



Bild: Ulrike Weis / KI / heise medien

Im Visier der Datensammler

Wie Sie anhand Ihrer digitalen Spuren verfolgt werden

Smartphones, Kundenkarten, Messenger, Fitness-Apps, Webbrowser – jede Interaktion erzeugt **Datenspuren**. Unternehmen und Behörden nutzen diese für Werbung, Prognosen und **Risikobewertungen**. Wir zeigen Ihnen, wer wo welche Informationen über Sie sammelt und **auswertet**, mit welchen **Risiken** das verbunden ist und was Sie tun können.

- [Digitale Spuren und ihre Auswirkungen Seite 54](#)
- [Wie aus Daten Profile werden Seite 60](#)
- [Der Handel mit Daten Seite 66](#)
- [Datenprofile: Die Rechtslage Seite 72](#)

kompakt

- Während Sie Ihr Leben führen, ziehen Sie eine enorme Datenspur hinter sich her, meist ohne es zu merken oder aktiv etwas dazu beizutragen.
- Der Einzelne bekommt in der Regel auch nicht mit, wer welche Daten über ihn sammelt und

verknüpft und was damit geschieht.

- Die Schattendaten können sich negativ auswirken, wenn Sie mehr kaufen, als Sie eigentlich benötigen, oder fälschlicherweise ins Visier polizeilicher Ermittlungen geraten.

Jeder Schritt, jeder Klick und jede Transaktion hinterlässt digitale Spuren. Während wir uns der Überwachungskameras an öffentlichen Plätzen bewusst sind, weil wir sie sehen, bleiben die meisten Datenspuren unsichtbar. Sie entstehen im Hintergrund, oft ohne aktives eigenes Zutun, während wir unser normales Leben führen. Fügt man alle diese Infoschnipsel zusammen, ergibt sich nicht nur ein beunruhigend vollständiges Abbild Ihres Lebens, sondern auch Ihrer Psyche.

Diese Transparenz ist aber nur einseitig: Die Datensammler und -händler wissen alles, geben über sich aber kaum etwas preis. Um dieses Ungleichgewicht zumindest etwas auszugleichen, fügen wir in dieser Artikelstrecke die Puzzlestücke zusammen: An welchen Stellen entstehen digitale Spuren? Wer sammelt sie? Was geschieht mit den Informationen? Und welche Firmen spielen dabei eine Rolle? Außerdem geht es darum, welche Konsequenzen die Schattenprofile für Sie haben.

Der Artikel ab [Seite 60](#) untersucht die technischen Grundlagen der psychologischen Profilbildung auf Basis von Nutzerdaten. Scheinbar harmlose Likes und Postings auf Social-Media-Plattformen ergänzen sich zu psychologischen Profilen, die es Werbetreibenden erlauben, gezielte Botschaften für Produkte oder Politikampagnen zu adressieren. Im Beitrag ab [Seite 66](#) werfen wir einen detaillierten Blick auf den Markt der Datenhändler, damit Sie einen Überblick bekommen, welche Daten da zu welchen Preisen überhaupt gehandelt werden, und auf welche es die Broker besonders abgesehen haben.

Ab der [Seite 72](#) betrachten wir die rechtliche Seite des Themas, ob hiesige Datenschutzgesetze ausreichen, um Bürger vor der kompletten Durchleuchtung und einer Ausnutzung ihrer persönlichen Schwächen zu schützen. Dort zeigen wir Ihnen auch, wie Sie zumindest ein Stück weit einen Überblick über den Datenabfluss bekommen und die Hoheit über Ihre digitale Identität wiedergewinnen.

Die digitale Grundausstattung

Beginnen wir mit dem Naheliegendsten: dem Smartphone. Dieser ständige Begleiter ist zugleich der größte Datensammler. Jede App darauf ist ein potenzieller Spion. Das liegt manchmal in der Natur der Anwendung. Google Maps etwa kann Ihnen keine Live-Wegbeschreibungen geben, ohne zu wissen, wo Sie sich befinden. Die Landkarten-App funkt daher permanent Ihre Position auf wenige Meter genau zu Googles Servern, wo die Routenberechnungen ablaufen.

