezogener Daten sein. Dazu gehört jedoch auch eine Interessenabwägung zwischen den berechtigten Interessen des Verantwortlichen und den Datenschutzinteressen der betroffenen Person. Im Zusammenhang mit digitaler Werbung stellt sich die Frage nach der berechtigten Erwartung der Menschen, insbesondere bei der Profiling-bezogenen Verarbeitung personenbezogener Daten. Untersuchungen zeigen, dass Menschen

25 Arbeitsgruppe zu Artikel 29, WP251rev.01 „Leitlinien zur automatisierten Einzelentscheidung und zum Profiling für die Zwecke der Verordnung (EU) 2016/679, zuletzt überarbeitet am 6. Februar 2018, bestätigt durch den Europäischen Datenschutzausschuss am 25. Mai 2018; http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053, Seite 22.

26 Arbeitsgruppe zu Artikel 29, WP251rev.01 „Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679“, zuletzt überarbeitet am 6. Februar 2018, http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053, Seite 24 der deutschen Fassung.

nicht verfolgt und überwacht werden wollen.[27] So fand eine Studie des Think-Tanks Doteveryone aus dem Jahr 2018 heraus, dass 91 % der Befragten es für wichtig halten, selbst zu entscheiden, wie viele Daten sie mit Unternehmen teilen,[28] während eine 2019 durchgeführte Eurobarometer-Umfrage der Europäischen Kommission ergab, dass Verbraucher, die keine Kontrolle über ihre Daten haben, generell besorgt darüber sind, keine vollständige Kontrolle zu haben.[29]

Rückschlüsse, die aus den gesammelten Daten gezogen werden, können sowohl aufgrund der Sensibilität als auch aufgrund des Umfangs sehr einschneidend sein. Die Mehrheit der Akteure im digitalen Werbe-Ökosystem hat keine direkte Beziehung zu Einzelpersonen. Unter Berücksichtigung des schwerwiegenden Eingriffs in grundlegende Datenschutzrechte ist es fraglich, ob die legitimen wirtschaftlichen Interessen der Akteure des Werbeökosystems überwiegen können.

42. Ein Vertrag kann in einigen Datenschutzkonzepten eine weitere Grundlage für die Verarbeitung sein, wenn eine Person mit einer Plattform einen Vertrag abschließt, z. B. im Rahmen allgemeiner Geschäftsbedingungen. In den meisten Fällen ist das Tracking von Nutzer*innen jedoch nicht erforderlich, um den vertragsgegenständlichen Dienst zu erbringen. Es stellt sich die Frage, ob es angemessen sein kann, dass ein Dienst von der Verwendung der Daten von Verbraucher*innen für die Profilerstellung und gezielte Werbung abhängig gemacht wird.

43. Die Einwilligung des Nutzers oder der Nutzerin könnte eine weitere mögliche Rechtsgrundlage für die Verarbeitung von Daten im Ökosystem sein. Die Einwilligung sollte jedoch frei, spezifisch, in Kenntnis der Sachlage und unzweideutig erteilt werden. Durch die Einwilligung erhalten die betroffenen Personen die Kontrolle über das Ausmaß, in dem ihre personenbezogenen Daten verarbeitet werden.

    Allerdings wird die Einwilligung in die Nutzung personenbezogener Daten für digitale Werbung und Profiling, sofern sie überhaupt eingeholt wird, häufig zur Bedingung für den Zugriff auf eine Webseite oder einen Dienst oder die Nutzung einer App gemacht. Im Gegensatz dazu würde eine freiwillig erteilte Einwilligung voraussetzen, dass eine echte Wahlmöglichkeit besteht, den Dienst mit oder ohne die entsprechende Datenverarbeitung zu nutzen. Es stellt sich auch die Frage des Nudging und der Gestaltung von Einwilligungsmechanismen.[30] Die Einwilligung erfordert eine eindeutige, bewusste Handlung der betroffenen Person. So ist das weitere Surfen eines Nutzers odereiner Nutzerin auf einer Webseite niemals gleichbedeutend mit einer Einwilligung dieses Nutzers bzw. dieser Nutzerin. Gleiches gilt für das reine Weglassen von Einstellungen, bei denen die Weitergabe der Daten standardmäßig eingestellt ist. Darüber hinaus dürfen Allgemeine Geschäftsbedingungen nicht als Methode zur Erlangung einer Einwilligung verwendet werden.

