TrutzBox® Kompendium

Teil 1: Das Geschäft mit Ihren Daten

Datenschutz, Datenhändler und digitale Selbstverteidigung

Version 13.8 · Ausgabe September 2026

Autor: Hermann Sauer, Dipl.-Informatiker

Comidio GmbH · Eltville am Rhein · www.trutzbox.de

Rechtliche Hinweise

Sorgfalt und Gewähr. Dieses Kompendium wurde mit größter Sorgfalt erstellt. Für Vollständigkeit, Richtigkeit und Aktualität der Inhalte, insbesondere der Angaben zu Produkten, Diensten und Praktiken Dritter, übernehmen die Comidio GmbH und der Autor keine Gewähr. Alle Angaben geben den Kenntnisstand zum Redaktionsschluss (September 2026) wieder; Quellen sind in den Fußnoten nachgewiesen. Unternehmen und Produkte können ihre Praktiken seither geändert haben.

Meinungen. Bewertungen und Einschätzungen geben die Auffassung des Autors wieder und sind als solche zu verstehen. Die rechtliche Bewertung einzelner Sachverhalte obliegt den zuständigen Behörden und Gerichten. Die Inhalte stellen keine Rechts- oder Sicherheitsberatung im Einzelfall dar.

Haftung. Comidio haftet uneingeschränkt für Vorsatz und grobe Fahrlässigkeit sowie nach den gesetzlichen Bestimmungen für Schäden aus der Verletzung von Leben, Körper oder Gesundheit; die Haftung nach dem Produkthaftungsgesetz bleibt unberührt. Bei einfach fahrlässiger Verletzung wesentlicher Vertragspflichten ist die Haftung auf den vorhersehbaren, vertragstypischen Schaden beschränkt; im Übrigen ist die Haftung ausgeschlossen.

Marken. TrutzBox® ist eine eingetragene Marke der Comidio GmbH. Alle weiteren genannten Marken, Firmen- und Produktnamen sind Eigentum ihrer jeweiligen Inhaber und werden ausschließlich beschreibend verwendet.

Impressum. Comidio GmbH, Eichendorffweg 2, 65343 Eltville. Vertreten durch: Hermann Sauer, Geschäftsführer. Registergericht: Amtsgericht Wiesbaden, Handelsregister B, Registernummer 27951. Umsatzsteuer-Identifikationsnummer gemäß § 27a UStG: DE296578929. Verantwortlich im Sinne von § 18 Abs. 2 MStV: Hermann Sauer, Eichendorffweg 2, 65343 Eltville. Kontakt: Telefon +49 6123 9748802, E-Mail info@comidio.de, Web www.trutzbox.de und www.comidio.de.

Inhaltsverzeichnis

Dokumenthistorie

Version	Datum	Änderungen
9.31	Aug. 2024	Letzte öffentliche Basisversion (Basis dieses Updates)
10.0	Jan. 2026	Xandr/650.000 Kategorien, Databroker Files, DSGVO-Einordnungen, Spear Phishing, CEO Fraud, Digitale Integrität, Smart-TV ACR, WhatsApp, Handynummer-Risiko
11.1	März 2026	Gesamtausgabe: alle vier Teile zusammengeführt, Inhaltsverzeichnis, 67 Fußnotenreferenzen, verlinkter Index, erheblich erweiterte Kapitel
12.11	Juli 2026	Drei Blockier-Methoden mit Vergleichstabelle, neues Kapitel zu Verkehr ohne sichtbaren Domain-Namen, IP-Blockierung (Angriffsschutz) verfügbar, TrutzChat-Korrekturen, Monitor statt Zugriffsprotokoll, 66 Abbildungen aus v10.2 wiederhergestellt (Quellenangaben aus v10.2 übernommen)
13.1	Sept. 2026	Redaktionelle und fachliche Überarbeitung nach Review: Titel, Version und Fußzeile vereinheitlicht, Inhaltsverzeichnis und Stichwortverzeichnis korrigiert; Fakten aktualisiert (Oracle Data Cloud 2024 eingestellt, Google-Cookie-Stand 2025, Encrypted Client Hello, Bußgelder, Studien- und Fallquellen); rechtlich entschärfte Formulierungen (Microsoft/Xandr, Kundenkartenprogramme, Sprachassistenten, Produktzusagen); Vergleichsgrafik Browser-Plugins entfernt; Empfehlung zu verschlüsseltem DNS auf Mobilgeräten präzisiert; Statistiken und Fallbeispiele auf Stand 2025/2026 gebracht (IBM, Verizon, FBI, Bitkom, CrowdStrike, W3Techs, Meta, Google, ICCL, IoT Analytics, FTC, Texas AG); neue Kapitel „Künstliche Intelligenz: Der neue Datenhunger“ und „Was die EU gegen die Datenmacht der Konzerne tut“, neuer Abschnitt zu Apple und App Tracking Transparency; Meta-Geschäftsmodell klargestellt (kein Datenverkauf); Ellison-Imperium und Verbleib der Oracle-Werbedaten ergänzt; Fremdgrafiken mit Datenstand vor 2024 entfernt, eigene Grafiken auf Ausgabe 2026 datiert; rechtliche Hinweise auf Seite 2 zusammengeführt, Fußzeile gekürzt; Produktdetails auf Kompendium Teil 2 verwiesen (Module nur noch im Überblick); Neugliederung in sieben Teile (Herausforderung, Datenhändler und Plattformen, Gerätehersteller, Tracking-Technik, Standortdaten, Staat und Kriminelle, Schutz), zusammengehörige Kapitel zusammengeführt, Doppelungen (DNS, VPN, Erpressung, Produktbeschreibung) verschmolzen; Ergänzungen aus Boxenstopp-Vorträgen und Artikeln 2024 bis 2026: Meta-Urteile, stille Nachrichten, KI-Angriffe, Behördenkauf von Werbedaten, Browser-Erweiterungen, Mail-Signatur, Deutschland 2026, Mobilfunknummer, Gesundheitsdaten, Einwilligung, Meta-

		Betrugsanzeigen, Smart-TV-Botnetz, utiq, Zeitserver, CLOUD Act, National Public Data, Filter-Messung
13.2	Sept. 2026	Alle Abbildungen mit erklärender Bildunterschrift, Rahmen und einheitlicher Ausrichtung, Menüpfad über den Monitor-Abbildungen, vereinheitlichte Abstände

Teil 1
Die Herausforderung

Warum Ihre Daten so wertvoll sind und wer sie haben will

Die Herausforderung

Für Einsteiger:

Stellen Sie sich vor, Sie gehen jeden Tag in ein Geschäft, und ein unsichtbarer Beobachter notiert genau, was Sie anschauen, wie lange Sie verweilen, was Sie kaufen und mit wem Sie sprechen. Genau das passiert im Internet: Jede Website, die Sie aufrufen, jede App, die Sie nutzen, sendet Informationen über Sie an Dutzende von Unternehmen, die diese Daten sammeln, auswerten und verkaufen. Das Internet ist heute weniger ein Ort der freien Information als ein globales Überwachungssystem, und die meisten Nutzer wissen nicht einmal, dass es existiert.

Technischer Hintergrund

Das Internet hat sich in den vergangenen drei Jahrzehnten von einem offenen Kommunikationsnetz in eine allgegenwärtige Überwachungsinfrastruktur verwandelt. Was 1969 als ARPANET, ein militärisches Forschungsnetz der USA, begann und in den frühen 1990er Jahren durch Tim Berners-Lee mit dem World Wide Web zur öffentlichen Nutzung freigegeben wurde, ist heute das Fundament eines globalen Geschäftsmodells, das auf der systematischen Ausbeutung persönlicher Daten beruht. Der einzelne Internetnutzer steht dabei vor einer paradoxen Situation: Er nutzt Dienste, die ihm kostenlos angeboten werden, und bezahlt dafür mit dem wertvollsten Gut, das er besitzt, seinen Daten, seiner Aufmerksamkeit und letztlich seiner Autonomie.[1]

Diese Entwicklung verlief keineswegs zufällig. Sie ist das Ergebnis bewusster Entscheidungen einer Handvoll mächtiger Technologiekonzerne in den frühen 2000er Jahren, als klar wurde, dass mit der Sammlung und Auswertung von Nutzerdaten immense Gewinne erzielbar sind. Google erkannte als erstes Unternehmen, dass die Suchmaschine nicht das eigentliche Produkt ist, das Produkt ist der Nutzer selbst, dessen Aufmerksamkeit und dessen Verhalten an Werbetreibende verkauft wird. Dieses Modell wurde seither von Facebook, Amazon und hunderten weiterer Unternehmen kopiert und verfeinert.

Die Dimension dieses Problems lässt sich an wenigen Zahlen ablesen. Tausende Unternehmen weltweit haben sich darauf spezialisiert, Daten über Internetnutzer zu sammeln, zu analysieren und gewinnbringend zu verkaufen, allein in den Datenhändler-Registern der US-Bundesstaaten Kalifornien, Texas, Vermont und Oregon sind rund 750 Firmen eingetragen (Stand 2025). Der globale Markt für Datenhandel wird für 2025 je nach Schätzung auf 300 bis 430 Milliarden US-Dollar beziffert, mehr, als weltweit für IT-Sicherheit ausgegeben wird (Gartner: rund 218 Milliarden US-Dollar 2025).[2]

[1] Shoshana Zuboff: The Age of Surveillance Capitalism. PublicAffairs, New York 2019. Zuboffs Standardwerk beschreibt, wie die Verhaltensmodifikation durch Technologiekonzerne zu einem vollständig neuen Wirtschaftszweig geworden ist.

Allein Acxiom wirbt mit Daten zu 2,6 Milliarden Menschen und mehr als 10.000 Merkmalen je Person; bei rund sechs Milliarden Internetnutzern weltweit (ITU 2025) ist damit ein Großteil der Online-Bevölkerung in kommerziellen Datenbanken verzeichnet, ohne davon zu wissen, ohne es jemals aktiv zugelassen zu haben und ohne die Möglichkeit, diese Daten wirksam zu löschen.[3]

Was macht das so gefährlich? Die systematische Erfassung von Nutzerdaten schafft eine neue Angriffsfläche, die weit über das hinausgeht, was herkömmliche Firewalls und Intrusion-Detection-Systeme schützen können. Die Daten fließen nicht durch offensichtliche Löcher in der Sicherheitsinfrastruktur, sie verlassen das Netzwerk als legitimer ausgehender Datenverkehr, vollständig unbemerkt von klassischen Sicherheitssystemen. Jeder Webseitenbesuch, jede App-Nutzung, jedes vernetzte Gerät im Haushalt wird zum Datenlieferanten.

Dieses Kompendium dokumentiert die Erkenntnisse, die das Comidio-Team über viele Jahre hinweg durch intensive Markt- und Technologieanalyse gewonnen hat. Es beschreibt zunächst die drei großen Gruppen von Akteuren, die Daten über Internetnutzer sammeln und ausnutzen: kommerzielle Daten-Tracker und Datenhändler, Geheimdienste und staatliche Behörden sowie Internet-Kriminelle. Darüber hinaus zeigt es, wie die TrutzBox als Privacy-Box einen umfassenden Schutz gegen alle drei Gruppen bietet, ohne dabei auf die Vorteile des modernen Internets verzichten zu müssen. Das folgende Kapitel ordnet sie in sechs Gefahrengruppen ein.

Die Comidio Mission

Comidio, abgeleitet aus dem Lateinischen commodus (bequem) und praesidio (Schutz), wurde 2014 von Hermann Sauer gemeinsam mit sieben erfahrenen IT-, Sicherheits-, Rechts- und Marketing-Experten gegründet. Das Unternehmen hat seinen Sitz in Eltville am Rhein. Ziel ist es, sowohl technischen Laien als auch IT-Experten wirksame Mittel an die Hand zu geben, sich gegen allumfassende Ausspähung im Internet zu wehren, ohne auf die Vorzüge des modernen Internets verzichten zu müssen. Die Comidio GmbH betreibt die TrutzBox ausschließlich auf eigener Infrastruktur in Deutschland und unterliegt damit ausschließlich deutschem und europäischem Datenschutzrecht.

Sechs Gefahrengruppen: Wer Ihre Daten will

Für Einsteiger:

Wer Ihre Daten will, ist nicht immer ein Krimineller. Auch ganz legale Unternehmen, staatliche Behörden und sogar die Hersteller Ihrer eigenen Geräte gehören dazu. Comidio hat sechs Gruppen von Akteuren identifiziert, die ein Interesse an Ihren Daten haben, und gegen die die TrutzBox jeweils spezifischen Schutz bietet. Zusammen bilden sie das vollständige Bedrohungsbild des modernen Internets.

[2]Fortune Business Insights: Data Broker Market, Stand August 2026 (304 Mrd. USD 2025, 327 Mrd. USD 2026); Knowledge Sourcing Intelligence / Research and Markets, Februar 2025 (434 Mrd. USD 2025). Privacy Rights Clearinghouse / EFF: Why Are Hundreds of Data Brokers Not Registering with States?, Juni 2025 (750 in mindestens einem US-Register eingetragene Datenhändler). Gartner: Forecast Information Security Spending, Juni 2026 (218,2 Mrd. USD 2025, 248,9 Mrd. USD 2026).

[3]Acxiom: Customer Data, „2.6B global audience, 10K+ unique attributes“, acxiom.com/customer-data (abgerufen September 2026). ITU: Facts and Figures 2025, 17. November 2025 (6,0 Milliarden Internetnutzer, drei Viertel der Weltbevölkerung).

🔧 Die sechs Gefahrengruppen und der TrutzBox-Schutz im Überblick

Das Comidio-Team hat auf Basis seiner langjährigen Analyse des Bedrohungsumfelds sechs Gefahrengruppen definiert, gegen die eine moderne Privacy-Box Schutz bieten muss. Diese Klassifikation ist bewusst breiter als die gängige IT-Sicherheitsliteratur, die sich meist auf die Abwehr externer Angriffe konzentriert. Die TrutzBox-Schutzphilosophie umfasst auch den Schutz vor kommerzieller Ausspähung durch eigentlich legitime Akteure sowie vor Datenlecks durch schlecht gesicherte Geräte im eigenen Netzwerk.

- 1. Kommerzielle Daten-Tracker: Werbeplattformen und Analysedienste, die Nutzerverhalten auf Websites und in Apps verfolgen, um Werbeprofile zu erstellen. Vertreter: Google Analytics, Meta-Pixel, Criteo, Hotjar, Doubleclick.
- 2. Datenhändler (Data Broker): Unternehmen, die Datensätze aus verschiedensten Quellen zusammenstellen, anreichern und an Dritte verkaufen. Vertreter: Acxiom, LiveRamp, Datastream Group sowie die auf dem Microsoft-Marktplatz Xandr handelnden Datenanbieter.
- 3. Geheimdienste und staatliche Autoritäten: Staatliche Akteure, die Internet-Kommunikation überwachen. Vertreter: NSA (PRISM, XKeyscore), BND, GCHQ sowie das Netzwerk aus 10.000 deutschen Behörden mit potenziellem Datenzugriff, dazu die Analysesoftware des US-Konzerns Palantir in mehreren Landespolizeien.
- 4. Internet-Kriminelle: Akteure mit krimineller Motivation, die Schadsoftware, Phishing und Social Engineering einsetzen. Vertreter: Ransomware-Gruppen (z.B. LockBit, ALPHV), CEO-Fraud-Syndikate, Phishing-Operatoren.
- 5. Nation-State Actors: Staatlich gesponserte Hackergruppen für Wirtschaftsspionage und strategische Sabotage. Vertreter: APT28/Fancy Bear (Russland), APT41 (China), Lazarus Group (Nordkorea).
- 6. Gerätehersteller mit zweifelhafter Datenpolitik: Unternehmen, die in ihre Produkte Datensammel-Mechanismen einbauen, die über den notwendigen Funktionsumfang hinausgehen. Vertreter: Smart-TV-Hersteller (Samsung ACR, LG ACR), Sprachassistenten-Anbieter (Amazon Alexa), App-Entwickler mit aggressiven Tracking-Praktiken.

Die TrutzBox adressiert alle sechs Gefahrengruppen durch ihre integrierten Schutzfunktionen. TrutzBrowse schützt vor kommerziellen Trackern und Datenhändlern auf Proxy-Ebene. TrutzMail und TrutzChat entziehen Inhalte und Metadaten der Kommunikation dem Zugriff Dritter, auch staatlicher Stellen. TrutzBase wehrt Angriffe aus dem Internet ab, soweit sie auf Netzwerkebene erkennbar sind. Das VPN-Modul schützt auch unterwegs. Der Monitor macht die Aktivitäten aller Geräte transparent und ermöglicht die Erkennung von IoT-Geräten mit zweifelhafter Datenpolitik. Wie die einzelnen Funktionen arbeiten, beschreibt Kompendium Teil 2 (Funktionen und Architektur).

Die Gefahrengruppen und ihre Anwendungsfälle im Überblick (Einstufung des Comidio-Teams):

Stufe	Bedrohungsart	Erläuterung	Eingesetzte Technik	Schutz und Umgehung
1	Ausspähen von Nutzerprofilen	Unternehmen wie Facebook erhalten nicht nur die Daten ihrer Mitglieder: Jede Seite mit einem „Gefällt mir“-Button meldet Nutzerdaten an Facebook. Plattformen und Datenhändler wie Acxiom oder LiveRamp führen die Daten zusammen. Die meisten Webseiten enthalten eingebautes Tracking, oft 10 bis 30 verschiedene Tracker auf einer einzigen Seite.	Cookies, Zählpixel (Web-Bugs), Evercookies, Browser-Fingerprinting. E-Mail-Tracking über 1×1-Pixel-Bilder und Tracking-Dienste. Dokumenten-Tracking durch nachgeladene Inhalte in Word- oder PDF-Dateien.	Cookies, Zählpixel, Evercookies und Fingerprinting im Browser kontrollieren oder unterbinden. HTML-Darstellung im E-Mail-Programm einschränken.
2	Ausspähen von Kommunikationsbeziehungen	Die Information „Wer kommuniziert mit wem“ lässt sich im Internet leicht gewinnen und ist für Unternehmen wie für Geheimdienste sehr wertvoll.	Auswertung des E-Mail-Verkehrs sowie der Kommunikation über soziale Netzwerke, Messenger und Blogs.	Wegwerf- und Einmal-E-Mail-Adressen sowie Remailer-Dienste verhindern das Mitlesen durch die Diensteanbieter.
3	Internet-Zensur durch Staaten und Inhalteanbieter	Staaten beschränken den Zugang zu Inhalten, die nach ihren Gesetzen unerwünscht sind. Anbieter wie YouTube sperren Inhalte aus Urheberrechts- und Lizenzgründen.	Auf Netzebene wird der gesamte Verkehr gegen Positiv- oder Sperrlisten von Quell- und Ziel-IP-Adressen geprüft.	VPN-Zugänge (IP-basiert) oder HTTP-Proxy-Server in einem anderen Land.
4	Zugriff auf oder Manipulation persönlicher Daten	Angriffe mit Viren, Würmern oder Trojanern. Sie dienen dem Ausspähen von Geschäftsdaten oder der Manipulation persönlicher Daten, etwa bei Bankgeschäften.	Schadsoftware greift auf lokal gespeicherte Daten zu, liest Eingaben mit oder manipuliert Kommunikationsdaten, zum Beispiel Banktransaktionen.	Infektionen vermeiden durch aktuelle Virenscanner und Kontrolle aktiver Inhalte (Skripte) in Browser, E-Mail-Programm und anderer Internet-Software. Verschlüsselte Verbindungen (HTTPS) verpflichtend.
5	Aufhebung der Anonymität im Netz	Internetanbieter protokollieren, welcher Kundenanschluss zu welcher Zeit welche IP-Adresse hatte. Mit richterlicher Anordnung erhalten Dritte Zugriff auf diese Daten und damit Name und Anschrift dessen, der einen Inhalt abgerufen hat.	Keine besondere Technik nötig. Es genügt die Aufzeichnung, welche Quell-IP-Adresse den Inhalt abgerufen hat.	Wie Stufe 3.
6	Unerlaubter Zugriff auf jugendgefährdende Inhalte	Im Internet sind grundsätzlich alle Inhalte für jeden erreichbar. Eltern wollen ihre Kinder vor ungeeigneten Inhalten schützen.	Je nach Alter des Kindes legen die Eltern fest, welche Inhaltsfilter für welches Kind aktiv sind.	Je nach eingesetzter Technik kann der Nutzer den Filter umgehen, indem er IP-Adressen statt Domain-Namen anspricht.

Teil 2
Datenhändler und Plattformen

Das Geschäft mit Ihren Daten: wer sammelt, wer handelt, wer profitiert

Kommerzielle Daten-Tracker und Datenhändler

Für Einsteiger:

Wer Geld verdienen möchte, braucht Kunden. Wer Kunden gezielt ansprechen möchte, braucht Informationen über sie. Genau das tun Datenhändler: Sie sammeln aus tausenden Quellen Informationen über jeden Internetnutzer, welche Seiten er besucht, was er kauft, wo er sich aufhält, und verkaufen diese Daten weiter. Plattformen wie Meta oder Google gehen einen anderen Weg: Sie verkaufen nicht die Daten, sondern den Zugang zu den Menschen, die sie damit beschreiben können. Diese bezahlen dafür, dass ihre Werbung genau den Menschen erreicht, der gerade nach ihrem Produkt sucht oder anfällig dafür ist. Das klingt nach harmlosem Marketing, dahinter steckt aber eine Industrie, die weit in das Privatleben der Menschen eindringt.

Technischer Hintergrund

Wenn ein Nutzer eine Webseite aufruft, läuft im Hintergrund eine unsichtbare Maschinerie an, die in ihrer Komplexität und Reichweite das Vorstellungsvermögen der meisten Menschen übersteigt. Tracker auf der aufgerufenen Seite, meist winzige JavaScript-Schnipsel, die kaum 1 KB groß sind, kommunizieren in Bruchteilen von Sekunden mit Dutzenden von Servern weltweit. Sie übermitteln: die IP-Adresse des Nutzers (aus der sich Standort, Internetanbieter und oft sogar der Haushalt ableiten lassen), den verwendeten Browser und seine Version, das Betriebssystem und die Version, die Bildschirmauflösung und Farbtiefe, die Zeitzone, die Systemsprache, installierte Schriftarten und Plugins, die aufgerufene URL und den gesamten Navigationspfad der Sitzung sowie die verweisende Seite (Referrer). Kombiniert ergeben diese scheinbar harmlosen technischen Parameter einen nahezu eindeutigen digitalen Fingerabdruck des Nutzers.[4]

Diese Daten werden nicht nur von der besuchten Website genutzt. Sie fließen in Echtzeit an ein globales Netzwerk von Datenhändlern, die diese Informationen bündeln, anreichern und weiterverkaufen. Dabei passiert ein einzelner Webseitenaufruf typischerweise eine Kette von fünf bis zwanzig verschiedenen Unternehmen: den eigentlichen Webseitenbetreiber, das Werbenetzwerk, die Analyseplattform, den Remarketing-Dienst, den Datenhändler und schließlich den Werbetreibenden, der die Auktion gewonnen hat. Das Ergebnis ist ein detailliertes Profil jedes Internetnutzers, das weit über das hinausgeht, was dieser selbst über sich weiß, oder wissen möchte.

[4] Electronic Frontier Foundation: Panopticlick / Cover Your Tracks. Browser Fingerprint Test. https://coveryourtracks.eff.org. Laut EFF ist ein vollständiger Browser-Fingerprint unter etwa 300.000 Nutzern eindeutig.

Douglas Merrill, ehemaliger Chief Information Officer bei Google, brachte das Geschäftsmodell auf den Punkt: „Alle Daten sind Kreditdaten, wir wissen nur noch nicht, wie wir sie einsetzen werden." Dieser Satz beschreibt präzise die Logik hinter dem modernen Datenhandel: Nicht der unmittelbare Verwendungszweck bestimmt den Wert der Daten, sondern ihr zukünftiges Potenzial. Daten, die heute harmlos erscheinen, können morgen für Entscheidungen über Kreditwürdigkeit, Versicherungsprämien, Beförderungen oder politische Einflussnahme genutzt werden.[5]

Was Datenhändler sammeln, bleibt zudem nicht bei ihnen. 2024 erbeuteten Angreifer beim US-Datenhändler National Public Data nach Gerichtsunterlagen bis zu 2,9 Milliarden Datensätze mit Namen, Anschriften, Geburtsdaten und Sozialversicherungsnummern aus den USA, Kanada und Großbritannien. Die Daten wurden zunächst für 3,5 Millionen US-Dollar zum Kauf angeboten und später kostenlos verbreitet; das Unternehmen meldete im Oktober 2024 Insolvenz an. Die Lehre: Jede legal aufgebaute Sammlung ist ein Angriffsziel, und was einmal abgeflossen ist, lässt sich nicht zurückholen.[6]

Die Firma Facebook (Meta)

Für Einsteiger:

Facebook kennen die meisten als soziales Netzwerk, um Fotos zu teilen und mit Freunden in Kontakt zu bleiben. Aber Facebook ist in erster Linie ein Werbeunternehmen. Es verdient sein Geld damit, genau zu wissen, wer Sie sind, was Sie interessiert und was Sie kaufen könnten, und auf dieser Basis zielgerichtete Werbeeinblendungen an Werbetreibende zu verkaufen. Was kaum jemand weiß: Facebook-Tracker sind auf Millionen von Websites eingebaut, auch auf Seiten, die nichts mit Facebook zu tun haben. Selbst wer kein Facebook-Konto hat, wird verfolgt.

Technischer Hintergrund

Facebook, heute unter dem Konzernnamen Meta Platforms Inc. firmierend, wurde 2004 von Mark Zuckerberg gegründet und hat das Social-Media-Modell des Datensammelns auf eine neue Stufe gehoben. Mit 3,6 Milliarden täglich aktiven Nutzern seiner Dienste (Juni 2026), das entspricht rund 44 Prozent der Weltbevölkerung und 60 Prozent aller Internetnutzer, verfügt Meta über den wohl umfangreichsten Datensatz über menschliches Sozialverhalten, der je zusammengestellt wurde.[7]

Was viele Nutzer nicht wissen: Facebook-Tracker sind nicht nur auf facebook.com aktiv. Der sogenannte Meta-Pixel, ein unsichtbares 1×1-Pixel-Bild kombiniert mit JavaScript-Code, ist in Millionen von Websites eingebunden, auch dort, wo Nutzer überhaupt kein Facebook-Konto haben. Wenn ein Nutzer eine solche Website besucht, übermittelt der Meta-Pixel Informationen über den Besuch automatisch an Meta-Server. Dies geschieht, ohne dass der Nutzer darauf hingewiesen wird oder aktiv einwilligen kann. Nach einer Messung von 40.000 Websites (PoPETs 2025) sind Meta-Tracker auf 28 Prozent der Seiten eingebunden, und auf 62 Prozent davon so konfiguriert, dass auch Formulareingaben erfasst werden.[8]

[5] Douglas Merrill, zitiert von Hermann Sauer in diversen Vorträgen und im TrutzBox Kompendium. Merrill gründete nach Google das Unternehmen ZestFinance, das Kreditwürdigkeitsanalysen auf Basis nichtklassischer Datenpunkte durchführt.

[6] Bloomberg Law: National Public Data files for bankruptcy after massive breach, Oktober 2024. Sauer, H.: Digitale Integrität: Warum Firewall und IDS nicht reichen, CSO Online, Januar 2026.

[7] Meta Platforms Inc.: Second Quarter 2026 Results, 29. Juli 2026. Family Daily Active People 3,60 Milliarden (Durchschnitt Juni 2026). Facebook allein wird seit 2024 nicht mehr ausgewiesen (zuletzt 3,07 Milliarden monatlich aktive Nutzer, Dezember 2023).

[8] Kieserman et al.: Tracker Installations Are Not Created Equal. Proceedings on Privacy Enhancing Technologies (PoPETs) 2025(4). HTTP Archive: Web Almanac 2025, Kapitel Privacy, Januar 2026 (Meta-Pixel auf 16 Prozent aller untersuchten Websites).

Die gesammelten Daten umfassen: alle geposteten Inhalte, Kommentare und Reaktionen auf Facebook und Instagram, Standortdaten aus dem Handy (sofern aktiviert), Browsing-Verhalten außerhalb von Facebook durch den Meta-Pixel und das Facebook Login SDK, Kontaktlisten (hochgeladen für die „Freunde finden"-Funktion), Finanzinformationen aus dem Facebook Marketplace sowie Gesundheitsdaten, die aus dem Surfverhalten auf medizinischen Websites abgeleitet werden.

Im Jahr 2022 wurde bekannt, dass der Meta-Pixel sensible Gesundheitsdaten von Krankenhauspatienten und Arztpraxen gesammelt hatte, darunter Informationen über Therapiestunden für psychische Erkrankungen, Krebsdiagnosen und Informationen über geplante Schwangerschaftsabbrüche. Das US-Justizministerium und mehrere Bundesstaatsanwaltschaften leiteten Ermittlungen wegen Verstoßes gegen den Health Insurance Portability and Accountability Act (HIPAA) ein.[9]

Der Skandal um Cambridge Analytica im Jahr 2018 zeigte das Ausmaß, in dem Facebook-Daten für politische Manipulation genutzt werden können. Die Daten von über 87 Millionen Facebook-Nutzern wurden ohne deren Wissen für die Entwicklung psychografischer Profile genutzt, die anschließend im US-Präsidentschaftswahlkampf 2016 für zielgerichtete Werbung eingesetzt wurden. Facebook einigte sich 2019 mit der US-Handelskommission (FTC) auf ein Bußgeld von fünf Milliarden US-Dollar, die bis dahin höchste Datenschutzstrafe in der Geschichte der USA.[10]

Trotz dieser Strafe und trotz der DSGVO in Europa hat Meta sein Geschäftsmodell nicht grundlegend verändert. Im November 2022 verhängte die irische Datenschutzbehörde DPC (Data Protection Commission, die als Lead Authority für Meta in Europa fungiert) eine Rekordstrafe von 265 Millionen Euro wegen eines massiven Datenlecks, bei dem die persönlichen Daten von mehr als 533 Millionen Facebook-Nutzern öffentlich zugänglich wurden. Im Januar 2023 folgte eine weitere Strafe von 390 Millionen Euro wegen unzulässiger Nutzung von Nutzerdaten für personalisierte Werbung ohne ausreichende Rechtsgrundlage. Im Dezember 2024 kamen 251 Millionen Euro für ein Datenleck von 2018 mit 29 Millionen betroffenen Konten hinzu; im April 2025 verhängte die EU-Kommission 200 Millionen Euro nach dem Digital Markets Act wegen des „Zustimmen oder zahlen"-Modells.[11]

Seit 2024 kommen Urteile deutscher Gerichte hinzu, die Betroffenen unmittelbar Ansprüche geben. Der Bundesgerichtshof entschied im November 2024 zum Datenleck von 2021, dass bereits der Verlust der Kontrolle über die eigenen Daten ein ersatzfähiger Schaden ist; ein Nachweis von Missbrauch ist nicht nötig. Im Februar 2026 verurteilten die Oberlandesgerichte Dresden, Naumburg und München Meta wegen des Trackings über Meta-Pixel und Business Tools zu Schadenersatz, in Dresden rechtskräftig 1.500 Euro je Kläger. Die Gerichte sahen in der Cookie-Einwilligung auf einer fremden Website keine wirksame Einwilligung gegenüber Meta. Das Landgericht Mainz hatte 2025 dokumentiert, auf welchen Seiten die Meta-Werkzeuge liefen, darunter nach dem Urteil Angebote der Deutschen Bahn, einer Versandapotheke und der Deutschen Krebshilfe. Eine Studie von DIW Berlin mit den Universitäten Zürich, Lausanne und Yale schätzt, dass Meta über diese Einbindungen bis zu 52 Prozent aller Webseitenbesuche nachverfolgen kann, bei Menschen ohne Facebook-Konto rund 44 Prozent ihrer Surfzeit; nach einer Auswertung von Consumer Reports liefern im Schnitt 2.230 Unternehmen Daten zu

[9] The Markup: Facebook Is Receiving Sensitive Medical Information from Hospital Websites, Juni 2022. https://themarkup.org/pixel-hunt/2022/06/16/facebook-is-receiving-sensitive-medical-information-from-hospital-websites

[10] Federal Trade Commission: FTC Imposes $5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook, 24. Juli 2019. https://www.ftc.gov/news-events/news/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions-facebook

[11] Irish Data Protection Commission: Meta Platforms Ireland Limited. Decision of January 2023, Record Fine of €390 million; Decision on Token Breach, 17. Dezember 2024 (251 Mio. Euro). https://www.dataprotection.ie. Europäische Kommission: Commission finds Apple and Meta in breach of the Digital Markets Act, 23. April 2025 (Meta 200 Mio. Euro).

einem einzelnen Nutzer an Meta. Genau diese Einbindungen sind es, die ein Proxy-Filter im Heimnetz für alle Geräte unterbindet.[12]

Viele Webseiten binden den Facebook-Like-Knopf ein. Er meldet den Besuch an Facebook, auch wenn niemand darauf klickt.

Was Meta mit den Daten macht, und was nicht

Meta verkauft keine Nutzerdaten, das betont der Konzern seit Jahren, und keine Aufsichtsbehörde hat ihm bisher das Gegenteil nachgewiesen. Das Geschäftsmodell ist ein anderes: Meta verkauft Werbetreibenden den Zugang zu Zielgruppen, die es aus den gesammelten Daten bildet. Der Werbekunde erfährt nur aggregiert, dass seine Anzeige etwa „von Frauen zwischen 25 und 34 in Madrid mit Interesse an Softwareentwicklung“ gesehen wurde, die Rohdaten bleiben bei Meta. Genau darin liegt der Wert: 2025 stammten 196 von 201 Milliarden US-Dollar Umsatz aus Werbung, also 97,6 Prozent; im ersten Halbjahr 2026 waren es 114 von 117 Milliarden. Jeder Nutzer der Meta-Dienste brachte 2025 im Durchschnitt rund 57 US-Dollar Werbeumsatz ein, im zweiten Quartal 2026 allein 16,86 US-Dollar. Europa steuerte 2025 etwa 48 Milliarden US-Dollar bei, knapp ein Viertel des Konzernumsatzes.[13]

Die Daten wandern also nicht als Ware zu Dritten, sondern fließen in immer feinere Zielgruppenmodelle. Seit Mitte 2026 nutzt Meta die von Partnern gemeldeten Aktivitäten. Käufe auf fremden Websites, Spiele, App-Nutzung, nicht mehr nur für Werbung, sondern auch für die Sortierung des Feeds und für Antworten seiner KI; die bisherige Kontrolle „Aktivitäten außerhalb von Meta-Technologien“ wurde abgeschafft. Seit dem 27. Mai 2025 trainiert Meta seine KI-Modelle zudem mit den öffentlichen Beiträgen erwachsener Nutzer in der EU sowie mit allen Unterhaltungen mit Meta AI; Rechtsgrundlage ist das „berechtigte Interesse“, Betroffene können lediglich widersprechen. Das Oberlandesgericht Köln lehnte im Mai 2025 den Eilantrag der Verbraucherzentrale NRW gegen dieses Vorgehen ab. Außerhalb der EU nutzt Meta seit Dezember 2025 auch den Inhalt von Gesprächen mit Meta AI, um Werbung und Inhalte zu personalisieren, ohne Widerspruchsmöglichkeit.[14]

Wo Daten dennoch bei Dritten landen, geschieht das ohne Verkauf, über die Schnittstellen, die Meta anderen öffnet. Cambridge Analytica erhielt 2018 die Daten von 87 Millionen Nutzern über eine App-Schnittstelle. Umgekehrt fließen über den Meta-Pixel und die Meta-SDKs in Apps massenhaft Daten Dritter zu Meta: Im August 2025 sprach eine Jury in Kalifornien Meta schuldig, über das SDK der Zyklus-App Flo Health jahrelang Angaben zu Schwangerschaft und Menstruation von Millionen Nutzerinnen empfangen zu haben; die Schadenssumme wird 2026 verhandelt, gesetzlich sind 5.000 US-Dollar je Verstoß vorgesehen. US-Kliniken, die den Meta-Pixel auf Patientenportalen einsetzten, zahlten 2026

[12] BGH, Urteil vom 18. November 2024, VI ZR 10/24. OLG Dresden, Urteil vom 3. Februar 2026, 4 U 196/25; OLG Naumburg, Urteil vom 5. Februar 2026; OLG München, Urteile vom 4. Februar 2026 und 26. Juni 2026. LG Mainz, Urteil vom 27. Juni 2025, 3 O 29/24. DIW Berlin / Universität Zürich / Universität Lausanne / Yale: Facebook Shadow Profiles, Discussion Paper. Consumer Reports: Who Shares Your Information With Facebook?, 2024. Sauer, H.: Meta spioniert Sie aus, auch ohne Facebook, Instagram oder WhatsApp, FOCUS Online, März 2026; Nach OLG-Urteil, wackelt jetzt das Geschäftsmodell von Meta?, FOCUS Online, Juli 2026.

[13] Meta Platforms Inc.: Fourth Quarter and Full Year 2025 Results, 28. Januar 2026 (Umsatz 200,97 Mrd. USD, davon Werbung 196,18 Mrd.); Second Quarter 2026 Results, 29. Juli 2026 (Halbjahr: 117,1 Mrd. USD, Werbung 114,4 Mrd.; Family Average Revenue per Person Q2 2026: 16,86 USD; Europa Q2 2026: 14,3 Mrd. USD). Meta: Datenschutzrichtlinie, Fassung 23. Juli 2026 (Beispiel zu aggregierten Werbeberichten). Meta Newsroom: „we still do not sell your information“, 26. Mai 2022.

[14] Meta Newsroom: Better personalization and changes to controls for your activity from other businesses, 9. Juni 2026. Meta Newsroom: Making AI Work Harder for Europeans, 14. April 2025; Irish Data Protection Commission: DPC statement on Meta AI, 21. Mai 2025. OLG Köln, Beschluss vom 23. Mai 2025, 15 UKl 2/25. Meta Newsroom: Improving Your Recommendations on Our Apps With AI at Meta, 1. Oktober 2025 (Nutzung von Meta-AI-Chats für Werbung ab 16. Dezember 2025; EU, UK und Südkorea ausgenommen).

Vergleiche zwischen 200.000 und 9,5 Millionen US-Dollar. Der Satz „Wir verkaufen Ihre Daten nicht“ ist also wahr, und sagt wenig darüber, wer sie am Ende hat.[15]

Die Präzision der Werbemaschine steht auch Kriminellen offen. Der Sicherheitsanbieter Gen Digital (Norton, Avast, Avira) prüfte über 42 Tage 13,7 Millionen Meta-Anzeigen in der EU, davon 5,6 Millionen in Deutschland: Rund ein Viertel wies nach seiner Bewertung Betrugsmerkmale auf, etwa gefälschte Shops oder erfundene Empfehlungen Prominenter. Die Nachrichtenagentur Reuters berichtete im November 2025 unter Berufung auf interne Meta-Unterlagen, der Konzern habe selbst geschätzt, dass rund zehn Prozent seines Werbeumsatzes 2024, etwa 16 Milliarden US-Dollar, aus Anzeigen für Betrug und verbotene Waren stammten, und habe den durch schärfere Prüfungen entstehenden Umsatzverlust intern begrenzt. Meta bezeichnete die Schätzung als grob und zu weit gefasst und verwies auf gesunkene Betrugsmeldungen. Nach dem Bedrohungsbericht von Gen Digital für das vierte Quartal 2025 entfielen 78 Prozent aller blockierten Betrugsklicks in sozialen Netzwerken auf Facebook; über 159.000 Betrugsvideos nutzten KI-erzeugte Gesichter und Stimmen.[16]

WhatsApp: Metadaten statt Inhalte

Für Einsteiger:

Viele Menschen nutzen WhatsApp, weil es kostenlos ist und ihre Nachrichten verschlüsselt. Das stimmt, niemand kann Ihre Nachrichten lesen. Aber WhatsApp gehört zu Meta (Facebook), und Meta sammelt trotzdem wertvolle Informationen: nicht den Inhalt Ihrer Nachrichten, aber alles darüber, wer Sie wann, wie oft und von wo aus anschreiben. Das klingt harmlos, ist es aber nicht: Aus diesen sogenannten Metadaten lässt sich erschreckend viel über eine Person herausfinden.

Technischer Hintergrund

Mit über drei Milliarden monatlichen Nutzern weltweit (Meta, Mai 2025) ist WhatsApp die meistgenutzte Messaging-Applikation der Welt. Die App wurde 2009 gegründet und 2014 für 19 Milliarden US-Dollar von Facebook (heute Meta) übernommen, damals eine der teuersten Technologie-Akquisitionen der Geschichte. Seitdem ist der Datenschutzstatus der App kontinuierlich umstrittener geworden.[17]

Technisch sind die eigentlichen Nachrichteninhalte durch Ende-zu-Ende-Verschlüsselung geschützt. Meta kann den Inhalt von Nachrichten nicht lesen. Was Meta jedoch sehr wohl liest und nutzt, sind die Metadaten: Wer kommuniziert mit wem? Wie oft? Zu welchen Uhrzeiten? Von welchem Standort aus? Mit welchem Gerät? In welchem Land? Wie groß sind die übermittelten Dateien? Diese Metadaten sind im Kontext einer Massenüberwachung oft wertvoller als der eigentliche Inhalt, denn sie verraten soziale Netzwerke, Gewohnheiten und Verhaltensweisen.

[15] Meta Newsroom: Restricting data access on Facebook, 4. April 2018 (87 Millionen Betroffene). Frasco v. Flo Health, N.D. Cal., Geschworenenurteil vom 1. August 2025 (Meta haftbar nach California Invasion of Privacy Act); Schadenshöhe offen, Anhörung 29. Oktober 2026. HIPAA Journal: Five healthcare providers pixel class action settlements, 7. August 2026 (Penn Medicine 9,5 Mio. USD, Concord Hospital 800.000 USD, Mount Sinai Florida 220.000 USD); Atrium Health 1,8 Mio. USD, Juli 2026.

[16] Gen Digital: Threat Report Q4/2025, 20. Januar 2026; Gen Digital: Analyse betrügerischer Anzeigen auf Meta-Plattformen in der EU, 2026. Reuters: Meta is earning a fortune on a deluge of fraudulent ads, documents show, 6. November 2025 (mit Stellungnahme von Meta). Sauer, H.: Jede vierte Anzeige auf Facebook ist Betrug, FOCUS Online, Februar 2026.

[17] Meta Platforms Inc.: Acquisition of WhatsApp Inc., Pressemitteilung 19. Februar 2014. Meta: Q1 2025 Earnings Call, 30. April 2025 (über 3 Milliarden monatliche Nutzer).

Im Dezember 2025 berichtete der Autor in CHIP Online über einen wenig bekannten, aber kritischen Aspekt: WhatsApp-Nutzer nach dieser Analyse des Autors auch dann erfasst werden, wenn sie kein Facebook-Konto besitzen: Die App übermittelt demnach regelmäßig Geräte-Fingerprint-Daten an Meta-Server, die eine Wiedererkennung des Geräts auch ohne explizite Anmeldedaten ermöglichen. Nach denselben Beobachtungen können gelöschte Nachrichten Metadaten-Spuren hinterlassen, die über Monate auf Meta-Servern verbleiben.[18]

Welche dieser Daten WhatsApp an den Mutterkonzern weitergibt, steht in der Datenschutzerklärung: Telefonnummer, Gerätekennungen, Hardwaremodell, Betriebssystem, Mobilfunknetz, Zeitpunkt der letzten Nutzung, Registrierungsdatum und Aktivitätszeiten, offiziell zu Zwecken wie Infrastruktur, Analyse und Sicherheit. Für Werbung dürfen andere Meta-Dienste diese Daten nach Angaben von WhatsApp nur nutzen, wenn der Nutzer sein WhatsApp-Konto freiwillig mit dem „Accounts Center“ verknüpft hat. Nachrichten mit Unternehmen, die Metas Cloud-Schnittstelle nutzen, gelten laut WhatsApp nicht als Ende-zu-Ende-verschlüsselt. Die irische Datenschutzbehörde verhängte 2021 wegen intransparenter Information über genau diese Datenflüsse 225 Millionen Euro Bußgeld.