In vielen Fällen übertragen Apps aber Daten ins Netz, die sie für ihre Aufgabe nicht benötigen. Dabei geht es oft um ihre Refinanzierung mit Werbung. Die Apps enthalten dafür Werbe- und Analytik-Bibliotheken von Drittanbietern, die das Nutzerverhalten aufzeichnen und ins Netz übertragen. Damit wollen die Werbepartner möglichst genaue Interessensprofile der Benutzer gewinnen, um ihnen zielgenaue Werbung einblenden zu können. Der nachfolgende Artikel geht detailliert auf das Thema ein und zeigt, welche psychologischen Modelle dabei zum Einsatz kommen und welche Rückschlüsse diese erlauben.

Soziale Netzwerke spielen eine besondere Rolle. Sie sind wahre Datenschätze. Facebook, Instagram, TikTok und LinkedIn erfassen nicht nur die Posts und Kommentare der Nutzer, sondern auch das Scroll-Verhalten, die Verweildauer bei bestimmten Inhalten, die Likes – mitunter sogar das, was sie in ein Textfeld tippen und dann doch nicht abschicken. Die Plattformen wissen, mit wem die Nutzer interagieren, welche Themen sie emotional bewegen und zu welchen Tageszeiten sie besonders aktiv sind. Für die Datensammler ist nicht nur interessant, was Sie schreiben, sondern auch, wie Sie es formulieren, mit wie vielen Personen Sie inter-

agieren und zu welchen Zeiten das geschieht.

Ein Messenger-Dienst wie WhatsApp kann zwar nicht auf die Ende-zu-Ende-verschlüsselten Inhalte der Nachrichten zugreifen, analysiert aber die Metadaten: Wer kommuniziert wann mit wem? Wie oft? Wie lang sind die Nachrichten? Selbst wenn die Inhalte verschlüsselt sind, verraten diese Metadaten viel über soziale Beziehungen und Verhaltensmuster.

Sowohl auf dem Smartphone als auch per Desktop-Browser sickern massenhaft Daten unbemerkt in verschiedene Kanäle. In vielen Fällen hat Onlinewerbung Tracker im Schlepptau. Werbeunternehmen erkennen Surfer Website-übergreifend wieder und zeichnen jede Mausbewegung, jeden Klick, jeden Tastaturanschlag auf – außer der Nutzer wehrt sich aktiv dagegen.

Einzelne Datenspuren an sich haben vielleicht noch keine hohe Aussagekraft. Aber wenn sie nicht komplett anonymisiert, sondern nur pseudonymisiert werden, lassen sie sich miteinander verknüpfen und ergeben so ein detailliertes Gesamtbild der Persönlichkeit. Insbesondere der Einsatz von KI ermöglicht hier Mustererkennungen, die weitere Rückschlüsse erlauben, weil sich einzelne Daten nicht nur statistisch, sondern kontextbezogen auswerten lassen.

Angesichts dieser Datenfülle mag es wenig beruhigend wirken, dass es der Werbeindustrie nicht darum geht, jedes einzelne Individuum zu durchleuchten. Vielmehr wollen die Werbetreibenden Personen in Gruppen einordnen, damit sie diese mit gezielten Botschaften ansprechen und die Reaktionsrate steigern können.

The screenshot shows a mobile browser interface. The main content is a news article from t-online.de titled "Unwetter auf Urlaubsinseln: 'richtig gefährlich'" with a sub-header "Mallorca und Ibiza". The article features a photo of a car accident. On the right side, there is a sidebar titled "Alle Ressourcen" listing various domains. Below this, a section titled "Auf dieser Seite blockiert" shows statistics: "13 (6 %)" and "Verbundene Domains 2 von 10". At the bottom right, there is a list of news headlines.

Regional Politik Ukraine Sport Wirtschaft & Finanzen Um

t-online. Suchbegriff

Mallorca und Ibiza

Unwetter auf Urlaubsinseln: "richtig gefährlich"

Auf dieser Seite blockiert 13 (6 %) Verbundene Domains 2 von 10 Seit der Installation blockiert 56.097 (9 %)

Mehr Weniger

Frau von Fußballprofi gibt Krebs-Update
Gaspreise steigen durch höhere Netzkosten
Vor Topspiel: Bayern-Star fällt aus
Airbag-Probleme: Großer Rückruf bei Skoda
Staatschef rockt vor Tausenden Fans
TV-Show floppt: Sender reagiert drastisch

Alle Schlagzeilen anzeigen →

Erst wenn man genau hinschaut, wie hier mit einem Werbeblocker, sieht man, wer auf einer Webseite alles mitliest.