    Ein weiteres potenzielles Risiko in diesem Ökosystem sind Einstellungen, bei denen Nutzer*innen aufgefordert werden, ihre Zustimmung für eine große Bandbreite an Aktionen zu geben (globale Zustimmung). Einzelpersonen werden gebeten, der Verarbeitung ihrer personenbezogenen Daten durch mehrere Parteien für mehrere Zwecke gebündelt zuzustimmen, im Gegensatz zu einer spezifischen Zustimmung. Es ist fraglich, ob eine solche Einwilligung den Zweck erfüllen kann, betroffenen Personen die Kontrolle über ihre personenbezogenen Daten zu geben. Die Einwilligung sollte detailliert sein und den Nutzer*innen separate Optionen für separate Zwecke

27 Siehe auch: UK Competition and Markets Authority, Online platforms and digital advertising Market study interim report, Appendix G: Summary of research on consumers' attitudes and behaviour (2019), https://assets.publishing.service.gov.uk/media/5df9ed39e5274a08dbcdfe0f/Appendix_G_digital_markets_study.pdf.

28 https://www.doteveryone.org.uk/wp-content/uploads/2018/06/People-Power-and-Technology-Doteveryone-Digital- Attitudes-Report-2018.compressed.pdf.

29 Europäische Kommission, Spezial-Eurobarometer 487a: die Datenschutzgrundverordnung, 2019.

30 Siehe hierzudie Fragen des Forbrukerrådet (Norwegischer Verbraucherrat), Deceived by design, How tech companies use dark patterns to discourage us from exercising our rights to privacy, 27. Juni 2018, https://www.forbrukerradet.no/undersokelse/no-undersokelsekategori/deceived-by-design/.

bieten, um den Nutzer*innen eine Kontrolle zu ermöglichen. Die Kontrolle wird zudem dadurch untergraben, dass der Widerruf einer erteilten Einwilligung extrem erschwert wird.

Unter Bezugnahme auf die oben hervorgehobenen Probleme hinsichtlich der Transparenz ist die Bereitstellung ausreichender Informationen, die es den Nutzer*innen ermöglichen, ihre Entscheidung zur Einwilligung in Kenntnis der Sachlage und in Kenntnis dessen zu treffen, was genau sie den verschiedenen Verantwortlichen im Ökosystem gestatten, eine weitere Herausforderung, die von den relevanten Akteuren nur schwer umzusetzen ist. Damit eine Einwilligung in Kenntnis der Sachlage erfolgen kann, muss der/die Nutzer*in in der Lage sein, alle verarbeitenden Parteien und die Art der Verarbeitung, die jede von ihnen durchführt, zu identifizieren.

44. Unabhängig von der Rechtsgrundlage sind alle Verantwortlichen und Auftragsverarbeiter in vielen Gesetzgebungen an die Grundsätze von „Privacy by Design“ und/oder „Privacy by Default“ gebunden, was bedeutet, dass datenschutzfreundliche technische Designs und Einstellungen von Anfang an zu implementieren sind. Wenn wir das Ökosystem der Werbung betrachten, können wir nicht viele ernsthafte Bemühungen erkennen, Technologien zu entwickeln, die diese Verpflichtungen erfüllen.

    Das Ökosystem der digitalen Werbung muss die Datenschutzverpflichtungen in Bezug auf die Integrität und Vertraulichkeit der Daten einhalten. Es wurden Bedenken geäußert, dass das Real-Time-Bidding-System in der digitalen Werbung die unbefugte und potenziell unbegrenzte Weitergabe und Verarbeitung personenbezogener Daten beinhaltet. [31]

Erosion der Zweckbindung

45. Personenbezogene Daten sollten für einen bestimmten, eindeutigen und rechtmäßigen Zweck erhoben und nicht in einer Weise weiterverarbeitet werden, die mit diesem Zweck unvereinbar ist. Die Beurteilung der Vereinbarkeit des Zwecks der Verarbeitung erfordert die Berücksichtigung des Kontexts, in dem die Daten erhoben wurden, und der angemessenen Erwartungen der betroffenen Person hinsichtlich der weiteren Verwendung sowie der Art der Daten und der Auswirkungen auf die betroffene Person. Sie sollte gegebenenfalls auch die Art der Beziehung zwischen dem für die Verarbeitung Verantwortlichen und der betroffenen Person berücksichtigen.

