Facebook - srsly?

Das seit 2004 existierende soziale Netzwerk Facebook erfreut sich auch bei politisch aktiven Menschen noch immer einer grossen Beliebtheit. Leider scheint in den politischen Zusammenhängen jegliches Bewusstsein zu fehlen, was die Folgen einer Nutzung dieser Plattform bedeuten können. Es entsteht sogar oft der Eindruck, dass grundsätzlich im Bezug auf Mediennutzung keine Auseinandersetzung mit den potentiellen Gefahren geführt wird. Auf dem Web2.0 Auge blind, sozusagen.

Die Benutzung von Facebook ist fahrlässig

Es tut uns leid, wenn wir euch das jetzt mal so direkt sagen müssen, aber wir haben uns schon lange genug den Mund fusselig geredet. Mit der Benutzung von Facebook gefährdet ihr euch, die Zusammenhänge in denen ihr aktiv seit und alle anderen AktivistInnen die mit euch oder euren Gruppen in Kontakt treten. Es ist schon klar, wenn ihr euch selbst exponieren wollt, könnt ihr das machen und gefährdet in direkter Folge nur euch selbst. Zu weiteren negativen Folgen eurer persönlichen Post Privacy Attitude lest den letzten Absatz. Aber die Leute die mit euch Kontakt haben (also euer soziales Netzwerk) haben im Fall von Facebook keine Möglichkeit sich zu wehren, sie können keinen Widerspruch dagegen einlegen, dass Infos durch euch über sie bekannt werden.

Das Ziel von Facebook ist es, soviele Daten über euch und eure sozialen Zusammenhänge zu sammeln wie es nur möglich ist. Dies passiert auf verschiedenste Art und Weise und Facebook ist federführend in der Entwicklung von Technologien zur Überwachung von UserInnen und der Zusammenführung und Auswertung von verschiedenen Datenquellen. Und es ist euch als UserInnen nicht möglich, euch gegen die Datensammelwut zu wehren. Weiters stellt Facebook auch Profile über Personen zusammen, die nicht auf Facebook sind. Facebook tut dies jedoch nicht aus Bosheit oder als Spitzeldienst, sondern weil die damit entstehenden Profile die Geschäftsgrundlage von Facebook sind.

Dennoch arbeitet Facebook mit den Behörden eng zusammen. Um das mal ein für alle Mal klarzustellen: "NutzerInnen von Facebook stimmen mit der Annahme der Datenschutzbestimmungen von Facebook automatisch der Nutzung und Verwendung aller Personendaten von mit Facebook kooperierenden Partnern zu. Hierzu gehören [...] auch deutsche und ausländische Polizeibehörden sowie die CIA und staatliche Stellen der USA über den Zugang als Miteigentümer des Netzwerkes." (Quelle: Wikipedia) Ausserdem überwacht Facebook auch die privaten Nachrichten von NutzerInnen: "Facebook hat nach eigenen Angaben bereits mehrfach den Strafverfolgungsbehörden in den USA und anderen Ländern verdächtige Aktivitäten und NutzerInnen gemeldet." (Quelle: Wikipedia)

Mitte 2012 wurde erstmals ein PDF veröffentlicht, das anschaulich macht, welche Daten von Facebook an Ermittlungsbehörden weitergegeben werden. Für zwei Accounts finden sich in den etwa 70 Seiten alle Daten die von dem Accountinhaber/der Accountinhaberin eingegeben wurden: Emailadressen, Instantmessaging Accounts, Geburtsdaten, Geburtsort, Adressen, schulische Laufbahn, gepostete Links, Wallposts, Status Updates, gelöschte Wallposts, die Liste der FreundInnen, die Liste gelöschter FreundInnen, Gruppen, Events (vergangene und zukünftige), Photos, Photos von anderen UserInnen in denen der/die UserIn getagged wurde und alle Seiten die von dem Account in Facebook aufgerufen wurden.

Pseudonyme schützen nicht

Viele Menschen glauben, dass es hilft, sich mittels eines Pseudonyms vor Facebook zu schützen. Das ist jedoch eine gefährliche Fehleinschätzung. Einerseits kann Facebook durch die Verknüpfung von Datenquellen (Adressbücher aus Emailaccounts, Kontaktdaten aus Telephonspeichern) mit Leichtigkeit eure wahre Identität errechnen. Andererseits arbeitet Facebook auch aktiv daran, dass die UserInnen die echten Namen von anderen UserInnen preisgeben. Wenn zum Beispiel jemand euren echten Namen mit eurer pseudonymen Emailadresse verknüpft hat (etwa im GMX Adressbuch) und diese Daten von Facebook importiert werden (was als 'Service' von Facebook angeboten wird) ist es schon vorbei mit der Pseudonymität. Oder wenn UserInnen Gesichter von Menschen in Fotos taggen und damit die Gesichtserkennungsalgorithmen von Facebook füttern.

Der Import von Adresslisten gefährdet auch AktivistInnen, die nicht auf Facebook sind. Damit hat Facebook Zugriff auf Personendaten, ohne dass die Personen jemals eingewilligt haben, dass die Daten zu Facebook gelangen. Und so werden von Menschen soziale Profile angelegt, die nicht auf Facebook sind.