The image shows the logo for Kleinanzeigen. It consists of a green square with a white stylized 'K' inside. To the right of the square, the word "Kleinanzeigen" is written in a bold, purple, sans-serif font.

Kleinanzeigen

9 Tracker

23 Berechtigungen

Version 100.65.2 - [andere Versionen anzeigen](#)

Quelle: Google Play

Bericht erstellt am 6. Oktober 2025 09:03

[Auf Google Play anzeigen](#) >

9 Tracker

Wir haben die **Code-Signatur** der folgenden Tracker in der Anwendung gefunden:

Adjust >

analytics

Amazon Advertisement >

Facebook Ads >

advertisement

Google AdMob >

advertisement

Google CrashLytics >

crash reporting

Google Firebase Analytics >

analytics

IAB Open Measurement >

advertisement

identification

Prebid Mobile >

advertisement

PubMatic >

advertisement

Ein Tracker ist eine Software zur Erfassung von Daten über Sie oder Ihre Nutzung.

[Weitere Informationen...](#)

In dieser App sind neun Tracker mit an Bord, außerdem

... fordert sie viele Berechtigungen an, mit denen sie Daten erheben kann.

Die vernetzte Privatsphäre

Viele Menschen haben digitale Helfer in ihr Zuhause geholt – eigentlich ein privater Rückzugsort. Doch manches Gadget überträgt fleißig Daten zu seinem Hersteller. Assistenten wie Alexa, Google Home oder Siri zeichnen Sprachbefehle auf und bei versehentlichen Aktivierungen auch schon mal mehr.

Moderne Haushaltsgeräte mit Internetanbindung, vom Kühlschrank bis zur Waschmaschine, sammeln ebenfalls Nutzungsdaten. Der Saugroboter legt detaillierte Raumpläne der Wohnung an und selbst Stromzähler werden smart. Alle Haushalte in Deutschland sollen bis 2032 digitale Stromzähler erhalten. Manche senden die Verbrauchsdaten an den Stromversorger oder den Netzbetreiber. Einzelne Geräte lassen sich anhand ihres individuellen Verbrauchsprofils genau identifizieren, zum Beispiel der Staubsauger und der Herd, was wiederum sehr detaillierte Rückschlüsse auf Vorlieben und Tagesablauf zulässt.

Smart-TVs beobachten uns beim Fernsehen: Welche Sendungen schauen wir? Wann spulen wir vor? Bei welchen Szenen drücken wir auf Pause? Streamingdienste wie Netflix und Spotify gehen noch weiter: Sie analysieren nicht nur, was wir konsumieren, sondern auch wie. Brechen wir eine Serie nach drei Folgen ab? Überspringen wir bestimmte Songs immer?

Fitness-Gadgets und Gesundheits-Apps sammeln hochsensible Daten: Schritte, Herzfrequenz, Menstruationszyklen, Schlafmuster, zurückgelegte Strecken, verbrannte Kalorien. Smartwatches gehen noch weiter und tracken nahezu ständig körperliche Parameter. Dating-Apps erfassen intimste Präferenzen und Verhaltensmuster in der Partnersuche.

Mobilität: Jede Bewegung zählt

Unsere Bewegungen im Raum hinterlassen ebenfalls einen detaillierten Datenstrom. In Einkaufszentren, Flughäfen und Innenstädten erfassen WLAN-Tracker die MAC-Adressen aller Smartphones. Damit lassen sich Laufwege und Verweildauern analysieren – selbst wenn wir uns nicht in ein Netzwerk einloggen.

Moderne Fahrzeuge sind rollende Computer, die ständig Daten sammeln und zum Hersteller senden. In welchem Ausmaß dies geschieht, untersuchte der ADAC anhand eines Mercedes der B-Klasse, der sich per 'me connect' mit dem Hersteller verbindet. Dabei übertrug das Fahrzeug etwa alle zwei Minuten Daten ans Mercedes-Backend: GPS-Position, Kilometerstand, Verbrauch, Tankfüllung, Reifendruck und Füllstände von Kühlmittel, Wischwasser oder Bremsflüssigkeit. Das Testfahrzeug hat sogar die Anzahl der elektromotorischen Gurtstraffungen gespeichert, was Rückschlüsse auf den Fahrstil ermöglicht.