46. Der Europäische Datenschutzbeauftragte hat in seiner Stellungnahme zur Online-Manipulation[32] die Bedeutung der Zweckgebundenheit im Zusammenhang mit dem Profiling erneut hervorgehoben und Folgendes festgestellt: „*Das Problem bei der Verwendung von Daten aus Profilen für verschiedene Zwecke durch Algorithmen besteht darin, dass die Daten aus ihrem ursprünglichen Kontext herausgerissen werden. Die Umnutzung von Daten kann die informationelle Selbstbestimmung einer Person gefährden, die Kontrolle der Betroffenen über ihre Daten weiter einschränken und damit das Vertrauen in digitale Umgebungen und Dienste beeinträchtigen. Daher kommt der Zweckbindung als Grundsatz des Datenschutzrechts eine so entscheidende Bedeutung zu.*“ [33] Zudem führt er aus: „*Bei der Datenanalyse handelt es sich um Methoden und Nutzungsmuster, die weder die erhebende Stelle noch die betroffene Person zum Zeitpunkt der Datenerhebung berücksichtigt hat oder sich vorstellen konnte. Die algorithmische Verarbeitung personenbezogener Daten eröffnet Möglichkeiten zur Generierung neuer Daten. Wenn eine betroffene Person einige vertrauliche Daten teilt, ist es oft möglich, dass diese Daten*

31 Siehe Beschwerden bei irischen, französischen und britischen Datenschutzbehörden https://fixad.tech/september2018/. Die Frage der Sicherheit wurde auch bei einem kürzlichen Fact-Finding-Forum des britischen ICO angesprochen https://ico.org.uk/about-the-ico/research-and-reports/adtech-fact-finding-forum.

32 Europäischer Datenschutzbeauftragter (EDSB), Stellungnahme zu Online-Manipulation und personenbezogenen Daten, Stellungnahme 3/2018, https://edps.europa.eu/sites/default/files/publication/18-03-19_opinion_online_manipulation_de.pdf.

33 Europäischer Datenschutzbeauftragter (EDSB), Stellungnahme zu Online-Manipulation und personenbezogenen Daten, Stellungnahme 3/2018, S. 19; https://edps.europa.eu/sites/default/files/publication/18-03-19_opinion_online_manipulation_de.pdf.

zusammengeführt werden, wodurch eine zweite und sogar dritte Generation von Daten über die Person entsteht."[34] Die gleiche Schlussfolgerung zieht Wolfie Christl, der feststellt: „Gleichzeitig werden *Informationen über das Verhalten, die sozialen Beziehungen und die privatesten Momente von Menschen zunehmend in Kontexten oder für Zwecke verwendet, die völlig anders sind als jene, für die sie aufgezeichnet wurden."* [35]

47. Im Web-Tracking-Ökosystem werden die gesammelten Daten nicht nur zum Zweck zielgerichteter Werbung und Nachrichten verwendet, sondern auch, um eine redaktionelle Personalisierung der Inhalte vorzunehmen, die den betroffenen Personen ohne das Wissen der Teilnehmer bereitgestellt werden. Veröffentlichende zeigen unterschiedliche Inhalte, sei es unterschiedliche Werbung, unterschiedliche Überschriften für einen Artikel oder ein anderes Design usw., und verfolgen sorgfältig das Online-Verhalten der Nutzer*innen, um herauszufinden, welcher Inhalt beim Publikum besser ankommt.[36] Dies zeigt, dass einmal gesammelte oder erfasste Daten im System für alle möglichen Zwecke verwendet werden können, ohne dass die Vorschrift der Zweckbindung eingehalten wird.

Auswirkungen auf die Rechtsausübung

48. Aufgrund der Komplexität und Undurchsichtigkeit des derzeitigen Systems ist es für Nutzer*innen nahezu unmöglich, ihre Datenschutzrechte in Bezug auf ihre persönlichen Daten wahrzunehmen, die im Werbe-Ökosystem gespeichert und verarbeitet werden. In vielen Fällen ist dem/der Nutzer*in nicht einmal bewusst, dass und von wem seine persönlichen Daten gesammelt werden, und er hat definitiv keine ausreichenden Informationen darüber, an wen diese Informationen weitergegeben werden. Dies macht es bereits unmöglich, die Unternehmen zu identifizieren, bei denen er den Zugriff auf seine Daten oder andere Rechte geltend machen müsste. Sollte der/die Nutzer*in dazu in der Lage sein, ist die Frage nach den technischen Mitteln, mit denen der/die Nutzer*in seine Identität nachweisen und seine Rechte ausüben kann, noch offen, insbesondere bei den Verantwortlichen, die „pseudonyme" Kennungen verwenden, die nicht trivial mit dem/der Nutzer*in verbunden sind.