Seit Juni 2025 zeigt WhatsApp Werbung, im Reiter „Aktuelles“ zwischen Status-Meldungen und Kanälen. Ausgewertet werden dafür laut WhatsApp Land oder Stadt, Sprache, abonnierte Kanäle und die Reaktion auf bisherige Anzeigen, bei verknüpftem Accounts Center zusätzlich die Werbepräferenzen aus den anderen Meta-Konten; Nachrichteninhalte, Anrufe und Gruppenmitgliedschaften sollen ausdrücklich nicht einfließen. In der EU verzögerte die irische Datenschutzbehörde den Start bis 2026 und setzte Änderungen durch, etwa strengere Beschränkungen für Nutzer ohne Altersnachweis. Parallel ist Meta AI in WhatsApp eingebaut: Gespräche mit dem Assistenten sind nicht Ende-zu-Ende-verschlüsselt und dienen Meta als Trainingsmaterial; erst im Mai 2026 kündigte Meta einen „Inkognito-Chat“ mit Meta AI an, der verschlüsselt, nicht gespeichert und nicht zum Training genutzt werden soll. Der Kern bleibt: WhatsApp verkauft keine Daten, es macht Meta reicher an Wissen über zwei Milliarden Beziehungsnetze.[19]

Die Firma Acxiom

Für Einsteiger:

Die meisten Menschen haben noch nie von Acxiom gehört, und genau das ist das Problem. Acxiom ist eines der größten Datensammelunternehmen der Welt und verfügt über detaillierte Profile von Milliarden Menschen. Das Unternehmen arbeitet unsichtbar im Hintergrund: Es kauft Daten von Einzelhändlern, Kreditkartenunternehmen und Online-Portalen, kombiniert sie zu umfassenden Persönlichkeitsprofilen und verkauft sie weiter. Ihr Name steht in keinem Nutzungsvertrag, dem Sie jemals zugestimmt haben, aber Acxiom weiß trotzdem, wer Sie sind.

[18] Hermann Sauer in CHIP Online: „So einfach werden WhatsApp-Nutzer ausspioniert, ohne es zu merken", 19. Dezember 2025. CHIP ist eine der meistgelesenen Technikpublikationen Deutschlands.

[19] WhatsApp: Datenschutzrichtlinie (EWR), Fassung 2. Juli 2026, Abschnitt „Wie wir mit anderen Meta-Unternehmen zusammenarbeiten“; WhatsApp: Privacy Questions (whatsapp.com/privacyquestions). Irish Data Protection Commission: Decision on WhatsApp Ireland, 2. September 2021 (225 Mio. Euro). WhatsApp Blog: Helping you find more channels and businesses on WhatsApp, 16. Juni 2025. Silicon Republic: WhatsApp ads in EU delayed to 2026, 19. Juni 2025; Delayed WhatsApp ads to go ahead in Ireland, 21. Mai 2026. Meta Newsroom: Introducing a Completely Private Way to Chat With AI, 13. Mai 2026.

Technischer Hintergrund

Acxiom ist einer der ältesten und größten Datenhändler der Welt. Mit Hauptsitz in Conway, Arkansas, sammelt das Unternehmen seit den 1960er Jahren Daten über Konsumenten, zunächst aus Postkatalogen, Haushaltsbefragungen und öffentlichen Registern, heute aus tausenden digitaler und analoger Quellen. Acxiom wirbt (Stand 2026) mit einer „globalen Zielgruppe“ von 2,6 Milliarden Menschen, 260 Millionen digital adressierbaren US-Konsumenten und mehr als 10.000 Merkmalen je Person. Das Unternehmen wurde 2018 für 2,3 Milliarden US-Dollar von der Interpublic Group (IPG) übernommen und firmiert seitdem als Acxiom LLC unter dem IPG-Dach.[20]

Besonders problematisch ist die Verflechtung von Acxiom mit scheinbar unabhängigen Diensten. Acxiom kooperiert seit Jahren mit Immobilienportalen, Kreditkartenunternehmen, Einzelhändlern und sogar Behörden. Die in solchen Portalen gesammelten Daten über das Interesse am Kauf oder der Miete von Wohnungen flossen nach den Recherchen von Cracked Labs direkt an Acxiom; bis zur Einstellung der „Partner Categories“ 2018 lieferte auch Facebook Daten an Acxiom. Das Ergebnis ist ein umfassendes Lebensprofil: Wohnort, Einkommenssituation, Kaufgewohnheiten, politische Neigungen, Gesundheitszustand, Familienstand und Religionszugehörigkeit.

Acxiom vermarktet seine Daten über das Produkt „Real Identity" und bietet Werbetreibenden die Möglichkeit, einzelne Personen geräteübergreifend zu verfolgen, also über Smartphone, Tablet, Laptop und Smart-TV hinweg als dieselbe Person zu identifizieren. Dies ist möglich, weil Acxiom die Online-Identifikatoren (Cookies, Device IDs) mit Offline-Daten (Name, Adresse, Telefonnummer) verknüpft, die aus Kauftransaktionen, Kundenkarten und öffentlichen Registern stammen.[21]

Verknüpfung von Online- und Offline-Daten

Für Einsteiger:

Datenhändler begnügen sich nicht mit dem, was Sie im Internet tun. Sie kombinieren Online-Daten mit Informationen aus dem echten Leben: Was kaufen Sie im Supermarkt (Kundenkarte)? Mit welcher Kreditkarte zahlen Sie? Wo wohnen Sie? Diese Kombination ergibt ein Bild von Ihnen, das weit über das hinausgeht, was Sie je bewusst preisgegeben haben. Und selbst wenn Daten angeblich "anonym" sind, zeigt die Wissenschaft: Die meisten Menschen lassen sich trotzdem eindeutig identifizieren.

Daten-Aggregation und Re-Identifizierung

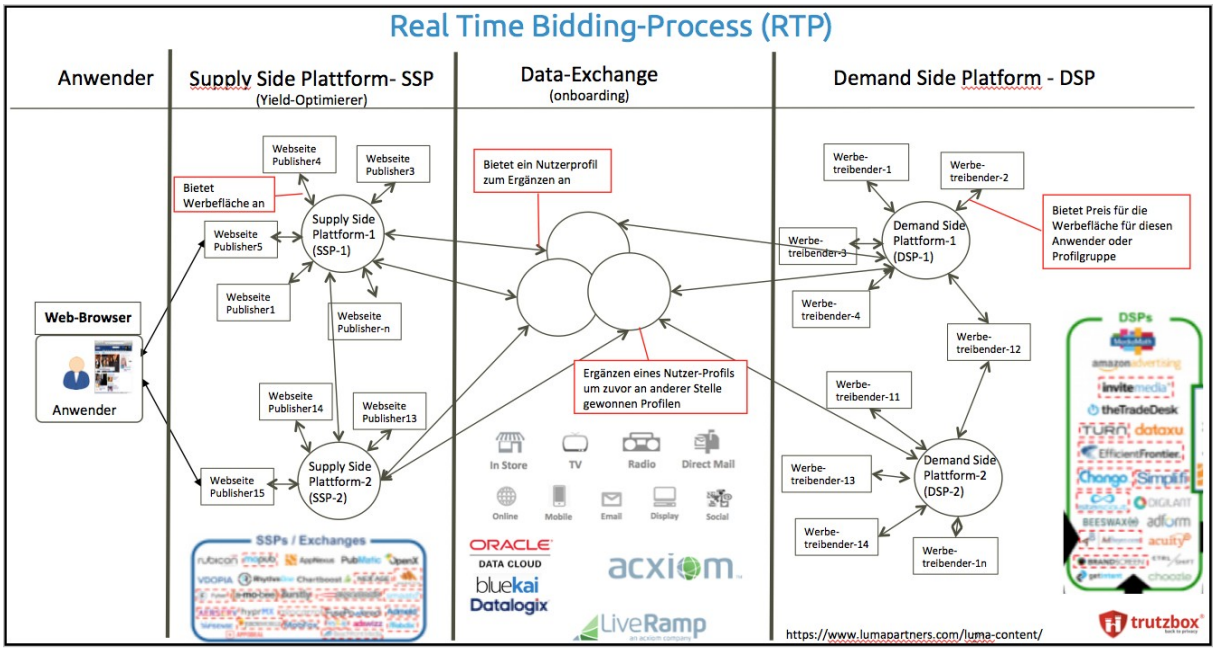
Die vielleicht unterschätzteste Dimension des modernen Datenhandels ist die Verknüpfung von Online-Verhalten mit Offline-Daten. Datenhändler wie Acxiom, LiveRamp und die in den Databroker Files beschriebenen Akteure begnügen sich nicht mit den Daten, die Menschen im Internet hinterlassen. Sie kombinieren digitale Spuren mit einem breiten Spektrum analoger Informationen: Einkaufsgewohnheiten aus Kundenkarten- und Bonusprogrammen, Kreditkartentransaktionen, Daten aus öffentlichen Registern (in Deutschland begrenzt verfügbar, in den USA deutlich umfangreicher), Umfrageantworten,

[20] Acxiom: Customer Data, acxiom.com/customer-data (abgerufen September 2026). Zur Übernahme durch IPG: Interpublic Group: IPG Acquires Acxiom Marketing Solutions, Pressemitteilung 2018.

[21] Wolfie Christl / Cracked Labs: Corporate Surveillance in Everyday Life. Wien 2017. Detaillierte Analyse des Acxiom-Datenmodells.

demographische Daten aus postalischen Mailings und, in jüngerer Zeit. Gesundheitsdaten aus App-Ökosystemen.

Die Rollen und Abläufe beim Onboarding im Überblick:



Der Weg eines Profils beim Onboarding: von der Webseite über Supply-Side- und Datenplattformen bis zu den Werbetreibenden.
(© 2026 Comidio GmbH)

Die Lüge von "anonymen Daten"

Ein häufig verwendetes Gegenargument der Datenhändler-Industrie lautet: „Unsere Daten sind anonymisiert." In der Praxis ist diese Behauptung in der überwältigenden Mehrheit der Fälle falsch oder zumindest irreführend. Wissenschaftliche Studien haben wiederholt gezeigt, dass vermeintlich anonymisierte Datensätze mit erschreckend geringem Aufwand re-identifiziert werden können.[22]

Eine wegweisende Studie im Fachmagazin Nature Communications (Rocher et al., 2019) zeigte, wie brüchig Anonymisierung sein kann: In einer Modellrechnung für die US-Bevölkerung ließen sich 99,98 Prozent der Personen anhand von nur 15 demographischen Attributen eindeutig zuordnen; nach einer früheren Studie (de Montjoye et al., 2013) genügen bereits vier räumlich-zeitliche Datenpunkte, um 95 Prozent der Personen in Mobilfunkdaten zu identifizieren. Das bedeutet: Vier Informationen wie „war am Montag um 8:30 Uhr an Adresse A" und „war am Dienstag um 17:15 Uhr an Adresse B" reichen aus, um eine Person in einem vermeintlich anonymen Datensatz zu finden.[23]

Die Databroker Files lieferten den praktischen Beweis in Deutschland: Ein Datensatz mit 3,6 Milliarden Einträgen, der angeblich nur Werbe-IDs und GPS-Koordinaten enthielt, keine Namen, keine Telefonnummern, keine E-Mail-Adressen, reichte aus, um konkrete Mitarbeiter von Bundesministerien

[22] Ohm, P.: Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization. UCLA Law Review, 57, 1701 (2010). Grundlegende rechtswissenschaftliche Analyse der Grenzen der Anonymisierung.

[23] Rocher, L. / Hendrickx, J.M. / de Montjoye, Y.A.: Estimating the success of re-identifications in incomplete datasets using generative models. Nature Communications 10, 3069 (2019). doi:10.1038/s41467-019-10933-3

und Geheimdiensten zu identifizieren. Die Identifizierung gelang durch die Analyse von Wohnort, Arbeitsort und regelmäßig besuchten Orten. Informationen, die durch einfache Häufigkeitsanalyse der GPS-Koordinaten gewonnen wurden.

Die Firma Oracle

Für Einsteiger:

Oracle kennt kaum jemand als Marke, dabei betreibt der Konzern die Rechenzentren für Regierungen, das US-Militär, Krankenhäuser und für die größten KI-Modelle der Welt. Gründer Larry Ellison, im September 2025 kurzzeitig reichster Mensch der Erde, hält 40 Prozent an Oracle. Sein Sohn David kontrolliert den Medienkonzern Paramount Skydance mit CBS und CBS News und hat den Kaufvertrag für Warner Bros. Discovery (CNN, HBO) unterschrieben; Oracle hält 15 Prozent am US-amerikanischen TikTok und betreibt dessen Server. Wer die Leitungen, die Sender und die Plattform besitzt, braucht keine Daten mehr zu kaufen.

Technischer Hintergrund

Oracle, gegründet von Larry Ellison, der im September 2025 temporär Elon Musk als reichsten Menschen der Welt überholte, hat sich vom Datenbanksoftware-Hersteller zu einem der einflussreichsten Daten- und Medienkonzerne der USA entwickelt. Oracles Kerngeschäft ist Cloud-Infrastruktur und Datenmanagement für Regierungen, Militär, Krankenhäuser und Privatunternehmen. Bis 2024 kamen Datenbrokerdienste hinzu: Die Oracle Data Cloud (aufgebaut durch Akquisitionen von BlueKai 2014, Datalogix 2014 und Moat 2017) verfügte über Datenprofile zu über 300 Millionen Konsumenten in den USA und Europa. Im Juni 2024 kündigte Oracle das Ende seines Werbe- und Datengeschäfts an; zum 30. September 2024 wurde die Oracle Data Cloud eingestellt.[24]

Im August 2024 einigte sich Oracle auf einen Vergleich über 115 Millionen US-Dollar in einem US-Sammelklageverfahren, das dem Unternehmen vorwarf, Nutzerdaten ohne hinreichende Einwilligung gesammelt und an Dritte verkauft zu haben; das Berufungsgericht bestätigte den Vergleich im Februar 2026, die Auszahlungen laufen seit September 2026. Eine Pflicht, die gesammelten Profile zu löschen, enthält der Vergleich nicht.[25]

Was aus den Datenbeständen geworden ist, hat Oracle nie vollständig offengelegt. Das Werbegeschäft setzte zuletzt noch rund 300 Millionen US-Dollar im Jahr um und passte, so Konzernchefin Safra Catz, „nicht mehr zur strategischen Vision“. Versuche, BlueKai und Datalogix zu verkaufen, fanden Branchenberichten zufolge keinen Käufer; die Produkte wurden abgeschaltet, nicht veräußert. In den Abschaltungs-Hinweisen an Kunden hieß es, Oracle beende die Verträge mit Datenlieferanten, bewahre Daten „gemäß Vertragsbedingungen“ zur Abholung und für Rechtsstreitigkeiten auf und lösche sie, „sobald diese Pflichten erfüllt sind“, ohne Datum, ohne unabhängige Prüfung und ohne Aussage zu den Kernbeständen, dem „ID Graph“ mit den verknüpften Identitäten von Hunderten Millionen Menschen.

[24] Oracle Corporation: Investor Relations. Acquisition History 2014 bis 2019. Oracle: Q4 FY2024 Earnings Call, 11. Juni 2024 (Ankündigung der Einstellung von Oracle Advertising zum 30. September 2024). Forbes Billionaires List: Larry Ellison, September 2025.

[25] US District Court, Northern District of California: Katz-Lacabe et al. v. Oracle America, Inc., Case No. 3:22-cv-04792, Settlement Agreement August 2024.

Die Mitarbeiter wechselten zu Wettbewerbern wie Integral Ad Science und DoubleVerify. Ob die Profile heute noch existieren, weiß außerhalb von Oracle niemand.[26]

Oracle und TikTok: Kontrolle über den US-Algorithmus

Im Januar 2026 wurde das Joint Venture „TikTok USDS LLC“ formell gegründet, um die US-Geschäfte von TikTok von der chinesischen Muttergesellschaft ByteDance abzuspalten, auf Basis des US-Bundesgesetzes Protecting Americans from Foreign Adversary Controlled Applications Act (2024), das ByteDance verpflichtete, die Mehrheitskontrolle abzugeben. Oracle, Silver Lake und das Abu-Dhabi-Investmentvehikel MGX halten jeweils 15 Prozent des Joint Ventures. ByteDance behält 19,9 Prozent; die verbleibenden 30,1 Prozent halten bestehende ByteDance-Investoren. Das Gesamtvolumen des Deals beträgt rund 14 Milliarden US-Dollar.[27]

Oracle übernimmt die zentrale Kontrollrolle im Joint Venture: Der Konzern hostet alle Nutzerdaten amerikanischer TikTok-Nutzer auf US-Servern, überwacht den Empfehlungsalgorithmus und validiert als „Trusted Security Partner“ die Einhaltung der vereinbarten nationalen Sicherheitsanforderungen. Der TikTok-Algorithmus soll ausschließlich mit US-Nutzerdaten neu trainiert werden. Die Content-Moderation für den US-Markt, also die Entscheidung darüber, welche Inhalte für amerikanische Nutzer sichtbar sind, liegt beim neuen Joint Venture unter Oracles Aufsicht.[28]

Larry und David Ellison: Aufbau eines Medienimperiums

Parallel zum TikTok-Deal baute die Familie Ellison in kurzer Zeit eines der größten Medienimperien der USA auf, in enger Verbindung mit der Trump-Administration. Im Sommer 2025 übernahm die von David Ellison (Sohn von Larry Ellison) geführte Produktionsfirma Skydance den Medienkonzern Paramount für rund acht Milliarden US-Dollar. Paramount umfasst CBS News, MTV, Nickelodeon, Paramount Pictures und den Streamingdienst Paramount+. Die New York Times berichtete im September 2025, dass Larry Ellison, entgegen der offiziellen Darstellung, die tatsächliche Entscheidungskontrolle bei Skydance inne hat.[29]

Zusätzlich gab Paramount Skydance eine feindliche Übernahmeofferte für Warner Bros. Discovery (WBD) in Höhe von 108 Milliarden US-Dollar ab, für die Larry Ellison eine persönliche Finanzgarantie von rund 40 Milliarden Dollar übernahm. Warner Bros. Discovery umfasst CNN, HBO und DC Studios. Der WBD-Vorstand empfahl zunächst das Konkurrenzangebot von Netflix; nachdem Paramount Skydance sein Angebot im Februar 2026 auf 31 Dollar je Aktie erhöht hatte, zog Netflix zurück, und Warner Bros. Discovery unterzeichnete den Fusionsvertrag mit Paramount Skydance. Der Kaufpreis von

[26] Oracle: Q4 FY2024 Earnings Call, 11. Juni 2024 (Safra Catz zum Werbegeschäft). AdExchanger: Inside the Fall of Oracle’s Advertising Business, 1. Juli 2024 (Verkaufsversuche ohne Käufer). Oracle: Advertising End of Life FAQ, Version 3.0, 12. August 2024 (oracle.com/a/ocom/docs/oracle-advertising-end-of-life-faqs.pdf). Digiday: As Oracle Advertising nears shutdown deadline, ad tech companies are competing to recruit its staff, 12. September 2024. Katz-Lacabe v. Oracle America: Detailed Notice, Frage 14 (keine Löschpflicht).

[27] TikTok-CEO Shou Zi Chew: Internes Memo, Dezember 2025, zitiert von ABC News und Axios. Bloomberg: TikTok signs deal to create new US joint venture, Dezember 2025. Benzinga: Oracle, Silver Lake and MGX will each hold 15%, Januar 2026.

[28] NPR: TikTok signs deal to give U.S. operations to Oracle-led investor group, Dezember 2025. ABC News: TikTok signs deal to create new US joint venture, Dezember 2025. CNBC: Oracle stock jumps 7% as cloud provider joins investor group, Dezember 2025.

[29] Meedia / KNA-Mediendienst: Rückblick. Wie Larry und David Ellison ein Trump-nahes Medienimperium aufbauen, Januar 2026. New York Times: The Real Power Behind Skydance Is Larry Ellison, September 2025.

31 Dollar je Aktie entspricht einem Unternehmenswert von rund 110 Milliarden US-Dollar; 47 Milliarden Eigenkapital stellen die Familie Ellison, der Investor RedBird und, mit rund 24 Milliarden. Staatsfonds aus Saudi-Arabien, Katar und den Emiraten. Das US-Justizministerium, die EU-Kommission und die britische Wettbewerbsbehörde gaben die Übernahme im Sommer 2026 frei. Vollzogen ist sie dennoch nicht: Zwölf demokratisch regierte US-Bundesstaaten unter Führung Kaliforniens klagten im Juli 2026 wegen Wettbewerbsbedenken, ein Bundesgericht stoppte den Abschluss per einstweiliger Verfügung; Paramount verpflichtete sich, nicht vor einem Urteil zu vollziehen, der Prozess ist für März 2027 angesetzt. Im Oktober 2025 kaufte Paramount Skydance für rund 150 Millionen US-Dollar das Onlineportal The Free Press und machte dessen Gründerin Bari Weiss zur Chefredakteurin von CBS News, ein neu geschaffener Posten, der direkt an David Ellison berichtet. Zuvor hatte Paramount 16 Millionen US-Dollar an Donald Trumps Präsidentenbibliothek gezahlt, um dessen Klage gegen ein „60 Minutes“-Interview beizulegen; drei Wochen später genehmigte die FCC die Skydance-Übernahme.[30]

Der Medienhistoriker Michael Socolow von der University of Maine ordnete die Entwicklung gegenüber NPR so ein: „Das Potenzial, Amerikaner zu beeinflussen, wenn man CBS News, TikTok und eines Tages CNN besitzt, ist in der Geschichte ohne Beispiel.“ Larry Ellison äußerte in einer Investorenansprache seine Vision einer vollständig überwachten Gesellschaft: „Bürger werden sich am besten verhalten, weil wir alles aufzeichnen und berichten, was vorgeht, und Oracle wird der Verwalter all dieser Daten sein.“[31] (Äußerung auf einem Oracle-Finanzanalystentreffen im September 2024, u. a. dokumentiert von Business Insider.)

Das Imperium der Familie Ellison in Zahlen (Stand September 2026): Oracle erzielte im Geschäftsjahr bis Mai 2026 einen Umsatz von 67 Milliarden US-Dollar mit 141.000 Beschäftigten; Larry Ellison hält 40,6 Prozent der Aktien, von denen er 346 Millionen als Kreditsicherheit verpfändet hat. Der Börsenwert schwankte innerhalb eines Jahres zwischen über 900 Milliarden (September 2025) und rund 430 Milliarden US-Dollar (September 2026); der Auftragsbestand von 638 Milliarden US-Dollar stammt überwiegend aus KI-Rechenzentrumsverträgen, allein OpenAI soll Berichten zufolge über 300 Milliarden zugesagt haben. Im Juli 2026 schloss das US-Verteidigungsministerium mit Oracle einen Softwarerahmenvertrag über bis zu 7 Milliarden US-Dollar für Pentagon, Geheimdienste und Küstenwache. Paramount Skydance (Umsatz 2025: 29 Milliarden US-Dollar, Börsenwert rund 12 Milliarden) wird zu 77,5 Prozent der Stimmrechte von der Familie kontrolliert; David Ellison ist Verwaltungsratsvorsitzender und Vorstandschef. Am TikTok-Joint-Venture hält Oracle 15 Prozent und einen von sieben Verwaltungsratssitzen, ist aber als „Trusted Security Partner“ der Betreiber: Es hostet die Daten aller US-Nutzer und trainiert den Empfehlungsalgorithmus neu. Larry Ellisons Privatvermögen beziffert Forbes im September 2026 auf 188 Milliarden US-Dollar; hinzu kommen die Hawaii-Insel Lanai, die er 2012 zu 98 Prozent kaufte, das Ellison Institute of Technology in Oxford und eine Milliardenbeteiligung an Elon Musks SpaceX, die aus seinem Einstieg bei Twitter hervorging.[32]

---

[30] Meedia / KNA: Ellison-Medienimperium, Januar 2026. NPR: Who is Larry Ellison, the billionaire Trump friend, Oktober 2025. Paramount Skydance: Paramount to acquire Warner Bros. Discovery, 27. Februar 2026 (31 USD je Aktie, 47 Mrd. USD Eigenkapital, 54 Mrd. USD Fremdkapital); CNBC: Paramount agrees to delay WBD merger close, 24. Juli 2026; NPR: Judge grants restraining order in states’ suit against Paramount-WBD, 20. Juli 2026. Bloomberg / Axios: Paramount buys The Free Press, names Bari Weiss CBS News chief, 6. Oktober 2025. CNN: Paramount settles Trump 60 Minutes lawsuit for 16 million, 2. Juli 2025; FCC: FCC approves Skydance’s acquisition of Paramount, 24. Juli 2025.

[31] NPR: Who is Larry Ellison, the billionaire Trump friend who’s part of the TikTok takeover, Oktober 2025. Larry Ellison: Remarks to Oracle investors, zitiert in NPR und Naked Capitalism, 2025.

[32] Oracle: Q4 and FY2026 Results, 10. Juni 2026 (Umsatz 67,4 Mrd. USD, Auftragsbestand 638 Mrd. USD); Oracle Form 10-K FY2026 (141.000 Beschäftigte); Oracle Proxy Statement 2025, 26. September 2025 (40,6 Prozent, 346 Mio. verpfändete Aktien). Wall Street Journal: OpenAI,Oracle-Vertrag über rund 300 Mrd. USD, 10. September 2025. Federal News Network: DoD awards Oracle software deal worth up to 7 billion, 24. Juli 2026. Paramount Skydance: Form 10-Q Q1 2026 (77,5 Prozent der Stimmrechte); Form 8-K, 25. Februar 2026 (Umsatz 2025: 29,2 Mrd. USD). TikTok Newsroom: Announcement from the new TikTok USDS Joint Venture LLC, 23. Januar 2026 (Eigentümer, Verwaltungsrat, Rolle Oracles). Forbes: Profil Larry Ellison, abgerufen 3. September 2026 (188,5 Mrd. USD). Bloomberg:

Die politische Nähe ist dokumentiert: Das Wall Street Journal berichtete 2026 über eine nicht offenlegungspflichtige Spende von 45 Millionen US-Dollar an eine Trump-nahe Organisation im Wahlkampf 2024; im Januar 2025 stand Ellison neben Trump, als im Weißen Haus das 500-Milliarden-Rechenzentrumsprojekt „Stargate“ mit OpenAI vorgestellt wurde; im März 2026 berief Trump ihn und Oracle-Chefin Safra Catz in den wissenschaftlichen Beraterrat des Präsidenten. Datenschutzrechtlich ist entscheidend: Wer die Server von TikTok, die Cloud der Regierung, die Rechenzentren der KI-Anbieter und einen der größten Fernsehkonzerne der USA kontrolliert, muss keine Datenhändler-Profile mehr kaufen, er sitzt an der Quelle.[33]

Datenmacht und Medienmacht: Die Ellison-Konstellation

Oracle hostet die Daten von über 170 Millionen US-TikTok-Nutzern und trainiert den Empfehlungsalgorithmus der meistgenutzten Kurzvideoapp der USA neu. Gleichzeitig kontrolliert die Familie Ellison über Paramount Skydance den Fernsehsender CBS News und hat den Kaufvertrag für Warner Bros. Discovery (CNN, HBO) unterzeichnet, der Vollzug ist bis zu einem Gerichtsurteil über die Klage von zwölf US-Bundesstaaten ausgesetzt (Prozess März 2027). Hinweis: Die medienrechtliche, wettbewerbsrechtliche und datenschutzrechtliche Bewertung dieser Konstellation obliegt den zuständigen Behörden, darunter FCC, Department of Justice und europäische Datenschutzbehörden.

Die Firma Alphabet (Google)

Für Einsteiger:

Google-Suche ist kostenlos, aber diesen Preis zahlen Sie mit Ihren Daten. Google verdient fast sein gesamtes Geld mit Werbung. Dafür braucht es möglichst genaue Informationen darüber, wer Sie sind und was Sie wollen. Da Google die Suchmaschine, YouTube, Gmail, Maps, den Chrome-Browser und das Android-Betriebssystem betreibt, kennt es Sie besser als jedes andere Unternehmen weltweit, und möglicherweise besser als Sie sich selbst.

Technischer Hintergrund

Google, heute Teil des Alphabet-Konzerns mit einem Börsenwert von rund vier Billionen US-Dollar (Mitte 2026), ist das wohl bekannteste und einflussreichste Beispiel für ein Unternehmen, dessen Geschäftsmodell vollständig auf der Verwertung von Nutzerdaten basiert. Die Suchmaschine, die täglich von Milliarden Menschen genutzt wird, ist dabei nur der offensichtlichste Datenpunkt. Google betreibt darüber hinaus das größte Werbenetzwerk der Welt (Google Ads und Google Display Network), YouTube mit nach eigenen Angaben „Milliarden“ monatlich angemeldeten Nutzern, Gmail mit drei Milliarden Nutzern (Google, Januar 2026), Google Maps, das auf praktisch allen Android-Smartphones vorinstalliert ist, sowie das Android-Betriebssystem, das auf über drei Milliarden Geräten weltweit läuft.[34]

Twitter backers’ patience repaid with 100 billion SpaceX stake, 15. Mai 2026.

[33] Fortune / Wall Street Journal: Larry Ellison’s 45 million donation, 25. Juni 2026. Washington Post: Trump announces Stargate, 21. Januar 2025. The White House: President Trump announces appointments to the President’s Council of Advisors on Science and Technology, 25. März 2026.

[34] Google: Gmail, „3 billion users“, Blog 8. Januar 2026; Google I/O 2025: über 3 Milliarden aktive Android-Geräte; YouTube Presseseite: „billions of monthly logged-in users“; Alphabet-Börsenwert ca. 4,1 Bio. USD (September 2026).

Google Analytics ist auf knapp der Hälfte aller Websites installiert (W3Techs, September 2026: 47,6 Prozent, über 80 Prozent Marktanteil unter Analysewerkzeugen); irgendein Google-Tracker findet sich auf 61 Prozent aller Webseiten (Web Almanac 2025). Google Analytics übermittelt bei jedem Seitenaufruf Nutzerdaten an Google, unabhängig davon, ob der Nutzer ein Google-Konto hat.[35]

Die Kombination all dieser Datenpunkte ermöglicht es Google, ein Profil zu erstellen, das jeden anderen Datenhändler in den Schatten stellt. Google weiß, wonach Menschen suchen (Suchmaschine), was sie sich ansehen (YouTube), mit wem und worüber sie kommunizieren (Gmail), wo sie sich bewegen (Maps), welche Apps sie nutzen (Android), wie sie surfen (Chrome) und was sie kaufen (Google Pay). Hinzu kommt Google Analytics auf Websites, das selbst auf Seiten Daten sammelt, die kein Google-Produkt anbieten.

Auch Google wurde in Europa bereits mehrfach mit Bußgeldern belegt, datenschutzrechtlich im dreistelligen Millionenbereich, kartellrechtlich sogar in Milliardenhöhe. Die französische Datenschutzbehörde CNIL verhängte 2019 eine Buße von 50 Millionen Euro wegen unzureichender Transparenz bei der Datenverarbeitung. Im Januar 2022 folgten weitere 150 Millionen Euro wegen mangelhafter Cookie-Einwilligungsimplementierung. Im September 2025 folgten 325 Millionen Euro, weil Google Werbung zwischen Gmail-Nachrichten platziert und bei der Kontoerstellung Cookies ohne wirksame Einwilligung gesetzt hatte. Kartellrechtlich verhängte die EU-Kommission im September 2025 2,95 Milliarden Euro für die Bevorzugung der eigenen Werbetechnik und im Juli 2026 890 Millionen Euro nach dem Digital Markets Act; im Juli 2026 bestätigte der Europäische Gerichtshof zudem endgültig die Android-Strafe von 4,1 Milliarden Euro. Trotz dieser Strafen hat sich das Kerngeschäftsmodell nicht geändert.[36]

Die Firma Microsoft: Vom Software-Konzern zum Datenmarktplatz-Betreiber

Für Einsteiger:

Microsoft kennen die meisten als Hersteller von Windows und Office. Doch Microsoft ist durch eine Reihe strategischer Käufe und Produktentscheidungen zu einem der global einflussreichsten Datensammler geworden, oft unbemerkt, weil die Datenerhebung im Hintergrund der vertrauten Software stattfindet. Windows sendet Telemetriedaten. LinkedIn trackt Berufsbiographien. Bing analysiert Suchanfragen. Und seit der Übernahme von Xandr betreibt Microsoft einen der größten Werbe-Datenmarktplätze der Welt.

Microsoft-Datenerhebung: Windows, LinkedIn, Bing, Teams, Xandr

Microsoft ist im Bereich Datenerhebung ein Akteur, der in der öffentlichen Wahrnehmung häufig hinter Google und Meta zurückbleibt, obwohl das Unternehmen über ein ebenso umfangreiches Datenökosystem verfügt. Die wichtigsten Datenquellen im Überblick:[37]

[35] W3Techs: Usage Statistics and Market Share of Traffic Analysis Tools, September 2026. HTTP Archive: Web Almanac 2025, Kapitel Privacy, Januar 2026. https://w3techs.com/technologies/overview/traffic_analysis

[36] CNIL (Commission Nationale de l'Informatique et des Libertés): Délibération SAN-2019-001 du 21 janvier 2019 (Google LLC); Délibération SAN-2022-001 (Januar 2022). CNIL-Pressemitteilungen 2019 und 2022; CNIL: Google fined 325 million euros, 1. September 2025. https://www.cnil.fr. Europäische Kommission: IP/25/1992, 5. September 2025 (2,95 Mrd. Euro Adtech); IP/26/1670, 23. Juli 2026 (890 Mio. Euro DMA). EuGH, Urteil vom 2. Juli 2026, C-738/22 P (Android, 4,125 Mrd. Euro).

[37] BSI: SiSyPHuS Win10. Analyse der Telemetriekomponente in Windows 10, 2018/2019. Microsoft: Privacy Statement. https://privacy.microsoft.com

- Windows-Telemetrie: Windows 10 und Windows 11 senden standardmäßig umfangreiche Telemetriedaten an Microsoft-Server. Dazu gehören Informationen über installierte Software, Hardwarekonfiguration, Nutzungsverhalten, Absturzdaten und, bei aktivierter Diagnosedaten-Einstellung „Vollständig", auch Browserverläufe aus Microsoft Edge. Das BSI hat in einer öffentlich zugänglichen Analyse dokumentiert, dass selbst bei der niedrigsten Datenschutzstufe (Sicherheit) Verbindungen zu Microsoft-Servern aufgebaut werden.[38]
- Microsoft Edge: Der Browser Edge übermittelt aufgerufene URLs an Microsoft-Server, auch dann, wenn der Nutzer nicht eingeloggt ist. Heise Online und der Sicherheitsexperte Rafael Rivera dokumentierten 2023, dass Edge im Hintergrund Seiten-URLs an den Microsoft-Dienst „SmartScreen" und an Bing übermittelt.[39]
- LinkedIn: Microsoft übernahm LinkedIn 2016 für 26,2 Milliarden US-Dollar. LinkedIn verfügt über berufliche Profile von über 1,3 Milliarden Mitgliedern weltweit (Microsoft, April 2026), mit Angaben zu Arbeitgeber, Position, Karriereverlauf, Ausbildung, Fähigkeiten und beruflichem Netzwerk. LinkedIn-Tracker sind auf Millionen von Unternehmenswebsites eingebunden und ermöglichen Microsoft, das berufliche Surfverhalten von Nutzern auch außerhalb von LinkedIn zu verfolgen.[40]
- Microsoft Teams und Office 365: Über die Nutzung von Microsoft-Cloud-Diensten wie Teams, Outlook.com und SharePoint sammelt Microsoft umfangreiche Metadaten: Kommunikationshäufigkeit, Dokumentenbearbeitung, Meetingverhalten und kollaborative Muster. Diese Daten werden nach eigenen Angaben für den Dienst „Microsoft Viva Insights" (früher MyAnalytics) genutzt, der Arbeitsgewohnheiten analysiert.[41]
- Bing und MSN: Die Suchmaschine Bing und das Nachrichtenportal MSN (mit über 550 Millionen monatlichen Nutzern) liefern Microsoft detaillierte Suchanfragen und Leseinteressen. Bing-Tracking ist zudem über das Bing Ads-Netzwerk auf Tausenden von Partnerwebsites eingebunden.[42]
- Xandr als Datenmarktplatz: Mit der Übernahme von Xandr (2022, ca. 1 Milliarde USD) von AT&T ergänzte Microsoft sein Portfolio um einen der größten Datenmarktplätze der Online-Werbeindustrie. Über Xandr handeln 93 Datenhändler, darunter Tochterunternehmen von Telekom und ProSiebenSat1. Nutzerprofile in mehr als 650.000 Kategorien. Den Einkaufs-Marktplatz (Microsoft Invest, die frühere Xandr-DSP) hat Microsoft zum 28. Februar 2026 geschlossen; der Verkaufs-Marktplatz Microsoft Monetize und der Datenhandel über „Curate“ laufen weiter. Microsoft ist damit sowohl Betriebssystem-Hersteller, Cloud-Anbieter, Suchmaschinen-Betreiber, Social-Network-Inhaber als auch Betreiber eines kommerziellen Datenmarktplatzes in einer einzigen Unternehmensstruktur.[43]

[38] BSI: Analyse der Telemetriekomponente in Windows 10. Untersuchung der Telemetriekomponenten (Projekt SiSyPHuS Win10), 2018/2019.

[39] Heise Online: Feature mit Bug. Microsoft Edge telefoniert besuchte Seiten nach Hause, 2023. Kuketz-Blog: Microsoft Edge Datensendeverhalten, Browser-Check, 2023.

[40] Microsoft Corporation: Acquisition of LinkedIn for $26.2 Billion. Pressemitteilung 2016. Microsoft: Q3 FY2026 Earnings, 29. April 2026 (1,3 Mrd. LinkedIn-Mitglieder). LinkedIn Insight Tag. Dokumentation für Websitebetreiber.

[41] Microsoft: Microsoft Viva Insights. Product Documentation. Privacy Statement for Microsoft 365. https://learn.microsoft.com

[42] StatCounter: Search Engine Market Share 2025. Microsoft Advertising Accelerate 2025 (MSN: 550 Mio. monatlich aktive Nutzer). Microsoft Advertising: Partner Network Documentation.

[43] Microsoft: Acquisition of Xandr from AT&T. Pressemitteilung 2022. netzpolitik.org / The Markup: Xandr-Recherche, Juni 2023. Digiday / AdExchanger, 14. Mai 2025: Microsoft to shut down Microsoft Invest (Xandr DSP) by February 2026.

Microsoft 365 und die europäischen Datenschutzbehörden

Die Konferenz der deutschen Datenschutzaufsichtsbehörden (DSK) kam im November 2022 zu dem Ergebnis, dass ein datenschutzkonformer Einsatz von Microsoft 365 auf Basis der damaligen Vertragsunterlagen nicht nachgewiesen werden könne. Der Europäische Datenschutzbeauftragte (EDPS) stellte im März 2024 fest, dass die Nutzung von Microsoft 365 durch die EU-Kommission in der geprüften Form gegen die Datenschutzvorschriften für EU-Institutionen verstieß. Mehrere europäische Datenschutzbehörden (darunter Österreich, Frankreich, Italien, Schweden, Dänemark und Norwegen) haben öffentlich Bedenken hinsichtlich der Nutzung von Microsoft-Produkten in Schulen und Behörden geäußert. Hinweis: Die individuelle rechtliche Bewertung obliegt den zuständigen Datenschutzbehörden und Gerichten.

Der CLOUD Act: Warum ein Server in Europa nicht reicht

Nach dem US-amerikanischen CLOUD Act von 2018 können US-Behörden amerikanische Unternehmen zur Herausgabe von Daten verpflichten, gleichgültig, in welchem Land die Server stehen. Was das bedeutet, zeigten 2025 zwei Fälle. Im August berichteten The Guardian und die israelischen Medien +972 Magazine und Local Call, ein israelischer Militärgeheimdienst habe auf Microsoft-Azure-Servern in den Niederlanden und Irland rund 11.500 Terabyte abgehörter Telefongespräche gespeichert; Microsoft bestätigte nach eigener Prüfung Teile der Berichte und beendete bestimmte Dienste für den Kunden. Im Mai hatte Microsoft nach US-Sanktionen gegen den Internationalen Strafgerichtshof das E-Mail-Konto von dessen Chefankläger gesperrt; Microsoft-Präsident Brad Smith sagte später zu, Abschaltanordnungen gegen europäische Kunden gerichtlich anzufechten.[44]

Hinzu kommt das neue Outlook, das seit 2024 die Windows-Mail-App ersetzt: Es überträgt nach Berichten von heise online auch Zugangsdaten und Inhalte fremder Postfächer, etwa von Gmail- oder IMAP-Konten, in die Microsoft-Cloud; der Einwilligungsdialog nannte zeitweise 772 Werbepartner. Für den einzelnen Haushalt heißt das: Nicht der Speicherort entscheidet über den Zugriff, sondern der Eigentümer des Dienstes. Mail und Kommunikation auf einem Gerät im eigenen Haus unterliegen keinem ausländischen Herausgabegesetz (siehe Kapitel „Sichere E-Mail-Kommunikation“).

[44] Clarifying Lawful Overseas Use of Data Act (CLOUD Act), 2018. The Guardian / +972 Magazine / Local Call: Berichte über die Nutzung von Azure durch die Einheit 8200, August 2025; Microsoft: Stellungnahme zum Abschluss der Prüfung, September 2025. AP / heise online: Microsoft sperrt Konto des IStGH-Chefanklägers, Mai 2025. Financial Times: Zusagen von Brad Smith zu europäischen Kunden, 2025. heise online: Das neue Outlook überträgt Zugangsdaten an Microsoft, Januar 2024. Sauer, H.: Ihre Daten kennen kein Heimatland, FOCUS Online, Mai 2026.

Xandr: 650.000 Kategorien und die Anatomie des Datenmarktes

Für Einsteiger:

Im Jahr 2023 wurde ein internes Dokument eines großen Datenhändlers öffentlich: eine Liste mit über 650.000 Kategorien, in die die Werbeindustrie Menschen einsortiert. Stellen Sie sich vor, jemand hätte ein riesiges Schubladensystem gebaut, und für jede mögliche Eigenschaft eines Menschen gibt es eine Schublade. "Frau über 40 mit Brustkrebs". "Mann mit Spielsucht". "Person mit Depressionen". "Schwangere, die finanzielle Probleme hat". In diese Schubladen werden Sie einsortiert, und Werbetreibende können diese Schubladen kaufen, um gezielt Menschen in bestimmten Lebenssituationen anzusprechen. Was wie ein Marketing-Instrument klingt, ist in Wirklichkeit ein tiefer Eingriff in die Würde und Privatsphäre von Millionen Menschen.

Technischer Hintergrund

Im Juni 2023 veröffentlichten netzpolitik.org und das US-amerikanische Investigativmedium The Markup eine Recherche, die als „Snowden-Moment der Online-Werbebranche“ bezeichnet wurde. Grundlage war ein Dokument, das der Wiener Datenschutz- und Tracking-Forscher Wolfie Christl aufgespürt hatte: eine Excel-Tabelle mit mehr als 650.000 Zeilen, die bis zu ihrer Entdeckung offen auf einer Dokumentationsseite des Datenmarktplatzes Xandr abrufbar war. Jede Zeile dieser Tabelle beschreibt ein sogenanntes Zielgruppensegment, eine Kategorie, in die die Werbeindustrie Menschen einsortiert, um ihnen dann zielgerichtete Werbung auszuspielen.[45]

Xandr, gegründet 2018 vom US-Telekommunikationskonzern AT&T durch die Zusammenführung von AppNexus (für 1,6 Milliarden USD erworben) und anderen Werbeeinheiten, 2022 für rund eine Milliarde Dollar von Microsoft übernommen, ist einer der größten sogenannten Demand-Side-Platforms und Datenmarktplätze der Werbewelt. Auf Xandr bieten 93 sogenannte „Data Provider" ihre Datensätze an, darunter sieben deutsche Unternehmen: Tochterunternehmen der Deutschen Telekom und von ProSiebenSat1 sowie weitere, kleinere deutsche Datenanbieter.[46]

Was diese Kategorien zeigen, geht weit über herkömmliche Werbezielgruppen wie „Männer, 25-34 Jahre, sportinteressiert" hinaus. Wolfie Christl, der die Datei entdeckte, bezeichnete sie als „das gewaltigste Dokument über den globalen Datenhandel, das ich je gesehen habe." Und tatsächlich: Ein Blick in die Kategorien offenbart ein System, das an Invasivität und Detailtiefe schockierend ist.[47]

Die Kategorien lassen sich in mehrere Gruppen einteilen. Zunächst demographische und ökonomische Segmente: von simplen Beschreibungen wie „Männer über 40" und „Einkommen: 1.000 bis 2.000 Euro" über „Einkommen: arm" bis hin zu spezifischen Angaben wie „Haushalt mit mehr als vier Kindern unter 12 Jahren" oder „Rentner mit Nebeneinkommen". Dann Gesundheitskategorien: „Brustkrebs", „Schlafprobleme", „Essstörung", „Spielsucht", „Depression", „Angststörung", „erektile Dysfunktion",

[45] Ingo Dachwitz, netzpolitik.org: „Das sind 650.000 Kategorien, in die uns die Online-Werbeindustrie einsortiert", 8. Juni 2023. https://netzpolitik.org/2023/microsofts-datenmarktplatz-xandr-das-sind-650-000-kategorien/: Diese Recherche erhielt den Alternativen Medienpreis 2024 in der Kategorie Vernetzung.

[46] Microsoft: Acquisition of Xandr from AT&T. Pressemitteilung 2022. netzpolitik.org: Analyse der deutschen Datenhändler in der Xandr-Datei, Juni 2023.

[47] Wolfie Christl, Cracked Labs, zitiert in netzpolitik.org, 8. Juni 2023. Christl ist einer der renommiertesten europäischen Forscher auf dem Gebiet der kommerziellen Datenüberwachung.