Manch ein Autofahrer lässt sich freiwillig ein Telematik-Gerät in sein Auto installieren, das Parameter wie Beschleunigung, Bremsverhalten, Geschwindigkeit, Kurvenfahrt und Tageszeit der Fahrt erfasst. Der Deal: Fahrer, die sicher und vorausschauend fahren, erhalten Rabatte auf ihre Versicherungsbeiträge.

Konsum und Handel

Beim Einkaufen hinterlassen Kunden ebenfalls reichhaltige Datenspuren. Online-Shopping-Plattformen wie Amazon oder eBay erfassen nicht nur, was sie kaufen, sondern auch, was sie suchen, was auf ihren Wunschlisten landet und welche Käufe sie im letzten Moment abgebrochen haben. Diese Daten verraten viel über Bedürfnisse, finanzielle Situationen und Lebensumstände.

Der stationäre Handel hat längst aufgeholt. Rabattsysteme wie die von Payback oder Shop-Apps analysieren das Kaufverhalten bis ins Detail: Wann kaufen Kunden was? Welche Marken bevorzugen sie? Wie reagieren sie auf Rabattaktionen? Diese Informationen verdichten die Anbieter zu Profilen und verkaufen sie mitunter auch weiter.

Bild: Martina Bruns / heise medien

Unsichtbare Infrastrukturen

Eine Datenerhebung solchen Ausmaßes wäre ohne eine allgegenwärtige, im Hintergrund arbeitende Infrastruktur nicht möglich. Die Mobilbetriebssysteme zum Beispiel, Android und iOS, funken fleißig nach Hause. Beide Systeme erfassen unter anderem Listen installierter Apps, Geräte-Identifikationsnummern, gescannte WLAN-Netzwerke in der Umgebung zur Standortbestimmung sowie Bluetooth-Kontakte. Beide Betriebssysteme vergeben zudem eindeutige Werbekennzeichner, sogenannte Mobile Advertising IDs, und stellen sie Apps zur Verfügung. Damit machen sie das Gerät über einzelne Apps hinweg erst wiedererkennbar.

Mobilfunkanbieter speichern Verbindungsdaten und können über Funkzellen unseren ungefähren Standort nachverfolgen. Einige Länder, auch europäische, sammeln diese Daten im Rahmen der Vorratsdatenspeicherung systematisch. In Deutschland wird immer wieder über die Einführung der Vorratsdatenspeicherung diskutiert.

Die persönlichen Finanzströme sind ebenso eine sehr reichhaltige Datenquelle, bei der es hierzulande sogar bereits so etwas wie eine Vorratsdatenspeicherung gibt: Finanzdienstleister müssen gemäß dem Geldwäschegesetz Transaktionsdaten über mehrere Jahre auf Vorrat speichern.

An manchen Stellen machen Hardwarehersteller und Dienstebetreiber ihre Nutzer zu – ungefragten und oft unwissenden – Komplizen, die ihnen Daten über Dritte zuspiesen. Bei Facebook etwa kann man sein Smartphoneadressbuch hochladen, um Freunde zu finden. Facebook erhält auf diese Weise die Daten der Kontakte frei Haus.

Amazon plant nach einem Bericht der Washington Post, bei seinen Ring-Türklingeln Gesichtserkennung scharf zu schalten. Das bedeutet, dass eine KI jeden, der sich vor der Klingel befindet, biometrisch erfasst – sei es ein Zusteller oder ein zufälliger Passant.

Mancher Nutzen ...

Die Aufzählung ist noch lange nicht vollständig, sollte aber klar machen: Es gibt kaum einen Bereich des Lebens – auch des analogen – in dem nicht massenhaft Daten erhoben werden. Jetzt mag man einwenden: Wo liegt eigentlich das Problem? Man kriegt ja von der Datenerhebung meist nichts mit, und wenn, dann profitiert man oft sogar davon – bei den Kundenkarten oder den Telematik-Versicherungen zum Beispiel spart man bares Geld.