Andere gefährdete grundlegende Freiheiten und Rechte

49. Datenschutzrecht und Anforderungen an den Schutz der Privatsphäre sind Grundrechte; sie sind auch Ermächtigungssrechte, die als Voraussetzung für die Ausübung anderer Grundrechte dienen. Wenn die Rechte auf Privatsphäre und Datenschutz nicht respektiert werden, hat dies Auswirkungen auf eine Reihe von gesellschaftlichen und politischen sowie sozialen, wirtschaftlichen und kulturellen Rechten.

50. Die Hohe Kommissarin der Vereinten Nationen für Menschenrechte hat bekräftigt, dass Staaten verpflichtet sind, die Regulierungshoheit über private Unternehmen auszuüben, um sicherzustellen, dass der Schutz der Menschenrechte auch für Menschen gilt, deren Privatsphäre durch die Unternehmen beeinträchtigt wird, die deren personenbezogene Daten erzeugen, sammeln und verwenden.[37] Staaten sind außerdem verpflichtet, *„die Auswirkungen auf die Menschenrechte durch [...] Macht- und Informationsasymmetrien"* zu mildern, die zwischen Menschen und privaten Unternehmen bei der Nutzung der personenbezogenen Daten von Menschen bestehen. Sie hob hervor, dass „*Unternehmen und Staaten kontinuierlich*

34 Europäischer Datenschutzbeauftragter (EDSB), Stellungnahme zu Online-Manipulation und personenbezogenen Daten, Stellungnahme 3/2018, S. 18; https://edps.europa.eu/sites/default/files/publication/18-03-19_opinion_online_manipulation_de.pdf

35 Wolfie Christl, Corporate Surveillance in Everyday Life, Cracked Labs, June 2017, http://crackedlabs.org/en/corporate- surveillance.

36 Wolfie Christl, Corporate Surveillance in Everyday Life, Cracked Labs, June 2017, http://crackedlabs.org/en/corporate- surveillance, para 7.7 p. 78.

37 Hohe Kommissarin der Vereinten Nationen für Menschenrechte, Recht auf Privatsphäre im digitalen Zeitalter, 3. August 2018, A/HRC/39/29, https://documents-dds-ny.un.org/doc/UNDOC/GEN/G18/239/58/PDF/G1823958.pdf?OpenElement (abgerufen am 27. März 2019).

personenbezogene Daten aus verschiedenen Quellen und Datenbanken austauschen und verknüpfen, wobei Datenbroker eine Schlüsselposition einnehmen. Infolgedessen befinden sich Einzelpersonen in einer Position der Machtlosigkeit, da es fast unmöglich scheint, den Überblick darüber zu behalten, wer welche Art von Informationen über sie besitzt, geschweige denn, die vielen Wege zu kontrollieren, auf denen diese Informationen verwendet werden können."[38]

51. Wenn Menschen sich Sorgen darüber machen, wie ihre Daten von privaten Unternehmen oder Behörden in einem auf Tracking und Profiling basierenden Ökosystem verwendet und missbraucht werden könnten, zensieren sie möglicherweise ihre Worte, Gedanken und Handlungen selbst. Dies schränkt ihre Fähigkeit ein, neue Informationen zu suchen, Ideen zu formulieren, Widerspruch zu äußern und sich zu organisieren, um einen sozialen Wandel zu bewirken. Das wiederum kann große Auswirkungen auf die Rechte des Einzelnen auf freie Meinungsäußerung (Artikel 19 der Allgemeinen Erklärung der Menschenrechte (AEMR)), Vereinigungsfreiheit (Artikel 19 AEMR) und das Recht auf politische Beteiligung (Artikel 21 AEMR) sowie auf Gleichheit vor dem Gesetz (Artikel 7 AEMR) haben.

52. Das Recht auf freie Meinungsäußerung und Informationsfreiheit beinhaltet die Freiheit, Meinungen ungehindert zu vertreten und Informationen und Ideen über alle Medien und ohne Rücksicht auf Grenzen zu suchen, zu empfangen und zu verbreiten. Diese Freiheit ist dort eingeschränkt, wo Informationen auf der Grundlage von hochgradig detaillierten Profilen gefiltert werden, die auf Faktoren wie dem bisherigen Verhalten (z. B. Browserverlauf, gelikte Seiten, gelesene Artikel), abgeleiteten Annahmen und anderen Daten aus einer Vielzahl von Quellen basieren. Menschen haben den Nachteil, dass sie entsprechend der Kategorisierung ihrer Daten gezielt mit Informationen und Nachrichten versorgt werden.

