

Zweckgebundener Widerstand

Wie EU-Gesetze Tracking, Profiling und personalisierte Werbung eindämmen sollen

DSGVO, DSA, DMA, TTPA: Die EU hat ein dichtes Netz aus Regeln gespannt, um Tech-Konzerne in den Griff zu bekommen. Zwischen Einwilligungs-Bannern, Pay-or-okay-Modellen und algorithmischer Werbung zeigt sich: Die US-Giganten rudern wenigstens ein wenig zurück.

Von Holger Bleich

Die Artikel auf den letzten Seiten haben Ihnen vor Augen geführt, wo Datenkraken zugreifen und wie sie dies zu Geld machen. Algorithmen dienen dazu, individualisierte Inhalte inklusive entsprechender Werbung auszuspielen. Längst servieren sie jedem Nutzer sein eigenes soziales Netzwerk, entsprechend den ermittelten Vorlieben und nach den Vorgaben der Aufmerksamkeitsökonomie.

Dabei bleiben nicht nur Datenschutz und Privatsphäre auf der Strecke. Wissenschaft und Politik benennen längst auch systemische Risiken, die Gefahren für Gesellschaft und Demokratie mit sich bringen. Microtargeting etwa bespielt unterschiedliche Zielgruppen mit entgegengesetzten Botschaften, ohne dass diese es mitbekommen. So könnte sich eine Gesellschaft über Werbung in sozialen Netzwerken polarisieren oder in eine bestimmte Richtung lenken lassen.

Von diesen Sorgen getrieben hat die Europäische Union in den vergangenen zehn Jahren eine Menge drakonischer Regelwerke verabschiedet, die vor allem US-Tech-Konzerne in die Schranken weisen sollen. Den Anfang machte die Datenschutz-Grundverordnung (DSGVO) 2016. Im Jahr 2022 folgten der Digital Services Act (DSA) und der Digital Markets Act (DMA). Als jüngster Spross wirkt seit dem 10. Oktober dieses Jahres die Verordnung über die Transparenz und das Targeting politischer Werbung (TTPA).

Nutzertracking

Die DSGVO schreibt vor, dass die Erhebung und Verarbeitung personenbezogener Daten nur gestattet ist, wenn der sogenannte Verantwortliche (also beispielsweise Meta oder Google) eine Rechtsgrundlage dafür vorweisen kann. In Art. 6 DSGVO sind diese Rechtsgrundlagen abschließend definiert. Es kann sich um vertragliche oder gesetzliche Pflichten zur Verarbeitung handeln, aber auch um ein sehr dehnbares „berechtigtes Interesse“, das beispielsweise oft herhalten muss, wenn der Verantwortliche ein rein datengetriebenes Geschäftsmodell verfolgt. Dies muss er aber stets mit den Grundrechten der betroffenen Bürger abwägen, es gilt nicht absolut. Im Fall von Nutzertracking überwiegen diversen Entscheidungen von Aufsichtsbehörden zufolge fast immer die Nutzerinteressen.

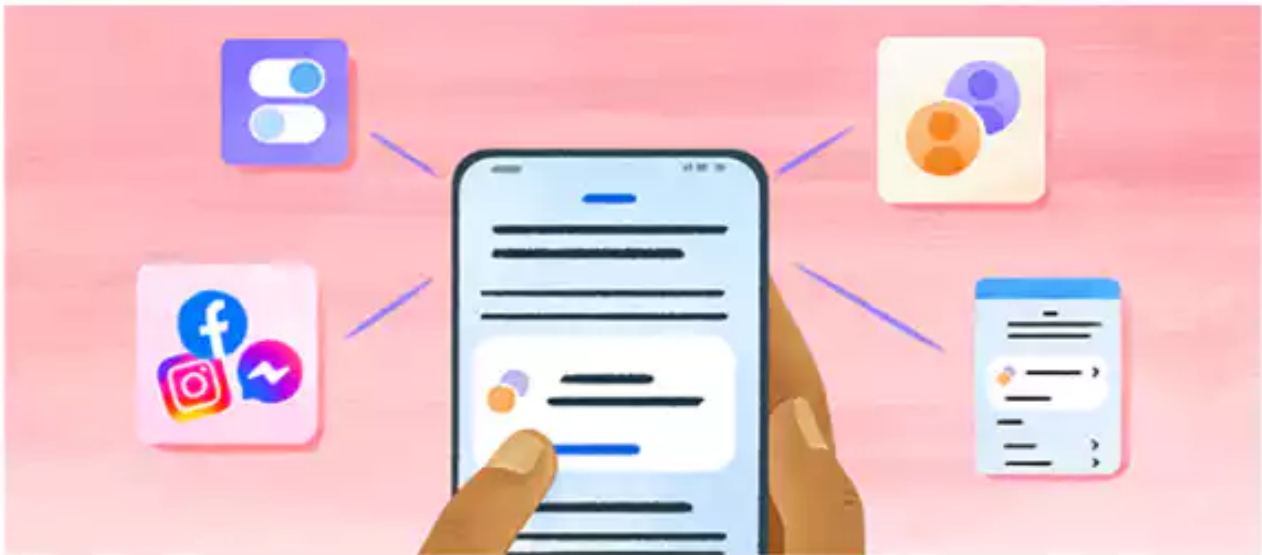
Einzig die freiwillige, informierte, zweckgebundene und widerrufbare Einwilligung gemäß Art. 6(1) DSGVO legitimiert Verantwortliche, Nutzerspuren personalisiert zu verfolgen. Der Meta-Konzern etwa hatte dies lange ignoriert und ein berechtigtes Interesse als Rechtsgrundlage in seinen Nutzungsbedingungen versteckt. Nach einem Bußgeld in Höhe von 390 Millionen Euro und klaren Ansagen des EU-Datenschutzaus-