Es kommt halt immer darauf an, was mit den Daten geschieht. Tatsächlich lassen sich viele nützliche Dinge mit den eingesammelten Informationen anfangen. Die Apple Watch hat nachweislich Menschen gerettet. Die EKG-Funktion der Uhr erkennt Vorhofflimmern und sendet automatisch Notrufe.

Manche Daten kommen nicht nur dem Einzelnen zugute, sondern der Allgemeinheit. Zum Beispiel bei Google Maps: Der Dienst plant mit den Standort- und Fahrtinformationen nicht nur individuelle Routen. Er verdichtet die von allen Nutzern einströmenden Daten auch zu einem Gesamtbild. So kann die Navigations-App erstaunlich verlässlich angeben, auf welchen Straßenabschnitten der Verkehr fließt und wo er stockt – und diese Informationen für die Routen-Berechnung verwenden.

... viel Schmu ...

Problematisch wird es, wenn der Einzelne nicht sieht, welche Daten andere über ihn gewinnen und diese gegen seine Interessen verwenden. Das ist in der Onlinewerbebranche oft der Fall. Während zu analogen Zeiten beim Einkauf im Geschäft klar ist, wer welche Information erhält, werden im digitalen Raum umfassende Verhaltensprofile angelegt – oft ohne explizite Zustimmung oder auch nur Kenntnis der Betroffenen. Es entsteht eine informelle Asymmetrie bei der Kaufvertragsanbahnung.

Dutzende Datenhändler und Werbeplattformen tauschen diese Informationen untereinander aus, sodass ein undurchschaubares Netzwerk entsteht. Selbst technisch versierte Menschen verlieren den Überblick darüber, wer welche Daten über sie besitzt, geschweige denn, wie diese kombiniert und interpretiert werden. Der Artikel ab Seite 66 beleuchtet den Datenhandel im Netz ausführlich.

Online-Werbeunternehmen schalten auf der Grundlage solcher Profile passgenaue, auf individuelle Interessen abgestimmte Werbung (siehe [Seite 60](#)). Eine andere Masche, das Retargeting, übt permanenten Werbedruck aus, um den Verbraucher zum Kauf zu bewegen. Hat er sich einmal für ein Produkt interessiert,

verfolgt ihn die Werbung dafür förmlich durchs Netz; egal wo er sich befindet, sie poppt immer und immer wieder auf.

Beim Dynamic Pricing analysieren Algorithmen in Echtzeit, welchen Preis ein Kunde vermutlich zu zahlen bereit ist, und passen das Angebot entsprechend an. Ein klassisches Beispiel sind Flugbuchungsportale: Wer wiederholt nach derselben Strecke sucht, bekommt tendenziell höhere Preise angezeigt, weil der Algorithmus daraus Kaufinteresse und Dringlichkeit ableitet. Online-Shops werten zudem Gerätetyp und Standort aus. Für dasselbe Produkt zahlen MacBook-Nutzer nachweislich häufig mehr als Windows-User, weil Online-Shops sie als kaufkräftiger einstufen.

... und handfeste Probleme

Wenn man in der Vergangenheit Probleme hatte, Kredite abzubezahlen, und Mahnbescheide erhalten hat, kann das gravierende Folgen haben: Banken verweigern neue Kredite oder Girokonten, Vermieter lehnen Mietinteressenten ab, Mobilfunkanbieter bieten nur Prepaid-Tarife an und Online-Shops verweigern den Kauf auf Rechnung.

Die Informationen, die solchen gravierenden Entscheidungen zugrunde liegen, stammen von darauf spezialisierten Wirtschaftsauskunfteien wie der Schufa. Diese sammeln Daten über Verbraucher und Firmen, um deren Bonität zu ermitteln. Banken, Handelsunternehmen und Dienstleister greifen auf die Datenbanken der Schufa zu.

Die Schufa berechnet einen Score, der Auskunft über die Bonität gibt. Nicht bediente Kredite, Mahnbescheide, Privatinsolvenzen oder Haftbefehle zur Erzwingung der Vermögensauskunft können sich negativ auf den Score auswirken. Ein schlechter Score wiederum kann Schwierigkeiten bei neuen Geldgeschäften mit sich bringen.