53. Die Daten und das Ökosystem können von jedem angezapft werden, der über ausreichende Ressourcen verfügt, und von allen Arten von Akteuren genutzt werden, unabhängig davon, was sie verkaufen wollen.[39] Jede Teilnahme am System birgt die damit verbundenen Risiken, wie z. B. die Möglichkeit, Einzelpersonen anzusprechen, wenn sie für eine strategische Beeinflussung anfällig sind,[40] oder auf eine Weise, die bestimmte Gruppen diskriminiert. Letzteres könnte der Versuch sein, Antidiskriminierungsgesetze [41] und den besonderen Schutz durch Datenschutzgesetze zu umgehen, indem Micro-Targeting als Ersatz verwendet wird, um die explizite Angabe von Rasse, politischer Meinung, Behinderung, Religion oder anderen Kategorien auf verbotene Weise zu umgehen.

54. Auch der Europäische Datenschutzbeauftragte (EDSB) hat seine Besorgnis über diese Branche geäußert, insbesondere im Hinblick auf die unzähligen Möglichkeiten, mit denen Datenanalysemethoden verwendet werden können, um Daten zusammenzuführen oder andere Daten über eine betroffene Person abzuleiten, zu erschließen oder vorherzusagen: *„Unternehmen, die im Verkauf digitaler Werbeflächen tätig sind, profitieren von der Platzierung zielgerichteter Inhalte ungeachtet aller ethischen Überlegungen: Es wird kein Unterschied zwischen einem guten oder schlechten Klick von einer demografischen Zielgruppe gemacht. Dieses Micro-Targeting mag auf einige Personen kaum Auswirkungen haben, aber die*

38 Hohe Kommissarin der Vereinten Nationen für Menschenrechte, Recht auf Privatsphäre im digitalen Zeitalter, 3. August 2018, A/HRC/39/29, https://documents-dds-ny.un.org/doc/UNDOC/GEN/G18/239/58/PDF/G1823958.pdf?OpenElement (abgerufen am 27. März 2019).

39 Function creep of the digital advertisement ecosystem: In Ghosh, Dipayan / Scott, Ben, „Digital Deceit - The Technologies behind Precision Propaganda on the Internet, 2018, https://www.newamerica.org/public-interest-technology/policy-papers/digitaldeceit/, wird argumentiert, dass es einen „fundamentalen Fehler" im digitalen Ökosystem gibt, der werbegestützte Plattformen anfällig dafür macht, von schlechten Akteuren aller Art manipuliert zu werden).

40 Beispiel in Nadler, Anthony/Crain, Matthew/Donovan, Joan, „Weaponizing the Digital Influence Machine: The Political Perils of Online Ad Tech", Data & Society (2018), https://datasociety.net/wp- content/uploads/2018/10/DS_Digital_Influence_Machine.pdf; S. *15.*

41 *Siehe z. B.* „Online personalization enables invisible -and illegal –discrimination*",* (https://privacyinternational.org/examples/868/online-personalisation-enables-invisible-and-illegal-discrimination .

Komplexität der Technologie, das geringe Vertrauen und die erklärten Absichten einiger wichtiger Tech-Player deuten auf eine Kultur der Manipulation in der Online-Umgebung hin. Diese Manipulation kann als Ergebnis der von den Marktteilnehmern selbst gewählten Geschäftsstrategien auftreten oder aufgrund der Handlungen von Einzelpersonen und Staaten, die versuchen, Plattformen als Vermittler zu nutzen, um Märkte und den öffentlichen Diskurs zu stören oder zu unterwandern."[42]

55. Viele dieser Bedenken erstrecken sich auf den Kontext des politischen Wahlkampfs und die damit verbundenen Risiken für die Demokratie:

    Wenn politische Kampagnen und Medieninhalte hochgradig individualisiert und auf den einzelnen Rezipienten zugeschnitten sind, werden sie von Medien und anderen Akteuren dem öffentlichen Diskurs entzogen, einer der Garantien der Demokratie (der so genannten 4. Gewalt), da Kampagnen und Botschaften nicht mehr für die gesamte Öffentlichkeit zugänglich sind.