Facebook geht mittlerweile sogar schon soweit, die UserInnen aufzufordern sich gegenseitig zu 'outen'- also die echten Personalien von anderen Accounts zu bestätigen oder aufzudecken. Könnt ihr allen euren Facebookfreundschaften trauen, dass dies nicht passiert? Weiters fordert Facebook von Zeit zu Zeit NutzerInnen auf, ihre Namen durch Ausweise zu belegen. Dieses Vorgehen wird mittlerweile auch bei Instragr.am angewandt, einer Plattform die von Facebook aufgekauft wurde.

Eure Surfgewohnheiten

Facebook beobachtet und speichert nicht nur euer Verhalten auf Facebook selber. In einer Unmenge an Websiten sind 'Like' Buttons eingebunden- durch die Einbindung dieser Buttons kann Facebook nachvollziehen, welche Websiten ihr aufgerufen habt und diese Daten wiederum verwerten.

Weitergabe von Daten zu Werbezwecken

Unter dem Begriff 'Instant Personalization' bezeichnet Facebook die Weitergabe von Daten an Partnerfirmen. Dabei gibt Facebook an Websiten, mit denen ein Abkommen geschlossen wurde, eine Menge an Daten weiter, die von Facebook als 'public information' bezeichnet werden: "name, profile picture, current city, gender, networks, complete list of your friends, and your complete list of connections (formerly the list of pages that you were a "fan" of, but now including profile information like your hometown, education, work, activities, likes and interests, and, in some cases, your likes and recommendations from non-Facebook pages around the web)." (Quelle: EFF) Die Daten können dabei an ganz unterschiedliche Unternehmen weitergegeben werden: Banken/KreditanbieterInnen, potentielle ArbeitgeberInnen etc.

Politische Einflussnahme

Im November 2011 gab es Proteste gegen Seiten auf Facebook, die Vergewaltigung und andere sexualisierte Gewalt abfeierten. Es brauchte eine Petition mit 186000 Unterschriften, damit die Seiten von Facebook nach zwei Monaten entfernt wurden. Im Gegensatz dazu wurde von Facebook selbst in etwa zur selben Zeit die Seite von Women on Waves zensiert, auf der Tips zu Abtreibung gegeben wurden. Es wurde später von Facebook behauptet, dass dies ein Versehen gewesen sei.

Das 'Privileg' von Post Privacy

Wenn ihr Facebook verwendet, tut ihr das oft aus einer privilegierten Position heraus. Durch die Verwendung und Bewerbung von Facebook betreibt ihr eine Normalisierung.

iheartdigitallife.de schreibt zu Post Privacy Experimenten: "[Es] besteht die Gefahr, dass die postprivaten Selbstexperimente nicht als etwas Partikulares angesehen werden, was eine bestimmte Gruppe von Menschen betreibt, sondern als neuer, für alle gültiger gesellschaftlicher Standard. Die Praxen normalisieren sich, wenn sie diese Gruppe von Menschen betreiben. Es werden z.B. Geschäftsideen dazu entwickelt und erwartet, dass alle mitmachen. Wer das nicht will, muss sich zunehmend aktiv dagegen wehren und ist dann die Spaßverderber_in, die sich nicht fotografieren lassen möchte."

Wenn ihr Facebook aktiv verwendet, wird ein Druck auf die Menschen in eurem Umfeld ausgeübt. Termine werden oft nur noch auf Facebook angekündigt (auch politische und/oder von Repression betroffene, wie Demos), wer nicht auf Facebook ist, wird dadurch aus dem sozialen Umfeld ausgeschlossen. Es werden Menschen gezwungen, ihre Privatsphäre aufzugeben, um an einem sozialen Leben teilhaben zu können. Jedoch gerade bei Facebook, wo es einer ständigen Auseinandersetzung mit den technischen Neuerungen bedarf, um die eigenen Daten zu schützen, kann dies gefährliche Folgen haben.

Auf Femgeeks.de steht dazu: "Es ist nicht sonderlich weit her geholt, dass Informationen von Menschen (und insbesondere Frauen) gegen ihren Willen veröffentlicht werden [...]. Tatsächlich gibt es bereits Webseiten die sich auf solche Veröffentlichungen aus Rache (“revenge porn”) spezialiseren, wo Menschen also aus Rache Nacktaufnahmen und Ähnliches ihrer Ex-Partner_innen veröffentlichen. Und es ergeben sich darüber hinaus noch weitere Probleme aus der Öffentlichkeit von Daten, wie zum Beispiel die Verknüpfung von scheinbar harmlosen Informationen, die [...] zu einer realen Gefahr für Frauen bzw. Mädchen werden." Diese reale Gefahr, die von femgeeks.de angesprochen wird, wird durch die ein neues 'Feature' von Facebook, 'Graph Search', noch verstärkt. Damit lassen sich die Informationen von den Facebook UserInnen noch leichter verknüpfen. So kann zum Beispiel nach Ort, Interesse oder Geschlecht gefiltert werden. Suchanfragen sehen dann zum Beispiel so aus: "Single women who live nearby and who are interested in men and like Getting Drunk" oder "Islamic men interested in men who live in Tehran, Iran".

Plötzlich plappern Anna und Arthur
www.nadir.org/news/Plötzlich_plappern_Anna_und_Arthur.html
Du wirst uns nicht auf Facebook finden...
at.indymedia.org/node/19892
Ihr werdet uns immer noch nicht auf Facebook finden
at.indymedia.org/node/20745
Facebook Seite der FSF:
www.fsf.org/facebook

tear the system down - bit. by. bit.
technologie in linksradikalen kontexten
bitbybit@riseup.net
www.bitxbit.es