Gefährliche Daten

Interne Dokumente, Whistleblower-Enthüllungen und wissenschaftliche Studien belegen, dass Social-Media-Plattformen bewusst Schaden in Kauf nehmen, um Engagement und Werbeeinnahmen zu maximieren. So können die Algorithmen der sozialen Netzwerke Kinder und psychisch labile Personen mit großer Präzision identifizieren. Diesen vulnerablen Gruppen haben die Netze in der Vergangenheit immer wieder gezielt Inhalte ausgespielt, die deren emotionale Abhängigkeit verstärken.

2018 kam der Cambridge-Analytica-Skandal ans Licht, der Super-GAU der illegitimen Nutzung von persönlichen Daten im Netz. Das britische Datenanalyseunternehmen Cambridge Analytica hatte Daten von bis zu 87 Millionen Facebook-Nutzern gesammelt. Eine scheinbar harmlose Persönlichkeitstest-App griff nicht nur Daten der App-Nutzer ab, sondern auch die ihrer Facebook-Freunde – ohne deren Wissen. Cambridge Analytica nutzte diese Daten, um gezielt politische Werbung zu schalten, unter anderem für die Trump-Kampagne 2016 und die Brexit-Kampagne.

Auch Kriminelle aller Art mögen Nutzerdaten. Sie missbrauchen diese auf verschiedene Weise, zum Beispiel für Stalking, Phishing, den Enkeltrick oder Identitätsdiebstahl. Daher ist es besonders ärgerlich, wenn eine große Plattform, etwa durch fehlerhafte Administration oder einen Angriff, die Daten ihrer Nutzer verliert.

2021 machte ein besonders großes Datenleck bei Facebook Schlagzeilen, durch das persönliche Daten von über 530 Millionen Facebook-Nutzern weltweit veröffentlicht wurden. Darunter befanden sich rund 6 Millionen Menschen aus Deutschland. Die offengelegten Daten umfassten unter anderem Telefonnummern, Namen, Geburtsdaten, teilweise auch E-Mail-Adressen, Wohnorte sowie Angaben zum Beziehungsstatus. Der Fall wird derzeit vor dem Oberlandesgericht in Hamburg verhandelt, wo Betroffene in einer Sammelklage der Verbraucherzentrale Schadensersatz erstreiten wollen.

Der CCC konnte aus schlecht gesicherten Bewegungsdaten von VW-Fahrzeugen darauf schließen, welche Fahrer beim Bundesnachrichtendienst arbeiten.

Ein Tochterunternehmen des Volkswagen-Konzerns hat teils extrem detaillierte Bewegungsdaten von 800.000 Elektroautos schlecht gesichert in der Amazon-Cloud abgelegt, zeigte der Chaos Computer Club. Einige Datensätze konnten die Experten mit persönlichen Profilen von Fahrzeughaltern verknüpfen. Teils hätten die detaillierten Bewegungsdaten gar mit Adressen und Handynummern zusammengeführt werden können.

Falsche Verdächtigungen

Sehr unangenehme Folgen kann es haben, wenn man aufgrund fehlerhafter oder unvollständiger Daten Probleme mit den Behörden bekommt. So hat die Detroiter Polizei Anfang 2020 Robert Williams verhaftet. Eine Gesichtserkennungssoftware hatte den schwarzen Mann aus Detroit fälschlicherweise mit einem Dieb verwechselt, den die Überwachungskamera eines Uhrengeschäfts gefilmt hatte.

Nach 30 Stunden hat die Polizei den Fehler bemerkt und Williams wieder freigelassen. Laut der Bürgerrechtsorganisation American Civil Liberties Union handelte es sich allerdings um ein systematisches Problem, weil die bei der Polizei eingesetzte Gesichtserkennungssoftware dunkelhäutige Menschen nicht gut voneinander unterscheiden kann.

Daten spielen auch eine wesentliche Rolle bei der US-amerikanischen Softwareplattform Palantir, die für polizeiliche und militärische Zwecke entwickelt wurde. Mehrere Bundesländer setzen Palantir bereits ein, andere planen die Anschaffung des Systems, mit denen sich die Polizeibehörden mehr Effizienz bei der

Verbrechensbekämpfung versprechen.

