L Erweiterung

Persönliche Daten und Selbstdatenschutz

Preisgabe von Daten

Social-Media-Angebote geben ihren Nutzerinnen und Nutzern die Möglichkeit der Selbstdarstellung, des Austauschs und der Vernetzung mit anderen. Wer die Angebote nutzen möchte, gibt persönliche Daten preis. Bereits bei der Anmeldung werden viele Daten abgefragt. Auch werden Nutzerinnen und Nutzer häufig von den Social-Media-Angeboten aufgefordert, in ihrem Profil weitere Daten über sich preiszugeben, z. B. durch Meldungen wie „erst 40 % des Profils sind ausgefüllt, mach heute weiter" oder „du hast schon länger keine Inhalte geteilt – erzähle anderen, was dich beschäftigt". Zugunsten einer umfassenden Selbstdarstellung werden online oft persönliche Daten preisgegeben, die man in einem persönlichen Gespräch oder einer anderen Alltagssituation eher vertraulich behandeln würde, wie Beziehungsstatus, Geschlechterzuordnung, sexuelle oder politische Orientierung oder Religionszugehörigkeit.

Spannungsfeld

Gerade für Kinder und Jugendliche ist es eine Herausforderung, ihr Bedürfnis nach Selbstdarstellung und den Schutz der eigenen Privatsphäre unter einen Hut zu bringen. Welche Nachteile für sie entstehen können, wenn Fremde auf ihre Daten Zugriff haben, ist ihnen oft nicht bewusst.

Rückschlüsse auf reale Person

Persönliche oder personenbezogene Daten sind sensible Daten, die Rückschlüsse auf die reale Person zulassen. Zu personenbezogenen Daten gehören Name, Geburtsdatum, Wohnort, Adresse, Telefonnummer, E-Mail-Adresse, das Alter, aber auch Hobbys und Vorlieben einer Person. Bestimmte Apps und Social-Media-Angebote greifen zudem auf GPS-Daten zu und können so den Aufenthaltsort nachvollziehbar machen sowie umfangreiche Bewegungsprofile erstellen. Gerade die Kombination verschiedener persönlicher Daten macht es Dritten möglich, Rückschlüsse auf die Verhaltensweisen und Vorlieben einer Person zu ziehen.

Datensammler

Personenbezogene Daten sind wie Gold für die Betreiber von Social-Media-Angeboten. Marktdatenhändler, Internet-Tracking-Unternehmen und die Werbewirtschaft freuen sich über so wertvolle Daten, die einzelne Nutzerinnen und Nutzer mit ihren Wohnorten, Hobbys, Nutzungsgewohnheiten etc. identifizierbar machen. Kein Wunder, dass es ein lukratives Geschäft ist, diese Daten an Dritte weiterzuverkaufen. Es lohnt, wie so oft, ein genauer Blick in die Datenschutzerklärung und in die Allgemeinen Geschäftsbedingungen. Besonders in der Kritik sind hier die Anbieter vieler Apps von Spielen und Social-Media-Angeboten. Hier müssen Nutzerinnen und Nutzer oft in die Weitergabe ihrer Daten einwilligen, wollen sie die Anwendung nutzen.

Stiftung Medienpädagogik Bayern
Digitale Schule der Zukunft

Datenmissbrauch

Daten können durch Dritte missbraucht werden. Sind beispielsweise an einem Profil keine oder kaum Privatsphäre-Einstellungen vorgenommen worden und persönliche Informationen öffentlich einsehbar, können dort angegebene Daten leicht missbraucht werden. Doch auch mit den richtigen Privatsphäre-Einstellungen können Daten gestohlen werden. Denn ohne dass Nutzerinnen und Nutzer Einfluss darauf haben, können Hacker sich z. B. durch Sicherheitslücken der Plattform Zugriff auf die Daten verschaffen.

Identitätsdiebstahl

Eine besondere Form des Datenmissbrauchs ist der Identitätsdiebstahl: Hier gibt sich eine Person als eine andere aus. Dazu wird beispielsweise ein gefälschtes Nutzerkonto (Fake-Profil) erstellt. Ziel ist es, der anderen Person zu schaden. So können über das Fake-Profil rufschädigende Nachrichten oder Bilder veröffentlicht werden. Werden andere Nutzerinnen und Nutzer von einem Fake-Profil aus kontaktiert, erkennen sie den Unterschied zum echten Profil häufig nicht: Es kann passieren, dass sie bei Kontaktaufnahmen der Person hinter dem Fake-Profil ebenfalls persönliche Informationen von sich preisgeben. Durch Identitätsdiebstahl kann auch ein wirtschaftlicher Schaden entstehen, z. B. wenn Bezahl- und Kontodaten missbraucht werden. Aber auch Name und Adresse des Opfers reichen oftmals aus, um Bestellungen bei Online-Versanddienstleistern im Namen des Opfers zu tätigen.

Unüberschaubare Verbreitung

Persönliche Daten können sich unüberschaubar verbreiten. Sind persönliche Daten einmal online, kann man sie nicht mehr zurückholen: Das Internet vergisst nichts und andere Nutzerinnen und Nutzer wie beispielsweise Lehrkräfte, zukünftige Arbeitgeberinnen und Arbeitgeber oder neue Partnerinnen und Partner können diese Daten auch Jahre später noch abrufen.