schusses drehte der Konzern hörbar grummelnd bei und bat die Nutzer von Facebook und Instagram um Einwilligung ins Tracking.

Weil so viele Webdienste personalisiertes Nutzertracking betreiben, um mit personalisierter Werbung Geld verdienen zu können, begegnen EU-Bürgern ständig die nach Art. 6(1) nötigen Einwilligungsbanner. Wenigstens dürfen diese Abfragen gemäß DSGVO nicht manipulativ sein und müssen Informationen liefern. Doch diese werden meist ungelesen weggeklickt. Kritiker monieren deshalb, dass dieser von der DSGVO provozierte „Einwilligungsfetisch“ dem Datenschutz einen Bärendienst erweise. Er nerve Nutzer nur noch, außerdem schaffe er eine Tracking-Legitimation, ohne den vorgesehenen Zweck zu erfüllen. Beobachten Sie Ihr eigenes Surfverhalten. Es könnte etwas dran sein, oder?

Übrigens müssen Webdienste ihren Service auch anbieten, wenn ihre Nutzer nicht ins Tracking einwilligen. Nach langen Diskussionen haben die EU-Datenschutzbehörden gestattet, dass die Anbieter in den Bannern statt Tracking auch eine Geldzahlung zur Kompensation der entgangenen Werbeeinnahmen abhaken lassen können. Dies war der Start sogenannter Pur-Abos oder auch Pay-or-okay-Modelle.

Auch Meta führte im November 2023 ein solches Modell ein, wohl, um mit recht satten Abopreis-Alternativen die Nutzer zur Tracking-Einwilligung zu drängen. Dieses Modell prüfte die EU-Kommission sofort und kam zu dem Schluss, dass Meta gemäß DMA damit seine marktbeherrschende Stellung missbrauche. Es setzte ein 200-Millionen-Euro-Bußgeld, und Meta musste Ende 2024 die Abopreise senken sowie eine kostenfreie Variante mit weniger personalisierter Werbung anbieten. Derzeit untersucht die Kommission, ob sie diese korrigierte Version von Metas Pay-or-okay für rechtskonform hält.



Gesetz über digitale Märkte

Diese Auswirkungen hat das Gesetz über digitale Märkte auf dich

Im Rahmen unserer Umsetzung des Gesetzes über digitale Märkte bieten wir dir verschiedene Optionen, wie du unsere Produkte nutzen kannst. Hier sind einige Beispiele:

Du kannst auswählen, welche Konten sich in derselben Kontenübersicht befinden, um auf bestimmte Funktionen zuzugreifen.	>
Du kannst Meta-Produkte kostenfrei mit Werbung nutzen oder ein Abo für die werbefreie Nutzung abschließen.	>
Du kannst den Messenger mit oder ohne Facebook nutzen.	>
Du kannst deine Facebook-Informationen in anderen Produkten nutzen.	>

Meta weist seine Nutzer an vielen Stellen darauf hin, zu welchen Maßnahmen es von der EU gezwungen wird.

Profiling

Im Fokus der EU-Gesetzgebung steht nicht nur das Tracking, also das Erheben der Daten, sondern auch, wie mit welchen Datenarten Profile erstellt werden. In Art. 4(4) DSGVO hat sie definiert, was sie unter „Profiling“ versteht. Schon das Zusammenführen von Surfverhalten, Standort oder Kaufinteressen zu einem digitalen Profil fällt eindeutig darunter. Scoring-Dienste wie die Schufa können sich dazu auf die DSGVO-Rechtsgrundlage der Vertragserfüllung beziehen. Die Profilbildung zum Ausspielen personalisierter Werbung hingegen bedarf eindeutig der Einwilligung.

Art. 26 DSA verbietet von vornherein, Nutzerprofile für Werbung zu nutzen, wenn diese auf sensiblen Daten nach Art. 9 DSGVO zum Beispiel zu Religion, Gesundheit, Sexualleben oder politischer Meinung beruhen. Etwas unscharf ist der Schutz Minderjähriger im DSA gehalten. Nach Art. 28 DSA dürfen Plattformen Minderjährigen gar keine personalisierte Werbung mehr anzeigen. Dies käme faktisch einem Tracking-Verbot gleich, sobald der Anbieter weiß oder mit vertretbarem Aufwand feststellen kann, dass es sich um minderjährige Nutzer handelt. Weil die EU-Kommission bei Meta und TikTok an dieser Stelle Bedenken hat, ermittelt sie wegen DSA-Verstößen gegen den Schutz von Minderjährigen.

