Unterwegs in den Sozialen Medien: Über Risiken und Nebenwirkungen

Die Nutzung der Dienste und Plattformen der Sozialen Medien macht Spaß und ermöglicht einen regen Gedanken- und Informationsaustausch unter Freunden, Bekannten wie auch mit Unbekannten. Doch damit verbinden sich ein paar ernst zu nehmende Risiken, die Du genau kennen solltest. Um diese geht es hier.

Wir beginnen mit einer Frage zu deinen **persönlichen Daten**:

Wie gehen die Plattformbetreiber (zum Beispiel: Instagram, TikTok) und Dienste-Anbieter (wie WhatsApp) mit ihnen um? Was denkst Du: Welche der in unserer Übersicht (Abschnitt 1.2) gezeigten Medien speichern folgende Daten von Dir:

1. deinen Benutzernamen zw. Deinen echten Namen (falls angegeben);
2. den Aufnahmestandort deines Fotos;
3. Informationen zum verwendeten Gerät, also z.B. das Betriebssystem, die Signalstärke, der verfügbare Speicherplatz, der Browsertyp, die App- und Dateinamen;
4. Informationen über deine Mausbewegungen, die ID deines Smartphones, die WLAN-Zugangspunkte und die Funkzellentürme in deiner Nähe;
5. Daten über deine Aktivitäten auf deinem Handy, also Ort, Uhrzeit, Objekt und Häufigkeit deiner Klicks (oder Wischen), die Dauer deiner Aktivität auf jeder App.
6. Die Inhalte deiner Aktivitäten, also deine Kommentare, Likes und Shares.
7. Daten auf deinem Handy, die gar nichts mit dem Medium zu tun haben, welches Du gerade nutzt (zum Beispiel dein Adressbuch mit allen Telefonnummern; andere Apps auf deinem Handy und solche Dinge).
8. Die auf deinem Handy gespeicherten Bilder, Fotos, Videos.

Hier die Antwort: Diese drei greifen die meisten Daten von Dir:

1. Instagram holt am meisten Daten (Punkte 1-5, 8)

2. Facebook ist ebenso datengierig (Punkte 1, 3, 4-7).

3. WhatsApp sammelt viele Informationen, die auf deinem Handy liegen (1, 2, 4, 7).

Du bezahlst mit deinen persönlichen Daten

Hinter diesem Datenhunger steckt der Mutterkonzern der drei Dienste, dem Medienkonzern Meta Platforms Inc. mit Sitz in Menlo Park, Kalifornien (bis 2021 unter dem Namen Facebook Inc.; Hauptaktionär Mark Zuckerberg). Die individuellen Nutzerdaten werden analysiert und zu sogenannten Nutzerprofilen verdichtet. Über jede Person, die WhatsApp oder Facebook oder Instagram nutzt, besitzt Meta ein Datenprofil. Falls Du eines oder mehrere dieser Dienste gebrauchst, kennt Meta dein persönliches Nutzerverhalten und auch die Daten deiner Online-Freund:innen.

Meta kennt zudem deine mutmaßlichen Vorlieben (zum Beispiel Klamotten), deine Interessen (zum Beispiel Frauenfußball) und deine Wünsche und Bedürfnisse (zum Beispiel ein neuer Rucksack der Marke XXX, die neue Musikaufnahme der Gruppe XXX, die Landschaft bei Görlitz, das Getränk Fritz-Cola und anderes mehr).

Deinem Profil entsprechend werden Dir vor allem Werbeanzeigen gezeigt, von denen die Anbieter meinen, dass Dich just diese Angebote speziell interessieren (und Du darum vermutlich mehr bestellst und kaufst).

Dieses „Profiling“ ist für Deine Freizeit- und Konsumwünsche nicht schlimm, manchmal sogar ganz praktisch.

Zum Problem wird diese Vorauswahl, wenn es um Informationen über Ereignisse und Vorgänge in der Welt geht. Wenn Du beispielsweise Nachrichten vor allem über irgendwelche Promis, über spanische Eisenbahnen und über Bergsteigerunfälle siehst – und kaum etwas über wichtige Vorgänge in Südamerika oder Taiwan oder der Türkei. Die Nachrichten-Vorauswahl führt zu sogenannten Filterblasen (filterbubble): Die News-Anbieter auf den Plattformen zeigen Dir bevorzugt das, was Du schon kennst. Über viele andere Ereignisse, die wichtig sein könnten, erfährst Du wenig oder nichts.