„Geburtenregelung", „Marihuana-Nutzer", „blind", „taub". Hinzu kommen Verhaltenssegmente wie „Moms who shop like crazy", „Heavy purchasers of pregnancy tests" oder „Depression-prone".[48]

Besonders brisant sind die politischen und sozialen Kategorien: „LGBT", „Black Lives Matter Supporter", „politische Entscheidungsträger", „Militärangehörige", „Polizisten", „Richter" und sogar „Geheimdienstmitarbeiter". Dass sicherheitsrelevante Personengruppen in kommerziellen Werbedatenbanken als Zielgruppe gehandelt werden, ist nicht nur ein Datenschutzproblem, es ist ein nationales Sicherheitsrisiko.

- Gesundheit: Brustkrebs, Schlafprobleme, Essstörung, Spielsucht, Depression, Angststörung, erektile Dysfunktion, Schwangerschaft[49]
- Soziale Identität: „LGBT", „Black Lives Matter Supporter", politische Entscheidungsträger, Militärangehörige[50]
- Verhaltensprofile: „Moms who shop like crazy", „Heavy purchasers of pregnancy tests", „Depression-prone"[51]
- Sicherheitsrelevant: Soldaten, Polizisten, Richter, Staatsanwälte, Geheimdienstmitarbeiter[52]
- Finanzielle Notlage: „Einkommen: arm", „finanzielle Schwierigkeiten", „keine Krankenversicherung"[53]

Die rechtliche Reaktion ließ nicht lange auf sich warten. Datenschutzbehörden in Bayern, Berlin, Hamburg und Baden-Württemberg leiteten nach der Veröffentlichung Prüfverfahren gegen beteiligte Unternehmen ein. Die Berliner Datenschutzbeauftragte Meike Kamp erklärte gegenüber netzpolitik.org, sie sei „skeptisch, dass Firmen sich bei derart umfassenden und intransparenten Datensammlungen auf die Einwilligung der Betroffenen berufen können."[54]

Die Datenschutzorganisation noyb (None of Your Business, gegründet von Max Schrems) nahm die Recherche zum Anlass für eine formelle Beschwerde bei der italienischen Datenschutzbehörde, in der sie unter anderem eine Geldbuße von bis zu vier Prozent des Jahresumsatzes von Xandr forderte; die italienische Behörde eröffnete im Februar 2025 ein Verfahren, das noch läuft (Stand September 2026). Xandr verweigerte konsequent jede Auskunft zu den eigenen Datenpraktiken, selbst gegenüber betroffenen Personen, die bei Xandr und rund 90 Partnern Auskunftsanfragen stellten.[55]

[48] The Markup: From Heavy Purchasers of Pregnancy Tests to the Depression-Prone: We Found 650,000 Ways Advertisers Label You, 8. Juni 2023. https://themarkup.org/privacy/2023/06/08/from-heavy-purchasers-of-pregnancy-tests-to-the-depression-prone-we-found-650000-ways-advertisers-label-you. The Markup hat ein interaktives Tool erstellt, mit dem alle 650.000 Kategorien durchsucht werden können.

[49] The Markup: Interactive Xandr Segment Database, 2023. https://themarkup.org/privacy/2023/06/08/

[50] netzpolitik.org / The Markup: Xandr-Datei, analysiert Juni 2023.

[51] The Markup: From Heavy Purchasers of Pregnancy Tests to the Depression-Prone, Juni 2023.

[52] Wolfie Christl: Xandr-Recherche, Twitter/X-Thread, 8. Juni 2023.

[53] netzpolitik.org: Liste der absurdesten Kategorien der Werbeindustrie, Juni 2023.

[54] Heise Online: Datenschutzbehörden leiten Prüfungen ein gegen Datenmarktplatz Xandr und Käufer, 16. Juni 2023. https://www.heise.de/news/Datenschutzbehoerden-leiten-Pruefungen-ein-gegen-Datenmarktplatz-Xandr-und-Kaeufer-9189885.html

[55] noyb.eu: Complaint against Xandr / Microsoft before Italian Data Protection Authority. Juli 2024. https://netzpolitik.org/2024/beschwerde-von-noyb-xandr-verweigert-jede-datenauskunft/

Die Firma Segment (Twilio)

Für Einsteiger:

Segment ist ein Unternehmen, das kaum jemand kennt, aber fast jeder hat schon unbewusst Daten dorthin gesendet. Segment funktioniert wie ein Datenvermittler: Es sammelt Informationen über Nutzer aus verschiedenen Apps und Websites und leitet sie gebündelt an Werbe- und Analyseplattformen weiter. Wenn Sie eine App nutzen, die "Segment" eingebaut hat, gelangen Ihre Daten, im Auftrag des jeweiligen App-Betreibers, automatisch an Dutzenden weiterer Unternehmen, ohne dass Sie davon wissen.

Technischer Hintergrund

Segment ist eine Kundendatenplattform (Customer Data Platform, CDP), die 2011 gegründet und 2020 für 3,2 Milliarden US-Dollar von Twilio übernommen wurde. Während Unternehmen wie Google und Facebook in der Öffentlichkeit bekannt sind, operiert Segment weitgehend im Verborgenen, und ist gerade deshalb so wirkmächtig. Segment fungiert als Datendrehscheibe: Es sammelt Nutzerdaten aus hunderten von Apps und Websites und leitet sie, nach Aufbereitung und Anreicherung, an Dutzende anderer Marketing- und Analyseplattformen weiter.[56]

Mit nach eigenen Angaben mehr als 25.000 Kundenunternehmen (Stand 2023) ist Segment tief in die digitale Infrastruktur eingebettet. Besonders problematisch ist die sogenannte „Identity Resolution": Segment kann Daten aus verschiedenen Sitzungen, Geräten und Kanälen zu einem einzigen Nutzerprofil zusammenführen, auch wenn der Nutzer keine konkreten personenbezogenen Daten angegeben hat. Die Verknüpfung erfolgt durch technische Fingerprinting-Merkmale und statistische Matching-Algorithmen.

Werbung im Internet und das System des Real-Time-Bidding

Für Einsteiger:

Wenn Sie eine Website aufrufen, passiert in weniger als einer Sekunde etwas, das Sie nie sehen: Ihr "Aufmerksamkeitsmoment" wird versteigert. Dutzende Werbeunternehmen bieten in Echtzeit darum, Ihnen ihre Werbung zu zeigen. Wer am meisten zahlt, gewinnt, und die Entscheidung, wie viel jemand für Ihre Aufmerksamkeit zahlt, hängt davon ab, wie viel er über Sie weiß. Je mehr Datenpunkte über Sie vorliegen, desto teurer sind Sie als Werbeziel. Diese unsichtbare Auktion findet bei jedem Seitenaufruf statt, und dabei landen Ihre Daten bei Hunderten, in Europa bei über tausend Unternehmen.

Technischer Hintergrund

Um die Gefahr kommerzieller Datenhändler vollständig zu verstehen, muss man das Geschäftsmodell verstehen, das sie antreibt: personalisierte Online-Werbung. Im Jahr 2025 flossen weltweit rund 715 Milliarden US-Dollar in digitale Werbung, knapp drei Viertel aller Werbeausgaben; 2026 überschreitet der gesamte Werbemarkt erstmals eine Billion US-Dollar. Das Wachstum wird fast vollständig durch das

[56] Twilio Inc.: Acquisition of Segment for $3.2 Billion. Press Release, 12. Oktober 2020.

sogenannte Programmatic Advertising getrieben, den automatisierten, datenbasierten Kauf und Verkauf von Werbeplatzierungen in Echtzeit.[57]

Das Prinzip klingt simpel: Werbetreibende wollen nicht irgendeine Website mit Werbung beliefern. Sie wollen genau die Person ansprechen, die wahrscheinlich ihr Produkt kauft. Dafür bezahlen sie extra, und die Datenhändler liefern die Zielgruppen. Je präziser das Profil, desto höher der Preis pro „Impression" (Werbeanzeigenausspielung). Ein Nutzer, der kürzlich nach Flügen gesucht und auf Reisewebsites gesurft hat, ist für Airline-Werbung bis zu 100-mal mehr wert als ein zufälliger Besucher.

Die „Marketing Technology Landscape“ zählt in der Ausgabe 2026 über 15.500 Anbieter von Marketing-Technologie, 2011 waren es 150.

Echtzeit-Versteigerung von Werbeflächen (Real-Time-Bidding)

🔧 Wie die Auktion im Detail funktioniert

Wenn Sie eine Website aufrufen, läuft in weniger als 100 Millisekunden eine komplexe Auktion ab, die Sie wahrscheinlich nie bewusst wahrgenommen haben. Ihr Browser übermittelt Ihre Identifikationsmerkmale (Cookie-ID, IP-Adresse, Browser-Fingerprint, Geolokation) an eine sogenannte Supply-Side-Platform (SSP). Diese meldet das verfügbare Werbeinventar (also den Platz auf der Webseite, wo Ihre Aufmerksamkeit verfügbar ist) an eine Ad Exchange, einen digitalen Marktplatz. Auf diesem Marktplatz bieten Dutzende von Demand-Side-Platforms (DSPs) auf Ihren „Aufmerksamkeitsmoment". Das Gebot richtet sich danach, wie wertvoll Ihr Datenprofil für den jeweiligen Werbetreibenden ist. Der Höchstbietende gewinnt, und seine Werbung erscheint in Ihrem Browser, noch bevor die Seite vollständig geladen hat.

In diesem Prozess gehen Ihre Daten an Hunderte Unternehmen, auch wenn am Ende nur eines die Auktion gewinnt: Allein Google nennt 1.102, Microsoft 1.647 Firmen, die in Europa RTB-Daten erhalten dürfen; die irische Bürgerrechtsorganisation ICCL zählte 71 Billionen solcher Übermittlungen pro Jahr über Menschen in Europa, im Schnitt 376 je Person und Tag. Jeder Teilnehmer an dieser Auktion erhält einen sogenannten „Bid Request" mit Ihren Datenpunkten: Alter, Geschlecht, Standort, Interessen, aktuell aufgerufene URL, Gerätetyp. Diese Datenpunkte landen in den Datenbanken der Bieter, unabhängig vom Ergebnis der Auktion. Eine einzige Woche normalen Surfens kann so Tausende von Bid Requests an Hunderte verschiedener Unternehmen generieren.[58]

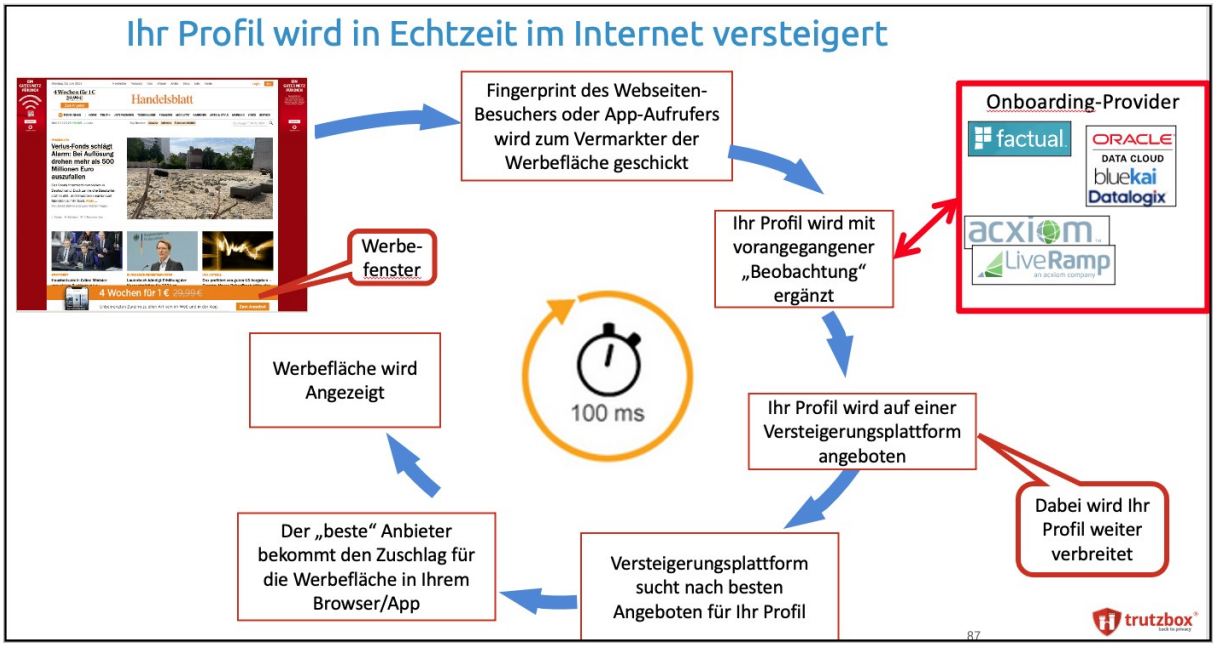
Das Bundeskartellamt stellte nach einer mehrjährigen Untersuchung 2023 fest, der Markt des Programmatic Advertising sei in hohem Maße intransparent gegenüber allen Beteiligten. Kartellamtspräsident Andreas Mundt fragte, ob man wirklich den vollständig vermessenen Internetnutzer wolle, allein damit Produkte vermarktet werden könnten.[59]

[57] Magna (IPG Mediabrands): Global Advertising Forecast, Juni 2025 (digitale Werbung 715 Mrd. USD 2025, Gesamtmarkt 979 Mrd. USD); Dentsu: Global Ad Spend Forecast, 3. Dezember 2025 (Gesamtmarkt über 1 Bio. USD 2026, Digitalanteil 68,7 Prozent).

[58] Papadopoulos, P. et al.: If You Are Not Paying for It, You Are the Product: How Much Do Advertisers Pay to Reach You? ACM SIGCOMM, 2017. Studie analysiert die Gebotsstruktur und Datenweitergabe im RTB-System. Irish Council for Civil Liberties (ICCL): Europe’s hidden security crisis, 14. November 2023; ICCL: The Biggest Data Breach, Mai 2022.

[59] Bundeskartellamt: Sektoruntersuchung Online-Werbung, Abschlussbericht 2023. https://www.bundeskartellamt.de

So läuft eine Echtzeit-Versteigerung einer Werbefläche ab:



Die Versteigerung einer Werbefläche in rund 100 Millisekunden; unterwegs wird das Profil bei den Onboarding-Anbietern angereichert.
(© 2026 Comidio GmbH)

Je präziser das Nutzerprofil, desto mehr zahlt ein Werbetreibender für eine einzige Einblendung, typische Größenordnungen (Stand 2025):

Werbeform	Typischer Preis pro 1.000 Einblendungen (TKP/CPM)
Ungezielte Display-Werbung	ca. 1 bis 3 €
Kontext-Targeting (thematisches Umfeld)	ca. 2 bis 5 €
Video-Werbung (z. B. YouTube)	ca. 3 bis 8 €
Verhaltensbasiertes Targeting / Retargeting (persönliches Profil)	deutlich höher, der Preis steigt mit der Präzision des Profils
Präzise Berufs-Profile (Business-Netzwerke)	zweistellige TKP-Werte

(Quellen: klickpiloten.de, ostend.digital, match2one.com; Zusammenstellung © 2026 Comidio GmbH)

Künstliche Intelligenz: Der neue Datenhunger

Für Einsteiger:

Die großen KI-Systeme sind aus dem Internet gebaut: Sie haben gelesen, was Milliarden Menschen je öffentlich geschrieben haben. Forenbeiträge, Bewertungen, Lebensläufe, Fotos. Und sie lernen weiter: aus jeder Frage, die Sie ChatGPT, Gemini oder Meta AI stellen. Gleichzeitig steuern KI-Modelle, welche Werbung Sie sehen, und werden mit genau den Tracking-Daten gefüttert, die dieses Kompendium beschreibt. Der Datenhunger der KI ist damit nicht ein neues Problem, sondern die Fortsetzung des alten mit größerem Appetit.

🔧 Trainingsdaten, Werbemodelle, Assistenten-Gedächtnis

Drei Datenströme fließen in die KI-Systeme der großen Anbieter: erstens die riesigen Textsammlungen aus dem offenen Netz, mit denen die Sprachmodelle trainiert werden; zweitens die Verhaltensdaten aus Tracking und Werbung, mit denen KI-Modelle die Anzeigenauslieferung steuern; drittens die Eingaben der Nutzer selbst, die Assistenten speichern, auswerten und zum Weitertrainieren verwenden. Alle drei sind mit Studien belegt.

Trainingsdaten aus dem Netz: Wer öffentlich schrieb, steckt im Modell

Die Trainingsdaten der Sprachmodelle stammen zum großen Teil aus Web-Archiven wie Common Crawl, die das offene Internet wahllos abgreifen. Was darin steckt, haben Forscher der Universitäten Washington, Carnegie Mellon und Georgetown 2025 an einem Ausschnitt des Bilddatensatzes „DataComp CommonPool“ (12,8 Milliarden Bild-Text-Paare) vermessen: Hochgerechnet enthält er mindestens 100 Millionen unverpixelte Gesichter, rund 136.000 Lebensläufe mit Namen, dazu gültige Pässe, Kreditkarten, Führerscheine und Geburtsurkunden; bei 28 Prozent der Bilder mit GPS-Angaben ließ sich der Aufnahmeort metergenau bestimmen. Eine Sicherheitsfirma fand im Common-Crawl-Archiv vom Dezember 2024 knapp 12.000 gültige Passwörter und API-Schlüssel.[60]

Dass die Modelle solche Daten nicht nur lesen, sondern behalten, zeigte ein Team um Google-Forscher 2023: Mit einfachen Tricks brachten sie ChatGPT dazu, Trainingsdaten wörtlich auszugeben, für 200 US-Dollar Abfragekosten über 10.000 eindeutige Textstücke, darunter Telefonnummern, E-Mail-Adressen und Wohnadressen realer Personen; fast 17 Prozent der so gewonnenen Ausgaben enthielten gespeicherte personenbezogene Daten. Noch beunruhigender ist, was Modelle aus harmlosen Texten ableiten: Forscher der ETH Zürich zeigten 2024, dass Sprachmodelle aus Reddit-Beiträgen Wohnort, Einkommen oder Geschlecht der Verfasser mit bis zu 85 Prozent Treffsicherheit erschließen, hundertmal billiger und zweihundertmal schneller als menschliche Analysten. Eine Studie von 2026 ließ KI-Agenten aus minimalen Angaben in unter zehn Minuten und für weniger als drei US-Dollar vollständige Personenprofile zusammentragen, zu über 90 Prozent korrekt.[61]

Der Europäische Datenschutzausschuss stellte im Dezember 2024 klar: Ein mit personenbezogenen Daten trainiertes KI-Modell ist nicht automatisch anonym; die DSGVO gilt, solange sich Daten aus dem Modell herausfragen lassen. Im Juli 2026 folgten Leitlinien zum Web-Scraping für generative KI. Die einzige Geldbuße gegen einen KI-Anbieter. 15 Millionen Euro der italienischen Datenschutzbehörde gegen OpenAI (Dezember 2024), hob ein Gericht in Rom im März 2026 aus Zuständigkeitsgründen wieder auf. Beschwerden der Datenschutzorganisation noyb gegen OpenAI wegen erfundener Falschbehauptungen über reale Personen (2024, 2025) sind offen.[62]

---

[60] Hong, Hutson, Agnew, Huda, Kohno, Morgenstern: A Common Pool of Privacy Problems. arXiv 2506.17185, Juni 2025 (rev. April 2026); MIT Technology Review, 18. Juli 2025. Truffle Security: Research. Common Crawl December 2024 (ca. 12.000 gültige Zugangsdaten), Februar 2025.

[61] Nasr, Carlini et al.: Scalable Extraction of Training Data from (Production) Language Models. arXiv 2311.17035, November 2023 (16,9 Prozent der Ausgaben mit gespeicherten personenbezogenen Daten). Staab, Vero, Balunović, Vechev: Beyond Memorization. Violating Privacy via Inference with Large Language Models. ICLR 2024. Chen et al.: Profiling for Pennies. Unveiling the Privacy Iceberg of LLM Agents. arXiv 2605.06232, Mai 2026.

[62] Europäischer Datenschutzausschuss: Opinion 28/2024 on certain data protection aspects related to the processing of personal data in the context of AI models, 17. Dezember 2024; EDSA: Guidelines 03/2026 on web scraping for generative AI, Juli 2026. Garante per la protezione dei dati personali: Provvedimento gegen OpenAI, 20. Dezember 2024 (15 Mio. Euro); Tribunale di Roma, Urteil vom 18. März 2026 (Aufhebung wegen Unzuständigkeit). noyb: Beschwerden gegen OpenAI, Österreich 29. April 2024, Norwegen 20. März 2025.

KI in der Werbemaschine: Tracking-Daten als Treibstoff

Die zweite Datenquelle ist das Tracking selbst. Metas Werbeauslieferung wird seit 2025 von „GEM“ gesteuert, nach Konzernangaben dem größten Empfehlungsmodell der Branche, „trainiert im Maßstab großer Sprachmodelle“, und zwar auf „Anzeigeninhalten und Nutzerinteraktionen aus Werbung und organischen Inhalten“ über Facebook, Instagram und Business Messaging hinweg. Meta beschreibt den Rohstoff offen: „lange Sequenzen aus Klicks, Ansichten und Interaktionen“ enthielten „reiche Signale über Vorlieben und Absichten“. Das Modell steigerte die Werbe-Konversionen auf Instagram um fünf Prozent. Google steuert seine Kampagnen mit „Performance Max“, das Zielgruppensignale aus Demografie, Interessen, Verhalten und Kundenlisten verarbeitet; TikToks Empfehlungssystem lernt im Minutentakt aus jeder Interaktion.[63]

Wie viel Tracking-Daten dabei wert sind, haben Ökonomen gemessen: Ohne Daten von fremden Websites steigen laut einer Studie mit Meta-Daten (2024) die Kosten eines Werbetreibenden je gewonnenem Kunden um 37 Prozent; Nutzer, die dem Tracking widersprechen, bringen Werbeplattformen 52 Prozent weniger ein. Datenhändler haben den Markt erkannt: LiveRamp bietet seit Januar 2026 „genehmigte Datensätze zu Konsumverhalten, Käufen, Mediennutzung und Transaktionen“ ausdrücklich zum Training und Feintuning von KI-Modellen an; Reddit verdient rund 43 Millionen US-Dollar je Quartal mit Lizenzen an OpenAI und Google. LinkedIn nutzt seit November 2025 auch in der EU Profile und öffentliche Beiträge seiner Mitglieder zum KI-Training, auf Basis des „berechtigten Interesses“, mit Widerspruchsmöglichkeit, aber ohne die bereits verwendeten Daten zurückzuholen. X (Twitter) hatte 2024 die Beiträge seiner Nutzer ohne Ankündigung für den Chatbot Grok freigeschaltet; die irische Datenschutzbehörde ermittelt seit April 2025.[64]

Was KI-Assistenten über Sie speichern, und wofür sie es nutzen

Die dritte Quelle sind Sie selbst. Wer ChatGPT, Gemini, Copilot oder Meta AI nutzt, spricht mit einem System, das sich erinnert. ChatGPT kann seit April 2025 auf alle früheren Gespräche eines Nutzers zurückgreifen; Eingaben von Privatkunden fließen standardmäßig ins Training ein, solange die Option „Das Modell für alle verbessern“ nicht abgeschaltet ist. Wie wenig „Löschen“ bedeutet, zeigte ein US-Gerichtsverfahren: Auf Antrag der New York Times musste OpenAI von Mai bis September 2025 sämtliche Chatprotokolle aufbewahren, auch die von Nutzern gelöschten. Seit Februar 2026 zeigt ChatGPT in den USA Werbung, ausgewählt nach dem aktuellen Gesprächsthema, früheren Chats und dem Gedächtnis des Assistenten.[65]

Google speichert Gemini-Gespräche standardmäßig 18 Monate; Mitarbeiter lesen Stichproben zur Qualitätskontrolle, weshalb Google selbst rät, „keine vertraulichen Informationen einzugeben, die ein Prüfer nicht sehen sollte“, geprüfte Gespräche bleiben bis zu drei Jahre gespeichert, auch nach dem Löschen. Seit Juli 2025 darf Gemini auf Android Telefon, Nachrichten und WhatsApp steuern,

[63] Meta Engineering: Meta’s Generative Ads Recommendation Model (GEM), 10. November 2025. Google Ads-Hilfe: Zielgruppensignale in Performance-Max-Kampagnen. ByteDance: Monolith. Real Time Recommendation System with Collisionless Embedding Table, RecSys 2022.

[64] Wernerfelt, Tuchman, Shapiro, Moakler: Estimating the Value of Offsite Tracking Data to Advertisers. Marketing Science, 2024 (+37 Prozent Kosten je Neukunde). Johnson, Shriver, Du: Consumer Privacy Choice in Online Advertising. Marketing Science, 2020 (‚52 Prozent). LiveRamp: LiveRamp expands its marketplace with data, models and agents for AI use, 6. Januar 2026. The Motley Fool / WSJ: Reddit’s data revenue, 17. August 2026. LinkedIn Hilfe: Data for Generative AI Improvement, gültig ab 3. November 2025; ICO: Statement on changes to LinkedIn AI data policy, 20. September 2024. Irish Data Protection Commission: Inquiry into X Internet Unlimited Company, 11. April 2025.

[65] OpenAI: Data Controls FAQ; OpenAI: Memory FAQ (Erweiterung auf alle Gespräche, 10. April 2025). United States District Court S.D.N.Y., The New York Times v. Microsoft/OpenAI: Preservation Order, 13. Mai 2025; Aufhebung 9. Oktober 2025 (Engadget, 9. Oktober 2025). OpenAI Hilfe: Ads in ChatGPT, Februar 2026; MacRumors: ChatGPT now has ads, 9. Februar 2026.

„unabhängig davon, ob Ihre Gemini-Aktivitäten ein- oder ausgeschaltet sind“; seit Januar 2026 greift die Funktion „Personal Intelligence“ in den USA auf Gmail, Fotos, YouTube und Suchverlauf zu. Microsoft trainiert seit Oktober 2024 mit Copilot-Gesprächen von Privatkunden (EU-Nutzer bislang ausgenommen) und hat mit Windows Recall eine Funktion eingeführt, die alle paar Sekunden den Bildschirm fotografiert, lokal verschlüsselt, aber laut Sicherheitsforschern 2026 weiterhin durch Schadsoftware auslesbar. Anthropic verlängerte im September 2025 die Speicherfrist für Claude-Gespräche, die ins Training einfließen, auf fünf Jahre, sofern Nutzer nicht widersprechen. Meta nutzt Gespräche mit Meta AI außerhalb der EU seit Dezember 2025 zur Werbepersonalisierung, ohne Widerspruchsmöglichkeit. Apple geht mit „Private Cloud Compute“ einen anderen Weg: Anfragen werden auf Servern verarbeitet, die keine Daten speichern dürfen und deren Software öffentlich prüfbar ist.[66]

Besonders weit reichen KI-Browser und Browser-Assistenten. Eine Studie der Universitäten UC Davis und UCL (2025) untersuchte neun verbreitete KI-Erweiterungen: Mehrere übertrugen den vollständigen Seiteninhalt, einschließlich Krankenakten, an ihre Anbieter; die Erweiterung Merlin schickte Formulareingaben samt US-Sozialversicherungsnummern von der Website der Steuerbehörde nach außen, zwei Erweiterungen protokollierten selbst im Privatmodus. Forscher von Brave und dem Imperial College prüften 2025 acht KI-Agenten, die im Auftrag des Nutzers surfen: Sieben schickten die besuchten Seiten an Server der Anbieter, vier klickten ungefragt „Alle Cookies akzeptieren“, sechs gaben persönliche Daten wie E-Mail-Adresse oder Zugangsdaten an Websites weiter. OpenAIs Browser Atlas (Oktober 2025) legte standardmäßig „Browser-Erinnerungen“ über alles Gesehene an und wurde im August 2026 wieder eingestellt.[67]

Rechtlich hinkt Europa hinterher. Die Pflichten des AI Act für große Sprachmodelle gelten seit August 2025; die Pflichten für Hochrisiko-Anwendungen wie KI-gestützte Personalauswahl verschob die EU im Juli 2026 auf Dezember 2027. Für den Alltag heißt das: Was Sie einem Assistenten erzählen, ist in der Regel dauerhaft gespeichert, wird von Menschen gelesen, fließt in künftige Modelle ein und, bei Werbefinanzierung, in Ihre Anzeigen. Die TrutzBox kann Inhalte dieser Gespräche nicht schützen; sie kann aber sichtbar machen, welche Geräte und Apps mit welchen KI-Anbietern sprechen, und diese Verbindungen für einzelne Geräte unterbinden.[68]

[66] Google: Gemini Apps Privacy Hub (support.google.com/gemini/answer/13594961). Google-E-Mail an Android-Nutzer, Juli 2025, dokumentiert von Malwarebytes, 2. Juli 2025. CNBC: Google launches Personal Intelligence in Gemini app, 14. Januar 2026. Microsoft: Transparency and control in consumer data use, 16. August 2024; Windows Central: Windows Recall general availability, 25. April 2025; GeekWire: One year after its rocky launch, Windows Recall still raises security red flags, 2026. Anthropic: Updates to Consumer Terms and Privacy Policy, 28. August 2025. Meta Newsroom, 1. Oktober 2025 (Meta-AI-Chats für Werbung). Apple Security Research: Private Cloud Compute, 10. Juni 2024.

[67] Vekaria et al.: Big Help or Big Brother? Auditing Tracking, Profiling and Personalization in Generative AI Assistants. USENIX Security 2025. Ukani, Haddadi, Shamsabadi, Snyder: Privacy Practices of Browser Agents. arXiv 2512.07725, Dezember 2025. OpenAI Hilfe: ChatGPT Atlas data controls and privacy, Oktober 2025; TechRepublic: ChatGPT Atlas shutdown and migration, August 2026.

[68] Europäische Kommission: Guidelines on the scope of obligations for general-purpose AI models, 18. Juli 2025. Verordnung zur Änderung der KI-Verordnung („AI Omnibus“), Amtsblatt der EU, 24. Juli 2026 (Hochrisiko-Pflichten ab 2. Dezember 2027).

Teil 3
Gerätehersteller

Wenn die eigenen Geräte Daten senden: Fernseher, Autos, Smart Home

Smart-TVs: Hersteller wissen, was Ihr Fernseher anzeigt

Für Einsteiger:

Ihr neuer Fernseher schaut zurück. Moderne Smart-TVs erzeugen in kurzen Abständen Prüfsummen (Fingerprints) des Bildschirminhalts und übermitteln diese an den Hersteller. Dort wird automatisch erkannt, was Sie gerade anschauen, egal ob Netflix, lineares Fernsehen oder eine DVD. Diese Informationen werden für Werbezwecke genutzt, dokumentierte Fälle, von Vizio (FTC-Verfahren 2017) bis zu den Klagen des Bundesstaats Texas gegen Samsung, LG, Sony, Hisense und TCL (2025), zeigen auch die Weitergabe an Dritte. Das alles passiert häufig standardmäßig, ohne dass es im Kaufprospekt steht.

Technischer Hintergrund

Moderne Fernseher sind in vieler Hinsicht Computer mit großem Bildschirm, und sie verhalten sich entsprechend: Sie sammeln Daten über ihre Nutzer, und zwar weit umfassender, als die meisten Käufer ahnen. Im Dezember 2025 berichtete der Autor in CHIP Online über das weitgehend unbekannte Phänomen des Automatic Content Recognition (ACR). Diese Technologie ist in Smart-TVs der Hersteller Samsung, LG, Sony, Vizio, Philips und vieler anderer eingebaut und funktioniert wie folgt: In regelmäßigen Abständen, meist mehrmals pro Minute, wird aus dem aktuell angezeigten Bild eine Prüfsumme (Fingerprint) errechnet und an die Server des Herstellers übermittelt. Dort werden diese Fingerprints mit einer riesigen Datenbank von Filmen, Serien, Werbespots und TV-Inhalten abgeglichen, um zu ermitteln, was der Nutzer schaut.[69]

Dieser Vorgang ist unabhängig von der Quelle des Inhalts: Ob der Nutzer Netflix streamt, lineares Fernsehen schaut, eine DVD abspielt oder einen USB-Stick nutzt. ACR erkennt den Inhalt in allen Fällen. Die Messungen der Studie von 2024 zeigen das Tempo: LG-Geräte erfassen laut Herstellerdokumentation alle 10 Millisekunden ein Bild und senden alle 15 Sekunden Fingerprints, Samsung erfasst alle 500 Millisekunden und lädt jede Minute hoch, auch dann, wenn nur ein Zuspielgerät per HDMI angeschlossen ist. Die gesammelten Daten werden sowohl für die Verbesserung eigener Dienste als auch für Werbezwecke genutzt und nach dokumentierten Fällen auch an Dritte weitergegeben. Samsung vermarktet ACR-Daten Medienberichten zufolge über seine Werbetochter Samsung Ads an Werbekunden und Messdienstleister.

Besonders problematisch ist, dass ACR in vielen Smart-TVs standardmäßig aktiviert ist und die Datenschutzhinweise, die Nutzer bei der Ersteinrichtung präsentiert bekommen, so komplex und verstreut

[69] Hermann Sauer in CHIP Online: „Studie zeigt: Hersteller wissen, was Ihr Fernseher gerade anzeigt", 17. Dezember 2025. Grundlage ist die Studie „Watching TV with the Second-Party: A First Look at Automatic Content Recognition Tracking in Smart TVs“ von University College London, University of California Davis und IMDEA Networks (2024).

gestaltet sind, dass Verbraucherschutzorganisationen regelmäßig Kritik an der Qualität der Datenschutzhinweise äußern. Bereits 2013 wurde bekannt, dass LG-Fernseher auch die Namen lokal gespeicherter Dateien auf angeschlossenen USB-Sticks übermittelten; das britische Information Commissioner's Office (ICO) leitete daraufhin eine Prüfung ein, LG stellte die Übermittlung per Firmware-Update ab. Im Dezember 2025 verklagte der Generalstaatsanwalt von Texas Samsung, LG, Sony, Hisense und TCL wegen heimlicher ACR-Datensammlung; Samsung (Februar 2026) und LG (Mai 2026) verpflichteten sich in Vergleichen zu ausdrücklicher Einwilligung beziehungsweise deutlich sichtbarer Abschaltmöglichkeit.[70]

> ⚠ **Praktischer Hinweis: ACR deaktivieren**
>
> In Samsung-TVs finden Sie die ACR-Einstellung unter Einstellungen → Allgemein → Datenschutz → Nutzungsbedingungen und Datenschutz → Zuschauerinformationsdienste. Bei LG unter Einstellungen → Allgemein → Zusatzeinstellungen → Live Plus. Die genaue Bezeichnung variiert je nach Modelljahr; die Einstellung ist oft tief verschachtelt und nach Software-Updates nicht selten wieder aktiviert. Die TrutzBox kann ACR-Verbindungen auf Netzwerkebene blockieren, ohne dass der Nutzer am Gerät selbst aktiv werden muss (Kompendium Teil 2, Kapitel „Netzwerk").

Connected Cars: Autos als Datenzentralen

> 💡 **Für Einsteiger:**
> Ihr neues Auto weiß mehr über Sie als Ihr Smartphone, und teilt diese Informationen fleißig. Moderne Fahrzeuge sind rollende Datenzentralen, die jeden Kilometer, jede Bremsung und zunehmend auch jedes Gespräch im Innenraum erfassen können. Die Daten werden an Hersteller übermittelt und häufig an Dritte weiterverkauft, oft ohne dass Fahrer davon wissen oder wirksam widersprechen können.

🔧 Technischer Hintergrund

Wer heute ein neues Auto kauft, erwirbt nicht nur ein Fortbewegungsmittel, sondern eine vernetzte Datenplattform. Moderne Fahrzeuge verfügen über Dutzende Sensoren, permanente Internetverbindungen und leistungsfähige Bordcomputer, die kontinuierlich Daten erheben und an die Server der Hersteller übermitteln. Die Mozilla Foundation veröffentlichte im September 2023 eine Untersuchung der Datenschutzrichtlinien von 25 großen Automarken. Das Ergebnis: Alle 25 Hersteller fielen laut Mozilla durch den Datenschutztest. In ihrem Bericht bezeichnete die Stiftung Autos als „schlechteste Produktkategorie", die sie je untersucht habe, schlechter als Mental-Health-Apps oder smarte Heimgeräte.[71]

Laut der Mozilla-Untersuchung von 2023 umfasst die Liste der potenziell erfassten Daten unter anderem: präzise GPS-Standorte und vollständige Bewegungsprofile, Fahrverhalten einschließlich

[70] UK Information Commissioner's Office (ICO): Prüfung der Datenübermittlung durch LG-Smart-TVs nach Berichten vom November 2013 (Blog „DoctorBeet", BBC News); LG stellte die Übermittlung von Dateinamen per Firmware-Update ab. Texas Attorney General: Klagen gegen Samsung, LG, Sony, Hisense und TCL, 15. Dezember 2025; Vergleiche mit Samsung (26. Februar 2026) und LG (11. Mai 2026).

[71] Mozilla Foundation: „Privacy Not Included: Cars", veröffentlicht September 2023. https://foundation.mozilla.org/en/privacynotincluded/categories/cars/. Alle im Text wiedergegebenen Feststellungen beziehen sich auf den Stand der Herstellerrichtlinien zum Untersuchungszeitpunkt; Mozilla hat das Projekt „Privacy Not Included" im August 2026 eingestellt, eine neuere Auto-Untersuchung gibt es nicht.

Geschwindigkeit, Beschleunigung und Bremsverhalten, biometrische Daten wie Gesichtserkennung, Fingerabdrücke und Stimmerkennung zur Fahreridentifikation, Gesundheitsdaten über Lenkradsensoren (Puls, Müdigkeit) sowie über verbundene Gesundheits-Apps, Sprachbefehle und potenziell Gespräche im Fahrzeuginnenraum über Mikrofone. Mozilla stellte ferner fest, dass mindestens zwei Hersteller, Nissan und Kia, in ihren zum Untersuchungszeitpunkt geltenden Datenschutzerklärungen angaben, Informationen über „sexuelle Aktivität“ und „Sexualleben“ erheben zu können.

Ein anschauliches Beispiel lieferte der Fall Volkswagen: Im Dezember 2024 berichtete der Chaos Computer Club (CCC) gemeinsam mit dem Nachrichtenmagazin Der Spiegel, dass die Standortdaten von rund 800.000 Fahrzeugen der Marken VW, Audi, Seat und Skoda durch eine Sicherheitslücke bei der VW-Softwaretochter Cariad frei im Internet zugänglich gewesen seien. Den Berichten zufolge lagen die Daten auf einem ungeschützten Amazon-Cloud-Speicher und ließen sich konkreten Fahrzeugen und damit Personen zuordnen, inklusive präziser Standorthistorien, die Rückschlüsse auf Wohnorte, Arbeitsplätze und persönliche Gewohnheiten ermöglichten. Dass Fahrzeugdaten tatsächlich verkauft werden, belegt der Fall General Motors: Der Konzern hatte über den Dienst OnStar erfasste Fahrdaten von Millionen Kunden an die Datenhändler LexisNexis und Verisk weitergegeben, die sie an Versicherer verkauften. Die US-Handelsbehörde FTC untersagte GM im Januar 2026 für fünf Jahre jede Weitergabe von Standort- und Fahrdaten an Auskunfteien; der Bundesstaat Texas klagt seit 2024. Honda und Hyundai erhielten laut US-Senat für ihre Fahrdaten 26 beziehungsweise 61 Cent je Fahrzeug.[72]

Besonders problematisch ist laut der Mozilla-Studie von 2023 die Frage der Einwilligung. Dem Bericht zufolge existiert eine echte Zustimmung bei vielen Herstellern nicht. Subaru etwa erkläre in seinen zum Untersuchungszeitpunkt gültigen Richtlinien, dass bereits Beifahrer als „Nutzer“ gelten und durch das bloße Einsteigen ins Auto der Datenschutzerklärung zugestimmt hätten. Einige Hersteller wiesen darauf hin, dass es die Aufgabe des Fahrers sei, Passagiere über die Datenschutzrichtlinien zu informieren. Wer versuche, der Datensammlung zu widersprechen, werde mitunter bestraft: Tesla warne Kunden, die sich gegen die Datenerhebung entschieden, dass das Unternehmen sie dann nicht mehr über Probleme mit ihrem Fahrzeug informieren könne. Mozilla stellte fest, dass zum Zeitpunkt der Untersuchung 84 Prozent der geprüften Hersteller die gesammelten Daten an Dritte teilten oder verkauften. Mehr als die Hälfte gab an, persönliche Daten auf einfache Anfrage, ohne Gerichtsbeschluss, an Behörden und Strafverfolgungsbehörden weiterzugeben.

Google im Cockpit: Android Automotive (Stand 2024/2025). Die Infotainment-Systeme moderner Fahrzeuge werden nach Berichten des Fachmagazins c’t (Ausgabe 08/2024) und der Frankfurter Allgemeinen Zeitung zunehmend von Google betrieben. Dabei gibt es zwei grundverschiedene Ansätze: Android Auto spiegelt lediglich das Smartphone auf dem Fahrzeugdisplay, während Android Automotive OS (AAOS) ein eigenständiges Betriebssystem ist, das direkt im Bordcomputer des Fahrzeugs läuft. AAOS wurde Stand 2024 bereits von Volvo, Renault, Ford, General Motors, Polestar, Honda und BMW eingesetzt, allerdings in unterschiedlicher Tiefe. In der Vollausstattung mit Google Automotive Services (GAS) sind Google Maps, der Play Store und der Google Assistant fest integriert, was bedeutet, dass sämtliche Fahrdaten, Standortdaten und Sprachbefehle potenziell an Google fließen können. BMW und Volkswagen nutzen zwar AAOS als Basis, verzichten jedoch bewusst auf die Google-Dienste und stellen eigene Apps bereit. Die Stellantis-Marken (Fiat, Opel, Chrysler, Citroën, Alfa Romeo) verwenden laut c’t ebenfalls keine Google-Services.[73]

[72] Der Spiegel / Chaos Computer Club (CCC): Bericht über die Offenlegung von Standortdaten von rund 800.000 VW-Konzernfahrzeugen, veröffentlicht Dezember 2024. Die Daten befanden sich den Berichten zufolge auf einem ungeschützten Amazon-Cloud-Speicher der VW-Softwaretochter Cariad. FTC: Final Order GM/OnStar, 14. Januar 2026. Senatoren Wyden/Markey: Brief an die FTC, 26. Juli 2024 (Honda 25.920 USD für 97.000 Fahrzeuge, Hyundai 1,04 Mio. USD für 1,7 Mio. Fahrzeuge). Texas Attorney General v. General Motors, 13. August 2024.

Das Bundeskartellamt äußerte in einer Pressemitteilung vom 20. Dezember 2023 „wettbewerbliche Bedenken“ im Zusammenhang mit Google Automotive Services. Besondere Sorge bereite die Zwangsbündelung reichweiten- und marktstarker Dienste mit weniger starken Diensten, ein Verhalten, das nach Einschätzung der Behörde zur Ausweitung von Marktmacht und zur Stärkung von Ökosystemen führen könne. Für Fahrzeuge mit Google-Integration standen Stand 2025 alternative App-Stores zur Verfügung: BMW und Mercedes-Benz setzten auf Forvia (Faurecia-Aptoide), Stellantis und die Volkswagen-Gruppe auf Samsung/Harman (Ignite App Store). Wer einen solchen alternativen App-Store nutzt, kann den Datenabfluss an Google zumindest reduzieren.[74]

Ford-Patent: Werbung durch Mithören (August 2024). Im August 2024 veröffentlichte das US-amerikanische Patent- und Markenamt (USPTO) die Ford-Patentanmeldung US-20240289844-A1 mit dem Titel „In-Vehicle Advertisement Presentation“. Wie unter anderem Auto Bild und CHIP im Oktober 2024 berichteten, beschreibt das Patent ein System, bei dem das Fahrzeug Gespräche der Insassen analysieren könne, um passende Werbung auf dem Infotainment-Display einzuspielen. Dem Patent zufolge würden Schlüsselwörter aus Unterhaltungen gefiltert und mit Standortdaten, Fahrverhalten und historischen Bewegungsmustern verknüpft. Fährt der Fahrer regelmäßig zu einem Supermarkt, könnte gezielt Werbung für Lebensmittelangebote erscheinen. Das System würde laut Patentbeschreibung sogar erkennen, wann ein günstiger Moment für Audio- oder Bildschirmwerbung sei, etwa in Gesprächspausen. Ford betonte gegenüber Medien, eine Patentanmeldung bedeute keine konkreten Produktpläne.[75]

Datenschutz-Schwächen deutscher Hersteller (Stand September 2025). Eine Analyse der zum Stand September 2025 veröffentlichten Datenschutzerklärungen und Privacy-Portale deutscher Automobilhersteller zeigt ebenfalls erhebliche Defizite. Volkswagen gab in seinem Privacy-Portal Aufbewahrungsfristen von bis zu 30 Jahren für bestimmte Daten an, ohne klar zu differenzieren, welche Kategorien so lange gespeichert würden, was nach Einschätzung von Datenschutzexperten gegen das DSGVO-Prinzip der Datenminimierung (Art. 5) verstoßen könnte. BMW informierte in seinen Dokumenten (BMW ConnectedDrive Privacy Policy), dass Opt-outs für Drittanbieter-Angebote teilweise nicht von BMW umgesetzt werden könnten und Nutzer die Drittanbieter selbst kontaktieren müssten. Mercedes-Benz beschrieb in seinen Connected-Service-Notices eine umfangreiche Verarbeitung von Telemetrie-, Standort- und Diagnosedaten, häufig auf Basis „berechtigter Interessen“. Dass die Datenschutzaufsichtsbehörden bislang kaum gegen diese Praktiken vorgehen, hat nach Einschätzung von Branchenbeobachtern mehrere Gründe: chronische Unterbesetzung der Behörden, die wirtschaftlich und politisch sensible Stellung der Automobilindustrie in Deutschland und Europa, das Zuständigkeitschaos zwischen 16 Landesbehörden und Datenverarbeitungs-Tochtergesellschaften in Irland, Luxemburg oder den USA sowie höchstrichterlich noch ungeklärte Rechtsfragen, etwa ob Fahrzeugdaten, die einer Fahrgestellnummer statt einem Fahrer zugeordnet sind, als personenbezogene Daten im Sinne der DSGVO gelten.[76]

---

[73] Google: Android Automotive OS, https://developers.google.com/cars/design/automotive-os?hl=de. Vgl. c’t Magazin für Computer Technik, Nr. 08/2024; FAZ: „Künftig fährt Google in jedem neuen Volvo mit“, 26.05.2022; FAZ: „Jetzt fährt auch Renault mit Google“, 22.04.2024.