Die Software verknüpft Informationen aus diversen, voneinander getrennten Datenbeständen und ermöglicht es, diese systematisch nach Zusammenhängen zu durchforsten. Auf diese Weise landen Millionen von Informationshäppchen über Menschen aus verschiedenen polizeilichen Datenbanken im System, die dadurch häufiger zum Ziel algorithmischer Abfragen werden. Kritiker wie die Gesellschaft für Freiheitsrechte bemängeln die „enorme Streubreite“ der Software, das „hohe Risiko falscher Verdächtigungen“ sowie die große Intransparenz bei deren Einsatz.

Staatliche Repression

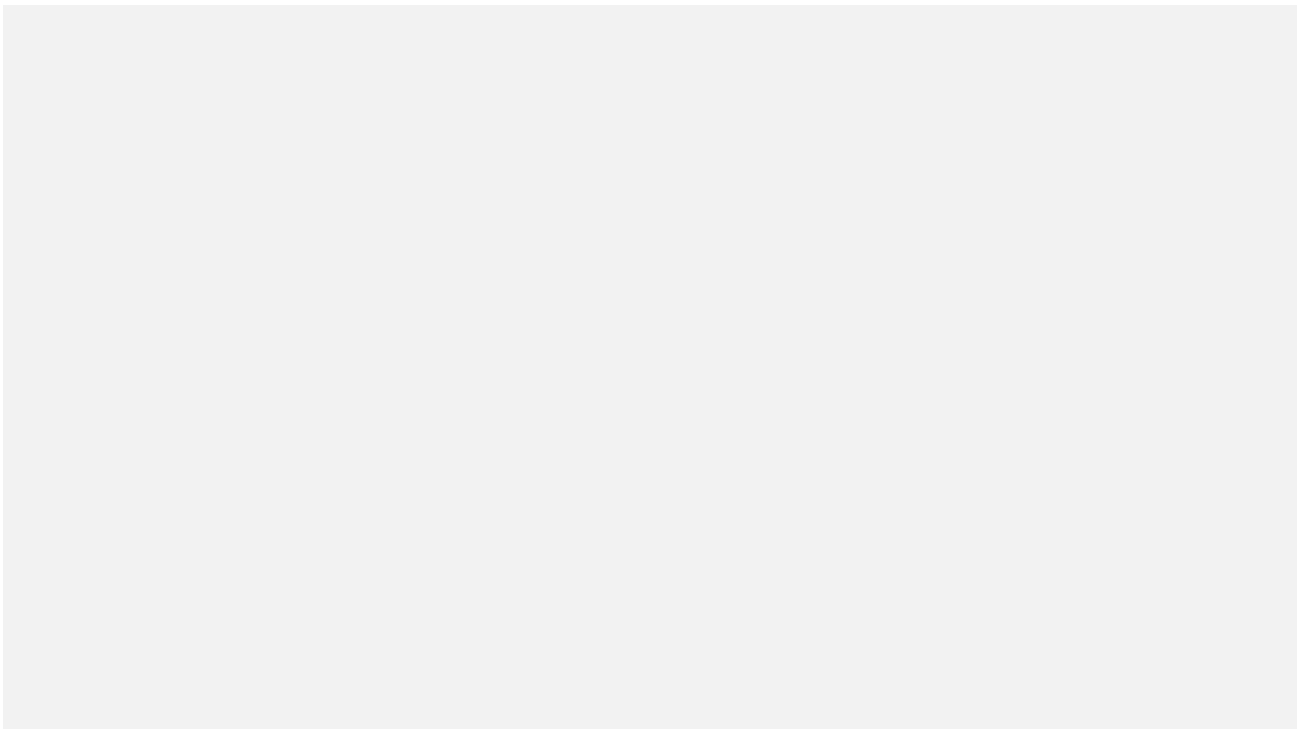
In den Händen autoritärer oder übergreifiger Behörden können Standortdaten, Suchanfragen und soziale Netzwerkaktivitäten sogar zu gefährlichen Waffen werden. In den USA der zweiten Trump-Amtszeit zeigt sich diese Entwicklung besonders eindrücklich.

Die Einwanderungs- und Zollbehörde United States Immigration and Customs Enforcement hat ihre Überwachungsmethoden massiv ausgebaut und greift dabei auf kommerzielle Datenbroker zurück, die Standortdaten von Millionen Smartphones sammeln und verkaufen. Diese Daten, ursprünglich von harmlosen Wetter- oder Gaming-Anwendungen erfasst, befähigen die Behörde, Bewegungsmuster von Personen ohne richterlichen Beschluss nachzuvollziehen.