Selbstdatenschutz

Kindern und Jugendlichen sollte deshalb bewusstgemacht werden, bei allen Online-Aktivitäten die Preisgabe ihrer Daten und den Schutz ihrer Privatsphäre im Blick zu behalten. Die folgenden Regeln zum Selbstdatenschutz können dabei helfen:

Datensparsamkeit

Mit persönlichen Daten wie Nachname, Adresse, Geburtsdatum und Telefonnummern sollte man sparsam umgehen und – wenn möglich – verschiedene Pseudonyme verwenden. Bei Minderjährigen sollten personenbezogene und persönliche Daten niemals ohne Rücksprache mit einem Erziehungsberechtigten herausgegeben werden. Fragt ein Angebot zu viele dieser Daten ab, sollte man überlegen, ob dessen Nutzung wirklich notwendig ist. Manchmal finden sich zu bestimmten Angeboten auch datensparsame Alternativen. Ganz allgemein gilt bei der Preisgabe der eigenen Daten die Faustregel: Weniger ist mehr. Daten, die nicht online stehen, können nicht so leicht missbraucht werden.

Privatsphäre-Einstellungen

Privatsphäre-Einstellungen sollten vorgenommen und regelmäßig überprüft werden. Social-Media-Angebote wie Instagram, Snapchat oder Facebook bieten die Möglichkeit, Privatsphäre-Einstellungen vorzunehmen, die über die Grundeinstellung bei der Anmeldung bzw. Installation hinausgehen. Eine der wichtigsten Funktionen in Social-Media-Angeboten ist die Möglichkeit, seine Daten vor der Öffentlichkeit zu verbergen und nur einem ausgewählten Publikum (den „Freunden“) sichtbar zu machen. Zwar bieten die Privatsphäre-Einstellungen keinen 100-prozentigen Schutz vor Missbrauch der Daten, doch das Risiko wird ein wenig eingedämmt. Wichtig ist, die Einstellungen immer wieder zu überprüfen und bei Bedarf neu anzupassen. Denn häufig werden Privatsphäre-Voreinstellungen bei der Weiterentwicklung eines Dienstes verändert, die Nutzerinnen und Nutzer aber nicht um ihre Einwilligung gebeten. So kann es passieren, dass Nutzerinnen und Nutzer Daten preisgeben ohne es zu merken. Je jünger die Nutzerinnen und Nutzer sind, desto strenger sollten die Privatsphäre-Einstellungen sein und regelmäßig kontrolliert werden.

Einschränkung von Zugriffsrechten

Zugriffsrechte von Apps können je nach Betriebssystem auch nach der Installation eingeschränkt werden, beispielsweise das Taggen von Fotos mit GPS-Daten. Generell ist es sinnvoll, vor der Installation zu prüfen, auf welche Daten eine App zugreift und ob sie diese Zugriffsrechte wirklich benötigt. Gegebenenfalls können diese deaktiviert werden. Allerdings können nicht bei allen Apps die Zugriffsrechte vor beziehungsweise nach der Installation manuell eingeschränkt werden, da die Apps sonst nicht genutzt werden können. Nutzerinnen und Nutzer sollten dann eine alternative App mit weniger Zugriffsrechten wählen.

Exkurs: DSGVO und Minderjährige

Um den Datenschutz von Personen gegenüber kommerziellen Interessen von Unternehmen zu stärken, gibt es seit Mai 2018 mit der Datenschutzgrundverordnung (DSGVO) europaweite Regelungen. Unternehmen ist es grundsätzlich untersagt, personenbezogene Daten ohne Einwilligung einer Person zu verarbeiten. Für die Daten von Kindern formuliert die DSGVO besondere Anforderungen. Bei Internetangeboten genügt eine Einwilligung von Minderjährigen unter 16 Jahren in die Datenverarbeitung nicht. Auch die Erziehungsberechtigten müssen zusätzlich einwilligen. [1] In der Praxis findet eine tatsächliche Überprüfung, ob Erziehungsberechtigte mit der Anmeldung in einem Social-Media-Angebot einverstanden sind, jedoch meist nicht statt. Bei Anmeldung muss lediglich ein Haken gesetzt oder es kann ein falsches Alter angegeben werden.

Quellenangaben

[1] Bayerische Landeszentrale für neue Medien (BLM) (Hrsg.) (2019): Recht am eigenen Bild. Tipps, Tricks und Klicks. Internet: **www.blm.de/aktivitaeten/medienkompetenz/materialien/recht_am_eigenen_bild.cfm** [Stand: 25.04.2022]

Der Text ist Bestandteil der bereits bestehenden Unterrichtseinheit „Liken, posten, teilen“ des Medienführerscheins Bayern für den Bereich der sonderpädagogischen Förderung. Die Unterrichtseinheit ist verfügbar unter: **www.medienfuehrerschein.bayern**. Die Entwicklung wurde gefördert durch die Bayerische Staatskanzlei.