Bist Du vor Datendiebstahl durch Online-Anbieter geschützt?

Die meisten kommerziellen Unternehmen wollen deine Nutzungsdaten nicht nur für die Werbewirtschaft. Sie verwerten sie auch für andere Zwecke, zum Beispiel, um die eigenen Dienste zu verbessern, um ihre Inhalte attraktiver zu machen oder um andere Angebote und Netzwerke zu entwickeln oder zu optimieren. Manche Online-Unternehmen verkaufen diese Daten auch weiter – oder sie werden von Cyber-gangs gestohlen, wie es zum Beispiel mit Facebook-Daten wiederholt geschah.

Immerhin, seit Mai 2018 müssen sie Dich darüber informieren. Denn seither gilt für alle Staaten der EU die *Datenschutz-Grundverordnung (DSGVO).* Sie sorgt dafür, dass die Internet-Unternehmen offenlegen, was sie mit den Daten ihrer Nutzer machen. Nach Artikel 30 der DSGVO müssen sie ein Verzeichnis führen, aus dem ersichtlich ist, welche personenbezogenen Daten sie verarbeiten. Außerdem müssen sie von ihren Nutzern die Zustimmung einholen, dass sie mit der Ermittlung und Speicherung ihrer Daten einverstanden sind. Deshalb fragen dich die Anbieter, wenn Du deren App oder Webseite aufrufst, ob sie Cookies auf

deinem Gerät platzieren können, und wenn ja: welche es sein dürfen. Auf vielen Apps kannst du durch Anklicken einer Liste mitentscheiden, welche Daten erfasst werden dürfen. Diese Cookies sind winzige Programme, die deine Aktionen registrieren und dem Anbieter der App übermitteln. Unternehmen, die sich nicht daran halten, können zu hohen Geldtrafen verurteilt werden.

Dank dieser Vorschrift ist vielen Menschen inzwischen klar, dass sie für die kostenfreie Nutzung kommerzieller Online-Dienste ihr Nutzungsverhalten offenlegen müssen, also quasi mit ihren persönlichen Daten bezahlen.

Seitdem es diese Regelung gibt, scheint die große Mehrheit mit der Speicherung ihrer Daten einverstanden zu sein. Eine im Dezember 2021 durchgeführte Erhebung des Deutschen Dialogmarketing Verbands (DDV) ergab, dass rund 90 Prozent der Jugendlichen mit der Datenerfassung und -weitergabe keine Probleme haben. Offenbar ist ihnen die kostenfreie Nutzung der Onlinedienste lieber (Quelle: DDV-Datenschutz-Report 2022).

Ausnahmen

Es gibt noch immer Dienste unter den Sozialen Medien, die grundsätzlich keine Daten erheben. Dazu zählen in erster Linie solche Anbieter, die sich nicht über Werbung finanzieren und nicht im kommerziellen Wettbewerb stehen. Sie benötigen kein „Profiling“, d. h. ihre Angebote werden nicht auf die Nutzer angepasst und erzeugen auch keine Filterblasen.

Diese Daten-Neutralität trifft auf die meisten Wikis zu (zur Definition siehe Kachel-Text zu Wiki auf der Schautafel 1.2) – zum Beispiel auf das Online-Lexikon **Wikipedia**, das über Spenden und Fördermittel finanziert wird (Näheres siehe Text „Wikipedia“). Für die Betreiber dieser Plattform zählt allein die gemeinschaftliche Erarbeitung von Sachbeiträgen.

Der Datenschutz wird ausgebaut

Übrigens trat im Dezember 2021 ein neues EU-Gesetz in Kraft, das die Datenschutz- und Verbraucherrechte stärken und dem „Cookie-Wahnsinn ein Ende bereiten“ soll (so die Tagesschau am 01.12.2021). Anstelle der Cookies wird es ein sogenanntes Personal Information Management Services (PIMS) geben. Allerdings wird es noch ein paar Jahre brauchen, ehe in Deutschland die erforderlichen Rechtsbestimmungen in Kraft treten werden. Dann werden die Nutzerinnen und Nutzer mit Hilfe des PIMS selbst festlegen, welche Daten sie generell freigeben und welche nicht. Diese Entscheidung ist dann für alle Medienanbieter verbindlich. (Mehr hierzu: https://www.tagesschau.de/inland/neues-telemediengesetz-cookies-101.html)

MH/07-11-2022