Zeitschrift: SuchtMagazin
Herausgeber: Infodrog
Band: 37 (2011)
Heft: 6

Artikel: Datenschutz bei sozialen Netzwerken
Autor: Meier, Francis
DOI: https://doi.org/10.5169/seals-800316

Datenschutz bei Sozialen Netzwerken

Soziale Netzwerksites SNS bilden heutzutage einen festen Bestandteil im Leben vieler Menschen. Allein in der Schweiz verfügen mehrere Millionen User und Userinnen über ein Profil bei Facebook, LinkedIn und Co., in dem sie Persönliches über sich und Dritte ausbreiten. Allerdings birgt die Nutzung dieser Plattformen zahlreiche Risiken. ExpertInnen raten denn auch, Personendaten wie Bilder, Meinungen oder Adressen nur mit Zurückhaltung preiszugeben.

Francis Meier
wissenschaftlicher Mitarbeiter des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten, Feldeggweg 1, CH-3003 Bern, info@edoeb.admin.ch

Dass viele NutzerInnen die Ratschläge zum sicheren Umgang mit Internetplattformen durchaus ernst nehmen, zeigt eine kürzlich in Deutschland durchgeführte Umfrage zum Schutz der Privatsphäre im Internet. Laut der Studie machen sich immerhin zwei Drittel der Internetnutzenden Gedanken darüber, welche Daten sie im Internet preisgeben.[1] Und vier von fünf halten den Schutz der Privatsphäre bei Facebook und anderen Sozialen Netzwerken für ungenügend.

Tatsächlich sind diese Plattformen aus Datenschutzsicht in vielerlei Hinsicht problematisch. So können etwa einmal hochgeladene Daten von anderen UserInnen heruntergeladen und gespeichert werden, was die Löschung des Ursprungsprofils quasi nutzlos macht, bleiben so die Daten doch erhalten. Zudem können sie mit Bildern, Angaben, Äusserungen aus anderen On- und Offline-Quellen verknüpft werden. So entsteht eine Unzahl von privaten Datensammlungen, und die Gefahr wächst, dass die Daten anders eingesetzt werden, als von den UserInnen ursprünglich beabsichtigt.

Zahlreiche Risiken

Da die Registrationshürden der meisten Netzwerke sehr niedrig sind, ist es unter Vorspiegelung falscher Tatsachen oder gar Annahme einer falschen Identität einfach, als «Freund» akzeptiert zu werden und in Besitz von Informationen zu gelangen, die einem das Gegenüber in einem Gespräch von Angesicht zu Angesicht vielleicht nicht mitteilen würde. Das birgt Gefahren der Infiltration dieser Communities zu verschiedenen negativen Zwecken wie Spamming (Massenwerbung) oder Phishing (bsw. um Zugangsdaten zu wichtigen Accounts oder Bankinformationen zu ergattern).

Auch Identitätsdiebstahl kann zum Thema werden: Ein Übeltäter legt sich ein Profil mit dem Namen einer bekannten Person an und profitiert von deren Berühmtheit – oder schädigt ihren Ruf durch bösartiges Verhalten. Gleichermassen kann man ein Profil im Namen einer Person aus Schule oder Nachbarschaft eröffnen und ihr schaden, indem man sie lächerlich macht oder in ihrem Namen Gemeinheiten verschickt. Oder man versteckt sich hinter einem gefälschten Profil und nutzt dabei die Möglichkeiten der SNS, um jemanden zu belästigen oder zu demütigen (Cybermobbing).

Ausserdem kann die Menge an Daten, die die Benutzerinnen und Benutzer über sich selber bekannt geben, durchaus dazu führen, dass ein Stalker die Adresse seines Opfers herausfindet, dessen Lebensgewohnheiten kennen lernt und die Person physisch verfolgen kann.

Das Geschäft mit den Userdaten

Auch wenn SNS ihre Dienste meistens gratis anbieten, handelt es sich nicht um gemeinnützige Einrichtungen. Es findet ein «Handel» statt: Dienstleistungen für Benutzerinnen und Benutzer im Tausch gegen deren Daten. Hinter den Portalen steckt eine geballte Marktmacht, stehen führende internationale Unternehmen, die unter dem Druck von Investoren und Aktionären wachsende Profite generieren müssen. Das einzige, was ein Social Networking Service anzubieten hat, sind Personendaten – und der Börsenwert eines SNS – Facebook wird auf 70 Milliarden Dollar geschätzt – spricht Bände über deren Wert.

Die SNS-Anbieter haben nicht nur Zugriff auf die Personendaten, sondern auch auf die Metadaten (Verbindungsdauer, grobe geografische Herkunft der IP-Adresse, Verweildauer und Bewegungen auf der Site, etc.).