[74] Bundeskartellamt: „Google Automotive Services-Verfahren: Markttest über Zusagen von Google“, Pressemitteilung 20.12.2023. https://www.bundeskartellamt.de/SharedDocs/Meldung/DE/Pressemitteilungen/2023/20_12_2023_Google_Automotive.html

[75] Ford Motor Company: US-Patentanmeldung US-20240289844-A1, „In-Vehicle Advertisement Presentation“, veröffentlicht durch das USPTO am 29. August 2024. https://www.documentcloud.org/documents/25108000-us-20240289844-a1_i. Vgl. Auto Bild: „Ford: Mit Patent wird Autowerbung revolutioniert“, Oktober 2024; CHIP: „Ford will Gespräche von Insassen mithören“, Oktober 2024. Ford erklärte gegenüber Medien, die Patentanmeldung bedeute keine konkreten Produktpläne.

[76] Analyse auf Basis der zum Stand September 2025 öffentlich zugänglichen Datenschutzerklärungen von Volkswagen Group (Privacy-Portal VW, VW-Driving-Experience), BMW Group (BMW Privacy Pages, BMW ConnectedDrive-DPP), Mercedes-Benz Group (Mercedes-Privacy-Portal, Mercedes-me Connect Privacy Notice), Ford (FordPass-Richtlinie), Opel/Stellantis (Stellantis Privacy Policy, Opel Web-Pages). Die Richtlinien können zwischenzeitlich geändert worden sein.

⚠ **Praktischer Hinweis: Datenabfluss im Auto reduzieren**
Wer seine Privatsphäre schützen möchte, sollte bei Fahrzeugen mit Android Automotive prüfen, ob Google-Apps verzichtbar sind. Alternative App-Stores wie Faurecia-Aptoide oder der Harman Ignite Store bieten datenschutzfreundlichere Alternativen. Grundsätzlich gilt: Je weniger vernetzte Dienste aktiviert werden, desto weniger Daten fließen ab. Die Europäische Datenschutz-Grundverordnung gibt Verbrauchern das Recht auf Auskunft, welche Daten über sie gespeichert werden, auch von ihrem Auto. Dieses Recht einzufordern, kann aufschlussreich sein. Der europäische Data Act (anwendbar seit September 2025) gibt Nutzern außerdem Zugangsrechte zu den vom Fahrzeug erzeugten Produkt- und Dienstdaten nach Maßgabe des Gesetzes.

IoT Devices: Das Internet der unsicheren Dinge

Für Einsteiger:

Ihr Smart-TV schaut zurück. Ihre vernetzte Waschmaschine berichtet Ihrer Herstellerfirma, wann und wie Sie waschen. Ihr Sprachassistent lauscht dauerhaft auf sein Aktivierungswort. Das sogenannte Internet of Things, alle internetfähigen Geräte außer PC und Smartphone, ist ein riesiges, schlecht gesichertes Datensendernetz, das Ihr Zuhause lückenlos überwacht. Die meisten Nutzer haben keine Ahnung, was ihre Geräte im Hintergrund übertragen.

IoT-Risiken und IP-Blockierung durch den Angriffsschutz

Nach Schätzungen von IoT Analytics (Oktober 2025) waren Ende 2025 weltweit 21,1 Milliarden IoT-Geräte vernetzt (ohne Smartphones, Tablets und PCs), bis 2030 werden rund 39 Milliarden erwartet. Darunter fallen Glühbirnen, Steckdosen, Waschmaschinen, Kühlschränke, Heizkessel, Türklingeln, Sicherheitskameras, Babyfone und Spielzeug. Viele dieser Geräte übermitteln regelmäßig Daten an die Server ihrer Hersteller: Nutzungszeiten, Einstellungen, Standortdaten und Verhaltensmuster.[77]

Ein besonders kritisches Beispiel sind Smart-Home-Sprachassistenten: Amazon Echo (Alexa), Google Home (Google Assistant) und Apple HomePod (Siri). Diese Geräte hören permanent lokal auf ihr Aktivierungswort; erst danach, und bei Fehlerkennungen auch unbeabsichtigt, werden Aufnahmen an die Server der Anbieter übertragen. Im Jahr 2019 wurde bekannt, dass Amazon, Apple, Google und Microsoft Mitarbeiter beschäftigen, die Aufzeichnungen von Sprachassistenten manuell transkribieren und qualitätsprüfen, darunter private Gespräche, intime Momente, ärztliche Beratungen und Kinderunterhaltungen. Die Richtung ist eindeutig: Zum 28. März 2025 strich Amazon bei Echo-Geräten die Option, Sprachaufnahmen nicht in die Cloud zu senden, seither werden alle Alexa-Anfragen auf Amazon-Servern verarbeitet, weil die neue KI-Version Alexa+ die Rechenleistung der Cloud voraussetzt.[78]

[77] IoT Analytics: State of IoT 2025. Number of connected IoT devices, 28. Oktober 2025. https://iot-analytics.com/number-connected-iot-devices/

[78] Bloomberg Technology: Apple, Amazon, Google, Microsoft Employees Are Listening to Your Voice Recordings. Mai bis August 2019. Betraf alle großen Sprachassistenten-Anbieter gleichzeitig. Amazon: E-Mail an Echo-Nutzer, März 2025 (Ende der Funktion „Do Not Send Voice Recordings“ zum 28. März 2025), berichtet u. a. von Ars Technica und Malwarebytes.

Wie aus dem Datenabfluss ein Missbrauch des ganzen Anschlusses wird, zeigte der Sommer 2026. Am 2. Juli 2026 beschlagnahmte das FBI nach Berichten des Sicherheitsjournalisten Brian Krebs die Infrastruktur eines sogenannten Residential-Proxy-Dienstes, der über zwei Millionen gekaperte Geräte, überwiegend Smart-TVs und Streaming-Boxen, als Weiterleitungsstationen für fremden Internetverkehr vermietete. Die Besitzer bemerkten nichts. Manche Billiggeräte waren nach diesen Berichten bereits ab Werk infiziert, andere über Gratis-Apps wie VPN-Tools, Bildschirmschoner oder PDF-Betrachter; einzelne Apps zahlten Nutzern sogar wenige Cent für das „Teilen“ ihrer Internetverbindung. Der Sicherheitsdienstleister Spur untersuchte im Juni 2026 rund 6.000 Apps aus den offiziellen Stores von LG und Samsung und fand entsprechende Bausteine nach eigener Angabe in rund 42 Prozent der LG-Apps und in über einem Viertel der Samsung-Apps. Der Fernseher sendet dann nicht nur Daten nach Hause, er wird zum Werkzeug: Über den heimischen Anschluss laufen Betrugsversuche, Passwortangriffe und Klickbetrug, für die zunächst der Anschlussinhaber verdächtig erscheint. Sichtbar wird so etwas nur, wenn der ausgehende Verkehr jedes Geräts beobachtet wird (Kompendium Teil 2, Kapitel „Monitor“).[79]

Ein leiser Dauerkontakt zum Hersteller bleibt selbst bei sauberen Geräten: die Uhrzeit. Jedes Gerät gleicht seine Uhr mehrmals pro Stunde über das Internet ab (Network Time Protocol, NTP), denn ohne korrekte Zeit funktionieren verschlüsselte Verbindungen, Logins und Zertifikate nicht. Standardmäßig fragen Windows-Rechner dafür bei Microsoft, iPhones und Macs bei Apple, Android-Geräte bei Google. Bei jeder Anfrage erfährt der Hersteller die IP-Adresse, also groben Standort und Internetanbieter, und wann das Gerät eingeschaltet ist, rund um die Uhr und unverschlüsselt. Den vom Heimrouter angebotenen Zeitserver beachten nach Messungen des Comidio-Teams nur Linux-Systeme, Drucker und viele IoT-Geräte; Windows und macOS lassen sich von Hand umstellen, iPhones bieten dafür keine Einstellung. Eine Privacy-Box kann die Zeitfrage im Heimnetz selbst beantworten. Die Uhren bleiben genau, ohne dass Microsoft, Apple oder Google erfahren, wann und von wo die Geräte online sind (Kompendium Teil 2, Kapitel „Geräte“).[80]

[79] Krebs on Security: FBI seizes infrastructure of residential proxy service NetNut, Juli 2026. Google Threat Intelligence Group und Spur: Residential proxy SDKs in smart TV apps, Juni 2026. Sauer, H.: War Ihr Fernseher dabei? FBI stoppt Botnetz aus 2 Millionen Geräten, FOCUS Online, Juli 2026.

[80] Comidio GmbH: Messung des Zeitserver-Verhaltens gängiger Betriebssysteme und Geräte im Heimnetz, Stand 28. Juni 2026. RFC 2132 (DHCP-Option 42, Zeitserver). Sauer, H.: Boxenstopp-Vortrag vom 6. August 2026.

Teil 4
Tracking-Technik

Cookies, Fingerprinting, Session Replay: wie Sie im Netz wiedererkannt werden

Tracking-Methoden: Von Cookies bis Browser Fingerprinting

> **Für Einsteiger:**
> Jedes Mal, wenn Sie eine Website aufrufen, hinterlassen Sie Spuren, ähnlich wie Fußabdrücke im Sand. Tracking-Technologien sind die Werkzeuge, mit denen diese Spuren aufgezeichnet werden. Die einfachste Methode sind Cookies, kleine Dateien, die im Browser gespeichert werden. Doch Tracker sind weit ausgefeilter geworden: Selbst wenn Sie alle Cookies löschen, können Sie anhand der einzigartigen Eigenschaften Ihres Browsers wiedererkannt werden, wie an einem Fingerabdruck.

Überblick der Tracking-Technologien

Tim Libert hat 2015 über eine Million Webseiten untersucht, mehr als 78 Prozent luden einen Tracker von Google. Aktuelle Messungen bestätigen die Größenordnung: Google-Tracker auf 61 Prozent aller Seiten (Web Almanac 2025) beziehungsweise 73 Prozent von 40.000 untersuchten Websites (PoPETs 2025), irgendein Fremd-Tracker auf drei Vierteln aller Seiten.

Cookies und Third-Party-Tracking

> **Für Einsteiger:**
> Ein Cookie ist eine kleine Textdatei, die eine Website auf Ihrem Computer speichert, damit die Seite Sie beim nächsten Besuch wiedererkennt. Das ist zunächst nützlich: Deshalb müssen Sie sich nicht bei jedem Besuch neu einloggen. Das Problem entsteht durch Cookies von Drittanbietern: Diese werden nicht vom besuchten Website-Betreiber gesetzt, sondern von eingebundenen Werbefirmen, und sie folgen Ihnen quer durch das gesamte Internet.

Third-Party-Cookies und das Ende der Cookie-Abschaffung

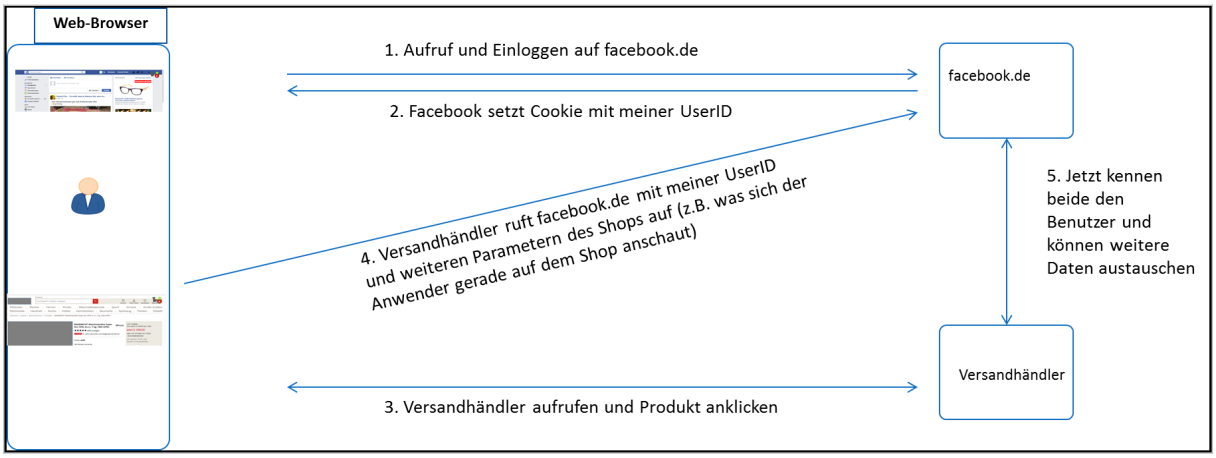
Cookies sind die älteste und immer noch meistverbreitete Tracking-Technologie im Internet. Ein Cookie ist eine kleine Textdatei, die beim Besuch einer Website im Browser des Nutzers gespeichert wird. Er enthält eine eindeutige ID, über die der Nutzer beim nächsten Besuch wiedererkannt wird. Cookies an sich sind nicht schädlich, sie sind notwendig für Funktionen wie eingeloggte Benutzerkonten, Warenkörbe in Online-Shops und gespeicherte Einstellungen. Das Problem liegt in den sogenannten Third-Party-Cookies:

Cookies, die nicht vom besuchten Website-Betreiber, sondern von eingebundenen Drittanbieter-Skripten gesetzt werden.[81]

Ein Drittanbieter-Cookie wie derjenige von Doubleclick.net (Google) oder Criteo.net wird auf Millionen von Websites gesetzt. Wer also amazon.de, spiegel.de und wetter.com besucht, hinterlässt auf allen diesen Seiten denselben Doubleclick-Cookie, und Google kann anhand dieser Informationen erkennen, dass dieselbe Person all diese Seiten besucht hat, in welcher Reihenfolge und wie lange sie auf jeder Seite verbracht hat.[82]

Google hatte ursprünglich angekündigt, Third-Party-Cookies in Chrome bis 2022 abzuschaffen, ein Datum, das mehrfach verschoben wurde. Im Juli 2024 verkündete Google, Third-Party-Cookies doch nicht abzuschaffen, sondern den Nutzern eine Wahlmöglichkeit anzubieten. Im April 2025 strich Google auch diese Abfrage: Third-Party-Cookies bleiben in Chrome standardmäßig aktiv; wer sie nicht will, muss sie selbst in den Browser-Einstellungen abschalten, was die wenigsten tun. Im Oktober 2025 stellte Google schließlich die gesamte „Privacy Sandbox“ ein. Kritiker wie die Electronic Frontier Foundation (EFF) bezeichneten die Kehrtwende als Verrat an der ursprünglichen Datenschutzzusage.[83]

Das folgende Beispiel zeigt in vier Schritten, wie ein zunächst anonymer Shop-Besucher über den Facebook-Cookie wiedererkannt wird:



Wiedererkennung über den Facebook-Cookie: Anmeldung, Cookie, Shop-Besuch und Datenabgleich in fünf Schritten.
(© 2026 Comidio GmbH)

[81] RFC 6265: HTTP State Management Mechanism (Cookies). April 2011. IETF Standards Track.

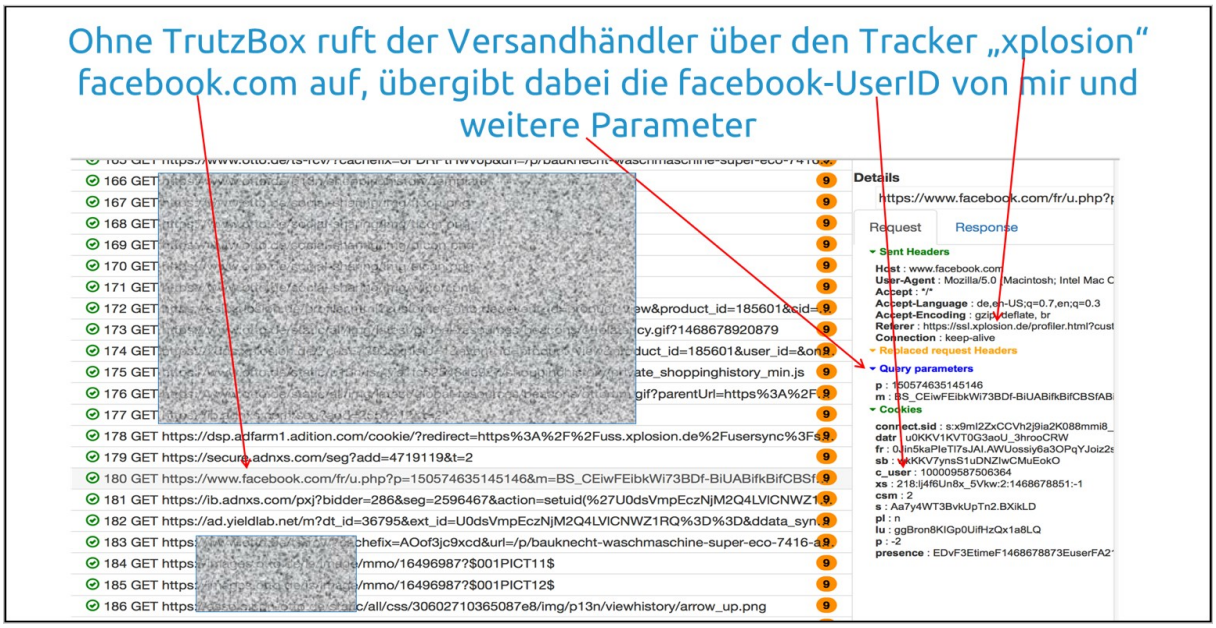
[82] EDPB: Guidelines 8/2020 on the targeting of social media users, April 2021. Enthält eine ausführliche Analyse von Third-Party-Tracking-Methoden.

[83] Google Blog: A new path for Privacy Sandbox on the web, Juli 2024. https://blog.google. EFF: Google Cookie Reversal Is Bad for Privacy, Juli 2024. Google Privacy Sandbox Blog: Next steps for Privacy Sandbox and tracking protections in Chrome, 22. April 2025; Google: Update on plans for Privacy Sandbox technologies, Oktober 2025.

In Facebook eingeloggt, setzt Facebook den Cookie im Browser:

Der Facebook-Cookie im Klartext: Das Feld „c_user" enthält die interne Facebook-Kennung des Benutzers.
(© 2026 Comidio GmbH)

Beim Besuch des Online-Shops schickt der Browser den Facebook-Cookie an Facebook zurück:



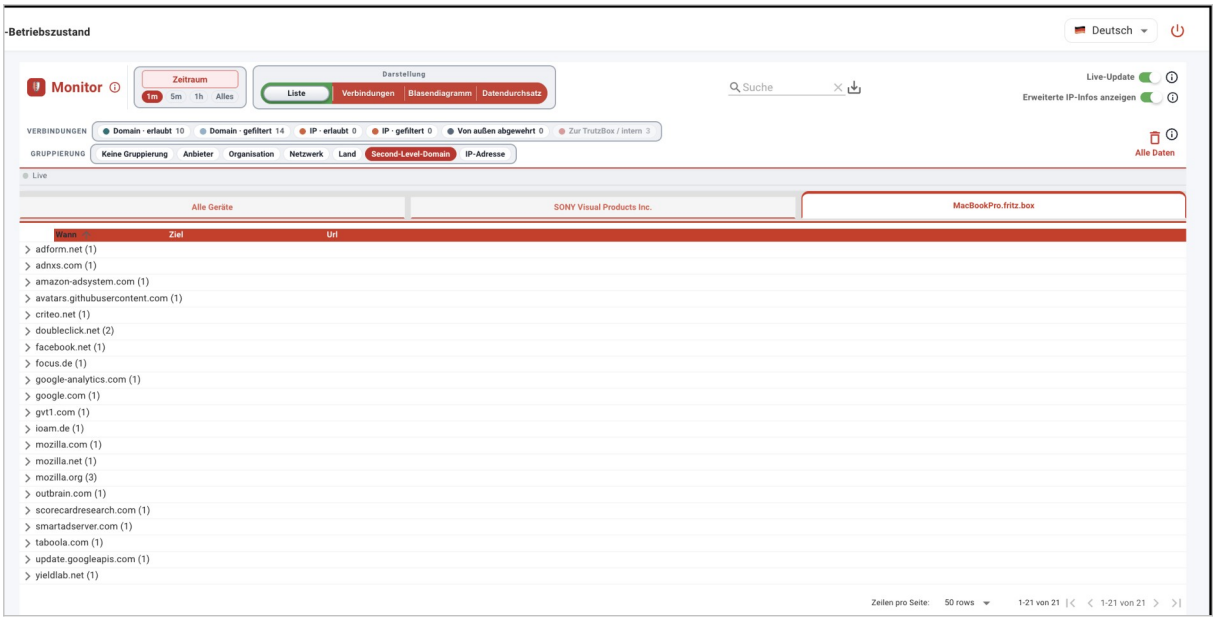
Ohne TrutzBox übergibt der Tracker des Versandhändlers die Facebook-Kennung samt weiterer Angaben an facebook.com.
(© 2026 Comidio GmbH)

Damit weiß Facebook, welches Produkt sich dieser Nutzer angesehen hat, die TrutzBox unterbindet genau diesen Austausch:

Mit TrutzBox wird der Aufruf des Trackers gesperrt; der Detail-Bereich nennt Benutzergruppe, Filterliste und Regel.
(© 2026 Comidio GmbH)

Wie viele Drittdienste ein einziger Artikel-Aufruf lädt, macht der Monitor der TrutzBox direkt sichtbar (Kompendium Teil 2, Kapitel „Monitor“): Der Aufruf einer einzigen focus.de-Seite erzeugt Verbindungen zu über zwanzig Werbe- und Tracking-Domains, von DoubleClick über Criteo bis Taboola. Die TrutzBox blockiert die Tracker („Domain · gefiltert“), die Seite selbst lädt normal weiter:

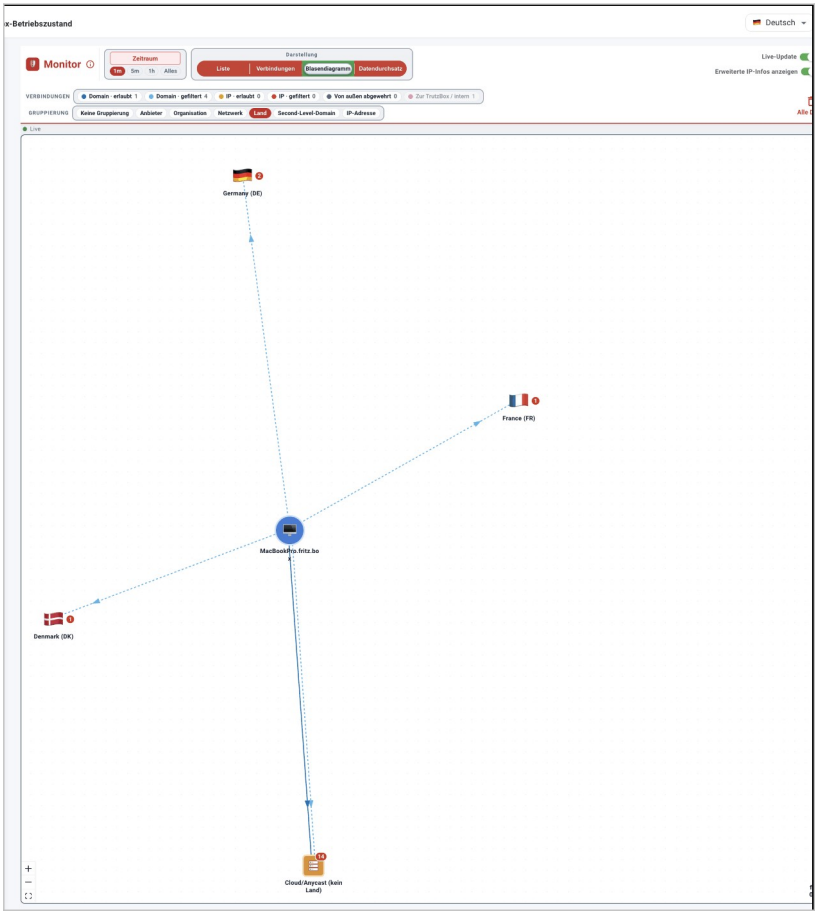
Menüpfad: Monitor



Ein einziger Seitenaufruf im Monitor der TrutzBox: die Liste der dabei kontaktierten Drittdienste. (© 2026 Comidio GmbH)

In welche Länder die Daten dabei fließen, zeigt das Blasendiagramm des TrutzBox-Monitors, hier für denselben Seitenaufruf: Verbindungen nach Deutschland und Frankreich sowie zu weltweit verteilten Cloud-Diensten ohne festen Standort (Anycast):

Menüpfad: Monitor



Derselbe Seitenaufruf im Blasendiagramm: wohin die Verbindungen geografisch gehen.

Browser Fingerprinting: Tracking ohne Cookies

> **Für Einsteiger:**
> Stellen Sie sich vor, jemand könnte Sie allein an Ihrer Handschrift, der Farbe Ihrer Augen und Ihrem Gang erkennen, ohne Ihren Namen zu kennen. Genau das macht Browser Fingerprinting: Ihr Browser verrät durch seine technischen Eigenschaften so viel über sich, dass er in fast allen Fällen eindeutig einer bestimmten Person zuzuordnen ist. Cookies löschen hilft dabei nicht, der Fingerabdruck bleibt.

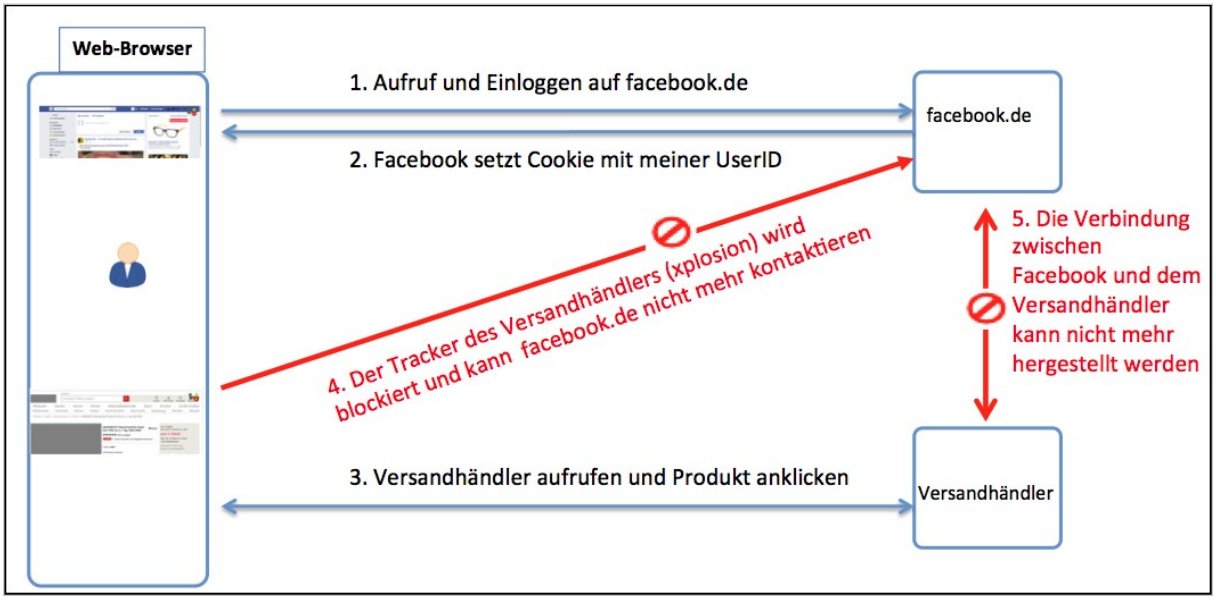
Wie Fingerprinting technisch funktioniert

Als Antwort auf die zunehmende Verbreitung von Cookie-Blockern haben Datenhändler und Tracking-Anbieter alternative Methoden entwickelt, die ohne Cookies funktionieren. Die wichtigste und wirkungsvollste ist das sogenannte Browser Fingerprinting. Die Idee dahinter ist einfach: Jeder Browser,

jedes Betriebssystem und jede Hardware-Konfiguration hat bestimmte einzigartige Eigenschaften. Durch die systematische Abfrage und Kombination dieser Eigenschaften entsteht ein „Fingerabdruck", der in der überwältigenden Mehrheit der Fälle eine bestimmte Person eindeutig identifiziert.

Welche Eigenschaften werden für das Fingerprinting genutzt? Zunächst die Standardinformationen aus dem User-Agent-Header: Betriebssystem und Version, Browser und Version, CPU-Architektur. Dann technische Browser-Eigenschaften: installierte Schriftarten, aktivierte Browser-Plugins und ihre Versionen, Bildschirmauflösung und Farbtiefe, Zeitzone, Systemsprache, Do-Not-Track-Einstellung, WebRTC IP-Adresse und Canvas/WebGL-Fingerprint. In der EFF-Studie „Panopticlick“ (2010) waren 84 Prozent der untersuchten Browser allein anhand solcher Merkmale eindeutig identifizierbar, mit aktiviertem Flash oder Java sogar 94 Prozent; neuere Großstudien kommen auf niedrigere, aber weiterhin erhebliche Anteile: Bei einer Untersuchung von Google-Forschern mit 8.400 Nutzern (2025) war der Fingerabdruck von rund 60 Prozent der Teilnehmer eindeutig, exakt der Wert, mit dem der kommerzielle Anbieter FingerprintJS wirbt.[84]

Auch ohne Cookies lässt sich ein Nutzer wiedererkennen:



Mit TrutzBox unterbleibt der Abgleich: Die Verbindung zwischen Versandhändler und Facebook kommt nicht zustande.
(© 2026 Comidio GmbH)

Canvas Fingerprinting

Canvas Fingerprinting ist eine besonders raffinierte Fingerprinting-Methode, die auf dem HTML5-Canvas-Element basiert. Ein unsichtbares JavaScript-Skript weist den Browser an, eine bestimmte geometrische Form oder einen Text auf einem versteckten Canvas-Element zu zeichnen. Da verschiedene Geräte dieselbe Zeichenanweisung aufgrund unterschiedlicher Grafiktreiber, Hardware-Beschleunigung und Betriebssystem-Render-Bibliotheken minimal unterschiedlich ausführen, entsteht ein pixelgenaues

[84] Eckersley, P.: How Unique Is Your Web Browser? Privacy Enhancing Technologies Symposium (PETS), 2010. Laperdrix, P. et al.: Browser Fingerprinting: A survey. ACM Transactions on the Web, 14(2), 2020. doi:10.1145/3386040. Gómez-Boix, A. et al.: Hiding in the Crowd: an Analysis of the Effectiveness of Browser Fingerprinting at Large Scale. WWW 2018 (2 Millionen Fingerprints, 33,6 Prozent eindeutig). Berke et al. (Google): How Unique is Whose Web Browser? PoPETs 2025 (8.400 US-Nutzer, rund 60 Prozent eindeutig).

Abbild, das für jede Hardware-Konfiguration nahezu einzigartig ist. Diese Methode ist für den Nutzer vollständig unsichtbar, sie erscheint nicht in der URL, produziert keinen Netzwerkverkehr, der in Standard-Monitoring-Tools sichtbar wäre, und wird von keinem einfachen Cookie-Blocker verhindert.[85]

AudioContext Fingerprinting

AudioContext Fingerprinting nutzt die Art, wie verschiedene Geräte Audiosignale mathematisch verarbeiten. Ein JavaScript-Skript erzeugt einen Audiosignal-Oszillator und analysiert, wie der Browser dieses Signal verarbeitet und zusammenfasst. Die minimalen Unterschiede in der Audio-Verarbeitungspipeline verschiedener Hardware und Software-Konfigurationen erzeugen einen einzigartigen numerischen Wert, ohne dass jemals ein hörbares Geräusch erzeugt wird.

WebGL Fingerprinting und Schriftarten-Erkennung

WebGL (Web Graphics Library) ist eine JavaScript-API für 3D-Grafiken im Browser. WebGL Fingerprinting analysiert die spezifische Rendering-Fähigkeit der Grafikkarte, die verwendeten WebGL-Parameter und die unterstützten Erweiterungen. Auch die Erkennung installierter Schriftarten ist eine klassische Methode: Durch das Rendern von Text in verschiedenen Schriftarten und das Messen der exakten Textbreite (die je nach installierter Schriftart variiert) kann ein Browser-Skript ermitteln, welche Schriftarten auf dem System installiert sind.

Die Kombination all dieser Methoden (Canvas, AudioContext, WebGL, Schriftarten, Zeitzone, Bildschirmauflösung und weitere Parameter) ergibt einen digitalen Fingerabdruck, der selbst nach vollständiger Browser-Neuinstallation und nach dem Löschen aller Cookies weiterhin funktioniert. In einer Studie von Cao et al. (Lehigh University/Washington University) konnten 99,2 Prozent der Nutzer in einem Fingerprint-Datensatz über Browserwechsel und Cookie-Löschungen hinweg kontinuierlich verfolgt werden.[86]

Session Replay: Vollständige Verhaltensaufzeichnung

Für Einsteiger:

Manche Websites schauen Ihnen buchstäblich über die Schulter: Sie zeichnen jeden Mausklick, jede Tastatureingabe und jede Mausbewegung auf, wie eine Videoaufnahme alles dessen, was Sie auf der Seite tun. Das nennt sich Session Replay und wird von Websitebetreibern zur Verbesserung ihrer Seiten eingesetzt. Problematisch wird es, wenn solche Aufzeichnungen auf sensiblen Seiten laufen, etwa beim Ausfüllen medizinischer Formulare oder beim Online-Banking.

[85] Mowery, K. / Shacham, H.: Pixel Perfect: Fingerprinting Canvas in HTML5. USENIX Security Symposium, 2012. Erste akademische Beschreibung der Canvas-Fingerprinting-Methode.

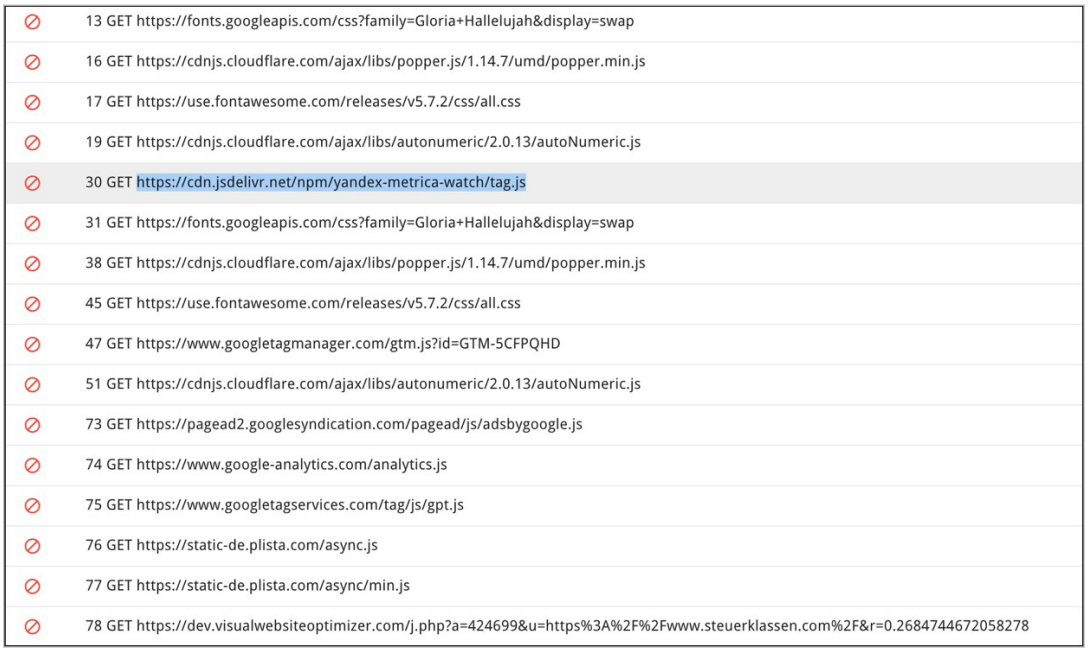
[86] Cao, Y. / Li, S. / Wijmans, E.: (Cross-)Browser Fingerprinting via OS and Hardware Level Features. Network and Distributed System Security Symposium (NDSS), 2017. 99,24 Prozent der Nutzer waren über Browserwechsel hinweg identifizierbar.

🔧 Session Replay. Technologie und Risiken

Session Replay ist eine Tracking-Methode, die weit über das Sammeln von Metadaten hinausgeht und eine nahezu vollständige Verhaltensaufzeichnung des Nutzers auf einer Website ermöglicht. Anbieter wie Hotjar, FullStory, LogRocket, Mouseflow und SessionCam bieten Websitebetreibern an, jeden Mausklick, jede Tastatureingabe, jede Mausbewegung und jeden Scroll-Vorgang eines Besuchers in Echtzeit aufzuzeichnen und in Form von „Session Replays", quasi Video-Aufzeichnungen des Browserfensters, wiederzugeben.

Aus der Perspektive des Websitebetreibers ist das ein wertvolles Werkzeug für die Benutzerfreundlichkeits-Analyse (UX-Optimierung): Wo klicken Nutzer? Wo verlassen sie die Seite? Welche Formularfelder bereiten Probleme? Aus der Perspektive des Nutzers ist es eine vollständige Verhaltensüberwachung, die weit sensibler ist als ein einfaches Cookie. Besonders problematisch wird Session Replay, wenn es auf Seiten mit sensiblen Formularen eingesetzt wird. Eine 2017 veröffentlichte Studie der Princeton University untersuchte 50.000 der meistbesuchten Websites und fand auf über 480 davon aktive Session-Replay-Skripte, darunter Seiten mit medizinischen Formularen, Kreditkartenanträgen und psychologischen Tests. Eine Nachfolgestudie von 2025 über die eine Million meistbesuchten Websites fand auf 38,5 Prozent der Seiten Fremdskripte, die Tastatureingaben mitlesen; mindestens 3,2 Prozent übertragen die abgefangenen Eingaben an Drittserver.[87]

Die TrutzBox blockiert Session-Replay-Dienstleister über ihre Sperrlisten, hier ein Beispiel:



Von den Sperrlisten der TrutzBox gestoppte Aufrufe, darunter ein Dienst zur Aufzeichnung des Nutzerverhaltens.
(© 2026 Comidio GmbH, TrutzBox-Bildschirmkopie)

[87] Englehardt, S. et al.: No Boundaries: Exfiltration of Personal Data by Session-Replay Scripts. Princeton Web Transparency & Accountability Project, 15. November 2017. https://freedom-to-tinker.com/2017/11/15/no-boundaries-exfiltration-of-personal-data-by-session-replay-scripts/. Munir, Demir, Li, Kollnig, Shafiq: Every Keystroke You Make. arXiv 2508.19825, August 2025.

Teil 5
Standortdaten

Das Smartphone als Peilsender: Werbe-ID, Databroker Files und was daraus folgt

Smartphones und mobile Daten

Für Einsteiger:

Ihr Smartphone ist das persönlichste Gerät, das Sie besitzen, und gleichzeitig das effektivste Überwachungsgerät, das je erfunden wurde. Es kennt Ihren genauen Standort, Ihre Kommunikation, Ihre Gesundheitsdaten, Ihre sozialen Kontakte und Ihre täglichen Routinen. All das fließt, wenn keine Schutzmaßnahmen aktiv sind, zu Datenhändlern, Werbefirmen und im schlimmsten Fall zu Kriminellen.

Advertising ID, IP-Tracking und Probabilistic Matching

Smartphones sind die effektivsten Datensammelgeräte, die Menschen je mit sich herumgetragen haben. Sie kennen unseren Standort in Echtzeit, unsere Kommunikation, unsere Apps und damit unsere Interessen, unseren Gesundheitszustand (Fitness-Apps, Health-Apps, Symptom-Tracker), unsere sozialen Verbindungen, unsere täglichen Routinen, unsere Reisegewohnheiten, unsere Zahlungsgewohnheiten und, in zunehmendem Maße, sogar unseren emotionalen Zustand.

Zwei Identifikationsmechanismen sind für das mobile Tracking besonders relevant. Die Advertising ID (bei Apple als IDFA, Identifier for Advertisers, bei Android als GAID, Google Advertising ID, bezeichnet) ist eine eindeutige, gerätespezifische Kennung, die ursprünglich für Werbezwecke gedacht war. Im Unterschied zu einem Cookie lässt sie sich nicht einfach durch das Löschen von Browser-Daten entfernen. Seit iOS 14.5 (April 2021) müssen Apps bei Apple explizit die Erlaubnis des Nutzers einholen, bevor sie auf die IDFA zugreifen dürfen. Auch 2026 stimmen weltweit nur rund 27 Prozent der iOS-Nutzer dem Tracking zu, in Deutschland 24 Prozent; wird der Dialog tatsächlich angezeigt, willigt etwa die Hälfte ein. Google kündigte 2022 mit der „Privacy Sandbox für Android“ ähnliche Maßnahmen an, gab das Projekt im Oktober 2025 jedoch auf; die Werbe-ID bleibt unter Android standardmäßig aktiv.[88]

Neben der Advertising ID ist die IP-Adresse der zweite wichtige Identifikator. Selbst ohne Advertising ID kann eine App die IP-Adresse des Geräts übermitteln, die zusammen mit anderen Geräteparametern für eine Identifizierung ausreicht. Hinzu kommt das sogenannte Probabilistic Matching: Auch ohne eindeutigen Identifier können Datenhändler über statistische Methoden mit hoher Wahrscheinlichkeit bestimmen, ob zwei verschiedene Datenpunkte zur selben Person gehören, basierend auf Geolokation, Tageszeit und Verhaltensmustern.

[88] Apple: App Tracking Transparency Framework. Developer Documentation, 2021. Adjust: ATT Opt-in Rates 2025/2026; AppsFlyer: Privacy Pulse 2025; Zusammenstellung Digital Applied, 21. April 2026 (global 27 Prozent, Deutschland 24 Prozent).