An der Grenze haben Beamte weitreichende Befugnisse, Smartphones und Laptops zu durchsuchen: Mitunter prüfen sie die Inhalte dabei nicht nur oberflächlich, sondern setzen forensische Software ein, um gelöschte Nachrichten, Cloud-Backups und verschlüsselte Kommunikation auszulesen.

Für Migranten, Asylsuchende oder auch amerikanische Staatsbürger mit ausländischer Herkunft kann ein kritischer Tweet, eine Mitgliedschaft in politischen WhatsApp-Gruppen oder der Besuch bestimmter Websites zur Ablehnung der Einreise oder sogar zur Deportation führen.

Demonstrierende verfolgen die Behörden mithilfe von Gesichtserkennung und Mobilfunkdaten. Frauen aus restriktiven US-Bundesstaaten, die einen Schwangerschaftsabbruch vornehmen wollen, geraten durch Zyklustracker-Apps und Standortdaten von Kliniken ins Visier.



Ein Blick in ein Werbe-Tool, wie hier der Ad Manager von Facebook, offenbart, wie detailliert das Targeting funktioniert.

Doch das Problem beschränkt sich nicht auf die USA. China kombiniert umfassende Überwachungssysteme wie das Social-Credit-System mit Gesichtserkennung, Online-Aktivitäten und Bewegungsdaten, um politische Dissidenten zu identifizieren und zu unterdrücken. Russland nutzt Metadaten von Messengern wie Telegram, um Oppositionelle aufzuspüren. Selbst in demokratischen Staaten Europas greifen Sicherheitsbehörden auf Vorratsdatenspeicherung und automatisierte Gesichtserkennung zurück (Großbritannien) oder liebäugeln zumindest damit.

Fazit

Die Summe unserer Datenspuren ergibt ein Bild, das umfassender ist als das, was selbst enge Freunde über uns wissen: einen digitalen Zwilling, der das Verhalten vorhersagen, die Schwächen offenlegen und die Zukunft beeinflussen kann. Besonders beunruhigend ist die Permanenz dieser Daten. Ein heute harmlos erscheinender Datensatz kann, aus dem Kontext gerissen oder unter einem anderen politischen Regime, zum Verhängnis werden.

Gegen behördliche Zugriffe auf Daten lässt sich kaum etwas unternehmen. Auch viele Informationsströme in der Datenschattenwirtschaft kann ein normaler Verbraucher nicht kontrollieren, wie der Artikel ab [Seite 66](#) zeigt. Hier sind stärkere staatliche Sanktionen notwendig.

Was können Sie also tun? Sich bewusst machen, wer welche Informationen über Sie sammelt. Bei den Unternehmen, die dies ermöglichen, eine Datenauskunft einholen. So sehen Sie, welche Informationen über Sie kursieren. Vor allem aber können Sie Ihre Spuren verwischen und deutlich weniger davon hinterlassen: Sperren Sie trackende Werbung mit Werbeblockern aus. Wechseln Sie zu datensparsamen Apps. Hinterfragen Sie Kundenkarten und andere vermeintliche Sparangebote kritisch: Ist es Ihnen wirklich ein paar Cent wert, dass jemand jahrelang Ihr digitales Abbild verkauft?

Der größte Elefant im Raum sind die Social-Media-Plattformen. Sie kosten in der Regel keine Gebühren, bringen den Betreibern wie Meta und Google aber jedes Jahr Milliardenumsätze, weil sie über die Nutzerprofile Daten zur gezielten Ausspielung von Werbung gewinnen. Das Geld der Nutzer gelangt also indirekt und unsichtbar an die Plattformbetreiber. Wer weniger Datenspuren hinterlassen will, sollte sich als Erstes fragen, ob der Nutzen dieser Plattformen für ihn größer ist als der Schaden durch den erhöhten Konsum, den das Werbettracking verursacht – und dann die Konsequenzen ziehen. (jo@ct.de)

Studien und Berichte zum Datenabfluss: ct.de/y3fr

► 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 ▶](#)