Bei vielen Anbietern ist unklar, was mit all diesen Daten geschieht. Klar ist hingegen, dass Personen- und Metadaten zusammen ausführliche Persönlichkeitsprofile ergeben können, die Aufschluss liefern über unsere Vorlieben, Hobbies, Meinungen oder unser Konsumverhalten. Diese Profile sind für die Werbebranche wertvoll, da sie es ihr ermöglichen, Onlinewerbung auf die Bedürfnisse der einzelnen UserInnen abzustimmen. Die kommerzielle Verwertung der Userdaten ist für Unternehmen wie Google und Facebook ein äusserst lukratives Geschäft, auf dem ihr Geschäftsmodell basiert.

Gesichtserkennung und Like-Button

Entsprechend suchen sie laufend nach neuen Wegen, um an neue Userdaten zu gelangen. Ein Beispiel dafür ist die automatische Gesichtserkennung, die Facebook in diesem Jahr eingeführt hat. Fotos, die einE NutzerIn hochlädt, werden automatisch gescannt und mit dem dazugehörenden Namen gespeichert. Die UserInnen werden auf Personen aus dem Bekanntenkreis hingewiesen, die sich auf den Bildern befinden und aufgefordert, diese zu kennzeichnen (taggen). So entsteht bei Facebook eine riesige Datenbank zur Gesichtserkennung. Heikel daran ist unter anderem, dass sich Personen, die über kein Facebook-Profil verfügen, nicht gegen das Tagging aussprechen können. Zudem ist das Widerspruchsverfahren für Facebook-NutzerInnen umständlich.

Im September 2011 präsentierte Mark Zuckerberg, der Gründer von Facebook, der Öffentlichkeit die neuesten Erweiterungen der Plattform, etwa die Einführung einer Timeline (Zeitleiste) oder die Möglichkeit, Musik, Filme und andere Inhalte mit seinen Freunden

zu teilen (Instant Sharing). Da das Teilen automatisch erfolgt, stellt sich die Frage, inwiefern sich die UserInnen dessen noch bewusst sind. Kritiker sehen im Instant Sharing einen «Euphemismus für die totale heimliche Überwachung».[2]
Auch der Like-Button mit dem nach oben zeigenden Daumen liefert dem Konzern nützliche Informationen. So werden Daten, welche die NutzerInnen beim Surfen auf Webseiten hinterlassen, in die der Button eingebunden ist, von Facebook gesammelt und ausgewertet. Betroffen davon sind auch Personen, die nicht beim sozialen Netzwerk registriert sind.

Was passiert mit den Userdaten?

Ein Vorwurf der im Zusammenhang mit Sozialen Netzwerken häufig fällt, ist jener der mangelnden Transparenz. Die Datenschutzerklärungen und Allgemeinen Geschäftsbedingungen äussern sich meist nur knapp oder gar nicht dazu, welche Nutzerdaten erhoben, wo sie gespeichert, zu welchen Zwecken sie bearbeitet werden und wer alles darauf zugreift. Auch änderten manche die Bedingungen im Nachhinein heimlich ab. Hinzu kommt, dass sich die Plattformen sehr weitgehende Freiheiten bezüglich Bearbeitung, Auswertung und Weitergabe der Daten an Dritte einräumen. Bei Kritik an ihrer Datenschutzpolitik verweisen die Anbieter gerne auf die Privatsphäre-Einstellungen, anhand derer jedeR NutzerIn selbst entscheiden könne, welche Daten sie oder er preisgeben möchte. Allerdings sind etwa bei Facebook die Standardeinstellungen so gewählt, dass die UserInnen einem breiten Personenkreis Zugang zu persönlichen Informationen gewähren. Mitglieder, die mehr Privatsphäre wünschen, müssen von sich aus tätig werden. Vorausgesetzt sie finden sich in den teils unübersichtlich gestalteten Einstellungen zurecht.

Rechtliche Vorgaben

Diese Aspekte sind auch aus rechtlicher Perspektive problematisch. Denn nach Schweizerischem Datenschutzgesetz muss, wer Daten bearbeitet, die betroffenen Personen, in diesem Fall vor allem die SNS-NutzerInnen, im Voraus klar und ausreichend über die Einzelheiten der Datenbearbeitung aufklären. Auch dürfen die Daten der UserInnen grundsätzlich nur mit ihrer Einwilligung gesammelt und weitergegeben werden. Opfer von Datenschutzverletzungen könnten ihre Persönlichkeitsrechte zwar per Klage geltend machen. Allerdings ist ein rechtliches Vorgehen gegen weltweit tätige Unternehmen wie Facebook äusserst schwerfällig, insbesondere dann, wenn sie über keine Zweigstelle in der Schweiz verfügen.
Dennoch haben kürzlich ein paar österreichische StudentInnen, die sich an der Datenschutzpraxis von Facebook störten, Beschwerde gegen das Netzwerk eingereicht; in Irland, wo der Konzern sein internationales Hauptquartier hat. In der Folge kündigte der irische Datenschutzbeauftragte eine vertiefte Abklärung der Datenbearbeitung Facebooks an. Man darf auf das Ergebnis der Untersuchung gespannt sein, denn sollte das Unternehmen zu einer Verbesserung des Datenschutzes gezwungen werden, würden davon auch Schweizer UserInnen profitieren. Facebook hat dies dem Schweizerischen Datenschutz- und Öffentlichkeitsbeauftragten ausdrücklich zugesichert.