Apple gegen die Werbeindustrie: Wie App Tracking Transparency ausgehebelt wird

Apples Abfrage „Erlauben, dass App dich trackt?“ (App Tracking Transparency, ATT) ist seit 2021 die wirksamste einzelne Maßnahme gegen mobiles Tracking, und seit 2025 das Ziel einer koordinierten Gegenoffensive der Werbewirtschaft, ausgetragen vor Wettbewerbsbehörden. Der Vorwurf lautet nicht, ATT schütze zu wenig, sondern zu einseitig: Apple zwinge Drittanbietern eine zusätzliche Abfrage auf, während die eigene Werbesparte Apple Ads mit einem einzigen, freundlicher formulierten Dialog auskomme. Die französische Wettbewerbsbehörde verhängte im März 2025 150 Millionen Euro, der Datenschutz sei legitim, die Umsetzung aber „weder notwendig noch verhältnismäßig“. Die italienische Kartellbehörde folgte im Dezember 2025 mit 98,6 Millionen Euro wegen „unfairer und unverhältnismäßiger“ Bedingungen; Polen und Rumänien eröffneten Verfahren, in Großbritannien fordern App-Entwickler zwei Milliarden Pfund Schadensersatz.[89]

Den entscheidenden Schritt erzwang das Bundeskartellamt: Nach vierjährigem Verfahren erklärte es im August 2026 Zusagen Apples für verbindlich, die ab Oktober 2026 EU-weit gelten. Die Abfrage für Apples eigene Apps und für Fremd-Apps wird „im Wesentlichen angeglichen“; das Wort „tracken“ verschwindet aus dem Dialog, die Schaltflächen heißen künftig „Erlauben“ und „Ablehnen“ statt „App bitten, nicht zu tracken“, das warnende orangefarbene Symbol wird blau, Entwickler dürfen die Abfrage mit ihrer DSGVO-Einwilligung verbinden, und Nutzer, die abgelehnt haben, jedes Jahr erneut fragen. Die EU-Kommission begrüßte die Änderungen; Datenschützer sprechen davon, dass eine Transparenzabfrage „weniger transparent“ gemacht werde. Für die Nutzer bedeutet das: Der Schutz bleibt formal bestehen, wird aber leiser, unauffälliger und jährlich neu zur Disposition gestellt.[90]

Wie durchlässig ATT ohnehin ist, zeigen Messungen. Schon 2022 stellten Oxford-Forscher fest, dass Apps nach Einführung von ATT zwar keine Werbe-ID mehr weitergaben, stattdessen aber Gerätemerkmale für probabilistisches Fingerprinting sammelten. Eine USENIX-Studie von 2024 fand in 59 Prozent von 4.000 untersuchten ATT-Dialogen manipulative Gestaltung, irreführende Texte, Belohnungsversprechen, verschwiegene Zwecke. Google-Forscher zählten 2025 in 178.000 Apps über 700 Familien von Software-Bausteinen, die Geräte-Fingerprints erheben, nur knapp ein Drittel davon für Werbung, der Rest für „Sicherheit“ oder unbekannte Zwecke, für die ATT gar nicht gilt. Im Juni 2025 deckten Forscher auf, dass Meta und Yandex auf Android-Geräten Browser-Kennungen über eine lokale Netzwerkverbindung an ihre installierten Apps durchreichten und so Inkognito-Modus und Berechtigungen umgingen; Meta stellte die Praxis am Tag der Veröffentlichung ein. Apple selbst kann die seit 2024 vorgeschriebenen „Privacy Manifests“, in denen Entwickler den Zweck heikler Schnittstellen erklären müssen, nicht überprüfen. Kritiker sprechen von einem „falschen Gefühl der Privatsphäre“. Und Apples eigenes Werbegeschäft wuchs seit ATT auf geschätzt sieben bis neun Milliarden US-Dollar jährlich.[91]

---

[89] Autorité de la concurrence: Targeted advertising, fine of 150,000,000 euros on Apple, 31. März 2025. Autorità Garante della Concorrenza e del Mercato: Verfahren A561, Entscheidung vom 16. Dezember 2025 (98,6 Mio. Euro). UOKiK: Is Apple restricting competition? President of UOKiK brings charges, 25. November 2025. Silicon Republic: Apple facing 2bn UK legal challenge over ATT policy, 3. September 2026.

[90] Bundeskartellamt: Pressemitteilung „Apple: Zusagen zum App Tracking Transparency Framework verbindlich“, 17. August 2026; FAQ zum Verfahren. 9to5Mac: The eight changes Apple is making to App Tracking Transparency in Europe, 18. August 2026. heise online: Nach Druck durch Bundeskartellamt. Apple schwächt Tracking-Warnung ab, August 2026. Eunews: Commission welcomes Apple’s changes, 18. August 2026.

[91] Kollnig et al.: Goodbye Tracking? Impact of iOS App Tracking Transparency and Privacy Labels. ACM FAccT 2022. Mohamed et al.: ATTention Please! An Investigation of the App Tracking Transparency Permission. USENIX Security 2024. Specter et al.: Fingerprinting SDKs for Mobile Apps and Where to Find Them. ACM CCS 2025. IMDEA Networks / Radboud / KU Leuven: Local Mess. Meta and Yandex bridging persistent identifiers to browsing histories, 3. Juni 2025. Mysk: Apple’s Required Reason API, a false sense of privacy, 3. Mai 2024. eMarketer: Apple ad business quietly contributes record services revenues, 2025 (US-Werbeumsatz 8,85 Mrd. USD 2025, Schätzung).

Parallel läuft der Machtkampf um den App Store, der die Privatsphäre indirekt berührt. Die EU-Kommission verhängte im April 2025 500 Millionen Euro nach dem Digital Markets Act, weil Apple Entwickler daran hinderte, Kunden auf günstigere Angebote außerhalb des App Store zu lenken; im März 2025 verpflichtete sie Apple, iOS-Funktionen wie Benachrichtigungen und Kopplung für fremde Smartwatches und Kopfhörer zu öffnen. Apple klagt dagegen, verzögerte in der EU Funktionen wie iPhone-Spiegelung und die KI-Version von Siri und argumentiert, der DMA zwinge es, Dritten „Zugang zu Nutzerdaten zu geben, die selbst Apple nicht sieht“, die Kommission hält dagegen, nichts im DMA verlange niedrigere Datenschutzstandards. In den USA befand ein Bundesgericht Apple im April 2025 der Missachtung einer Anordnung im Verfahren mit Epic Games für schuldig; der Supreme Court hat den Fall im Juni 2026 angenommen, das Justizministerium verhandelt seit Juli 2026 über einen Vergleich seiner Monopolklage. Ob am Ende mehr Wettbewerb oder mehr Tracking steht, entscheidet sich an Details wie der Formulierung eines Dialogfensters.[92]

utiq: Wenn der Netzbetreiber selbst zum Tracker wird

Unabhängig von Cookies und Werbe-IDs bietet seit 2024 auch der Mobilfunkvertrag selbst eine Wiedererkennung. Deutsche Telekom, Vodafone, Telefónica und Orange betreiben das Gemeinschaftsunternehmen utiq (vormals TrustPid), das die EU-Kommission 2023 genehmigt hat. Das Prinzip: Ruft ein Kunde über das Mobilfunknetz eine teilnehmende Website auf, kann der Netzbetreiber den Aufruf mit einem Kennzeichen versehen, das aus dem Vertrag abgeleitet ist. Verlage und Werbekunden erkennen den Nutzer damit wieder, auch wenn er Cookies löscht oder den Browser wechselt. Die Einwilligung wird nach Darstellung von utiq je Website eingeholt, in der Regel über die üblichen Einwilligungsbanner, die viele Nutzer für gewöhnliche Cookie-Abfragen halten. Ein Widerspruch über das utiq-Portal gilt nach den dortigen Nutzungsbedingungen (Stand 2026) nur für ein Jahr, ist nur aus dem Mobilfunknetz möglich und muss für jeden Vertrag getrennt erklärt werden.[93]

Der Mechanismus wirkt nur, wenn der Netzbetreiber den Aufruf sieht. Läuft der Datenverkehr des Smartphones über einen VPN-Tunnel ins eigene Heimnetz, erreicht die Anfrage die Website vom Festnetzanschluss aus, ohne Mobilfunk-Kennzeichen (siehe Kapitel „Tracking-Schutz für mobile Devices“).

Mobiles Tracking durch WLAN-Hotspots

Selbst ohne aktive GPS-Nutzung können mobile Geräte präzise geortet werden, durch WLAN-Scanning und WLAN-Hotspots. Smartphones senden im Standby-Modus regelmäßig sogenannte Probe-Requests aus, um bekannte WLAN-Netze in der Nähe zu finden. Diese Requests enthalten die MAC-Adresse des Geräts sowie die Namen (SSIDs) der bereits bekannten WLAN-Netze. Aus den SSIDs bekannter Netze kann auf die Bewegungshistorie des Gerätes geschlossen werden: Wer die SSIDs „HomeWLAN", „BüroNetz" und „McDonalds-Free-WiFi" im Gerätespeicher hat, hat sich offenkundig regelmäßig an diesen Orten aufgehalten.[94]

---

[92] Europäische Kommission: Commission finds Apple and Meta in breach of the Digital Markets Act, 23. April 2025 (IP/25/1085); Commission provides guidance under Digital Markets Act to facilitate development of innovative products on Apple’s platforms, 19. März 2025. Apple Newsroom: The Digital Markets Act’s impacts on EU users, 25. September 2025; Due to DMA, Siri AI delayed in EU for iOS 27, 8. Juni 2026. Epic Games v. Apple, N.D. Cal., Contempt Order vom 30. April 2025; Ninth Circuit, 11. Dezember 2025; Supreme Court, Zulassung der Revision Nr. 25-1311, 30. Juni 2026. Bloomberg: Apple in early settlement talks with DOJ over antitrust case, 17. Juli 2026.

[93] Europäische Kommission: Genehmigung des Gemeinschaftsunternehmens von Deutsche Telekom, Orange, Telefónica und Vodafone, IP/23/721, Februar 2023. c’t 6/2023: TrustPid. kuketz-blog.de: utiq, Tracking durch Mobilfunkanbieter. utiq.com, Consent Hub, Stand 2026.

[94] Cunche, M. / Kaafar, M.A. / Boreli, R.: I Know Who You Are and I Saw You. IEEE Communications Magazine, 2014.

Wer an verschiedenen Stellen WLAN-Router mit Logging-Funktion aufstellt, kann die Bewegungsprofile von Passanten erstellen, ohne dass diese sich einwählen oder irgendetwas tun müssen. Einzelhändler, Einkaufszentren und sogar Städte haben diese Technologie für Kundenströmungsanalysen eingesetzt.

Tracking über Bluetooth und BLE-Beacons

🔧 Bluetooth-Tracking: Von der Näherungserkennung zur Überwachung

Neben WLAN ist Bluetooth, insbesondere Bluetooth Low Energy (BLE), eine der am häufigsten genutzten Technologien zur Standorterfassung und Bewegungsverfolgung in geschlossenen Räumen. BLE-Beacons sind kleine, batteriebetriebene Sender, die in regelmäßigen Abständen ein Signal mit einer eindeutigen Kennung ausstrahlen. Smartphones in Reichweite, typischerweise 10 bis 30 Meter, empfangen diese Signale und können daraus ihre Position im Raum bestimmen. Die beiden verbreitetsten Standards sind Apples iBeacon und Googles Eddystone.

Einzelhändler, Einkaufszentren, Flughäfen und Museen setzen BLE-Beacons ein, um Kundenströme zu analysieren, personalisierte Angebote auf das Smartphone zu senden und Verweilzeiten vor bestimmten Regalen oder Exponaten zu messen. Der Nutzer muss dafür lediglich Bluetooth aktiviert haben und eine entsprechende App installiert haben, oder eine App, die im Hintergrund auf Beacon-Signale lauscht, ohne dass der Nutzer davon weiß. Studien zeigen, dass zahlreiche Shopping- und Coupon-Apps BLE-Scanning im Hintergrund durchführen.

Auch ohne Beacons ist Bluetooth-Tracking möglich. Geräte, die Bluetooth aktiviert haben, senden regelmäßig sogenannte Advertisement-Pakete mit ihrer MAC-Adresse. Obwohl neuere Betriebssysteme die MAC-Adresse randomisieren, haben Forscher der University of California San Diego 2022 gezeigt, dass Bluetooth-Geräte anhand subtiler Unterschiede in der Signalcharakteristik, sogenannter Physical-Layer Fingerprints, dennoch eindeutig identifiziert werden können. Diese hardwarebedingten Abweichungen sind für jedes Gerät einzigartig und lassen sich nicht per Software ändern.

Eine besondere Dimension hat das Bluetooth-Tracking durch Apples „Wo ist?“-Netzwerk (Find My) und ähnliche Systeme erhalten. AirTags und kompatible Tracker nutzen das weltweite Netz von Hunderten Millionen Apple-Geräten als passive Infrastruktur zur Standortermittlung. Jedes iPhone in der Nähe eines AirTags übermittelt dessen Position über Bluetooth an Apple-Server. Was als nützliches Hilfsmittel zum Wiederfinden von Schlüsseln und Koffern konzipiert wurde, wird nachweislich auch für Stalking missbraucht. Polizeiberichte aus den USA, Großbritannien und Deutschland dokumentieren Fälle, in denen AirTags heimlich in Handtaschen, Autos oder Kleidung von Opfern platziert wurden.

Databroker Files 2024: Standortdaten als Sicherheitsrisiko

> 💡 **Für Einsteiger:**
>
> Ihr Smartphone kennt jeden Schritt, den Sie gehen. Und diese Information können Fremde kaufen, für wenig Geld. Im Jahr 2024 machten Journalisten einen erschreckenden Test: Sie kauften Bewegungsdaten von Millionen deutschen Handys. Mit diesen Daten konnten sie herausfinden, wo Menschen wohnen, wo sie arbeiten, wen sie treffen und sogar, welche geheimdienstlichen Einrichtungen sie regelmäßig besuchen. Das alles war keine illegale Aktion, es war ein legaler Kauf auf einem offiziellen Datenmarktplatz. Jeder hätte diese Daten kaufen können.

🔧 Technischer Hintergrund

Im Juli 2024 veröffentlichten netzpolitik.org und der Bayerische Rundfunk (BR) die Ergebnisse einer monatelangen Investigativrecherche, die mit dem Grimme Online Award 2024 (Kategorie Spezial), dem Datenschutz Medienpreis 2024 und dem European Press Prize 2025 ausgezeichnet wurde: die Databroker Files. Die Geschichte begann im Januar 2024 mit einem Tipp des niederländischen Investigativjournalisten Eric van den Berg, der über einen Berliner Datenmarktplatz berichtet hatte. Dieser Marktplatz heißt Datarade und vermittelt mit Sitz in Berlin Kontakte zwischen Datenhändlern und Käufern aus aller Welt.[95]

Das Rechercheteam wandte sich mit offener journalistischer Identität an den US-amerikanischen Datenhändler Datastream Group mit Sitz in Florida. Als kostenlose Kostprobe, gewissermaßen als Werbung für ein kostenpflichtiges Jahresabonnement im Wert von rund 14.000 US-Dollar, erhielt das Team einen Datensatz mit 3,6 Milliarden Standorteinträgen von bis zu 11 Millionen deutschen Mobilgeräten. Die Daten umfassten zwei Monate aus dem Herbst 2023 und enthielten für jedes Gerät eine eindeutige Werbe-ID (IDFA oder GAID), präzise GPS-Koordinaten, Zeitstempel sowie teilweise die zugehörige App-ID.[96]

Die Auswertung der Daten offenbarte eine neue Dimension der Massenüberwachung. Aus den Bewegungsprofilen ließen sich für die meisten Geräte problemlos Wohnort und Arbeitsort ableiten, und damit konkrete Personen identifizieren. Das Rechercheteam identifizierte unter anderem:

- Mitarbeiter von Bundesministerien, deren morgendliche Pendelrouten vom Wohnort zum Ministerium in Berlin nachvollziehbar waren[97]
- Personen, die für einen deutschen Geheimdienst arbeiten, identifiziert anhand regelmäßiger Besuche an einer bekannten Geheimdienstadresse[98]
- Bundeswehrangehörige auf Kasernengeländen, deren Bewegungsprofile systematisch ausgewertet werden könnten[99]
- Einen Grindr-Nutzer in Norwegen, der auf keinen Fall gefunden werden wollte, geoutet durch seine GPS-Daten[100]

Die politische Reaktion war unmittelbar. Das Büro des US-Senators Ron Wyden schaltete im Sommer 2024 das Pentagon ein, nachdem Berichte über amerikanische Soldaten in deutschen Kasernen die USA erreicht hatten; im Mai 2026 machte Wyden mit 13 weiteren Abgeordneten öffentlich, dass das US-Zentralkommando den Einsatz kommerzieller Standortdaten durch gegnerische Kräfte gegen US-Soldaten im Nahen Osten bestätigt hatte. Die damals designierte Bundesdatenschutzbeauftragte Louisa Specht-Riemenschneider sprach von einer „Rechtsschutzlücke". Konstantin von Notz (Grüne), Vorsitzender des Parlamentarischen Kontrollgremiums, bezeichnete den Zustand als „unhaltbar". Katharina Barley (SPD), Vizepräsidentin des EU-Parlaments, sah eine „klaffende Lücke" beim Schutz personenbezogener Daten.[101]

---

[95] Sebastian Meineck, Ingo Dachwitz, netzpolitik.org; Katharina Brunner, Rebecca Ciesielski, Maximilian Zierer, Robert Schöffel, Eva Achinger, BR Data: „Wie Datenhändler Deutschlands Sicherheit gefährden", 16. Juli 2024. Übersichtsseite: https://netzpolitik.org/2024/databroker-files-die-grosse-datenhaendler-recherche-im-ueberblick/

[96] netzpolitik.org / BR: „Firma verschleudert 3,6 Milliarden Standorte von Menschen in Deutschland", 16. Juli 2024. https://netzpolitik.org/2024/databroker-files-firma-verschleudert-36-milliarden-standorte-von-menschen-in-deutschland/

[97] netzpolitik.org / BR: Databroker Files, 16. Juli 2024.

[98] netzpolitik.org / BR: Databroker Files, 16. Juli 2024.

[99] WIRED / netzpolitik.org / BR: „Anyone Can Buy Data Tracking US Soldiers and Spies", November 2024.

[100] netzpolitik.org / BR: Databroker Files. Outing durch Standortdaten, 2024.

Eine Folgeveröffentlichung im November 2024, gemeinsam mit WIRED, zeigte, dass dieselben Methoden nicht nur in Deutschland, sondern global funktionieren. In einem Datensatz mit 380 Millionen Standortdaten aus 137 Ländern fanden sich Bewegungsprofile von Nutzern von Wetter Online, Focus Online und Kleinanzeigen, und von 40.000 verschiedenen Apps weltweit. Auch NATO-Stützpunkte und Nuklearanlagen in Deutschland konnten kartiert werden.[102]

[101] netzpolitik.org / BR: Databroker Files. Wie Datenhändler NATO und US-Militär bloßstellen, 20. November 2024 (Kontakt des Wyden-Büros zum Pentagon im Sommer 2024). Senator Ron Wyden u. a.: Brief an den CIO des US-Verteidigungsministeriums, 28. Mai 2026 (CENTCOM-Bestätigung vom 14. April 2026). Heise Online: Politischer Aufruhr nach Databroker-Recherche, Juli 2024.

[102] WIRED / netzpolitik.org / BR: „Anyone Can Buy Data Tracking US Soldiers and Spies to Nuclear Vaults and Brothels in Germany", 20. November 2024.

Im April 2026 wurde das Rechercheprojekt als ARD-Dokumentation „Gefährliche Apps: Im Netz der Datenhändler“ verfilmt. Die Ergebnisse und vier eindringliche Fallbeispiele beschreiben die folgenden Abschnitte.

Was Tracker über einen Smartphone-Besitzer wissen: permanente Standortermittlung

> **Für Einsteiger:**
> GPS-Daten klingen zunächst harmlos: Koordinaten auf einer Karte. Aber aus einem längeren Bewegungsprofil lässt sich erschreckend viel über eine Person ableiten, ohne dass auch nur ein einziges persönliches Wort gesprochen oder geschrieben wurde. Die folgenden Abschnitte zeigen Schritt für Schritt, was Tracker aus einem kontinuierlichen Standortdatenstrom über Sie herausfinden können, von Ihrer Wohnadresse bis zu Ihrem Gesundheitszustand.

Persönlichkeitsprofile aus GPS-Daten

Das Smartphone in der Hosentasche ist kein passives Kommunikationsgerät. Es ist ein aktives Überwachungsinstrument, das, sofern Tracker ungehindert arbeiten können, ein erschreckend vollständiges Bild seines Besitzers zeichnet. Die permanente Standortermittlung durch GPS, WLAN-Scanning, Mobilfunkzellentriangulation und Bluetooth-Signale liefert dabei eine Datentiefe, die weit über das hinausgeht, was die meisten Nutzer für möglich halten. Der folgende Abschnitt beleuchtet systematisch, was aus einem kontinuierlichen Standortdatenstrom über eine Person abgeleitet werden kann, und warum diese Daten, obwohl sie technisch anonym erscheinen, in der Praxis ein vollständiges Persönlichkeitsprofil ergeben.

Wohnort und Lebensmittelpunkt

Der einfachste und zuverlässigste Rückschluss aus Standortdaten: Wo hält sich das Gerät nachts regelmäßig auf? Diese Koordinaten entsprechen in nahezu allen Fällen der Wohnadresse des Besitzers. Da Standortdaten typischerweise mit Zeitstempeln versehen sind, lässt sich die genaue Adresse durch simple Häufigkeitsanalyse der GPS-Koordinaten zwischen 22:00 und 07:00 Uhr bestimmen. Die Databroker Files bestätigten dies: Im untersuchten Datensatz konnten die Wohnadressen der Betroffenen mit einer Genauigkeit von wenigen Metern ermittelt werden, ohne Namen, ohne Registrierungsdaten, allein aus dem Bewegungsmuster.[103]

Arbeitgeber und berufliche Tätigkeit

Analog zur Wohnadresse ergibt sich der Arbeitsplatz aus dem häufigsten Aufenthaltsort während der Kernarbeitszeiten (09:00 bis 17:00 Uhr an Werktagen). In Verbindung mit öffentlich verfügbaren Informationen, etwa dem Namen des Unternehmens an dieser Adresse aus Google Maps oder

[103] Meineck / Dachwitz, netzpolitik.org / BR: Databroker Files. Methodik der Personenidentifikation, 16. Juli 2024.

OpenStreetMap, lässt sich automatisiert der Arbeitgeber ermitteln. Zusätzlich können aus der Häufigkeit der Anwesenheit, den Arbeitszeiten und der Positionierung im Gebäude Rückschlüsse auf die berufliche Hierarchiestufe gezogen werden: Wer jeden Tag das Bürogebäude betritt, aber selten im Meetingraum des Vorstands sitzt, ist vermutlich kein Führungsmitarbeiter, und umgekehrt. Die Databroker Files identifizierten auf diese Weise Mitarbeiter von Bundesministerien, der Bundeswehr und deutschen Geheimdiensten.[104]

Fachkonferenzen, Messen und Kongresse: Der Besuch einer IT-Fachmesse, einer medizinischen Fachtagung, eines Bankenkongresses oder einer Rüstungsmesse verrät Branchenzugehörigkeit, fachliche Interessen und berufliche Schwerpunkte. Wer die Hannover Messe besucht und dort drei Tage in Halle 9 (Antriebstechnik) verbringt, ist kein zufälliger Besucher. Wer eine Cybersecurity-Konferenz wie die Black Hat besucht, gibt Aufschluss über seine IT-Sicherheitsrolle. Wer regelmäßig Immobilienmessen aufsucht, plant offensichtlich Investitionen. Für Wettbewerber, Headhunter oder Geheimdienste sind das hochrelevante Informationen.

Von der Identifizierung zur Erpressbarkeit: Kritische Standorte

Wohnort und Arbeitsplatz sind der Schlüssel: Sobald ein Datensatz diese beiden Koordinaten enthält, ist die angeblich anonyme Werbe-ID einer konkreten Person zugeordnet. Jeder weitere Standort in diesem Datensatz wird damit zu einer persönlichen Information über einen identifizierten Menschen. Und genau hier liegt die eigentliche Gefahr: Viele Orte, die Menschen aufsuchen, sind harmlos. Supermarkt, Bäckerei, Tankstelle. Aber eine erhebliche Zahl von Standorten ist hochsensibel, weil sie Rückschlüsse auf Lebensumstände zulassen, die die Betroffenen um jeden Preis verborgen halten wollen.

Sexuelle Orientierung und Identität: Der regelmäßige Besuch von LGBTQ-Bars, schwulen oder lesbischen Clubs, CSD-Veranstaltungen oder queeren Beratungsstellen verrät die sexuelle Orientierung einer Person. In den Databroker Files wurde der Fall eines Grindr-Nutzers in Norwegen dokumentiert, der allein durch seine GPS-Daten geoutet werden konnte. In 65 Staaten weltweit (ILGA World, Mai 2026) steht Homosexualität unter Strafe, dort können solche Standortdaten lebensbedrohlich sein. Aber auch in Deutschland kann ein unfreiwilliges Outing das soziale Umfeld, die Familie oder die berufliche Existenz eines Menschen zerstören.

Ehe- und Beziehungskrisen: Besuche bei einem Scheidungsanwalt, einer Ehe- oder Paarberatung oder einer Mediation sind in Standortdaten eindeutig erkennbar. Wer regelmäßig eine Kanzlei für Familienrecht aufsucht, plant möglicherweise eine Trennung, eine Information, die in Sorgerechtsstreitigkeiten, Unterhaltsverfahren oder schlicht als Druckmittel missbraucht werden kann. Ebenso verraten Standortdaten außereheliche Beziehungen: regelmäßige Besuche an einer fremden Privatadresse zu ungewöhnlichen Zeiten lassen sich automatisiert erkennen.

Schwangerschaft und reproduktive Entscheidungen: Besuche bei einer Schwangerschaftskonfliktberatung, einer Abtreibungsklinik oder einem Reproduktionsmediziner sind aus Standortdaten direkt ableitbar. Die ARD-Dokumentation von 2026 zeigte den Fall einer Frau aus Texas, deren Reise zu einer Abtreibungsklinik in Colorado über Databroker-Daten hätte rekonstruiert werden können, mit strafrechtlichen Konsequenzen in ihrem Heimatstaat. Auch in Deutschland, wo Schwangerschaftsabbrüche unter bestimmten Bedingungen legal sind, ist die gesellschaftliche

[104] netzpolitik.org / BR: Wie Datenhändler Deutschlands Sicherheit gefährden. Methodik der Identifikation sicherheitsrelevanter Personen, 16. Juli 2024.

Stigmatisierung erheblich. Standortdaten, die den Besuch einer entsprechenden Einrichtung belegen, können für Erpressung oder soziale Ächtung genutzt werden.

Sucht und psychische Erkrankungen: Der Besuch von Suchtberatungsstellen, Entzugskliniken, Methadon-Ausgabestellen, Treffen der Anonymen Alkoholiker oder psychiatrischen Tageskliniken hinterlässt eindeutige Spuren. In den Databroker Files fand sich der Fall einer Person, die regelmäßig ein Gebäude besuchte, in dem eine Selbsthilfegruppe für Suchterkrankte tagt, damit war die Person in der Datenbank faktisch mit einer Suchterkrankung assoziiert. Für Arbeitgeber, Versicherungen oder das persönliche Umfeld wären solche Informationen verheerend.

Politische Aktivitäten und Demonstrationen: Wer an einer Klimaschutzdemo, einer Pegida-Veranstaltung, einem Gewerkschaftstreffen oder einer Kundgebung gegen Waffenexporte teilnimmt, hinterlässt Standortdaten, die seine politische Haltung offenlegen. In autoritären Staaten ist die Teilnahme an Protesten lebensgefährlich. Aber auch in Demokratien kann die Zuordnung zu einer politischen Bewegung berufliche Konsequenzen haben: Ein Polizeibeamter auf einer linksradikalen Demo, ein Richter auf einer AfD-Kundgebung, eine Lehrerin auf einer Legalisierungsveranstaltung. Standortdaten machen solche Zusammenhänge sichtbar und potentiell erpressbar.

Strafverteidigung, Justiz und Strafvollzug: Regelmäßige Besuche bei einem Strafverteidiger, einer Bewährungshilfe oder einem Gericht deuten auf strafrechtliche Verwicklungen hin. Besuche in einer Justizvollzugsanstalt, ob als Insasse, der Freigang hat, oder als Angehöriger, der regelmäßig einen Inhaftierten besucht, lassen sich aus Standortdaten eindeutig ablesen. Wer jeden Samstag dieselbe JVA aufsucht, hat offensichtlich eine enge Verbindung zu einem Gefangenen. In den Händen von Arbeitgebern, Vermietern oder Versicherungen können solche Daten existenzbedrohend sein.

Sensible Arbeitsorte und Berufsgeheimnisse: Der Arbeitsplatz verrät nicht nur den Arbeitgeber, sondern oft auch die konkrete Tätigkeit. Wer täglich ein Gebäude des Bundesnachrichtendienstes betritt, arbeitet vermutlich für den Geheimdienst. Wer regelmäßig eine Kaserne der Spezialkräfte aufsucht, ist wahrscheinlich KSK-Soldat. Aber auch zivile Arbeitsplätze können sensibel sein: Mitarbeiter von Rüstungsunternehmen, Kernkraftwerken, forensischen Laboren, Drogenentzugskliniken, Abtreibungskliniken oder Abschiebezentren haben allesamt Berufsgeheimnisse oder gesellschaftlich umstrittene Tätigkeiten, die durch Standortdaten offengelegt werden. Die Databroker Files identifizierten auf diese Weise Mitarbeiter von Bundesministerien und Geheimdiensten, und die ARD-Dokumentation 2026 zeigte, dass deutsche Rüstungsunternehmen die Enttarnung ihrer geheimen Produktionsstätten in der Ukraine fürchten.

Rotlichtmilieu und Sexualverhalten: Besuche in Bordellen, Swingerclubs, Laufhäusern, Erotik-Kinos oder bei Escort-Services sind in Standortdaten genauso sichtbar wie jeder andere Aufenthaltsort. Für Personen des öffentlichen Lebens, etwa Politiker, Geistliche oder Unternehmensführer, können solche Daten karrierezerstörend sein. Im Xandr-Datenkatalog fanden sich Kategorien wie „Adult Entertainment“ als käufliche Werbesegmente.

Frauenhäuser und Schutzeinrichtungen: Besonders gefährlich wird Standort-Tracking für Personen, die vor häuslicher Gewalt in ein Frauenhaus geflohen sind. Die Adressen dieser Schutzeinrichtungen sind aus gutem Grund geheim. Wenn die Standortdaten des Smartphones einer geflüchteten Frau in einer Databroker-Datenbank landen, kann der gewalttätige Partner, oder ein von ihm beauftragter Dritter, die Adresse des Frauenhauses ermitteln. Dasselbe gilt für Zeugenschutzprogramme und sichere Häuser für bedrohte Journalisten oder Whistleblower.

Glücksspiel und Verschuldung: Regelmäßige Besuche von Spielhallen, Wettbüros, Casinos oder Online-Glücksspiel-Lounges lassen auf eine mögliche Spielsucht schließen. In Kombination mit Besuchen

bei Schuldnerberatungsstellen, Pfandleihhäusern oder dem Insolvenzgericht entsteht ein Profil finanzieller Verzweiflung, das für Erpressung oder gezielte Manipulation nutzbar ist.

Die entscheidende Erkenntnis: Jeder dieser Standorte ist für sich genommen ein Datenpunkt. Aber in Kombination mit der Identität der Person, ermittelt aus Wohnort und Arbeitsplatz, werden sie zu einem detaillierten Erpressungsprofil. Und diese Daten liegen nicht bei einem Geheimdienst, der richterlichen Kontrollen unterliegt. Sie liegen bei kommerziellen Datenhändlern, die sie für wenige tausend Dollar an jeden verkaufen, der ein Formular ausfüllt.

Doch nicht nur offensichtlich sensible Orte sind problematisch. Auch Orte, die für sich genommen harmlos wirken, vervollständigen das Profil entscheidend: Messen, Vereine, Treffen, Einkäufe. Was sich daraus ablesen lässt, zeigen die folgenden Abschnitte. Je mehr Datenpunkte ein Profil enthält, desto berechenbarer und manipulierbarer wird der Mensch dahinter.

Soziales Umfeld und Beziehungsnetz

Wer trifft sich regelmäßig mit wem? Aus Standortdaten mehrerer Personen, wie sie ein Datenhändler mit Zugang zu Millionen von Profilen hat, lässt sich ableiten, welche Geräte (und damit Personen) sich regelmäßig zur selben Zeit am selben Ort aufhalten. Treffen zwei Geräte täglich morgens an Adresse X und gelegentlich abends an Adresse Y, handelt es sich sehr wahrscheinlich um Arbeitskollegen und möglicherweise um ein Paar. Regelmäßige Besuche eines bestimmten Hauses an Wochenenden deuten auf Familie oder enge Freunde hin. Diese Co-Location-Analyse ist ohne Kenntnis der Telefonnummern, ohne Zugriff auf Kontaktbücher und ohne Abhören von Gesprächen möglich, allein aus den GPS-Koordinaten.[105]

Treffen mit anderen identifizierten Personen: Besonders aufschlussreich wird Standort-Tracking, wenn die Profile mehrerer Personen miteinander abgeglichen werden. Wenn ein Kommunalpolitiker sich regelmäßig mit einem Immobilienentwickler in einem Restaurant trifft, entsteht der Verdacht der Vetternwirtschaft. Wenn ein Manager eines Unternehmens wiederholt einen Manager eines Konkurrenten in einem Hotel trifft, liegt der Verdacht einer Absprache nahe. Wenn ein Journalist sich regelmäßig an einem abgelegenen Ort mit einem Ministeriumsmitarbeiter trifft, deutet das auf einen Informanten hin. Und wenn eine verheiratete Person regelmäßig dieselbe Privatwohnung aufsucht wie eine andere identifizierte Person, liegt der Schluss auf eine Affäre nahe. Die Databroker-Datensätze enthalten Millionen von Profilen, die Möglichkeiten der Kreuzreferenzierung sind nahezu unbegrenzt.

Religionszugehörigkeit und politische Überzeugung

Standortdaten verraten, welche Institutionen jemand regelmäßig aufsucht. Wer jeden Freitag eine Moschee besucht, jeden Sonntag eine Kirche oder regelmäßig eine Synagoge, das ist aus GPS-Daten unmittelbar ableitbar. In Verbindung mit einer Datenbank öffentlich bekannter Adressen von Gotteshäusern, politischen Büros und Parteizentralen entsteht ein detailliertes Bild religiöser und politischer Überzeugungen. Die Xandr-Datenbankeinträge zeigen, dass genau diese Informationen in kommerziellen

[105] De Montjoye, Y.A. et al.: Unique in the Crowd: The privacy bounds of human mobility. Scientific Reports 3, 1376 (2013). doi:10.1038/srep01376

Datenhändler-Systemen als Zielgruppensegmente gehandelt werden: „regelmäßige Kirchgänger", „Besucher von Moscheen", „Teilnehmer politischer Veranstaltungen".[106]

Thematische Ausstellungen und Kulturveranstaltungen: Der Besuch einer Waffenmesse, einer Esoterik-Ausstellung, einer Infoveranstaltung einer umstrittenen religiösen Gruppierung, eines Reichsbürger-Vortrags oder einer Veranstaltung der Identitären Bewegung ist für sich genommen legal, kann aber in einem Profil als Indiz für Radikalisierung, Extremismus oder Verschwörungsanfälligkeit gewertet werden. Auch vermeintlich harmlose kulturelle Präferenzen wie Opernbesuche, Punk-Konzerte, Schützenvereinsfeste oder Poetry-Slams verfeinern das Persönlichkeitsprofil und machen den Menschen berechenbarer.

Gesundheitszustand und medizinische Behandlungen

Regelmäßige Besuche einer Arztpraxis, einer Klinik, eines Krankenhauses oder einer Apotheke hinterlassen eindeutige Spuren in den Standortdaten. Aus der Häufigkeit, dem Fachgebiet der aufgesuchten Einrichtung (Onkologie, Psychiatrie, Suchtmedizin, Reproduktionsmedizin) und der Regelmäßigkeit der Besuche lassen sich mit hoher Wahrscheinlichkeit medizinische Diagnosen oder zumindest Krankheitsverdachte ableiten. Welche konkreten Gesundheitseinrichtungen, Beratungsstellen und medizinischen Orte besonders sensibel sind, wird im vorangehenden Abschnitt „Kritische Standorte“ im Detail beschrieben.

Die Xandr-Datenbank enthielt käufliche Werbesegmente wie „Besucher von Krebszentren“, „mögliche Schwangerschaft“ und „psychische Erkrankung“. Dies sind nicht hypothetische Szenarien, dies ist dokumentierte Praxis des Datenhandels.

Hinzu kommen Datenbestände, die nicht aus Tracking stammen, aber dieselben Begehrlichkeiten wecken. Seit Januar 2025 erhalten gesetzlich Versicherte automatisch eine elektronische Patientenakte, sofern sie nicht widersprechen; seit März 2024 stehen Abrechnungsdaten der Krankenkassen nach dem Gesundheitsdatennutzungsgesetz der Forschung ebenfalls mit Widerspruchslösung zur Verfügung. Die Daten werden pseudonymisiert, doch der Bundesbeauftragte für den Datenschutz weist selbst darauf hin, dass Pseudonymisierung keinen absoluten Schutz bietet. Eine Studie der ETH Zürich zeigte im Februar 2026, dass Sprachmodelle bei bis zu 67 Prozent der untersuchten Pseudonyme die dahinterstehende Person ermitteln konnten. Der Terminvermittler Doctolib, nach eigenen Angaben mit rund 20 Millionen Patienten in Deutschland, übermittelte nach Recherchen von mobilsicher.de zeitweise Daten an Facebook und den Werbedienst Outbrain und nutzt seit Februar 2025 Nutzerdaten für das Training eigener KI-Systeme. Was eine Privacy-Box hier leisten kann, ist begrenzt: Sie blockiert Werbe-Tracker auf Gesundheitsportalen und in Apps, nicht aber den Datenfluss zwischen Praxis, Kasse und Akte. Dort bleibt das Widerspruchsrecht, das jede Krankenkasse anbieten muss.[107]

[106] The Markup: Xandr-Datenbankanalyse: Segmente zu Religion und politischen Überzeugungen. Juni 2023.

[107] Bundesbeauftragter für den Datenschutz und die Informationsfreiheit: Hinweise zur elektronischen Patientenakte (Opt-out seit 15. Januar 2025) und zum Gesundheitsdatennutzungsgesetz (in Kraft seit 26. März 2024). Lermen, D. et al.: LLM-basierte Re-Identifizierung pseudonymer Personen, arXiv 2602.16800, Februar 2026. mobilsicher.de: Analyse der Doctolib-App, 2025. Sauer, H.: Wie sicher sind unsere Gesundheitsdaten wirklich?, FOCUS Online, März 2026.

Finanzielle Situation und Konsumverhalten

Standortdaten verraten, wo jemand einkauft, und daraus lässt sich die finanzielle Situation ableiten: Wer regelmäßig bei Aldi und Lidl einkauft, hat ein anderes Einkommensprofil als jemand, der regelmäßig KaDeWe, Whole Foods oder Bio-Supermärkte aufsucht. Regelmäßige Besuche von Pfandleihern, Schuldnerberatungsstellen oder Jobcentern signalisieren finanzielle Schwierigkeiten. Urlaubs- und Reiseverhalten (Flughafenbesuche, Hotelaufenthalte, Reiseziele) erlauben Rückschlüsse auf Reisebudget und Lebensstandard. All diese Informationen sind in der Xandr-Datenbank als Kategorien vertreten: „Einkommenssegment arm", „Konsument in finanziellen Schwierigkeiten", „Frequent Traveler Business Class".

Einkaufsverhalten und Alltagsroutinen: Selbst der wöchentliche Einkauf beim Bio-Supermarkt, der Besuch einer bestimmten Apotheke, die Stammbäckerei oder das Lieblingscafé sind Datenpunkte, die ein Profil abrunden.

Privates Leben: Freizeitverhalten, Hobbys und Lebensstil

Wo verbringt jemand seine Freizeit? Regelmäßige Besuche eines Sportstudios, eines Fußballstadions, einer Bibliothek oder eines Vereinsheims, all das lässt sich aus Standortdaten ablesen. Die Kombination dieser Informationen ergibt ein detailliertes Lebensstilprofil, das in seiner Intimität einem Tagebuch ähnelt. Welche Freizeitorte besonders brisant sind, von LGBTQ-Lokalen über Spielhallen bis zu politischen Veranstaltungen, beschreibt der Abschnitt „Kritische Standorte“.

Vereinszugehörigkeiten und regelmäßige Aktivitäten: Wer jeden Mittwoch ein Vereinsheim aufsucht, jeden Donnerstag einen Schützenverein und jeden Samstag einen Kleingarten, verrät nicht nur Hobbys, sondern auch soziale Schicht, Wertvorstellungen und potenziell politische Neigungen. Der Besuch einer Freimaurerloge, eines Burschenschaftshauses, eines Rotary-Clubs oder eines Jagdvereins signalisiert Zugehörigkeit zu bestimmten gesellschaftlichen Netzwerken. Für Profiler, ob kommerziell oder geheimdienstlich, sind solche Muster Gold wert.

In der Summe entsteht aus Hunderten solcher „harmloser“ Standorte ein Bewegungs- und Verhaltensmuster, das den Alltag eines Menschen so präzise abbildet, dass Abweichungen, ein unerwarteter Arztbesuch, eine ungewöhnliche Reise, ein Treffen an einem neuen Ort, sofort als Anomalie erkennbar sind. Geheimdienste nennen dieses Verfahren „Pattern of Life Analysis“, und es steht über kommerzielle Datenhändler jedem offen, der bereit ist, dafür zu bezahlen.

Sicherheitsrelevante Informationen: Das nationale Risiko

Für staatliche Akteure und Geheimdienste bieten permanente Standortdaten eine neue Dimension der Aufklärung. Die Databroker Files und die WIRED-Recherche vom November 2024 (siehe oben) zeigten: Aus frei käuflichen Standortdaten ließen sich Bewegungsprofile von Mitarbeitern von Bundesministerien, der Bundeswehr und deutschen Sicherheitsbehörden erstellen. Daraus gewinnbare Informationen: Dienstzeiten und Routinen (wann verlässt ein Geheimdienstmitarbeiter sein Büro?), Wohnadressen von Personen in sicherheitssensiblen Positionen, soziale Kontakte außerhalb des Dienstgebäudes, Besuche in

anderen Sicherheitseinrichtungen (Querverbindungen zwischen Behörden) und sogar die Identifikation von V-Leuten oder verdeckten Ermittlern anhand ungewöhnlicher Bewegungsmuster.[108]

> ⚠ **Nationales Sicherheitsrisiko durch kommerziellen Datenmarkt**
>
> Für rund 14.000 USD jährlich kann jeder zahlungsfähige Käufer, ob Krimineller, ausländischer Geheimdienst oder investigativer Journalist, einen Datenstrom mit Milliarden von Standortpunkten deutscher Mobilgeräte abonnieren. Darunter befinden sich nachweislich Bewegungsprofile von Mitarbeitern sicherheitssensibler Einrichtungen. Das US-Zentralkommando bestätigte im April 2026, dass gegnerische Kräfte kommerzielle Standortdaten nutzen, um US-Soldaten im Nahen Osten ins Visier zu nehmen, der Datenmarkt gefährdet nachweislich die nationale Sicherheit. Die Bundesregierung hat den möglichen Datenkauf durch den BND zum Staatsgeheimnis erklärt, und damit implizit bestätigt, dass dieser Markt auch von Sicherheitsbehörden genutzt werden könnte.

Databroker Files 2026: Die ARD-Dokumentation

🔧 Die ARD-Dokumentation „Gefährliche Apps“ (April 2026)

Im April 2026 strahlten ARD, Arte und Deutsche Welle die Dokumentation „Gefährliche Apps: Im Netz der Datenhändler“ aus, produziert vom Bayerischen Rundfunk als Fortsetzung des Databroker-Files-Rechercheprojekts von 2024. Die Dokumentation zeigt anhand konkreter Einzelschicksale, welche realen Gefahren entstehen, wenn Milliarden von Standortdaten aus Smartphone-Apps über Werbenetzwerke an Datenhändler fließen.

Vier Fälle illustrieren die Bandbreite der Bedrohung: Erstens ukrainische Soldaten an der Front, deren Stellungen und Hauptquartiere über Standortdaten aus Smartphone-Apps in den Datensätzen von Databrokern auftauchten, einschließlich Geräten, die über Starlink verbunden waren. Ein ehemaliger Soldat namens Dmytro konnte sein früheres Hauptquartier in den Kartendaten identifizieren. Zweitens eine ägyptische Exil-Journalistin in Berlin, die vor dem Regime in Kairo geflohen war und deren Wohnung, besuchte Spielplätze und Krankenhaus in den Databroker-Daten verzeichnet waren, „als wäre ich gehackt worden“, beschrieb sie das Gefühl.

Der dritte Fall betrifft eine 18-jährige Schülerin aus Bayern, deren tägliche Wege (Schule, Supermarkt, Spaziergänge mit dem Hund) lückenlos in den Daten dokumentiert waren. „Wenn irgendein Mann diese Daten hätte, so Stalking-mäßig“, kommentierte sie. Der vierte Fall zeigt eine Frau aus Texas, die für einen medizinisch notwendigen Schwangerschaftsabbruch nach Colorado reisen musste, weil Texas Abtreibungen verboten hat. Ihre Reise zur Klinik wäre über die Standortdaten der Databroker rekonstruierbar gewesen, mit potenziell strafrechtlichen Konsequenzen in ihrem Heimatstaat.

Die Dokumentation belegt zudem Risiken für die nationale Sicherheit: Deutsche Rüstungsunternehmen fürchten, dass ihre geheimen Produktionsstätten in der Ukraine durch frei käufliche Standortdaten enttarnt werden könnten. Die EU-Kommission äußerte offizielle Besorgnis. Experten fordern ein vollständiges Verbot von Tracking und Profilbildung zu Werbezwecken, die geltenden Datenschutzgesetze seien zwar theoretisch anwendbar, könnten aber von den Aufsichtsbehörden nicht wirksam durchgesetzt werden.

[108] WIRED / netzpolitik.org / BR: Anyone Can Buy Data Tracking US Soldiers and Spies to Nuclear Vaults and Brothels in Germany. 20. November 2024. Senator Ron Wyden u. a.: Brief an das US-Verteidigungsministerium, 28. Mai 2026 (CENTCOM: gegnerische Nutzung kommerzieller Standortdaten gegen US-Soldaten).