Generell hat die EU mit ihren Verordnungen das Geschäftsmodell der digitalen US-Konzerne massiv angegriffen. Meta etwa kann im europäischen Wirtschaftsraum längst nicht mehr so viel Geld generieren, wie es gerne würde. Werbetreibende dürfen seit Längerem nicht mehr Zielgruppen adressieren, deren Profile auf Generierung oder Auswertung von Art.-9-Daten beruhen, also etwa nach Religion oder politischer Gesinnung.

Und seit dem 10. Oktober ist auch das Geschäft mit politischen Microtargeting-Werbeanzeigen de facto stillgelegt: Die Verordnung über die Transparenz und das Targeting politischer Werbung (TTPA) verbietet nun politisches Targeting ohne ausdrückliche, getrennte Einwilligung. Psychologische Profile wie das OCEAN-Modell sollen fürs Microtargeting untersagt sein. Nutzer sollen in jeder politischen Anzeige prominent angezeigt bekommen, wie sie vom System selektiert wurden.

Diese Regeln waren Meta und Google zuviel: Die beiden Konzerne haben bereits mitgeteilt, dass sie innerhalb der EU künftig gänzlich auf politische Werbeschaltungen verzichten werden. TikTok tut dies schon seit Jahren. Untersuchungen zeigen allerdings, dass der Mutterkonzern ByteDance sowieso umfangreich von Kurzvideos politischer Influencer profitiert, die er auf der Plattform algorithmisch pusht. Die direkten Werbeprovisionen wären wohl sowieso nur Beigabe.

Data Broker

Der Fall der so titulierten „Databroker Files“ hatte Mitte 2024 den Handel mit Tracking-Daten schlaglichtartig beleuchtet. Netzpolitik.org und der Bayerische Rundfunk hatten vom Datenmarktplatz Datatrade einen Satz mit 3,6 Milliarden Standortdaten von einem US-Händler kostenlos als Probe erhalten. Nach ihren Recherchen gehen die Journalisten davon aus, dass diese von einer Vielzahl von Anwendungen stammen, beispielsweise von Apps zur Wettervorhersage, für Dating oder Navigation.

Experten zerbrachen sich in der Folge den Kopf darüber, welche Datenschutzverstöße hier vorliegen könnten. So ist denkbar, dass den Betroffenen die Tragweite ihrer erfolgten Einwilligung nach DSGVO zur Erfassung der Standortdaten nicht klar sein konnte. Eventuell könnte auch gegen das Zweckbindungsgebot der DSGVO verstoßen worden sein – die Nutzer wussten nicht, dass ihre Daten zum Handel für andere Zwecke freigegeben würden.

Festzuhalten bleibt: Der kommerzielle Datenhandel ist ein weitgehend unregulierter Raum, der bisher kaum sanktioniert ist, zumal viele der Daten in den USA landen. In den Vereinigten Staaten gibt es kein einheitliches Bundesgesetz, das Data Broker umfassend ins Visier nimmt. Die Regulierung des Datenhandels variiert stattdessen je nach Bundesstaat. Nur Kalifornien, Vermont, Oregon und Texas haben überhaupt eigene Gesetze erlassen. Aber selbst die in diesen Gesetzen festgeschriebenen Minimalanforderungen erfüllen viele Data Broker nicht, wie eine Untersuchung der Universität von Kalifornien in Irvine zeigt. In dem US-Bundesstaat müssen sich alle Datenhändler registrieren. Bürger können ihre bei den Brokern befindlichen Daten anfordern und löschen lassen – ähnlich wie bei der DSGVO. Die Forscher haben alle 543 registrierten Broker kontaktiert. Mehr als 40 Prozent haben nicht einmal geantwortet.

Hierzulande bleibt Betroffenen immerhin, von ihren Rechten nach Art. 12 bis 23 DSGVO Gebrauch zu machen: Wehren Sie sich, in dem sie die identifizierten Unternehmen nerven. Sie haben das Recht, Auskunft über die von ihnen dort gespeicherten Daten zu verlangen. Außerdem müssen die Firmen Daten berichtigen und/oder löschen, wenn Sie es verlangen. In einer der kommenden Ausgaben von c't berichten wir Ihnen, welche Erfahrungen wir damit gemacht haben. (hob@ct.de)

► **Kommentieren**



Leserbrief schreiben



Artikel als PDF herunterladen



Auf Facebook teilen



Auf X teilen

[Kontakt](#)

[Impressum](#)

[Datenschutzhinweis](#)

[Nutzungsbedingungen](#)

[Mediadaten](#)

[Verträge kündigen](#)



Heftinhalt

Lesezeichen



vorheriger Artikel

nächster Artikel