Die Verantwortung der NutzerInnen

Die Kritik an den Betreibern von SNS ändert jedoch nichts an der Tatsache, dass die UserInnen Mitverantwortung für den Schutz ihrer Privatsphäre tragen. Sie sollten sich vor Augen führen, dass die von ihnen preisgegebenen persönlichen Informationen Geld wert sind; und abwägen, ob es das Angebot wert ist, Persönliches ins Internet zu stellen. Selbstverantwortung wahrnehmen heisst, vor allem das Kleingedruckte lesen und sich vergewissern, welche Informationen man wirklich freigeben will – im Bewusstsein, dass damit sehr detaillierte Persönlichkeitsprofile kreiert werden können. Die NutzerInnen müssen auch wissen, dass sie keine Informationen über Freunde und Bekannte – wie Fotos von Familienfesten oder Betriebsausflügen – ohne deren Einwilligung hochladen dürfen.

Tipps zur sicheren Nutzung sozialer Netzwerke

Hilfreiche Hinweise und Tipps für einen verantwortungsvollen Umgang mit Personendaten in sozialen Netzwerken gibt es zur Genüge. Entsprechende Informationen und Links finden Interessierte auf der Website des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten unter www.derbeauftragte.ch. Nachfolgend ein paar der wichtigsten Regeln:

- Seien Sie vorsichtig bei der Veröffentlichung Ihrer Personendaten (Name, Adresse, Telefonnummer) und anderer persönlicher Informationen (bspw. politische Überzeugungen) auf einer SNS. Benutzen Sie Pseudonyme.
- Achten Sie darauf, wen Sie in Ihren virtuellen Freundeskreis aufnehmen. So können Sie die Gefahr des Datenmissbrauchs einschränken. Gewähren Sie unbekannten Personen nicht ohne weiteres Zugang zum eigenen Profil. Bei manchen SNS können die zugangsberechtigten Personen verschiedenen Kategorien zugeteilt werden (z.B. FreundInnen und KollegInnen). So können Sie Einfluss darauf nehmen, welche NutzerInnen Ihre Inhalte zu Gesicht bekommen.
- Fragen Sie sich vor der Veröffentlichung immer, ob Sie in einem Bewerbungsgespräch mit den entsprechenden Daten konfrontiert werden möchten – und zwar auch noch in zehn Jahren. Schon heute suchen angeblich zwei Drittel der Personalverantwortlichen in SNS und Google nach Informationen über Bewerberinnen und Bewerber. Kontrollieren Sie die Informationen, die Ihre FreundInnen aufschalten und fordern Sie sie auf, unerwünschtes Material zu entfernen.
- Verzichten Sie darauf, Ihre elektronischen Adressbücher in SNS hochzuladen oder abzugleichen, ohne dass die Einwilligung der Betroffenen vorliegt. Verzichten Sie auf das Hochladen und Beschriften von Fotos von Dritten.
- In den SNS können Profile leicht gefälscht werden, was für die Betroffenen sehr unangenehm sein kann. Durchsuchen Sie deshalb das Web regelmässig nach Ihrem Namen und möglichen Profilen. Dazu eignen sich insbesondere die auf SNS spezialisierten Suchmaschinen wie 123people.com und Yasni.de. Sollten Sie fündig werden, können Sie den Betreiber der Website auffordern, die entsprechenden Seiten zu entfernen.
- Rufen Sie sich in Erinnerung, dass Ihr Profil von den SNS gespeichert wird. Sind die Daten einmal auf dem Web, ist es schwierig, die Übersicht über ihre Verwendung zu behalten. Halten Sie sich auch vor Augen, dass von den UserInnen gelöschte Profile manchmal von den Betreibern der SNS zwar deaktiviert, aber nicht entfernt werden.

Schwerpunkt Sensibilisierung

SNS bergen viele Vorzüge für die Gesellschaft, so z. B. die Möglichkeit, Networking zu betreiben, Kontakte über Landesgrenzen hinaus zu knüpfen oder eigene Inhalte zu publizieren. Es ist daher nicht erstrebenswert, sie grundsätzlich zu verurteilen. Das Ziel muss es aus Sicht des Datenschutzes vielmehr sein, Behörden, AnbieterInnen und UserInnen für einen korrekten und datenschutzkonformen Umgang mit Personendaten bei sozialen Netzwerken zu sensibilisieren.●

Endnoten

1 Verbraucher fürchten um den Schutz ihrer Privatsphäre im Internet, www.tinyurl.com/d7b3xyt, Zugriff 14.11.2011.
2 It's the end of the web as we know it, www.tinyurl.com/3uyrucx, Zugriff 17.11.2011.