Tracking-Schutz für mobile Devices

Um das Tracking auf mobilen Geräten zu reduzieren, empfiehlt das Comidio-Team eine Kombination von Maßnahmen: Erstens die regelmäßige Zurücksetzung der Advertising ID (iOS: Einstellungen → Datenschutz → Tracking; Android: Google-Einstellungen → Werbung). Zweitens die Nutzung eines mobilen VPN-Clients, der den gesamten Traffic des Geräts über die TrutzBox leitet, auch unterwegs (Kompendium Teil 2, Kapitel „Fernzugriff: VPN“); der Tunnel unterläuft zugleich das Netzbetreiber-Tracking utiq, weil die Website den Aufruf dann vom Festnetz aus sieht. Drittens die kritische Überprüfung der App-Berechtigungen: Welche App benötigt tatsächlich Standortzugriff, Mikrofonzugriff oder Kontaktzugriff? Viertens, nur unterwegs und ohne VPN-Verbindung zur TrutzBox, die Nutzung eines vertrauenswürdigen verschlüsselten DNS-Dienstes (DNS-over-HTTPS oder DNS-over-TLS), damit Mobilfunknetz oder fremdes WLAN die Namensauflösung nicht mitlesen können. Im Heimnetz und über VPN übernimmt die TrutzBox diese Aufgabe; dort sollte kein eigener DoH/DoT-Dienst konfiguriert sein, weil er sonst an den Filtern der Box vorbeiliefe.

Teil 6
Staat, Kriminelle und Schäden

Geheimdienste, staatliche Hacker, Betrüger und die Folgen für Einzelne und Gesellschaft

Geheimdienste und staatliche Überwachung

Für Einsteiger:

Nicht nur Werbeunternehmen wollen wissen, was Sie im Internet tun. Auch Behörden und Geheimdienste überwachen digitale Kommunikation, zum Teil im großen Stil. In Deutschland haben mehr als 10.000 Behörden das Recht, unter bestimmten Voraussetzungen Daten von Internetanbietern abzurufen. International wurden durch den Whistleblower Edward Snowden Programme enthüllt, die zeigen, dass US-Geheimdienste den weltweiten Internetverkehr systematisch überwachen. Und zunehmend kaufen staatliche Stellen einfach Daten auf dem kommerziellen Markt, legal und ohne Gerichtsbeschluss.

Technischer Hintergrund

Geheimdienste sind die zweite große Gruppe, die Daten über Internetnutzer sammelt. Im Unterschied zu kommerziellen Datenhändlern verfolgen sie keine wirtschaftlichen, sondern nationale Sicherheits- und geopolitische Interessen. Doch die Grenze zwischen legitimer Sicherheitsarbeit und unverhältnismäßiger Massenüberwachung ist fließend, und wurde durch die Enthüllungen von Edward Snowden im Sommer 2013 für alle sichtbar.

Edward Snowden, ehemaliger NSA-Subunternehmer, enthüllte die Existenz umfassender Programme zur globalen Massenüberwachung: PRISM erlaubt der NSA, so die Darstellung in den Snowden-Dokumenten. Zugriff auf Nutzerdaten bei Microsoft, Google, Apple, Facebook und anderen US-Technologiekonzernen. XKeyscore analysiert den gesamten unverschlüsselten Internetverkehr in Echtzeit und ermöglicht die Suche nach Inhalten und Metadaten. Upstream-Sammlung zapft die transatlantischen Glasfaserkabel ab, über die ein Großteil des globalen Internetverkehrs läuft. Durch das „Five Eyes"-Abkommen teilen USA, Großbritannien, Kanada, Australien und Neuseeland ihre Geheimdiensterkenntnisse automatisch.[109]

Im Januar 2026 berichtete der Autor in FOCUS Online über einen weiteren Aspekt staatlicher Überwachung, der sich noch wesentlich näher an den Bürgern abspielt als NSA-Programme: Mehr als 10.000 Behörden in Deutschland haben das Recht, unter bestimmten Umständen Zugang zu Nutzerdaten bei Mobilfunkanbietern, Internetprovidern und App-Betreibern zu fordern. Darunter nicht nur Staatsanwaltschaften und Polizei, sondern auch Ordnungsämter, Finanzbehörden und sogar kommunale

[109] Greenwald, G. / MacAskill, E.: NSA PRISM program taps in to user data of Apple, Google and others. The Guardian, 7. Juni 2013. Snowden, E.: Permanent Record. Metropolitan Books, 2019.

Einrichtungen. Die Schwelle für eine solche Datenabfrage ist in vielen Fällen deutlich niedriger als öffentlich bekannt.[110]

Wie konkret die im vorangegangenen Kapitel beschriebene Werbedaten-Infrastruktur für staatliche Überwachung missbraucht werden kann, zeigte im April 2026 eine gemeinsame Recherche des Citizen Lab der Universität Toronto und des ungarischen Investigativmediums VSquare. Demnach hatte die Regierung unter Viktor Orbán Lizenzen für das Überwachungstool **Webloc** erworben, ein Produkt der US-Firma Penlink (vormals Cobwebs Technologies, gegründet in Israel). Mindestens drei ungarische Sicherheitsbehörden waren seit den frühen 2020er-Jahren Kunden: der Inlandsgeheimdienst, das National Information Center und der Special Service for National Security.[111]

Webloc nutzt genau die Datenströme, die beim Real-Time-Bidding (RTB) anfallen: Während digitaler Werbeauktionen werden Nutzerdaten an Hunderte von Bietern übermittelt, und Überwachungsfirmen wie Penlink zapfen diese Ströme über Datenbroker oder direkte Auktionsteilnahme an. Ergänzend kaufen sie Standortdaten, die über in Apps eingebettete Software Development Kits (SDKs) gesammelt werden. Laut den analysierten Dokumenten verschafft Webloc Zugriff auf einen „ständig aktualisierten Datenstrom von bis zu 500 Millionen Mobilgeräten“, inklusive präziser GPS-Standorte, Gerätekennungen, demografischer Daten, Interessenprofilen und historischer Bewegungsdaten der vergangenen drei Jahre. Damit lässt sich nicht nur feststellen, wo sich eine Zielperson gerade aufhält, sondern auch, wo sie in der Vergangenheit war, welche Orte sie regelmäßig aufsucht und mit welchen anderen Geräten sie sich am selben Ort befand.[112]

Die politische Brisanz dieser Enthüllung lag auch im Zeitpunkt: Sie wurde nur zwei Tage vor der ungarischen Parlamentswahl am 12. April 2026 veröffentlicht, einer Wahl, bei der Orbáns Fidesz-Partei erstmals seit 2010 die Mehrheit zu verlieren drohte. Die Herausfordererpartei TISZA unter Péter Magyar führte in Umfragen deutlich. Der Verdacht lag nahe, dass Webloc gegen Oppositionelle, Journalisten oder Migranten eingesetzt werden könnte. Die Plattform Meta hatte die Vorgängerfirma Cobwebs Technologies bereits zuvor gesperrt, nachdem Kundenkonten „Aktivisten, Oppositionspolitiker und Regierungsbeamte“ ins Visier genommen hatten. Neben Webloc vertreibt Penlink weitere problematische Werkzeuge: *Tangles* zur Social-Media-Überwachung mit Gesichtserkennung, *Lynx* zur Verwaltung verdeckter Fake-Accounts und *Trapdoor* als Social-Engineering-Plattform für Phishing-Operationen. Zu den dokumentierten Kunden weltweit zählen neben Ungarn auch die US-Einwanderungsbehörde ICE, das US-Militär, Polizeibehörden in Los Angeles, Dallas und Baltimore sowie die Nationalpolizei von El Salvador.

Der Fall Webloc macht eine zentrale Erkenntnis greifbar: Staaten müssen heute keine Spyware mehr auf Endgeräten installieren und keine Sicherheitslücken mehr ausnutzen, um Millionen von Menschen zu überwachen. Die kommerzielle Werbeinfrastruktur, dasselbe System, das im vorangegangenen Kapitel beschrieben wurde, liefert dieselben Daten frei Haus, legal käuflich und ohne richterlichen Beschluss.

Für Unternehmen stellt die staatlich geförderte Cyberspionage durch sogenannte Nation-State Actors eine besondere und wachsende Bedrohung dar. Laut dem US-amerikanischen Cybersicherheitsunternehmen CrowdStrike nahmen chinesische Cyber-Spionage-Aktivitäten 2024 um 150 Prozent und 2025 um weitere 38 Prozent zu, in der Logistikbranche 2025 um 85 Prozent; nordkoreanische Operationen stiegen 2025 um

[110] Hermann Sauer in FOCUS Online: „Totale Überwachung durch die Hintertür: Wie 10.000 Behörden Zugriff auf Ihre Daten kriegen", 13. Januar 2026.

[111] netzpolitik.org: „Vor Schicksalswahl: Orbán-Regierung soll neuartige Überwachungsprogramme angeschafft haben“, 10. April 2026. https://netzpolitik.org/2026/vor-schicksalswahl-orban-regierung-soll-neuartige-ueberwachungsprogramme-angeschafft-haben/

[112] Citizen Lab, University of Toronto: „Analysis of PenLink’s Ad-Based Geolocation Surveillance Tech“, 10. April 2026. https://citizenlab.ca/research/analysis-of-penlinks-ad-based-geolocation-surveillance-tech/

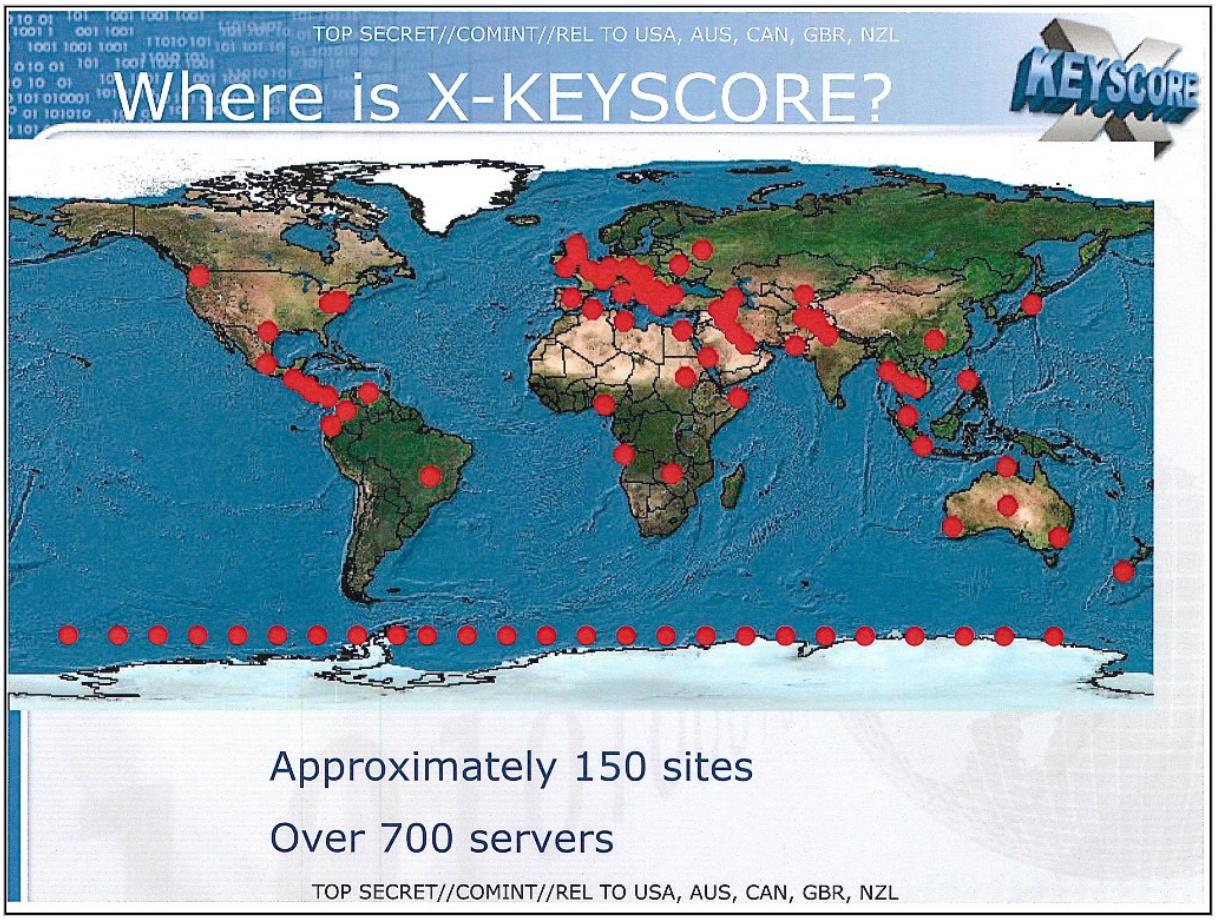
130 Prozent. Bitkom zufolge führte bei 37 Prozent der 2026 angegriffenen deutschen Unternehmen die Spur zu ausländischen Geheimdiensten. Russische Gruppen wie APT28 (Fancy Bear, verbunden mit dem russischen Militärgeheimdienst GRU) und APT29 (Cozy Bear, Auslandsgeheimdienst SVR) sind für Angriffe auf kritische Infrastruktur, Regierungseinrichtungen und Unternehmen in Europa und den USA verantwortlich.[113]

Staatliche Hackergruppen tarnen ihren Verkehr mit denselben Mitteln, die auch Werbe-Tracker unsichtbar machen. Die Russland zugerechnete Gruppe APT29 nutzte nach Analysen von Sicherheitsfirmen über Jahre das sogenannte Domain Fronting: Nach außen wird eine harmlose Adresse eines großen Cloud-Anbieters angesprochen, das eigentliche Ziel steckt im verschlüsselten Teil der Verbindung. Umgekehrt entschlüsselt die chinesische Internetzensur nach einer 2025 auf der Sicherheitskonferenz USENIX vorgestellten Untersuchung seit April 2024 gezielt die ersten Pakete des QUIC-Protokolls, um Zielnamen zu lesen; Cloudflare reagierte mit der Verschlüsselung genau dieser Namen. Jede Sichtbarkeit im Netz hat damit eine immer kürzere Halbwertszeit, für Zensoren wie für Schutzfilter.[114]

[113] CrowdStrike: Global Threat Report 2025 (27. Februar 2025) und Global Threat Report 2026 (24. Februar 2026). https://www.crowdstrike.com/global-threat-report/. Bitkom: Wirtschaftsschutz 2026, 26. August 2026.

[114] MITRE ATT&CK: T1090.004 Domain Fronting (APT29). Zohaib, A. et al.: Exposing and Circumventing SNI-based QUIC Censorship of the Great Firewall of China, USENIX Security Symposium 2025. Cloudflare: Announcing Encrypted Client Hello.

Geheimdienste zapfen das Internet an zentralen Datenknoten an, hier eine Folie aus einer NSA-Präsentation zum Programm XKeyscore:



Folie einer NSA-Präsentation zu XKeyscore
(Quelle: NSA, veröffentlicht 2013 im Zuge der Snowden-Enthüllungen; als Werk der US-Bundesregierung gemeinfrei)

Deutschland 2026: Mehr Befugnisse, mehr Datenzugriff

Auch in Deutschland wachsen die staatlichen Zugriffsrechte. Im April 2026 beschloss das Bundeskabinett zwei Vorhaben. Zugangsanbieter sollen die IP-Adressen ihrer Kunden drei Monate lang ohne Anlass speichern, damit Behörden nachträglich ermitteln können, welcher Anschluss wann welche Adresse hatte; die Bundesregierung rechnet nach eigenen Angaben mit rund 143.000 Abfragen pro Jahr. Grundlage ist ein Urteil des Europäischen Gerichtshofs vom April 2024, das eine solche Speicherung auch zur Verfolgung einfacher Straftaten zulässt. Das zweite Vorhaben, das sogenannte Sicherheitspaket, soll Bundeskriminalamt, Bundespolizei und dem Bundesamt für Migration den biometrischen Abgleich von Gesichtern mit öffentlich zugänglichen Fotos im Internet erlauben, ausdrücklich auch von Kontaktpersonen, Zeugen und Opfern, sowie die automatisierte Auswertung großer Datenbestände mit künstlicher Intelligenz. Die Konferenz der Datenschutzaufsichtsbehörden, Bürgerrechtsorganisationen und der Chaos Computer Club halten Teile davon für verfassungswidrig; das Gesetzgebungsverfahren läuft (Stand September 2026).[115]

Für die automatisierte Auswertung setzen die Polizeien in Hessen, Nordrhein-Westfalen und Bayern bereits Software des US-Konzerns Palantir ein, Baden-Württemberg folgt 2026. Die Systeme führen Daten aus Melderegistern, Funkzellenabfragen, Telefonüberwachung sowie Fahrzeug- und Waffenregistern zusammen. Das Bundesverfassungsgericht stellte 2023 fest, dass dabei „millionenfach erhobene Daten überwiegend unbeteiligter Personen“ einfließen, und setzte dem Einsatz enge Grenzen. Der Schweizer Armeestab kam Ende 2024 in einer Bewertung zu dem Ergebnis, ein Abfluss der Daten in die USA lasse sich angesichts der dortigen Gesetze technisch nicht ausschließen, und riet vom Einsatz ab. Gegen den bayerischen Einsatz ist eine Verfassungsbeschwerde anhängig.[116]

Seit dem 18. August 2026 gilt zudem die EU-Verordnung über elektronische Beweismittel (E-Evidence). Ermittlungsbehörden aller EU-Staaten können damit Anbieter von E-Mail-, Messenger- und Cloud-Diensten unmittelbar zur Herausgabe von Inhalten und Verbindungsdaten verpflichten, in der Regel binnen zehn Tagen, in Eilfällen binnen acht Stunden, nach dem Recht des anfragenden Staates. Nach Schätzungen der EU-Kommission sind davon rund 400.000 Anbieter betroffen. Ein Entwurf für ein neues Nachrichtendienstrecht sieht darüber hinaus vor, dass der Bundesnachrichtendienst Standortdaten vernetzter Fahrzeuge direkt beim Hersteller abrufen darf (siehe Kapitel „Connected Cars“).[117]

[115] Bundesregierung: Kabinettsbeschlüsse vom 22. April 2026 (Speicherung von IP-Adressen) und 29. April 2026 (Sicherheitspaket). EuGH, Urteil vom 30. April 2024, C-470/21 (La Quadrature du Net II). Stellungnahmen der Datenschutzkonferenz, der Gesellschaft für Freiheitsrechte und des Chaos Computer Clubs, Mai 2026. Sauer, H.: Dobrindts Sicherheitspaket, FOCUS Online, Mai 2026; Bürger unter Generalverdacht, FOCUS Online, Mai 2026.

[116] Bundesverfassungsgericht, Urteil vom 16. Februar 2023, 1 BvR 1547/19 (automatisierte Datenanalyse). Schweizer Armeestab: Evaluationsbericht zu Palantir, 4. Dezember 2024. Gesellschaft für Freiheitsrechte: Verfassungsbeschwerde gegen Art. 61a BayPAG, 23. Juli 2025. Sauer, H.: Palantir, Deutschlands Behörden in der Hand eines US-Konzerns, FOCUS Online, Februar 2026.

[117] Verordnung (EU) 2023/1543 über Europäische Herausgabe- und Sicherungsanordnungen, anwendbar ab 18. August 2026. Bundesministerium der Justiz: Referentenentwurf zur Modernisierung des Nachrichtendienstrechts, Stand Juli 2026. Sauer, H.: Geheimdienst-Reform 2026, FOCUS Online, Juli 2026; Überwachung, was die Regierung dem Bundestag verschweigt, FOCUS Online, Juni 2026.

Was der Betrieb eigener Dienste ändert, und was nicht

Die neuen Befugnisse richten sich fast ausnahmslos an Diensteanbieter: Provider, Mail-, Messenger- und Cloud-Betreiber, die Daten ihrer Kunden verwahren. Wer E-Mail, Chat und Videokonferenz auf einem eigenen Gerät im eigenen Haus betreibt, wie es die TrutzBox mit TrutzMail, TrutzChat und TrutzMeeting vorsieht, hat keinen solchen Anbieter dazwischen. Es gibt dann keinen Dritten, der Inhalte oder Verbindungsdaten auf Anordnung herausgeben oder, wie bei großen Plattformen üblich, Nachrichten automatisch auf verdächtige Inhalte durchsuchen könnte. Ein staatlicher Zugriff bleibt möglich, aber auf den Wegen, die auch für Papierakten und Endgeräte gelten, etwa mit einer richterlich angeordneten Durchsuchung oder, unter engeren gesetzlichen Voraussetzungen, mit einem verdeckten Zugriff auf ein Endgerät.
Nicht geändert wird dadurch die Speicherung der Anschluss-IP-Adresse beim Internetanbieter, die Auswertung von Mobilfunkdaten (Funkzellen, stille SMS) oder die Zusammenführung behördlicher Register. Diese Darstellung beschreibt die technische Lage nach Kenntnis des Comidio-Teams und ersetzt keine Rechtsberatung im Einzelfall.

Internet-Kriminelle: Phishing, CEO Fraud und Ransomware

Für Einsteiger:

Nicht alle, die Ihre Daten ausnutzen wollen, sind Werbekonzerne oder Geheimdienste. Viele sind schlichte Kriminelle, die Ihr Geld wollen. Sie versenden täglich Milliarden gefälschter E-Mails, geben sich als Ihr Chef aus, um Überweisungen zu veranlassen, oder sperren den Computer eines Unternehmens und fordern Lösegeld. Was diese Angriffe so effektiv macht: Die Kriminellen nutzen Datenbrokerdaten, um ihre Betrugsversuche täuschend echt aussehen zu lassen, mit Ihrem echten Namen, Ihrer Funktion, Ihrem aktuellen Projekt.

Technischer Hintergrund

Die dritte große Gruppe sind Internet-Kriminelle: organisierte Gruppen und Einzeltäter, die das Internet für Betrug, Erpressung, Identitätsdiebstahl und andere Formen der Kriminalität nutzen. Die Ökonomie des Cybercrime hat sich in den vergangenen zwei Jahrzehnten von einem Nischenphänomen zu einer globalen Schattenwirtschaft mit professionellen Strukturen entwickelt. Es gibt spezialisierte Foren für den Kauf und Verkauf gestohlener Kreditkartendaten, einen Markt für sogenannte Exploit-Kits (vorgefertigte Schadsoftware-Werkzeuge) und sogar Kundensupport-Dienste für Ransomware-Gruppen.

Die durchschnittlichen Kosten eines durch Phishing verursachten Datenlecks betragen laut IBM Cost of a Data Breach Report 2026 rund 5,29 Millionen US-Dollar. Phishing (einschließlich Betrugsanrufen und SMS) ist damit der häufigste und zugleich teuerste Angriffsweg. Die Zahl der täglich versandten Phishing-Mails wird seit Jahren mit rund 3,4 Milliarden angegeben, etwa ein Prozent des weltweiten E-Mail-Aufkommens; belastbarere aktuelle Zählungen gibt es nicht. Der wichtigste Verteilweg für Betrugsanzeigen sind nach Branchenzahlen die sozialen Netzwerke, allen voran Facebook (siehe Kapitel „Was Meta mit den Daten macht, und was nicht“).[118]

Auch Schadsoftware nutzt die Lücken, die Filtern die Sicht nehmen. Mehrere Schadprogramm-Familien wickeln ihre Steuerbefehle über verschlüsselte DNS-Anfragen an Google oder Cloudflare ab, was im Heimnetz wie gewöhnlicher Datenverkehr aussieht. Andere verstecken sich hinter vertrauenswürdigen Diensten: Microsoft beschrieb im März 2025 eine Werbe-Kampagne, bei der Schadsoftware zum Passwortdiebstahl über die Entwicklerplattform GitHub ausgeliefert wurde und rund eine Million Geräte erreichte. Die US-Cybersicherheitsbehörde CISA stufte im April 2025 das rasche Wechseln von Domains und Adressen („Fast Flux“) als Bedrohung der nationalen Sicherheit ein, weil Sperrlisten damit nicht mehr Schritt halten. Wer GitHub oder Google sperrt, sperrt zugleich legitime Dienste; genau in dieser Grauzone bewegen sich Angreifer (siehe Kapitel „Warum Filter Jahr für Jahr blinder werden“).[119]

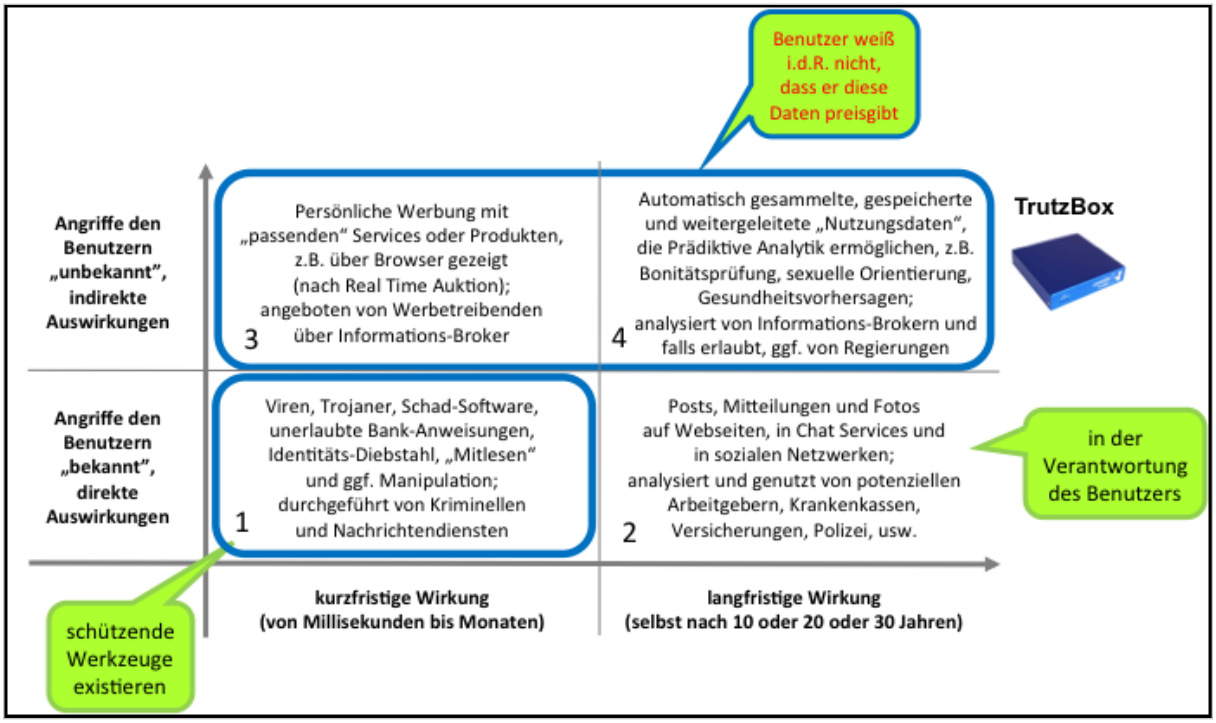
Der größte Umbruch ist der Preis eines Angriffs. Im November 2025 berichtete der KI-Anbieter Anthropic, eine mutmaßlich staatlich unterstützte Gruppe habe sein Modell für eine Spionagekampagne gegen rund 30 Unternehmen und Behörden eingesetzt; nach Darstellung des Unternehmens erledigte die KI 80 bis 90 Prozent der Arbeitsschritte selbst. Im Juli 2026 rekonstruierte die Sicherheitsfirma Dream einen Angriff auf Behörden in Taiwan, bei dem frei verfügbare KI-Agenten in vier Tagen 21 Systeme kartierten, 85 Konten übernahmen und 2.564 Personalakten kopierten. Die Sicherheitsforscher von Palo Alto Networks beobachteten im Mai 2026 einen Einzeltäter, dessen Agent selbständig 647.000 Installationen abklopfte, 460 Angriffe versuchte und 14-mal erfolgreich war. Die Trefferquote ist unerheblich, wenn der Versuch fast nichts kostet. Nach dem Jahresbericht 2026 des Sicherheitsanbieters Darktrace war Deutschland 2025 das am stärksten angegriffene Land Europas; 58 Prozent der Vorfälle begannen mit gestohlenen Zugangsdaten, nicht mit einem technischen Einbruch. Die Folge für den einzelnen Haushalt: Die alte Annahme, man sei als Ziel zu klein und zu uninteressant, gilt nicht mehr, wenn Angriffe Rechenzeit statt Gehälter kosten.[120]

[118] IBM: Cost of a Data Breach Report 2026, 29. Juli 2026 (globaler Durchschnitt 4,99 Mio. USD; Phishing häufigster Vektor mit 17 Prozent und teuerster mit 5,29 Mio. USD). https://www.ibm.com/reports/data-breach. Valimail: Spring 2019 Email Fraud Landscape (3,4 Mrd. gefälschte Mails täglich), seither in Branchenstatistiken fortgeschrieben.

[119] Microsoft Security Blog: Malvertising campaign leads to info stealers hosted on GitHub, 6. März 2025. CISA / NSA / FBI: Fast Flux: A National Security Threat, AA25-093A, April 2025. BleepingComputer: Chinese hackers use DNS-over-HTTPS for Linux malware communication (ChamelDoH).

[120] Anthropic: Disrupting the first reported AI-orchestrated cyber espionage campaign, November 2025 (Angaben des Anbieters). Dream Security: Analyse des Angriffs auf taiwanische Behörden, Juli 2026. Palo Alto Networks Unit 42: Bericht zu autonomen Angriffsagenten, Mai 2026. Darktrace: Annual Threat Report 2026. Sauer, H.: Hackerangriffe auf Rekordniveau, FOCUS Online, März 2026; KI-Agenten machen Cyberangriffe zur Massenware, finanzen100.de, September 2026.

Die Auswirkungen von Angriffen lassen sich nach vier Quadranten einteilen:



Die vier Quadranten: bekannte und unbekannte Angriffe, kurzfristige und langfristige Wirkung. (© 2026 Comidio GmbH)

Die Mobilfunknummer als Generalschlüssel

Für Einsteiger:

Ihre Handynummer ist längst mehr als eine Nummer. Sie ist der Schlüssel zu WhatsApp, zu Bank-Freigaben per SMS, zu Passwort-Zurücksetzungen und zu vielen Online-Konten. Wer sie kennt und mit einem Gesicht oder Namen verbinden kann, hat einen Zugang zu Ihrem digitalen Leben. Genau deshalb sammeln Datenhändler, Betrüger und Forscher diese Nummern in Milliardenhöhe.

🔧 Zensus, SIM-Tausch und Betrugsanrufe

Im November 2025 zeigten Forscher der Universität Wien und des Forschungszentrums SBA Research, dass sich das gesamte WhatsApp-Verzeichnis automatisiert auslesen ließ: Über die Kontaktsuche prüften sie mehr als 100 Millionen Nummern pro Stunde und bestätigten rund 3,5 Milliarden aktive Konten weltweit. Bei 57 Prozent war das Profilbild öffentlich, bei 29 Prozent der Info-Text; in einer Stichprobe zeigten zwei Drittel der Bilder ein erkennbares Gesicht. Damit lag das Rohmaterial für eine weltweite Zuordnung von Nummer, Gesicht und Person offen. Meta schloss die Lücke nach der Meldung der Forscher. Fast die Hälfte der 2021 aus Facebook abgeflossenen 500 Millionen Nummern war zu diesem Zeitpunkt weiterhin bei WhatsApp aktiv.[121]

Die Nummer ist zugleich Angriffsziel. Beim sogenannten SIM-Tausch (SIM-Swap) bringt ein Betrüger den Mobilfunkanbieter mit gestohlenen Personendaten dazu, die Nummer auf eine neue SIM-Karte zu übertragen. Ab diesem Moment landen alle SMS-Codes für Bank, E-Mail und Messenger beim Täter. Das FBI beziffert die in den USA gemeldeten Schäden für 2023 auf über 48 Millionen US-Dollar; der britische Branchenbericht Fraudscape zählte für 2024 einen Anstieg um rund 1.055 Prozent auf fast 3.000 Fälle. In Deutschland verzeichnete die Bundesnetzagentur für 2024 rund 11.400 Beschwerden über betrügerische SMS (Smishing), Warn-Apps registrierten 2025 rund 5,9 Millionen gemeldete Spam-Anrufe. Das Oberlandesgericht Bremen entschied im Januar 2025, dass ein Bankkunde, der nach Anrufen mit gefälschter Bank-Rufnummer einen Freigabecode weitergegeben hatte, den Schaden von 10.000 Euro selbst trägt.[122]

Wie leicht Nummern zu beschaffen sind, zeigte 2025 ein italienischer IT-Berater: Über Marketing-Erweiterungen für das Berufsnetzwerk LinkedIn fand er nach Medienberichten die privaten Handynummern von Regierungsmitgliedern und Vorständen großer Konzerne. Entsprechende Zugänge werden von Datenhändlern ab etwa 30 Euro im Monat angeboten.[123]

[121] Gegenhuber, G. / Frenzel, P. / Weippl, E. (Universität Wien, SBA Research): Hey there! You are using WhatsApp: Enumerating Three Billion Accounts for Security and Privacy, November 2025. Sauer, H.: WhatsApp-Hack: 3,5 Milliarden Konten auslesbar, AP-Verlag, Januar 2026.

[122] FBI Internet Crime Complaint Center: Internet Crime Report 2023 (SIM Swapping). Cifas: Fraudscape 2025. Bundesnetzagentur: Jahresbericht 2024, Rufnummernmissbrauch. Clever Dialer: Spam-Report 2025. OLG Bremen, Urteil vom Januar 2025, 1 U 32/24. Sauer, H.: Ihr Telefon kann zur Waffe werden, FOCUS Online, April 2026.

[123] Der Spiegel: Bericht über den Handel mit Handynummern von Spitzenpolitikern über LinkedIn-Erweiterungen, 2025. Sauer, H.: Die Mobilfunknummer reicht, Dezember 2025.

Wer die Nummer hat, kann mehr als anrufen. Forscher der Universität Wien zeigten 2024, dass sich WhatsApp und Signal über unsichtbare Protokollnachrichten, etwa eine Reaktion auf eine nicht existierende Nachricht, zu Zustellbestätigungen bringen lassen, ohne dass der Empfänger etwas sieht. Aus der Antwortzeit, rund eine drittel Sekunde bei geöffneter App, bis zu zwei Sekunden im Ruhezustand, lassen sich Schlafzeiten, Arbeitszeiten, der Wechsel zwischen WLAN und Mobilfunk und die Zahl der genutzten Geräte ablesen. Nötig ist nur die Telefonnummer, kein Kontakt. Die Forscher meldeten die Lücke im September 2024; nach ihren Angaben stufte Meta sie als nicht schwerwiegend ein, Signal antwortete nicht, und Ende 2025 war sie weiterhin nutzbar. Threema, das ohne Telefonnummer arbeitet, war nicht betroffen. Hinzu kommt: WhatsApp-Sicherungen in der Google- oder Apple-Cloud sind in der Grundeinstellung nicht Ende-zu-Ende-verschlüsselt, die Verschlüsselung der Sicherung muss eigens aktiviert werden.[124]

Was hilft: beim Mobilfunkanbieter eine Sperre gegen unbefugte Rufnummern-Übertragung einrichten, für Freigaben eine Authentifizierungs-App statt SMS nutzen, die Nummer aus öffentlichen Profilen entfernen und Profilbild sowie Info-Text in WhatsApp nur für Kontakte freigeben. Grundsätzlicher ist der Verzicht auf die Telefonnummer als Kennung. Ein Chat-Dienst auf eigener Domain, wie ihn TrutzChat bietet, nutzt eine Adresse nach dem Muster einer E-Mail-Adresse. Sie lässt sich nicht wie ein Nummernbereich durchprobieren, ist an keine SIM-Karte gebunden, und es wird kein Adressbuch hochgeladen. Wer die Adresse nicht kennt, kann weder Zustellbestätigungen abfragen noch das Konto über einen SIM-Tausch übernehmen (Kompendium Teil 2, Kapitel „Videokonferenz und Chat (TrutzRTC)“).

CEO Fraud: Die Macht der Datenbrokerdaten für Betrug

Für Einsteiger:

Stellen Sie sich vor, Sie erhalten eine E-Mail von Ihrem Chef, mit seiner echten E-Mail-Adresse, seinem echten Namen und einem Verweis auf ein laufendes Projekt. Er bittet Sie dringend, 50.000 Euro auf ein neues Konto zu überweisen. Was Sie nicht wissen: Die E-Mail stammt nicht von Ihrem Chef, sondern von einem Betrüger, der genug über Ihr Unternehmen weiß, um die Täuschung perfekt zu machen. Dieses Wissen hat er sich aus Datenbrokerdatenbanken zusammengestellt.

[124] Gegenhuber, G. et al. (Universität Wien): Careless Whisper: Exploiting Silent Delivery Receipts to Monitor Users on Mobile Instant Messengers, arXiv 2411.11194, November 2024, mit Stand der Meldung an Meta und Signal. WhatsApp: Hilfebereich zur Ende-zu-Ende-Verschlüsselung von Backups. Sauer, H.: So kann man Ihr WhatsApp-Verhalten überwachen, FOCUS Online, Dezember 2025.

🔧 Technischer Hintergrund

Beim CEO Fraud (auch Business Email Compromise oder BEC genannt) geben sich Angreifer als Geschäftsführer oder Führungskräfte aus, um Mitarbeiter zur Überweisung von Geldern oder zur Herausgabe sensibler Informationen zu verleiten. Zwischen 2013 und 2023 führten laut FBI über 305.000 solcher Vorfälle zu weltweiten Verlusten von über 55 Milliarden US-Dollar; allein 2025 meldeten US-Bürger und Unternehmen dem FBI knapp 25.000 BEC-Fälle mit gut 3 Milliarden US-Dollar Schaden. In Deutschland waren laut Bitkom 2026 96 Prozent der Unternehmen von Datendiebstahl, Spionage oder Sabotage betroffen oder vermutlich betroffen; 16 Prozent meldeten Schäden durch Phishing.[125]

Was CEO Fraud so gefährlich effektiv macht, ist die Qualität der verwendeten Informationen. Ein Angreifer, der sich vergleichbare Datenbroker-Datensätze beschafft, könnte wissen: Wer ist der CFO des Zielunternehmens? Welche Reisepläne hat der CEO diese Woche? An welchen Projekten arbeitet das Unternehmen gerade? Welche Geschäftspartner gibt es? Mit diesen Informationen lässt sich eine E-Mail formulieren, die selbst sehr vorsichtige Mitarbeiter täuscht. Die E-Mail erscheint im richtigen Kontext, bezieht sich auf reale Ereignisse und simuliert den vertrauten Schreibstil der Führungskraft.

Spear Phishing: Gezielte Attacken durch Personendaten

> 💡 **Für Einsteiger:**
>
> Normales Phishing ist wie das Auswerfen eines Fischernetzes, es trifft viele zufällige Opfer. Spear Phishing ist der gezielte Wurf mit der Angel: Der Angreifer kennt genau, wen er angreift, und formuliert eine E-Mail so persönlich und glaubwürdig, dass selbst aufmerksame Menschen getäuscht werden. Der Stachel dieser Angriffe ist Ihr eigenes Datenprofil, das der Angreifer aus Datenbrokerdatenbanken zusammengestellt hat.

[125] FBI IC3: Business Email Compromise: The $55 Billion Scam, PSA vom 11. September 2024 (305.033 Vorfälle, 55,5 Mrd. USD, 2013 bis 2023); FBI IC3: Internet Crime Report 2025, 7. April 2026 (BEC: 24.768 Beschwerden, 3,05 Mrd. USD; Gesamtverluste 20,9 Mrd. USD). Bitkom: Wirtschaftsschutz 2026, Presseinformation 26. August 2026.

🔧 Technischer Hintergrund

Im Unterschied zu breit gestreutem Phishing, das auf Masse setzt, zielt Spear Phishing auf spezifische Mitarbeiter oder Führungspersonen. Obwohl Spear Phishing nur einen winzigen Teil des E-Mail-Volumens ausmacht, gehört es laut den jährlichen Verizon-Data-Breach-Berichten zu den häufigsten Einfallstoren erfolgreicher Angriffe, eine Effizienz, die auf der Personalisierung basiert.[126]

Ein konkretes Beispiel, wie Datenbrokerdaten für Spear Phishing genutzt werden: Ein Angreifer kauft aus einer Datenbrokerdatenbank Informationen über den Einkaufsleiter eines mittelständischen Pharmaunternehmens. Er weiß dessen vollständigen Namen, seinen genauen Titel, seinen Arbeitgeber und dessen Adresse, seine Telefonnummer (aus einer anderen Datenquelle), seine LinkedIn-Aktivitäten der letzten drei Monate (aus dem LinkedIn-Tracking), seinen ungefähren Wohnort (aus Standortdaten) sowie den Namen seines Vorgesetzten. Mit diesen Informationen verfasst er eine personalisierte E-Mail, die vorgibt, von einem bekannten Geschäftspartner zu stammen, und einen infizierten Anhang enthält. Die E-Mail nennt den Namen des Empfängers, bezieht sich auf ein aktuelles, aus LinkedIn bekanntes Projekt und fordert eine dringende Prüfung eines Lieferangebots.

Kosten eines Cyber-Angriffs

Die direkten finanziellen Schäden durch Cyberkriminalität sind nur die Spitze des Eisbergs. Hinzu kommen Reputationsschäden, Betriebsunterbrechungen, Kosten für forensische Untersuchungen, rechtliche Folgekosten und der Verlust von Geschäftsgeheimnissen. Cybersecurity Ventures, auf deren Zahlen sich auch das Weltwirtschaftsforum stützt, beziffert den globalen jährlichen Schaden durch Cyberkriminalität auf 10,5 Billionen US-Dollar für 2025 und 10,8 Billionen für 2026, wäre Cyberkriminalität eine Volkswirtschaft, läge sie damit nach den USA und China an dritter Stelle. Für deutsche Unternehmen ermittelt der Digitalverband Bitkom für 2026 Schäden zwischen 211 und 271 Milliarden Euro durch Diebstahl von IT-Ausrüstung und Daten, digitale und analoge Industriespionage sowie Sabotage; rund drei Viertel davon entfallen auf Cyberangriffe.[127]

[126] Verizon: 2026 Data Breach Investigations Report; Verizon: 2025 Data Breach Investigations Report.

[127] Cybersecurity Ventures: Global Cybercrime Damage Costs (10,5 Bio. USD 2025, 10,8 Bio. USD 2026, 12,2 Bio. USD 2031), zitiert u. a. vom World Economic Forum. Bitkom: Wirtschaftsschutz 2026, 26. August 2026 (Schadenskorridor 211 bis 270,8 Mrd. Euro, Cyberanteil 76 Prozent). https://www.bitkom.org. Sophos: State of Ransomware 2026, Juli 2026 (im Schnitt drei Wochen bis zur Wiederherstellung, Wiederherstellungskosten 1,7 Mio. USD).

Ransomware stellt dabei eine besonders akute Bedrohung dar. Laut Bitkom erlitt 2026 jedes vierte deutsche Unternehmen Schäden durch Ransomware (2025: jedes dritte). Nach der Sophos-Erhebung 2026 brauchen betroffene Unternehmen im Schnitt drei Wochen bis zur vollständigen Wiederherstellung, eine Zeit, in der Produktion, Kommunikation und Kundenservice stillstehen; die Wiederherstellungskosten liegen im Mittel bei 1,7 Millionen US-Dollar je Vorfall.

Welchen Schaden können Tracker-Daten anrichten?

Für Einsteiger:

Man könnte denken: "Was soll schon passieren, wenn jemand weiß, welche Websites ich besuche?" Aber die Folgen reichen weit über lästige Werbung hinaus. Wer Ihre Daten hat, kann entscheiden, ob Sie einen Kredit bekommen. Wer Ihre Gewohnheiten kennt, kann Sie politisch manipulieren. Wer Ihren Standort hat, kann Sie verfolgen. Und wer genug über Sie weiß, kann sich als Ihr Chef ausgeben und Ihre Kollegen um Geld bitten. Datenmissbrauch hat echte, greifbare Konsequenzen für das Leben der Betroffenen.

Die Gefahr von Tracker-Daten liegt nicht allein darin, dass jemand weiß, welche Websites man besucht. Die eigentliche Gefahr entsteht durch die Aggregation und Analyse von Daten über lange Zeiträume hinweg, durch die Verknüpfung von Online- und Offline-Daten sowie durch die Möglichkeit, diese Daten in den Händen verschiedener Akteure für unterschiedliche Zwecke zu nutzen.

A. Dokumentierte Schadenfälle für den Einzelnen

Für Einsteiger:

Die Frage „Ich habe doch nichts zu verbergen“ ist verständlich, sie verkennt aber, wie Daten konkret genutzt werden. Datenprofil-Missbrauch trifft Menschen ganz persönlich: beim Kreditantrag, bei der Bewerbung, bei der Krankenversicherung. Die folgenden Beispiele sind dokumentierte Fälle aus Forschung und Berichterstattung.