    Wenn politische Botschaften präzise angepasst werden, kann das Risiko für den Herausgeber minimiert werden, dass diese Botschaften angefochten oder in Frage gestellt werden. Negative Reaktionen können noch weiter reduziert werden, indem die Reaktion des Publikums live überwacht und das Targeting entsprechend angepasst wird. Dieser Mechanismus ermöglicht es den Akteuren, sehr extreme Botschaften zu verbreiten, ohne von breiten Backlash-Effekten bedroht zu sein [43].

    Wenn politische Kampagnen und Medieninhalte sehr zielgerichtet sind, werden Personen mit Nachrichten und Argumenten konfrontiert, die sehr ähnlich oder manchmal auch sehr gegensätzlich sind (um Konfrontation für mehr Engagement zu nutzen). Dies beraubt den Einzelnen der Möglichkeit, andere Stimmen und Meinungen zu hören, und kann somit demokratische Prozesse schädigen.

56. Das Tracking-Ökosystem beinhaltet ein hohes Potenzial für die Manipulation des Verhaltens von Personen. Das vertiefte Wissen über einzelne Nutzer*innen, insbesondere über die emotionale Verfassung, kann genutzt werden, um persönliche Vorurteile und Schwächen zu identifizieren und erlaubt es Herausgebern jeder Art, diese auszunutzen, um individuelles Verhalten zu beeinflussen oder sogar zu kontrollieren. Laut Zuboff gibt es bereits einen Markt für Verhaltenskontrolle, der aus denjenigen besteht, die Möglichkeiten zur Verhaltensbeeinflussung verkaufen, und denjenigen, die diese Möglichkeiten kaufen:[44] Der Konzentrationsprozess des Werbemarktes[45]

---

42 Europäischer Datenschutzbeauftragter (EDSB), Stellungnahme zu Online-Manipulation und personenbezogenen Daten, Stellungnahme https://edps.europa.eu/sites/default/files/publication/18-03-19_opinion_online_manipulation_de.pdf.

43 Nadler, Anthony/Crain, Matthew/Donovan, Joan, „Weaponizing the Digital Influence Machine: The Political Perils of OnlineAdTech", Data & Society (2018), https://datasociety.net/wp- content/uploads/2018/10/ DS_Digital_Influence_Machine.pdf; Kapitel 3, S. 31/32.

44 Zuboff, Shoshana, Big Other: surveillance capitalism and the prospects of an information civilization, 4. April 2015, Journal of Information Technology (2015) 30, 70-89; https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2594754&download=yes, S. 85.

45 Eine von Forschern der Universität Princeton im Jahr 2016 durchgeführte Studie ergab, dass Google Analytics, ein Produkt zur Protokollierung von Webseitenbesuchern, das in die Ad-Targeting-Systemen des Unternehmens integriert ist, auf fast 70 Prozent der Webseiten zu finden war. DoubleClick, ein spezielles Ad-Serving-System von Google, wurde auf fast 50 Prozent der Webseiten gefunden. Die fünf am häufigsten verwendeten Tracking-Tools gehören alle zu Google. Zusammenfassend lässt sich sagen, dass Google mehr als 228 Produkte und Dienste von Gmail und Google Alerts bis hin zu Google AdWords Editor und YouTube (https://www.webrankinfo.com/google) anbietet und fast 200 Startups, Online-Unternehmen und Robotersysteme etc. aufgekauft hat. In einem Bericht vom Dezember 2018 deckte Privacy International auf, wie Facebook routinemäßig Nutzer, Nicht-Nutzer und abgemeldete Nutzer außerhalb seiner Plattform über Facebook Business Tools, insbesondere das Facebook SDK, verfolgt. In ähnlicher Weise fand ein Bericht von Digital Content Next heraus, dass „ein großer Teil der Datensammlung von Google stattfindet, während ein Nutzer nicht direkt mit einem seiner Produkte beschäftigt ist". Dies sind nur einige Beispiele für die breite Palette an Tracking-Methoden, die von Unternehmen eingesetzt werden. Durch all die Unternehmen, die sie besitzen und kontrollieren, kennen sie unsere Lebensweise, indem sie unsere persönlichen Informationen verfolgen und abgleichen, und es ist mittlerweile fast unmöglich geworden, online anonym zu bleiben.

hat dieses Manipulationspotenzial einer Handvoll großer Technologieunternehmen zur Verfügung gestellt, deren Nutzer*innenbasis sich über die ganze Welt erstreckt.