1. Bonitätsbewertung durch Verhaltensdaten (ZestFinance)

Das US-amerikanische Unternehmen ZestFinance (heute Zest AI) hat ein System entwickelt, das Kreditwürdigkeit anhand von über 70.000 Datenpunkten bewertet. Darunter fallen Verhaltensmerkmale wie Tippgeschwindigkeit bei der Dateneingabe, Großschreibung des eigenen Namens, genutzte Browser und Betriebssysteme sowie das Einkaufsverhalten. Unternehmen wie LenddoEFL und Experian Boost nutzen Social-Media-Aktivitäten, App-Nutzungsdaten und Einkaufsgewohnheiten zur Bonitätsbewertung. In den USA ist diese Praxis unter dem Begriff „Alternative Data“ verbreitet.[128]

2. Personalentscheidungen durch KI-Profiling (Evolv)

Das US-amerikanische Workforce-Analytics-Unternehmen Evolv (2014 von Cornerstone OnDemand übernommen) und vergleichbare Anbieter haben Daten von über drei Millionen Bewerbern und Angestellten für automatisierte Personalentscheidungen erfasst. KI-Systeme analysieren Bewerbungsvideos, Tippverhalten, Antwortmuster und Social-Media-Aktivitäten, um Kandidaten zu bewerten. Der EU AI Act (Verordnung (EU) 2024/1689) stuft derartige Systeme in Anhang III als Hochrisiko-KI ein.[129]

3. Preisdiskriminierung durch Nutzerprofil (Surveillance Pricing)

Google hält ein Patent (US 9,009,065 B1), das beschreibt, wie auf Basis von Nutzerprofilen unterschiedliche Preise für identische Produkte angezeigt werden können. Wie weit die Praxis inzwischen reicht, zeigte die US-Handelsbehörde FTC im Januar 2025 in einer Untersuchung von acht Preis-Dienstleistern (darunter Mastercard, Accenture und McKinsey): Standort, Browserverlauf, Mausbewegungen und abgebrochene Warenkörbe fließen in individuelle Preise für rund 250 Kundenunternehmen ein („Surveillance Pricing“). Im Dezember 2025 wies Consumer Reports nach, dass der Lieferdienst Instacart für dasselbe Produkt im selben Laden bis zu fünf verschiedene Preise anzeigte, im Schnitt 13 Prozent auseinander; Instacart stellte die Preistests daraufhin ein. Die Fluggesellschaft Delta

[128] Hurley, M. / Adebayo, J.: Credit Scoring in the Era of Big Data. Yale Journal of Law and Technology, 18(1), 2016. Zest AI: Machine Learning for Credit Underwriting. https://www.zest.ai. National Consumer Law Center: Big Data. A Big Disappointment for Scoring Consumer Creditworthiness, 2014.

[129] FTC: Aiming for Truth, Fairness, and Equity in Your Company’s Use of AI. FTC Report, 2021. Europäisches Parlament: Verordnung (EU) 2024/1689 (AI Act), Anhang III.

setzt KI-Preisbildung für einen wachsenden Anteil ihrer Inlandstickets ein, bestreitet aber eine Personalisierung nach Kundendaten.[130]

4. Risikobewertung aus Verhaltensdaten: Versicherer und Fahrdaten

Dass Verhaltensdaten ohne Wissen der Betroffenen in Versicherungsentscheidungen einfließen, ist seit 2024 dokumentiert: General Motors gab über OnStar erfasste Fahrdaten (Bremsverhalten, Beschleunigung, nächtliche Fahrten) an die Datenhändler LexisNexis und Verisk weiter, die daraus Risikoprofile für Kfz-Versicherer bildeten; Betroffene erfuhren davon erst durch gestiegene Prämien oder abgelehnte Anträge. Der Bundesstaat Texas verklagte im Januar 2025 zudem den Versicherer Allstate, dessen Tochter Arity Bewegungsdaten von 45 Millionen Menschen über in fremden Apps versteckte Software-Bausteine gesammelt hatte. Das Prinzip lässt sich auf Gesundheit übertragen: Kaufmuster (Tabletten, Diätprodukte), besuchte Orte (Apotheken, Schnellrestaurants) und Suchanfragen können als Indikatoren für Gesundheitsrisiken ausgewertet werden. US-amerikanische Krankenversicherer setzen derartige prädiktive Modelle seit Jahren ein.[131]

5. Erpressung von Berufsgeheimnisträgern (StPO § 53)

In Deutschland gibt es rund 900.000 Berufsgeheimnisträger im Sinne des § 53 StPO: Ärzte, Rechtsanwälte, Steuerberater, Notare, Psychologen, Apotheker, Geistliche und Journalisten. Wenn Standortdaten dieser Personen frei handelbar sind, wie die Databroker Files zeigen, können aus Bewegungsmustern Rückschlüsse gezogen werden, welche Kanzlei einen Whistleblower berät, welcher Arzt einen bestimmten Patienten behandelt oder welcher Journalist mit welchem Informanten in Kontakt steht. Damit werden die Vertrauensverhältnisse dieser Berufsgruppen mittelbar kompromittiert.[132]

6. Phishing und Social Engineering durch Micro-Targeting

Micro-Targeting bezeichnet die hochpräzise Ansprache von Einzelpersonen auf Basis detaillierter Datenprofile. Mit Kenntnissen über Berufsbezeichnung, aktuelle Projekte, Hobbys und persönliche Netzwerke lassen sich hochgradig glaubwürdige Phishing-E-Mails formulieren, die sich von echten Nachrichten kaum unterscheiden. Laut Verizon Data Breach Investigations Report 2026 ist bei 62 Prozent aller Datenpannen der „menschliche Faktor“ beteiligt; Phishing steht hinter 16 Prozent, Pretexting (vorgetäuschte Identität) hinter 6 Prozent aller Datenpannen; personalisiertes Spear Phishing gehört dabei zu den wirksamsten Einfallstoren.[133]

---

[130] FTC: Surveillance Pricing Study Indicates Wide Range of Personal Data Used to Set Individualized Consumer Prices, 17. Januar 2025; FTC: Proposed Enforcement Policy Statement on Personalized Pricing, 19. August 2026. Groundwork Collaborative / Consumer Reports: Instacart-Preisstudie, 9. Dezember 2025; New York Attorney General: Letter to Instacart, 8. Januar 2026. Delta Air Lines: Delta responds to misinformation around AI pricing, 31. Juli 2025. US Patent Nr. 9,009,065 B1 (Google, Inc.): Pricing of digital content based on user context.

[131] The New York Times (Kashmir Hill): Automakers Are Sharing Consumers' Driving Data With Insurance Companies, 11. März 2024. FTC: Final Order GM/OnStar, 14. Januar 2026. Texas Attorney General v. Allstate/Arity, 13. Januar 2025.

[132] Strafprozessordnung (StPO) § 53: Zeugnisverweigerungsrecht der Berufsgeheimnisträger. Bundesrechtsanwaltskammer: Stellungnahme zu Datenhandel und Berufsgeheimnis, 2024.

[133] Verizon: 2026 Data Breach Investigations Report (Human Element 62 Prozent, Phishing 16 Prozent, Pretexting 6 Prozent).

7. Digitale Filterblasen und algorithmische Konditionierung

Algorithmen von Facebook, YouTube, TikTok und Google News personalisieren Inhalte so, dass Nutzer zunehmend nur noch Informationen sehen, die ihren bestehenden Ansichten entsprechen, die sogenannte Filterblase. Wissenschaftliche Studien bestätigen: Filterblasen verstärken politische Polarisierung und die Bereitschaft, Fehlinformationen zu übernehmen. Der Begriff wurde 2011 von Eli Pariser geprägt.[134]

Algorithmen, die personalisierte Inhalte ausspielen, können gezielt populistische Überzeugungen verstärken und Nutzer von breiten Informationsquellen isolieren. Ehemalige Mitarbeiter von Google, Facebook und Twitter haben in öffentlichen Anhörungen vor dem US-Kongress beschrieben, wie Empfehlungsalgorithmen auf Engagement-Maximierung optimiert werden, was nachweislich extremere Inhalte begünstigt. Der Netflix-Dokumentarfilm „Das Dilemma mit den sozialen Medien“ (2020) beleuchtet diese Mechanismen anhand von Aussagen ehemaliger Mitarbeiter.[135]

Empfehlung: Netflix-Dokumentarfilm

Der Dokumentarfilm „Das Dilemma mit den sozialen Medien“ (The Social Dilemma, Regie: Jeff Orlowski, Netflix 2020) zeigt anhand von Interviews mit ehemaligen leitenden Mitarbeitern von Google, Facebook, Instagram und Twitter die gesellschaftlichen Folgen algorithmischer Empfehlungssysteme. Abrufbar unter: https://www.netflix.com/de/title/81254224

B. Gefahren für Gesellschaft und Weltordnung

Für Einsteiger:

Die Risiken des unkontrollierten Datenhandels enden nicht beim Einzelnen. Sie reichen bis in die Grundlagen unserer Demokratie, Wirtschaftsordnung und nationalen Sicherheit. Was wie ein technisches Problem erscheint, ist eine geopolitische Herausforderung.

8. Manipulation von Wahlen

Der Cambridge-Analytica-Skandal hat gezeigt, dass Massenprofilierung und Micro-Targeting demokratische Wahlen beeinflussen können. Die US-Senatsuntersuchung zum Einfluss auf die US-Wahl 2016 dokumentierte, wie über soziale Netzwerke zielgerichtete Desinformationskampagnen an unterschiedliche Wählergruppen ausgespielt wurden. Das Oxford Internet Institute dokumentiert Computational Propaganda in über 70 Ländern jährlich.[136]

[134] Pariser, E.: The Filter Bubble: What the Internet Is Hiding from You. Penguin Press, 2011. Bail, C. et al.: Exposure to Opposing Views on Social Media Can Increase Political Polarization. PNAS, 115(37), 2018.

[135] Harris, T.: Testimony before US Senate Commerce Committee, 2019. Orlowski, J.: The Social Dilemma. Netflix, 2020. https://www.netflix.com/de/title/81254224.

[136] US Senate Select Committee on Intelligence: Report on Russian Active Measures Campaigns and Interference in the 2016 U.S. Election, 2020. Bradshaw, S. / Howard, P.: The Global Disinformation Disorder. Oxford Internet Institute, 2019.

9. Erpressung und Manipulation: von Politikern bis zum Identitätsdiebstahl

Politiker, Richter, Staatsanwälte und andere öffentliche Entscheidungsträger sind aus Sicht von Akteuren mit manipulativer Absicht besonders interessante Ziele. Standortdaten, Kommunikationsmetadaten und Verhaltensprofile können genutzt werden, um private Gewohnheiten zu dokumentieren oder Druck auf Personen auszuüben. Die NSA-Enthüllungen von Snowden dokumentierten, dass auch ausländische Staatschefs durch Metadaten-Analyse überwacht wurden.[137]

Wer weiß, dass jemand regelmäßig eine Selbsthilfegruppe für Suchtkranke besucht, eine Klinik für psychische Erkrankungen aufsucht oder an bestimmten politischen Veranstaltungen teilnimmt, verfügt über Informationen, die für Druckmittel genutzt werden könnten. Identitätsdiebstahl, die missbräuchliche Nutzung gestohlener Personendaten für Kredite, Käufe oder andere Transaktionen, verursacht in Deutschland jährlich Schäden in dreistelliger Millionenhöhe. Wie aus frei gehandelten Standortdaten solche Erpressungsprofile entstehen, zeigt Teil 5 im Abschnitt „Kritische Standorte“.[138]

10. Manipulation des Wirtschaftsgleichgewichts und Börsenmissbrauch

Wer Zugriff auf Echtzeitdaten über das Konsumverhalten von Millionen Menschen hat, verfügt über Informationsvorteile, die an Finanzmärkten ausgenutzt werden können. Hedgefonds kaufen bereits seit Jahren alternative Datensätze wie Kreditkartentransaktionen, Geolokationsdaten und Social-Media-Stimmungen, um Kursbewegungen vorherzusagen. Die US-Wertpapieraufsicht SEC hat mehrfach Untersuchungen zu Insiderhandel auf Basis alternativer Daten eingeleitet.[139]

11. Sabotage kritischer Infrastruktur

Internet-Backbone-Router bilden die physische Grundlage des globalen Internets. Staatlich gesponserte Hackergruppen haben dokumentiert Angriffe auf Netzwerkinfrastruktur durchgeführt. Die US-Behörde CISA veröffentlichte 2024 ein Advisory über dokumentierte Angriffe auf kritische Infrastruktur durch staatliche Akteure.[140]

12. Gezielte Tötung auf Basis von Metadaten

Michael Hayden, ehemaliger Direktor der NSA und der CIA, sagte 2014 öffentlich: „Wir töten Menschen auf Basis von Metadaten.“ (englisch: „We kill people based on metadata.“) Diese Aussage bezog sich auf die Praxis der US-Drohnenangriffe, bei denen Zielpersonen durch die Analyse von Kommunikationsmetadaten identifiziert wurden. Das Zitat verdeutlicht: Daten, die kommerziell als

[137] Snowden, E.: Permanent Record. Metropolitan Books, 2019. The Guardian: NSA Monitored Calls of 35 World Leaders, Oktober 2013.

[138] Bundeskriminalamt (BKA): Cybercrime: Bundeslagebild 2023. Verbraucherzentrale Bundesverband: Identitätsdiebstahl: Ausmaß und Folgen, 2023.

[139] SEC: Staff Report on Algorithmic Trading in U.S. Capital Markets, 2020. Alternative Data Council: The Use of Alternative Data in Investment Management, 2023.

[140] CISA: Advisory on PRC State-Sponsored Cyber Actors Compromising U.S. Critical Infrastructure, 2024. NSA: UPSTREAM Collection, dokumentiert durch The Guardian und Washington Post, 2013.

Werbedaten eingestuft werden, können in anderen Händen Grundlage gravierender Entscheidungen werden.[141]

Die Kette dahinter ist inzwischen dokumentiert. Die US-Firma Anomaly Six hatte nach Recherchen des Magazins The Intercept ihren Software-Baustein in über 500 Apps eingebettet und verfolgte damit Hunderte Millionen Telefone; in einer Vorführung für Regierungskunden ortete sie nach dem Bericht Mitarbeiter der Geheimdienste CIA und NSA. Das US-Militär kaufte Standortdaten der Gebets-App Muslim Pro. Eine frühere Mitarbeiterin des US-Drohnenprogramms beschrieb 2025 gegenüber netzpolitik.org, wie solche Massendaten in einer „Kill Cloud“ per Software zu Zielvorschlägen verdichtet werden. Der Weg beginnt jedes Mal beim Werbe-Baustein in einer alltäglichen App.[142]

13. Staatliche Ausspähung durch kommerziellen Datenmarkt

Ein Bericht des Office of the Director of National Intelligence (ODNI) aus dem Jahr 2022 bestätigte, dass US-Geheimdienste in großem Umfang kommerziell erhältliche Daten kaufen und nutzen. In Deutschland hat die Bundesregierung laut netzpolitik.org den möglichen Datenkauf durch den BND zum Staatsgeheimnis erklärt.[143]

Seither ist der Handel weder eingedämmt noch unsichtbar geworden. Die US-Handelsaufsicht FTC ging im Dezember 2024 gegen die Datenhändler Gravy Analytics, Venntel und Mobilewalla vor: Gravy und Venntel sammelten nach den Beschwerdeschriften täglich über 17 Milliarden Standortsignale von rund einer Milliarde Smartphones, Mobilewalla hielt Daten zu über einer Milliarde Menschen, rund 60 Prozent davon aus Werbeauktionen. Die US-Grenzschutzbehörde CBP räumte 2026 in einem internen Dokument ein, solche Werbe-Standortdaten ohne richterlichen Beschluss zur Verfolgung von Mobiltelefonen genutzt zu haben; Dokumente der Bürgerrechtsorganisation ACLU belegen Verträge mehrerer US-Behörden mit dem Anbieter Babel Street. Die Zeitung Le Monde zeigte 2025, dass sich über Werbedaten Identität und Bewegungen französischer Polizisten und Eliteeinheiten offenlegen lassen. Und der Markt bedient jede Anfrage: netzpolitik.org zählte im September 2025 auf dem Berliner Datenmarktplatz Datarade 2.598 Anbieter, 122 davon aus Deutschland; der dortige KI-Assistent lieferte auf die Anfrage nach Gesundheitsdaten von Kindern zwischen sechs und neun Jahren in Deutschland Krankheitsdatenbanken und eine Liste mit über 52.000 Kindergarten-Adressen. Die Beispielsuche wurde nach der Veröffentlichung abgeschaltet. Jeder dieser Datenströme beginnt im Heimnetz, mit einem Tracker in einer App oder auf einer Website, und genau dort lässt er sich unterbrechen.[144]

[141] Hayden, M.: Remarks at Johns Hopkins University, 2014. Cole, D.: We Kill People Based on Metadata. The New York Review of Books, 10. Mai 2014. Scahill, J. / The Intercept: The Drone Papers, Oktober 2015.

[142] The Intercept: American Phone-Tracking Firm Demo’d Surveillance Powers by Spying on CIA and NSA, April 2022. Vice / Motherboard: How the U.S. Military Buys Location Data from Ordinary Apps (Muslim Pro), November 2020. netzpolitik.org: Interview zur „Kill Cloud“, 2025. Sauer, H.: Boxenstopp-Vortrag vom 3. April 2025.

[143] Office of the Director of National Intelligence (ODNI): Report on Intelligence Community Use of Commercially Available Information (CAI), Januar 2022. netzpolitik.org: Bundesregierung macht Datenkauf zum Staatsgeheimnis, 2024.

[144] Federal Trade Commission: Beschwerden und Vergleiche mit Gravy Analytics, Venntel und Mobilewalla, Dezember 2024. 404 Media und Electronic Frontier Foundation: Berichte zu CBP und Werbe-Standortdaten, März 2026. ACLU: FOIA-Dokumente zu Babel Street, 2025. Le Monde: Recherche zu Standortdaten französischer Sicherheitskräfte, 2025. netzpolitik.org: Datarade-Recherche, 16. September 2025. Sauer, H.: Wie Strafverfolgungs- und Sicherheitsbehörden genau wissen können, wo sich jemand befindet, FOCUS Online, Januar 2026.

Teil 7

Schutzmaßnahmen und Privacy-Box

Regulierung, digitale Selbstverteidigung und die TrutzBox als integrierte Lösung

Was die EU gegen die Datenmacht der Konzerne tut, und warum das nicht reicht

> **Für Einsteiger:**
> Europa hat die strengsten Datenschutzgesetze der Welt und seit 2024 zusätzlich Regeln, die gezielt die größten Plattformen treffen. Die Bilanz ist gemischt: Milliardenstrafen, aber Verfahren, die Jahre dauern; neue Pflichten, aber auch Vorschläge aus Brüssel, den Schutz wieder zu lockern. Dieses Kapitel ordnet ein, was gilt, was wirkt, und warum Sie sich nicht allein auf den Gesetzgeber verlassen sollten.

DSGVO, DMA, DSA, AI Act: Bilanz und Gegenwind

Die Datenschutz-Grundverordnung (DSGVO) gilt seit Mai 2018. Bis September 2026 haben europäische Aufsichtsbehörden nach der Zählung der Kanzlei CMS 3.211 Bußgelder über zusammen 6,3 Milliarden Euro verhängt. Die fünf höchsten trafen Meta (1,2 Milliarden Euro, 2023, Datentransfers in die USA), TikTok (530 Millionen, 2025, Transfers nach China), Instagram (405 Millionen, 2022), Meta (390 Millionen, 2023) und TikTok (345 Millionen, 2023, Kinderdaten); insgesamt summieren sich Metas DSGVO-Strafen auf rund 2,3 Milliarden Euro. Die 746-Millionen-Strafe gegen Amazon aus 2021 hob ein Luxemburger Gericht im März 2026 wegen Verfahrensfehlern auf. Zum Vergleich: Meta setzte allein 2025 rund 201 Milliarden US-Dollar um, die Summe aller je verhängten DSGVO-Strafen entspricht gut einem Prozent eines einzigen Jahresumsatzes.[145]

Wirksamer als Geldbußen erwiesen sich die Regeln, die das Geschäftsmodell selbst treffen. Der Digital Markets Act (DMA) gilt seit März 2024 für sieben „Gatekeeper“. Alphabet, Amazon, Apple, ByteDance, Meta, Microsoft und Booking, mit 23 Kernplattformdiensten. Er verbietet ihnen unter anderem, Nutzerdaten über Dienste hinweg ohne echte Einwilligung zu kombinieren. Die ersten Bußgelder kamen im April 2025: 500 Millionen Euro gegen Apple, 200 Millionen gegen Meta, dessen „Zustimmen oder zahlen“-Modell keine datensparsame Alternative bot; seit Januar 2026 müssen Meta-Nutzer in der EU zwischen voll personalisierter Werbung und einer Variante mit „90 Prozent weniger Daten“ wählen können. Im Juli 2026 folgten 890 Millionen Euro gegen Google. Der Digital Services Act (DSA) verbietet seit 2024 Werbung auf Basis sensibler Daten und personalisierte Werbung an Minderjährige; erste Strafe waren 120 Millionen Euro gegen X (Dezember 2025), gegen Meta und TikTok laufen 2026 Verfahren wegen süchtig machender Gestaltung und mangelhaften Altersprüfungen. Der Data Act gibt seit

[145] CMS: GDPR Enforcement Tracker. Statistics, Stand 3. September 2026 (3.211 Bußgelder, 6,31 Mrd. Euro); Global Security Mag: GDPR violations have cost Meta almost 2.3 billion euros. Cour administrative du Luxembourg, Urteil vom 12. März 2026, Nr. 52757C (Aufhebung der CNPD-Entscheidung gegen Amazon). Meta Platforms Inc.: Fourth Quarter and Full Year 2025 Results, 28. Januar 2026.

September 2025 Nutzern Zugriff auf die Daten ihrer vernetzten Geräte, der AI Act verpflichtet seit August 2025 die Anbieter großer KI-Modelle zu Transparenz über Trainingsdaten.[146]

Auch gegen die Werbe-Infrastruktur gab es Urteile: Der Europäische Gerichtshof stufte 2024 den Einwilligungs-Code des Werbeverbands IAB Europe („TC String“) als personenbezogenes Datum ein, der französische Staatsrat bestätigte 2026 eine 40-Millionen-Strafe gegen den Werbetechnik-Konzern Criteo, pseudonyme Kennungen seien personenbezogen, sobald sich eine Person „ohne unverhältnismäßigen Aufwand“ herausgreifen lasse. Das EU-US-Datenabkommen „Data Privacy Framework“, Grundlage der meisten Transfers an US-Konzerne, hielt im September 2025 vor dem Gericht der EU stand; die Revision vor dem EuGH ist anhängig.[147]

Der Gegenwind kommt inzwischen aus Brüssel selbst. Im Februar 2025 zog die Kommission den seit 2017 verhandelten Entwurf der ePrivacy-Verordnung zurück, die Tracking und Cookies eigentlich strenger regeln sollte. Im November 2025 legte sie den „Digital Omnibus“ vor: Er soll den Begriff des personenbezogenen Datums enger fassen, KI-Training auf Basis des „berechtigten Interesses“ erleichtern und die Cookie-Regeln in die DSGVO verlagern. Der Europäische Datenschutzausschuss und der Datenschutzbeauftragte warnten im Februar 2026, die Neudefinition widerspreche der Rechtsprechung des EuGH und würde den Schutz „erheblich verengen“; Datenschutzorganisationen sprechen vom größten Rückschritt seit 2018. Der Rat strich die umstrittene Definition im Juni 2026 aus seinem Kompromiss, das Parlament berät noch. Die Hochrisiko-Pflichten des AI Act wurden bereits um 16 Monate auf Dezember 2027 verschoben. Ein „Digital Fairness Act“ gegen manipulative Gestaltung, Suchtmechanismen und personalisierte Preise ist für Ende 2026 angekündigt.[148]

Das Fundament all dieser Regeln, die informierte Einwilligung, trägt in der Praxis nicht. Eine Auswertung des Autors ergab 2026: Die Datenschutzerklärungen der 20 meistbesuchten deutschen Websites umfassen im Schnitt 8.800 Wörter, die von Facebook fast 20.000. Wer die rund 400 neuen Websites, die ein deutscher Nutzer laut einer GESIS-Erhebung pro Jahr aufruft, vollständig läse, bräuchte dafür etwa 135 Arbeitstage. Nach einer Umfrage des Bundesdatenschutzbeauftragten von 2025 wissen nur 43 Prozent der Befragten, was ein Cookie ist; 83 Prozent wünschen sich eine zentrale Einstellung statt täglicher Banner. Die Einwilligungs-Infrastruktur ist zudem selbst Teil des Marktes: Der Datenhändler LiveRamp kaufte 2019 den Consent-Anbieter Faktor. Eine Privacy-Box setzt deshalb nicht am Banner an, sondern dahinter: Sie blockiert Tracker und Consent-Dienste unabhängig davon, was angeklickt wurde. Ein zweites Beispiel für die Lücke zwischen Regel und Praxis: Die EU-Ausnahme, die Google, Meta, Microsoft und Snap seit 2021 das automatische Durchsuchen privater Nachrichten nach Missbrauchsdarstellungen erlaubte, lief am 3. April 2026 aus, nachdem das Europäische Parlament eine Verlängerung abgelehnt hatte. Die Unternehmen erklärten einen Tag später, freiwillig weiter zu scannen. Wer Nachrichten über einen selbst

[146] Europäische Kommission: Gatekeepers Portal (digital-markets-act.ec.europa.eu); Pressemitteilungen IP/25/1085 (23. April 2025, Apple 500 Mio., Meta 200 Mio. Euro) und IP/26/1670 (23. Juli 2026, Google 890 Mio. Euro); Meta commits to give EU users choice on personalised ads under the DMA, 8. Dezember 2025. Europäische Kommission: Commission fines X 120 million euros under the Digital Services Act, 5. Dezember 2025; Preliminary findings against Meta (29. April und 10. Juli 2026) und TikTok (24. Juli 2026). Verordnung (EU) 2023/2854 (Data Act), anwendbar seit 12. September 2025. Verordnung (EU) 2024/1689 (KI-Verordnung), Pflichten für Modelle mit allgemeinem Verwendungszweck seit 2. August 2025.

[147] EuGH, Urteil vom 7. März 2024, C-604/22 (IAB Europe); Marktgericht Brüssel, Urteil vom 15. Mai 2025. Conseil d’État, Entscheidung vom 4. März 2026 (Criteo, 40 Mio. Euro). Gericht der Europäischen Union, Urteil vom 3. September 2025, T-553/23 (Latombe/Kommission); Rechtsmittel C-703/25 P, eingelegt 31. Oktober 2025.

[148] Europäische Kommission: Arbeitsprogramm 2025, 11. Februar 2025 (Rücknahme des ePrivacy-Vorschlags). Europäische Kommission: Digital Omnibus, COM(2025) 837, 19. November 2025. EDSA/EDSB: Joint Opinion 2/2026 on the Digital Omnibus proposal, 11. Februar 2026. IAPP: EU member states’ leaked Digital Omnibus compromise eliminates revised GDPR definition of personal data, Juni 2026. Amtsblatt der EU, 24. Juli 2026 (Änderungsverordnung zur KI-Verordnung, Hochrisiko-Pflichten ab 2. Dezember 2027). Europäisches Parlament, Legislative Train: Digital Fairness Act (Vorschlag geplant 4. Quartal 2026).

betriebenen Dienst austauscht, ist von solchen Durchsuchungen nicht betroffen (siehe Kapitel „Sichere Chat- und Audio-/Video-Kommunikation (RTC)“).[149]

Was folgt daraus für den einzelnen Haushalt? Erstens: Die Gesetze wirken, aber langsam, zwischen Beschwerde und Bußgeld liegen bei den großen Verfahren regelmäßig drei bis fünf Jahre, und die höchsten Strafen stehen in keinem Verhältnis zu den Gewinnen aus dem Datengeschäft. Zweitens: Durchgesetzt werden die Regeln vor allem gegenüber Konzernen mit Sitz in der EU und den Adressaten des DMA. Für die Tausenden Datenhändler, App-Anbieter und Werbenetzwerke in Drittstaaten, deren Datenströme die Databroker Files sichtbar gemacht haben, gilt die DSGVO zwar ebenfalls, sobald sie sich an Menschen in der EU richten; sie dort durchzusetzen ist aber ungleich schwerer. Drittens: Der politische Wind hat sich gedreht, „Wettbewerbsfähigkeit“ und „Bürokratieabbau“ sind 2026 die Leitbegriffe, nicht Datenschutz. Wer seine Daten schützen will, kann auf Brüssel hoffen, sollte sich aber nicht darauf verlassen. Genau hier setzen die folgenden Kapitel an: bei dem, was jeder selbst im eigenen Netz tun kann.

Die zehn Gebote der Internet-Sicherheit

IT-Sicherheitsexperten haben grundlegende Verhaltensregeln zusammengestellt, die jeder Nutzer selbst befolgen kann, vier absolute Pflicht-Regeln und sechs weitere Empfehlungen. Wer diese „zehn Gebote der Internet-Sicherheit" konsequent umsetzt, senkt sein Angriffsrisiko bereits drastisch.

Die vier Pflicht-Regeln

Niemals blind auf Links oder E-Mail-Anhänge klicken

Phishing ist die häufigste Eintrittspforte für Angriffe. Bei Zweifeln an einer Mail gilt: Absenderadresse genau prüfen, mit der Maus über den Link fahren ohne zu klicken, im Zweifel die Webseite manuell aufrufen. Anhänge und Bilder sollten im Mail-Programm nicht automatisch geladen werden.

Starke Passwörter, für jeden Dienst ein anderes

Wer dasselbe Passwort mehrfach verwendet, öffnet bei einem einzigen Datenleck alle Konten gleichzeitig. Ein Passwort-Manager erzeugt für jeden Dienst ein eigenes Passwort aus mindestens zwölf Zeichen und speichert es verschlüsselt; zu merken ist nur noch ein Master-Passwort.

Updates sofort installieren, auch bei Smart-Home-Geräten

Updates schließen häufig Sicherheitslücken, die Angreifer aktiv ausnutzen. Das gilt nicht nur für Smartphone und PC, sondern auch für jede smarte Türklingel, jeden WLAN-Staubsauger und jede vernetzte Glühbirne. Geräte ohne Update-Versorgung gehören vom Netz getrennt oder ersetzt. Das gilt

[149] Sauer, H.: Datenschutz lesen? Das kostet Sie 100 Arbeitstage, FOCUS Online, April 2026 (Datenbasis: GESIS-Erhebung mit 2.148 Nutzern und knapp 50.000 Domains). BfDI: Repräsentative Umfrage zu Cookie-Bannern, 2025. LiveRamp: Übernahme von Faktor, Pressemitteilung 2019. Europäisches Parlament: Abstimmung vom 26. März 2026 zur Verlängerung der Verordnung (EU) 2021/1232; gemeinsame Erklärung der Unternehmen vom 4. April 2026. Sauer, H.: Kinderschutz oder Massenüberwachung?, FOCUS Online, April 2026.

umso mehr, als der Entwurf zum neuen Nachrichtendienstrecht vorsieht, dass bekannte Sicherheitslücken auch an Nachrichtendienste gemeldet werden dürfen, statt ausschließlich geschlossen zu werden.[150]

Regelmäßige Backups

Ransomware-Angriffe nehmen dramatisch zu. Regelmäßige Sicherungskopien wichtiger Dateien, auf einer nicht dauerhaft verbundenen externen Festplatte oder in einem verschlüsselten Cloud-Speicher, nehmen einer solchen Erpressung die Grundlage, weil sich die Daten wiederherstellen lassen. Gegen die zweite Drohung, die Veröffentlichung zuvor abgeflossener Daten, helfen sie nicht.

Sechs Empfehlungen für erweiterte Sicherheit

WLAN und Bluetooth unterwegs deaktivieren

Aktives WLAN sucht ständig nach bekannten Netzen und gibt Informationen preis. Angreifer können gefälschte Hotspots mit Namen wie „Telekom" einrichten; verbindet sich das Gerät automatisch, ist der Datenverkehr offen. Bluetooth bietet ähnliche Angriffsflächen, unterwegs beide Funkschnittstellen abschalten.

Smart-Home-Geräte überwachen und kontrollieren

Viele IoT-Geräte kommunizieren unbemerkt mit Servern in Drittländern. Soweit möglich nur Geräte ohne Internet-Zwang anschaffen, IoT in ein separates Netz setzen und Security- bzw. Privacy-Boxen einsetzen, die den Datenverkehr aller Geräte zentral analysieren und blockieren.

VPN-Verbindung für unterwegs

Öffentliche WLANs in Cafés, Hotels und Flughäfen sind ein Paradies für Datendiebe. Unterwegs gehört der gesamte Datenverkehr deshalb in einen VPN-Tunnel zum eigenen Heimnetz oder Firmennetz; die TrutzBox bringt den VPN-Server dafür mit (Kompendium Teil 2, Kapitel „Fernzugriff: VPN“). Was kommerzielle VPN-Dienste leisten und wo ihre Grenzen liegen, beschreibt das Kapitel „VPN-Dienste: Schutz mit Einschränkungen“.

[150] Bundesministerium der Justiz: Referentenentwurf zur Modernisierung des Nachrichtendienstrechts, Stand Juli 2026, Regelungen zum Umgang des BSI mit Schwachstellen. Sauer, H.: Geheimdienst-Reform 2026, FOCUS Online, Juli 2026.

Weniger Apps, mehr Sicherheit

Jede App ist ein potenzielles Sicherheitsrisiko. Viele kostenlose Apps finanzieren sich durch den Verkauf der Nutzerdaten, eine Taschenlampen-App mit Zugriff auf Kontakte, Standort und Mikrofon verfolgt genau dieses Ziel. Regelmäßig den App-Bestand prüfen und nicht genutzte Apps löschen.

Zwei-Faktor-Authentifizierung aktivieren

Auch das stärkste Passwort kann durch Datenleck, Phishing oder Schadsoftware abhandenkommen. Besonders kritisch ist dies bei E-Mail-Konten, über die sich alle anderen Passwörter zurücksetzen lassen. 2FA überall aktivieren, wo sie angeboten wird; Authenticator-Apps sind sicherer als SMS-Codes. Zusätzlich beim Mobilfunkanbieter eine Sperre gegen unbefugte Rufnummern-Übertragung einrichten (siehe Kapitel „Die Mobilfunknummer als Generalschlüssel“).

Smartphone absichern

Bildschirmsperre mit mindestens sechsstelliger PIN, Geräteverschlüsselung, App-Berechtigungen für Kamera, Mikrofon und Standort einzeln einschränken, App-Tracking-Transparenz (iOS) bzw. Datenschutz-Einstellungen (Android) nutzen, Nachrichteninhalte auf dem Sperrbildschirm ausblenden, Fernortung und Fernlöschung aktivieren.

Warum die TrutzBox dennoch gebraucht wird

Wer die zehn Gebote konsequent befolgt, ist gegen einen Großteil der Alltagsangriffe gut gewappnet. Alle Regeln haben jedoch gemeinsame strukturelle Grenzen, die in modernen Haushalten nicht mehr von der Disziplin Einzelner kompensiert werden können.
Erstens setzen sie voraus, dass jeder Nutzer jederzeit aufmerksam bleibt. Ein einziger unbedachter Klick eines Kindes oder Gastes reicht aus, um das gesamte Heimnetz zu kompromittieren. Zweitens verweisen mehrere Gebote, insbesondere zu IoT, WLAN und VPN, explizit auf Security- und Privacy-Boxen als technische Lösung. Genau diese Funktion erfüllt die TrutzBox: zentrale Kontrolle des Datenverkehrs aller Geräte, unabhängig von individueller Disziplin.
Drittens greifen große Teile heutiger Bedrohungen, kommerzielles Tracking, Real-Time-Bidding, Browser-Fingerprinting, Datenabflüsse aus Smart-TVs und Connected Cars, Microsoft-Telemetrie, nicht über Phishing oder Schadsoftware, sondern über legale Kanäle, die jedes Gerät selbst öffnet. Gegen diesen Datenabfluss helfen weder Passwörter noch Updates oder 2FA, sondern nur die Kontrolle des ausgehenden Verkehrs auf Netzwerkebene, wie sie TrutzBrowse mit Proxy-/URL-Filterung und zusätzlich mit IP-Blockierung (Angriffsschutz) leistet. Viertens lassen sich IoT-Geräte, smarte Lautsprecher, Türklingeln, Kameras, Fernseher, von Endnutzern weder härten noch mit 2FA absichern; sie funken, was und wohin der Hersteller will. Nur eine vorgelagerte Filterinstanz wie die TrutzBox macht diesen Verkehr sichtbar und kontrollierbar.
Die zehn Gebote bleiben damit die unverzichtbare Basis der digitalen Selbstverteidigung. Sie genügen jedoch nicht mehr, sobald mehrere Personen, mehrere Geräte und mehrere Hersteller mit eigenen wirtschaftlichen Interessen im Spiel sind, also in praktisch jedem heutigen Haushalt. Genau dort setzt die TrutzBox an.

Warum klassische Sicherheitsmaßnahmen nicht ausreichen

Für Einsteiger:

Eine Firewall ist wie ein Wachmann am Eingang eines Gebäudes, er prüft, wer hereinkommt, und hält Ungebetene fern. Aber er schaut nicht, was die Mitarbeiter in ihrer Tasche nach draußen tragen, wenn sie das Gebäude verlassen. Genau das ist das Problem: Klassische Sicherheitssysteme sind auf Eindringlinge von außen ausgerichtet. Den stillen, täglichen Abfluss von Nutzerdaten über normale Internetverbindungen bemerken sie nicht.

Grenzen von Firewall und IDS aus Sicherheitsperspektive

Im Januar 2026 veröffentlichte der Autor in CSO Online einen viel beachteten Artikel über die Grenzen klassischer IT-Sicherheitskonzepte. Die Kernaussage: Traditionelle Sicherheitswerkzeuge wie Firewalls und Intrusion-Detection-Systeme schützen gut gegen externe Angreifer, die versuchen, in ein Netzwerk einzudringen. Sie sind jedoch strukturell blind gegenüber dem stillen Abfluss von Daten über legitime ausgehende Verbindungen, und genau dieses Szenario ist im Zeitalter des allgegenwärtigen Trackings das relevanteste.[151]

Eine Firewall ist unverzichtbar und bildet die erste Verteidigungslinie gegen externe Angriffe. Aber sie hat fundamentale Einschränkungen: Sie ist hauptsächlich reaktiv und auf bekannte Bedrohungen konfiguriert. Bei täglich über 450.000 neuen Schadprogrammen (AV-TEST) entstehen zwangsläufig Sicherheitslücken. Zudem kontrolliert sie primär eingehenden Verkehr, die unkontrollierte Übertragung sensibler Daten nach außen bleibt oft unbemerkt, weil sie als legitimer HTTP/HTTPS-Verkehr erscheint. Eine Firewall-Regel, die ausgehenden Web-Traffic erlaubt, erlaubt damit auch die Übermittlung von Tracking-Daten an hunderte externe Server.[152]

Intrusion-Detection-Systeme (IDS) erkennen Eindringlinge erst, wenn diese bereits im System sind, vergleichbar mit einem Rauchmelder, der vor einem Brand warnt, ihn aber nicht verhindert. Advanced Persistent Threats (APTs), hochentwickelte, zielgerichtete Angriffe, die typischerweise staatlichen Akteuren oder hochprofessionellen kriminellen Gruppen zugeschrieben werden, können so monatelang unentdeckt in Netzwerken verweilen. Im Durchschnitt dauert es laut IBM-Studie 2026 rund 180 Tage, bis eine Datenpanne überhaupt entdeckt wird, und weitere zwei Monate, bis sie eingedämmt ist.[153]

Das entscheidende Problem aus der Perspektive des Datenschutzes: Selbst ein perfekt konfiguriertes Firewall-IDS-System schützt nicht vor dem systematischen Datenabfluss durch kommerzielles Tracking. Ein Mitarbeiter, der morgens spiegel.de aufruft, übermittelt dabei an bis zu 50 verschiedene Tracking-Dienste Informationen über seinen Browser, seinen Standort und sein Interesse für die gelesenen Artikel. Diese Übermittlung passiert die Firewall völlig ungehindert, sie ist ja kein Angriff, sondern normaler HTTP-Traffic.

[151] Hermann Sauer: Digitale Integrität: Warum Firewall und IDS nicht reichen. CSO Online, 26. Januar 2026. https://www.csoonline.com/article/4121937/digitale-integritat-warum-firewall-und-ids-nicht-reichen.html (zuletzt abgerufen Januar 2026; der Artikel ist inzwischen nicht mehr online)

[152] MITRE ATT&CK Framework: Exfiltration Techniques (TA0010). https://attack.mitre.org/tactics/TA0010/. AV-TEST: Malware-Statistik, av-test.org (über 450.000 neue Schadprogramme und PUA pro Tag, 2026).

[153] IBM: Cost of a Data Breach Report 2026. Zeit bis Erkennung und Eindämmung 247 Tage (2025: 181 Tage Erkennung + 60 Tage Eindämmung).

Digitale Integrität für Unternehmen: Was IBM Cost of a Data Breach 2026 zeigt

Der IBM-Bericht 2026 beziffert die durchschnittlichen Kosten einer Datenpanne auf 4,99 Millionen US-Dollar (USA: 11,5 Millionen). Phishing ist mit 17 Prozent der Fälle der häufigste Einstieg und mit 5,29 Millionen US-Dollar je Vorfall der teuerste, gefolgt von Innentätern und gestohlenen Zugangsdaten. Phishing, Social Engineering und Business Email Compromise werden erheblich durch Datenbrokerdaten ermöglicht und effektiver gemacht. Ein Unternehmen, das seine Mitarbeiter und deren Aktivitäten vor dem kommerziellen Tracking schützt, reduziert damit auch direkt das Risiko von Phishing und CEO Fraud.

Drei Methoden, Netzwerkzugriffe zu erkennen und zu blockieren

Für Einsteiger:

Die TrutzBox blockiert unerwünschte Verbindungen auf zwei Ebenen: als Proxy, der HTTPS-Verbindungen analysiert und URLs gezielt sperren oder anonymisieren kann (TrutzBrowse, TrutzContent), und zusätzlich auf Netzwerkebene durch direkte IP-Adress-Blockierung (Angriffsschutz), die alle Protokolle abdeckt. DNS-Filterung setzt die TrutzBox nicht ein, da ein Proxy-Filter eine deutlich präzisere und überlegene Kontrolle ermöglicht.

Proxy-Filter und IP-Blockierung: die zwei Schutzebenen

Die TrutzBox setzt auf zwei komplementäre Methoden zur Kontrolle des Netzwerkverkehrs; am Markt üblich ist daneben eine dritte, die DNS-Blockierung. Warum die TrutzBox auf DNS-Sperren verzichtet und was DNS-Filter grundsätzlich nicht sehen, erklärt der Abschnitt „Warum Filter Jahr für Jahr blinder werden“ weiter unten. Die folgende Tabelle stellt die drei Methoden gegenüber:

Methode	Vorteile	Nachteile
DNS-Sperre („Nameserver“, z. B. Pi-hole)	• Einfach umzusetzen, geringer Aufwand • Sperrt unerwünschte Domains flächendeckend	• Leicht zu umgehen (andere DNS-Server, DoH/DoT) • Hilft nicht bei direkt angesprochenen IP-Adressen • Kann nicht innerhalb einer Domain unterscheiden
IP-Blockierung (TrutzBox: Angriffsschutz)	• Wirkt für alle Protokolle und Geräte, auch ohne sichtbaren Domain-Namen • Fängt auch Schadsoftware, die feste IP-Adressen nutzt	• IP-Adressen wechseln häufig (CDN, Cloud) • Kann bei gemeinsam genutzten Servern zu viel sperren • Sperrlisten müssen aktuell gehalten werden (erledigt die TrutzBox selbst)
Proxy/URL-Filter (TrutzBox: TrutzBrowse, TrutzContent)	• Am präzisesten: einzelne Seiten statt ganzer Domains • Anonymisiert zusätzlich die übertragenen Daten	• Nur für http/https (Port 80/443) • Braucht das TrutzBox-Zertifikat auf dem Gerät • Verschlüsselter Verkehr (QUIC, VPN, Apple Private Relay) und Apps mit fest eingebautem Zertifikat laufen vorbei

Methode 1: Proxy/URL-Filter, TrutzBrowse und TrutzContent

> **Für Einsteiger:**
> Ein Proxy ist wie ein aufmerksamer Türsteher, der jeden Datenfluss zwischen Ihrem Gerät und dem Internet sieht, prüft und, bei Bedarf, stoppt oder anonymisiert. Das ist die präziseste Kontrollmethode: Nicht ganze Domains werden gesperrt, sondern einzelne URLs oder Datenpakete, je nach Filtergruppe des anfragenden Geräts.

Proxy/URL-Filter: Genauigkeit, HTTPS-Prüfung, Einsatz

Ein Proxy-Filter sieht den HTTP/HTTPS-Datenverkehr aller Geräte im Netzwerk. Vorteile gegenüber einfacher DNS-Filterung:

- Granulare URL-Kontrolle: Einzelne Pfade innerhalb einer Domain können unterschiedlich behandelt werden. Tracking-Skripte auf einer ansonsten erlaubten Domain werden blockiert, der eigentliche Inhalt bleibt zugänglich.
- Geräteindividuelle Regeln: Ein Proxy kann je Gerät und Nutzer eigene Regeln anwenden (Kinder-, Erwachsenen-, IoT-Profil). DNS-Filterung kann das nicht.