57. So manipulierte Facebook im Jahr 2012 den Newsfeed von 1,9 Millionen seiner Nutzer*innen in den USA, um sie zum Wählen zu bewegen. Facebook behauptet, dass sie den Anteil der Wähler*innen innerhalb dieser Gruppe um 3 Prozentpunkte erhöhen konnten.[46] Würden Facebook oder andere soziale Netzwerke eine solche Manipulation hypothetisch nur bei Nutzer*innen eines bestimmten politischen Spektrums anwenden, könnte das einen entscheidenden Einfluss auf den Ausgang von Wahlen haben. Ähnliche Mechanismen könnten auch eingesetzt werden, um Menschen dazu zu bringen, nicht oder auf eine bestimmte Weise zu wählen. Dies ist nur ein Beispiel, das die enormen Einflussmöglichkeiten privater Akteure auf Demokratie und Gesellschaft aufzeigt. Tatsächlich ist nicht bekannt, ob und inwieweit dieser Einfluss bereits in Wahlprozessen genutzt wird.

Empfehlungen

Gesetzgeber

58. Das gesamte Tracking- und Targeting-Ökosystem hat sich offensichtlich trotz klarer Vorschriften in einigen Gesetzen über Ländergrenzen hinweg entwickelt. Das bedeutet, dass sich einige gängige Geschäftspraktiken des Ökosystems als illegal entpuppen könnten, da die Verfassung des Ökosystems nicht die Grundlage für die Regulierung sein kann. Um das Problem anzugehen, sollte der Gesetzgeber anerkennen, dass eine Stärkung der Datenschutzregulierung und der Rechte auf Privatsphäre andere Grundrechte schützt und das Funktionieren der Demokratie sicherstellt. Wo es nicht klar genug ist, muss eine spezifischere, klarere und konkretere Datenschutzregelung eingeführt werden, die keinen Zweifel daran lässt, was zulässig ist und was nicht.

59. Datenschutzgesetze sollten stärker der Tatsache Rechnung tragen, dass es oft nicht einen einzigen Datenverantwortlichen gibt, sondern dass die Datenverarbeitung zunehmend in Ketten von Verantwortlichen oder in Systemen erfolgt, die von vielen Organisationen kontrolliert werden. Es wird immer wichtiger, dass die Regulierung Mechanismen bereitstellt, um die Verantwortung klar zuzuordnen. In diesem Zusammenhang sollte ein größeres Augenmerk auf Szenarien gelegt werden, in denen die Verantwortlichen anderen Verantwortlichen den Zugriff auf die Daten der Endnutzer*innen ermöglichen, indem sie beispielsweise Technologien in ihre Webseiten einbetten. Insbesondere in Fällen gemeinsamer Kontrolle sollten die Verantwortlichen verpflichtet werden, durch verbindliche Vereinbarungen und wirksame Kontrollen sicherzustellen, dass andere Verantwortliche, mit denen sie zusammenarbeiten, rechenschaftspflichtig und zuverlässig sind und die weitere Verarbeitung der Daten rechtmäßig erfolgt.

60. Gesetzgeber sollten berücksichtigen, dass das gesamte Ökosystem von Tracking und Targeting eine hochspezialisierte Industrie ist, deren Hauptziel es ist, möglichst viele personenbezogene Daten zu sammeln, zu verknüpfen, auszuwerten und für die individuelle Beeinflussung des Verhaltens von Menschen zu nutzen. Dies stellt eine Gefahr für die Grundrechte und -freiheiten dar. Daher ist eine effektive Datenschutzgesetzgebung unerlässlich, um jene zukünftig zu gewährleisten.

61. Gesetzgeber sollten den Unternehmen, die Personen tracken, spezifische Transparenzpflichten auferlegen, auch wenn sie keinen direkten Kontakt mit dem/der Nutzer*in haben.

46 Sifry, Micah L., Facebook Wants You to Vote on Tuesday. Here's How It Messed With Your Feed in 2012, MotherJones, Politics, 31 October 2014, https://www.motherjones.com/politics/2014/10/can-voting-facebook-button-improve- voter-turnout/.

62. Angesichts der starken Abhängigkeit und Beziehung zwischen dem Datenschutz und dem Schutz der Privatsphäre in diesem Zusammenhang sollten die Gesetzgeber sicherstellen, dass die Durchsetzung der Rechtsvorschriften zum Tracking den Datenschutzbehörden und nicht anderen Regulierungsbehörden zugewiesen wird. Die Unterhaltung zweier gesonderter Behörden für die Durchsetzung der Vorschriften zum Schutz der Privatsphäre und des Datenschutzes ist eindeutig weniger effizient als die einer einzigen.