- Anonymisierung: Ein Proxy kann Daten nicht nur sperren, sondern auch verändern, etwa verräterische Browser-Kennungen entfernen. Eine DNS-Sperre kann das nicht.
- Anwendungsbereich: HTTP/HTTPS-Verkehr auf Port 80 und 443. Andere Protokolle (z. B. proprietäre IoT-Protokolle) erreicht der Proxy nicht, dafür ist die IP-Blockierung zuständig. Wie die TrutzBox diese Methode mit TrutzBrowse und TrutzContent umsetzt und was dafür auf den Geräten nötig ist: Kompendium Teil 2, Kapitel „TrutzBox-Proxy: Funktion und interner Aufbau“, „TrutzContent“ und „TrutzBrowse“.

Methode 2: IP-Blockierung, der Angriffsschutz

Für Einsteiger:

Die TrutzBox blockiert zusätzlich direkte IP-Adressen, auf Netzwerkebene, für alle Protokolle. Bekannte unerwünschte IP-Adressen und -Bereiche landen auf einer Blacklist und werden gesperrt. Das ist besonders wichtig für IoT-Geräte, die oft eigene Protokolle nutzen und am Proxy vorbeikommunizieren. Die nötigen Sperrlisten bringt die TrutzBox mit und hält sie selbsttätig aktuell.

IP-Sperren auf Netzwerkebene: alle Protokolle, alle Geräte

Die IP-Blockierung ergänzt den Proxy-Filter um eine Netzwerkebene, die alle Protokolle abdeckt. Sie arbeitet ausschließlich per Blacklist: bekannte unerwünschte IP-Adressen und IP-Bereiche werden gesperrt. Kernaspekte:

- Protokollunabhängig: IP-Blockierung greift unabhängig vom genutzten Protokoll. MQTT (IoT-Protokoll), proprietäre Hersteller-Protokolle, UDP-Verbindungen, alle können auf Basis von IP-Adressen gefiltert werden.
- IoT-Schutz: IoT-Geräte wie Smart-TVs, Heizungssteuerungen, Kameras und Haushaltsgeräte nutzen typischerweise eigene Protokolle, die am HTTP/HTTPS-Proxy vorbeilaufen. IP-Blockierung schließt diese Lücke, auch wenn das Gerät kein Zertifikat unterstützt.
- Herausforderung: IP-Adressen von CDN-Diensten (Cloudflare, Akamai, AWS) rotieren häufig. Für Web-Verkehr bleibt der Proxy die primäre Filtermethode; IP-Blockierung entfaltet ihren größten Nutzen bei IoT-Geräten mit stabilen Serverzielen. Umsetzung in der TrutzBox (Sperrlisten, Ausnahmen, Angriffsschutz, blockierte Adressen): Kompendium Teil 2, Kapitel „Netzwerk“.

Warum Filter Jahr für Jahr blinder werden

Für Einsteiger:

Viele bekannte Lösungen wie Pi-hole oder AdGuard Home blockieren Tracker über den Namensdienst (DNS). Das Blockprotokoll füllt sich, das Gefühl ist gut. Doch die Statistik zeigt nur, was der Filter überhaupt zu sehen bekommt; alles, was an ihm vorbeiläuft, taucht nirgends auf, und dieser unsichtbare Anteil wächst seit Jahren. Die TrutzBox setzt deshalb nicht allein auf den Domain-Namen. Sechs Wege, auf denen Verkehr am Filter vorbeiläuft:

- Viele Smart-TVs, Sprachassistenten und Spielkonsolen ignorieren den heimischen Namensdienst und fragen direkt bei Google oder Cloudflare an.

- Browser und Apps verschlüsseln ihre Adress-Anfragen (DoH/DoT, verschlüsseltes DNS), ein DNS-Filter im Heimnetz sieht davon nichts mehr.
- Mit „Encrypted Client Hello“ (ECH), das Cloudflare Ende 2024 für alle Kunden aktiviert hat, ist auch der Empfänger-Name beim Verbindungsaufbau verschlüsselt.
- Rund jede fünfte Web-Verbindung (Cloudflare 2025: 21 Prozent) läuft über HTTP/3 (QUIC) und ist für klassische Netzwerk-Inspektion kaum auswertbar.
- Push-Dienste von Apple und Google nutzen fest einprogrammierte Server-Adressen, ganz ohne DNS-Abfrage.
- Apples iCloud Private Relay leitet auf iPhones mit iCloud+ den Safari-Verkehr durch Apple-Server; Apple dokumentiert selbst, dass damit auch Schul- und Firmenfilter umgangen werden.

🔧 DNS-Sperre gegen Proxy-Filter, und was beide nicht sehen

DNS-Blockierung sperrt Domains, bevor eine Verbindung aufgebaut wird, indem auf DNS-Anfragen keine IP-Adresse zurückgegeben wird. Dieser Ansatz hat spezifische Schwächen, die ein Proxy-Filter nicht hat:

- Keine Unterscheidung innerhalb einer Verbindung: Einzelne Hostnamen kann ein DNS-Filter getrennt behandeln, je nach Werkzeug auch einzelne Geräte oder Gruppen. Pfade, Skripte und Inhalte derselben Domain sieht er dagegen nicht. Ein Proxy kann gezielt einzelne Pfade oder Skripte sperren, ohne die ganze Domain zu blockieren.
- Keine Anonymisierung: DNS-Blockierung verhindert Verbindungen, anonymisiert aber keine Daten. TrutzBrowse geht darüber hinaus und anonymisiert den Datenverkehr aktiv.
- Keine geräteindividuellen Regeln: Standard-DNS-Filterung gilt für alle Geräte gleich. TrutzContent ermöglicht gerätespezifische Filterprofile, das ist nur auf Proxy-Ebene möglich.
- Umgehung durch DoH/DoT: Viele Geräte und Apps nutzen DNS-over-HTTPS (DoH) oder DNS-over-TLS (DoT) und umgehen damit lokale DNS-Filter vollständig. Der Proxy-Filter ist davon nicht betroffen, weil er den Verkehr selbst sieht, nicht nur die Namensanfrage. Die TrutzBox zwingt zusätzlich alle Geräte auf ihren eigenen Namensdienst (Kompendium Teil 2, Kapitel „DNS-Auflösung“).

🔧 Wie viel ist heute noch sichtbar? Eine Messung

Ein typischer Haushalt mit 8 bis 15 vernetzten Geräten erzeugt in 24 Stunden mehrere tausend Verbindungen. Eine eigene, ausdrücklich nicht repräsentative Messung des Autors in einem Heimnetz mit zwölf Geräten im Mai 2026 ergab: Nur rund ein Drittel des ausgehenden Datenverkehrs lief über klassische, für einen DNS- oder Proxy-Filter erkennbare Verbindungen. Rund zwei Drittel liefen daran vorbei; der größte Einzelposten war das neue Transportprotokoll QUIC mit etwa 65 Prozent aller ausgehenden Bytes. Mehrere hundert Verbindungen kamen ganz ohne Namensabfrage zustande, direkt zu fest einprogrammierten Adressen der Push-Dienste von Apple und Google und zu Telemetrie-Servern der Fernsehhersteller. Drei Geräte im selben Netz zeigten drei verschiedene Muster:

- Ein Windows-PC verhielt sich kooperativ: Alle 360 Verbindungen liefen sichtbar durch den Filter.
- Ein Sony-Fernseher öffnete 440 Verbindungen, rund die Hälfte am Filter vorbei, überwiegend Push-Dienste und die Bilderkennung ACR.
- Ein iPhone öffnete 720 Verbindungen, davon 23 Prozent über QUIC ohne erkennbaren Zielnamen. Seine Namensabfragen schickte es verschlüsselt an Google, der lokale Filter sah keine einzige.

Diese Zahlen sind ein Schnappschuss aus einem einzelnen Netz, sie decken sich aber mit dem, was Studien strukturell zeigen: Eine Untersuchung an über 200 Haushalten fand, dass rund 70 Prozent der Smart-TVs den heimischen Namensdienst ignorieren, bei Sprachassistenten waren es fast alle. Die Internet-Standardisierungsorganisation IETF sah sich 2025 veranlasst, Hersteller in einem eigenen Dokument zur Beachtung des Heimnetz-Namensdienstes zu ermahnen. Zur Einordnung: Die neuen Verschlüsselungsstandards wurden nicht entwickelt, um Filter im Wohnzimmer auszuhebeln, sondern zum Schutz vor neugierigen Providern und vor Zensur. Dass sie zugleich dem eigenen Filter die Sicht nehmen, ist ein Nebeneffekt, den Gerätehersteller, Schadsoftware und staatliche Akteure gleichermaßen nutzen (siehe Teil 6). Ehrlich ist auch: Selbst ein Proxy mit eigenem Zertifikat scheitert an Apps, die nur ihr fest eingebautes Zertifikat akzeptieren, an Apples Private Relay und an Verkehr, der nicht über die Web-Ports läuft. Die Antwort ist darum nicht die nächstlängere Sperrliste, sondern die Kombination: den Umweg zu fremden Namensdiensten sperren, bekannte verschlüsselte DNS-Anbieter blockieren, QUIC im Heimnetz abschalten, damit Browser auf den sichtbaren Weg zurückfallen, Fernseher und Sprachassistenten in ein eigenes Netz trennen, und vor allem Sichtbarkeit: wissen, was überhaupt hinausgeht.[154]

🔧 So schließt die TrutzBox die Lücke

Zwei der drei Methoden, DNS-Sperre und Proxy-Filter, brauchen den Domain-Namen. Die TrutzBox kombiniert deshalb alle drei Ebenen: Sie sperrt anhand der IP-Adresse auch ohne Domain-Namen, zwingt eigenmächtige Geräte auf ihren eigenen Namensdienst, unterbindet QUIC, und der Monitor macht jeden dieser Fälle sichtbar. Marktübliche DNS-Filter sind an dieser Stelle blind. Einzelheiten: Kompendium Teil 2, Kapitel „Netzwerk“, Abschnitte „Verkehr ohne sichtbaren Domain-Namen“ und „DNS-Auflösung“.

[154] Sauer, H.: Warum Werbe- und Trackingfilter Jahr für Jahr blinder werden, Kuketz-Forum, 2026. Sauer, H.: Werbeblocker im Test: So tricksen Tracker Pi-hole und AdGuard aus, FOCUS Online, Mai 2026. Mazhar, M. H. / Shafiq, Z.: Characterizing Smart Home IoT Traffic in the Wild, 2020 (arXiv 2001.08288). RFC 9726: Operational Considerations for Use of DNS in IoT Devices, IETF, März 2025. Cloudflare Radar: 2025 Year in Review. Apple Support 102022: Manage iCloud Private Relay.

Etablierte Schutzlösungen und ihre Grenzen

Für Einsteiger:

Es gibt viele Werkzeuge, die versprechen, Ihre Privatsphäre im Internet zu schützen: Browser-Plugins, die Werbung blockieren, VPN-Dienste, die Ihre IP-Adresse verbergen, oder spezielle Browser, die weniger Daten weitergeben. All diese Werkzeuge leisten etwas, aber jedes schützt nur einen kleinen Ausschnitt. Es ist wie eine Regenjacke ohne Hose: Der Oberkörper bleibt trocken, aber die Hälfte wird nass. Wirklicher Schutz braucht eine Lösung, die alles gleichzeitig abdeckt.

Überblick der gängigen Einzellösungen

Vor der Beschreibung der TrutzBox als integrierter Lösung lohnt ein systematischer Überblick über die verfügbaren Einzellösungen und ihre jeweiligen Stärken und Grenzen. Denn das Verständnis dieser Grenzen ist entscheidend dafür, warum eine integrierte Lösung auf Netzwerkebene notwendig ist.

„Werbung blocken“ klingt nach einer Disziplin, ist aber technisch eine Familie sehr unterschiedlicher Werkzeuge. Erstens DNS-Filter wie Pi-hole oder AdGuard Home, die Anfragen nach unerwünschten Domains ins Leere laufen lassen. Zweitens Browser-Erweiterungen wie uBlock Origin, die einzelne Adressen innerhalb einer Seite sperren, aber nur in genau einem Browser auf genau einem Gerät wirken. Drittens Filter-Apps auf dem Smartphone, die das ganze Gerät durch einen lokalen Tunnel leiten, an dem manche Apps vorbeigehen. Viertens transparente Proxys mit eigenem Zertifikat, die den verschlüsselten Web-Verkehr aller Geräte prüfen können, im Unternehmensumfeld seit Jahren üblich, im Heimnetz von wenigen Geräten wie der TrutzBox umgesetzt. Fünftens Filter-Dienste in der Cloud, die den Namensdienst beim Anbieter statt zu Hause betreiben. Alle fünf teilen eine Annahme: Das Gerät spricht den Weg, den der Filter erwartet. Wie brüchig diese Annahme geworden ist, beschreibt das Kapitel „Warum Filter Jahr für Jahr blinder werden“. Die folgende Übersicht ordnet gängige Lösungen für Heim- und Kleinbüro-Netze ein, ohne Anspruch auf Vollständigkeit, nach öffentlich zugänglichen Herstellerangaben (Stand 2026):

Lösung	Art	Bemerkenswertes
Pi-hole, AdGuard Home (lokal)	DNS-Filter	Klassiker; ohne zusätzliche Firewall-Regeln anfällig für DNS-Umgehung
NextDNS, Control D, AdGuard DNS	DNS-Filter in der Cloud	Profile je Gerät, die Anfragen liegen beim Anbieter
Cloudflare 1.1.1.3, Quad9	Öffentlicher Filter-Namensdienst	Feste Sperrliste, keine eigene Anpassung
Firewalla Gold, Plus	Heim-Firewall	Bietet nach Herstellerangaben die Prüfung von QUIC-Verkehr an
Gryphon	Mesh-Router	Schwerpunkt Kindersicherung
TrutzBox	Privacy-Box mit lokaler Datenhaltung	Profile je Gerät, transparenter Proxy mit URL-Filter, IP-Sperren, Betrieb ohne Cloud-Anbindung
pfSense mit Suricata	Firewall zum Selbstbau	Erkennung über Verbindungsmerkmale, keine Regeln je Gerät
OPNsense mit Zenarmor	Firewall zum Selbstbau	Entschlüsselung mit eigenem Zertifikat, QUIC-Sperre, kostenpflichtiges Zusatzmodul

(Zusammenstellung © 2026 Comidio GmbH, nach Herstellerangaben)

Browser-Plugins: Notwendig, aber nicht ausreichend

Für Einsteiger:

Browser-Erweiterungen wie uBlock Origin oder Privacy Badger blockieren bekannte Werbetracker und machen das Surfen spürbar ruhiger: weniger Werbung, weniger Aufpoppen, weniger Verfolgung. Das ist gut. Aber sie schützen nur den Browser auf dem einen Gerät, auf dem sie installiert sind, und nur so lange, wie der Tracker bekannt ist. Ihr Smartphone, Ihr Smart-TV und Ihre Spielkonsole bleiben komplett ungeschützt.

Schutzumfang und Grenzen von Browser-Erweiterungen

Browser-Erweiterungen wie uBlock Origin, Privacy Badger, Ghostery, AdBlock Plus und DuckDuckGo Privacy Essentials bieten einen ersten, wichtigen Schutz-Layer gegen Tracker und Werbung. Sie können bekannte Tracker-Skripte blockieren und verhindern, dass offensichtliche Werbeplattformen Nutzerdaten sammeln. uBlock Origin blockiert Werbung und Tracker auf Basis regelmäßig aktualisierter Listen und gilt als eines der wirksamsten frei verfügbaren Browser-Schutzwerkzeuge, ist allerdings seit 2025 wegen der Umstellung von Chrome auf „Manifest V3“ dort nicht mehr verfügbar, weiterhin aber für Firefox.[155]

Erweiterungen sind zudem selbst ein Risiko. Eine im Februar 2026 veröffentlichte Analyse von 32.000 Chrome-Erweiterungen fand 287, die den Browserverlauf aktiv an fremde Server senden, mit zusammen 37,4 Millionen Nutzern, darunter auch Werbeblocker. Im Juli 2025 beschrieb die Sicherheitsfirma Spin.AI die Kampagne „RedDirection“: 36 zunächst harmlose Erweiterungen mit 16,5 Millionen Nutzern erhielten den Schadcode erst über ein späteres Update. Wer Erweiterungen nutzt, sollte deshalb so wenige wie möglich installieren und nur solche, deren Herausgeber bekannt ist. Der Abfluss selbst läuft als gewöhnlicher verschlüsselter Web-Verkehr zu Servern, die ein Filter im Heimnetz sperren und ein Netzwerk-Monitor sichtbar machen kann.[156]

Die Grenzen dieser Werkzeuge sind jedoch erheblich und strukturell bedingt. Sie schützen ausschließlich den Browser, alle anderen Anwendungen (E-Mail-Client, Office-Software, VoIP-Apps) und alle anderen Geräte im Netzwerk (Smartphone, Smart-TV, IoT-Geräte) sind vollständig ungeschützt. Sie sind auf bekannte Tracker-Listen angewiesen: Neue, unbekannte Tracker passieren ungehindert, bis sie erkannt und in eine Blockliste aufgenommen wurden, was Wochen dauern kann. Fingerprinting-Methoden (Canvas, Audio, WebGL) können sie in der Regel nicht verhindern. Auf mobilen Geräten funktionieren sie nur in bestimmten Browsern, nicht in Apps.

- Schutzbereich: nur der jeweilige Browser, nicht das Gerät, nicht das Netzwerk[157]
- Keine Wirkung gegen Fingerprinting[158]
- Auf mobilen Geräten nur begrenzt einsetzbar[159]
- Keine Wirkung gegen IoT-Tracking[160]

[155] Electronic Frontier Foundation: Privacy Badger. https://privacybadger.org/. Gorhill: uBlock Origin. GitHub Repository. https://github.com/gorhill/uBlock

[156] Q Continuum: Analyse „spying-extensions“ (GitHub), Februar 2026. Spin.AI: RedDirection Browser Hijacking Campaign, Juli 2025. Sauer, H.: Browser-Datenschutz im Test, FOCUS Online, 2026.

[157] uBlock Origin Dokumentation: Scope and Limitations. https://github.com/gorhill/uBlock/wiki

[158] EFF: Cover Your Tracks. Test your browser's fingerprinting. https://coveryourtracks.eff.org

[159] Mozilla: Firefox Focus als mobile Lösung. https://www.mozilla.org/de/firefox/browsers/mobile/focus/

[160] Princeton IoT Inspector: Tracking in Smart Home Devices. https://iot-inspector.princeton.edu

VPN-Dienste: Schutz mit Einschränkungen

Für Einsteiger:

Ein VPN (Virtual Private Network) ist wie ein getöntes Autofenster: Von außen kann niemand hineinschauen, aber der Fahrer des Auto-Verleihs, bei dem Sie das Fahrzeug gemietet haben, weiß sehr wohl, wo Sie hinfahren. Bei VPN bedeutet das: Statt Ihrem Internetanbieter vertrauen Sie nun dem VPN-Anbieter. Gute, bezahlte VPN-Dienste leisten einiges. Kostenlose VPN-Dienste finanzieren sich oft durch den Verkauf Ihrer Nutzungsdaten, das genaue Gegenteil von Datenschutz.

VPN-Technik, Vertrauensfrage und Grenzen

Ein Virtual Private Network (VPN) leitet den gesamten Internetverkehr eines Geräts über einen Server des VPN-Anbieters um. Gegenüber den besuchten Websites erscheint die IP-Adresse des VPN-Servers, nicht die des Nutzers. Das bietet einen gewissen Schutz gegen IP-basiertes Tracking und verhindert, dass der eigene Internetanbieter (ISP) den Datenverkehr protokolliert.[161]

Die Grenzen von VPN-Diensten sind jedoch grundlegend. Erstens muss der Nutzer dem VPN-Anbieter vertrauen: Wer seinen Internetverkehr nicht von seinem ISP protokolliert haben möchte, zeigt ihn stattdessen dem VPN-Anbieter. Bei kommerziellen, kostenlosen VPN-Diensten besteht ein erhebliches Risiko, dass Nutzerdaten verkauft werden, das Geschäftsmodell „kostenloser Dienst gegen Daten" funktioniert für VPN genauso wie für soziale Netzwerke. Wer einen kommerziellen Dienst nutzt, sollte auf einen Sitz in der EU und eine unabhängig geprüfte No-Log-Zusage achten; die bessere Lösung ist ein VPN-Tunnel ins eigene Netz, wie ihn die TrutzBox bereitstellt (Kompendium Teil 2, Kapitel „Fernzugriff: VPN“).

Zweitens verhindert VPN weder Fingerprinting noch Cookie-Tracking. Wer sich bei Google einloggt, ist für Google identifiziert, unabhängig von der IP-Adresse. Der Meta-Pixel trackt weiterhin. Session-Replay-Skripte funktionieren weiterhin. Drittens verändert VPN nicht das Verhalten von Apps und Betriebssystemen, die im Hintergrund Daten senden. Smart-TVs, IoT-Geräte und Betriebssystem-Telemetrie sind durch VPN nicht geschützt, es sei denn, VPN wird auf Router-Ebene für das gesamte Netzwerk konfiguriert.

Tor: Anonymität auf Kosten der Performance

Für Einsteiger:

Das Tor-Netzwerk ist der Goldstandard für digitale Anonymität. Stellen Sie sich vor, Sie schicken Ihren Brief zunächst zu drei verschiedenen Weiterleitstationen in verschiedenen Ländern, und jede Station kennt nur die nächste Adresse, aber nicht den Ursprung. Tor funktioniert ähnlich, ist aber spürbar langsamer als normales Internet und wird von vielen Websites blockiert. Für Journalisten und Aktivisten unter autoritären Regierungen ist es unverzichtbar, für die tägliche Nutzung der meisten Menschen zu unpraktisch.

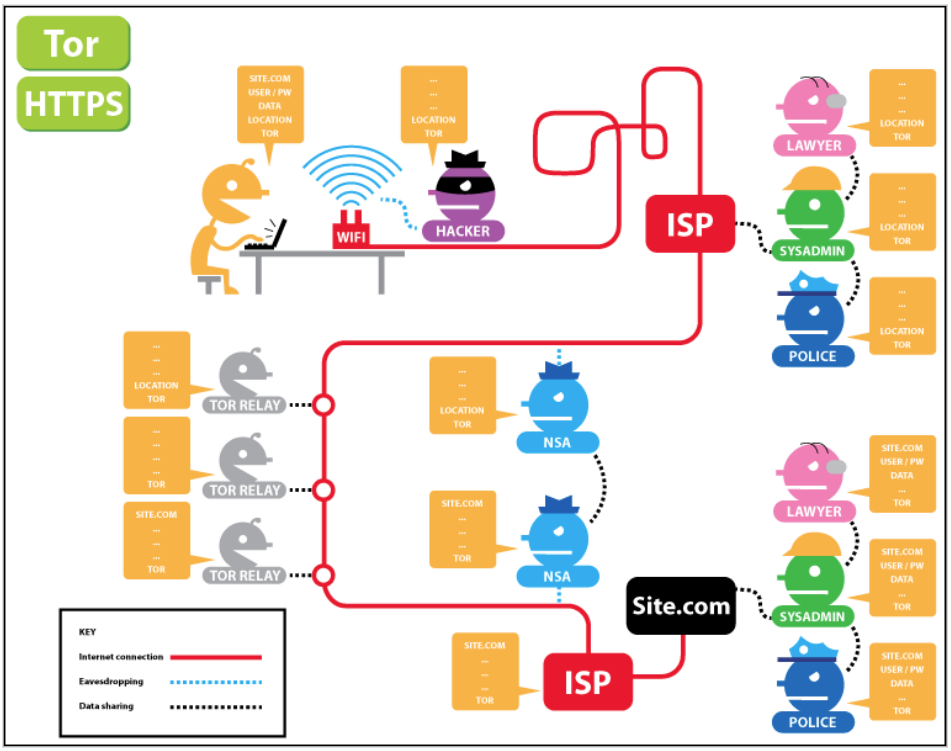
[161] Electronic Frontier Foundation: Privacy Tools. VPN vs. Tor. https://www.eff.org/pages/tor-and-https. Enthält eine visuelle Erklärung der Unterschiede zwischen verschiedenen Schutzmechanismen.

Das Tor-Netzwerk: Architektur und Grenzen

Das Tor-Netzwerk (The Onion Router) bietet einen deutlich höheren Anonymitätsgrad als VPN. Statt über einen einzelnen Server wird der Datenverkehr über eine Kette von drei zufällig ausgewählten Relay-Servern geleitet, einem Entry-Guard, einem Middle-Relay und einem Exit-Node. Jeder Server kennt dabei nur den vorherigen und den nächsten in der Kette, nicht den Ursprung und das Ziel gleichzeitig. Die Verschlüsselung ist mehrschichtig (daher „Zwiebel"-Struktur): Nur der Entry-Guard kennt die IP-Adresse des Nutzers, aber nicht das Ziel; nur der Exit-Node kommuniziert mit dem Ziel, aber nicht mit dem Nutzer direkt.[162]

Tor bietet echte und nachgewiesene Anonymität und wird von Journalisten, Whistleblowern, Aktivisten und Personen in autoritären Staaten intensiv genutzt. Die Grenzen: Tor ist deutlich langsamer als normales Internet (typischerweise 5-10-fach längere Ladezeiten), manche Dienste blockieren bekannte Tor-Exit-Knoten (Netflix, Online-Banking, viele größere Websites), und in einigen Ländern ist die Nutzung von Tor verdächtig oder sogar kriminalisiert. Für den alltäglichen Gebrauch ist Tor für die meisten Nutzer zu unpraktisch.

Wer bei der Nutzung von Tor und HTTPS welche Daten sehen kann, zeigt die Übersicht der EFF:



Was Angreifer, Anbieter und Netzbetreiber jeweils sehen, wenn Tor und HTTPS ein- oder ausgeschaltet sind.
(Quelle: EFF, eff.org/pages/tor-and-https, Lizenz CC BY 3.0 US)

[162] Tor Project: How does Tor work? https://www.torproject.org/about/history/. Dingledine, R. / Mathewson, N. / Syverson, P.: Tor: The Second-Generation Onion Router. USENIX Security Symposium, 2004.

Die Zusammenfassung der Sichtbarkeiten im Überblick:

Wer kann meine Daten sehen	User: Anwender	Hacker: der beim Anwender das WLAN/Router abhört	Lawyer : Anwender-ISP-Lawyer: (Abmahn-) Anwalt	SYSADMIN: Anwender-ISP SysAdmin – Systemtechniker	POLICE: Anwender-ISP Police: Polizei, Ermittlungsbehörden	TorRelay1: Betreiber eines Tor-Eintritts-Servers	TorRelay2: Betreiber eines Tor-Vermittlungs-Servers	TorRelay3: Betreiber eines Tor-Austritts-Servers	NSA1: Geheimdienste die den Internet-Backbone vor TOR abhören	NSA2: Geheimdienste die den Internet-Backbone nach TOR abhören	ISP: Internet-Service-Provider des Server Betreibers	Lawyer : Server Betreiber-ISP-Lawyer: (Abmahn-) Anwalt	SYSADMIN2: Systemtechniker des Server Betreibers	POLICE: Server Betreiber-ISP Police: Polizei, Ermittlungsbehörden
Ohne HTTPS und ohne TOR	Ziel-Seite, Uid+PW, Daten, Standort	Ziel-Seite, Uid+PW, Daten, Standort	Ziel-Seite, Uid+PW, Daten, Standort	Ziel-Seite, Uid+PW, Daten, Standort	Ziel-Seite, Uid+PW, Daten, Standort	Ziel-Seite, Uid+PW, Daten, Standort	Ziel-Seite, Uid+PW, Daten, Standort	Ziel-Seite, Uid+PW, Daten, Standort	Ziel-Seite, Uid+PW, Daten, Standort	Ziel-Seite, Uid+PW, Daten, Standort	Ziel-Seite, Uid+PW, Daten, Standort	Ziel-Seite, Uid+PW, Daten, Standort	Ziel-Seite, Uid+PW, Daten, Standort	Ziel-Seite, Uid+PW, Daten, Standort
nur mit TOR	Ziel-Seite, Uid+PW, Daten, Standort, TOR	....., ..., ..., Standort, TOR	....., ..., ..., Standort, TOR	....., ..., ..., Standort, TOR	....., ..., ..., Standort, TOR	....., ..., ..., Standort, TOR	....., ..., ..., ..., TOR	Ziel-Seite, Uid+PW, Daten, ..., TOR	....., ..., ..., Standort, TOR	Ziel-Seite, Uid+PW, Daten, ..., TOR	Ziel-Seite, Uid+PW, Daten, ..., TOR	Ziel-Seite, Uid+PW, Daten, ..., TOR	Ziel-Seite, Uid+PW, Daten, ..., TOR	Ziel-Seite, Uid+PW, Daten, ..., TOR
nur mit HTTPS	Ziel-Seite, Uid+PW, Daten, Standort	Ziel-Seite, ..., ..., Standort	Ziel-Seite, ..., ..., Standort	Ziel-Seite, ..., ..., Standort	Ziel-Seite, ..., ..., Standort	Ziel-Seite, ..., ..., Standort	Ziel-Seite, ..., ..., Standort	Ziel-Seite, ..., ..., Standort	Ziel-Seite, ..., ..., Standort	Ziel-Seite, ..., ..., Standort	Ziel-Seite, ..., ..., Standort	Ziel-Seite, Uid+PW, Daten, Standort	Ziel-Seite, Uid+PW, Daten, Standort	Ziel-Seite, Uid+PW, Daten, Standort
HTTPS und TOR	Ziel-Seite, Uid+PW, Daten, Standort, TOR	....., ..., ..., Standort, TOR	....., ..., ..., Standort, TOR	....., ..., ..., Standort, TOR	....., ..., ..., Standort, TOR	....., ..., ..., Standort, TOR	....., ..., ..., ..., TOR	Ziel-Seite, ..., ..., Standort	....., ..., ..., Standort, TOR	Ziel-Seite, ..., ..., ..., TOR	Ziel-Seite, ..., ..., ..., TOR	Ziel-Seite, Uid+PW, Daten, ..., TOR	Ziel-Seite, Uid+PW, Daten, ..., TOR	Ziel-Seite, Uid+PW, Daten, ..., TOR

Wer welche Daten sehen kann, je nach Kombination aus HTTPS und Tor.
(© 2026 Comidio GmbH)

Warum ein einzelner Ansatz nicht ausreicht

Für Einsteiger:

Ein Browser-Plugin schützt den Browser, aber nicht Ihr Smartphone. Ein VPN verbirgt Ihre IP, aber nicht den Fingerabdruck Ihres Browsers. Eine sichere E-Mail-App schützt Ihre E-Mails, aber nicht Ihre IoT-Geräte. Jedes Einzelwerkzeug lässt Angriffslücken offen. Datenschutz, der von dauerhafter persönlicher Konfiguration abhängt, funktioniert im Alltag nicht, das haben zwei Jahrzehnte gescheiterter Datenschutzinitiativen gezeigt.

Fragmentierung als Hauptproblem von Einzellösungen

Das zentrale Problem aller Einzellösungen ist ihre Fragmentierung. Browser-Plugins schützen den Browser. VPN schützt die IP-Adresse. Tor schützt die Anonymität für bestimmte Aktivitäten. Sichere E-Mail-Lösungen schützen die E-Mail-Kommunikation. Sichere Messenger schützen das Chatten. Aber keine dieser Lösungen schützt das gesamte Netzwerk, alle Geräte gleichzeitig, gegen alle drei Angreifer-Gruppen gleichzeitig, ohne erheblichen technischen Aufwand für den Nutzer.

Hinzu kommt das Problem der Konsistenz: Wer zehn verschiedene Datenschutzwerkzeuge konfigurieren und aktuell halten muss, wird irgendwann Fehler machen oder ein Tool vergessen zu aktualisieren. Datenschutz, der von aktivem Nutzerengagement abhängt, ist im Alltag nicht haltbar, das zeigen zwei Jahrzehnte gescheiterter Datenschutzinitiativen. Was gebraucht wird, ist eine integrierte Lösung, die im Hintergrund arbeitet, keine ständige Aufmerksamkeit des Nutzers erfordert und alle Angriffsvektoren gleichzeitig adressiert.

Sichere E-Mail-Kommunikation

Für Einsteiger:

Eine normale E-Mail ist so vertraulich wie eine Postkarte: Jeder Postbote, der sie in den Händen hält, kann sie lesen. Verschlüsselung macht aus der Postkarte einen versiegelten Brief, nur Empfänger und Absender können ihn lesen. TrutzMail erledigt die Verschlüsselung automatisch im Hintergrund: Sie schreiben Ihre E-Mail wie immer, und die TrutzBox kümmert sich um den Rest, ohne technisches Vorwissen.

PGP, S/MIME und das Metadaten-Problem

E-Mail ist das älteste und immer noch meistgenutzte Kommunikationsmedium im Internet, und gleichzeitig eines der unsichersten. Eine normale, unverschlüsselte E-Mail ist in ihrer Vertraulichkeit vergleichbar mit einer Postkarte: Jeder Server, der sie auf dem Weg vom Absender zum Empfänger berührt, kann sie lesen. Die Inhalte werden im Klartext übertragen, die Betreffzeile ebenfalls, und alle Metadaten, wer schreibt wem, wann, von welchem Server aus, wie groß ist die Nachricht, sind für Dritte vollständig einsehbar.

Ende-zu-Ende-Verschlüsselung durch Standards wie PGP (Pretty Good Privacy, entwickelt 1991 von Phil Zimmermann) oder S/MIME (Secure/Multipurpose Internet Mail Extensions) löst das Inhaltsproblem: Nur Sender und Empfänger können den Inhalt lesen, alle Zwischenstationen sehen nur verschlüsselte Daten. Das Metadaten-Problem, wer kommuniziert mit wem und wie oft, bleibt jedoch bestehen. Und die Schlüsselverwaltung ist für technische Laien sehr komplex: Öffentliche Schlüssel müssen ausgetauscht und verifiziert werden, private Schlüssel müssen sicher verwahrt werden.[163]

Verschlüsselung ist nicht dasselbe wie Echtheit. Das zeigte ein Fall vor dem Oberlandesgericht Schleswig-Holstein: Ein Handwerker hatte eine Rechnung über knapp 15.000 Euro per E-Mail verschickt, gesichert allein durch die übliche Transportverschlüsselung, unterwegs wurde die Kontonummer ausgetauscht, der Kunde zahlte an Betrüger. Das Gericht entschied Ende 2024, dass der Handwerker den Betrag nicht noch einmal verlangen kann und wegen des fehlenden Schutzes der Daten haftet. Eine reine Verschlüsselung hätte den Betrug nicht sicher verhindert, denn auch ein Angreifer kann eine Nachricht mit dem öffentlichen Schlüssel des Empfängers verschlüsseln. Erst eine digitale Signatur, die mit dem privaten Schlüssel des Absenders erzeugt wird, macht jede nachträgliche Änderung sichtbar. PGP und S/MIME können beides, Verschlüsseln und Signieren; für S/MIME gibt es kostenlose Zertifikate.[164]

TrutzMail, die E-Mail-Lösung der TrutzBox, löst beide Probleme: Zwischen TrutzBoxen werden Inhalte und Metadaten verschlüsselt, die Schlüsselverwaltung läuft automatisch; zu Standard-Postfächern (Gmail, Outlook) wird PGP genutzt, sofern der Gegenseite ein öffentlicher Schlüssel bekannt ist. Funktionsweise, Schlüsselverwaltung und Grenzen: Kompendium Teil 2, Kapitel „E-Mail (TrutzMail)“.

[163] Zimmermann, P.: Why I Wrote PGP. 1991. https://www.philzimmermann.com/EN/essays/WhyIWrotePGP.html. Zimmermann entwickelte PGP als Reaktion auf das Fehlen einer einfachen Verschlüsselungslösung für politische Aktivisten.

[164] OLG Schleswig-Holstein, Urteil vom 18. Dezember 2024, 12 U 9/24 (Haftung nach Art. 82 DSGVO bei unverschlüsselter Rechnungs-Mail). heise online: Auslegungssache 129, 2025. Sauer, H.: Boxenstopp-Vortrag vom 3. April 2025.

Sichere Chat- und Audio-/Video-Kommunikation (RTC)

Für Einsteiger:

WhatsApp, Zoom und Microsoft Teams sind bequem, aber die Kommunikation läuft dort über zentrale Server der Anbieter, die Nutzungs- und Metadaten gemäß ihren Datenschutzerklärungen verarbeiten. TrutzChat und TrutzMeeting bieten dasselbe: Nachrichten schreiben, Videoanrufe machen, aber vollständig auf Ihrem eigenen Server, ohne fremden Anbieter dazwischen; zu Gästen außerhalb des eigenen Netzes läuft die Verbindung naturgemäß über das Internet. Bei TrutzMeeting genügt Gästen ohne TrutzBox ein normaler Browser und ein Link, keine App-Installation, kein Account.

XMPP, Jitsi und selbst betriebene Kommunikationsdienste

Messaging-Dienste wie WhatsApp oder Telegram bieten Ende-zu-Ende-Verschlüsselung für Inhalte, die Metadaten werden dennoch gesammelt. Signal gilt als sicherster kommerzieller Messenger, weil das Signal-Protokoll auch die Metadaten minimiert und der Quellcode öffentlich überprüfbar ist. Dennoch läuft Signal auf den Servern der Signal Foundation in den USA und unterliegt damit dem US-Recht. Signal und WhatsApp setzen zudem die Telefonnummer als Kennung voraus, mit den im Kapitel „Die Mobilfunknummer als Generalschlüssel“ beschriebenen Folgen; Threema und selbst betriebene XMPP-Dienste kommen ohne Nummer aus.

XMPP (Extensible Messaging and Presence Protocol) ist ein offener Standard für sichere Kommunikation, der auf einem eigenen Server betrieben werden kann. Auf eigenem Server betrieben bietet XMPP den höchsten Datenschutz für Messaging: kein zentraler Dienstanbieter, keine Metadaten-Sammlung, volle Kontrolle durch den Nutzer. TrutzChat, der XMPP-basierte Messaging-Dienst der TrutzBox, verschlüsselt Nachrichten mit den TrutzMail-Schlüsseln der Teilnehmer und leitet sie zwischen TrutzBoxen über Tor-Hidden-Services; Inhalte und Metadaten bleiben damit gleichermaßen geschützt. Einrichtung und Nutzung: Kompendium Teil 2, Kapitel „Videokonferenz und Chat (TrutzRTC)“.

TrutzMeeting, der integrierte Videokonferenzserver, basiert auf Jitsi Meet, einer in Europa verbreiteten, vollständig quelloffenen Videokonferenzlösung. Im Unterschied zu Zoom, Teams oder Google Meet läuft die Konferenz vollständig auf der TrutzBox des Gastgebers; externe Teilnehmer brauchen nur einen Browser und einen Link. Leistungsgrenzen und Einrichtung: Kompendium Teil 2, Kapitel „Videokonferenz und Chat (TrutzRTC)“.

Was ist eine Privacy-Box?

Für Einsteiger:

Eine Privacy-Box ist ein kleines Gerät, das zwischen Ihrem Internetrouter und Ihren Geräten sitzt und den gesamten Netzwerkverkehr kontrolliert. Stellen Sie sich vor: Statt dass jedes Gerät im Haus einzeln geschützt werden muss, läuft alles, ob PC, Smartphone, Smart-TV, Spielkonsole oder Thermostat, über einen gemeinsamen Schutzfilter. Tracker werden blockiert, E-Mails verschlüsselt, Videokonferenzen gesichert, vollautomatisch, ohne technisches Vorwissen des Nutzers.

🔧 Konzept, Hardware und Betriebsmodi der TrutzBox

Eine Privacy-Box ist ein elektronisches Gerät in Form einer Hardware-Software-Kombination, das größtmögliche Privatheit bei der Nutzung des Internets bieten soll. Diese Definition, die das Comidio-Team vor der Entwicklung der TrutzBox erarbeitet hat, formuliert klare Anforderungen: Eine Privacy-Box soll Privatheit bei möglichst allen Tätigkeiten im Internet ermöglichen, beim Mailen, Surfen (Browsen), Chatten und bei Video-Audio-Konferenzen. Sie soll ohne tiefgehende Fachkenntnisse bedienbar sein und alle im Netzwerk befindlichen Geräte gleichzeitig schützen.[165]

Im Unterschied zu gerätespezifischen Einzellösungen, die auch nur ein bestimmtes Sicherheitsbedürfnis erfüllen können, integriert die TrutzBox mehrere Sicherheitslösungen und zusätzlich Kommunikationsanwendungen in einer Box. Die TrutzBox überwacht ein- und ausgehenden Datenverkehr und schützt damit alle Netzwerkteilnehmer und internetfähigen Geräte, unabhängig davon, ob es sich um PCs, Smartphones, Smart-TVs oder IoT-Geräte handelt.

Die Hardware der TrutzBox ist ein kompakter PC im Formfaktor eines kleinen Routers, der als Netzwerkgerät im Heimnetzwerk oder Firmennetzwerk platziert wird. Die Rechenleistung ist bewusst ausreichend dimensioniert, um alle TrutzBox-Funktionen in Echtzeit auf dem gesamten Netzwerkdurchsatz auszuführen, in typischen Heim- und Büronetzen ohne spürbare Beeinträchtigung der Internetgeschwindigkeit.

Die Module der TrutzBox im Überblick

Was die einzelnen Module leisten, wie sie eingestellt werden und wo ihre Grenzen liegen, beschreibt Kompendium Teil 2 (Funktionen und Architektur). Hier nur der Überblick:

- TrutzBrowse: anonymisiert als Proxy die zwischen Gerät und Internet ausgetauschten Daten; die Stärke bestimmt der Security-Slider, die Einstellung gilt auch für alle im Hintergrund kontaktierten Drittserver; braucht das TrutzBox-Zertifikat auf dem Gerät. Kompendium Teil 2, Kapitel „TrutzBrowse“.
- TrutzContent: Zugangskontrolle je Gerät und Nutzer über Filtergruppen (Kinder, Erwachsene, IoT), für den Nutzer nicht ohne Weiteres umgehbar und nur vom Administrator änderbar. Kompendium Teil 2, Kapitel „TrutzContent“.
- TrutzBase: Firewall, Angriffserkennung und Angriffsschutz mit IP-Sperrlisten, Schutz vor DNS-Umgehung, VPN-Server für unterwegs. Kompendium Teil 2, Kapitel „Mehrschichtiger Netzwerk-Schutz (TrutzBase)“ und „Netzwerk“.
- TrutzMail: automatisch verschlüsselte E-Mail zwischen TrutzBoxen, PGP zu Standard-Postfächern. Kompendium Teil 2, Kapitel „E-Mail (TrutzMail)“.
- TrutzChat und TrutzMeeting: Chat und Videokonferenz auf der eigenen Box, ohne fremde Server. Kompendium Teil 2, Kapitel „Videokonferenz und Chat (TrutzRTC)“.
- Monitor: macht jede Verbindung jedes Geräts sichtbar, mit Herkunft, Betreiber, Land und Sperre per Klick. Kompendium Teil 2, Kapitel „Monitor“.
- Betriebsmodi: Proxy-Modus (nur ausgewählte Geräte, zum Ausprobieren) oder Gateway-Modus (alle Geräte automatisch, für vollen Schutz empfohlen). Kompendium Teil 2, Kapitel „TrutzBox Setup“.

[165] Comidio GmbH: Definition Privacy-Box. https://trutzbox.de/2017/10/was-ist-eine-privacy-box/

TrutzBox: Technische Dokumentationsfunktionen

Der Monitor protokolliert alle ausgehenden Verbindungen mit Zeitstempel, Ziel, Betreiber und Datenmenge und liefert damit maschinenlesbare Belege für Audits und interne Dokumentation (Kompendium Teil 2, Kapitel „Monitor“). Hinweis: Ob und inwieweit der Einsatz der TrutzBox spezifische datenschutzrechtliche Anforderungen erfüllt, ist im Einzelfall mit dem zuständigen Datenschutzbeauftragten oder einer spezialisierten Rechtsberatung zu klären.

Für weiterführende Informationen zum Thema Internet-Sicherheit und Datenschutz empfiehlt sich ein Blick in das Privacy-Handbuch (privacy-handbuch.de), Security in a Box (securityinabox.org) oder das Cryptoparty-Handbook. Funktionen, Einstellungen und Architektur der TrutzBox beschreibt Kompendium Teil 2; das TrutzBox-Handbuch unter wiki.trutzbox.de bietet Schritt-für-Schritt-Anleitungen für Einrichtung und Betrieb.

Stichwortverzeichnis

Alle Einträge sind direkt mit dem jeweiligen Abschnitt im Dokument verlinkt. Klicken Sie auf einen Begriff, um direkt dorthin zu springen.

E

F

G

I

K

M

N

O

P

R

S

T

U

V

W

X

Z