Aufsichtsbehörden/Datenschutzbehörden

63. Wo Gesetzgeber die Regelung zur Datenverarbeitung im Ökosystem von Tracking und Targeting nicht spezifizieren, ist es die Aufgabe der Datenschutzbehörden, die abstrakten Regelungen zu interpretieren und mit Nachdruck durchzusetzen. Dazu gehören klare Vorgaben für die Verantwortlichen, was erlaubt ist und was nicht, sowie die Durchsetzung bei mangelnder Einhaltung.

64. Da das System aus einem komplexen Netzwerk von Verantwortlichen auf der ganzen Welt besteht, ist die internationale Zusammenarbeit der Behörden entscheidend, um ein bedeutendes Gegengewicht zur Tracking-Industrie zu bilden.

65. Wie oben dargestellt, betrifft das Tracking-Ökosystem nicht nur die Privatsphäre einzelner Betroffener, sondern hat weitreichende Folgen für die Grundrechte und das öffentliche Interesse. Daher sollten andere Überwachungsgremien wie nationale Wahlkommissionen und Wahlbeobachter, Verbraucherverbände, Beauftragte für Gleichstellung und Antidiskriminierung in ihren speziellen Zuständigkeitsbereichen einbezogen werden.

66. Die Behörden müssen - im Rahmen ihrer rechtlichen Möglichkeiten - den Datenschutz auf die Strukturen als Ganzes anwenden, einschließlich systemischer Beschwerden und kollektiver Rechtsmittel, und dürfen ihre Maßnahmen nicht auf die Beurteilung von Einzelbeschwerden beschränken.

Unternehmen

67. Unternehmen haben in erster Linie die Pflicht, den entsprechenden gesetzlichen Rahmen einzuhalten. Es liegt in ihrer Verantwortung, Geschäftsmodelle zu entwickeln, die in vollem Einklang mit der Datenschutzgesetzgebung stehen und die Persönlichkeitsrechte der Betroffenen sowie alle oben angesprochenen Aspekte respektieren. Es wäre höchst effizient, wenn durch Gruppen oder Verbände der Verantwortlichen und der Auftragsverarbeiter Rahmenstandards geschaffen würden, z. B. als verbindlicher Verhaltenskodex.

68. Wo immer Verbände oder andere Akteure Standards dieser Art entwickeln, sollten sie sich von den zuständigen Datenschutzbehörden oder anderen Sachverständigen beraten lassen, um im Vorfeld sicherzustellen, dass sie der gesetzlichen Verpflichtung entsprechen.

69. Private Unternehmen oder Behörden sollten keine Dienstanbieter*innen nutzen, die keine klaren Informationen über das Tracking von Nutzer*innen und die Verarbeitung von persönlichen Daten der Nutzer*innen anbieten.

70. Wenn Unternehmen neue Geschäftsmodelle und die dazugehörigen technischen Werkzeuge entwickeln, sollten sie von Anfang an alle geltenden Datenschutzgesetze berücksichtigen, insbesondere die Grundsätze Privacy by Default und Privacy by Design.

71. Als erste Schnittstelle der Nutzer*innen zum Internet können Browser eine wichtige Rolle bei der Umsetzung von Maßnahmen zum Schutz von Daten und Privatsphäre spielen. Als solche sind Anbieter*innen von Browsern an das Prinzip des Datenschutzes per Voreinstellung gebunden und sollten Mittel implementieren, mit denen die Nutzer*innen ihre Wahl bezüglich der Annahme von

Cookies oder der weiteren Verarbeitung ihrer Daten zum Ausdruck bringen können, sowie Mittel, mit denen Unternehmen die Nutzer*innen kontaktieren können, um sie auf standardisierte Weise um ihre Zustimmung zu bitten.

72. Wenn die Einwilligung des Nutzers oder der Nutzerin die Rechtsgrundlage für die Verarbeitung von Daten darstellt, müssen Unternehmen sicherstellen, dass diese Einwilligung freiwillig, spezifisch, informiert und eindeutig erteilt wird, indem sie sicherstellen, dass der/die Nutzer*in eine echte Wahl hat, „ja“ oder „nein“ zu sagen.

73. Der Zugriff auf die Inhalte von Webseiten sollte nicht von der Akzeptanz des User-Trackings abhängig gemacht werden.